HP Data Protector A.06.10

Disaster recovery guide

Part number: B6960-96038
First edition: November 2008

Legal and notice information

Printed in the US

Contents

Figures

Tables

Publication history

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

Table 1 Edition history

Part number	Guide edition	Product
B6960-96004	July 2006	Data Protector Release A.06.00
B6960-96038	November 2008	Data Protector Release A.06.10

About this guide

This guide provides information about:

- planning and preparing for a disaster
- testing a disaster recovery procedure
- successfully performing a disaster recovery

Intended audience

This guide is intended for backup administrators responsible for planning, preparing, testing, and executing a disaster recovery, with knowledge of:

- Data Protector concepts
- Data Protector backup and restore procedures

Documentation set

Other documents and online Help provide related information.

Guides

Data Protector guides are available in printed format and in PDF format. Install the PDF files during the Data Protector setup procedure by selecting the `English Documentation & Help` component on Windows or the `OB2-DOCS` component on UNIX. Once installed, the guides reside in the *`Data_Protector_home`*`\docs` directory on Windows and in the `/opt/omni/doc/C` directory on UNIX.

You can find these documents from the Manuals page of the HP Business Support Center website:

http://www.hp.com/support/manuals

In the Storage section, click **Storage Software** and then select your product.

- *HP Data Protector concepts guide*

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

- *HP Data Protector installation and licensing guide*

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

- *HP Data Protector troubleshooting guide*

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

- *HP Data Protector disaster recovery guide*

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

- *HP Data Protector integration guides*

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

  - *HP Data Protector integration guide for Microsoft applications: SQL Server, SharePoint Portal Server, Exchange Server, and Volume Shadow Copy Service*

    This guide describes the integrations of Data Protector with the following Microsoft applications: Microsoft Exchange Server, Microsoft SQL Server, and Volume Shadow Copy Service.

  - *HP Data Protector integration guide for Oracle and SAP*

    This guide describes the integrations of Data Protector with Oracle, SAP R3, and SAP DB/MaxDB.

  - *HP Data Protector integration guide for IBM applications: Informix, DB2, and Lotus Notes/Domino*

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

  - *HP Data Protector integration guide for VMware Virtual Infrastructure, Sybase, Network Node Manager, and Network Data Management Protocol Server*

    This guide describes the integrations of Data Protector with VMware Virtual Infrastructure, Sybase, Network Node Manager, and Network Data Management Protocol Server.

- *HP Data Protector integration guide for HP Service Information Portal*

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

- *HP Data Protector integration guide for HP Reporter*

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

- *HP Data Protector integration guide for HP Operations Manager for UNIX*

  This guide describes how to monitor and manage the health and performance of the Data Protector environment with HP Operations Manager and HP Service Navigator on UNIX.

- *HP Data Protector integration guide for HP Operations Manager for Windows*

  This guide describes how to monitor and manage the health and performance of the Data Protector environment with HP Operations Manager and HP Service Navigator on Windows.

- *HP Data Protector integration guide for HP Performance Manager and HP Performance Agent*

  This guide provides information about how to monitor and manage the health and performance of the Data Protector environment with HP Performance Manager (PM) and HP Performance Agent (PA) on Windows, HP-UX, Solaris, and Linux.

- *HP Data Protector zero downtime backup concepts guide*

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

- *HP Data Protector zero downtime backup administrator's guide*

  This guide describes how to configure and use the integration of Data Protector with HP 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 Data Protector zero downtime backup integration guide*

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

describes how to configure and use Data Protector to perform backup and restore using the Microsoft Volume Shadow Copy Service.

- *HP Data Protector MPE/iX system user guide*

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

- *HP Data Protector Media Operations user's guide*

  This guide provides tracking and management of offline storage media. It describes the tasks of installing and configuring the application, performing daily media operations and producing reports.

- *HP Data Protector product announcements, software notes, and references*

  This guide gives a description of new features of HP Data Protector A.06.10. It also provides information on supported configurations (devices, platforms and online database integrations, SAN, and ZDB), required patches, and limitations, as well as known problems and workarounds. An updated version of the supported configurations is available at http://www.hp.com/support/manuals.

- *HP Data Protector product announcements, software notes, and references for integrations to HP Operations Manager, HP Reporter, HP Performance Manager, HP Performance Agent, and HP Service Information Portal*

  This guide fulfills a similar function for the listed integrations.

- *HP Data Protector Media Operations product announcements, software notes, and references*

  This guide fulfills a similar function for Media Operations.

- *HP Data Protector command line interface reference*

  This guide describes the Data Protector command-line interface, command options and their usage as well as provides some basic command-line examples.

Online Help

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

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

- ***Windows:*** Unzip `DP_help.zip` and open `DP_help.chm`.
- ***UNIX:*** Unpack the zipped tar file `DP_help.tar.gz`, and access the online Help system through `DP_help.htm`.

Documentation map

Abbreviations

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

Abbreviation	Guide
CLI	Command line interface reference
Concepts	Concepts guide
DR	Disaster recovery guide
GS	Getting started guide
Help	Online Help
IG-IBM	Integration guide for IBM applications: Informix, DB2, and Lotus Notes/Domino
IG-MS	Integration guide for Microsoft applications: SQL Server, SharePoint Portal Server, Exchange Server, and Volume Shadow Copy Service
IG-O/S	Integration guide for Oracle and SAP
IG-OMU	Integration guide for HP Operations Manager for UNIX
IG-OMW	Integration guide for HP Operations Manager for Windows
IG-PM/PA	Integration guide for HP Performance Manager and HP Performance Agent
IG-Report	Integration guide for HP Reporter
IG-SIP	Integration guide for HP Service Information Portal
IG-Var	Integration guide for VMware Virtual Infrastructure, Sybase, Network Node Manager, and Network Data Management Protocol Server

Abbreviation	Guide
Install	Installation and licensing guide
MO GS	Media Operations getting started guide
MO RN	Media Operations product announcements, software notes, and references
MO UG	Media Operations user guide
MPE/iX	MPE/iX system user guide
PA	Product announcements, software notes, and references
Trouble	Troubleshooting guide
ZDB Admin	ZDB administrator's guide
ZDB Concept	ZDB concepts guide
ZDB IG	ZDB integration guide

Map

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

	Help	GS	Concepts	Install	Trouble	DR	PA	Integration Guides: MS	O/S	IBM	Var	OV	OVOU	OVOW	ZDB: Concept	Admin	IG	MO: 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															
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 guides for details of the following integrations:

Integration	Guide
HP Operations Manager for UNIX/for Windows	IG-OMU, IG-OMW
HP Performance Manager	IG-PM/PA
HP Performance Agent	IG-PM/PA

Integration	Guide
HP Reporter	IG-R
HP Service Information Portal	IG-SIP
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 Server	IG-MS, ZDB IG
Microsoft Exchange Single Mailbox	IG-MS
Microsoft SQL Server	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

Integration	Guide
Sybase	IG-Var
EMC Symmetrix	all ZDB
VMware	IG-Var

Document conventions and symbols

Table 2 Document conventions

Convention	Element
Blue text: Table 2 on page 19	Cross-reference links and e-mail addresses
Blue, underlined text: http://www.hp.com	website addresses
Italic text	Text emphasis
`Monospace` text	• File and directory names • System output • Code • Commands, their arguments, and argument values
`Monospace, italic` text	• Code variables • Command variables
text	Emphasized monospace text

△ CAUTION:

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

IMPORTANT:

Provides clarifying information or specific instructions.

NOTE:

Provides additional information.

TIP:

Provides helpful hints and shortcuts.

Data Protector graphical user interface

Data Protector provides a cross-platform (Windows and UNIX) graphical user interface. You can use the original Data Protector GUI (Windows only) or the Data Protector Java GUI. For information about the Data Protector graphical user interface, see the online Help.

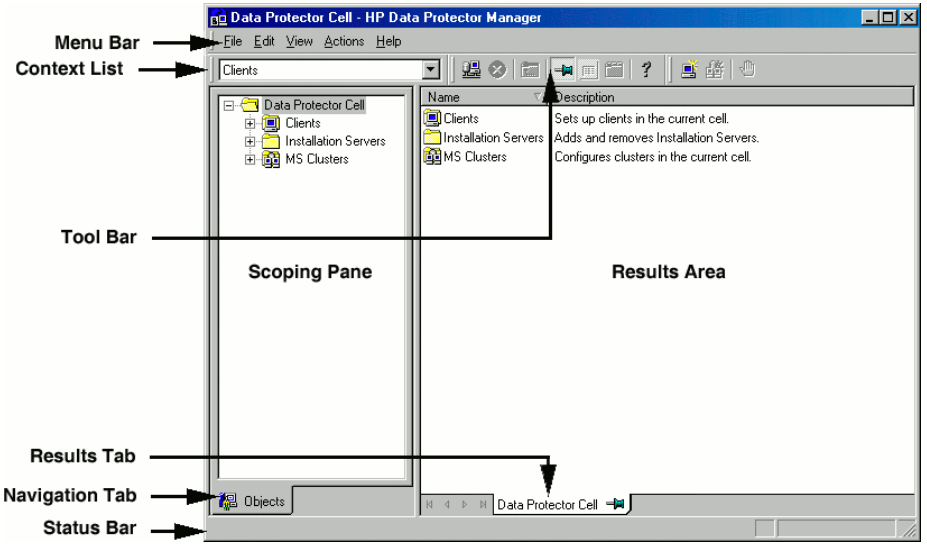


Figure 1 Data Protector graphical user interface

General information

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

HP technical support

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

http://www.hp.com/support

Before contacting HP, collect the following information:

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

Subscription service

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

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

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

HP websites

For additional information, see the following HP websites:

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

Documentation feedback

HP welcomes your feedback.

To make comments and suggestions about product documentation, please send a message to DP.DocFeedback@hp.com. All submissions become the property of HP.

1 Introduction

Overview

This chapter provides a general overview of the disaster recovery process, explains the basic terms used in the Disaster Recovery guide and provides an overview of disaster recovery methods.

A **computer disaster** refers to any event that renders a computer system unbootable, whether due to human error, hardware or software failure, virus, natural disaster, etc. In these cases it is most likely that the boot or system partition of the system is not available and the environment needs to be recovered before the standard restore operation can begin. This includes repartitioning and/or reformatting the boot partition and recovery of the operating system with all the configuration information that defines the environment. *This has to be completed in order to recover other user data.*

Original system refers to the system configuration backed up by Data Protector before a computer disaster hit the system.

Target system refers to the system after the computer disaster has occurred. The target system is typically in a non-bootable state and the goal of Data Protector disaster recovery is to restore this system to the original system configuration. The difference between the crashed and the target system is that the target system has all faulty hardware replaced.

A **boot disk/partition/volume** refers to the disk/partition/volume that contains the files required for the initial step of the boot process, whereas the **system disk/partition/volume** refers to the disk/partition/volume that contains the operating system files.

NOTE:

Microsoft defines the boot partition as the partition that contains the operating system files and the system partition as one that contains the files required for the initial step of the boot process.

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

Auxiliary disk is a bootable disk that has a minimal operating system with networking and Data Protector Disk Agent installed. It can be carried around and used to boot the target system in Phase 1 of Disk Delivery Disaster Recovery of UNIX clients.

Disaster recovery operating system (DR OS) is the operating system environment where the process of disaster recovery is running. It provides Data Protector a basic runtime environment (disk, network, tape and filesystem access). It has to be installed and configured before the Data Protector disaster recovery can be performed.

DR OS can be either temporary or active. **Temporary DR OS** is used exclusively as a host environment for some other operating system restore along with the target operating system configuration data. It is deleted after the target system is restored to the original system configuration. **Active DR OS** not only hosts the Data Protector disaster recovery process but is also a part of the restored system because it replaces it's own configuration data with the original configuration data.

Critical volumes are volumes required to boot the system and Data Protector files. Regardless of the operating system, these volumes are:

- boot volume
- system volume
- Data Protector executables
- IDB (Cell Manager only)

NOTE:

If IDB is located on different volumes than all volumes where IDB resides, are critical.

Apart from the critical volumes stated above, CONFIGURATION is also a part of the critical volumes set for Windows systems. Services are backed up as a part of the CONFIGURATION backup.

Some items included in the CONFIGURATION can be located on volumes other than system, boot, Data Protector or IDB volumes. In this case these volumes are also part of critical volumes set:

- user profiles volume
- Certificate Server database volume on Windows Server
- Active Directory Service volume on domain controller on Windows Server
- quorum volume on Microsoft Cluster Server.

Online recovery is performed when Cell Manager is accessible. In this case most of Data Protector functionalities are available (Cell Manager runs the session, restore sessions are logged in the IDB, you can monitor the restore progress using GUI, etc.).

Offline recovery is performed if the Cell Manager is not accessible (for example, due to network problems, Cell Manager has experienced a disaster, online recovery has failed, etc.). Only standalone and SCSI Library devices can be used for offline recovery. Note that recovery of Cell Manager is always offline.

Remote recovery is performed if all Media Agent systems specified in SRD file are accessible. If any of them fails, disaster recovery process fails over to **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. Note that offline OBDR is always local.

Disaster is always serious, however the following factors can exacerbate the situation:

- The system has to be returned to online status as quickly and efficiently as possible.
- Administrators are not familiar with the required steps to perform the disaster recovery procedure.
- The available personnel to perform the recovery may only have fundamental system knowledge.

Disaster recovery is a complex task that involves extensive planning and preparation before execution. You have to have a well-defined, step-by-step process in place to prepare for, and recover from, disastrous situations.

Disaster recovery process

The **disaster recovery process** consists of 4 phases:

- **Phase 0** (preparation) is the prerequisite for a successful disaster recovery. The planning and preparation must done *before* a disaster occurs.
- In **Phase 1**, DR OS is installed and configured, which usually includes repartitioning and reformatting of the boot partition, since the boot or system partition of the system are not always available and the environment needs to be recovered before normal restore operations can resume.
- The Operating system with all the configuration information that defines the environment with Data Protector (as it was) is restored in **Phase 2**.
- Only after this step is completed, is the restore of applications and user data possible (**Phase 3**).

A well-defined, step-by-step process has to be followed to ensure fast and efficient restore.

Disaster recovery methods

This section provides a general overview of disaster recovery methods. For a list of supported disaster recovery methods for a particular operating system, see the Support Matrices in the *HP Data Protector product announcements, software notes, and references* or on the Web:

http://www.hp.com/support/manuals

NOTE:

Each disaster recovery method has limitations you should consider before implementation.

Table 3 on page 26 provides an overview of the Data Protector disaster recovery methods.

Table 3 Overview of disaster recovery methods

Phase 0	Phase 1	Phase 2	Phase 3
Manual Disaster Recovery			
Full client backup, IDB backup (Cell Manager only). Update SRD file (Windows only). Collect information on the original system to enable installation and configuration of DR OS.	Install DR OS with network support. Repartition the disk and re-establish the original storage structure.	Execute the `drstart` command to automatically recover critical volumes. Additional steps are required to perform advanced recovery tasks.	Restore user and application data using the standard Data Protector restore procedure.
See "Assisted manual disaster recovery of a Windows system" on page 41 or "Manual disaster recovery of a UNIX Cell Manager " on page 123.			
Disk Delivery Disaster Recovery (DDDR)			

Phase 0	Phase 1	Phase 2	Phase 3
Full client backup, IDB backup (Cell Manager only), create auxiliary disk (UNIX only).	***Windows***: Connect a replacement disk to a hosting system. ***UNIX***: Connect the auxiliary disk to the target system. All systems: repartition the replacement disk and re-establish the original storage structure.	***Windows***: Restore critical volumes using DDDR wizard, remove the replacement disk from the hosting system and connect it to the target system. ***UNIX***: Restore the boot disk of the original system onto the replacement disk, remove the auxiliary boot disk. All systems: reboot the system. Additional steps are required to perform advanced recovery tasks.	Restore user and application data using the standard Data Protector restore procedure.
See "Disk Delivery Disaster Recovery of a Windows client " on page 49 or "Manual disaster recovery of a UNIX Cell Manager " on page 123.			
Enhanced Automated Disaster Recovery (EADR)			
Full client backup, IDB backup (Cell Manager only). Prepare and update SRD. Prepare DR CD.	Boot the system from the DR CD and select scope of recovery.	Automatic restore of critical volumes. Additional steps are required to perform advanced recovery tasks.	Restore user and application data using the standard Data Protector restore procedure.
See "Enhanced automated disaster recovery of a Windows system" on page 53.			
One Button Disaster Recovery (OBDR)			
Full client backup using OBDR wizard. Prepare and update SRD.	Boot the target system from the OBDR tape and select scope of recovery.	Automatic restore of critical volumes.	Restore user and application data using the standard Data Protector restore procedure.
See "One Button Disaster Recovery of a Windows system" on page 68.			
Automated System Restore (ASR)			

Phase 0	Phase 1	Phase 2	Phase 3
Full client backup, ASR diskettes with an updated SRD file and DP binaries are prepared.	Boot the system from the Windows installation medium and enter the ASR mode. Provide ASR diskette.	Critical volumes are restored. Additional steps to perform advanced recovery tasks are required.	Restore user and application data using the standard Data Protector restore procedure.
See "Automated System Recovery" on page 81.			

The following has to be completed before you can proceed to the next phase:

- *Phase 0*:

  A full client backup and the IDB backup (Cell Manager only), must be performed, and enough information must be collected by the administrator from the original system to enable installation and configuration of the DR OS. An auxiliary boot disk should be created for Disk Delivery Disaster Recovery on UNIX.

- *Phase 1*:

  DR OS must be installed and configured and the original storage structure must be re-established (all volumes are ready to be restored). The replacement disk for Disk Delivery Disaster Recovery on UNIX must be made bootable.

- *Phase 2*:

  Critical volumes are restored. Additional steps to perform advanced recovery tasks are required. Refer to "Advanced recovery tasks" on page 91.

- *Phase 3*:

  Check if application data is restored correctly (e.g. databases are consistent, etc.)

Manual disaster recovery method

This is a basic and very flexible disaster recovery method that involves recovering the target system to the original system configuration.

First, you need to install and configure the DR OS. Then use Data Protector to restore data (including the operating system files), replacing the operating system files with the restored operating system files.

With manual recovery, it is important to collect the information regarding the storage structure, which is not kept in flat files (such as partition information, disk mirroring, and striping).

Disaster recovery using disk delivery

This method is supported on Windows and UNIX clients.

On Windows clients, the disk of the crashed system (or the replacement disk for the physically damaged disk) is temporarily connected to a hosting system. After being restored, it can be connected to the faulty system and booted.

On UNIX systems, the auxiliary disk with a minimal operating system, networking, and Data Protector agent installed is used to perform Disk Delivery Disaster Recovery.

This is a fast and simple method to recover clients. On Windows systems, the operating system state is restored automatically as well.

TIP:

This method is especially useful with hot swap hard disk drives, because you can disconnect a hard disk drive from a system and connect a new one while the power is still on and the system is operating.

See "Disk Delivery Disaster Recovery of a Windows client " on page 49.

One Button Disaster Recovery (OBDR)

One Button Disaster Recovery (OBDR) is an automated Data Protector recovery method for Windows clients and Cell Manager, where user intervention is reduced to a minimum.

It collects all relevant Windows environment data automatically at backup time. During a full backup, data required for temporary DR OS setup and configuration is packed in a single large OBDR image file and stored on the backup tape. When a disaster occurs, an OBDR device (a backup device, capable of emulating a CD ROM) is used to boot the target system directly from the tape that contains the OBDR image file with disaster recovery information.

Data Protector then installs and configures the disaster recovery operating system (DR OS), formats and partitions the disks and finally restores the original operating system with Data Protector as it was at the time of backup.

IMPORTANT:

You need to prepare a new OBDR boot tape after each hardware, software or configuration change. This also applies to any network configuration changes, such as change of IP address or DNS server.

Automated System Recovery

Automated System Recovery (ASR) is an automated system on Windows systems, which reconfigures a disk to its original state (or resizes the partitions if the new disk is larger than the original disk) in the case of a disaster. This includes disk partitioning and logical volume configuration (file formats, drive letter assignments, volume mountpoints, and volume characteristics). ASR thus enables the Data Protector `drstart.exe` command to install the active DR OS that provides Data Protector disk, network, tape and file system access.

Data Protector then recovers the target system to the original system configuration and finally restores all user data.

Enhanced Automated Disaster Recovery (EADR)

Enhanced Automated Disaster Recovery (EADR) is an automated Data Protector recovery method for Windows clients and Cell Manager, where user intervention is reduced to minimum.

The EADR procedure for Windows platforms collects all relevant environment data automatically at backup time. During configuration backup, data required for temporary DR OS setup and configuration is packed in a single large **DR OS image file** and stored on the backup tape (and optionally on Cell Manager) for each backed up client in the cell.

In addition to this image file, a Phase 1 startup information (stored in the **P1S** file), required for correct formatting and partitioning of the disk is stored on the Cell Manager. When a disaster occurs, EADR wizard is used to restore the DR OS image from the backup medium (if it has not been saved on the Cell Manager during the full backup) and convert it to a **disaster recovery CD ISO image**. CD ISO image can then be burned on a CD using any burning tool and used to boot the target system.

Data Protector then automatically installs and configures DR OS, formats and partitions the disks and finally recovers the original system with Data Protector as it was at the time of backup.

IMPORTANT:

Perform a new backup and prepare a new DR CD after each hardware, software or configuration change. This also applies to any network configuration changes, such as change of IP address or DNS server.

The recovered volumes are:

- the boot partition
- the system partition
- the partitions containing Data Protector

Any remaining partitions can be recovered using the standard Data Protector recovery procedure.

Data Protector integrations and disaster recovery

Disaster recovery is a very complex process that involves products from several vendors. As such, successful disaster recovery depends on all the vendors involved. Use the information provided here only as a guideline.

Check the instructions of the database/application vendor on how to prepare for disaster recovery.

This is a general procedure on how to recover an application:

1. Perform Disaster Recovery.
2. Install, configure, and initialize the database/application so that data on Data Protector media can be loaded back to the system. Consult database/application vendor documentation for a detailed procedure and steps needed to prepare the database.
3. Ensure that the database/application server has the required Data Protector client software installed and is configured for the database/application. Follow the procedures in the appropriate HP Data Protector integration guide.
4. Start the restore. When the restore is complete, follow the instructions of the database/application vendor for any additional steps required to bring the database back online.

2 Planning and preparing for a disaster recovery

In this chapter

Carefully follow the instructions in this chapter to prepare for a disaster recovery and to ensure fast and efficient restore. Preparation does not depend on the disaster recovery method, however, it does include developing a detailed disaster recovery plan, performing consistent and relevant backups and updating the SRD file on Windows.

This chapter contains the general preparation procedure for disaster recovery for all disaster recovery methods. Additional preparation is required for each particular disaster recovery method. Refer to corresponding sections for additional preparation steps.

Planning

Developing a detailed disaster recovery plan has a major impact on the success of a disaster recovery. To deploy disaster recovery in a large environment with many different systems, proceed as follows:

1. **Plan**

   Planning must be prepared by IT administration and should include the following:

   - Determine the systems that need to be recovered as well as the time and level of recovery. Critical systems are all systems required for network to function properly (DNS servers, domain controllers, gateways, etc.), Cell Managers and Media Agent clients.
   - Determine a recovery method to be used (impacts the required preparations).
   - Determine a method to obtain the required information at recovery time, such as the media that holds the IDB, location of updated SRD file and location and labels of the Cell Manager backup media.
   - Create a step-by-step detailed checklist to guide you through the process.
   - Create and execute a test plan to confirm that the recovery will actually work.

2. **Prepare for recovery**

   Depending on the recovery method to be used, the preparation should include:

   UNIX:

   - Creation of tools, such as the auxiliary disk with the minimum operating system, network resources, and the Data Protector Disk Agent installed.
   - Creation of pre-execution scripts, which collect the storage structure and other client-specific preparations.

   Windows:

   - Updating **System Recovery Data (SRD)** and storing it to a safe place. You should restrict access to SRD files due to security reasons.

   All systems:

   - Performing regular and consistent backups.

3. **Perform recovery procedures**

   Follow the procedures and checklists you have tested to recover the crashed system.

Consistent and relevant backup

In the case of a disaster, the target system should be put back into the state it was at the time of the last valid known backup. Additionally, the system should function as it had functioned just before the last valid backup performance.

NOTE:

On UNIX systems, some daemons or processes are active as soon as the system finishes booting, for various reasons (HP-UX example: License server at run level-2). Such an early process may even read the data into memory and write a “dirty flag” into some file while it runs. A backup taken at the standard operating stage (the standard run level-4) cannot be expected to yield a problem-free restart of such an application. To follow the example, the license server, if started after such a pseudo recovery, will realize that the data read from the file is inconsistent and will refuse to run the service as expected.

On Windows, while the system is up and running, many system files cannot be replaced because the system keeps them locked. For example, the user profiles that are currently being used cannot be restored. The login account has to be changed or the relevant service has to be stopped.

Data consistency of an application can be violated depending on what is active on the system when the backup runs, thereby causing re-start and execution issues after recovery.

Creating a consistent and relevant backup

- Ideally, you would perform a backup with the relevant partition(s) set off-line, which is usually not possible.
- Examine the activity on the system during the backup. Only operating system related processes and database services which are backed up online can remain active during the backup execution.
- None of the low-level (UNIX) or background-level (Windows) application specific services should be running.

What should be included in the consistent and relevant backup depends on the disaster recovery method you plan to use and other system specifics (for example, disaster recovery of Microsoft Cluster). See the sections pertaining to particular disaster recovery methods.

Encrypted backups

If your backups are encrypted, you must ensure that the encryption keys are safely stored and available when you start a disaster recovery. Without the access to the appropriate encryption key, the disaster recovery procedure aborts.

Data Protector A.06.10 introduces changes in the encryption model compared to Data Protector A.06.00. The encryption keys are stored on the Cell Manager so the disaster recovery client must either be connected to the Cell Manager to get the encryption key or you must provide the encryption key on a removable medium. For details on encryption concepts, see the online Help index: "encryption".

Two disaster recovery scenarios are possible:

- Recovery of a client where you can establish a connection to the Cell Manager. No additional encryption-related preparations are needed for such a scenario, as Data Protector automatically obtains the encryption keys.
- Disaster recovery of a Cell Manager or standalone client recovery, where you cannot establish a connection to the Cell Manager. You must provide the encryption keys when prompted.

  The keys are not part of the disaster recovery ISO image and are exported to the key file. You must manually store the keys to a separate removable media. Ensure that you have always an appropriate copy of the keys for each backup that is prepared for disaster recovery. If the encryption key is not available, disaster recovery is not possible.

Updating and editing the system recovery data (SRD)

System recovery data (SRD) is a Unicode text file that contains information required for the configuration and restore of the Windows target system. A SRD file is generated when CONFIGURATION backup is performed on a Windows client and then stored in:

- On a Windows Cell Manager:
  Data_Protector_home\Config\server\dr\srd
- On a UNIX Cell Manager: /etc/opt/omni/server/dr/srd/

IMPORTANT:

When IDB is not available, information about objects and media is stored only in SRD file.

The SRD filename on the Cell Manager is identical to the hostname of the computer where it was generated - for example computer.company.com.

After the CONFIGURATION backup, the SRD contains only system information required for installation of the DR OS. In order to perform a disaster recovery, additional information about backup objects and corresponding media must be added to the

SRD. The SRD can be updated only on a Windows client. The name of the updated SRD file is `recovery.srd`.

There are three different methods possible for updating the SRD file:

- Update SRD File wizard
- `omnisrdupdate` command as a standalone utility
- `omnisrdupdate` command as a backup session post-exec script

Updating using the SRD update wizard

To update the SRD file using the Update SRD File wizard, proceed as follows:

1. In the Data Protector Manager switch to the Restore context and then click the **Tasks** Navigation tab.
2. In the Scoping Pane of the Tasks Navigation tab, check the **Disaster Recovery**.
3. In the Results Area, check the **SRD File Update** option button, select the client and click **Next**.
4. For each of the critical objects, select an object version and click **Next**.
5. Type the destination directory where the updated SRD file is to be placed and click **Finish**.

IMPORTANT:

Because the SRD file is saved on the Cell Manager system, it is not accessible if the Cell Manager fails. As a result, you need an additional copy of the Cell Manager's SRD which should be stored in a vault. In addition to the Cell Manager, you should save the updated SRD file to several secure locations as a part of the disaster recovery preparation policy. See "Preparation" on page 51.

Updating using omnisrdupdate

It is also possible to update the SRD file using the `omnisrdupdate` command as a standalone command. The `omnisrdupdate` command is located in the *`Data_Protector_home`*`\bin` directory.

`Omnisrdupdate` requires a session_ID to update an existing SRD file with backup object information belonging to the given session. Using this value, `omnisrdupdate` will update the SRD file with the backup object information which belongs to the

passed session_ID value. After the SRD is updated it will be saved back on the Cell Manager.

This procedure will only succeed if all critical backup objects (as specified in the SRD file) were actually backed up during the specified session. To view which objects are considered as critical for the SRD update, open the SRD file in a text editor and find the objects section. All critical objects for the SRD update are listed there. Note that the database is represented as "/".

Here is an example of an objects section of the SRD file:

```
-section objects
-objcount 3
-object /C -objtype 6 -objpurpose 283
-endobject /C
-object / -objtype 3 -objpurpose 32
-endobject /
-object /CONFIGURATION -objtype 6 -objpurpose 4
-endobject /CONFIGURATION
-endsection objects
```

In this case, there are 3 critical objects: /C, / (database) and /CONFIGURATION.

TIP:

To obtain the session ID, execute the omnidb command with the option -session. To obtain the latest session ID, at the command prompt type omnidb -session -latest.

The updated SRD file should be kept in a safe place so that it is not lost in the case of disaster. To locate where the updated SRD file will be saved, use the -location option with the omnisrdupdate command. There can be more than one -location parameters specified (including network shares on which you have write permission), each of which will receive an updated copy of the SRD file. See "Preparation" on page 51.

To determine for which hostname the SRD file from the Cell Manager should be updated, use the option -host with the command omnisrdupdate. If you don't specify the hostname, the local host is assumed. SRD file on the Cell Manager is not updated.

Example

To update the SRD file with the backup object information which belongs to a session 2002/05/02-5 for the client with the hostname computer.company.com and to

store an updated copy of the SRD file on the floppy disk and in the `SRDfiles` share on computer with the hostname `computer`2, type

```
omnisrdupdate -session 2002/05/02-5 -host computer.company.com
-location a: -location
```

```
\\computer2\SRDfiles
```

Make sure that you have the write permission on that share.

Updating using a post-exec script

Another method to update the SRD is using the `omnisrdupdate` command as a backup post-exec script. To do so, either modify an existing backup specification or create a new one. Perform the following steps to modify a backup specification so that the SRD file is updated with information about backed up objects when the backup session stops:

1. In the Backup context, expand the Backup Specifications item and then Filesystem.
2. Select the backup specification that you would like to modify (it must include all backup objects marked as critical in the SRD file, otherwise the update will fail. It is recommended to perform the client backup with disk discovery) and click **Options** in the Results Area.
3. Click the **Advanced** button under the Backup Specification Options.
4. Type `omnisrdupdate.exe` in the post-exec text box.
5. In the On client drop down list, select the client on which this post-exec script will be executed and confirm with **OK**. This should be the client that was marked for backup on the source page.

When `omnisrdupdate` command is executed as a post-exec utility, the session ID is obtained automatically from the environment and the user is not required to specify the session ID.

All other options can be specified the same way as with the standalone utility (`-location` *`path`*, `-host` *`name`*).

Editing the SRD file

It is possible, that the information about backup devices or media stored in the SRD file is out of date at the time disaster recovery is being performed. In this case edit the SRD file to replace the incorrect information with the relevant information before performing the disaster recovery. See "Recovery using an edited SRD file" on page 103.

IMPORTANT:

You should restrict access to the SRD files due to security reasons.

3 Disaster recovery for Windows

Assisted manual disaster recovery of a Windows system

The following sections explain how to prepare and execute an Assisted Manual Disaster Recovery on Windows systems. For details on supported operating systems, refer to the *HP Data Protector product announcements, software notes, and references.*

Overview

The general procedure for Assisted Manual Disaster Recovery of a Windows client is:

1. **Phase 0**
   a. Perform a full client backup and an IDB backup (Cell Manager only).
   b. Update the SRD file. Collect information on the original system to enable installation and configuration of the DR OS.
2. **Phase 1**
   a. Replace the faulty hardware.
   b. Reinstall the operating system. (Create and format the necessary partitions).
   c. Reinstall service packs.
   d. Manually re-partition the disk and re-establish the storage structure with original drive letter assignments.

TIP:

You can combine Phase 1 of Manual Disaster Recovery with automated deployment tools.

3. **Phase 2**
   a. Execute the Data Protector `drstart.exe` command that will install the DR OS and start the restore of critical volumes.
   b. The computer must be rebooted after the `drstart` command finishes.
   c. Additional steps are required if you are recovering a Cell Manager or performing advanced recovery tasks. Refer to "Advanced recovery tasks" on page 91 for more information.
4. **Phase 3**
   a. Use the Data Protector standard restore procedure to restore user and application data.

Requirements

- The partitions have to be the same size or larger than the partitions on the failed disk. This way the information stored on the failed disk can be restored to the new one. Also, the type of filesystem and compression attributes of the volumes must match (FAT, NTFS).
- The hardware configuration of the target system must be the same as of the original system. This includes SCSI BIOS settings (sector remapping).
- If there were volume mounts points created before disaster, these mount points must be recreated before starting the disaster recovery procedure as volume mount points are not restored automatically. If the mount points are not recreated, data might be restored to wrong location.

Limitation

- Internet Information Server (IIS) Database, Terminal Services Database and Certificate Server Database are not restored automatically during Phase 2. They can be restored on the target system using the standard Data Protector restore procedure.

Preparation

To prepare for a successful disaster recovery, you should follow the instructions related to the general preparation procedure together with the specific method requirements. Advance preparation is essential to perform the disaster recovery fast and efficiently. You should also give special attention to the disaster recovery preparation of the Cell Manager and Microsoft Cluster Server.

△ CAUTION:

It is too late to prepare for a disaster recovery once a disaster has occurred.

See also "Planning" on page 33, for the general preparation procedure for all disaster recovery methods before completing the steps listed in this section. To recover from a disaster quickly and efficiently, consider the following steps and prepare your environment accordingly:

1. You need a Windows bootable installation CD-ROM to enable your system to start from the CD-ROM. If you do not have a bootable CD-ROM, use the standard procedure for booting the computer from diskettes.
2. Ensure that you have drivers for the system you want to recover. You may need to install some drivers, such as network, HBA and SCSI drivers during Windows Setup.
3. To recover the crashed system, you need the following information about the system before the disaster (stored also in the SRD file):
   - If DHCP was not used before the disaster, the TCP/IP properties (IP address, Default gateway, Subnet mask and DNS order)
   - Client properties (Hostname)

4. Ensure that the following is true:
   - You should have a successful full client backup. See
     See the online Help index: “backup, Windows specific” and “backup, configuration”.
   - You should have a SRD file updated with information about backed up objects in the chosen successful backup session. See “Updating and editing the system recovery data (SRD)” on page 36.
   - In the case of a Cell Manager recovery, you need a successful IDB backup of the Cell Manager. See the online Help index: “IDB, configuration” for more information on how to configure and perform a IDB backup.
   - In case of Microsoft Cluster Server, consistent backup includes (in the same backup session):
     - all nodes
     - administrative virtual server (defined by the administrator)
     - if Data Protector is configured as a cluster aware application, Cell Manager virtual server and IDB.

     See “Restoring the Microsoft Cluster Server specifics” on page 91 for details.
   - The disk with the boot partition requires free disk space that is needed for the Data Protector disaster recovery installation (15 MB) and active DR OS installation. Additionally, you also need as much free disk space, as required for the restore of the original system.
5. Copy the contents of *Data_Protector_home*\Depot\DRSetup or \i386\tools\DRSetup (located on Data Protector installation medium) for 32 bit Windows Client or Cell Manager on three floppy disks (**drsetup diskettes**) or *Data_Protector_home*\Depot\DRSetup64 or \i386\tools\DRSetup64 (Data Protector installation medium) for 64 bit Windows systems on four floppy disks. In case of a disaster, save the updated SRD file of the crashed client to the first floppy disk (disk1). Only one set of drsetup diskettes is required per site for all Windows systems, but you must always copy an updated SRD file of the crashed client on the first floppy disk. If multiple SRD files are found, Data Protector will ask you to select the appropriate version.

6. In order to re-create disk partitions to their initial state prior to the disaster, record the following information for each partition (it will be needed during the recovery process):
   - partitions length and order
   - drive letters assigned to the partitions
   - partitions filesystem type

   This information is stored in the SRD file. The `-type` option in the diskinfo section of the SRD file shows the partition filesystem type for a particular partition:

Table 4 How to determine the filesystem type from the SRD File

Type number	Filesystem
1	Fat12
4 and 6	Fat32
5 and 15	Extended partition
7	NTFS
11 and 12	Fat32
18	EISA
66	LDM partition

The table on the next page is an example of the preparation for the disaster recovery. Note that data in the table belongs to a specific system and cannot be used on any other system. Refer to "Windows manual disaster recovery preparation template" on page 143 for an empty template which can be used when preparing for the Assisted Manual Disaster Recovery.

Table 5 Example of the AMDR preparation template

Client properties	computer name	ANDES
	hostname	andes.company.com
Drivers		hpn.sys, hpncin.dll
Windows Service Pack		Windows SP3
TCP/IP properties	IP address	3.55.61.61

	default gateway	10.17.250.250
	subnet mask	255.255.0.0
	DNS order	11.17.3.108, 11.17.100.100
Medium label / Barcode number		“andes - disaster recovery” / [000577]
Partition information and order	1st disk label	
	1st partition length	31 MB
	1st drive letter	
	1st filesystem	EISA
	2nd disk label	BOOT
	2nd partition length	1419 MB
	2nd drive letter	C:
	2nd filesystem	NTFS/HPFS
	3rd disk label	
	3rd partition length	
	3rd drive letter	
	3rd filesystem	

Recovery

Follow the procedure below to recover a Windows system using Assisted Manual Disaster Recovery. If you are performing advanced recovery tasks (such as disaster recovery of a Cell Manager or IIS), see also “Advanced recovery tasks” on page 91.

1. Install the Windows system from the CD-ROM and install additional drivers if needed. The Windows operating system has to be installed on the same partition as prior to the disaster. Do not install the Internet Information Server (IIS) during the installation of the system. Refer to "Restoring Internet Information Server (IIS) specifics" on page 101 for more details.

IMPORTANT:

If Windows has been installed using the Windows unattended setup, use the same script now to install Windows to ensure that the `$SystemRoot$` and `\Documents and Settings` folders are installed to the same position.

2. When the Windows Partition Setup screen appears, proceed as follows:
   - If an vendor-specific partition (e.g. EISA Utility Partition) existed on the system before the crash, create (if it does not exist due to the crash) and format a "dummy" FAT partition using the EUP information gathered from the SRD file. The EUP will be later on recovered to the space occupied by the "dummy" partition. Create and format a boot partition immediately after the "dummy" partition. To do this, you need the data as described in "Preparation" on page 51.
   - If an EUP did not exist on the system before the crash, create (if the boot partition does not exist due to the crash) and format the boot partition as it existed on the disk before the crash. To do this, you need the data as described in "Preparation" on page 51.

   Install Windows into its original location, i.e. the same drive letter and directory as in the original system before the disaster. This information is stored in the SRD file.

NOTE:

During the installation, do not add the system to the previous location where the Windows domain resided, but add the system to a workgroup instead.

3. Install TCP/IP protocol. If DHCP was not used before the disaster, configure the TCP/IP protocol as prior to the disaster by providing the following information: hostname of the crashed client, its IP address, default gateway, subnet mask and DNS server. Make sure that the field labeled `Primary DNS suffix of this computer` contains your domain name.

NOTE:

By default, Windows install the Dynamic Host Configuration Protocol (DHCP) during the Windows setup.

4. Create a new temporary disaster recovery account in the Windows Administrators group and add it to the Data Protector admin group on the Cell Manager. See the online Help index "adding Data Protector users".

   The account must not have existed on the system before the disaster. The temporary *Windows* account will be removed at a later time during this procedure.

5. Log off and log in to the system using the newly created account.

6. If the information in the SRD file is not up to date (for example, because you changed the backup device after the disaster) and you are performing an offline recovery, edit the SRD file before continuing with this procedure. See "Recovery using an edited SRD file" on page 103.

7. Run the `drstart.exe` command from the *`Data_Protector_home`*`\Depot\drsetup\Disk1` (Windows Cell Manager) or `\i386\tools\drsetup\Disk1` (Data Protector installation medium) directories. If you have prepared the drsetup diskettes (see "Preparation" on page 42), you can also execute the `drstart.exe` command from the first diskette.

8. `Drstart.exe` first scans the current working directory, floppy and CD drives for the location of disaster recovery setup files (`Dr1.cab` and `omnicab.ini`). If the required files are found, the `drstart` utility installs the disaster recovery files in the *`%SystemRoot%`*`\system32\OB2DR` directory. Otherwise enter their path in the `DR Installation Source` text box or browse for the files.

9. If the `recovery.srd` file is saved in the same directory as `dr1.cab` and `omnicab.ini` files, `drstart.exe` copies `recovery.srd` file to the `%SystemRoot%\system32\OB2DR\bin` directory and the `omnidr` utility is started automatically. Otherwise, enter the location of SRD file (`recovery.srd`) in the `SRD Path` field or browse for the file. Click `Next`.

   If multiple SRD files are found on the floppy disk, Data Protector will ask you to select an appropriate version of the SRD file.

   After `omnidr` successfully finishes, all critical objects required for a proper boot of the system are restored.

10. Remove the temporary *Data Protector* user account (added in step Step 4) from the Data Protector admin group on the Cell Manager, unless it existed on the Cell Manager before the disaster recovery.
11. Reboot the computer, log on and verify that the restored applications are running.
12. Additional steps are required if you are recovering a Cell Manager or performing advanced recovery tasks (such as restoring MSCS or IIS, editing the `kb.cfg` and SRD files). See "Restoring the Data Protector Cell Manager specifics " on page 98 and "Advanced recovery tasks" on page 91 for more information.
13. Use Data Protector to restore user and application data.

The temporary DR OS will be deleted after the first login except in the following cases:

- You have interrupted the Disaster Recovery wizard during the 10 seconds pause after it has found the DR installation and SRD file on the backup medium, and have selected the **Debugs** option.
- You have manually started the `omnidr` command with the `no_reset` or `debug` options.
- Disaster recovery fails.

Disk Delivery Disaster Recovery of a Windows client

To perform the Disk Delivery Disaster Recovery, use a working Data Protector client (Data Protector disaster recovery host) to create the new disk while connected to this client. The administrator has to ensure before the disaster that enough data is collected to correctly format and partition the disk. However, Data Protector automatically stores the relevant information as part of the configuration backup.

The recovered partitions are:

- the boot partition

- the system partition
- the partitions containing Data Protector

Any remaining partitions can be recovered by using the standard Data Protector recovery procedure.

For details on supported operating systems, refer to the *HP Data Protector product announcements, software notes, and references.*

TIP:

This method is specially useful with hot swap hard disk drives, because you can disconnect a hard disk drive from a system and connect a new one while the power is still on and the system is operating.

Overview

The general steps using the Disk Delivery method for a Windows client are:

1. **Phase 0**
   a. Perform a full client backup and an IDB backup (Cell Manager only).
   b. Gather the necessary information about each partition.
2. **Phase 1**
   a. Connect the replacement disk to a hosting system.
   b. Manually re-partition the replacement disk and re-establish the storage structure. For information on Windows mountpoints, see the online Help.
3. **Phase 2**
   a. Use the Data Protector Disk Delivery wizard to restore the critical disks of the original system onto the replacement disk.
   b. Shut down the hosting system, remove the replacement disk and connect it to the target system. You do not need to shut down the system if you are using a hot-swappable hard disk drive.
   c. Reboot the target system from the replaced disk.
4. **Phase 3**
   a. Use the Data Protector standard restore procedure to restore user and application data.

Requirements

- The partitions have to be the same size or larger than the partitions on the failed disk. This way the information stored on the failed disk can be restored to the new one. Also, the type of filesystem format has to match (FAT, NTFS).
- The system on which the disk is created and the system in which the disk is used have to use the same sector mapping/addressing (SCSI BIOS enabled/disabled; EIDE: both systems have to use the same addressing mode: LBA, ECHS, CHS).

Limitations

- Disk Delivery Disaster Recovery is not supported for Microsoft Cluster Server.
- RAID is not supported. This includes software RAIDs (fault-tolerant volumes and dynamic disks).
- Internet Information Server (IIS) Database, Terminal Services Database and Certificate Server Database are not restored automatically during Phase 2. They can be restored on the target system using the standard Data Protector restore procedure.

Preparation

Complete a few steps in order to prepare for disaster recovery. See also "Planning" on page 33, for the general preparation procedure for all disaster recovery methods before completing the steps listed in this section.

IMPORTANT:

Prepare for disaster recovery *before* a disaster occurs.

In order to recover from a disaster quickly, efficiently and effectively, you need the following:

- The last valid known full backup of the client that you want to recover.
- A new hard disk to replace your crashed disk.
- A Data Protector hosting system, which has to be of the same operating system as the crashed client and must have the same hardware I/O path required to connect the new disk.

In order to re-create disk partitions to their initial state prior to the crash, record the following information for each partition (it will be needed during the recovery process):

- partitions length and order
- drive letters assigned to the partitions
- partitions filesystem type

You can refer to Table 5 on page 45 as an example of the preparation for the Disk Delivery disaster recovery. Refer to "Windows manual disaster recovery preparation template" on page 143 for an empty template which can be used when preparing for the Disaster Recovery.

Recovery

This section provides the procedure for recovering your Windows client using the Disk Delivery method. See also "Advanced recovery tasks" on page 91

With the Disk Delivery method on Windows, use a Data Protector disaster recovery host (DR host) to restore the last valid known full backup of your crashed disk to a new hard disk connected to the client. Then replace your crashed disk on the faulty system with this new hard disk.

The actual Disk Delivery Disaster Recovery procedure consists of the following steps:

1. Connect the new disk to a DR host.
2. Reboot the DR host to recognize the new disk.
3. Use Data Protector GUI on disaster recovery host and switch to the Restore context and click the Tasks tab. Select the **Disaster Recovery** item in the Scoping Pane, select the client from the drop down list and check the **Disaster recovery with disk delivery** in the Results Area.
4. For each of the critical objects, select an object version that will be restored and click **Next**.
5. If partitioning has not already been done, partition the new disk using the Disk Administrator. Use the partition information you have gathered as part of the preparation for Disk Delivery disaster recovery.

6. When partitioning the system, assign partitions in the same order as prior to the time that the full backup was performed. This simplifies drive letter reassignment after the restore and prevents a possibility of failure at system restart because of an inappropriate path to the system partition in the `boot.ini` file.

IMPORTANT:

Assign drive letters for Windows mountpoints. In this case you must have enough unassigned drive letter available in order to be able to assign a drive letter for each mount point.

7. Perform all necessary drive letter mappings by right clicking on the original drive letter. This is necessary because drive letters on hosting and original system can be different.
8. Press **Finish**.
9. Remove the new disk from the DR host, and then connect it to the target system.
10. Power on the target system.
11. Use the standard Data Protector restore procedure to restore user and application data. This completes the recovery of the client.

Disk Delivery can also be a valuable method in case one of disks in a multi boot system has crashed, and the user can still boot at least one configuration.

NOTE:

Data Protector does not restore volume-compression flag after recovery. All files, that were compressed at backup time, will be restored as compressed but you will have to manually set volume compression if you want any new files created to be compressed as well.

Enhanced automated disaster recovery of a Windows system

Data Protector offers an enhanced disaster recovery procedure for the Windows Cell Manager and clients. For details on supported operating systems, refer to the *HP Data Protector product announcements, software notes, and references*.

EADR collects all relevant environment data automatically at backup time. During a full backup, data required for the temporary DR OS setup and configuration is packed in a single large **DR OS image file** and stored on the backup tape (and optionally on the Cell Manager) for each backed up client in the cell.

In addition to this image file, a **Phase 1 Startup file** (P1S file), required for correct formatting and partitioning of the disk is stored on a backup medium and on the Cell Manager. When a disaster occurs, the Enhanced Automated Disaster Recovery wizard is used to restore the DR OS image from the backup medium (if it has not been saved on the Cell Manager during the full backup) and convert it into a **disaster recovery CD ISO image**. The CD ISO image can be burned on a CD using any CD burning tool and used to boot the target system.

Data Protector then automatically installs and configures the DR OS, formats and partitions the disks, and finally recovers the original system with Data Protector as it was at the time of backup.

IMPORTANT:

It is recommended to restrict access to backup media, DR images, SRD files and disaster recovery CDs.

Overview

The general steps using the Enhanced Automated Disaster Recovery method for a Windows client are:

1. **Phase 0**
   a. Perform a full client backup.
   b. Use the Enhanced Automated Disaster Recovery wizard to prepare a DR CD ISO image from the DR OS image file of the crashed system and burn it on a CD. If the DR OS image has not been saved on the Cell Manager during the full backup, the Enhanced Automated Disaster Recovery wizard will restore it from the backup medium.

IMPORTANT:

You need to perform a new backup and prepare a new DR CD after each hardware, software, or configuration change. This also applies to any network changes, such as a change of IP address or DNS server.

c. If the full client backup was encrypted, store the encryption key on a removable medium so that it is available for disaster recovery. You will need the key for a Cell Manager recovery or if the connection to the Cell Manager cannot be established.

2. **Phase 1**
   a. Replace the faulty hardware.
   b. Boot the target system from the disaster recovery CD and select the scope of recovery. This is a completely unattended recovery.
3. **Phase 2**
   a. Critical volumes (the boot partition, the operating system and the partition containing Data Protector) are automatically restored.
4. **Phase 3**
   a. Use the standard Data Protector restore procedure to restore user and application data.

IMPORTANT:

Prepare a disaster recovery CD in advance for any critical systems that must be restored first (especially DNS servers, Cell Managers, Media Agent clients, file servers, etc.).

Prepare removable media containing encryption keys in advance for Cell Manager recovery.

The following sections explain the limitations, preparation, and recovery that pertains to EADR of the Windows clients. See also "Advanced recovery tasks" on page 91.

Requirements

Before selecting this method of disaster recovery, consider the following requirements and limitations:

- The Data Protector Automatic Disaster Recovery component must be installed on clients for which you want to enable recovery using this method and on the system, where the DR CD ISO image will be prepared. See the *HP Data Protector installation and licensing guide*.
- The hardware configuration of the target system must be the same as of the original system. This includes SCSI BIOS settings (sector remapping).
- Replacement disks have to be attached to the same host bus adapter on the same bus.

- The boot partition (on which the DR OS is installed) must be larger than 200 MB or disaster recovery will fail. If you enabled the Compress drive option to save disk space option on the original partition, you must have 400 MB free.
- During the EADR preparation, the partition on which Data Protector is installed should have at least 200 MB of temporary free space. This space is required to create a temporary image.
- All drivers required for boot must be installed under `%SystemRoot%` folder. If not, they must be specified in the file `kb.cfg`. See "Editing the kb.cfg file" on page 102.
- Network must be available when you boot the system in Safe Mode with Networking or in Directory Services Restore Mode (Domain Controller only), but you must perform the backup of the system after it was booted with the normal boot process.
- The system's BIOS must support bootable CD extensions as defined in the El-Torito standard and read/write access to hard disk drive using LBA addressing via INT13h function XXh. The BIOS options can either be checked in the user's manuals of the system or by inspecting the system setup before the boot.
- When backing up the client, the default 64 kB block size should be used to write to the device if you plan to perform an offline restore. This is the only default block size available on Windows when performing disaster recovery. To verify that the default 64 kB block size is set, choose **Advanced** in the Properties box, as shown in Figure 2 on page 57.

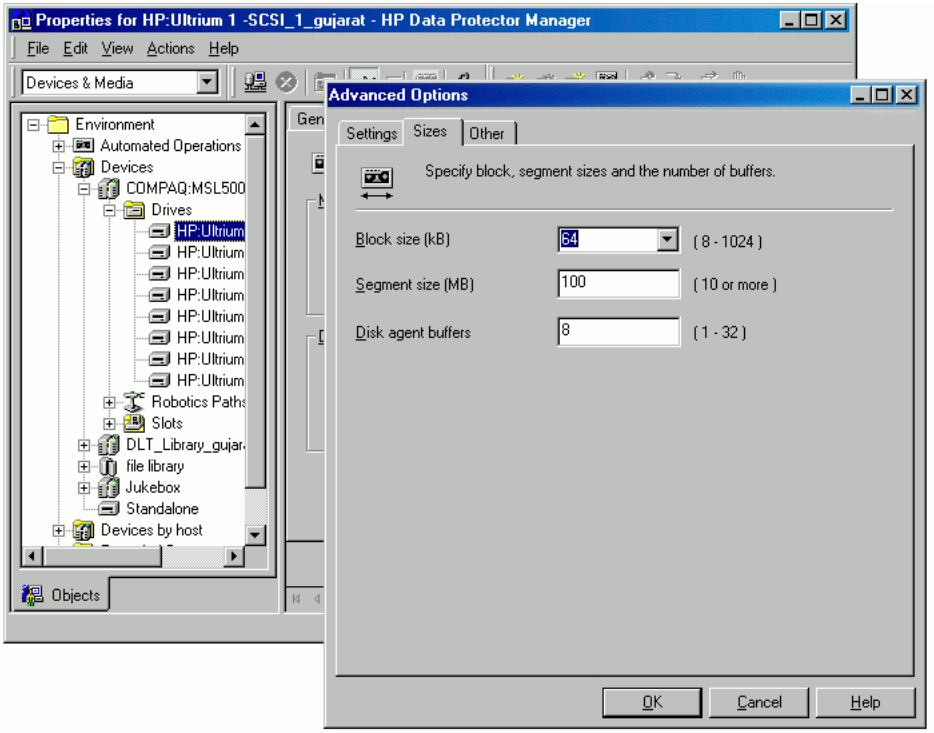


Figure 2 Verifying the default block size

- A backup of all necessary data for disaster recovery may require a significant amount of free space. While normally 500 MB is enough, up to 1 GB may be required depending on the operating system.
- In a cluster environment, a cluster node can be successfully backed up if the bus address enumeration on each cluster node is the same. This means that you need:
  - an equal cluster node motherboard hardware
  - the same OS version on both nodes (service packs and updates)
  - the same number and type of bus controllers
  - bus controllers must be inserted in the same PCI motherboard slots.
- For Windows XP, if the operating system was not activated at the time of the backup and the activation period expires, disaster recovery fails.
- When creating an ISO CD image from an AES encrypted backup, the `kms_allow_hosts` file must be present unless the image is prepared on the Cell Manager and contain the fully qualified domain name of the client for which

the image is prepared. See "ISO image creation for an AES encrypted backup fails if kms_allow_hosts file is missing" on page 139.

- To create an ISO CD image for Windows Vista, the system on which you will create the image must have the Windows Automated Installation Kit (WAIK) 1.1 installed. Older versions of WAIK are not supported.
- To back up the IIS configuration object on Windows Vista, install the IIS 6 Metabase Compatibility package.

Limitations

- Dynamic disks are not supported (including mirror set upgraded from Windows NT).
- New disk must be the same size or bigger than the crashed disk. If it is larger than the original disk, the difference will remain unallocated.
- Only vendor specific partitions of the type 0x12 (including EISA) and 0xFE are supported for Enhanced Automated Disaster Recovery.
- Multiboot systems that do not use Microsoft's boot loader are not supported.
- Internet Information Server (IIS), Terminal Services Database and Certificate Server Database are not restored automatically during Phase 2. They can be restored on the target system using the standard Data Protector restore procedure.
- Disaster recovery ISO images cannot be created on systems where Data Protector is installed on FAT/FAT32 partitions. You need at least one client in the cell where Data Protector is installed on an NTFS volume to be able to create disaster recovery images.

Preparation

See also "Planning" on page 33, for the general preparation procedure for all disaster recovery methods before completing the steps listed in this section. See also "Advanced recovery tasks" on page 91.

IMPORTANT:

Prepare for disaster recovery *before* a disaster occurs.

Prerequisites

- Perform a full client backup (including the CONFIGURATION).

See the online Help index: “backup, Windows specific” and “backup, configuration”.

- ***Microsoft Cluster Server:*** In case of Microsoft Cluster Server, consistent backup includes (in the same backup session):
  - all nodes
  - administrative virtual server (defined by the administrator)
  - if Data Protector is configured as a cluster aware application, Cell Manager virtual server and IDB.

  See “Restoring the Microsoft Cluster Server specifics” on page 91 for details.

After you performed the backup, merge the P1S files for all nodes in the MSCS, so that P1S file of each node contains information on the shared cluster volumes configuration. Refer to “Merging P1S files of all nodes for EADR” on page 95 for instructions.

DR image file

Data required for temporary DR OS installation and configuration (DR image) is packed in a single large file and stored on the backup medium and optionally on the Cell Manager during a full client backup. If you want to save the full disaster recovery image file to the Cell Manager for all clients in the backup specification, perform the following steps:

1. In the Context List, select **Backup**.
2. In the Scoping pane, expand the Backup Specifications and then Filesystem.
3. Select the backup specification you will use for a full client backup (create it if you have not created it already).
4. In the Results Area, click **Options**.
5. Under Filesystem Options, click **Advanced**.
6. Click **WinFS Options** and select **Copy full DR image to disk**.

   For Windows Vista systems, select also **Detect NTFS hardlinks** and **Use Shadow Copy**.

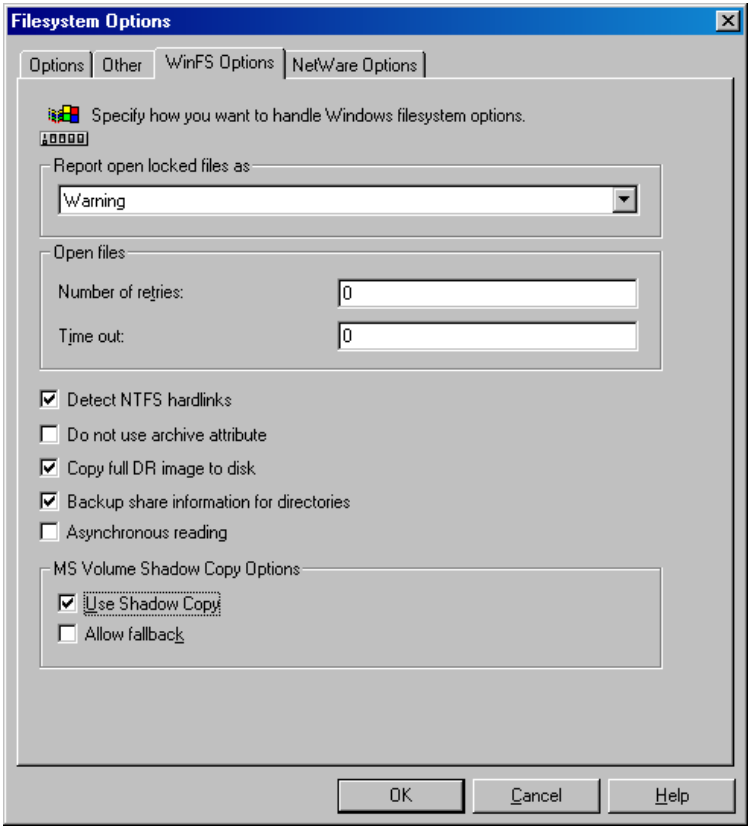


Figure 3 WinFS options tab

To copy the DR image files only for particular clients in the backup specification, perform the following steps:

1. In the Context List, select **Backup**.
2. In the Scoping pane, expand the Backup Specifications and then Filesystem.
3. Select the backup specification you will use for a full client backup. If you have not created it yet, do so. See the online Help index “creating, backup specifications”.
4. In the Results Area, click **Backup Object Summary**.
5. Select the client for which you would like to store the DR image file onto the Cell Manager and click **Properties**.
6. Click the **WinFS Options** and select **Copy full DR image to disk** .

Saving the full DR image to the Cell Manager is useful if you plan to burn the disaster recovery CD on the Cell Manager, because it is much faster to obtain the DR image from the hard disk than to restore it from a backup medium. The DR image file is by default saved into `Data_Protector_home\Config\server\dr\p1s` (Windows Cell Manager) or into `/etc/opt/omni/server/dr/p1s` (UNIX Cell Manager) with the name `client name.img`. To change the default location, specify a new global variable `EADRImagePath = valid_path` (for example, `EADRImagePath = /home/images` or `EADRImagePath = c:\temp`) in the global options file. Refer to the online Help index "Global Options File, modifying".

TIP:

If you do not have enough free disk space in the destination directory, you can create a link to another volume on UNIX or create a mount point on Windows.

kb.cfg file

The purpose of this file is to provide a flexible method to enable Data Protector to include drivers (and other needed files) in the DR OS to cover systems with specific boot relevant hardware or application configurations. The default `kb.cfg` file already contains all files necessary for industry standard hardware configurations.

Create and execute a test plan using the default version of the `kb.cfg` file. If the DR OS does not boot normally or cannot access network, then you may need to modify the file. Refer to "Editing the kb.cfg file" on page 102.

Preparing the encryption keys

For a Cell Manager recovery or an offline client recovery, you must ensure that the encryption keys are available during the disaster recovery by storing them on a removable medium. For a Cell Manager recovery, prepare the removable medium in advance, before the disaster occurs.

The encryption keys are not part of the DR OS image file. The keys are automatically exported during the disaster recovery image creation to `Data_Protector_home\Config\Server\export\keys\DR-ClientName-keys.csv`, where `ClientName` is the name of the client for which the image is being created.

Ensure that you have the correct encryption key for each backup that is prepared for a disaster recovery.

Phase 1 Startup file (P1S)

In addition to the DR image file, a Phase 1 Startup file (P1S) is created during full backup. It is saved on backup medium and on the Cell Manager into *Data_Protector_home*\Config\server\dr\p1s directory (Windows Cell Managers) or into /etc/opt/omni/server/dr/p1s directory (UNIX Cell Manager) with the filename equal to the hostname (for example, computer.company.com). It is a Unicode UTF-8 encoded file that contains information on how to format and partition all disks installed in the system, whereas the updated SRD file contains only system information and data about backup objects and corresponding media.

After a disaster occurs, you can use the EADR wizard to merge DR image, SRD and P1S files with disaster recovery installation into a **disaster recovery CD ISO image**, which can be burned on a CD using any CD burning tool that supports the ISO9660 format. This **disaster recovery CD** can then be used to perform automated disaster recovery.

IMPORTANT:

Disaster recovery CD has to be prepared in advance for the Cell Manager.

Additional steps are required if you are preparing disaster recovery CD of a Microsoft Cluster node. See "Restoring the Microsoft Cluster Server specifics" on page 91.

IMPORTANT:

It is recommended to restrict access to backup media, DR images, SRD files and disaster recovery CDs due to security reasons.

Preparing DR CD ISO image

To prepare a DR CD ISO image, perform the following steps:

1. In the Context List, select **Restore**.
2. Click the **Tasks** navigation tab and select Disaster Recovery.
3. From the drop down list, select the client you would like to prepare the ISO image for.
4. Click **Enhanced Automated Disaster Recovery** and then **Next**.

5. For each critical object select an appropriate object version and click **Next**.
6. If you have saved the DR image file on the Cell Manager, specify or browse for its location, otherwise click **Restore image file from a backup**. Click **Next**.
7. Select the destination directory where you want to place the ISO CD image (`recovery.iso`) and click **Finish** to create the ISO CD image.

△ CAUTION:

If you place a new ISO CD image to a location where an ISO image (`recovery.iso`) is already located, the old ISO CD image will be overwritten by the new one without a warning.

Windows Vista systems: Specify the WAIK options:

- Windows Automated Installation Kit (WAIK) directory. Once you enter the location, Data Protector saves it and uses it as the default selection in the GUI the next time an ISO CD image is created.
- Drivers, that you want to insert into the ISO CD image. You can use this option to add missing drivers to the DR OS.

  To insert the drivers that are part of the Windows Vista client recovery set, click **Inject**. The drivers from the *`%Drivers%`* part of the recovery set will be automatically injected in the Insert drivers dialog window. Only drivers with the `.inf` extension will be listed.

NOTE:

The drivers collected during the backup procedure and stored within the Recovery Set's *`%Drivers%`* directory may not be always appropriate for using in the DR OS. In some cases, Windows PE specific drivers may have to be injected to ensure that the hardware works properly during the recovery.

8. Burn the disaster recovery ISO CD image on a CD using any CD burning tool that supports the ISO9660 format.

IMPORTANT:

Perform a new backup and prepare a new DR CD after each hardware, software or configuration change. This also applies to any network configuration changes, such as change of IP address or DNS server.

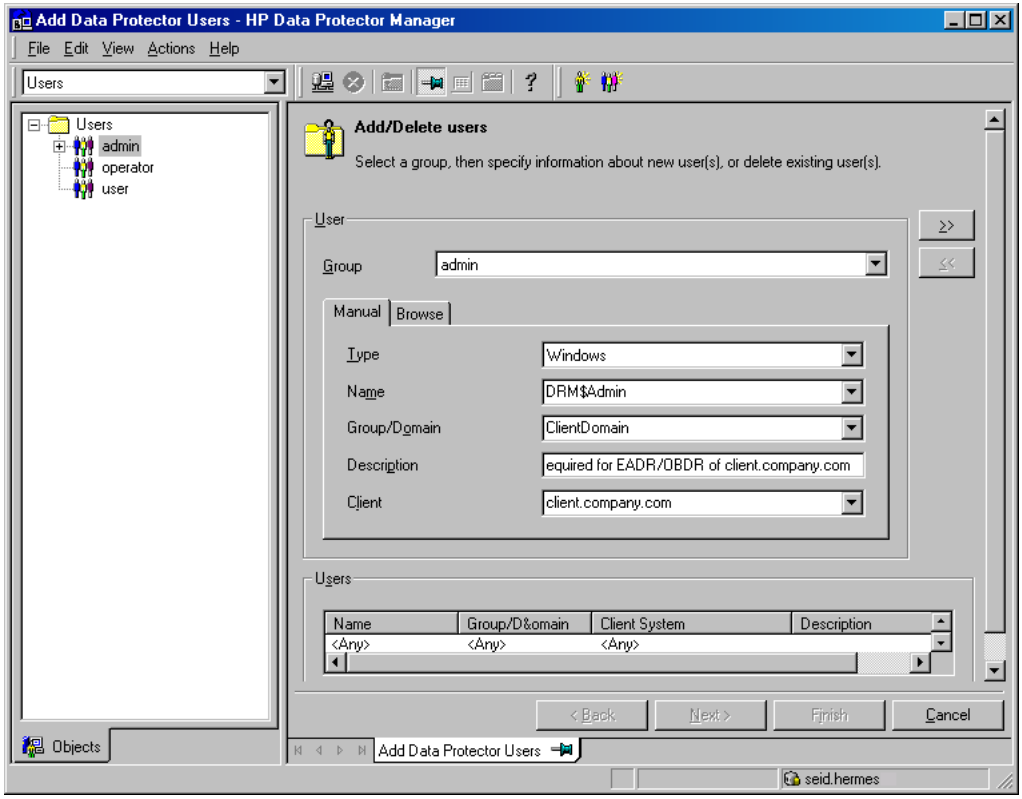
Recovery

You need the following to successfully perform a disaster recovery on the crashed system:

- A new hard disk to replace your crashed disk.
- A successful full client backup of the client that you want to recover.
- The Data Protector disaster recovery CD.

The following is a step-by-step procedure for performing EADR of a Windows system:

1. Unless you are performing an offline disaster recovery, add the account `SYSTEM/NT Authority` (Windows Vista) or `DRM$Admin` (other Windows systems) to the Data Protector Admin user group on the Cell Manager. See the online Help index “adding Data Protector users”.



2. Boot the client system from the disaster recovery CD of the original system. Ensure that no external USB disks (including USB keys) are connected to the system before you start the recovery procedure.
3. Press **F12** when the following message is displayed: `To start recovery of the machine` *`HOSTNAME`* `press F12.`

4. On Windows Vista, the DR OS is loaded first into memory and then the scope menu is displayed. On other Windows systems, the scope selection menu is displayed at the beginning of the boot process.

   Select the scope of recovery and press **Enter**. There are 5 different scopes of recovery:

   - **Reboot**: Disaster recovery is not performed and the computer is rebooted.
   - **Default Recovery**: Critical volumes are recovered. All other disks are not partitioned and formatted and are ready for Phase 3.
   - **Minimal Recovery**: Only system and boot disks are recovered (available for EADR and OBDR only).
   - **Full Recovery**: All volumes are recovered, not just the critical ones.
   - **Full with Shared Volumes**: Available for Microsoft Cluster Server (MSCS) only. This option should be used if all nodes in the MSCS have crashed and you are performing EADR on the first node. It will recover all volumes in the Restore Set including cluster shared volumes that were locked by the backed-up node at backup time.

     If at least one node is up and MSCS is running, then shared volumes will not be restored because the node keeps them locked. In this case, you should use `Default Recovery`.

   Depending on the platform or operating system, there are additional options, which are mainly used in cases where the disaster recovery does not finish completely or requires additional steps:

   - **Restore BCD**: Available on Windows Vista only. By default, Data Protector restores the Boot Configuration Data (BCD) store during a disaster recovery. If the BCD store is not restored, it may not be possible to boot the machine.
   - **Restore DAT**: Available on Windows Vista only. Enables you to restore writers' data, which is stored in DAT files as a part of the DR OS, before or after the Data Protector restore.
   - **Remove Boot Descriptor**: Available on Intel Itanium systems only. Removes all Boot Descriptors left over by the disaster recovery processes. See "Intel Itanium specifics" on page 140
   - **Manual disk selection**: Available on Intel Itanium systems only. If the disk setup has changed significantly, the disaster recovery module may not be able to find the boot disk(s). Use this option to select the correct boot disk. See "Intel Itanium specifics" on page 140.

   Windows Vista only: If the volumes are encrypted using BitLocker Drive Encryption, a menu will display, enabling you to unlock the encrypted drives. See "Windows Vista BitLocker Drive Encryption" on page 107.

5. After you have selected the scope of the recovery, Data Protector sets up the DR OS directly to the hard disk. You can monitor the progress and, when the DR OS is set up, the system reboots. On Windows Vista systems, this step is skipped, and the reboot is not performed.

   Wait for 10 seconds when prompted `To start recovery of the machine HOSTNAME press F12`, to boot from the hard disk and not from the CD.

   The Disaster Recovery wizard appears. To modify the disaster recovery options, press any key to stop the wizard during the countdown and modify the options. Click **Finish** to continue with the disaster recovery.

6. If the disaster recovery backup is encrypted by Data Protector and you are either recovering the Cell Manager or a client where the Cell Manager is not accessible, the following prompt is displayed:

   ```
   Do you want to use AES key file for decryption [y/n]?
   ```

   Press **y**.

   Ensure that the key store (`DR-ClientName-keys.csv`) is available on the client (by inserting a medium on which you have the key) and enter the full path to the key store file. The key store file is copied to the default location on the DR OS and is used by the Disk Agents. Disaster recovery now continues without further interruption.

7. If you are performing an offline recovery and the information in the SRD file is not up to date (for example, because you changed the backup device after the disaster), edit the SRD file, before you can continue with this procedure. Refer to "Recovery using an edited SRD file" on page 103.

8. Data Protector will then reestablish the previous storage structure within the selected scope of recovery and restore all critical volumes. The temporary DR OS will be deleted after the first login, except in the following cases:

   - **Minimal Recovery** is selected.
   - You have interrupted the Disaster Recovery wizard during the 10 seconds pause after it has found the DR installation and SRD file on the backup medium, and have selected the **Debugs** option.
   - You have manually started the `omnidr` command with the `no_reset` or `debug` options.
   - Disaster recovery fails.

   On Windows Vista systems, the temporary DR OS is never retained.

9. Remove the client's local Administrator account created in step Step 1 from the Data Protector Admin user group on the Cell Manager, unless it existed on the Cell Manager before the disaster recovery.

10. Additional steps are required if you are recovering a Cell Manager or performing advanced recovery tasks (such as restoring MSCS or IIS, editing the `kb.cfg` and SRD files). See "Restoring the Data Protector Cell Manager specifics " on page 98 and "Advanced recovery tasks" on page 91 for more information.
11. Restore user and application data using the standard Data Protector restore procedure.

NOTE:

Data Protector does not restore the volume-compression flag after recovery. All files that were compressed at backup time will be restored as compressed, but you will have to manually set the volume compression if you want any newly created files to be compressed as well.

One Button Disaster Recovery of a Windows system

One Button Disaster Recovery (OBDR) is an automated Data Protector recovery method for Windows clients and Cell Manager, where user intervention is reduced to minimum. For details on supported operating systems, refer to the *HP Data Protector product announcements, software notes, and references*.

OBDR collects all relevant environment data automatically at backup time. During backup, data required for temporary DR OS setup and configuration is packed in a single large OBDR image file and stored on the backup tape. When a disaster occurs, OBDR device (backup device, capable of emulating CD-ROM) is used to boot the target system directly from the tape which contains the OBDR image file with disaster recovery information.

Data Protector then installs and configures the disaster recovery operating system (DR OS), formats and partitions the disks and finally restores the original operating system with Data Protector as it was at the time of backup.

IMPORTANT:

Perform a new backup after each hardware, software or configuration change. This also applies to any network configuration changes, such as change of IP address or DNS server.

The recovered volumes are:

- the boot partition

- the system partition
- the partitions containing Data Protector

Any remaining partitions can be recovered using the standard Data Protector recovery procedure.

Overview

The general steps using the One Button Disaster Recovery method for a Windows client are:

1. **Phase 0**
   a. You need an OBDR backup (create the backup specification using the Data Protector One Button Disaster Recovery wizard).
   b. If you are using encrypted backups, store the encryption key on a removable medium so that it is available for disaster recovery. You will need the key for a Cell Manager recovery or if the connection to the Cell Manager cannot be established.
2. **Phase 1**

   Boot from the recovery tape and select the scope of recovery.
3. **Phase 2**

   By default, critical volumes (the boot partition, the operating system and the partition containing Data Protector) are restored.
4. **Phase 3**

   Restore any remaining partitions using the standard Data Protector restore procedure.

IMPORTANT:

It is recommended to restrict access to OBDR boot tapes.

The following sections explain the requirements, limitations, preparation and recovery pertaining to One Button Disaster Recovery on Windows systems. See also "Advanced recovery tasks" on page 91.

Requirements

- Data Protector Automatic Disaster Recovery and User Interface components must be installed on the systems for which you want to enable recovery using this method. See *HP Data Protector installation and licensing guide*.
- It is essential to have an OBDR capable computer configuration: the system's BIOS must support bootable CD extensions as defined in the El-Torito standard and read/write access to hard disk drive using LBA addressing via INT13h function XXh. The OBDR device must conform to the same standard when emulating the CD-ROM. The BIOS options can either be checked in the user's manuals of the system or by inspecting the system setup before the boot.

  For more information about supported systems, devices and media, please refer to the HP StorageWorks Tape Hardware Compatibility Table on the World Wide Web:

  http://www.hp.com/support/manuals. Also see the *HP Data Protector product announcements, software notes, and references.*
- The hardware configuration of the target system must be the same as of the original system. This includes SCSI BIOS settings (sector remapping).
- Replacement disks have to be attached to the same host bus adapter on the same bus.
- The boot partition (on which the mini OS is installed) must be larger than 200 MB or disaster recovery will fail. If you enabled the Compress drive to save disk space option on the original partition, you must have 400 MB free.
- During OBDR backup, the partition on which Data Protector is installed should have at least 200 MB of temporary free space. This space is required to create a temporary image.
- All drivers, required for boot must be installed under the `%SystemRoot%` folder.
- Network must be available when you boot the system in Safe Mode with Networking or in Directory Services Restore Mode (Domain Controller only), but you must do the backup of the system after it was booted with normal boot process.
- A media pool with a Non-appendable media usage policy and Loose media allocation policy has to be created for the OBDR capable device. Only the media from such pool can be used for disaster recovery.
- When backing up the client, the default 64 kB block size should be used to write to the device if you plan to perform an offline restore. This is the only default block size available on Windows when performing disaster recovery. To verify that the default 64 kB block size is set, choose **Advanced** in the Properties box, as shown in Figure 4 on page 71.

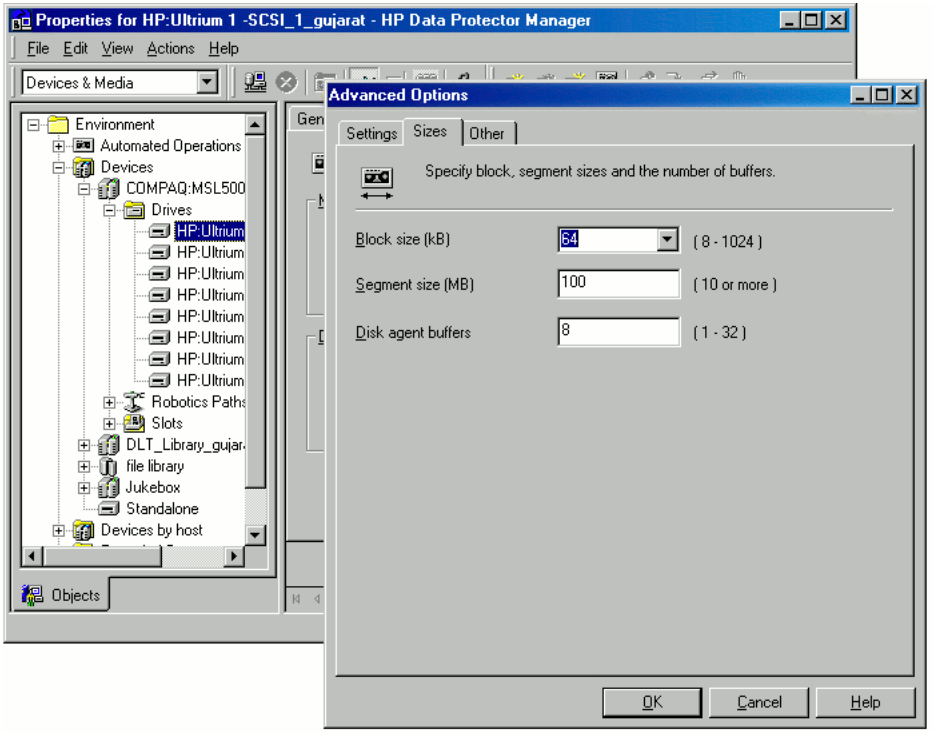


Figure 4 Verifying the default block size

- Before starting an AES encrypted OBDR backup, the `kms_allow_hosts` file must be present and contain the fully qualified domain name of the client for which the image is prepared. See "ISO image creation for an AES encrypted backup fails if kms_allow_hosts file is missing" on page 139.
- The Windows Automated Installation Kit (WAIK) 1.1 must be installed on the client which will be backed up. Older versions of WAIK are not supported.
- To back up the IIS configuration object on Windows Vista, install the IIS 6 Metabase Compatibility package.

Limitations

- Multiboot systems that do not use Microsoft's boot loader are not supported.
- Internet Information Server (IIS) Database, Terminal Services Database and Certificate Server Database are not restored automatically during Phase 2. They

can be restored on the target system using the standard Data Protector restore procedure.

- One Button Disaster Recovery backup session can only be performed for one selected client or Cell Manager on the same OBDR device at a time. This has to be done on a single, locally attached OBDR capable device.
- Dynamic disks are not supported (including mirror set upgraded from Windows NT).
- New disk has to be the same size or bigger than the crashed disk. If it is larger than the original disk, the difference will remain unallocated.
- Only vendor specific partitions of type 0x12 (including EISA) and 0xFE are supported for OBDR.
- OBDR is supported only on systems where Data Protector is installed on an NTFS volume.
- On Windows Vista, LDM disks are not supported.
- On Intel Itanium systems, recovery of a boot disk is supported only for local SCSI disks.

Preparation

See also "Planning" on page 33, for the general preparation procedure for all disaster recovery methods before completing the steps listed in this section. See also "Advanced recovery tasks" on page 91.

IMPORTANT:

Prepare for disaster recovery *before* a disaster occurs.

Create a media pool for DDS or LTO media with `Non-appendable` media usage policy (to ensure that this will be the only backup on tape) and `Loose` media allocation policy (because the tape is formatted during OBDR backup). In addition, select this media pool as a default media pool for the OBDR device. See the online Help index: "creating media pool". Only media from such pool can be used for OBDR.

Microsoft Cluster Server: In case of Microsoft Cluster Server, consistent backup includes (in the same backup session):

- all nodes
- administrative virtual server (defined by the administrator)

- if Data Protector is configured as a cluster aware application, Cell Manager virtual server and IDB.

See "Restoring the Microsoft Cluster Server specifics" on page 91 for details.

To enable an automatic restore of all shared disk volumes on the MSCS using the OBDR method, move all volumes temporarily to the node for which you are preparing the OBDR boot tape so that shared disk volumes are not locked by another node during the OBDR backup. It is namely impossible to collect enough information for configuring the disk during Phase 1 for shared disk volumes that are locked by another node during the backup.

OBDR backup

Use the following steps to perform OBDR backup locally on the system, for which you want to enable recovery using OBDR:

1. In the Context List, select **Backup**.
2. Click **Tasks** navigation tab and check **One Button Disaster Recovery wizard** in the Scoping Pane.
3. Click **Next**.
4. All critical objects are already selected (including the IDB in case of the Cell Manager OBDR backup) and can not be deselected. Manually select any other partitions you want to keep, because during the recovery procedure, Data Protector deletes all partitions from your system. Click **Next**.
5. Select the locally attached OBDR device you are going to use for backup and click **Next**.

6. Select backup options. For more details on available options, see the online Help index: “backup options”.

   Windows Vista systems: Specify the WAIK options:

   - Windows Automated Installation Kit (WAIK) directory. Once you enter the location, Data Protector saves it and uses it as the default selection in the GUI the next time an ISO CD image is created. If no directory is specified, Data Protector will use the default WAIK paths.
   - Drivers that you want to insert into the ISO CD image. You can use this option to add missing drivers to the DR OS.

     To insert the drivers which are part of the Windows Vista client recovery set, select **Autoinject drivers from Recovery Set**. The drivers from the `%Drivers%` part of the recovery set will be automatically injected into the DR OS image.

   NOTE:

   The drivers collected during the backup procedure and stored within the recovery sets' `%Drivers%` directory may not be always appropriate for using in the DR OS. In some cases, Windows Preinstall Environment specific drivers may have to be injected to ensure that the hardware works properly during the recovery.

   To add drivers manually, click **Add** and enter the missing drivers.

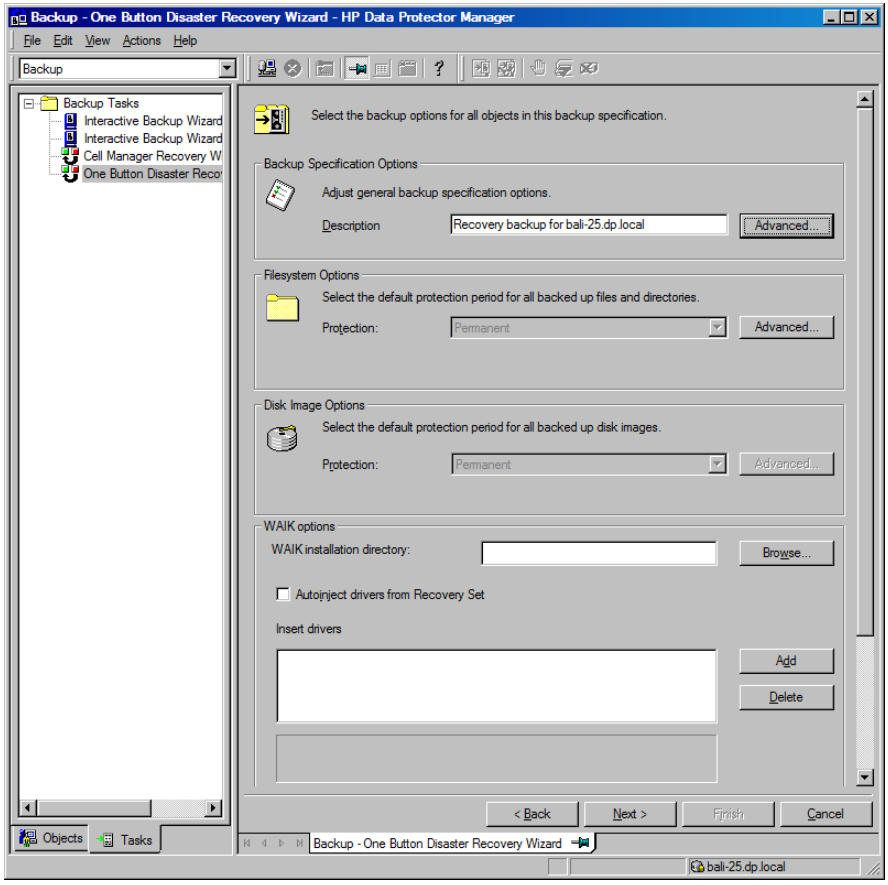


Figure 5 Windows Vista client backup options

7. Click **Next** to proceed to the Scheduler page, which can be used to schedule the backup. See the online Help index "scheduling backups on specific dates and times".

8. Click **Next** to display the Backup Object Summary page, in which you can review the backup options.

NOTE:

In the Summary page, you cannot change a previously selected backup device or the order in which the backup specifications follow one another (move up and move down functionalities are not available). Only OBDR non-essential backup objects can be deleted as well as general object properties can be viewed.

However, a backup object's description can be changed.

9. In the final page of the Backup wizard, you can save the backup specification, start the interactive backup, or preview the backup.

   It is recommended to save the backup specification so that you can schedule or modify it later.

   Once a backup specification is saved, you can edit it. Right-click the backup specification and select **Properties**. You are offered to treat the modified backup specification as a standard Data Protector backup specification or as an OBDR backup specification. Save it as an OBDR backup specification to keep it in the original One Button Disaster Recovery format. If saved as a standard backup specification, it is not usable for OBDR purposes.

10. Click **Start Backup** to run the backup interactively. The Start Backup dialog box appears. Click **OK** to start the backup.

A bootable image file of the system, containing all information required for installation and configuration of temporary DR OS, will be written at the beginning of the tape to make it bootable.

IMPORTANT:

Perform a new backup and prepare a bootable backup medium after each hardware, software or configuration change. This also applies to any network configuration changes, such as change of IP address or DNS server.

kb.cfg file

The purpose of this file is to provide a flexible method to enable Data Protector to include drivers (and other needed files) in the DR OS to cover systems with specific

boot relevant hardware or application configurations. The default `kb.cfg` file already contains all files necessary for industry standard hardware configurations.

Create and execute a test plan using the default version of the `kb.cfg` file. If the DR OS does not boot normally or cannot access network, then you may need to modify the file. Refer to "Editing the kb.cfg file" on page 102.

△ CAUTION:

It is recommended to restrict access to backup media due to security reasons.

Preparing the encryption keys

For a Cell Manager recovery or an offline client recovery, you must ensure that the encryption keys are available during the disaster recovery by storing them on a removable medium. For a Cell Manager recovery, prepare the removable medium in advance, before the disaster occurs.

The encryption keys are not part of the DR OS image file. The keys are automatically exported during the disaster recovery image creation to *Data_Protector_home*\Config\Server\export\keys\DR-*ClientName*-keys.csv, where *ClientName* is the name of the client for which the image is being created.

Ensure that you have the correct encryption key for each backup that is prepared for a disaster recovery.

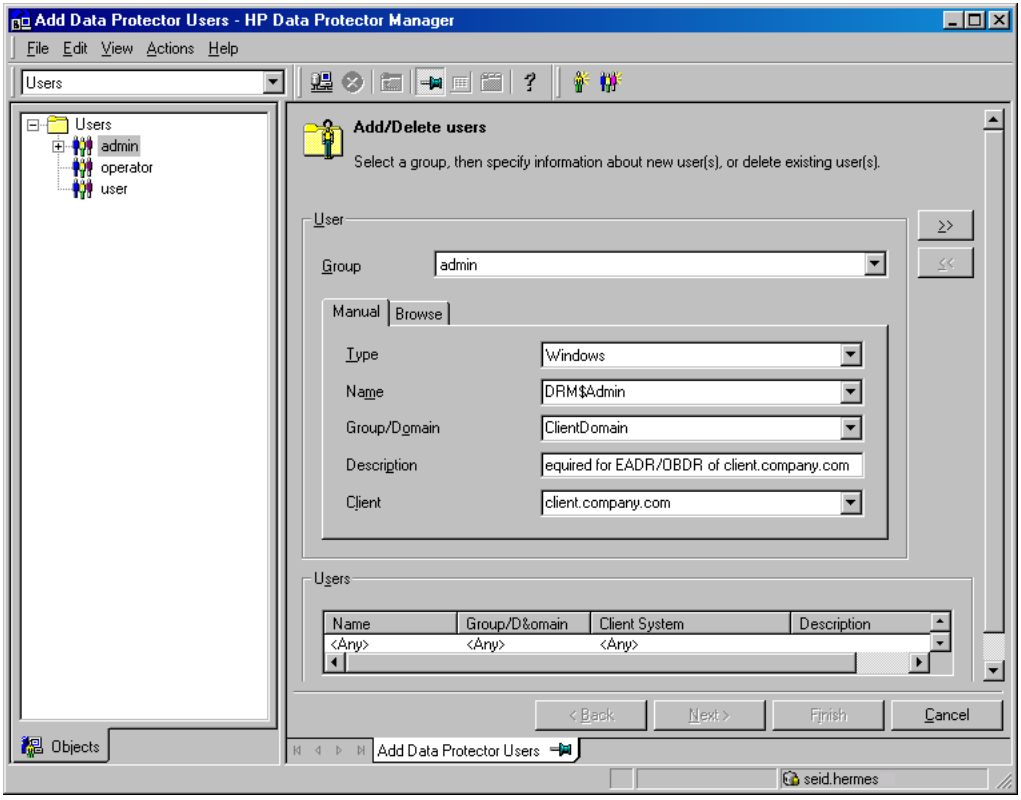
Recovery

You need the following to successfully perform a disaster recovery on the crashed system:

- A new hard disk to replace your crashed disk (if needed).
- A bootable backup medium with all critical objects of the client that you want to recover.
- An OBDR device connected locally to the target system.

The following is a step-by-step procedure for performing a One Button Disaster Recovery of a Windows system:

1. Unless you are performing an offline disaster recovery, add the account `SYSTEM/NT Authority` (Windows Vista) or `DRM$Admin` (other Windows systems) to the Data Protector Admin user group on the Cell Manager. See the online Help index “adding Data Protector users”.



2. Insert the tape containing the image file and your backed up data into an OBDR device.
3. Shut down the target system and power off the tape device. Ensure that no external USB disks (including USB keys) are connected to the system before you start the recovery procedure.
4. Power on the target system and while it is being initialized, press the eject button on the tape device and power it on. For details see the device documentation.

5. On Windows Vista, the DR OS is loaded first into memory and then the scope menu is displayed. On other Windows systems, the scope selection menu is displayed at the beginning of the boot process.

   Select the scope of recovery and press **Enter**. There are 5 different scopes of recovery:

   - **Reboot**: Disaster recovery is not performed and the computer is rebooted.
   - **Default Recovery**: Critical volumes are recovered. All other disks are not partitioned and formatted and remain empty and ready for Phase 3.
   - **Minimal Recovery**: Only system and boot disks are recovered (available for EADR and OBDR only).
   - **Full Recovery**: All volumes are recovered, not just the critical ones.
   - **Full with Shared Volumes**: Available for Microsoft Cluster Server (MSCS) only. This option should be used if all nodes in the MSCS have crashed and you are performing One Button Disaster Recovery of the first node. It will recover all volumes in the Restore Set including cluster shared volumes that were locked by the backed-up node at backup time.

   TIP:

   To enable automatic restore of all shared disk volumes in the MSCS, move all volumes temporarily to the node, for which you are preparing an OBDR boot tape. It is not possible to collect enough information to configure disks in Phase 1 for shared disk volumes that are locked by another node at backup.

   If at least one node is up and running than shared volumes will not be restored because the node keeps them locked. In this case, you should use Default Recovery.

Depending on the hardware platform or operating system, there are additional options, which are mainly used when the disaster recovery does not finish completely or requires additional steps:

- **Restore BCD**: Available for Windows Vista only. By default, Data Protector restores the Boot Configuration Data (BCD) store during a disaster recovery. If the BCD store is not restored, it may not be possible to boot the machine.
- **Restore DAT**: Available on Windows Vista only. Enables you to restore writers' data, which is stored in DAT files as a part of the DR OS, before or after the Data Protector restore.

- **Remove Boot Descriptor**: Available on Intel Itanium systems only. Removes all Boot Descriptors left over by the disaster recovery processes. See "Intel Itanium specifics" on page 140
- **Manual disk selection**: Available on Intel Itanium systems only. If the disk setup has changed significantly, the disaster recovery module may not be able to find the boot disk(s). Use this option to select the correct boot disk. See "Intel Itanium specifics" on page 140.

Windows Vista only: If the volumes are encrypted using BitLocker Drive Encryption, a menu will display, enabling you to unlock the encrypted drives. See "Windows Vista BitLocker Drive Encryption" on page 107.

6. After you have selected the scope of recovery, Data Protector starts setting up the DR OS directly to the hard disk. You can monitor the progress and, when the DR OS is set up, the system reboots. On Windows Vista, the DR OS is not installed and the reboot is not performed.

   To modify the disaster recovery options, press any key to stop the wizard during the countdown and modify the options. Click **Finish** to continue with the disaster recovery.

7. If the disaster recovery backup is encrypted and you are either recovering the Cell Manager or a client where the Cell Manager is not accessible, the following prompt will appear:

   ```
   Do you want to use AES key file for decryption [y/n]?
   ```

   Press **y**.

   Ensure that the key store (`DR-ClientName-keys.csv`) is available on the client (for example, by inserting a CD-ROM, floppy disk, or a USB flash key) and enter the full path to the key store file. The key store file is copied to the default location on the DR OS and is used by the Disk Agents. Disaster recovery now continues without further interruption.

8. If you are performing an offline recovery and the information in the SRD file is not up to date (for example, because you changed the backup device after the disaster), edit the SRD file, before you can continue with this procedure. Refer to "Recovery using an edited SRD file" on page 103.

9. Data Protector will then reestablish the previous storage structure and restore all critical volumes.

   The temporary DR OS will be deleted after the first login, except for the following cases:

   - Minimal Recovery is selected.
   - You interrupted the Disaster Recovery wizard during the 10 seconds pause (after it had found the DR installation and the SRD file on the backup medium), and selected the **Debugs** option.
   - You manually started the `omnidr` command with the `-no_reset` or `-debug` options.
   - Disaster recovery fails.

   On Windows Vista, the temporary DR OS is never retained.

10. Remove the client's local Administrator account created in step Step 1 from the Data Protector Admin user group on the Cell Manager, unless it existed on the Cell Manager before the disaster recovery.
11. Additional steps are required if you are recovering a Cell Manager or performing advanced recovery tasks (such as restoring MSCS or IIS, editing the `kb.cfg` and SRD files). See "Restoring the Data Protector Cell Manager specifics " on page 98 and "Advanced recovery tasks" on page 91 for more information.
12. Restore the user and application data using the standard Data Protector restore procedure.

NOTE:

Data Protector does not restore the volume-compression flag after recovery. All files that were compressed at backup time will be restored as compressed, but you will have to manually set the volume compression if you want any new files created to be compressed as well.

Automated System Recovery

Automated System Recovery (ASR) is an automated system on Windows systems, which reconfigures a disk to its original state (or resizes the partitions if the new disk is larger than the original disk) in the case of a disaster. This includes disk partitioning and logical volume configuration (file formats, drive letter assignments, volume mountpoints, and volume characteristics). ASR thus enables the Data Protector

`drstart.exe` command to install the active DR OS which provides Data Protector disk, network, tape, and file system access.

Data Protector then recovers the target system to the original system configuration and finally restores all user data.

For details on supported operating systems, refer to the *HP Data Protector product announcements, software notes, and references.*

IMPORTANT:

Perform a full client backup after each hardware, software or configuration change and update the ASR diskettes. This also applies to any network configuration changes, such as change of the IP address or DNS server.

IMPORTANT:

Create the ASR set for the Cell Manager in advance, because you will not be able to obtain the ASR archive file after the disaster. ASR sets for other systems can be created using Cell Manager when a disaster occurs.

The recovered volumes are:

- the boot partition
- the system partition
- the partitions containing Data Protector

Any remaining partitions can be recovered using the standard Data Protector recovery procedure.

Overview

The general steps for using the ASR method for a Windows client are:

1. **Phase 0**
   a. Perform a full client backup.
   b. Prepare ASR diskettes with Data Protector binaries and update the first diskette after each configuration change.
   c. If you are using encrypted backups, store the encryption key on a removable medium so that it is available for disaster recovery. You will need the key

for a Cell Manager recovery or if the connection to the Cell Manager cannot be established.

2. **Phase 1**
   a. Boot from the Windows installation medium and enter the ASR mode by pressing **F2**.
   b. Provide the first (updated) diskette from the ASR set.
   c. After reboot, provide information about the location of DR installation and SRD file (`a:\`).
   d. Change diskettes when prompted.
3. **Phase 2**
   a. All critical objects are automatically restored. Reboot the system and remove the Windows installation medium and ASR diskette.
4. **Phase 3**
   a. Restore user and application data using the standard Data Protector restore procedure.

ASR is used to perform (a part of) preparation for a disaster and repartitioning and reformatting the boot partition. Data Protector provides all other features such as easy central administration, high performance backup, high availability support, easy restore, monitoring, reporting and notifications, etc.

The following sections explain the requirements, limitations, preparation, and recovery pertaining to Automated System Recovery on Windows systems. See also "Advanced recovery tasks" on page 91.

Requirements

- Data Protector Automatic Disaster Recovery component must be installed on systems for which you want to enable recovery using ASR. See the *HP Data Protector installation and licensing guide*.
- If you are using a firewall, ports 1071 and 1073 must be open. ASR does not support the `OB2PORTRANGE` and `OB2PORTRANGESPEC` variables.

Hardware configuration

- The hardware configuration of the target system must be identical to that of the original system, except for hard disk drives, video cards and network interface cards. If you have replaced a network card or a video card, you will have to manually configure it.
- Floppy disk drive must be installed.

- Floppy and CD drives must be connected to IDE or SCSI controllers. External devices such as USB or PCMCIA devices are not supported.

  However, ASR using the USB floppy drive is supported on HP Integrity servers (IA-64 platform). For details, see the "*Recovering Windows Server 2003 on HP Integrity servers*" whitepaper available at http://docs.hp.com/en/windows.html.

Hard Disk Drives

- The target system must have the same number of physical disks with critical volumes as the original system.
- Replacement disks must be attached to the same host bus adapter on the same bus.
- The storage capacity of each replacement disk on the target system must be bigger than or equal to the capacity of the corresponding disk on the original system. In addition, disk geometry of the replacement disk must be the same as on the replaced disk.
- All disks on the target system must have 512 bytes-per-sector.
- All disks used in ASR must be accessible to the system (hardware RAID must be configured, SCSI disks must be correctly terminated, etc.)
- When backing up the client, the default 64 kB block size should be used to write to the device if you plan to perform an offline restore. This is the only default block size available on Windows when performing disaster recovery. To verify that the default 64 kB block size is set, choose **Advanced** in the Properties box, as shown in Figure 6:

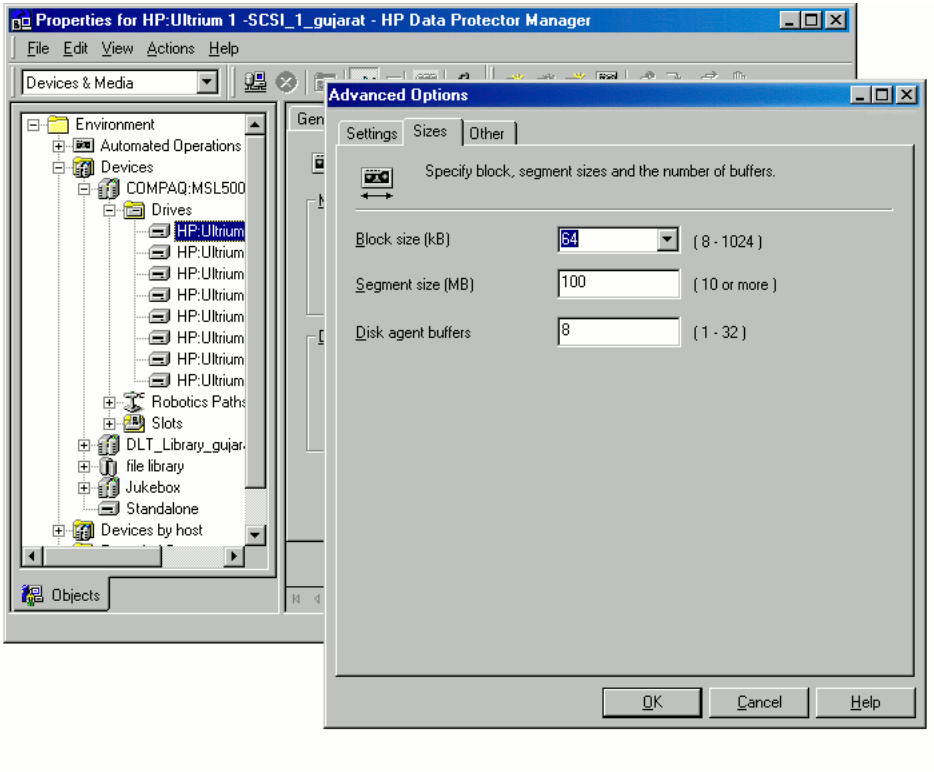


Figure 6 Verifying the Default Block Size

Limitations

- Windows XP Home Edition does not support ASR.
- Multiboot systems that do not use Microsoft's boot loader are not supported.
- Internet Information Server (IIS) Database, Terminal Services Database, and Certificate Server Database are not restored automatically during Phase 2. They can be restored on the target system using the standard Data Protector restore procedure.
- Data stored on vendor specific partitions is not automatically restored during ASR. The partitions will be recreated during the ASR but you will have to restore the data manually using the vendor specific procedure for restoring data. However, you can restore data on EISA utility partition using the standard Data Protector restore procedure.

- Only those local backup devices are supported, that can be installed by Windows during OS installation (no additional drivers are required).

Preparation

See also "Planning" on page 33, for the general preparation procedure for all disaster recovery methods before completing the steps listed in this section. See also "Advanced recovery tasks" on page 91 in order to prepare for disaster recovery.

IMPORTANT:

Prepare for disaster recovery *before* a disaster occurs.

Prerequisites

- A full client backup (including the configuration) is a prerequisite for successful ASR. See the online Help index: "backup, Windows specific" and "backup, configuration".

  In case of Microsoft Cluster Server, consistent backup includes (in the same backup session):

  - all nodes
  - administrative virtual server (defined by the administrator)
  - if Data Protector is configured as a cluster aware application, Cell Manager virtual server and IDB.

  See "Restoring the Microsoft Cluster Server specifics" on page 91 for details.

After you performed the full client backup prepare an ASR set. An ASR set is a collection of files stored on three or four diskettes, required for proper reconfiguration of the replacement disk (disk partitioning and logical volume configuration) and automatic recovery of the original system configuration and the 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 Windows or in `/etc/opt/omni/server/dr/asr/` on UNIX) as well as on the backup medium. ASR archive file is extracted to three diskettes for 32-bit Windows system or four diskettes for 64-bit Windows system after a disaster occurs. You need these diskettes to perform ASR.

NOTE:

Create the ASR set for the Cell Manager in advance, because you will not be able to obtain the ASR archive file after the disaster.

Perform the following steps to create an ASR set:

1. Perform a full client backup.
2. Insert a diskette in the floppy drive.
3. In the HP Data Protector Manager, switch to the Restore context.
4. Click the **Tasks** navigation tab and select **Disaster Recovery** in the Scoping Pane.
5. From the drop down list in the Results Area, select the client for which you would like to create an ASR set.
6. Click **Create Automated System Recovery set** and then click **Next**.

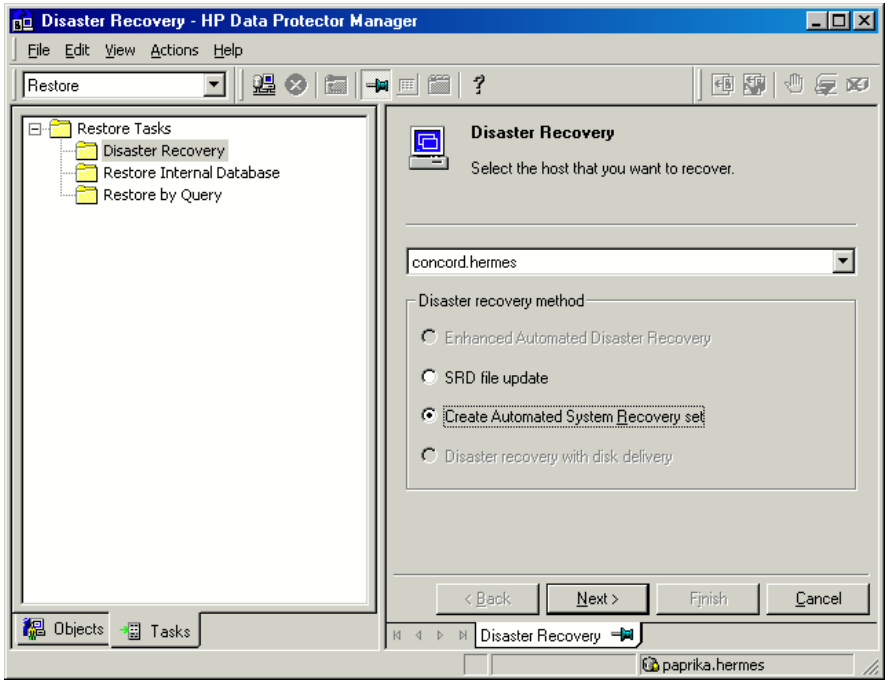


Figure 7 Creating ASR set

Data Protector will obtain the ASR archive file from the Cell Manager. If it is not saved on the Cell Manager, the Disaster Recovery wizard will offer you to recover it from the backup medium.

7. For each critical object, select the appropriate object version and click **Next**.
8. ASR archive file created during a full client backup is downloaded from the Cell Manager. Select the destination location where you want your ASR archive file extracted and select the **Copy DR installation** check box to copy DR installation files to the same location. The recommended destination is your floppy drive because you will need these files stored on diskettes (ASR set) to perform ASR.

   Data Protector will create three diskettes for a 32 bit Windows system and four diskettes for a 64 bit Windows system. ASR set for the Cell Manager has to be prepared in advance, while you can prepare ASR diskettes for other systems using the Cell Manager when a disaster occurs.

Once the ASR set is created, you have to update only the first diskette (which contains ASR information) after each hardware, software or configuration change. This also applies to any network configuration changes, such as a change of the IP address or DNS server. In order to update the first diskette from the ASR set, repeat the whole procedure, but you do not have to select the Copy DR installation check box. This option copies the DR installation files (to a selected destination), which do not need to be updated.

IMPORTANT:

It is recommended to restrict access to ASR diskettes due to security reasons.

Local devices

If you are using a locally attached device for ASR, test if it is supported. To do so, perform the following steps:

1. Run `devbra -dev` from the command prompt (from *`Data_Protector_home`*`\bin`).
2. Rename the `scsitab` file (located in *`Data_Protector_home`*) and run `devbra -dev` from the command prompt again.
3. Compare the both outputs of the `devbra -dev` command. If they are identical, ASR using this device is possible, otherwise copy the `scsitab` file to the first ASR diskette. You have to copy the `scsitab` file only the first time you are

preparing the ASR set. You do not have to copy it when you are only updating the ASR set. See the online Help index: “support of new devices”.

4. Rename the `scsitab` file back to the original name.

Recovery

To successfully perform a disaster recovery of the crashed system, you need the following:

- A new hard disk to replace your crashed disk.
- A successful full client backup of the client that you want to recover.
- Updated ASR set.
- Windows installation medium.

The following is a step-by-step procedure for performing ASR:

1. Boot from the Windows installation medium.
2. Press **F2** during the start of the OS setup to enter the ASR mode.
3. Provide the first (updated) diskette from the ASR set.
4. After reboot, Disaster Recovery wizard pops-up and requires input for the DR installation source and SRD Path. DR installation and SRD file are both located on the first diskette of the ASR set (`a:\`).

   To modify other ASR settings, press any key to stop the wizard during the countdown and select the options. Click **Finish** to continue with ASR.

   If the information in the SRD file on the ASR diskette is not up to date (for example, because you changed the backup device after the disaster) and you are performing an offline recovery, edit the SRD file before continuing with this procedure. See “Recovery using an edited SRD file” on page 103.

NOTE:

If original OS medium does not include appropriate network drivers, ASR will fail. You can install the network using the New Hardware wizard which can be invoked with the following command:

```
%SystemRoot%\System32\rundll32.exe
shell32.dll,Control_RunDLL hdwwiz.cpl
```

5. Unless you are performing an offline disaster recovery, add the client's local system account to the Data Protector Admin user group on the Cell Manager. See the online Help index: "users, Data Protector".

   Enter the same information as in Figure 8 on page 90.

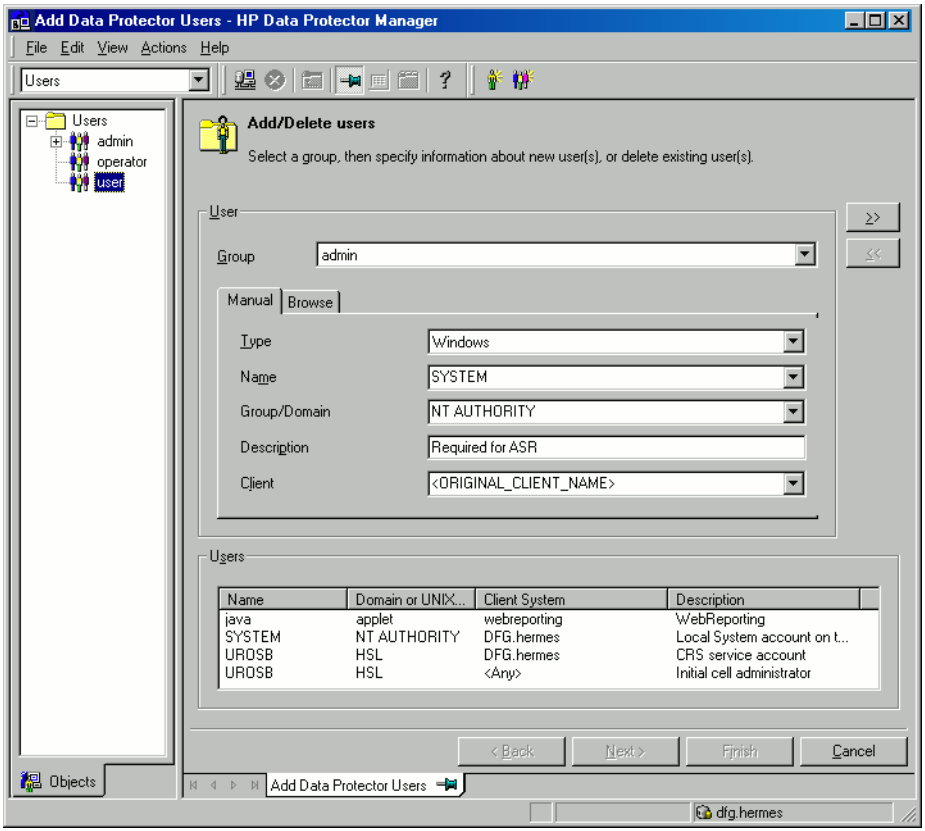


Figure 8 User Name for ASR

6. Change diskette(s) when prompted.
7. Reboot the system when prompted and remove the Windows installation medium and ASR diskette.

8. If the disaster recovery backup is encrypted by Data Protector and you are either recovering the Cell Manager or a client where the Cell Manager is not accessible, the following prompt is displayed:

   ```
   Do you want to use AES key file for decryption [y/n]?
   ```

   Press **y**. Ensure that the key store (`DR-ClientName-keys.csv`) is available on the client (by inserting a medium on which you have the key) and enter the full path to the key store file. The key store file is copied to the default location on the DR OS and is used by the Disk Agents.

9. Remove the client's local system account (created in step Step 5 on page 90) from the Data Protector Admin user group on the Cell Manager, unless it existed on the Cell Manager before the disaster recovery.

10. Restore user and application data using the standard Data Protector restore procedure.

Advanced recovery tasks

This section provides explanation of the steps you will need to take if you want to perform advanced recovery tasks such as restoring Microsoft Cluster Server and Internet Information Server.

Restoring the Microsoft Cluster Server specifics

This section provides explanation of the steps you will need to take if you want to perform disaster recovery of a Microsoft Cluster Server (MSCS). For concepts and general information please refer to the clustering section in the *HP Data Protector concepts guide* and see the online Help index: "cluster".

Select the disaster recovery method that is appropriate for your cluster and include it in your disaster recovery plan. Consider the limitations and requirements of each disaster recovery method before making your decision. Perform tests from the test plan.

Possible scenarios

There are two possible scenarios for disaster recovery of a MSCS:

- at least one of the nodes is up and running
- all nodes in the cluster have experienced a disaster

IMPORTANT:

MSCS can be recovered using any disaster recovery method except for Disk Delivery Disaster Recovery. All specifics, limitations and requirements pertaining a particular disaster recovery method you are going to use also apply for the disaster recovery of a MSCS. For details on supported operating systems, refer to the *HP Data Protector product announcements, software notes, and references*.

All prerequisites for disaster recovery (i.e. consistent and up-to-date backup, updated SRD file, all faulty hardware replaced...) must be met to recover MSCS.

Consistent backup for MSCS should include (in the same backup session):

- all nodes
- administrative virtual server (defined by the administrator)
- if Data Protector is configured as a cluster aware application, Cell Manager virtual server and IDB.

Disaster recovery of a secondary node

This is the basic scenario for disaster recovery of a MSCS. The following must be true in addition to other prerequisites for disaster recovery:

- at least one of the cluster nodes is functioning properly
- the cluster service is running on that node
- all physical disk resources must be online (i.e. owned by the cluster)
- all normal cluster functionality is available (the cluster administration group is online)
- the Cell Manager is online

In this case, the disaster recovery of a cluster node is the same as the disaster recovery of a Data Protector client. You should follow the instructions for the specific disaster recovery method that you will use to restore the secondary node.

NOTE:

Only local disks are restored, because all shared disks are online and owned by the working node(s) during recovery and locked.

After the secondary node has been recovered, it will join the cluster after boot.

You can restore the MSCS database after all nodes have been recovered and have joined the cluster to ensure its coherency. The MSCS database is part of the CONFIGURATION on Windows. See online Help index: “restore of configuration objects”.

Disaster recovery of the primary node

In this case all nodes in the MSCS are unavailable and the cluster service is not running.

The following must be true in addition to other prerequisites for disaster recovery:

- the primary node must have write access to the quorum disk (the quorum disk should not be locked)
- the primary node must have write access to all IDB volumes, when recovering the Cell Manager
- all other nodes must be shut down until all physical disk resources are online

In this case, restore the primary node with the quorum disk first. The IDB has to be restored as well if the Cell Manager has been installed in the cluster. Optionally you can restore the MSCS database. After the primary node has been restored, you can restore all remaining nodes.

NOTE:

The MSCS service uses a hard disk signature written into the MBR of every hard disk to identify physical disks. If the shared cluster disks have been replaced, this means that the disk signatures were changed during Phase 1 of disaster recovery. As a consequence, the Cluster Service will not recognize the replaced disks as valid cluster resources, and cluster groups depending on those resources will fail. See “Restoring hard disk signatures on Windows” on page 96 for more information.

Perform the following steps to restore the primary node:

1. Perform disaster recovery of the primary node (including the quorum disk).
   - Assisted Manual Disaster Recovery: All user and application data on the quorum disk will be restored automatically by the drstart command. (`-full_clus` option)
   - EADR and OBDR: When you are asked to select the scope of recovery, select **Full with Shared Volumes** to restore quorum disk.
   - Automated System Recovery: All user and application data on the quorum disk will be automatically restored.

   TIP:

   To enable automatic restore of all shared disk volumes in the MSCS using OBDR method, move all volumes temporarily to the node for which you are preparing OBDR boot tape. It is namely impossible to collect enough information to configure the disk in Phase 1 for shared disk volumes that are locked by another node.

2. Reboot the computer.
3. Restore the cluster database. MSCS database is part of the CONFIGURATION on Windows. See online Help index: "restore of configuration objects".

   NOTE:

   The MSCS service must be running in order to be able to restore the MSCS database. Therefore it can not be restored automatically during Phase 2 of disaster recovery. However, the cluster database can be restored at the end of Phase 2 using the standard Data Protector restore procedure.

4. Make the IDB consistent if you are recovering a Cell Manager. See "Making IDB consistent (all methods)" on page 98.

5. The quorum and IBD volumes are restored. All other volumes are left intact and are claimed by the recovered primary node if they are not corrupted.

   If they are corrupted you have to:

   a. disable the cluster service and cluster disk driver (the steps required to do so are described in MSDN Q176970)

   b. reboot the system

   c. reestablish the previous storage structure

   d. enable the cluster disk driver and cluster service

   e. reboot the system

   f. restore user and application data

6. Restore the remaining nodes. See "Disaster recovery of a secondary node" on page 92.

Merging P1S files of all nodes for EADR

Another step is required for EADR after backup has been performed. It is impossible to collect enough information to configure the disk in Phase 1 for shared disk volumes that are locked by another node during backup. This information is necessary to enable the restore of all shared cluster volumes. To include information on shared cluster volumes in the P1S files for all nodes in the cluster, do one of the following:

- After a full client backup has been performed, merge the information on shared cluster volumes in the P1S files for all nodes in the cluster, so that the P1S file of each node contains information on the shared cluster volumes configuration.
- Move all shared cluster volumes temporarily to the node which you are going to back up. This way all required information about all shared cluster volumes can be collected, but only that node can be the primary node.

To merge the P1S files of all nodes, execute the `mmerge.cmd` command from the *`Data_Protector_home`*`\bin\drim\bin`:

```
mmerge p1sA_path ... p1sX_path
```

Where `p1sA` is the full path of the first node's P1S file and `p1sX` is the full path of the P1S file of the last node in the MSCS. Merged P1S files will be saved in the same directory as the source P1S files with the `.merged` appended to their filename (for example, `computer.company.com.merged`). Move the original files to another location and then rename the merged P1S files back to the original name (delete the `.merged` extension).

UNIX Cell Manager only: The `mmerge.cmd` command works only on Windows systems with Data Protector Automatic Disaster Recovery component installed. If you are using a UNIX Cell Manager, copy the P1S files to a Windows client which has Automatic Disaster Recovery component installed and merge the files. Rename the merged P1S files back to the original name and copy them back to the Cell Manager.

Example

Example for merging P1S files for MSCS with 2 nodes: `mmerge` *`Data_Protector_home`*`\Config\server\dr\p1s\node1.company.com` *`Data_Protector_home`*`\Config\server\dr\p1s\node2.company.com`. Enclose the path in quotes on Windows if the path contains a space character. The merged files will be `node1.company.com.merged` and `node2.company.com.merged`. Rename the files back to their original names (you will have to rename the source P1S files first): node1.company.com and node2.company.com.

Restoring hard disk signatures on Windows

The MSCS service uses a hard disk signature written into the MBR of every hard disk to identify physical disks. If the shared cluster disks have been replaced, this means that the disk signatures were changed during Phase 1 of disaster recovery. As a consequence, the Cluster Service will not recognize the replaced disks as valid cluster resources, and cluster groups depending on those resources will fail. This applies only to the restore of the active node, since shared cluster resources are operational as long as at least one of the nodes is up and running and claims ownership of the resources. This problem does not apply to EADR and OBDR critical disks because the original disk signatures of all EADR/OBDR critical disks are automatically recovered. In case you have replaced any other disks, you will have to restore their hard disk signatures as well.

The most critical shared disk is the cluster quorum resource. If it has been replaced, than the original disk signature must be restored, or the cluster service will not start.

During Phase 2, the MSCS Database is restored into the `\TEMP\ClusterDatabase` directory on the system volume. After the system is rebooted, the cluster service will not be running, because the quorum resource will not be identified due to the changed hard disk signature in Phase 1. This can be resolved by running the `clubar` utility (located in the *`Data_Protector_home`*`\bin\utilns`), which restores the original hard disk signature. After clubar successfully finishes, the cluster service is automatically started.

Example

At the command prompt type `clubar r c:\temp\ClusterDatabase force q:` to restore a MSCS Database from `c:\temp\ClusterDatabase`.

For more information on clubar usage and syntax, see the `clubar.txt` file located in the *`Data_Protector_home`*`\bin\utilns`.

If the Data Protector shared disk on the Cell Manager is different from the quorum disk, it has to be restored as well. To restore the signature of the Data Protector shared disk and any other application disk, you should use the `dumpcfg.exe` utility included in the Windows 2000 Resource Kit. For details on using `dumpcfg.exe`, run `dumpcfg /?` or see the Windows 2000 Resource Kit documentation. For more information on the problems with hard disk signatures on Windows, see MSDN article Q280425.

You can obtain the original hard disk signatures from the SRD files. The signature is a number following the `volume` keyword in the SRD file.

Example

```
-volume 5666415943 -number 0 -letter C -offslow 32256
-offshigh 0 -lenlow 320430592 -lenhigh 2 -fttype 4 -ftgroup
0 -ftmember 0
```

```
-volume 3927615943 -number 0 -letter Q -offslow 320495104
-offshigh 2 -lenlow 1339236864 -lenhigh 0 -fttype 4 -ftgroup
0 -ftmember 0
```

The number following the `-volume` keyword is the signature of the hard disk. In this case the SRD file stores information about a local hard disk (with drive letters C) and quorum disk (with drive letter Q). The signature of the quorum disk is stored only in the SRD file of the active node (at backup time), because it keeps the quorum disk locked and thus prevents other nodes from accessing the quorum disk. It is therefore recommended to always back up the whole cluster, because you need the SRD files of all nodes in the cluster, since only all SRD files together include enough information to configure the disk in Phase 1 for shared disk volumes. Note that a hard disk signature stored in the SRD file is represented as a decimal number, whereas `dumpcfg` requires hexadecimal values.

Automated System Recovery on a Majority Node Set cluster

To perform an Automates System Recovery (ASR) on a Majority Node Set (MNS) cluster, follow these steps:

1. Set up the MNS cluster and install a Data Protector client in it.

   Note that it is not possible to install a Cell Manager on a MNS cluster, it is not supported.
2. Perform a filesystem backup, configuration backup, and an IDB backpup.
3. Create an ASR disk set.

   Refer to online Help, index keyword "Automated System Recovery" for instructions on how to prepare for ASR, preparation to create an ASR set, recovery using ASR.
4. Perform Disaster Recovery on the node.

   Refer to online Help, index keyword "disaster recovery" for detailed instructions on how to prepare for disaster recovery and so on.

The node is recovered and can join the cluster.

Restoring the Data Protector Cell Manager specifics

This section explains additional steps for particular methods that should be performed when restoring Windows Cell Manager.

Making IDB consistent (all methods)

The procedure described in this section should only be used after you have performed the general disaster recovery procedure.

To make the IDB consistent, import the medium with the last backup so that the information about the backed up objects is imported to the database. In order to do so, perform the following steps:

1. Using the Data Protector GUI, recycle the medium or media with the backup of the partitions that remain to be restored for enabling the medium or media to be imported in the IDB. Refer to “Recycling Media” on page 110 for more information on how to do this. Sometimes it is not possible to recycle a medium since Data Protector keeps it locked. In such a case stop Data Protector processes and delete the `\tmp` directory by running the following commands:

   Data_Protector_home`\bin\omnisv -stop`

   `del` *Data_Protector_program_data*`\tmp\*.*` (Windows Vista)

   `del` *Data_Protector_home*`\tmp\*.*` (other Windows systems)

   Data_Protector_home`\bin\omnisv -start`

2. Using the Data Protector GUI, export the medium or media with the backup of the partitions that remain to be restored. See the online Help index: "exporting, media" for more information on how to do this.
3. Using the Data Protector GUI, import the medium or media with the backup of the partitions that remain to be restored. See the online Help index: "importing, media" for more information on how to do this.

Enhanced Automated Disaster Recovery specifics

Two additional steps are required in Phase 0 if you are recovering Windows Cell Manager using Enhanced Automated Disaster Recovery:

- Disaster recovery CD for the Cell Manager should be prepared in advance.

IMPORTANT:

Perform a new backup and prepare a new DR CD after each hardware, software or configuration change. This also applies to any network changes, such as change of IP address or DNS server.

- In addition to the Cell Manager, you should save the updated SRD file of the Cell Manager on several secure locations as a part of the disaster recovery preparation policy, because the SRD file is the only file in Data Protector where information about objects and media is stored, when IDB is not available. If the SRD file is saved only on the Cell Manager, it is not accessible if the Cell Manager fails. See "Preparation" on page 42.
- If your backups are encrypted, you must save the encryption key to a removable medium before a disaster occurs. If the encryption key is saved only on the Cell Manager, it is not accessible if the Cell Manager fails. Without the encryption key, disaster recovery is not possible.

  See "Preparation" on page 42.

IMPORTANT:

It is recommended to restrict access to backup media, DR images, SRD files, removable media with encryption keys, and disaster recovery CDs.

One Button Disaster Recovery specifics

Since the IDB is not available if the Cell Manager has crashed, you have to know the location of OBDR bootable medium.

IMPORTANT:

Perform a new OBDR backup and prepare a new bootable medium after each hardware, software or configuration change. This also applies to any network changes, such as change of IP address or DNS server.

If your backups are encrypted, you must save the encryption key to a removable medium before a disaster occurs. If the encryption key is saved only on the Cell Manager, it is not accessible if the Cell Manager fails. Without the encryption key, disaster recovery is not possible.

See "Preparation" on page 42.

IMPORTANT:

It is recommended to restrict access to backup media and removable media with encryption keys.

Automated System Recovery specifics

An additional step is required in Phase 0 if you are recovering Windows Cell Manager using Automated System Recovery (ASR):

- ASR diskette for the Cell Manager should be prepared in advance.

IMPORTANT:

Perform a new backup and update the ASR diskette after each hardware, software or configuration change. This also applies to any network changes, such as change of IP address or DNS server.

IMPORTANT:

It is recommended to restrict access to backup media and ASR diskettes.

Restoring Internet Information Server (IIS) specifics

Internet Information Server (IIS) is not supported for disaster recovery. To perform Assisted Manual Disaster Recovery of an IIS, follow these steps (in addition to the steps required for Assisted Manual disaster recovery):

1. Do not install the IIS during clean installation of the system.
2. Stop or uninstall the IIS Admin Service, if it is running.
3. Run the `drstart` command.
4. The IIS Database is restored as a plain file (with the filename `DisasterRecovery`) into the default IIS location (`%SystemRoot%\system32\inetsrv`).
5. After the successful boot, restore the IIS Database using the standard Data Protector restore procedure or IIS Backup/Restore snap-in. Note that this may take quite some time.

Troubleshooting

1. If any of the IIS dependant services (for example, SMTP, NNTP) do not start automatically, try to start them manually.
2. If this fails, stop the `IIS Admin Service` and restore the `%SystemRoot%\system32\inetsrv\MetaBase.bin` file, using the overwrite option.

NOTE:

`%SystemRoot%\system32\inetsrv` is the default location of `IIS Service`. If you have installed the service into other location, use this location as a destination for restore of `MetaBase.bin` file.

3. Start the IIS Admin Service and all dependant services.

Editing the kb.cfg file

Some drivers have their functionality split into several separate files which are all required for the driver to function properly. Sometimes, it is impossible for Data Protector to identify all driver files during the creation of DR image file, if they are not listed in the `kb.cfg` file on a case-by-case basis. In this case, they will not be included in the disaster recovery operating system and as a consequence, some driver or service will not be operational after the boot of the DR OS.

The `kb.cfg` file is located in the *`Data_Protector_home`*`\bin\drim\config` directory and stores information on the location of driver files, located under the *`%SystemRoot%`* directory. When you execute the test plan, make sure that all required services are running and that all drivers are operational after the boot of the OS.

If you want to back up these drivers, add information about dependant files to the `kb.cfg` file in the appropriate format as described in the instructions at the beginning of the `kb.cfg` file.

The easiest way to edit the file is to copy and paste an existing line and just replace it with the relevant information. Note that the path separator is "`/`" (forward slash). White space is ignored except inside quoted-pathname so the depend entry can therefore span several lines. You can also add comment lines that start with a "`#`" (pound) sign and extend to the end of line.

After you finished editing the file, save it to the original location. Then perform another full client backup as described in "Preparation" on page 58, to include the added files in the DR image.

Due to the numerous configurations of system hardware and applications, it makes it impossible to provide an "out of the box" solution for all possible configurations. Therefore you can modify this file to include drivers or other files at your own risk.

Any modification to this file are at your own risk and as such not supported by Hewlett-Packard.

⚠ WARNING!

It is required to create and execute a test plan to be sure the recovery will work after you have edited the `kb.cfg` file.

Recovery using an edited SRD file

Information about backup devices or media stored in the SRD file may be out of date at the time you are performing disaster recovery. This is not a problem if you are performing an online recovery, because the required information is stored in the IDB on the Cell Manager. But if you are performing an offline recovery, the information stored in the IDB is not accessible.

For example, a disaster struck not only the Cell Manager, but also a backup device connected to it. If you replace the backup device with a different backup device after the disaster, the information on backup devices stored in the updated SRD file (`recovery.srd`) will be wrong and the recovery will fail. In this case, edit the updated SRD file before performing Phase 2 of disaster recovery to update the wrong information and thus enable a successful recovery.

To edit the SRD file, open it in a text editor and update the information that has changed.

TIP:

You can display the device configuration information using the `devbra -dev` command.

For example, if the client name of the computer you are trying to recover has changed, replace the value of the `-host`option. You can also edit the information about the:

- Cell Manager client name (`-cm`).
- Media Agent client (`-mahost`).
- Logical device or drive (library) name (`-dev`).
- Device type (`-devtype`).

  Refer to the `sanconf` man page or HP Data Protector command line interface reference for possible `-devtype` option values.
- Device SCSI address (`-devaddr`).
- Device policy (`-devpolicy`).

  Policy can be defined as `1` (Standalone), `3` (Stacker), `5` (Jukebox), `6` (external control), `8` (Grau DAS exchanger library), `9` (STK Silo medium library) or `10` (SCSI-II Library).
- Robotics SCSI address (`-devioctl`).
- Library slot (`-physloc`)
- Logical library name (`-storname`)

After you have edited the file, save it in Unicode format to the original location.

Example

Changing a MA Client

You performed a disaster recovery backup using a backup device connected to the client `old_mahost.company.com`. At the time of disaster recovery, the same backup device is connected to the client `new_mahost.company.com` with the same SCSI address. To perform a disaster recovery, replace the `-mahost old_mahost.company.com` string in the (updated) SRD file with `-mahost new_mahost.company.com`, before performing the Phase 2 of disaster recovery.

If the backup device has a different SCSI address on the new MA client, modify the value of the `-devaddr` option in the updated SRD file accordingly.

Example

Changing a backup device and MA client

To perform disaster recovery using another device than the one which was used for the backup (MA client is the same), modify the following option values in the updated SRD file: `-dev`, `-devaddr`, `-devtype`, `-devpolicy`, and `-devioctl`. If you are using a library device for restore, modify also the values of the following options in the SRD file: `-physloc`, and `-storname`.

For example, you performed backup for disaster recovery purposes using an HP StorageWorks Ultrium standalone device with the device name `Ultrium_dagnja`, connected to the MA host `dagnja` (Windows). However, for the disaster recovery you would like to use an HP StorageWorks Ultrium robotics library with the logical library name `Autoldr_kerala` with drive `Ultrium_kerala` connected to the MA client `kerala` (Linux).

First, run the `devbra -dev` command on `kerala` to display the list of configured devices and their configuration information. You will need this information to replace the following option values in the updated SRD file:

```
-dev "Ultrium_dagnja" -devaddr Tape4:1:0:1C -devtype 13
-devpolicy 1 -mahost dagnja.company.com
```

with something like:

```
-dev "Ultrium_kerala" -devaddr /dev/nst0 -devtype 13
-devpolicy 10 -devioctl /dev/sg1 -physloc " 2 -1" -storname
"AutoLdr_kerala" -mahost kerala.company.com.
```

The procedure on using the edited SRD file for disaster recovery is different for each disaster recovery method. Specific details are explained in the sections pertaining to disaster recovery methods.

IMPORTANT:

You should restrict access to the SRD files due to security reasons.

AMDR/ASR

Perform the following before proceeding with the normal AMDR/ASR recovery procedure:

1. Open the `recovery.srd` file (located on the first `drsetup` / ASR diskette) in a text editor and make the necessary changes.
2. Save the file to its original location in Unicode format.

EADR/OBDR

Perform the following additional steps before proceeding with the normal EADR/OBDR recovery procedure:

1. When the Disaster Recovery wizard appears, press any key to stop the wizard during the countdown, select the **Install only** option and click **Finish**. This option will install only the temporary operating system to the target system and thus finish Phase 1 of disaster recovery. Phase 2 of disaster recovery will not start automatically if the Install only option is selected.

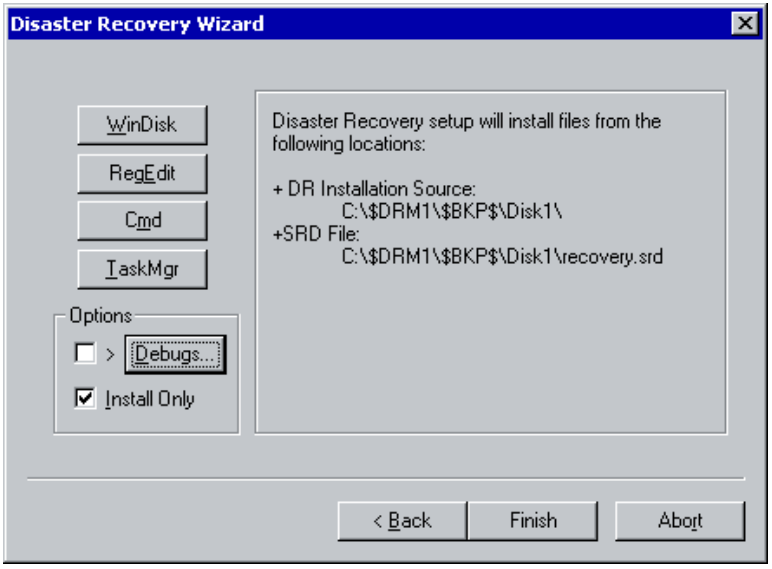


Figure 9 Install only option in the Disaster Recovery wizard

2. Run Windows Task Manager (press **Alt**+**Ctrl**+**Del** and select **Task Manager**).
3. Click **File** and then **New task (Run...).** Type `notepad c:\DRSYS\System32\OB2DR\bin\recovery.srd` and press **Enter**. The SRD file will be opened in the Notepad.
4. Edit the SRD file. For details on how to edit it, refer to "Updating and editing the system recovery data (SRD)" on page 36.
5. After you have edited and saved the SRD file, run the following command from `c:\DRSYS\System32\OB2DR\bin`:

   ```
   omnidr -drimini c:\$DRIM$.OB2\OBRecovery.ini
   ```

6. Proceed with the next step in the normal EADR/OBDR recovery procedure.

Updating the ASR diskettes using the CLI interface

Data Protector does not offer a command line interface command to *automatically* create ASR diskettes. However, you can manually update the contents of the first diskette in the ASR set by running the `omnisrdupdate` command. Insert the first diskette from the ASR set in to the floppy drive and specify `a:\` as the location, for example:

```
omnisrdupdate -session 11/04/2005-1 -host computer1.com
-location a:\ -asr
```

To *manually* create an ASR diskette, you also need to copy the `DR`*`disk_number`*`.cab` files from *`Data_Protector_home`*`\Depot\DRSetup\Disk`*`disk_number`* folders to the appropriate ASR diskette.

Windows Vista BitLocker Drive Encryption

If the volumes are encrypted using BitLocker Drive Encryption, the disaster recovery module will detect them and offer the option to unlock the encrypted drives:

```
System storage inspection discovered n locked volume(s).
Unlock? [y/n]
```

1. Press **y** to start the unlocking procedure.
2. Press **2** to open the selection menu.

3. Check if the volume containing the password (for example an USB key) is listed in the search path. The message will look similar to the following one:

```
Search dir(s): [a:\]
[d:\]
```

If the path is not listed:

a. Enter `search`. A new menu will display.

b. Enter the search directory, for example `m:` if your USB key is mounted under `m:\`. You can add several directories at once.

The directory is now listed in the search path.

```
Search dir(s): [a:\]
[d:\]
[m:\]
```

4. Enter the volume to unlock, for example `c:`. You can also specify a volume without the drive letter, the volume GUID (for example `\\?\Volume{`*`GUID`*`}`), or multiple volumes at once.

To unlock all volumes, enter `all`.

If the key files cannot be retrieved from the USB key or floppy, the following prompt will display:

```
Type one of the following:
* External key path
* Numerical password (groups separated by hyphens)
* Exit
```

Enter the numerical password.

4 Disaster recovery for UNIX

Manual disaster recovery of an HP-UX client

This section explains the procedure that should be used to recover an HP-UX client from a disaster.

The procedure is based on the Ignite-UX product; an application primary developed for HP-UX system installation and configuration tasks, which offers (in addition to a powerful interface for the system administration) preparation and recovery of the system from a disaster.

While Ignite-UX is focused on the disaster recovery of the target client (Phase 1 and Phase 2), Data Protector has to be used to restore the user and application data in order to complete the Phase 3 of disaster recovery.

NOTE:

This section does not cover the full functionality of Ignite-UX. For detailed information refer to the *Ignite-UX administration guide*.

Overview

Ignite-UX offers 2 different approaches to prepare a system for and recover a system from a disaster:

- Using custom installation medium (Golden Image)
- Using system recovery tools (**make_tape_recovery**, **make_net_recovery**)

While the usage of Golden Image is most suitable for IT environments with a large number of basically identical hardware configurations and OS releases, the usage of the system recovery tools supports the creation of recovery archives, which are customized for your individual systems.

Both methods allow the creation of bootable installation media like DDS-Tapes or CD's. Using these media, the system administrator is able to perform a local disaster

recovery directly from the system console of the failed client. In addition, both methods can also be used to run a network based recovery of the client by assigning the failed client a suitable Golden Image or the previously created “recovery archive”. In this case, the client boots directly from the Ignite Server and runs the installation from the assigned depot, which has to be located on a NFS share on your network.

Use Ignite-UX GUI where it is supported.

Using custom installation medium

Overview

Large IT environments often consist of a large number of systems that are based on identical hardware and software. Installation of OS, applications and required patches can be significantly reduced if a complete snapshot of the installed system is used to install other systems. Ignite-UX includes a feature, which allows you to modify parameters like networking or filesystem settings and add software like Data Protector to the image (with Ignite-UX command `make_config`) before you assign such a Golden Image to another system. This feature can thus be used to recover a system from a disaster.

The general steps using a custom installation medium are:

1. **Phase 0**
   a. Create a Golden Image of a client system.
2. **Phase 1 and 2**
   a. Replace the faulty disk with a replacement disk.
   b. Boot the HP-UX client from the Ignite-UX server and configure the network.
   c. Install the Golden Image from the Ignite-UX server.
3. **Phase 3**
   a. Use the standard Data Protector restore procedure to restore user and application data.

Preparation

The following steps explain how to create a Golden Image of a client system on a target system, which will share the image via NFS to your network. In this example, Data Protector client is already installed on the client system and will be included in the “Golden Image” without additional configuration steps.

1. Copy the `/opt/ignite/data/scripts/make_sys_image` file from your Ignite-UX Server into a temporary directory on the client system.
2. Run the following command on the client node to create a compressed image of the client on another system: `make_sys_image -ddirectory of the archive-n`*`name of the archive`*`.gz -s`*` IP address of the target system`*

   This command will create a gzipped file depot in the specified directory on the system defined with the `-d` and `-s` options. Make sure that your HP-UX client has granted a passwordless access to the target system (an entry in the `.rhosts` file with the name of the client system on the target system) otherwise the command will fail.
3. Add the target directory to the `/etc/exports` directory on the target system and export the directory on the target server (`exportfs -av`).
4. On the Configuring Ignite-UX server, copy the archive template file `core.cfg` to `archive_`*`name`*`.cfg`: `cp /opt/ignite/data/examples/core.cfg /var/opt/ignite/data/`*`OS_Release`*`/archive_`*`name`*`.cfg`

Example

```
cp /opt/ignite/data/examples/core.cfg
/var/opt/ignite/data/Rel_B.11.11/archive_HPUX11_11_DP50_CL.cfg
```

5. Check and change the following parameters in the copied configuration file:
   - In the `sw_source` section:

     ```
     load_order = 0
     source_format = archive
     source_type="NET"
     # change_media=FALSE
     post_load_script = "/opt/ignite/data/scripts/os_arch_post_l"
     post_config_script =
     "/opt/ignite/data/scripts/os_arch_post_c"
     nfs_source = "IP Target System:Full Path"
     ```
   - In the matching `OS archive` section:

     ```
     archive_path = "archive_name.gz
     ```

6. Determine the “impacts” entries by running the command `archive_impact` on your image file and copy the output in the same “OS archive” section of your configuration file:

   ```
   /opt/ignite/lbin/archive_impact -t -g archive_name.gz
   ```

Example

```
/opt/ignite/lbin/archive_impact -t -g
/image/archive_HPUX11_11_DP50_CL.gz
impacts = "/" 506Kb
impacts = "/.root" 32Kb
impacts = "/dev" 12Kb
impacts = "/etc" 26275Kb
impacts = "/opt" 827022Kb
impacts = "/sbin" 35124Kb
impacts = "/stand" 1116Kb
impacts = "/tcadm" 1Kb
impacts = "/usr" 729579Kb
impacts = "/var" 254639Kb
```

7. To make Ignite-UX aware of the new created depot, add an `cfg` entry to the `/var/opt/ignite/INDEX` file with the following layout:

   ```
   cfg "This_configuration_name" {
   description "Description of this configuration”
   "/opt/ignite/data/OS/config"
   "/var/opt/ignite/data/OS/ archive_name.cfg
   }
   ```

Example

```
cfg "HPUX11_11_DP50_Client" {
description "HPUX 11.i OS incl Patches and DP50 Client"
"/opt/ignite/data/Rel_B.11.11/config"
"/var/opt/ignite/data/Rel_B.11.11/archive_HPUX11_11_DP50_CL.cfg
"
}
```

8. Make sure that one or more IP addresses reserved for booting clients are configured in the `/etc/opt/ignite/instl_boottab` file. The number of IP addresses is equal to the number of parallel booting clients.

After the above described procedure is completed, you have a Golden Image of an HP-UX client (with a specific hardware and software configuration), which can be used to recover any client of a similar layout.

Repeat these steps to create a Golden Image for all systems with different hardware and software configuration.

NOTE:

Ignite-UX enables you to create a bootable tape or CD based on the created Golden Image. Please refer to the *Ignite-UX administration guide* for more information. Ignite-UX enables you to create a bootable tape or CD based on the created Golden Image. Please refer to the Ignite-UX Administration Guide for more information.

Recovery

To recover an HP-UX client by applying the Golden Image, which is located on a NFS share on your network, perform the following steps:

1. *On the Client System:*
   a. Replace the faulty hardware.
   b. Boot the HP-UX client from the Ignite-UX server: `boot lan.`*`IP-address Ignite-UX server`*`install`.
   c. Select **Install HP-UX** when the Welcome to Ignite-UX screen appears.
   d. Choose **Remote graphical interface running on the Ignite-UX server** from the UI Option screen.
   e. Respond to the Network configuration dialog.
   f. The system is now prepared for a remote Ignite-UX Server controlled installation.
2. *On the Ignite-UX Server:*
   a. Right click the **client** icon in the Ignite-UX GUI and select **Install Client – New Install.**
   b. Select the Golden Image you want to install, check the settings (network, filesystem, time zone,...) and click the **Go!** button.
   c. You can check the installation progress by right clicking the **client** icon and choosing **Client Status...**
   d. After the installation has finished, restore additional user and application data using the standard Data Protector restore procedure.

Using system recovery tools

Overview

The usage of the system recovery tools, bundled with the Ignite-UX, enables you a fast and easy recovery from a disk failure. The recovery archive of system recovery tools includes only essential HP-UX directories. However, it is possible to include other files and directories (for example, additional volume groups or the Data Protector files and directories) in the archive to speed up the recovery process.

`make_tape_recovery` creates a bootable recovery (installation) tape, customized for your system and enables you unattended disaster recovery by connecting the backup device directly to the target system and booting the target system from the bootable recovery tape. The backup device has to be locally connected to the client during the creation of the archive and recovery of the client.

`make_net_recovery` allows you to create a recovery archive over the network onto the Ignite-UX server or any other specified system. The target system can be recovered across subnets after booting ether from a bootable tape created by the Ignite-UX `make_boot_tape` command or the system boots directly from the Ignite-UX server. Booting directly from the Ignite-UX server can be automated with the Ignite-UX `bootsys` command or interactively specified on the boot console.

The general steps using system recovery tools are:

1. **Phase 0**
   a. Create a recovery archive of an HP-UX client using the Ignite-UX GUI on the Ignite-UX server.
2. **Phase 1 and 2**
   a. Replace the faulty disk with a replacement disk.
   b. For local restore, boot from the prepared recovery tape.
   c. In case of a local restore, the recovery process starts automatically.

      For network restore, boot from the Ignite-UX client and configure the network and UI.

      In case of a network restore, install the Golden Image from the Ignite-UX server.
3. **Phase 3**
   a. Use the standard Data Protector restore procedure to restore user and application data.

Preparation

The easiest way to create a recovery archive of an HP-UX client is to use the Ignite-UX GUI on the Ignite-UX server. All GUI commands can also be executed from the command line. Refer to the *Ignite-UX administration guide* for more information.

Prerequisites

Before you are able to prepare your system for disaster, the Ignite-UX fileset has to be installed on the client in order to enable the Ignite-UX server to communicate with the client. Make sure that the revisions of the Ignite-UX fileset on the Ignite-UX server and on the client are the same. The simplest way to keep everything consistent is to install Ignite-UX from a depot build on the Ignite-UX server. This depot can be constructed by running the following command on the Ignite-UX server:

```
pkg_rec_depot -f
```

This creates an Ignite-UX depot under `/var/opt/ignite/depots/recovery_cmds`, which can be specified as a source directory by `swinstall` on the client for the Ignite-UX software installation.

After you have installed Ignite-UX on the client node, you can use the GUI on the Ignite-UX server to create recovery archives using `make_net_recovery` or `make_tape_recovery`.

Creating an archive using make_tape_recovery

Perform the following steps to create an archive using `make_tape_recovery`:

1. Make sure that a backup device is connected to the HP-UX client.
2. Start the Ignite-UX GUI by executing the following command:
   `/opt/ignite/bin/ignite &`
3. Right click the **client** icon and select **Create Tape Recovery Archive**.
4. Select a tape device, if more than one device is connected to the HP-UX client.
5. Select the volume groups you want to include into the archive.

6. The tape creation process will now begin. Check the status and log file on the Ignite-UX server by right clicking the **client** icon and selecting **Client Status**.

NOTE:

Ignite-UX recommends the usage of 90m DDS1 backup tapes to ensure that the tape will work with all DDS with any DDS drive.

Creating an archive using make_net_recovery

The procedure for creating a recovery archive using `make_net_recovery` is almost the same as using `make_tape_recovery`. The advantage is that there is no need for a locally attached backup device, as the recovery archive is stored on the Ignite-UX server by default.

1. Start the Ignite-UX GUI by executing the following command:
   `/opt/ignite/bin/ignite &`
2. Right click the **client** icon and select **Create Network Recovery Archive**.
3. Select the destination system and directory. Make sure that there is enough space to store the compressed archive.
4. Select the volume groups you want to include into the archive.
5. The archive creation process will now begin. Check the status and log file on the Ignite-UX server by right clicking the **client** icon and selecting **Client Status**.

NOTE:

Ignite-UX allows you to create bootable archive tape out of the compressed archive file. See the chapter Create a Bootable Archive Tape via the Network in the *Ignite-UX Administration Guide*.

Recovery

Recovery from the backup tape

To recover a system from a disaster using the bootable tape created by `make_tape_recovery` follow the steps below:

1. Replace the faulty hardware.

2. Make sure that the tape device is locally connected to the crashed HP-UX client and insert the medium with the archive you want to restore.
3. Boot from the prepared recovery tape. To do so, type in `SEARCH` at the boot admin menu to get a list of all available boot devices. Determine which one is the tape drive and type in the boot command: `boot` *`hardware path`* or `boot Pnumber`.
4. The recovery process starts automatically.
5. After the recovery has completed successfully, restore additional user and application data using the standard Data Protector restore procedure.

Recovery from the network

To recover an HP-UX client from a disaster via the network, follow the instructions on how to perform recovery with a Golden Image. Make sure you have selected the desired archive for the installation.

- **On the Client:**
  1. Replace the faulty hardware.
  2. Boot the HP-UX client from the Ignite-UX server:

     `boot lan.`*`IP-address Ignite-UX server`*`install`
  3. Select **Install HP-UX** from the Welcome to Ignite-UX screen.
  4. Choose **Remote graphical interface running on the Ignite-UX server** on the UI Option screen.
  5. Respond to the Network configuration dialog.
  6. The system is now prepared for a remote installation controlled from the Ignite-UX Server.
- **On the Ignite-UX Server:**
  1. Right click the **client** icon within the Ignite-UX GUI and select **Install Client – New Install**.
  2. Under Configurations: select the **Recovery Archive** you want to install, check the settings (network, filesystem, time zone,...) and click the **Go!** button.
  3. You can check the installation progress by right clicking the **client** icon and choosing **Client Status...**
  4. After the recovery has completed successfully, restore additional user and application data using the standard Data Protector restore procedure.

Disk delivery disaster recovery of a UNIX client

To perform a disk delivery disaster recovery of a UNIX client, connect a bootable disk that contains a minimal OS installation and Data Protector Disk Agent to the crashed system. The administrator has to ensure (before the disaster) that enough data has been collected to correctly format and partition the disk.

For details on supported operating systems, refer to the *HP Data Protector product announcements, software notes, and references*.

Overview

Disk Delivery of a UNIX client is performed using an auxiliary disk (which can be carried around), with a minimal operating system with networking and a Data Protector agent installed on it.

The general steps using an auxiliary disk for a UNIX client are:

1. **Phase 0**
   a. Perform a full client backup and IDB backup (Cell Manager only).
   b. Create an auxiliary disk.
2. **Phase 1**
   a. Replace the faulty disk with a replacement disk, connect the auxiliary disk to the target system and reboot the system with the minimal operating system installed on the auxiliary disk.
   b. Manually re-partition the replacement disk and re-establish the storage structure and make the replacement disk bootable.
3. **Phase 2**
   a. Use the standard Data Protector restore procedure to restore the boot disk of the original system onto the replacement disk (use the Restore into option).
   b. Shut down the system and remove the auxiliary disk. You do not need to shut down the system if you are using a hot-swappable hard disk drive.
   c. Reboot the system.
4. **Phase 3**
   a. Use the standard Data Protector restore procedure to restore user and application data.

Limitations

- This description does not cover the recovery of a cluster environment. Depending on the configuration of the cluster environment, additional steps and modification to the environment are necessary.
- RAID is not supported.
- Auxiliary disk should be prepared on a system of the same hardware class as the target system.

Preparation

Preparation for this disaster recovery method should be performed on several levels: gathering the information for your backup specification, preparing the disk, preparing your backup specification (pre-exec), and executing the backup. All of these preparatory steps are necessary before executing disaster recovery of the client.

This section provides a list of items that need to be executed for each target system at backup time, in order to perform successful disaster recovery. If the information is collected as part of a pre-exec command, it is important to document the location of these files in the Disaster Recovery plan so that the information can be found once disaster strikes. Also version administration (there is a collection of the "auxiliary information" per backup) has to be considered.

- If the system that will be backed up has application processes active at low run levels, establish a state of *minimal activity* (modified *init 1 run level*) and enter the single user mode to prevent errors after recovery (see "Consistent and relevant backup" on page 34). Consult your operating system documentation for details.

  HP-UX:

Example

1. Move some kill links from `/sbin/rc1.d` to `/sbin/rc0.d` and complement the changes for the boot-up section. The kill links include the basic services that would otherwise be suspended by moving to run level 1, and they are needed for the backup. For an example, see "Move kill links on HP-UX 11.x" on page 143.

2. Ensure that `rpcd` is configured on the system (configure the variable `RPCD=1` within the file `/etc/rc.config.d/dce`).

   This prepares the system so that it enters the state of minimal activity. The state can be characterized as follows:

   - `Init-1` (`FS_mounted, hostname_set, date_set, syncer_running`)
   - Network must be running
   - The following processes should also be running: `inetd`, `rpcd`, `swagentd`

Solaris:

Example

1. Move the `rpc` kill link from `/etc/rc1.d` to `/etc/rc0.d` and complement the change for the boot-up section. The kill links include the basic services that would otherwise be suspended by moving to run level 1, and they are needed for the backup.
2. Ensure that `rpcbind` is configured on the system.

   This prepares the system so that it enters the state of minimal activity. The state can be characterized as follows:

   - `Init 1`
   - Network must be running
   - The following processes should also be running: `inetd`, `rpcbind`.

Tru64:

Example

1. If the system is powered down, boot up the system and enter the System Reference Manual (SRM) console (the firmware console).
2. Execute the following command from the SRM console to enter the single user mode:

   - `boot -fl s` to boot using already generated vmunix file
   - `boot -fi genvmunix -fl s` to boot into the single user mode with the generic kernel.
3. If the system is already powered up and running, change from the current run level to single-user mode by executing the following command: `init s`

AIX:

No action is required, because the `alt_disk_install` command, used to prepare the auxiliary disk, ensures consistent disk image without entering the state of minimal system activity.

- If you want to work with the auxiliary boot disk, you have to prepare it. Only one bootable auxiliary disk is required per site and platform. This disk has to contain the operating system and network configuration, and has to be bootable.
- Provide a Pre-exec script that performs the following:
  - Physical and logical storage structure of the storage
  - Current logical volume structure (for example, on HP-UX, using `vgcfgbackup` and `vgdisplay -v`)
  - ServiceGuard configuration data, disk-mirroring, striping
  - Filesystems and mountpoints overview (for example, on HP-UX, using bdf or copy of `/etc/fstab`)
  - System paging space information, for example, on HP-UX, using the output of the `swapinfo` command
  - I/O-structure overview (for example, on HP-UX, using ioscan -fun and `ioscan -fkn`)
  - Client network settings

  Collects all the necessary information about the environment and puts it in an available location in case of a disaster recovery. It is suggested to put it onto a different system which can be accessed easily. The information should cover:
  - An emergency copy of the data can also be put into the backup itself. If done so, the information has to then be extracted prior to the actual recovery.
  - Consider logging out all users from the system.
  - Shut down all applications, unless the application data gets backed up separately, for example, using online database backup.
  - You may want to restrict network access to the system, so that no one can log on to the system while the backup is running (for example, on HP-UX, overwrite `inetd.sec` and use `inetd -c`).
  - If needed, enter the state of minimal system activity (for example, on HP-UX, use `sbin/init 1`; wait 60; check if run_level 1 is reached). Note that this is a modified “init 1" state.
- Provide a post-exec script that elevates the system to the standard run-level, restarts applications, and so on.

- Setup a backup specification for the client on the Data Protector Cell Manager. It should include all the discs (with disc discovery) and include the pre- and post-exec scripts.
- Execute this backup procedure and repeat it on a regular basis, or at least at every major system configuration change, especially any change in the logical volume structure (for example, using LVM on HP-UX).

Recovery

This section describes how to restore a system to the state when the backup was done. You will need the following to successfully perform a Disk Delivery Disaster Recovery:

- A new hard disk to replace your crashed disk.
- An auxiliary disk containing the relevant operating system and the Data Protector agents.
- A successful full backup of the client that you want to recover.

The following steps need to be performed:

1. Replace the faulty disk with a new disk of comparable size.
2. Attach the auxiliary disk (which contains the relevant operating system and the Data Protector client) to the system and make it the boot device.
3. Boot from the auxiliary operating system.
4. Reconstruct the logical volume structure if applicable (for example, using LVM on HP-UX). Use the saved data for the non-root volume groups (for example, with `vgcfgrestore` or SAM on HP-UX).
5. Additionally, the root volume group to be restored has to be created on the repaired disk (for example, using `vgimport` on HP-UX). It will not look like a root volume group during the restore process. This is because the OS from the auxiliary disk will be running. For more information on `vgimport`, see its man page.
6. Make the new disk bootable.
7. Reconstruct any other storage structures like mirror, striping, service guard, and so on from the data saved on a secondary storage device during backup.
8. Create the filesystems and mount them as required by the data from the backup; use similar but not the original mountpoint names (like `/etc_restore` for `/etc`, and so on).
9. Remove any files in the mountpoints to be restored, they must be clean.

10. Start the Data Protector GUI and open a connection to the Cell Manager. Import the system with the auxiliary disk into the cell.
11. Select the version from which you want to restore. First list all the required media for the restore and make sure they are available. Restore all the required mountpoints including the (future) root-volume to the system, using the option **Restore As** *new_mountpoint*. The root-volume from the backup is restored to the root-volume on the repaired disk. Nothing is restored to the currently-running auxiliary operating system on the auxiliary disk.
12. Shut down the system that was just restored.
13. Disconnect the auxiliary disk from the system.
14. Reboot the system from the new (or repaired) disk.

NOTE:

Instead of using an auxiliary disk, the new disk can also be temporarily connected to a client that has to have a Disk Agent installed. After being restored, it can be connected to the faulty system and booted.

Manual disaster recovery of a UNIX Cell Manager

Manual Disaster Recovery is a basic method, that involves recovering the system by reinstalling it in the same way as it was initially installed. In addition, Data Protector is used to then restore all files, including the operating system.

Overview

The general procedure for a manual disaster recovery of a UNIX Cell Manager is:

1. **Phase 0**
   a. Perform a full client backup and IDB backup.
   b. Collect information on the original system to enable installation and configuration of DR OS.
2. **Phase 1:**
   a. Replace the faulty hardware.
   b. Manually re-partition the disk and re-establish the storage structure.
   c. Reinstall the operating system.

d. Reinstall patches.

3. **Phase 2**
   a. Reinstall the Data Protector Cell Manager.
   b. Restore the latest backup of the IDB to simplify the restore of all other files from media.
   c. Replace the Data Protector configuration information (`/etc/opt/omni`) with the latest Data Protector configuration information from the backup to re-create the previous configuration.
4. **Phase 3**
   a. Use Data Protector standard restore procedure to restore user and application data.
   b. Reboot the system.

Limitation

For details on supported operating systems, refer to the *HP Data Protector product announcements, software notes, and references*.

This description does not cover the recovery of a cluster environment. Depending on the configuration of the cluster environment, additional steps and modification to the environment are necessary.

Preparation

Perform the same preparatory steps without the steps pertaining to the auxiliary disk, as for Disk Delivery Disaster Recovery of an HP-UX or Solaris client. See "Preparation" on page 119 for reference. In addition to completing those steps, you also have to complete the following:

1. The IDB has to be backed up regularly, ideally in a separate backup specification, scheduled after the backup of the Cell Manager.
2. The IDB and configuration backup must run to a specific device located on the Cell Manager system, to make the administrator aware that the medium in the device contains the most recent version of the IDB.

Recovery

Use the following method to recover your UNIX Cell Manager.

Prerequisites

You will need the following to successfully perform a disaster recovery:

- Media containing the last valid known backup of the root partition of the Cell Manager and IDB.
- A device connected to the Cell Manager.

The following steps need to be performed to recover a Cell Manager:

1. Replace the crashed disk.
2. Boot your system from the installation media of your operating system.
3. Reinstall the operating system. Refer to your system administrator's manual for instructions. During the installation, using the data gathered during the preparation phase (pre-exec script), re-create and configure the physical and logical storage structure of the storage, logical volume structure, filesystem and mountpoints, network settings and other.
4. Reinstall the Data Protector on the Cell Manager.
5. Restore the latest backup of your database and `/etc/opt/omni` to a temporary directory. This simplifies the restore of all other files from media.

NOTE:

You cannot restore the database directly. See the online Help for instructions. This includes stopping all Data Protector processes with the `/opt/omni/sbin/omnisv -stop` command. This ensures that no files will be in use.

6. Remove the `/etc/opt/omni` directory and replace it with the `/etc/opt/omni` directory from the temporary area. This re-creates the previous configuration.
7. Start Data Protector processes with the `/opt/omni/sbin/omnisv -start` command.
8. Start the Data Protector user interface and restore all the files used from your backup.
9. Reboot the system.

Your Cell Manager should now be successfully recovered.

5 Troubleshooting disaster recovery

In this chapter

This chapter contains descriptions of problems you might encounter while performing a disaster recovery. You can start with problems connected to a particular disaster recovery method and continue with general disaster recovery problems. See "The autodr.log file" on page 127 for information where to find the error messages.

For general Data Protector troubleshooting information, see the *HP Data Protector troubleshooting guide*.

Before you begin

- Ensure that the latest official Data Protector patches are installed. See the online Help index: "patches" on how to verify this.
- See the *HP Data Protector product announcements, software notes, and references* for general Data Protector limitations, as well as known problems and workarounds.
- See http://www.hp.com/support/manuals for an up-to-date list of supported versions, platforms, and other information.

General troubleshooting

The autodr.log file

`Autodr.log` is a log file located in the *`Data_Protector_home`*`\tmp` directory and contains messages relevant to the automatic disaster recovery methods (EADR, ODBR, ASR). You should inspect it if an error has occurred. `Autodr.log` logs many different messages, mostly for development and support purposes. Only some of

them are relevant to you and indicate that an error has occurred. These error messages are usually logged at the end of the log file with a traceback appended.

There are four types/levels of messages in the `autodr.log` (note that they do not correspond to the same report levels for messages that are reported at the end of a backup session in the Data Protector GUI):

- `Critical error`: The error is so serious that the backup of the object can not continue and will be aborted.
- `Error`: The error may be critical, but it depends on different factors.

  For example, `autodr.log` reports an error that some driver has not been included in the disaster recovery operating system. The missing driver may be the reason for the recovered system not to be operational after the recovery or only for some non-critical service not to be running after the boot of the operating system. It depends on which driver has not been backed up.
- `Warning` and `Info`: These are not error messages and usually do not mean that anything is wrong.

Some of the most common messages stated in the `autodr.log` file are:

- `unsupported location`: Data Protector notices that a certain file that is required by a service or a driver that will be included in the disaster recovery operating system (DR OS), is not located under the *`%SystemRoot%`* directory.

  Such drivers are often used by the antivirus and remote control software (for example pcAnywhere). This message is important, because it can mean that the service/driver that requires the missing file, will not be operational after the boot. It depends on which service or driver was affected, if the disaster recovery will fail or succeed. A possible solution for this problem is copying the missing file into the *`%SystemRoot%`* directory and changing its path in the Windows Registry. Note that incorrect editing of the Windows Registry may severely damage your system.

Debugging the disaster recovery session

You can instruct Data Protector to create and save debug logs during a disaster recovery session. This option is available only for EADR and OBDR.

To enable debugging:

1. Select the check mark to the left of the Debugs button in the Disaster recovery wizard.

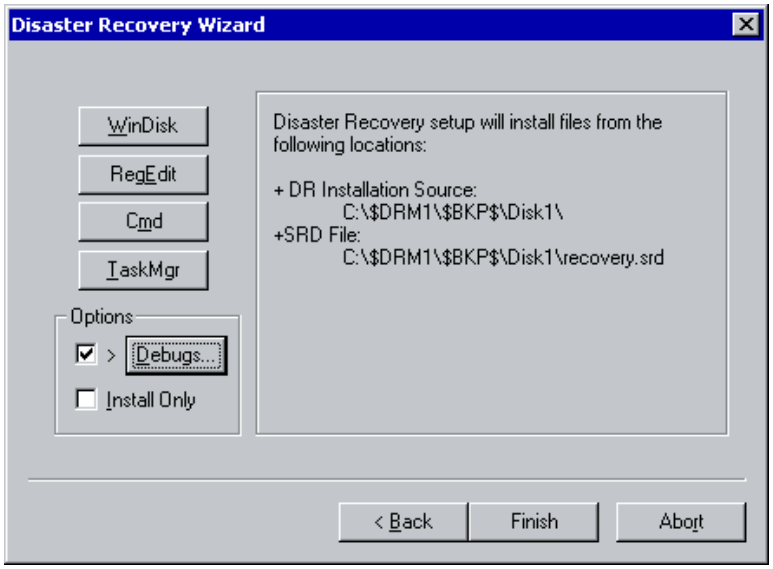


Figure 10 Enabling debugs during a disaster recovery session

2. To specify the debug options, such as the location where the debugs are saved, click **Debugs**. By default, the debugs are saved in to `%System32%\ob2dr\tmp`.

NOTE:

On Windows Vista systems, you must specify the location to which the debugs are saved if you expect that the restore session will produce a large amount of debugs. The amount of available space on the Windows Vista RAM disk is very limited (typically less than 32 MB), and if the limit is exceeded, Data Protector may behave unpredictably.

3. The Debug Options window appears.

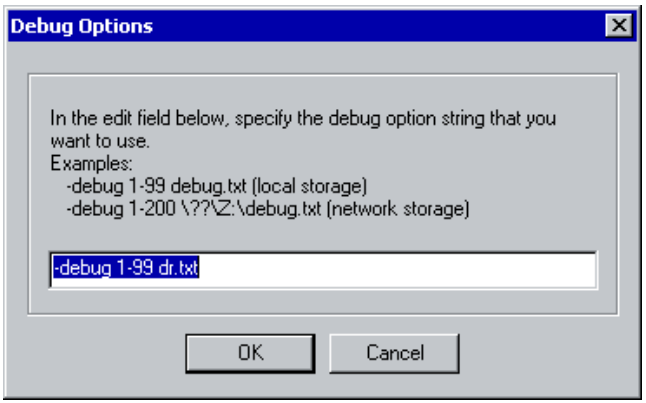


Figure 11 Changing the debug logs location

Enter the location where the debug logs are saved. The drive letter must be preceded by `\\?`, for example, `\\?\Z:\debug.txt`.

If you choose to save the debugs on a network share, use the `net use` command to mount the share to which the debug logs are written. For example:

`NET USE X: "\\client\debug_output_folder /user:username password"`

Setting omnirc options during disaster recovery on Windows

For general information on `omnirc` options, see the *HP Data Protector troubleshooting guide*.

If you need to set an omnirc option during the disaster recovery on Windows (except for Disk Delivery Disaster Recovery), perform the following steps:

1. When the Disaster Recovery Wizard appears, press any key to stop the wizard during the countdown.

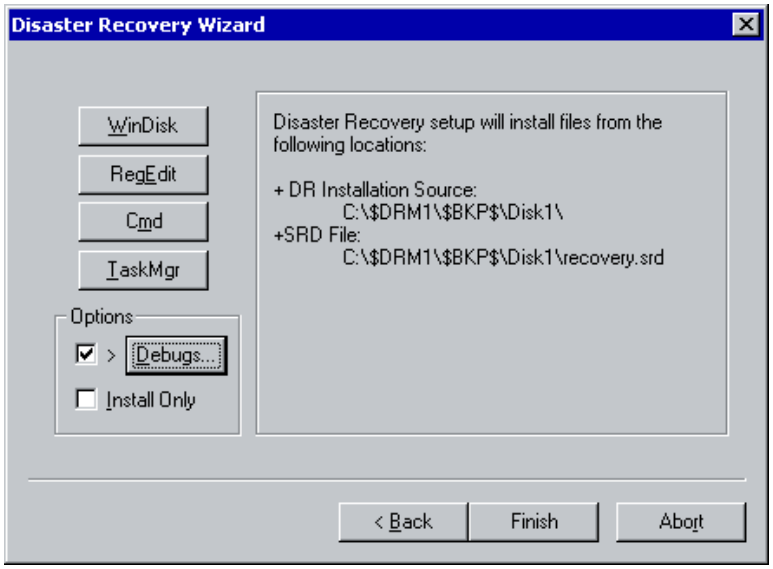


Figure 12 Disaster recovery wizard

2. Click **Cmd** to start the command prompt.
3. Run the following command:

   `echo variable > %systemroot%\system32\OB2DR\omnirc`

   where `variable` is the omnirc option exactly as it should be written in the `omnirc` file.

   For example:

   ```
   echo OB2RECONNECT_RETRY=1000 >
   %systemroot%\system32\OB2DR\omnirc
   ```

   This command creates an `omnirc` file in the disaster recovery operating system with the `OB2RECONNECT_RETRY` variable set to `1000` seconds.
4. Close the command prompt and click **Next** in the Disaster Recovery Wizard to proceed with disaster recovery.

The drm.cfg file

The Data Protector disaster recovery configuration is set up to cover a broad range of system configurations. However, in some cases, these settings may not be the most appropriate, or you may want to modify some of the settings in order to troubleshoot issues on your system.

The `drm.cfg` file contains several parameters that you can modify and which affect the disaster recovery process, along with a description of their impact. The `drm.cfg` file is available only for EADR and OBDR.

To change the variables:

1. Copy the template file `drm.cfg.tmpl` to `drm.cfg`.

   The template is created during an installation or upgrade in *`Data_Protector_home`*`\bin\drim\config`, with all variables set to their default values.

2. Edit the `drm.cfg` file. Set the desired value for variables. Follow the instructions in the file.

General problems

Problem

Problems logging on to the system after Disaster Recovery finishes

You may receive the following error message after the system is recovered:

```
The system cannot log you on to this domain, because the
system's computer account in its primary domain is
missing or the password on that account is incorrect.
```

This type of message is usually caused by one of the following reasons:

- After collecting all information for successful disaster recovery (including full backup), you reinstalled Windows and (re)inserted into the offending domain.
- After collecting all information for successful disaster recovery (including full backup), you removed your system from the offending domain and later (re)inserted it into the same or some other domain.

Action

In cases like this, Windows generates new system security information, which is incompatible with information that is restored during disaster recovery. The solution is the following:

1. Log on to the system locally with an administrator account.
2. In the Control Panel, click **Network** and, using the Identification tab, remove the system from its current domain to a temporary workgroup (for example, TEMP). After this is done, reinsert the system into the domain from which it was previously removed. You need a domain administrator's password.
3. After the computer is again in the proper domain, click **OK** in the Network window. Windows will force you to reboot the system.
4. To update this new state with disaster recovery, you should perform all necessary procedures (collecting system data, backup) once more, as described in the "Preparing for a Disaster Recovery" section.

Problem

Disaster recovery from a copy

You cannot perform a disaster recovery from a media copy or an object copy.

Data Protector by default uses the original media set to perform a disaster recovery. Thus, copy object versions are not displayed in the Disaster Recovery Wizard of the Data Protector GUI.

Action

To perform a disaster recovery from a media copy or an object copy, if your original media set is not available or is damaged, proceed as follows:

- Object copy: Export all media in the original media set from the IDB and then regenerate the SRD file. Data Protector then offers you the first available copy of the original media set in the Disaster Recovery Wizard.

  See the online Help index "exporting media" and "Updating and editing the system recovery data (SRD)" on page 36.
- Media copy: In the SRD file, replace the media IDs of the original media with the media IDs of the media copies. Data Protector then offers you the first available copy of the original media set in the Disaster Recovery Wizard.

  Refer to "Updating and editing the system recovery data (SRD)" on page 36.

Problem

Configuration backup fails while collecting data for automatic disaster recovery methods (EADR, OBDR, or ASR)

When running a full client backup, the CONFIGURATION backup may fail while collecting data needed for a certain backup method even though this method will not be used for disaster recovery, because Data Protector by default collects data for all automatic disaster recovery methods. For example, this may happen while Data Protector collects data for EADR if the boot disks are LDM disks.

Action

Disable automatic collecting of data for the disaster recovery method that failed. This will allow Data Protector to collect data needed for other methods.

Set the variable `OB2_TURNOFF_COLLECTING` to one of the following values:

0 Default setting, data collection is turned on for all automatic methods (EADR, OBDR, ASR).

1 Turn off collecting of EADR/OBDR data. ASR data is still collected.

2 Turn off collecting of ASR data. EADR/OBDR data is still collected.

3 Turn off collecting for all methods.

See "Setting omnirc options during disaster recovery on Windows" on page 130.

Assisted manual disaster recovery

Problem

Drstart reports: "Can not copy *`filename`*"

This error is reported because the `drstart` utility can not copy the specified file. One of the reasons may be that the file is locked by the system. For example, if `drstart` cannot copy `omniinet.exe`, it might be because the `Inet` service is already running. This is not a normal scenario and should not happen after a clean install.

Action

A dialog box will appear asking you whether you would like to proceed with copying the rest of the files. If you click `Yes`, `drstart` will skip the locked file and continue copying other files. This will solve the problem if the file is locked by the system, as the process required for the disaster recovery is already running and therefore the file does not need to be copied.

You can also close the `drstart` utility by clicking the `Abort` button.

Disk delivery disaster recovery

Problem

Cannot find physical location of drives selected for disk delivery

When using the Disk Delivery method for disaster recovery, it is possible that you will receive the following error:

```
Cannot find physical location of drives selected for disk delivery
```

Objects will be restored when creating a partition on the new disk if you select a drive letter that has not been used before. The better solution would be:

Action

Disaster recovery checks disk information before restoring objects. An internal function reads the Registry value Information, which is created by the Disk Administrator. If the Disk Administrator is started several times, the `Information` value becomes corrupted (format is changed during update) - the parsers fail in such cases. If you delete the `HKEY_LOCAL_MACHINE\SYSTEM\DISK Information` key and restart the Disk Administrator, the function will succeed.

Problem

No operating system found

After performing disaster recovery, if the final boot of a Windows system fails with `No Operating System Found`.

Action

Check the `boot.ini` file for information about where the partition information is located. See Step 4 in the section "Updating and editing the system recovery data (SRD)" on page 36 for additional information.

Problem

Disk delivery disaster recovery of a Media Agent client

If you are performing a Disk Delivery disaster recovery, Data Protector first tries to connect to the original client where the backup device was attached (Media Agent client) in order to use the same device for restore. However, when you are performing Disk Delivery disaster recovery of the crashed Media Agent client where the backup has been made, Data Protector will not be able to connect to it and will proceed with offline restore and search for a local device for the restore. If there is no local device attached, Data Protector will issue a notification that there is no local device attached and will abort the disaster recovery.

Action

There are tow methods to avoid this:

- Move the media to another pool. This way you assign the media to the new device. Then proceed with Disk Delivery disaster recovery.
- The second method involves preparation prior to the disaster. If you have two Media Agent clients in the cell, you can back up of the first Media Agent client to another and vice versa before the disaster to avoid problems when performing Disk Delivery disaster recovery of a Media Agent client.

Enhanced automated disaster recovery and one button disaster recovery

Problem

Automatic DR information could not be collected

When using EADR or OBDR, it is possible that you will receive the following error:

```
Automatic DR information could not be collected. Aborting the
collecting of system recovery data
```

Action

- Check if all storage devices are configured correctly. If Device Manager reports a device as "`Unknown Device`", install the proper device drivers before you can perform EADR/OBDR.
- There must be enough registry space available. It is recommended to set the maximum registry size to at least twice that of the current registry size. If there is not enough registry space available, a similar entry would appear in the `autodr.log`:

  ```
  ERROR registry 'Exception while saving registry'
  ...
  ```

If the problem persists, uninstall the Data Protector Automatic Disaster Recovery component (so that at least Manual Disaster Recovery and Disk Delivery Disaster Recovery will work) and contact technical support.

Problem

Some non-critical errors were detected

When using EADR or OBDR, it is possible that you will receive the following error:

```
Some non-critical errors were detected during the collecting
of Automatic DR data. Please review the Automatic DR log file.
```

A non-critical error detected during the execution of the Automatic Disaster Recovery module, means that such backup can most likely still be used for disaster-recovery purposes. Possible reasons for non-critical errors are stored in `autodr.log` (located in *`Data_Protector_home`*`\tmp`):

Action

- Services or drivers outside of the *`%SystemRoot%`* folder (for example, virus scanners). `Autodr.log` would contain a similar error message:

  ```
  ERROR safeboot  'unsupported location' 'intercheck support 06' 2
  u'\\??\\D:\\Program Files\\Sophos SWEEP for NT\\icntst06.sys'.
  ```

  You can ignore this error message, as it does not affect the success of disaster recovery.

Problem

Network is not available during restore

Action

Ensure that the problem is not with switch, cables, etc. Another possibility is also that the DNS server (as configured at backup time) is offline during the restore. Since the configuration of the DR OS is the same as at backup time, the network will not be available. In this case perform offline restore and change the DNS settings after recovery. You can also edit the registry (`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters`) before Phase 2 is started. In this case reboot before Phase 2 for the changes to take effect. After Phase 2 finishes, you can correct the settings before Phase 3 can be started.

△ CAUTION:

Editing the registry incorrectly can result in failed disaster recovery.

Problem

Auto logon does not work

Action

Sometimes auto logon does not work and you have to manually log on using the `DRM$ADMIN` account.

Problem

Computer stops responding

Action

Check if the CD/tape is readable. Do not reuse CD-RWs/tapes too many times.

Problem

Cannot create a CD ISO image for EADR of Microsoft Cluster Server

Action

The quorum disk has to be backed up in order to be able to create an CD ISO Image.

Problem

ISO image creation for an AES encrypted OBDR or EADR backup fails on client if the kms_allow_hosts file is missing on the Cell Manager

The ISO image is created on the client system and the `kms_allow_hosts` file is either missing or does not contain the fully qualified name of the EADR or OBDR client for which the ISO image is prepared.

The issue does not appear if the ISO image is created on the Cell Manager.

Action

1. If the file *`Data_Protector_home`*`\config\server\cell\kms_allow_hosts` is not present, create it and add the name of the client to the file.
2. Restart the Data Protector services.

Problem

Volume is not re-mounted during phase 1

On some systems (depending on the disk controller and its configuration) a volume (without a drive letter assigned) associated with a mount point on a different volume may not be re-mounted properly during phase 1 of the disaster recovery. This may occur if the volume containing the mount point is recreated or reformatted (for example the System Volume with MiniOS), causing the operating system to boot in "Safe Mode" and to miss the detection of the file system present on the original mount point's target volume. Consequently, the disaster recovery module does not recognize this volume and reports it as `MISSING` in the `drecovery.ini` file. The contents of such a volume are intact, even if it is not recognized.

Action

- Mount the volume with a drive letter and verify it with the `chkdsk /v /f` command or wait until the system is completely restored and then recreate the original mount point.
- Manually reboot the system directly to MiniOS (do not reboot from the recovery CD). The previously unmounted volume will be automatically mounted to a drive letter.

Problem

On Windows Vista, network is not available due to missing network drivers

During a disaster recovery, the network is not available because the DR OS does not support the network card.

Action

Inject the missing drivers into the DR OS image. See "Preparing DR CD ISO image" on page 62 (EADR) or "OBDR backup" on page 73 (OBDR).

Problem

Creating an ISO image fails with the message "Unsupported version of drecovery.ini"

When creating an image for a Windows 2000 Server client from the GUI started on Windows Server 2003 or Windows XP and you select a backup created with the old Data Protector client, the following error is displayed:

```
Unsupported version of drecovery.ini file. The drecovery.ini
file of your client is created with old version of Disaster
Recovery Module and is not supported by the Disaster Recovery
Module on this client. Go to the client that has the old
version of Disaster Recovery Module and create ISO image for
your client there.
```

Before you upgrade from Data Protector versions A.05.10, A.05.50, or A.06.00 without the patch DPWIN_00270, a disaster recovery image can be created only from a GUI started on Windows 2000 systems because the old disaster recovery is present only on these systems. After the upgrade, the GUI on any client can be used to create images for any client.

Action

To create the ISO image for your client, use a client that has the old version of the disaster recovery module.

If possible, upgrade all Windows 2000 clients to the new version.

Intel Itanium specifics

Problem

After a failed or aborted disaster recovery, Boot Descriptors may be left in EFI

On Intel Itanium systems, after a failed or aborted disaster recovery session, Boot Descriptors (named `DRM Temporary OS`) may be left in the EFI environment. This can cause unwanted behavior when restarting the disaster recovery process.

Action

Remove the boot descriptor using the option **Remove Boot Descriptor** from the scope selection menu. After the boot descriptor is removed, you can proceed with disaster recovery, by selecting the scope.

Problem

A wrong or no boot disk is selected on Intel Itanium systems

On Intel Itanium systems, the wrong boot disk (or no boot disk at all) is selected.

Action

1. Select **Manual Disk Selection** from the scope selection menu. A new menu, listing all available disks, will display.
2. Determine the correct boot disk. Press **o** to view information about the original disk and **d** to see details about the selected one.
3. Select the disk from the list using cursor keys and press **b**. You can remove a selection by pressing **c**.

   If the boot disk is not the same as the system disk (usually, both disks are the same), you must select the system disk as well.

   Select **Back**.
4. Select the scope of the recovery and disaster recovery will continue.

Automated system recovery

Problem

Network problems during ASR

Network problems can be the cause of different problems during ASR.

For example, the target system has two network adapters installed and one of them had been disabled when the disaster recovery backup was performed. During ASR, all devices are enabled by default. If both network adapters are active on the target system during ASR, the network may not be configured properly, resulting in problems connecting to the Cell Manager and Media Agent client. In this case, Data Protector will switch to offline or local recovery, display a connection error or ASR will fail.

Action

To resolve the error, follow the normal ASR recovery procedure and press **F8** when the following text is displayed in the Disaster Recovery wizard:

```
Press F8 in the next 5 seconds to skip network
configuration...
```

This will revert from Data Protector ASR network configuration to the standard Microsoft ASR network configuration.

Problem

ASR aborts if network card drivers are not present

This problem occurs during ASR on newer machines, for which no appropriate network adapter driver is found on the Windows installation CD. When `omnidr` attempts to configure the use of static IP addresses, it fails because network adapters are not properly installed:

```
[Major] Failed to recreate the original network (TCP/IP)
configuration. Verify that the network adapters are properly
installed and working.
```

Action

- Install the appropriate network drivers before starting `omnidr` or if possible, use a newer/slipstreamed version of the Windows installation CD that already includes the required network drivers.

  To install the network driver before starting the Disaster Recovery, use the New Hardware Wizard, which can be invoked with the following command:

  ```
  %SystemRoot%\System32\rundll32.exe
  shell32.dll,Control_RunDLL hdwwiz.cpl
  ```

- You may use the default ASR (DHCP) network installation.

  Follow the normal ASR procedure and press **F8** when the following text is displayed in the Disaster Recovery wizard: `Press F8 in the next 5 seconds to skip network configuration...`

  This will revert from Data Protector ASR network configuration to the standard Microsoft ASR network configuration.

A Further information

Move kill links on HP-UX 11.x

Proceed as shown below on the system which you want to back up to move some links:

```
# The system will go from "run-level" 4 to "run-level 1"
# retaining the inetd, networking, swagentd services up.
#The state is called "minimum activity" for backup
#purposes (need networking).
# IMPORTANT: ensure the links are present in /sbin/rc1.d before
# moving and they do have this exact name. You have to
#rename them for the rc0.d directory. Put them BELOW the
#lowest (original "/sbin/rc0.dKxx") "K...-link" in rc0.d
# Move K430dce K500inetd K660net K900swagentd into ../rc0.d BELOW
#the lowest kill link!!!
echo "may needto be modified for this system"
exit 1
#
cd /sbin/rc1.d
mv K430dce../rc0.d/K109dce
mv K500inetd../rc0.d/K110inetd
mv K660net../rc0.d/K116net
mv K900swagentd ../rc0.d/K120swagentd
```

Windows manual disaster recovery preparation template

The template on the next page can be used to prepare for Windows Assisted Manual Disaster Recovery, as described in the Chapter 3 on page 41.

Client properties	computer name	
	hostname	

Drivers		
Windows Service Pack		
TCP/IP properties	IP address	
	default gateway	
	subnet mask	
	DNS order	
Medium label / Barcode number		
Partition information and order	1st disk label	
	1st partition length	
	1st drive letter	
	1st filesystem	
	2nd disk label	
	2nd partition length	
	2nd drive letter	
	2nd filesystem	
	3rd disk label	
	3rd partition length	
	3rd drive letter	
	3rd filesystem	

B Third-party software included in this release

Parts of this product contain third party software licensed under the following licenses:

1. **Boost**

   Revised $Date: 2005/12/05 04:16:19 $ Copyright Beman Dawes, David Abrahams, 1998-2003. Copyright Rene Rivera 2004-2005. Distributed under the Boost Software License, Version 1.0. (See accompanying file LICENSE_1_0.txt or copy at http://www.boost.org/LICENSE_1_0.txt):

   Boost Software License - Version 1.0 - August 17th, 2003

   Permission is hereby granted, free of charge, to any person or organization obtaining a copy of the software and accompanying documentation covered by this license (the "Software") to use, reproduce, display, distribute, execute, and transmit the Software, and to prepare derivative works of the Software, and to permit third-parties to whom the Software is furnished to do so, all subject to the following:

   The copyright notices in the Software and this entire statement, including the above license grant, this restriction and the following disclaimer, must be included in all copies of the Software, in whole or in part, and all derivative works of the Software, unless such copies or derivative works are solely in the form of machine-executable object code generated by a source language processor.

   THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR ANYONE DISTRIBUTING THE SOFTWARE BE LIABLE FOR ANY DAMAGES OR OTHER LIABILITY, WHETHER IN CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

2. **MKIsofs**

   Copyright (C) 1999, 2000, 2001 Joerg Schilling

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.

See the GNU General Public License for more details. You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA.

3. **ZLIB The zlib/libpng License**

Copyright (C) 1995-2005 Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software. Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

a. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

b. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

c. This notice may not be removed or altered from any source distribution.

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.

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

AML — *(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.

Audit Logs Data files to which auditing information is stored.

Audit Report User-readable output of auditing information created from data stored in audit log files.

Auditing Information Data about every backup session that was performed over an extended, user-defined period for the whole Data Protector cell.

autochanger *See* library.

autoloader *See* library.

Automatic Storage Management *(Oracle specific term)* Automatic Storage Management is an Oracle 10g/11g 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.

automigration *(VLS specific term)* The functionality that allows data backups to be first made to the VLS' virtual tapes and then migrated to physical tapes (one virtual tape emulating one physical tape) without using an intermediate backup application.
See also Virtual Library System (VLS) and virtual tape.

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

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

backup chain *See* restore chain.

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

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

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

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

- Client name: Hostname of the Data Protector client where the backup object resides.
- Mount point: For filesystem objects — the access point in a directory structure on the client where the backup object is

located (drive on Windows and mount point on UNIX). For integration objects — backup stream identification, indicating the backed up database/application items.

- Description: For filesystem objects — uniquely defines objects with identical client name and mount point. For integration objects — displays the integration type (for example, SAP or Lotus).
- Type: Backup object type. For filesystem objects — filesystem type (for example, WinFS). For integration objects — "Bar".

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

backup session A process that creates a copy of data on storage media. The activities are specified in a backup specification or an interactive session. All clients configured in one backup specification are backed up together in one backup session using the same backup type (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 backup specification, incremental backup, and full backup.

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

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

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

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

See also application system, target volume, and replica.

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

backup to IAP A Data Protector based backup to the HP Integrated Archiving Platform (IAP) appliance. It takes advantage of the IAP capability to eliminate redundancies in the stored data at a block (or chunk) level, by creating a unique content address for each data chunk. Only changed chunks are transmitted over the network and added to the store.

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 should be connected 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 manual disaster recovery is equivalent to manual AND disaster AND recovery.

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

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

See also BRBACKUP, and BRRESTORE.

BRBACKUP

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

BRRESTORE

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

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

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

BSM

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

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
See CMMDB.

Database (CMMDB)

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

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

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

- type 'disk'
- type 'sbt_tape'

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

chunking *(IAP specific term)* The process of dividing data into blocks (chunks), where each chunk gets a unique content address. This address is then used to determine whether a particular chunk is already backed up to the IAP appliance. If the duplicate data is identified (two addresses are identical, that is the address is the same as for another data chunk already stored into IAP), it is not backed up. This way, the data redundancy is eliminated and the optimal data storage is achieved.
See also backup to IAP.

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

client backup A backup of all filesystems mounted on a client. Filesystems mounted on the client after the backup specification was created are not automatically detected.

client backup with disk discovery

A backup of all filesystems mounted on a client. When the backup starts, Data Protector discovers the disks on the clients. Client backup with disk 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, and so on).

cluster continuous replication

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

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

See also Exchange Replication Service and local continuous replication.

CMD Script for Informix Server

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

CMMDB

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

between the MoM cell and the other Data Protector cells is highly recommended
See also MoM.

COM+ 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 (CLI)

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

Command View (CV) EVA

(HP StorageWorks EVA specific term) The user interface that 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 Storage Management Appliance, and is accessed by a Web browser.
See also HP StorageWorks EVA SMI-S Agent and HP StorageWorks SMI-S EVA provider.

Command View VLS

(VLS specific term) A web browser-based GUI that is used to configure, manage, and monitor the VLS through a LAN.
See also Virtual Library System (VLS).

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), which runs on the Data Protector Cell Manager, and starts and controls the backup and restore sessions. The service is started as soon as Data Protector is installed on the Cell Manager. On Windows systems,

the CRS runs under the account of the user specified at installation time. On UNIX systems, it runs under the account `root`.

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

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 stream Sequence of data transferred over the communication channel.

Data_Protector_home On Windows Vista and Windows Server 2008, the directory containing Data Protector program files. On other Windows operating systems, the directory containing Data Protector program files and data files. Its default path is `%ProgramFiles%\OmniBack`, but the path can be changed in the Data Protector Setup Wizard at installation time.
See also Data_Protector_program_data.

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

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

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

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 contains 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 on the Cell Manager in the directory *`Data_Protector_program_data`*`\db40` (Windows Server 2008), *`Data_Protector_home`*`\db40` (other Windows systems), or `/var/opt/omni/server/db40` (UNIX systems). You can create more DC directories and use a custom location. Up to 50 DC directories are supported per cell. The default maximum size of a DC directory is 16 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. Its maximum size is limited by the file system settings.

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 also incremental backup.

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

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

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-based encryption

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

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 Log (Data Protector Event Log)

A central repository of all Data Protector related notifications. By default, all notifications are sent to the Event Log. The Event Log is accessible only to Data Protector users in the `Admin` group

and to Data Protector users who are granted the `Reporting and notifications` user rights. You can view or delete all events in the Event Log.

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

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

exchanger 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

bi-directional transmission of large data files and can be deployed between sites kilometers apart. Fibre Channel connects nodes using three physical topologies: point-to-point, loop, and switched.

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

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

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

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

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

file tree walk *(Windows specific term)* The process of traversing a filesystem to determine which objects have been created, modified, or deleted.

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

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

first-level mirror *(HP 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 number.

flash recovery area

(Oracle specific term) Flash recovery area is an Oracle 10g/11g 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 (medium ID, description, and location) is saved in the IDB as well as on the respective media (media header). Data Protector media with protected data are not formatted until the protection expires or the media are unprotected/recycled.

free pool

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

full backup

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

full database backup

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

full mailbox backup

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

full ZDB

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

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 on the Cell Manager in

	the directory *Data_Protector_program_data*\Config\Server\Options (Windows Server 2008), *Data_Protector_home*\Config\Server\Options (other Windows systems), or /etc/opt/omni/server/options (HP-UX or Solaris 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 graphical user interface provided by Data Protector for easy access to all configuration, administration, and operation tasks. Besides the original Data Protector GUI that runs on Windows, Data Protector also provides a Java-based graphical user interface with the same look and feel, which runs on numerous platforms.
hard recovery	*(Microsoft Exchange Server specific term)* A Microsoft Exchange Server database recovery that is performed after a restore by the database engine, using transaction log files.
heartbeat	A cluster data set with a time stamp carrying information about the operational status of a particular cluster node. This data set or packet is distributed among all cluster nodes.
Hierarchical Storage Management (HSM)	A method for optimizing the use of expensive hard disk storage by migrating less frequently used data to less expensive optical platters. When needed, the data is migrated back to hard disk storage. This balances the need for fast retrieval from hard disk with the lower cost of optical platters.
Holidays file	A file that contains information about holidays. You can set different holidays by editing the Holidays file on the Cell Manager in the directory *Data_Protector_program_data*\Config\Server\holidays (Windows Server 2008), *Data_Protector_home*\Config\Server\holidays (other Windows systems), or /etc/opt/omni/server/Holidays (UNIX systems).
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 Operations Manager

HP Operations Manager provides powerful capabilities for operations management of a large number of systems and applications in a network. Data Protector provides an integration into this management product. This integration is implemented as a SMART Plug-In for HP Operations Manager management servers on Windows, HP-UX, Solaris, and Linux. Earlier versions of HP Operations Manager were called IT/Operation, Operations Center, Vantage Point Operations, and OpenView Operations.

HP Operations Manager SMART Plug-In (SPI)

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

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, 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 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.

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

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

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

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

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

IP address An 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.

Java GUI Client The Java GUI Client is a component of the Java GUI that contains only user interface related functionalities and requires connection to the Java GUI Server to function.

Java GUI Server The Java GUI Server is a component of the Java GUI that is installed on the Data Protector Cell Manager system. The Java GUI Server receives requests from the Java GUI Client, processes them and then sends the responses back to the Java GUI Client. The communication is done through Hypertext Transfer Protocol (HTTP) on port 5556.

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".

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.

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.

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

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

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.

local continuous replication

(Microsoft Exchange Server specific term) Local continuous replication (LCR) is a single-server solution that creates and maintains an exact copy (LCR copy) of a storage group. An LCR copy is located on the same server as the original storage group. When an LCR copy is created, it is kept up to date through change propagation (log replay) technology. The replication feature in LCR guarantees that logs that have not been replicated are not deleted. The implication of this behavior is that running backups in a mode that deletes logs may not actually free space if replication is sufficiently far behind in its log copying.

An LCR copy is used for disaster recovery because you can switch to the LCR copy in a few seconds. If an LCR copy is used for backup and if it is located on a different disk than the original data, then the I/O load on a production database is minimal. A replicated storage group is represented as a new instance of Exchange writer called Exchange Replication Service and can be backed up (using VSS) as a normal storage group.
See also cluster continuous replication and Exchange Replication Service.

lock name

You can configure the same physical device several times with different characteristics, by using different device names. The lock name is a user specified string that is used for locking all such device configurations to prevent collision if several such devices (device names) are used concurrently. Use an identical lock name for all device definitions which use the same physical device.

log_full shell script

(Informix Server UNIX 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

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

login information to the Oracle Target Database

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

- *user_name* is the name by which a user is known to Oracle Server and to other users. Every user name is associated with a password and both have to be entered to connect to an Oracle Target Database. This user must have Oracle SYSDBA or SYSOPER rights.
- *password* must be the same as the password specified in the Oracle password file (orapwd), which is used for authentication of users performing database administration.
- *service* is the name used to identify an SQL*Net server process for the target database.

login information to the Recovery Catalog Database

(Oracle specific term) The format of the login information to the Recovery (Oracle) Catalog Database is *user_name*/*password*@*service*, where the description of the user name, password, and service name is the same as in the Oracle SQL*Net V2 login information to the Oracle target database. In this case, *service* is the name of the service to the Recovery Catalog Database, not the Oracle target database. Note that the Oracle user specified here must be the owner of the Oracle Recovery Catalog.

Lotus C API

(Lotus Domino Server specific term) An interface for the exchange of backup and recovery information between Lotus Domino Server and a backup solution, like Data Protector.

LVM

A Logical Volume Manager is a subsystem for structuring and mapping physical disk space to logical volumes on UNIX systems. An LVM system consists of several volume groups, where each volume group has several volumes.

Magic Packet

See Wake ONLAN.

mailbox

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

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

Main Control Unit (MCU) *(HP StorageWorks Disk Array XP specific term)* An HP StorageWorks XP disk array that contains the primary volumes for the CA and BC configurations 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* MoM.

make_net_recovery `make_net_recovery` is an Ignite-UX command, which allows you to create a recovery archive over the network onto the Ignite-UX server or any other specified system. The target system can be recovered across subnets after booting either from a bootable tape created by the Ignite-UX `make_boot_tape` command or the system boots directly from the Ignite-UX server. Booting directly from the Ignite-UX server can be automated with the Ignite-UX `bootsys` command or interactively specified on the boot console.

make_tape_recovery `make_tape_recovery` is a command on Ignite-UX which creates a bootable recovery (installation) tape, customized for your system and enables you unattended disaster recovery by connecting the backup device directly to the target system and booting the target system from the bootable recovery tape. The backup device has to be locally connected to the client during the creation of the archive and recovery of the client.

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

MCU *See* Main Control Unit (MCU).

Media Agent A process that controls reading from and writing to a device, which reads from or writes to a medium (typically a tape). During a backup session, a Media Agent receives data from the Disk Agent and sends it to the device for writing it to the medium.

During a restore 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.

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.

medium 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, replica, and 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)* Mirror Unit number. 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 (several minutes or 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 (several 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 (several minutes or 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 (several 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.

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

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

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

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

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

overwrite

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

ownership

Backup ownership affects the ability of users to see and restore data. Each backup session and all the data backed up within it is assigned an owner. The owner can be the user that starts an interactive backup, the account under which the CRS process is running, or the user specified as the owner in the backup specification options.
If a user starts an existing backup specification without modifying it, the backup session is not considered as interactive.
If a modified backup specification is started by a user, the user is the owner unless the following is true:

- The user has the Switch Session Ownership user right.
- The backup session owner is explicitly defined in the backup specification, where the username, group or domain name, and the system name are specified.

If a backup is scheduled on a UNIX Cell Manager, the session owner is root:sys unless the above conditions are true.
If a backup is scheduled on a Windows Cell Manager, the session owner is the user specified during the installation, unless the above conditions are true.

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\Se ver\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 re-synchronizing. 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 re-synchronized 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) and Main Control Unit (MCU).

protection

See data protection and also catalog protection.

public folder store

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

public/private backed up data

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

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

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 *See* Remote Control Unit (RCU).

RDBMS Relational Database Management System.

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

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/11g 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 (RCU)

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

Removable Storage Management Database

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

reparse point

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

replica

(ZDB specific term) An image, at a particular point in time, of the data in source volumes that contain user-specified backup objects. Depending on the hardware or software with which it is created, the image may be an independent exact duplicate (clone) of the storage blocks at the physical disk level (for example, a split mirror or snapclone), or a virtual copy (for example, a snapshot). From perspective of a basic operating system, the complete physical disk containing backup objects

is replicated. However, if a volume manager is used on UNIX, the whole volume or disk group containing a backup object (logical volume) is replicated. If partitions are used on Windows, the whole physical volume containing the selected partition is replicated.
See also snapshot, snapshot creation, split mirror, and split mirror creation.

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

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

restore chain 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.

resync mode *(HP StorageWorks Disk Array XP VSS provider specific term)* One of two XP VSS hardware provider operation modes. When the XP provider is in the resync mode, the source volume (P-VOL) and its replica (S-VOL) are in the suspended mirror relationship after a backup. The maximum number of replicas (S-VOLs per a P-VOL) rotated is three provided that MU range is 0-2 or 0, 1, 2. Restore from a backup in such a configuration is possible only by re-synchronization of an S-VOL with its P-VOL.
See also VSS compliant mode, source volume, primary volume (P-VOL), replica, secondary volume (S-VOL), MU number, and replica set rotation.

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

RSM The Data Protector Restore Session Manager controls 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.

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) and Main Control Unit (MCU)

session

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

session ID

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

session key

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

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

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

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

shared disks A Windows disk on another system that has been made available to other users on the network. Systems with shared disks can be backed up without a Data Protector Disk Agent installed.

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.

single instancing *(IAP specific term)* The process of recognizing redundancy of data, at both a whole object and a chunk level. It computes a strong hash for each data chunk and uses it as a unique content address needed to determine whether attempts to store duplicates are being made.
See also backup to IAP.

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.

smart copy *(VLS specific term)* A copy of the backed up data created from the virtual tape to the physical tape library. The smart copy process allows Data Protector to distinguish between the source and the target medium thus enabling media management.
See also Virtual Library System (VLS).

smart copy pool *(VLS specific term)* A pool that defines which destination library slots are available as smart copy targets for a specified source virtual library.
See also Virtual Library System (VLS) and smart copy.

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, and high-speed databases. If sparse file processing is not enabled during restore, it might be impossible to restore this file.

split mirror *(EMC Symmetrix 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.

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

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

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

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

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 faulty system and a target system is that a target system has all faulty hardware replaced.

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

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

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

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

TLU Tape Library Unit.

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

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

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

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

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

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

transaction logs *(Data Protector specific term)* Keep 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 *(Microsoft VSS specific term)* A shadow copy that is created on the application system and can be presented to the backup system where a backup can be performed.
See also Microsoft Volume Shadow Copy Service (VSS).

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 a text file located in the `SYS:SYSTEM\TSA` directory on the server where `TSANDS.NLM` is loaded.

UIProxy The Java GUI Server (`UIProxy` service) runs on the Data Protector Cell Manager. It is responsible for communication between the Java GUI Client and the Cell Manager, moreover, it performs business logic operations and sends only important information to the client. The service is started as soon as Data Protector is installed on the Cell Manager.

unattended operation *See* lights-out operation.

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

User Account Control (UAC) A security component in Windows Vista and Windows Server 2008 that limits application software to standard user privileges until an administrator authorizes an increase in privilege level.

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

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

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

user rights User rights or access rights are the permissions needed to perform specific Data Protector tasks. Configuring a backup, starting a backup session, or starting a restore session are typical

user rights. Users have the access rights of the user group to which they belong.

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 *(Microsoft 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 Library System (VLS) A disk-based data storage device hosting one or more virtual tape libraries (VTLs).

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

virtual tape

(VLS specific term) An archival storage technology that backs up data to disk drives in the same way as if it were being stored on tape. Benefits of virtual tape systems include improved backup and recovery speed and lower operating costs.
See also Virtual Library System (VLS) and Virtual Tape Library.

Virtual Tape Library (VTL)

(VLS specific term) An emulated tape library that provides the functionality of traditional tape-based storage.
See also Virtual Library System (VLS).

VMware management client

(VMware integration specific term) The client that Data Protector uses to communicate with VMware Virtual Infrastructure. This can be a VirtualCenter Server system (VirtualCenter environment) or an ESX Server system (standalone ESX Server environment).

volser

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

volume group

A unit of data storage in an LVM system. A volume group can consist of one or more physical volumes. There can be more than one volume group on the system.

volume mount point

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

Volume Shadow Copy Service

See Microsoft Volume Shadow Copy Service.

VSS

See Microsoft Volume Shadow Copy Service.

VSS compliant mode

(HP StorageWorks Disk Array XP VSS provider specific term) One of two XP VSS hardware provider operation modes. When the XP provider is in the VSS compliant mode, the source volume (P-VOL) and its replica (S-VOL) are in simplex, unpaired state after a backup. Therefore the number of replicas (S-VOLs per a P-VOL) rotated is not limited. Restore from a backup in such a configuration is possible only by switching of the disks.

See also resync mode, source volume, primary volume (P-VOL), replica, secondary volume (S-VOL), and replica set rotation.

VxFS Veritas Journal Filesystem.

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

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

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

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

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

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

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

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

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, 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

E

H

I

R

S

T

U

W