

HP Data Protector 6.20 Integration Guide for Sybase, Network Node Manager, and Network Data Management Protocol Server

HP Part Number: N/A
Published: December 2011
Edition: Fourth



© Copyright 2004, 2011 Hewlett-Packard Development Company, L.P.

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

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

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

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

Adobe and Acrobat are trademarks of Adobe Systems Incorporated.

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

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

UNIX® is a registered trademark of The Open Group.

Contents

Publication history.....	6
About this guide.....	7
Intended audience.....	7
Documentation set.....	7
Guides.....	7
Online Help.....	9
Documentation map.....	10
Abbreviations.....	10
Map.....	10
Integrations.....	11
Document conventions and symbols.....	12
Data Protector graphical user interface.....	12
General information.....	13
HP technical support.....	13
Subscription service.....	13
HP websites.....	13
Documentation feedback.....	14
1 Data Protector Sybase Server integration.....	15
Introduction.....	15
Integration concepts.....	15
Data Protector CLI commands.....	16
Configuring the integration.....	16
Prerequisites.....	17
Before you begin.....	17
Cluster-aware clients.....	17
Configuring Sybase users.....	17
Configuring Sybase instances.....	17
Before you begin.....	18
Using the Data Protector GUI.....	18
Using the Data Protector CLI.....	20
Checking the configuration.....	20
Using the Data Protector GUI.....	20
Using the Data Protector CLI.....	20
Backup.....	21
Creating backup specifications.....	21
Modifying backup specifications.....	24
Scheduling backup specifications.....	24
Previewing backup sessions.....	25
Using the Data Protector GUI.....	25
Using the Data Protector CLI.....	26
What happens during the preview?.....	26
Starting backup sessions.....	26
Using the Data Protector GUI.....	26
Using the Data Protector CLI.....	27
Using Sybase commands.....	27
Restore.....	27
Localized database names.....	27
Finding information for restore.....	28
Using the Data Protector GUI.....	28
Using the Data Protector CLI.....	28

Using the Data Protector syb_tool command.....	28
Using the standard Data Protector CLI commands.....	32
Restoring using the Sybase isql command.....	33
Restore examples.....	35
Restoring using another device.....	36
Monitoring sessions.....	36
Troubleshooting.....	36
Before you begin.....	36
Checks and verifications.....	37
Problems.....	38
2 Data Protector HP Network Node Manager integration.....	40
Introduction.....	40
Integration concept.....	40
Configuring the integration.....	41
Prerequisites.....	41
Before you begin.....	41
Tasks for the NNM administrator.....	41
Backup.....	41
Creating backup specifications.....	42
Modifying backup specifications.....	42
Scheduling backup specifications.....	42
Starting backup sessions.....	43
Restore.....	43
Monitoring sessions.....	43
Acceptable warnings on Windows.....	44
Troubleshooting.....	44
Before you begin.....	45
Problems.....	45
3 Data Protector Network Data Management Protocol Server integration.....	48
Introduction.....	48
Integration concept.....	48
Configuring the integration.....	50
Prerequisites.....	50
Importing NDMP Server systems.....	51
Creating media pools.....	52
Configuring NDMP devices	52
Configuring tape libraries.....	54
Configuring standalone devices.....	56
Network Appliance configuration.....	57
Standalone tape devices and drives in a tape library.....	57
Library robotics.....	57
EMC Celerra configuration.....	58
SCSI devices.....	58
BlueArc and Hitachi configuration.....	58
Standalone tape devices and drives in a tape library.....	58
Library robotics.....	59
Block size.....	59
Backup.....	60
Before you begin.....	61
Creating backup specifications.....	61
Modifying backup specifications.....	63
Starting backup sessions.....	63
Restore.....	63
Restoring using the Data Protector GUI.....	64

Direct access restore.....	65
Restoring using another device.....	66
NDMP environment variables.....	66
The NDMP specific omnirc file variables.....	67
Media management.....	69
Troubleshooting.....	70
Before you begin.....	70
Problems.....	70
A Data Protector NetApp SnapManager solution.....	72
Introduction.....	72
Concepts.....	72
Installation.....	72
Prerequisites.....	72
Installation.....	72
Configuration.....	73
Backup.....	73
Limitations.....	73
Creating a backup specification.....	73
Restore.....	75
omnisnapmgr.pl reference page.....	78
SYNOPSIS.....	78
DESCRIPTION.....	78
OPTIONS.....	78
NOTES.....	78
EXAMPLES.....	78
Glossary.....	80
Index.....	110

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
B6960-96010	July 2006	Data Protector Release A.06.00
B6960-96044	November 2008	Data Protector Release A.06.10
B6960-90160	September 2009	Data Protector Release A.06.11
N/A	March 2011	Data Protector Release 6.20
N/A	March 2011 (second edition)	Data Protector Release 6.20
N/A	December 2011	Data Protector Release 6.20 with any of the following patches: DPWIN_00551, PHSS_42652, DPSOL_00477, DPLNX_00183
N/A	December 2011 (fourth edition)	Data Protector Release 6.20 with any of the following patches: DPWIN_00551, PHSS_42652, DPSOL_00477, DPLNX_00183

About this guide

This guide describes how to configure and use Data Protector with Sybase, Network Node Manager, Network Data Management Protocol Server, and NetApp SnapManager.

Intended audience

This guide is intended for backup administrators responsible for planning, setting up, and maintaining network backups. It assumes you are familiar with:

- Basic Data Protector functionality
- Administration of the respective application

Conceptual information can be found in the *HP Data Protector Concepts Guide*, which is recommended to fully understand the fundamentals and the model of Data Protector.

Documentation set

Other documents and online Help provide related information.

Guides

Data Protector guides are available in the electronic PDF format. Install the PDF files during the Data Protector setup procedure by selecting the *English Documentation (Guides, 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 Information Management Digital Hub website:

<http://www.hp.com/go/imhub>

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 six guides:
 - *HP Data Protector Integration Guide for Microsoft Applications: SQL Server, SharePoint Server, and Exchange Server*
 This guide describes the integrations of Data Protector with the following Microsoft applications: Microsoft SQL Server, Microsoft SharePoint Server, and Microsoft Exchange Server.
 - *HP Data Protector Integration Guide for Oracle and SAP*
 This guide describes the integrations of Data Protector with Oracle Server, SAP R/3, and SAP MaxDB.
 - *HP Data Protector Integration Guide for IBM Applications: Informix, DB2, and Lotus Notes/Domino*
 This guide describes the integrations of Data Protector with the following IBM applications: Informix Server, IBM DB2 UDB, and Lotus Notes/Domino Server.
 - *HP Data Protector Integration Guide for Sybase, Network Node Manager, and Network Data Management Protocol Server*
 This guide describes the integrations of Data Protector with Sybase Server, HP Network Node Manager, and Network Data Management Protocol Server.
 - *HP Data Protector Integration Guide for Virtualization Environments*
 This guide describes the integrations of Data Protector with virtualization environments: VMware Virtual Infrastructure and VMware vSphere, Microsoft Hyper-V, and Citrix XenServer.
 - *HP Data Protector Integration Guide for Microsoft Volume Shadow Copy Service*
 This guide describes the integration of Data Protector with the Microsoft Volume Shadow Copy Service. This guide also documents application writer specifics.
- *HP Data Protector Integration Guide for 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 on Windows.
- *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 P6000 EVA Disk Array Family, HP P9000 XP Disk Array Family, HP P4000 SAN Solutions, and EMC Symmetrix Remote Data Facility and TimeFinder. It is intended for backup administrators or operators. It covers the zero downtime backup, instant recovery, and the restore of filesystems and disk images.

- *HP Data Protector Zero Downtime Backup Integration Guide*
This guide describes how to configure and use Data Protector to perform zero downtime backup, instant recovery, and standard restore of Oracle Server, SAP R/3, Microsoft Exchange Server, and Microsoft SQL Server databases.
- *HP Data Protector Granular Recovery Extension User Guide for Microsoft SharePoint Server*
This guide describes how to configure and use the Data Protector Granular Recovery Extension for Microsoft SharePoint Server. The Data Protector Granular Recovery Extension is integrated into Microsoft SharePoint Server Central Administration and enables you to recover individual items. This guide is intended for Microsoft SharePoint Server administrators and Data Protector backup administrators.
- *HP Data Protector Granular Recovery Extension User Guide for VMware vSphere*
This guide describes how to configure and use the Data Protector Granular Recovery Extension for VMware vSphere. The Data Protector Granular Recovery Extension is integrated into VMware vCenter Server and enables you to recover individual items. This guide is intended for VMware vCenter Server users and Data Protector backup administrators.
- *HP Data Protector Media Operations User Guide*
This guide provides information for network administrators responsible for maintaining and backing up systems on the 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 6.20. It also provides information on installation requirements, required patches, and limitations, as well as known issues and workarounds.
- *HP Data Protector Product Announcements, Software Notes, and References for Integrations to HP Operations Manager*
This guide fulfills a similar function for the HP Operations Manager integration.
- *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 providing some basic command-line examples.

Online Help

Data Protector provides Help topics and context-sensitive (F1) Help for Windows and UNIX platforms. You can access the online Help from the top-level directory of any installation DVD-ROM without installing Data Protector:

- **Windows:** 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
GRE-SPS	Granular Recovery Extension User Guide for Microsoft SharePoint Server
GRE-VMware	Granular Recovery Extension User Guide for VMware vSphere
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 Server, and Exchange Server
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-Var	Integration Guide for Sybase, Network Node Manager, and Network Data Management Protocol Server
IG-VirtEnv	Integration Guide for Virtualization Environments
IG-VSS	Integration Guide for Microsoft Volume Shadow Copy Service
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
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							ZDB			GRE	MO			CLI				
								MS	O/S	IBM	Var	VSS	VirtEnv	OMU	OMW	Concept	Admin	IG	SPS	VMware	GS		User	PA		
Backup	X	X	X					X	X	X	X	X	X	X	X	X										
CLI																									X	
Concepts/ techniques	X		X					X	X	X	X	X	X	X	X	X	X	X								
Disaster recovery	X		X			X																				
Installation/ upgrade	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								X	
New features	X						X																		X	
Planning strategy	X		X												X											
Procedures/ tasks	X			X	X	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	X							X	X	X	
Restore	X	X	X					X	X	X	X	X	X			X	X	X	X							
Supported configurations															X											
Troubleshooting	X			X	X			X	X	X	X	X	X	X		X	X	X	X							

Integrations

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

Software application	Guides
HP Network Node Manager (NNM)	IG-Var
HP Operations Manager	IG-OMU, IG-OMW
IBM DB2 UDB	IG-IBM
Informix Server	IG-IBM
Lotus Notes/Domino Server	IG-IBM
Media Operations	MO User
Microsoft Exchange Server	IG-MS, ZDB IG
Microsoft Hyper-V	IG-VirtEnv
Microsoft SharePoint Server	IG-MS, ZDB IG, GRE-SPS
Microsoft SQL Server	IG-MS, ZDB IG
Microsoft Volume Shadow Copy Service (VSS)	IG-VSS
Network Data Management Protocol (NDMP) Server	IG-Var
Oracle Server	IG-O/S, ZDB IG
SAP MaxDB	IG-O/S
SAP R/3	IG-O/S, ZDB IG

Software application	Guides
Sybase Server	IG-Var
VMware vSphere	IG-VirtEnv, GRE-VMware

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


Disk array family	Guides
EMC Symmetrix	all ZDB
HP P4000 SAN Solutions	ZDB Concept, ZDB Admin, IG-VSS
HP P6000 EVA Disk Array Family	all ZDB, IG-VSS
HP P9000 XP Disk Array Family	all ZDB, IG-VSS

Document conventions and symbols

Table 2 Document conventions

Convention	Element
Blue text: "Document conventions" (page 12)	Cross-reference links and e-mail addresses
Blue, underlined text: http://www.hp.com	Website addresses
Bold text	<ul style="list-style-type: none"> Keys that are pressed Text typed into a GUI element, such as a box GUI elements that are clicked or selected, such as menu and list items, buttons, tabs, and check boxes
<i>Italic</i> text	Text emphasis
Monospace text	<ul style="list-style-type: none"> File and directory names System output Code Commands, their arguments, and argument values
<i>Monospace, italic</i> text	<ul style="list-style-type: none"> Code variables Command variables
Monospace, bold text	Emphasized monospace text

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

 **IMPORTANT:** Provides clarifying information or specific instructions.

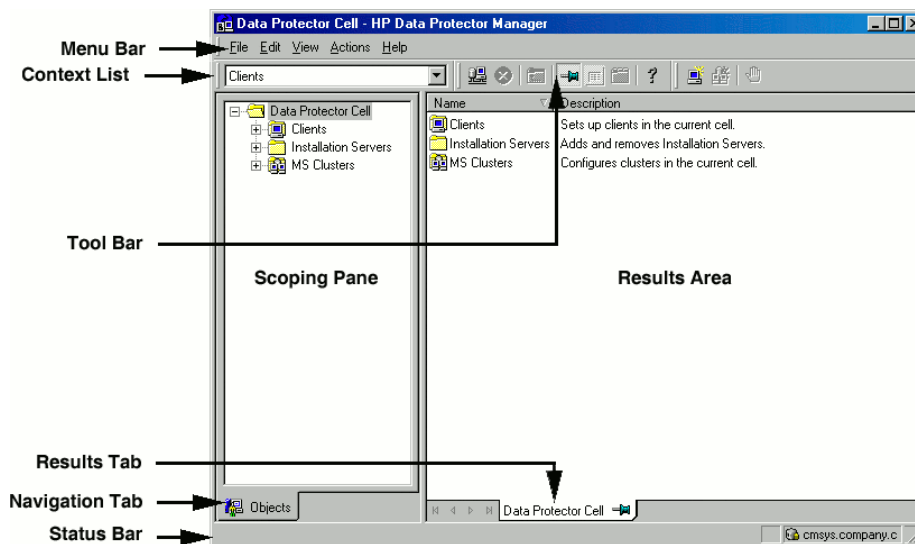
NOTE: Provides additional information.

 **TIP:** Provides helpful hints and shortcuts.

Data Protector graphical user interface

Data Protector provides a 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/go/imhub>
- <http://support.openview.hp.com/selfsolve/manuals>
- <http://www.hp.com/support/downloads>

Documentation feedback

HP welcomes your feedback.

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

1 Data Protector Sybase Server integration

Introduction

This chapter explains how to configure and use the Data Protector Sybase Adaptive Server (**Sybase Server**) integration. It describes concepts and methods you need to understand to back up and restore Sybase databases.

Data Protector offers interactive and scheduled backups of the following types:

Table 3 Backup types

Full	Backs up all selected Sybase databases and transaction logs.
Trans	Backs up changes made to the transaction logs since the last backup of any type.

During backup, the database is online and actively used.

Sybase databases are restored using the `isql` utility. You can restore a database:

- To a specific point in time
- To a new database
- To another Sybase instance

This chapter provides information specific to the Data Protector Sybase Server integration. For general Data Protector procedures and options, see online Help.

Integration concepts

Data Protector integrates with Sybase Backup Server through the Data Protector Database Library based on a common library called Data Protector **BAR** (Backup And Restore). The Data Protector Database Library channels communication between the Data Protector Session Manager, and, via the **Sybase Backup Server API**, the Sybase Server `isql` utility. “[Sybase integration architecture](#)” (page 15) shows the architecture of the Data Protector Sybase integration.

Figure 2 Sybase integration architecture

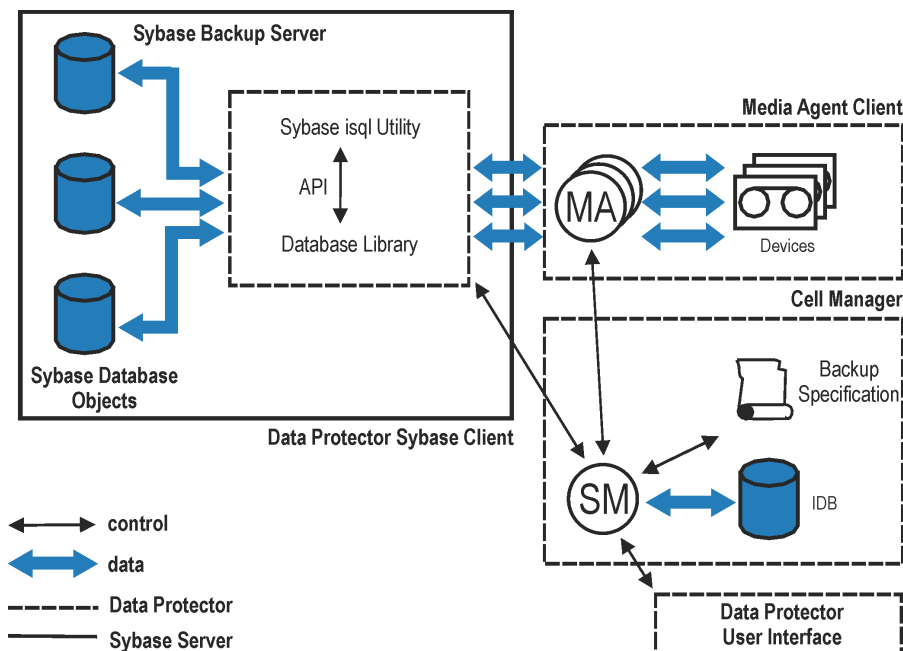


Table 4 Legend

SM	Data Protector Session Manager: Backup Session Manager during backup and Restore Session Manager during restore.
API	Sybase Backup Server Application Programming Interface.
Database Library	A set of Data Protector executables that enable data transfer between the Sybase Backup Server and Data Protector.
MA	Data Protector General Media Agent.
Backup Specification	A list of objects to be backed up, backup devices, and options to be used.
IDB	The Data Protector Internal Database.

The `isql` utility sends backup and restore commands (issued through the Data Protector GUI or CLI, or the Sybase `isql` command line interface) to Sybase Backup Server, initiating data transfer between Sybase databases and Data Protector media.

While Sybase Backup Server is responsible for read/write operations to disk, Data Protector manages devices and media used for backup and restore.

Data Protector CLI commands

Run the Data Protector CLI commands from the following directories:

Windows systems: `Data_Protector_home\bin`

UNIX systems:

Command	Directory
<code>omnib</code>	<code>opt/omni/bin</code>
<code>omnidb</code>	
<code>syb_tool</code>	
<code>testbar</code>	
<code>omnigetmsg</code>	<code>opt/omni/lbin</code>
<code>util_cmd</code>	
<code>util_sybase.pl</code>	

To run the commands, you must have appropriate Data Protector user rights. For information, see the online Help index: “user groups” and “adding users”.

If the names of the database or database instances are in a non-ASCII encoding, set the `OB2_CLI_UTF8` environment variable to 1 to enable unicode output of the Data Protector Sybase CLI utilities. The terminal application must also use a UTF-8 locale.

Configuring the integration

You need to configure Sybase users and every Sybase Adaptive Server instance (**Sybase instance**) you intend to back up from or restore to.

Prerequisites

- Ensure that you have correctly installed and configured Sybase Server.
 - For supported versions, platforms, devices, and other information, see the *HP Data Protector Product Announcements, Software Notes, and References* or <http://www.hp.com/support/manuals>.
 - For information on the Sybase Server, see the *Adaptive Server Enterprise System Administration Guide* and *Adaptive Server Enterprise Installation and Configuration Guide*.

Every Sybase instance and its default Sybase Backup Server must be configured on the same system.

- Ensure that you have correctly installed Data Protector. On how to install the Data Protector Sybase integration in various architectures, see the *HP Data Protector Installation and Licensing Guide*.

Every Sybase Server system you intend to back up from or restore to must have the Data Protector Sybase Integration component installed.

Before you begin

- Configure devices and media for use with Data Protector.
- To test whether the Sybase Server system and the Cell Manager communicate properly, configure and run a Data Protector filesystem backup and restore on the Sybase Server system.

Cluster-aware clients

Configure Sybase instances only on one cluster node, since the configuration files reside on the Cell Manager.

If you intend to use the Data Protector CLI, set the Data Protector environment variable `OB2BARHOSTNAME` to the virtual server name.

Configuring Sybase users

On UNIX, add user `root` and the Sybase Server administrator (the owner of the `isql` utility) to the Data Protector `admin` or `operator` user group. For information, see the online Help index: "adding users".

This chapter assumes that the Sybase Server administrator is user `sybase` in the group `sybase`.

Configuring Sybase instances

Provide Data Protector with Sybase instance configuration parameters:

- Pathname of the Sybase Server home directory
- Pathname of the Sybase `isql` utility
- Sybase instance name
- Sybase instance user
- Password of the Sybase instance user
- Name of the Sybase `SYBASE_ASE` directory
- Name of the Sybase `SYBASE_OCS` directory

Data Protector then creates the Sybase instance configuration file on the Cell Manager and verifies the connection to the Sybase Backup Server.

To configure a Sybase instance, use the Data Protector GUI. On UNIX, you also use the Data Protector CLI.

Before you begin

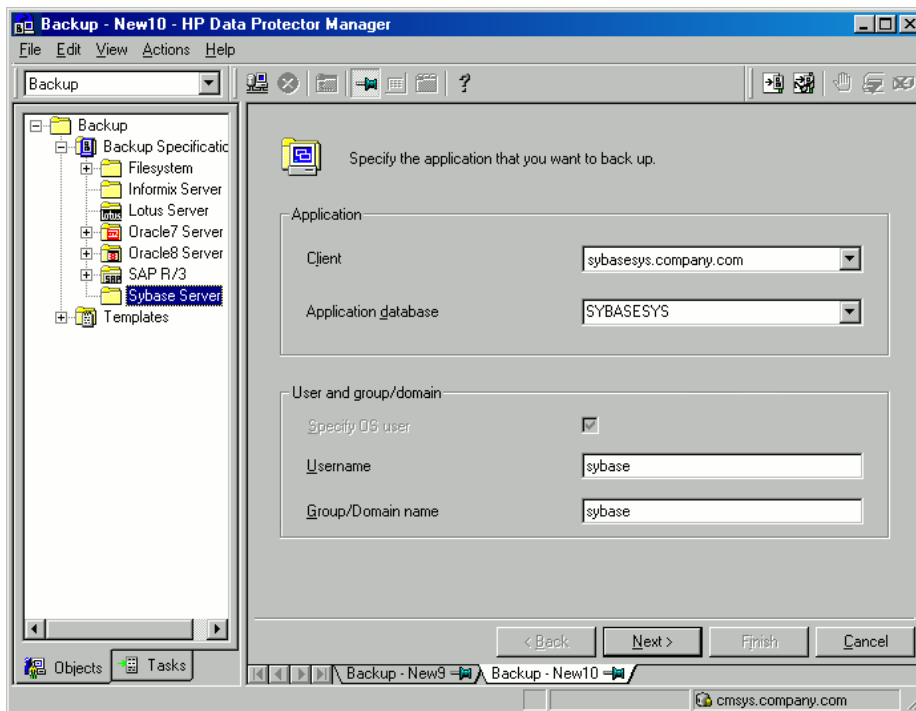
- Ensure that the default Sybase Backup Server of the Sybase instance is online.

Using the Data Protector GUI

1. In the Context List, click **Backup**.
2. In the Scoping Pane, expand **Backup Specifications**, right-click **Sybase Server**, and click **Add Backup**.
3. In the **Create New Backup** dialog box, click **OK**.
4. In **Client**, select the Sybase Server system. In a cluster environment, select the virtual server. In **Application database**, type the Sybase instance name.

UNIX systems only: Type `sybase` in both **Username** and **Group/Domain name**. This user becomes the backup owner.

Figure 3 Specifying the Sybase instance



Click **Next**.

5. In the **Configure Sybase** dialog box, review and, if necessary, correct the configuration parameters that are filled in automatically. On Windows, all configuration parameters are determined automatically. On UNIX, you need to set the Sybase Server home directory, and username and password of the Sybase instance user that has the Sybase rights to back up and restore databases. See [“Configuring a Sybase instance \(Windows systems\)”](#) (page 19) and [“Configuring a Sybase instance \(UNIX systems\)”](#) (page 19).

Figure 4 Configuring a Sybase instance (Windows systems)

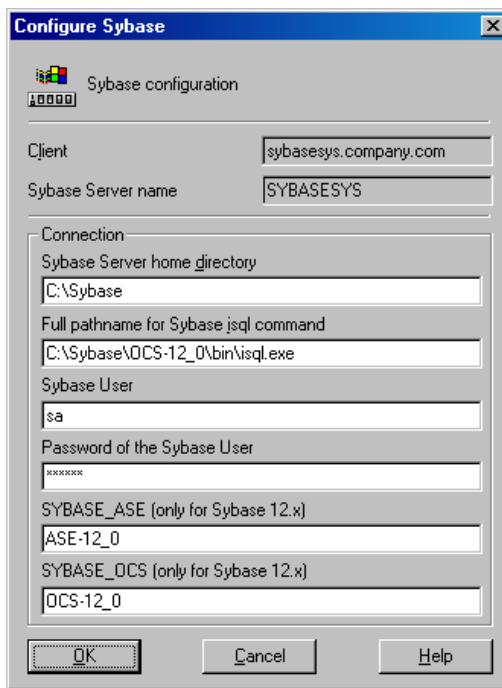
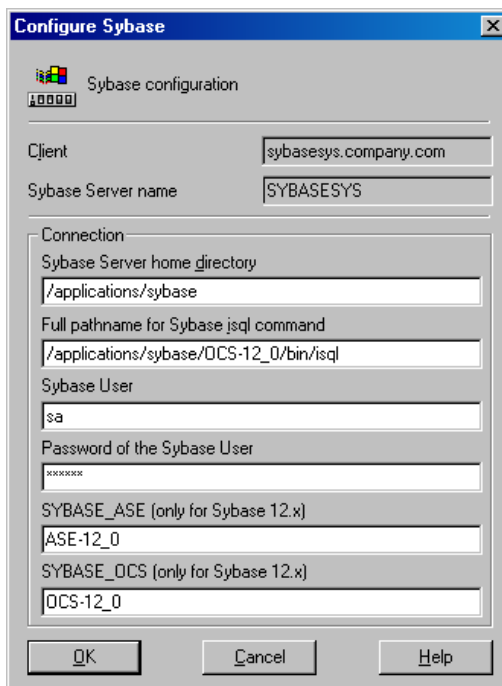


Figure 5 Configuring a Sybase instance (UNIX systems)



Click **OK**.

6. The Sybase instance is configured. Exit the GUI or proceed with creating the backup specification at [Step 6](#).

Using the Data Protector CLI

Run:

Windows systems: perl -I..\lib\perl util_sybase.pl -CONFIG \
*Sybase_instance Sybase_home isql_path Sybase_user Sybase_password \
Sybase_ASE Sybase_OCS*

UNIX systems: util_sybase.pl -CONFIG *Sybase_instance Sybase_home \
isql_path Sybase_user Sybase_password Sybase_ASE Sybase_OCS*

Parameter description

<i>Sybase_instance</i>	Name of the Sybase instance.
<i>Sybase_home</i>	Pathname of the Sybase Server home directory.
<i>isql_path</i>	Pathname of the Sybase isql command.
<i>Sybase_user</i>	Sybase instance user with the Sybase right to back up and restore databases.
<i>Sybase_password</i>	Password of the Sybase instance user.
<i>Sybase_ASE</i>	Name of the Sybase <i>Sybase_ASE</i> directory.
<i>Sybase_OCS</i>	Name of the Sybase <i>Sybase_OCS</i> directory.

The message *RETVAL*0 indicates successful configuration. Otherwise, you receive *RETVAL**error_number*. To get the error description, run:
omnigetmsg 12 *error_number*.

Example 1

To configure the Sybase instance *mysybase*, run:

```
util_sybase.pl -CONFIG mysybase /applications/sybase.15/ \  
/applications/sybase.15/OCS-15_0/bin/isql sa " " ASE-15_0 OCS-15_0
```

Checking the configuration

You can check the configuration of a Sybase instance after you have created at least one backup specification for the Sybase instance. Use the Data Protector GUI. On UNIX, you can also use the Data Protector CLI.

Using the Data Protector GUI

1. In the Context List, select **Backup**.
2. In the Scoping Pane, expand **Backup Specifications** and then **Sybase Server**. Click the backup specification to display the Sybase instance to be checked.
3. Right-click the instance and click **Check configuration**.

Using the Data Protector CLI

Run:

Windows systems: perl -I..\lib\perl util_sybase.pl -CHKCONF \
Sybase_instance_name

UNIX systems: util_sybase.pl -CHKCONF *Sybase_instance_name*

Backup

The Data Protector Sybase integration provides online backup of the following types:

Table 5 Backup types

Full	Backs up all selected Sybase databases and transaction logs.
Trans ¹	Backs up changes made to the transaction logs since the last backup of any type.

¹ For this backup type, the transaction logs must be placed on a separate Sybase database device. Otherwise, the backup fails. For details of how to place transaction logs on a separate Sybase database device, see the Sybase documentation.

To be prepared for hardware or software failures on your system:

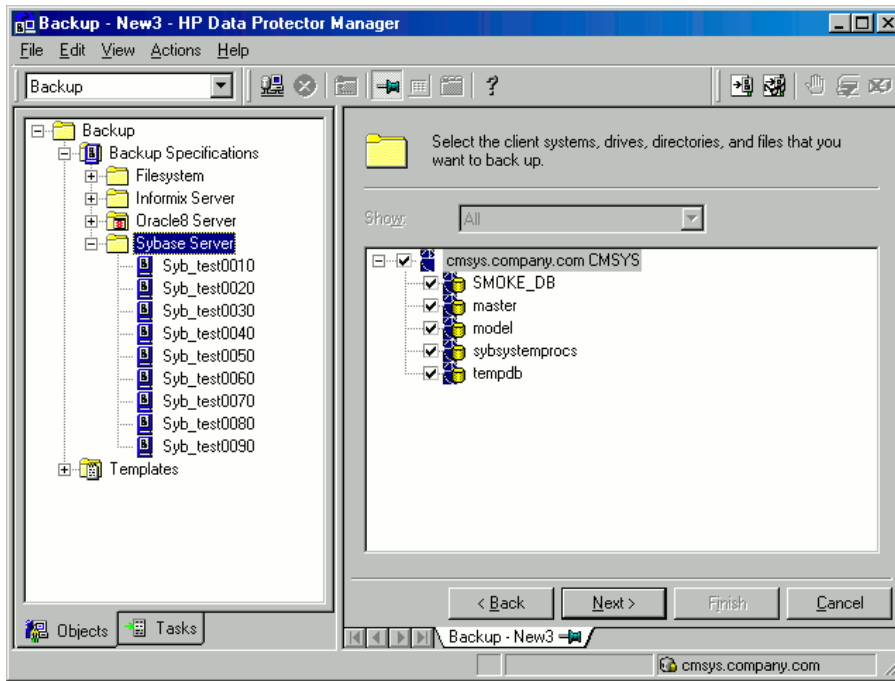
- Regularly back up Sybase system databases.
Back up the `master` database every time you create, alter, or delete a device or database. Back up the `model` database and `system procedure` database every time you change them.
- Keep a copy of the following system tables:
 - `sysusages`
 - `sysdatabases`
 - `sysdevices`
 - `sysloginroles`
 - `syslogins`

Creating backup specifications

Create a backup specification using the Data Protector GUI.

1. In the Context List, click **Backup**.
2. In the Scoping Pane, expand **Backup Specifications**, right-click **Sybase Server**, and click **Add Backup**.
3. In the **Create New Backup** dialog box, click **OK**.
4. In **Client**, select the Sybase Server system. In a cluster environment, select the virtual server.
In **Application database**, type the Sybase instance name.
UNIX systems only: Type `sybase` in both **Username** and **Group/Domain name**. This user becomes the backup owner.
Click **Next**.
5. If the Sybase instance is not configured for use with Data Protector, the **Configure Sybase** dialog box is displayed. Configure it as described in [“Configuring Sybase instances” \(page 17\)](#).
6. Select the databases you want to back up.

Figure 6 Selecting backup objects



Click **Next**.

7. Select devices to use for the backup.

To specify device options, right-click the device and click **Properties**.

Click **Next**.

8. Set backup options. For information on application-specific options, see “[Sybase backup options](#)” (page 24).

Figure 7 Pre- and post-exec commands (Windows systems)

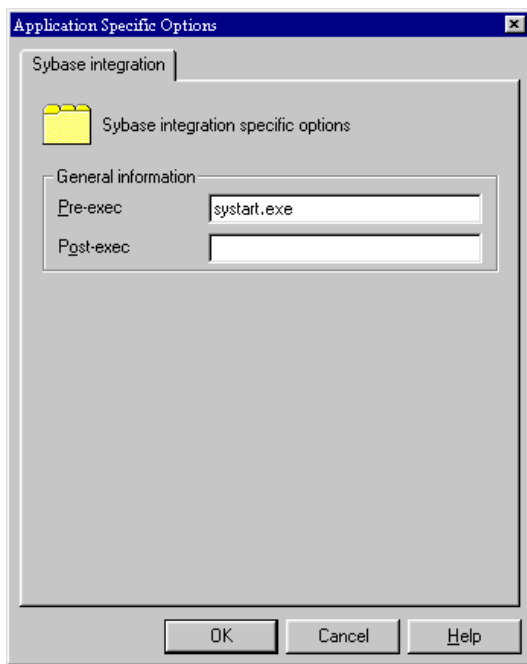
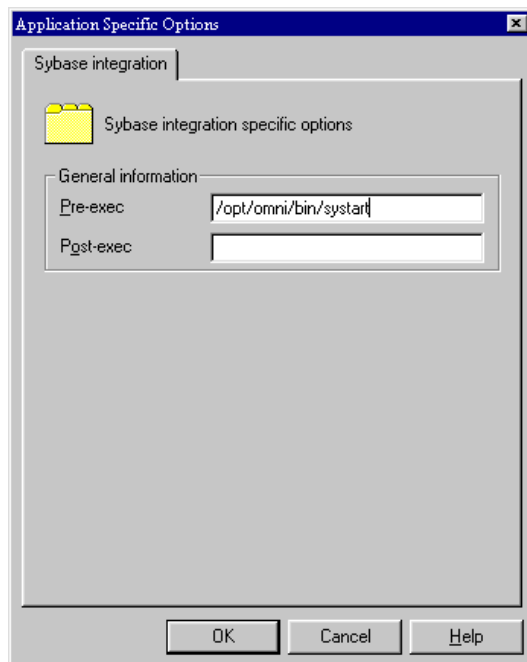


Figure 8 Pre- and post-exec commands (UNIX systems)



Click **Next**.

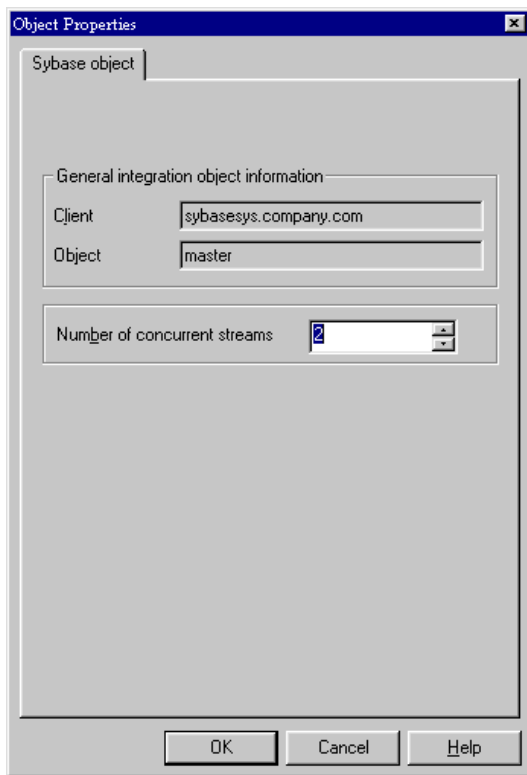
9. Optionally, schedule the backup. For more information, see [“Scheduling backup specifications” \(page 24\)](#).

Click **Next**.

10. View the properties of objects selected for backup. If you have selected only specific databases, not the whole instance, you can specify the number of concurrent data streams for backing up a particular database: right-click the database and click **Properties**.

This option is equivalent to Sybase *dump striping*.

Figure 9 Specifying the number of concurrent streams



The Sybase Backup Server then splits the database into approximately equal parts and sends the parts concurrently to devices according to device concurrency values.

If the total sum of device concurrencies is big enough, two or more databases can be backed up simultaneously.

Click **Next**.

11. Save the backup specification, specifying a name and a backup specification group.



TIP: Preview your backup specification before using it for real. See “[Previewing backup sessions](#)” (page 25).

Table 6 Sybase backup options

Pre-exec, Post-exec	<p>Specify a command that will be started by <code>ob2sybase.exe</code> (Windows systems) or <code>ob2sybase.pl</code> (UNIX systems) on the Sybase Server system before the backup of every selected database (<code>pre-exec</code>) or after it (<code>post-exec</code>). Do not use double quotes.</p> <p>Windows systems: Provide only the name of the command. The command must reside in the <code>Data_Protector_home\bin</code> directory. See “Pre- and post-exec commands (Windows systems)” (page 22).</p> <p>UNIX systems: Provide the pathname of the command. See “Pre- and post-exec commands (UNIX systems)” (page 23).</p>
---------------------	--

Modifying backup specifications

To modify your backup specification, click its name in the Scoping Pane of the Backup context, then click the appropriate tab, and apply the changes.

Scheduling backup specifications

You can run unattended backups at specific times or periodically. For details on scheduling, see the online Help index: “[scheduled backups](#)”.

Example

To schedule `Full` backups at 8:00, 13:00, and 18:00 during week days:

1. In the **Schedule** property page, select the starting date in the calendar and click **Add** to open the **Schedule Backup** dialog box.
2. Under **Recurring**, select **Weekly**. Under **Time options**, select **8:00**. Under **Recurring Options**, select **Mon, Tue, Wed, Thu, and Fri**. Under **Session options**, select the **Full** backup type. See “Scheduling a backup specification” (page 25). Click **OK**.
3. Repeat **Step 1** and **Step 2** to schedule another backup at 13:00, and another one at 18:00.
4. Click **Apply** to save the changes.

Figure 10 Scheduling a backup specification

The screenshot shows the 'Schedule Backup' dialog box with the following configuration:

- Recurring:** None, Daily, Weekly, Monthly
- Time options:** Time: 8:00, Use starting, Start date: 7/ 3/2007
- Recurring options:** Every 1 week(s) on, Sun, Mon, Tue, Wed, Thu, Fri, Sat
- Session options:** Backup type: Full, Network load: High, Medium, Low, Backup protection: Default

Previewing backup sessions

Preview the backup session to test it. Use the Data Protector GUI or CLI.

Using the Data Protector GUI

1. In the Context List, click **Backup**.
2. In the Scoping Pane, expand **Backup Specifications** and then **Sybase Server**. Right-click the backup specification you want to preview and click **Preview Backup**.
3. Specify the **Backup type** and **Network load**. Click **OK**.

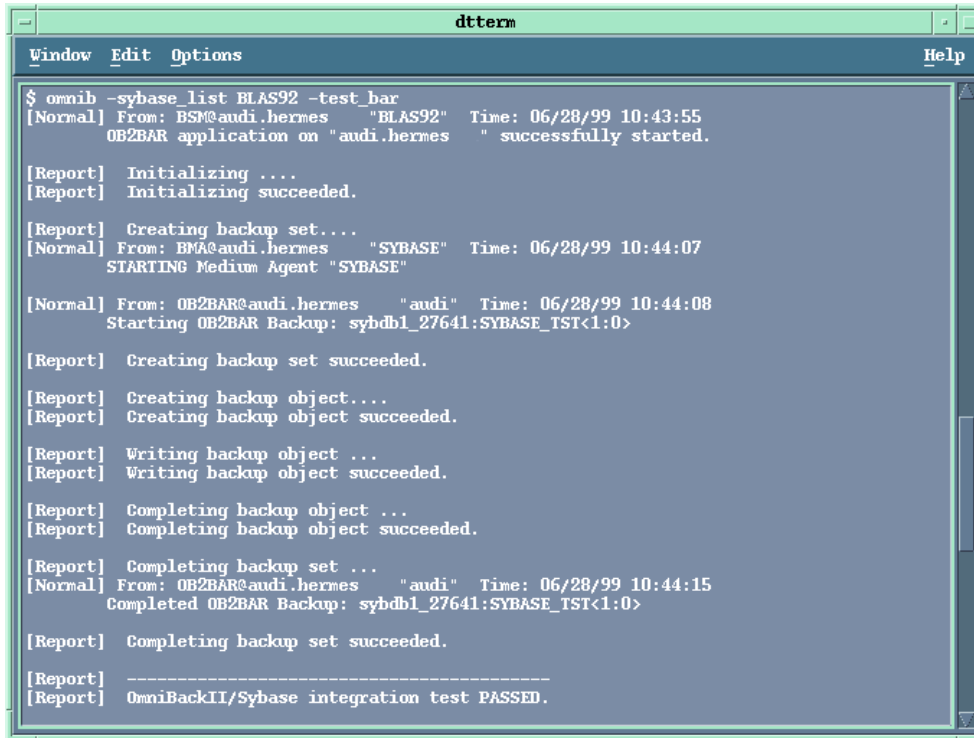
The message `Session completed successfully` is displayed at the end of a successful preview.

Using the Data Protector CLI

Run:

```
omnib -sybase_list backup_specification_name -test_bar
```

Figure 11 Example of previewing a backup



```
dtterm
Window Edit Options Help
$ omnib -sybase_list BLAS92 -test_bar
[Normal] From: BSM@audi.hermes "BLAS92" Time: 06/28/99 10:43:55
OB2BAR application on "audi.hermes" " successfully started.

[Report] Initializing ....
[Report] Initializing succeeded.

[Report] Creating backup set....
[Normal] From: BMA@audi.hermes "SYBASE" Time: 06/28/99 10:44:07
STARTING Medium Agent "SYBASE"

[Normal] From: OB2BAR@audi.hermes "audi" Time: 06/28/99 10:44:08
Starting OB2BAR Backup: sybdb1_27641:SYBASE_TST<1:0>

[Report] Creating backup set succeeded.

[Report] Creating backup object...
[Report] Creating backup object succeeded.

[Report] Writing backup object ...
[Report] Writing backup object succeeded.

[Report] Completing backup object ...
[Report] Completing backup object succeeded.

[Report] Completing backup set ...
[Normal] From: OB2BAR@audi.hermes "audi" Time: 06/28/99 10:44:15
Completed OB2BAR Backup: sybdb1_27641:SYBASE_TST<1:0>

[Report] Completing backup set succeeded.

[Report] -----
[Report] OmniBackII/Sybase integration test PASSED.
```

What happens during the preview?

The following are tested:

- Communication between the Sybase instance and Data Protector
- The syntax of the backup specification
- If devices are correctly specified
- If the necessary media are in the devices
- Configuration of the Sybase instance

Starting backup sessions

Interactive backups are run on demand. They are useful for urgent backups or for restarting failed backups.

Start a backup in any of the following ways:

- Use the Data Protector GUI.
- Use the Data Protector CLI.
- Use the Sybase `isql` utility.

Using the Data Protector GUI

1. In the Context List, click **Backup**.
2. In the Scoping Pane, expand **Backup Specifications** and then **Sybase Server**. Right-click the backup specification you want to use and click Start Backup.
3. Select the **Backup type** and **Network load**. Click **OK**.

Successful backup displays the message `Session completed successfully`.

Using the Data Protector CLI

Run:

```
omnib -sybase_list backup_specification [-barmode sybase_mode] [options]
```

Parameter description

<i>backup_specification</i>	Name of the Data Protector Sybase backup specification.
<i>sybase_mode</i>	Backup type. Select between <code>full</code> and <code>trans</code> .
<i>options</i>	For information, see the <code>omnib</code> man page.

Example

To perform a full backup using the backup specification `FullSybase`, run:

```
omnib -sybase_list FullSybase -barmode full
```

Using Sybase commands

To start a database backup from the client where the database is located, using the Sybase `isql` utility:

1. Check if the devices to be used contain formatted (initialized) media with enough free space.
2. Verify the backup options in the Data Protector Sybase backup specification.
3. Log in to the Sybase Server system as user `sybase`.
4. Run the Sybase `isql` command:

```
isql -SSybase_instance -USybase_user -PSybase_password dump \  
database database to "ob2syb::backup_specification"
```

Parameter description

<i>Sybase_instance</i>	Sybase instance name.
<i>Sybase_user</i>	Sybase instance user.
<i>Sybase_password</i>	Password of the Sybase instance user.
<i>database</i>	Name of the database to be backed up.
<i>backup_specification</i>	Name of the Data Protector Sybase backup specification.

Restore

Restore Sybase databases using the Sybase `isql` utility.

To restore a Sybase database:

1. Restore a full backup of the Sybase database.
2. Restore subsequent transaction backups (if they exist).

Localized database names

If the names of backed up objects contain characters that cannot be displayed using the current language group (on Windows) or code page (on UNIX):

1. Set the encoding used on the terminal to UTF-8.
2. **Windows only:** Set the environment variable `OB2_CLI_UTF8` to 1.
3. When gathering information for restore, redirect the output of the `syb_tool` or `omnidb` command to a text file.

If you need to edit the file containing the load command, use a UTF-8 aware editor that does not set the first byte ("BOM"), since such a file is not supported by `isql`. Note that the Windows Notepad editor cannot be used.

For details, see [“Finding information for restore” \(page 28\)](#).

4. When restoring the objects, add the `-i file_name -J utf8` options to the `isql` command, where `file_name` is the file with the load command.

For details, see [“Restoring using the Sybase isql command” \(page 33\)](#).

Finding information for restore

To restore a corrupted database, first find the necessary media and the session ID of the last full backup. If you have backed up the database using several streams, also determine the number of streams.

Use the Data Protector GUI or CLI.

Using the Data Protector GUI

In the Internal Database context, expand `Objects` or `Sessions`. To view details on a session, right-click the session and click `Properties`.

Using the Data Protector CLI

Use the Data Protector `syb_tool` command or the standard Data Protector CLI commands.

Using the Data Protector `syb_tool` command

The Data Protector `syb_tool` command returns the exact Sybase `load` command needed for restore.

The syntax of the `syb_tool` command is:

```
syb_tool database Sybase_instance
  -date YYYY/MM/DD.hh:mm:ss
  [ -new_db new_database ]
  [ -new_server new_Sybase_instance ]
  [ -file file ]
  [ -media ]
```

Parameter description

<code>database</code>	Database to be restored.
<code>Sybase_instance</code>	Sybase instance from which the database to be restored was backed up.
<code>date</code>	Point in time. The first backup version created after this point in time is restored. Use the 0-24h time format.
<code>new_database</code>	Target database to which to restore.
<code>new_Sybase_instance</code>	Target Sybase instance to which to restore.
<code>file</code>	Pathname of a file to which the <code>load</code> command or command sequence is recorded.
<code>-media</code>	Lists media needed for the restore.

To define the time interval between the closure of transaction logs and the start of a backup session, set the global variable `OB2SybaseTransLogDelay`. The default value is 20 seconds.

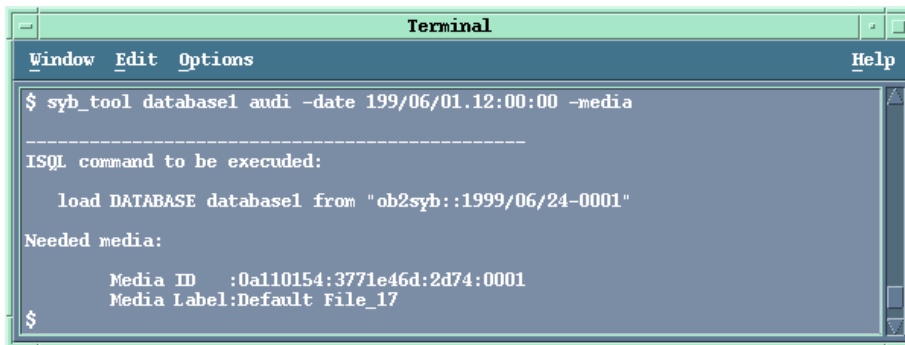
Example 1

To get the `load` command that restores `database1` of the Sybase instance `audi` from the first backup performed after 12.00 noon on June 1, 1999, and to get the necessary media, run:

```
syb_tool database1 audi -date 1999/06/01.12:00:00 -media
```

See [“Running the `syb_tool` command” \(page 29\)](#).

Figure 12 Running the syb_tool command



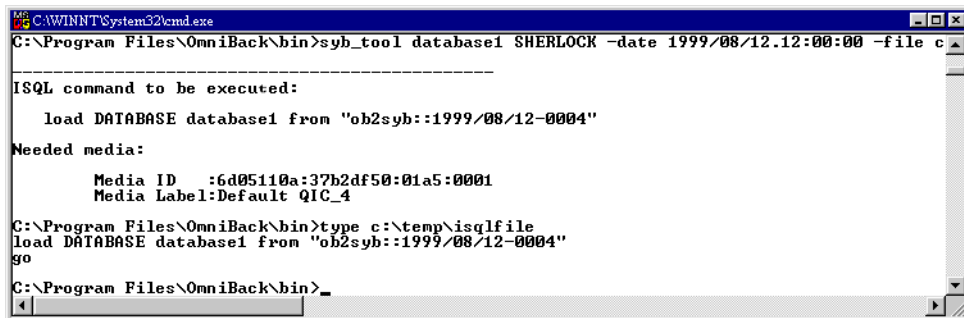
```
Terminal
Window Edit Options Help
$ syb_tool database1 audi -date 199/06/01.12:00:00 -media
-----
ISQL command to be executed:
    load DATABASE database1 from "ob2syb::1999/06/24-0001"
Needed media:
    Media ID   :0a110154:3771e46d:2d74:0001
    Media Label:Default File_17
$
```

Example 2

To get the load command that restores database1 of the Sybase instance sherlock from the first backup performed after 12.00 noon on June 1, 1999, to get the necessary media, and to record the load command to the file c:/tmp/isqlfile (Windows), run:

```
syb_tool database1 sherlock -date 1999/06/01.12:00:00 -file \
c:\tmp\isqlfile -media
```

Figure 13 Running the syb_tool command with the -file and -media options



```
C:\WINNT\System32\cmd.exe
C:\Program Files\OmniBack\bin>syb_tool database1 SHERLOCK -date 1999/08/12.12:00:00 -file c
-----
ISQL command to be executed:
    load DATABASE database1 from "ob2syb::1999/08/12-0004"
Needed media:
    Media ID   :6d05110a:37b2df50:01a5:0001
    Media Label:Default QIC_4
C:\Program Files\OmniBack\bin>type c:\tmp\isqlfile
load DATABASE database1 from "ob2syb::1999/08/12-0004"
go
C:\Program Files\OmniBack\bin>
```

Example 3

To get the load command that restores database1 to database2 from the first backup performed after 12.00 noon on June 1, 1999, run:

```
syb_tool database1 audi -date 1999/06/01.12:00:00 -new_db database2 \
-media
```

Figure 14 The load command for restore to a different database



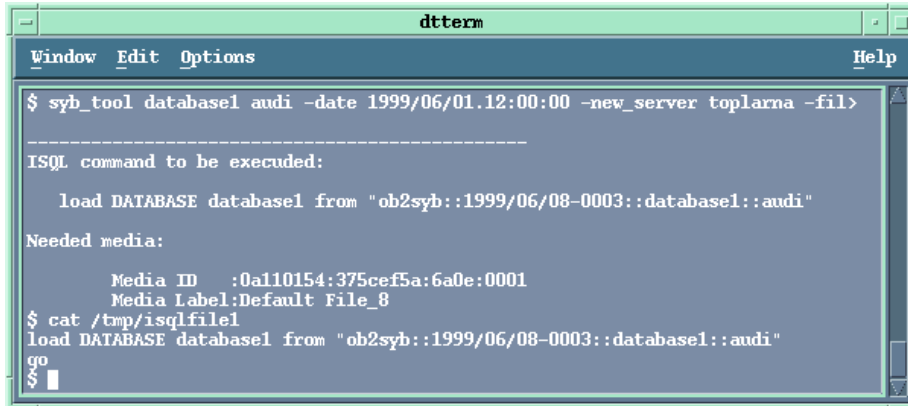
```
dtterm
Window Edit Options Help
$ syb_tool database1 audi -date 1999/06/01.12:00:00 -new_db database2 -media
-----
ISQL command to be executed:
    load DATABASE database2 from "ob2syb::1999/06/08-0003::database1"
Needed media:
    Media ID   :0a110154:375cef5a:6a0e:0001
    Media Label:Default File_8
$
```

Example 4

To get the load command that restores database1 of the Sybase instance audi to the Sybase instance toplarna, run:

```
syb_tool database1 audi -date 1999/06/01.12:00:00 -new_server toplarna  
\  
-file /tmp/isql -media
```

Figure 15 The load command for restore to a different server



```
dtterm  
Window Edit Options Help  
$ syb_tool database1 audi -date 1999/06/01.12:00:00 -new_server toplarna -fil>  
-----  
ISQL command to be executed:  
    load DATABASE database1 from "ob2syb::1999/06/08-0003::database1::audi"  
Needed media:  
    Media ID   :0a110154:375cef5a:6a0e:0001  
    Media Label:Default File_8  
$ cat /tmp/isqlfile1  
load DATABASE database1 from "ob2syb::1999/06/08-0003::database1::audi"  
go  
$
```

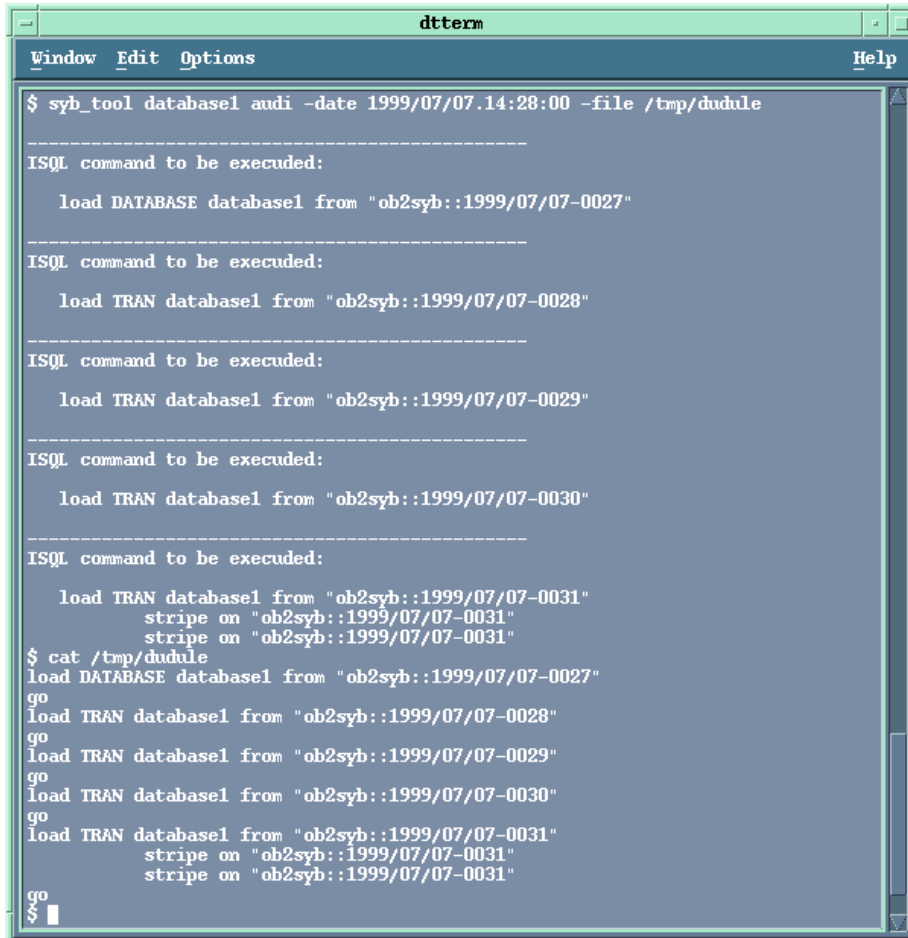
Example 5

To get the load command that restores database1 of the Sybase instance audi from the first backup performed after 14:28 on July 7, 1999, and to record the load command to the file /tmp/dudule, run:

```
syb_tool database1 audi -date 1999/07/07.14:28:00 -file /tmp/dudule
```

You see in “Loading transaction logs from multiple backups” (page 31) that you need to restore one full backup and four transaction log backups, the last one backed up with concurrency 3.

Figure 16 Loading transaction logs from multiple backups



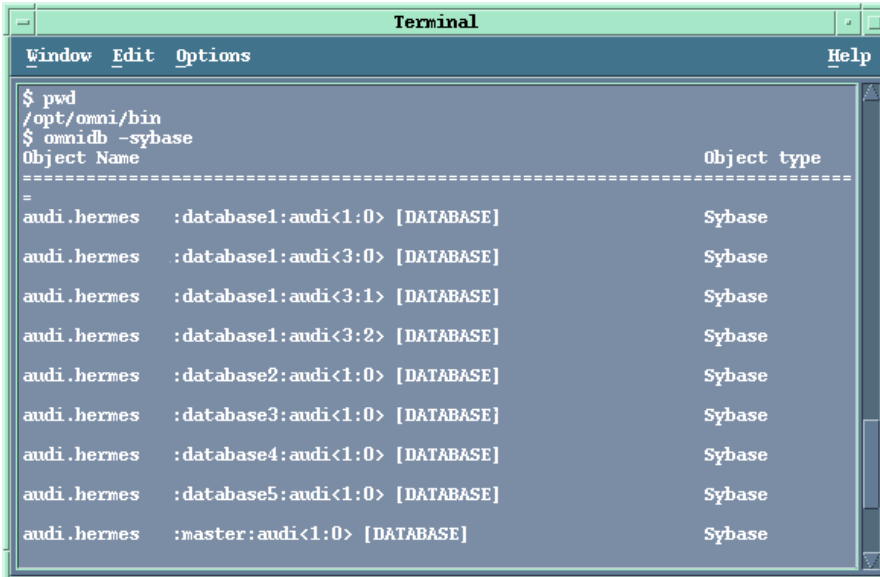
```
dtterm
Window Edit Options Help
$ syb_tool database1 audi -date 1999/07/07.14:28:00 -file /tmp/dudule
-----
ISQL command to be executed:
    load DATABASE database1 from "ob2syb::1999/07/07-0027"
-----
ISQL command to be executed:
    load TRAN database1 from "ob2syb::1999/07/07-0028"
-----
ISQL command to be executed:
    load TRAN database1 from "ob2syb::1999/07/07-0029"
-----
ISQL command to be executed:
    load TRAN database1 from "ob2syb::1999/07/07-0030"
-----
ISQL command to be executed:
    load TRAN database1 from "ob2syb::1999/07/07-0031"
    stripe on "ob2syb::1999/07/07-0031"
    stripe on "ob2syb::1999/07/07-0031"
$ cat /tmp/dudule
load DATABASE database1 from "ob2syb::1999/07/07-0027"
go
load TRAN database1 from "ob2syb::1999/07/07-0028"
go
load TRAN database1 from "ob2syb::1999/07/07-0029"
go
load TRAN database1 from "ob2syb::1999/07/07-0030"
go
load TRAN database1 from "ob2syb::1999/07/07-0031"
    stripe on "ob2syb::1999/07/07-0031"
    stripe on "ob2syb::1999/07/07-0031"
go
```

Using the standard Data Protector CLI commands

1. Get a list of backed up Sybase databases:

```
omnidb -sybase
```

Figure 17 Example of a list of backed up Sybase databases

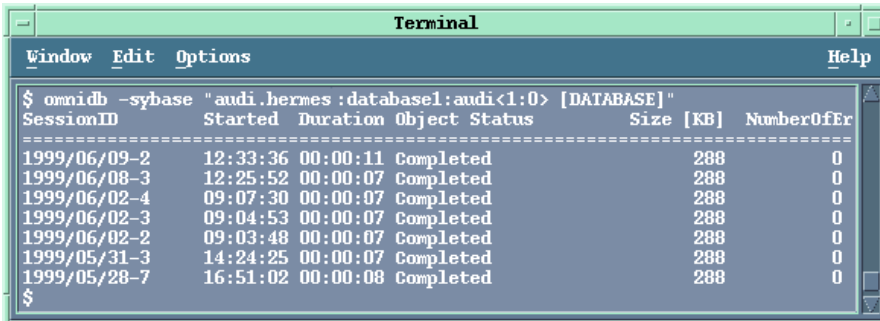


```
Terminal
Window Edit Options Help
$ pwd
/opt/omni/bin
$ omnidb -sybase
Object Name                                     Object type
-----
audi.hermes :database1:audi<1:0> [DATABASE]    Sybase
audi.hermes :database1:audi<3:0> [DATABASE]    Sybase
audi.hermes :database1:audi<3:1> [DATABASE]    Sybase
audi.hermes :database1:audi<3:2> [DATABASE]    Sybase
audi.hermes :database2:audi<1:0> [DATABASE]    Sybase
audi.hermes :database3:audi<1:0> [DATABASE]    Sybase
audi.hermes :database4:audi<1:0> [DATABASE]    Sybase
audi.hermes :database5:audi<1:0> [DATABASE]    Sybase
audi.hermes :master:audi<1:0> [DATABASE]      Sybase
```

2. Get a list of backup sessions for a specific object, including the session ID:

```
omnidb -sybase "object_name"
```

Figure 18 Example of a list of backup sessions for a specific object



```
Terminal
Window Edit Options Help
$ omnidb -sybase "audi.hermes :database1:audi<1:0> [DATABASE]"
SessionID   Started   Duration Object Status      Size [KB]  NumberOfEr
-----
1999/06/09-2 12:33:36 00:00:11 Completed 288        0
1999/06/08-3 12:25:52 00:00:07 Completed 288        0
1999/06/02-4 09:07:30 00:00:07 Completed 288        0
1999/06/02-3 09:04:53 00:00:07 Completed 288        0
1999/06/02-2 09:03:48 00:00:07 Completed 288        0
1999/05/31-3 14:24:25 00:00:07 Completed 288        0
1999/05/28-7 16:51:02 00:00:08 Completed 288        0
$
```

-
- ① **IMPORTANT:** For object copies, use the object's backup ID (which equals the object's backup session ID). Do not use the object's copy session ID.
-

3. Get a list of media needed for restore:
`omnidb -session session_id -media`

Figure 19 Example of finding media needed for restore

```

Terminal
Window Edit Options Help
$ omnidb -session 1999/06/09-2 -media
Medium Label           Medium ID              Free Block
-----
Default File_14       0a110154:375e3de9:34c4:0001  9889
6
Default QTC_1         0a110154:375e2996:2e13:0001  416816
0
$

```

For details on the omnidb command, see the omnidb man page.

Restoring using the Sybase isql command

1. On UNIX, log in to the Sybase Server system as user sybase.
2. Run the Sybase isql utility:

```
isql -SSybase_instance -USybase_user -PSybase_password [-i \
input_file -J utf8]
```

Parameter description

<i>Sybase_instance</i>	Sybase instance name.
<i>Sybase_user</i>	Sybase instance user.
<i>Sybase_password</i>	Password of the Sybase instance user.
<i>input_file</i>	The file to which the load parameter was saved. See also “Localized database names” (page 27).

- If you did not provide the load command in a file, type the desired `load` command in the first line. To run the command(s), type `go` in the last line and press **Enter**.

The syntax of the Sybase `load` command is:

```
load {database|transaction} new_database from
"ob2syb::version[:database[:Sybase_instance]] "
stripe on
"ob2syb::version[:database[:Sybase_instance]] "
```

Parameter description

<code>{database transaction}</code>	Defines whether databases or transaction logs are to be restored.
<code>version</code>	Session ID of the backup version to restore from. You can also type <code>latest</code> <code>version</code> to restore from the latest backup.
<code>new_database</code>	Target database to which to restore.
<code>database</code>	Database to be restored.
<code>Sybase_instance</code>	Sybase instance from which the database to be restored was backed up.

The `stripe` part is needed only when restoring a database backed up with several streams. The number of streams used for backup is displayed in the Data Protector Monitor during the backup session.

- IMPORTANT:** To restore a database to a new database, first create a new database. The new database should have the same structure as the database to be restored.

To restore a database to a different Sybase instance on another client system, set the `OB2HOSTNAME` variable on the target client: add the `OB2HOSTNAME=BackupClient.company.com` variable entry to the `Sybase_TargetInstance.cfg` configuration file. The location of the directory depends on the operating system:

Windows systems: `Data_Protector_home\tmp`

HP-UX and Solaris systems: `/var/opt/omni/tmp`

For details on the Sybase `load` command, see the *Adaptive Server Enterprise System Administration Guide*.

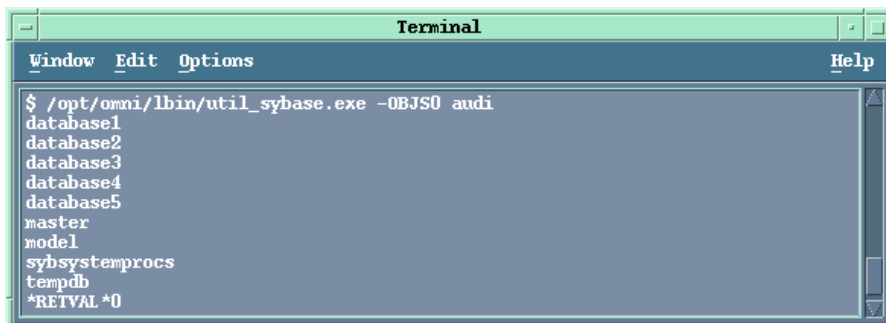
- TIP:** To list all Sybase databases of a particular Sybase instance, run:

Windows systems: `perl -I..\lib\perl util_sybase.pl -OBJS0 \`

`Sybase_instance_name`

UNIX systems: `util_sybase.pl -OBJS0 Sybase_instance_name`

Figure 20 Example of a list of Sybase databases



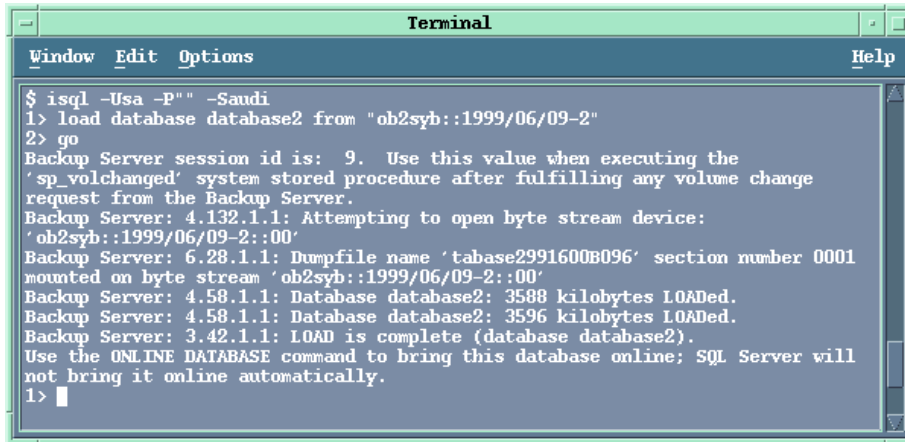
Restore examples

Example 1

To restore the database `database2` from the backup session `1999/06/09-2`, run:

```
1>load database database2 from "ob2syb::1999/06/09-2"  
2>go
```

Figure 21 Restoring a database from a specific session



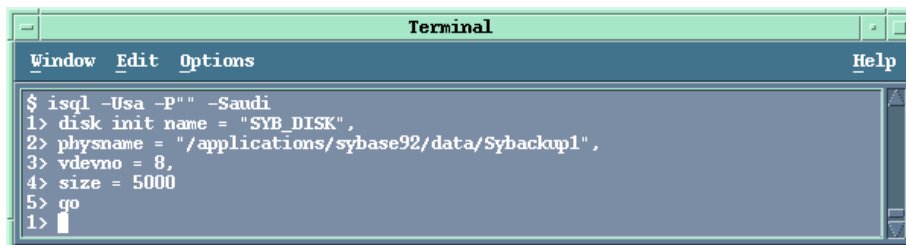
```
Terminal  
Window Edit Options Help  
$ isql -Usa -P"" -Saudi  
1> load database database2 from "ob2syb::1999/06/09-2"  
2> go  
Backup Server session id is: 9. Use this value when executing the  
'sp_volchanged' system stored procedure after fulfilling any volume change  
request from the Backup Server.  
Backup Server: 4.132.1.1: Attempting to open byte stream device:  
'ob2syb::1999/06/09-2::00'  
Backup Server: 6.28.1.1: Dumpfile name 'tabase2991600B096' section number 0001  
mounted on byte stream 'ob2syb::1999/06/09-2::00'  
Backup Server: 4.58.1.1: Database database2: 3588 kilobytes LOAded.  
Backup Server: 4.58.1.1: Database database2: 3596 kilobytes LOAded.  
Backup Server: 3.42.1.1: LOAD is complete (database database2).  
Use the ONLINE DATABASE command to bring this database online; SQL Server will  
not bring it online automatically.  
1> █
```

Example 2

To restore the latest version of the database `Sybddata` to a new database, named `Sybddata1`:

1. Create a database device. See ["Creating a database device"](#) (page 35).

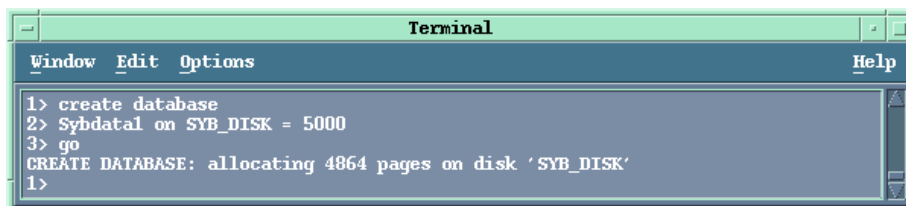
Figure 22 Creating a database device



```
Terminal  
Window Edit Options Help  
$ isql -Usa -P"" -Saudi  
1> disk init name = "SYB_DISK",  
2> physname = "/applications/sybase92/data/Sybbackup1",  
3> vdevno = 8,  
4> size = 5000  
5> go  
1> █
```

2. Create an empty database, named `Sybddata1`. See ["Creating an empty database"](#) (page 35).

Figure 23 Creating an empty database



```
Terminal  
Window Edit Options Help  
1> create database  
2> Sybdatal on SYB_DISK = 5000  
3> go  
CREATE DATABASE: allocating 4864 pages on disk 'SYB_DISK'  
1> █
```

3. Restore `Sybddata` to `Sybddata1` by running:

```
1>load database Sybdatal from "ob2syb::latest version::Sybdatal"  
2>go
```

Example 3

To restore the latest version of the database `database3` backed up with three streams, run:

```
1>load database database3 from "ob2syb::latest version"  
2>stripe on "ob2syb::latest version"  
3>stripe on "ob2syb::latest version"  
4>go
```

Example 4

To start a restore a database from the instance "instance1", which name contains Cyrillic and Latin characters, and for which the load command was saved in the file `restore_20100609-2.txt`, run :

```
isql -S instance1 -U admin -PSybase_password -J utf8 -i  
restore_20100609-2.txt
```

Restoring using another device

You can restore using a device other than that used for backup.

Specify the new device in the file:

Windows systems: `Data_Protector_home\Config\server\Cell\restoredev`

UNIX systems: `/etc/opt/omni/server/cell/restoredev`

Use the format:

```
"DEV 1" "DEV 2"
```

where DEV 1 is the original device and DEV 2 the new device.

❗ **IMPORTANT:** Delete this file after use.

On Windows, use the Unicode format for the file.

Monitoring sessions

You can monitor currently running sessions in the Data Protector GUI. When you run an interactive backup or restore session, a monitor window shows you the progress of the session. Closing the GUI does not affect the session.

You can also monitor sessions from any Data Protector client with the `User Interface` component installed, using the `Monitor` context.

On how to monitor a session, see the online Help index: "viewing currently running sessions".

Troubleshooting

This section lists general checks and verifications.

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 recognized issues and workarounds.
- See <http://www.hp.com/support/manuals> for an up-to-date list of supported versions, platforms, and other information.

Checks and verifications

If your configuration, backup, or restore failed:

- Examine system errors written to `debug.log`, located on the Sybase Server system in:
Windows systems: `Data_Protector_home\log`
UNIX systems: `/var/opt/omni/log`
- Make a test backup and restore of any filesystem on the problematic client. For information, see online Help.
- In a cluster environment, before performing procedures from the Data Protector CLI, ensure that the environment variable `OB2BARHOSTNAME` is set to the virtual server name. When the Data Protector GUI is used, this is not required.
- Ensure that the Sybase instance and its default Sybase Backup Server are online.
- **UNIX systems only:** Ensure that user `root` and user `sybase` are added to the Data Protector `admin` or `operator` user group.

Additionally, if your configuration or backup failed:

- If you use non-default Sybase settings, ensure that they are registered in:
Windows systems: The `System Properties` dialog box, which you access by double-clicking `System` in the `Control Panel`.
UNIX systems: The Data Protector Sybase configuration file.

Additionally, if your backup failed:

- Check the configuration of the Sybase instance described in [“Checking the configuration” \(page 20\)](#).
- Test the backup specification as described in [“Previewing backup sessions” \(page 25\)](#).

If the Data Protector part of the test fails:

1. **UNIX systems only:** Ensure that the owner of the backup specification is user `sybase` and that it is added to the Data Protector `operator` or `admin` user groups.
2. Create a Sybase backup specification to back up to a null or file device. If the backup succeeds, then the problem is probably related to devices. For information on troubleshooting devices, see the HP Data Protector Troubleshooting Guide.

If the test succeeds, start a backup directly from the Sybase Server. See [“Using Sybase commands” \(page 27\)](#).

Additionally, if your backup or restore failed:

- Test Data Protector data transfer using the `testbar` utility. Log in to the Sybase Server system as user `sybase` and run:
 - If your backup failed:

```
testbar -type:Sybase -appname:Sybase_instance_name \  
-bar:backup_specification_name -perform:backup
```
 - If your restore failed:

```
testbar -type:Sybase -appname:Sybase_instance_name \  
-bar:backup_specification_name -perform:restore \  
-object:object_name -version:object_version
```

where `object_name` is the name of the object to be restored.

If the test fails:

- Troubleshoot errors. See the text file `Trouble.txt` located on the Cell Manager in:
 - Windows systems:** `Data_Protector_home\help\enu`
 - UNIX systems:** `/opt/omni/gui/help/C`
- On the Sybase Server system, examine system errors, reported in:
 - Windows systems:** `Data_Protector_home\log\debug.log`
 - UNIX systems:** `/var/opt/omni/log/debug.log`

Additionally, if your restore failed:

- Ensure that the Data Protector operator user group has the `See private objects` user right selected. On how to change user rights, see the online Help index: "changing user rights".

Problems

Problem

Restore to another client system fails

When you start a restore of a database to the original Sybase instance, the session finishes successfully. However, when you start a restore of the database to a different Sybase instance on another client, your restore session fails with a message similar to the following:

```
Mar 11 18:16:13 2010: Backup Server: 4.124.2.1: Archive API error  
for device='ob2syb::2010/03/11-19::test_db:  
:incprod::00': Vendor application name=Data Protector A.06.10,  
Library version=221, API routine=syb_read(), Message=Object version  
not found.ar 11 18:16:13 2010: Backup Server: 6.32.2.3: ob2syb::  
2010/03/11-19::test_db::incprod::00: volume not valid or not requested  
(server: , session id: 62.) Mar 11 18:20:07 2010: Backup Server:  
4.132.1.1: Attempting to open byte stream device: 'ob2syb::  
2010/03/11-19::test_db::incprod::00'
```

The problem is that the IDB uses the name of the destination client instead of the name of the client from which the database was backed up.

Action

1. Set the OB2HOSTNAME variable on the target client: add the OB2HOSTNAME=*BackupClient.company.com* variable entry to the *Sybase_TargetInstance.cfg* configuration file. The location of the directory depends on the operating system:

Windows systems: *Data_Protector_home\tmp*

HP-UX and Solaris systems: */var/opt/omni/tmp*

2. Restart the restore of the database.

2 Data Protector HP Network Node Manager integration

Introduction

This chapter explains how to configure and use the Data Protector HP Network Node Manager (NNM) integration. It describes concepts and methods you need to understand to back up and restore the NNM database.

You can back up or restore NNM objects: the whole database or only parts of it.

Data Protector offers interactive and scheduled backups of the following types:

Table 7 Backup types

Full	Backs up the selected NNM objects.
Incremental	Backs up changes made to the selected NNM objects since the last full backup.

This chapter provides information specific to the Data Protector HP Network Node Manager integration. For general Data Protector procedures and options, see online Help.

Integration concept

The basic components of the Data Protector NNM integration are the following Perl scripts:

Table 8 Data Protector NNM integration components

<code>NNMpre.ovpl</code>	A script without arguments that: <ol style="list-style-type: none">1. Initiates a special NNM backup, instructing the NNM database to make a direct copy of itself to a location specified in the <code>solid.ini</code> file, from which Data Protector backs it up later.2. Pauses the eight NNM processes, so that Data Protector can actually back up the NNM data.
<code>NNMpost.ovpl</code>	A script without arguments that restarts the NNM processes after the backup completes.
<code>NNMScript.exe</code> (Windows systems only)	A script with a pre- and post- argument that locates the NNM Perl compiler and <code>NNMpre.ovpl</code> or <code>NNMpost.ovpl</code> , and starts the script.

NOTE: Files created by the embedded database remain on the disk and are overwritten by future backups. Remove the files manually to free the disk space.

The NNM Perl compiler is used for `NNMpre.ovpl` and `NNMpost.ovpl`.

While HP Network Node Manager is responsible for read/write operations to disk, Data Protector reads from and writes to devices and manages media.

Configuring the integration

Prerequisites

- Ensure that you have correctly installed and configured NNM.
 - For supported versions, platforms, devices, and other information, see the *HP Data Protector Product Announcements, Software Notes, and References* or <http://www.hp.com/support/manuals>.
 - For information on backup and recovery strategies and NNM concepts, see the HP Network Node Manager documentation.
- Ensure that you have correctly installed Data Protector. For information of how to install the Data Protector NNM integration in various architectures, see the *HP Data Protector Installation and Licensing Guide*.

Every NNM system you intend to back up from or restore to must have the Data Protector HP Network Node Manager Backup Integration and Disk Agent components installed.

Before you begin

- Configure devices and media for use with Data Protector. For information, see online Help.
- To test whether the NNM system and the Cell Manager communicate properly, configure and run a Data Protector filesystem backup and restore on the NNM system.

Tasks for the NNM administrator

- Communicate the location of the NNM backup directory, specified in the NNM embedded database file `solid.ini`.
- In `solid.ini`, comment out the line beginning with `At=` that schedules a nightly backup of the NNM embedded database.

Backup

The Data Protector NNM integration provides two backup types and two backup modes.

Table 9 Backup types

Full	Backs up all selected NNM objects.
Incremental	Backs up changes made to the selected NNM objects since the last full backup.

Table 10 Backup modes

Offline	The database is taken offline. Consequently, no changes can be made to the database during the backup process, leaving it in a consistent state.
Online	The database is in a paused state and the changes made to the database during the backup process are recorded to temporary files. When the backup completes, the database resumes its normal state and the changes from the temporary files are applied to the database, bringing it to a consistent state.

To perform an offline backup:

1. On the NNM system, take the NNM database offline by running:
`ovstop`
2. Back up the complete NNM directory using Data Protector.
3. On the NNM system, bring the NNM database online by running:
`ovstart`

Creating backup specifications

Create a backup specification using the Data Protector Manager.

1. In the Context List, click **Backup**.
2. In the Scoping Pane, expand Backup Specifications, right-click **Filesystem**, and click **Add Backup**.
3. Select a template:

Windows systems: NT_NNM_template

UNIX systems: Unix_NNM_template

You can also select the Blank Filesystem Backup template or any other template.

Click **OK**.

4. Select the appropriate client and directories to be backed up from the client.

Click **Next**.

5. Select devices to use for the backup.

To specify device options, right-click the device and click **Properties**.

Click **Next**.

6. Set backup options.

-
- ① **IMPORTANT:** If you have selected the NNM template, do not change the default pre- and post-exec options. If you have selected a different template, specify exactly the same pre-exec and post-exec scripts as specified in the NNM template.
-

Click **Next**.

7. Optionally, schedule the backup. For more information, see [“Scheduling backup specifications” \(page 24\)](#).

Click **Next**.

8. Save the backup specification, specifying a name and a backup specification group.

-
- 🔍 **TIP:** Preview backup session for your backup specification before using it. For details, see the online Help index: “previewing a backup”. Note that the backup preview does not run pre-exec and post-exec scripts.
-

Modifying backup specifications

To modify your backup specification, click its name in the Scoping Pane of the Backup context, then click the appropriate tab, and apply the changes.

Scheduling backup specifications

You can run unattended backups at specific times or periodically. For details on scheduling, see the online Help index: “scheduled backups”.

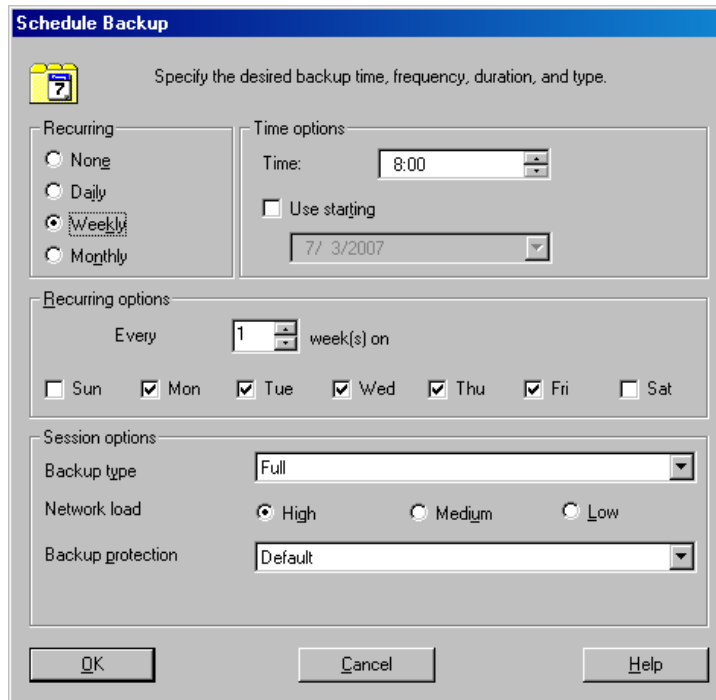
Example

To schedule backups at 8:00, 13:00, and 18:00 during week days:

1. In the Schedule property page, select the starting date in the calendar and click **Add** to open the Schedule Backup dialog box.
2. Under Recurring, select **Weekly**. Under Time options, select **8:00**. Under Recurring Options, select **Mon, Tue, Wed, Thu, and Fri**. See [“Scheduling a backup specification” \(page 43\)](#).
Click **OK**.
3. Repeat [Step 1](#) and [Step 2](#) to schedule another backup at 13:00, and another one at 18:00.

- Click **Apply** to save the changes.

Figure 24 Scheduling a backup specification



Starting backup sessions

Interactive backups are run on demand. They are useful for urgent backups or for restarting failed backups. Use the Data Protector GUI.

- In the Context List, click **Backup**.
- In the Scoping Pane, expand Backup Specifications and then Filesystem. Right-click the backup specification you want to use and click **Start Backup**.
- Specify Backup type and Network load. Click **OK**.

The message `Session completed successfully` is displayed at the end of a successful backup session.

Restore

To restore NNM objects:

- Stop all NNM processes.
- Restore the NNM objects using the Data Protector GUI.
- Perform the NNM recovery procedures.
- Restart the NNM processes.

For details, see the online Help index: “standard restore procedure” and the *NNM reporting and data analysis* manual.

Monitoring sessions

You can monitor currently running sessions in the Data Protector GUI. When you run an interactive backup or restore session, a monitor window shows you the progress of the session. Closing the GUI does not affect the session.

You can also monitor sessions from any Data Protector client with the `User Interface` component installed, using the Monitor context.

For information of how to monitor a session, see the online Help index: “viewing currently running sessions”.

Messages generated by scripts, NNM, and Data Protector are logged to the IDB.

Acceptable warnings on Windows

The following warnings, which are likely to occur during an NNM backup, have no impact on the validity of the backup. They are only informational.

Message

```
[Warning] From: session_owner Time: mm/dd/yy hr:mn:sc  
[error code] path\HP OpenView\NNM\bin\tcl7.5.dll  
Cannot preserve time attributes: ([5] Access is denied.).
```

Description

The file `tcl7.5.dll` is backed up, but the time attributes, which are not significant to Data Protector, are not preserved.

Message

```
[Warning] From: session_owner Time: mm/dd/yy hr:mn:sc  
[error code] path\HP OpenView\NNM\databases\analysis\default\solid.db  
Cannot open: ([33] The process cannot access the file ....).
```

Description

The embedded database file referenced in this message has already been backed up as part of the pre-exec script. Its default location is in the `path\HP OpenView\NNM\databases\analysis\default\backup` directory, which is specified in the `solid.ini` file. After the restore, copy the backed up `solid.db` file from that directory to the active `path\HP OpenView\NNM\databases\analysis\default` directory.

Message

```
[Warning] From: session_owner Time: mm/dd/yy hr:mn:sc  
[error code] path\HP OpenView\NNM\databases\openview\topo\netmon.lock  
Cannot open: ([33] The process cannot access the file ....).
```

Message

```
[Warning] From: session_owner Time: mm/dd/yy hr:mn:sc  
[error code] path\HP OpenView\NNM\databases\snmpCollect\dblock Cannot  
open: ([33] The process cannot access the file ....).
```

Description

These files are not significant to Data Protector.

Troubleshooting

This section lists problems you might encounter when using the Data Protector NNM integration.

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" for information of how to verify this.
- See the *HP Data Protector Product Announcements, Software Notes, and References* for general Data Protector limitations, as well as recognized issues and workarounds.
- See <http://www.hp.com/support/manuals> for an up-to-date list of supported versions, platforms, and other information.

Problems

Problem

The system is already in a paused state

NNM reports:

```
The system is already in a paused state. 'ovpause' cannot continue, If a synchronization error has occurred, try removing the file e:\Program Files\HP OpenView\tmp\ovpause.lock (Windows system) or /var/opt/OV/tmp/ovpause.lock (UNIX system) and then retrying the 'ovpause' command.
```

Action

Ensure that the NNM processes are not paused manually before the Data Protector NNM session starts. Otherwise, the pre-exec script `NNMpre.ovpl` fails.

Problem

The system is not in a paused state

NNM reports:

```
The system is not in a paused state. 'ovresume' cannot continue. If a synchronization error has occurred, try creating the empty file e:\Program Files\HP OpenView\tmp\ovpause.lock (Windows systems) or /var/opt/OV/tmp/ovpause.lock (UNIX systems) and then retrying the 'ovresume' command.
```

Action

Ensure that the NNM processes are not resumed manually during the Data Protector NNM session. Otherwise, the post-exec script `NNMpost.ovpl` fails and Data Protector displays the message Backup completed with errors.

Problem

ODBC Error: SQLSTATE=HY000

Data Protector reports:

```
ODBC Error:SQLSTATE=HY000 NATIVE ERROR=21306 SOLID Communication Error 21306: Server 'tcpip 2690' not found, connection failed Connect to ODBC data Source "ovdbrun" failed.
```

Action

Ensure that no NNM processes are paused manually before the Data Protector NNM session starts. Otherwise, the pre-exec script `NNMpre.ovpl` fails because it cannot connect to the NNM embedded database.

Problem

Embedded database is currently in the backup process

NNM reports:

```
Embedded database is currently in the backup process.
```

```
Aborting Data Protector backup.
```

Action

Ensure that the default scheduled backup in the `solid.ini` file is commented out. A Data Protector NNM backup and an active backup of the NNM embedded database cannot be performed simultaneously.

Problem

Wrong number of arguments

On Windows, Data Protector reports:

```
Wrong number of arguments. Please specify pre or post backup.
```

```
"NNMScript.exe pre" for pre-exec script "NNMScript.exe post" for  
post-backup script.
```

Action

Correct the number of arguments for `NNMScript.exe`, as specified in the pre-exec and post-exec backup options.

Problem

Couldn't find HP Network Node Manager key

On Windows, Data Protector reports:

```
Couldn't find HP Network Node Manager key in registry.
```

Action

Ensure that NNM is installed on the target client and that the registry key `HP Network Node Manager` exists under `HKEY_LOCAL_MACHINE\SOFTWARE\Hewlett-Packard\OpenView`.

Problem

Couldn't find the HP Network Node Manager PathName

On Windows, Data Protector reports:

```
Couldn't find the HP Network Node Manager PathName in registry.
```

Action

Ensure that a registry entry with the name `PathName` exists under

```
HKEY_LOCAL_MACHINE\SOFTWARE\Hewlett-Packard\OpenView\HP Network Node  
Manager and has a string value.
```

Problem

Couldn't find OmniBack II key

On Windows, NNM reports:

```
Couldn't find OmniBack II key in registry.
```

Action

Ensure that Data Protector with a Disk Agent is installed on the target client and that the registry key `OmniBack II` exists under

HKEY_LOCAL_MACHINE\SOFTWARE\Hewlett-Packard\OpenView. Any other name causes problems, potentially requiring reinstallation of the Disk Agent.

Problem

Couldn't find the Data Protector HomeDir

On Windows, NNM reports:

Couldn't find the Data Protector HomeDir in registry.

Action

Ensure that a registry entry with the name HomeDir exists under

HKEY_LOCAL_MACHINE\SOFTWARE\Hewlett-Packard\OpenView\OmniBackII\ Common, having a string value for the Data Protector path. Otherwise, create it or reinstall the Disk Agent.

Problem

Incorrect argument

On Windows, Data Protector reports:

Incorrect arguments. Use "pre" or "post".

Action

Ensure that NNMScript.exe has correct arguments, as specified in the pre- and post-exec backup options. The arguments are not case-sensitive.

Problem

Failure starting NNM_perl_compiler_path Data_Protector_home\bin*.ovpl.

On Windows, Data Protector reports:

Failure starting NNM_perl_compiler_path Data_Protector_home\bin*.ovpl.

Action

Ensure that the NNM Perl compiler has not been removed and paths for Data Protector and NNM in the registry are correct.

Problem

Execution of NNM_perl_compiler_path Data_Protector_home\bin*.ovpl failed

On Windows, NNM reports:

Execution of NNM_perl_compiler_path Data_Protector_home\bin*.ovpl failed.

Action

Ensure that *path*\HP OpenView\NNM\bin is in the PATH and scripts are in the *Data_Protector_home*\bin directory. Otherwise, the command that starts NNMpre.ovpl or NNMpost.ovpl fails.

3 Data Protector Network Data Management Protocol Server integration

Introduction

This chapter explains how to configure and use the Data Protector Network Data Management Protocol Server integration (**NDMP Server integration**). It describes concepts and methods you need to understand to perform filesystem backups and restores on a Network Attached Storage device.

Network Data Management Protocol (**NDMP**) is a protocol used to manage backup and restore operations on a Network Attached Storage (**NAS**) device. NDMP uses a client server model, where the Data Protector NDMP Media Agent client controls the backup, while the NDMP Server performs the actual backup operations.

The Data Protector NDMP Server integration offers interactive and scheduled filesystem backups of the following types:

- Full
- Incr1

For information on these backup types, see the *HP Data Protector Concepts Guide*.

The Data Protector NDMP Server integration offers two restore types:

- Standard filesystem restore
- Direct access restore

The Data Protector NDMP Server integration supports the following two types of backup:

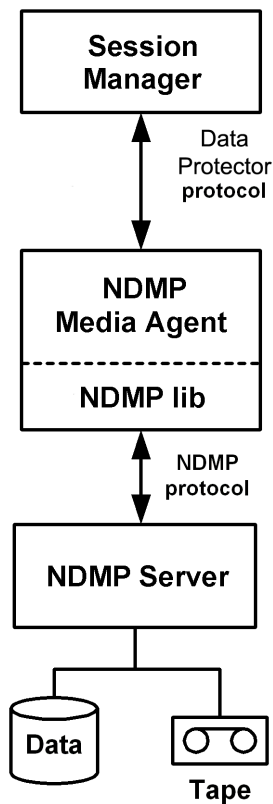
- for EMC Celerra (**Celerra**):
 - Dump
The default backup type, that backs up data at a file level.
 - NDMP volume backup (**NVB**)
An EMC-specific NDMP backup type, that backs up data blocks at a volume level.
- for Network Appliance (**NetApp**):
 - Dump
The default backup type, that backs up data at a file level.
 - Snap mirror to tape backup (**SMTape backup**)
A NetApp-specific NDMP backup type, that creates a snapshot of the source volume and backs up the current and all previous snapshot copies.

This chapter provides information specific to the Data Protector NDMP Server integration. For general Data Protector procedures and options, see online Help.

Integration concept

Data Protector integrates with NDMP Server through the Data Protector NDMP library and the NDMP Media Agent. The Data Protector NDMP library channels communication between the Data Protector Session Manager, and, through the NDMP interfaces, the NDMP Server. [“Data Protector NDMP Server integration architecture” \(page 49\)](#) shows the architecture of the integration.

Figure 25 Data Protector NDMP Server integration architecture



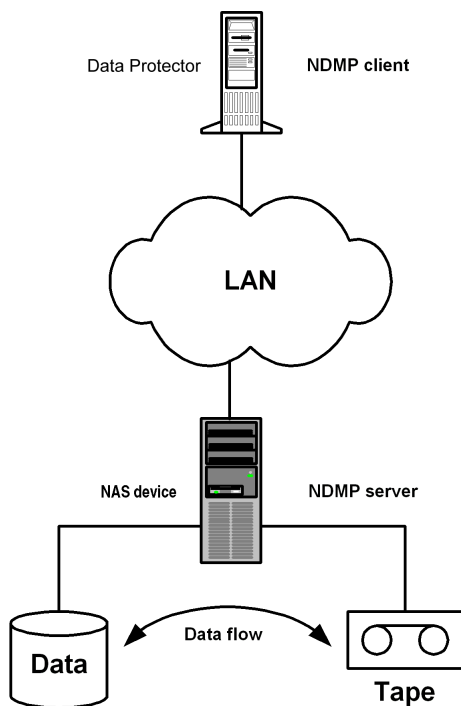
Legend	
Session Manager	Data Protector Session Manager: Backup Session Manager during backup and Restore Session Manager during restore. No Data Protector Disk Agents are involved in the session because the whole functionality is already implemented within the NDMP Media Agent.
NDMP Media Agent	The NDMP client, which contains a layer called the NDMP library. The library enables the NDMP Media Agent to communicate with the NDMP Server through the NDMP interfaces.

For more information on the NDMP protocol and NDMP interfaces, see the NDMP documentation. Data Protector supports the following NDMP Server types:

- NetApp NAS device (**NetApp**)
- Celerra NAS device (**Celerra**)
- BlueArc NAS device (**BlueArc**)
- Hitachi NAS device (**Hitachi**)
- HP-X9000 NAS device (**HP-X9000**)

In a typical environment (“[The NDMP environment configuration](#)” (page 50)), the NDMP Server system and the Data Protector client with the NDMP Media Agent installed (**NDMP client**) are connected to the LAN. However, data from the NDMP Server disks does not flow through the LAN, it is backed up to a tape device connected to the NDMP Server system. The NDMP client initiates, monitors, and controls data management and the NDMP Server executes these operations, having a direct control over devices connected to it and over the backup and restore speed.

Figure 26 The NDMP environment configuration



Due to the NDMP catalog handling design, Data Protector caches the entire catalog on the NDMP client before storing it to the Data Protector internal database (IDB). Since the catalog can increase in size significantly, the NDMP client caches parts of the catalog into **file history swap files**, located in the following directory:

Windows systems: `Data_Protector_home\tmp`

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

For more information on file history swap files, see “The NDMP specific omnirc file variables” (page 67).

Configuring the integration

To configure the Data Protector NDMP Server integration:

1. Import the NDMP Server system into the Data Protector cell.
2. Create a media pool for NDMP media.
3. Configure NDMP devices.

Prerequisites

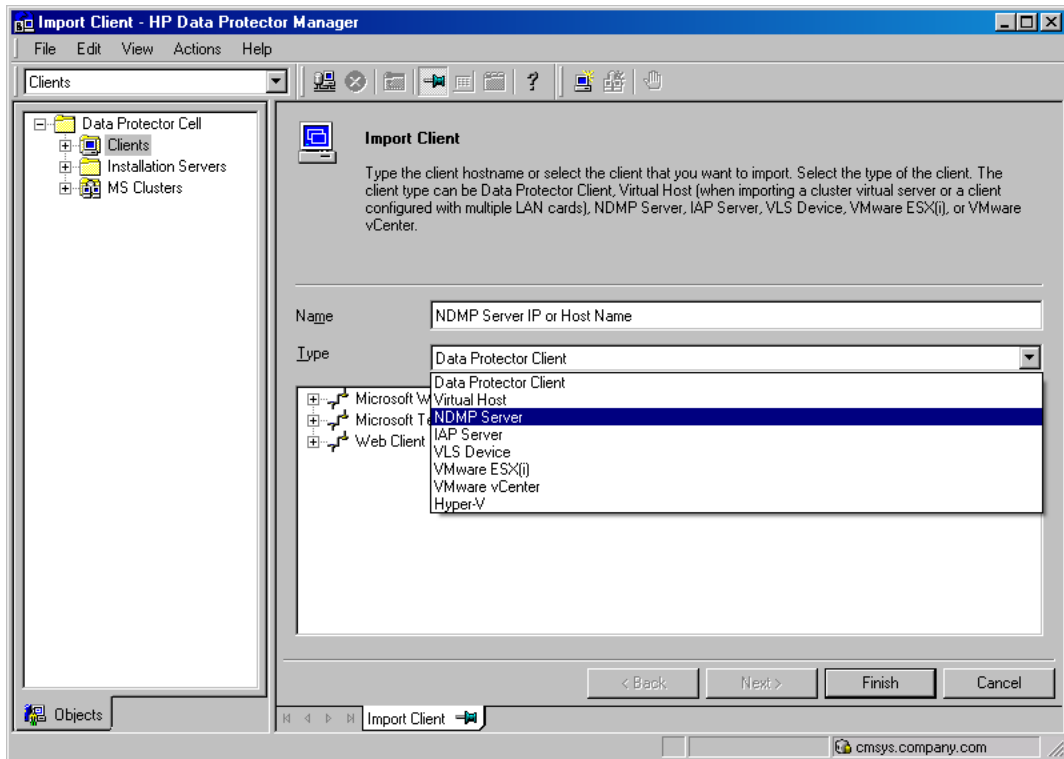
- Ensure that you have correctly installed and configured NDMP Server.
 - For supported versions, platforms, devices, and other information, see the *HP Data Protector Product Announcements, Software Notes, and References* or <http://www.hp.com/support/manuals>.
 - For information on installing, configuring, and using NDMP Server, see the NDMP Server documentation.
- Ensure that you have correctly installed Data Protector. For information of how to install Data Protector in various architectures, see the *HP Data Protector Installation and Licensing Guide*. Every NDMP client (Data Protector client that controls the NDMP Server backup) must have the Data Protector NDMP Media Agent component installed.

Importing NDMP Server systems

Import the NDMP Server system using the Data Protector GUI:

1. In the Context List, click **Clients**.
2. In the Scoping Pane, right-click **Clients** and click **Import Client**.
3. In the **Name** text box, type the name of the NDMP Server system you want to import. In the **Type** drop-down list, select **NDMP Server**.

Figure 27 Specifying an NDMP Server system



Click **Next**.

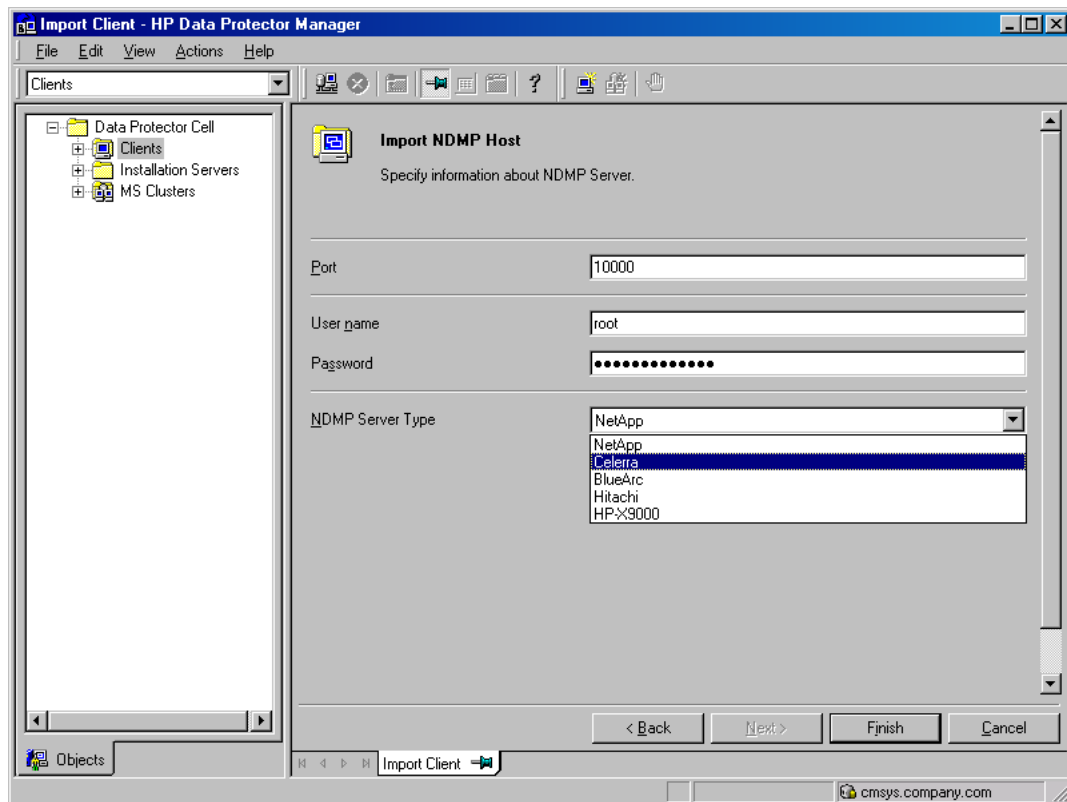
4. In the **Port** text box, specify the TCP/IP port number of the NDMP Server. The default number is 10000.

Provide the NDMP Server system user account that will be used by Data Protector to connect to the NDMP Server system. This user must have permission to read from and write to the NDMP media.

The Data Protector NDMP integration supports the "none", "text", and "MD5" NDMP authentication methods. Data Protector automatically detects and uses the method supported by your NDMP Server.

In the **NDMP Server Type** drop-down list, select the NAS device type.

Figure 28 Specifying an NDMP Server system



Click **Finish**.

Creating media pools

Create a special media pool for NDMP media. For information, see the online Help index: "creating media pools".

The NDMP media pool can only be used by devices using the NDMP data format (**NDMP devices**).

Limitations

- A medium cannot be used by different NDMP Server types. Consequently, the data that was backed up from an NDMP Server of a particular type (for example, NDMP-NetApp) cannot be restored to an NDMP Server of another type (for example, NDMP-Celerra).

Configuring NDMP devices

Configure NDMP devices using the Data Protector GUI.

Prerequisites

- The NDMP Server system must have a tape drive connected to it.
The drive must be supported by both NDMP Server and Data Protector.

Library robotics can be connected to:

- NDMP Server system (“Library configuration 1” (page 53)).
- NDMP client (“Library configuration 2” (page 54)).
- Data Protector client with the general Media Agent installed (**general Media Agent client**) (“Library configuration 2” (page 54)).

If it is connected to the NDMP Server system, the library robotics must be supported by both NDMP Server and Data Protector.

Figure 29 Library configuration 1

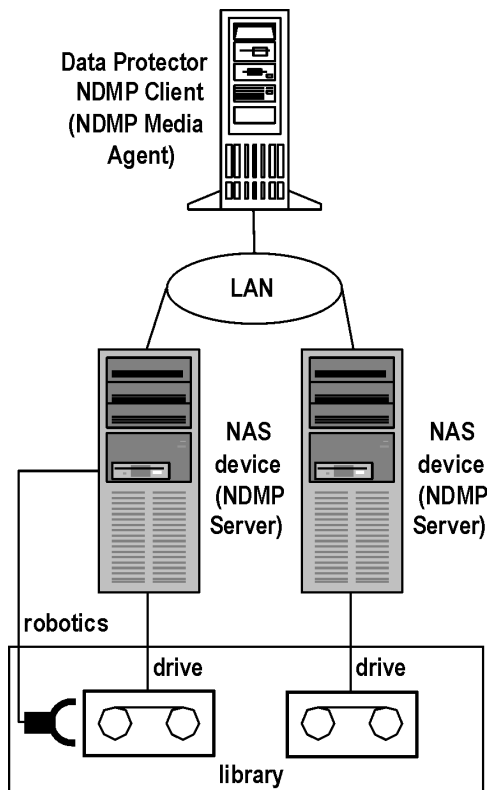
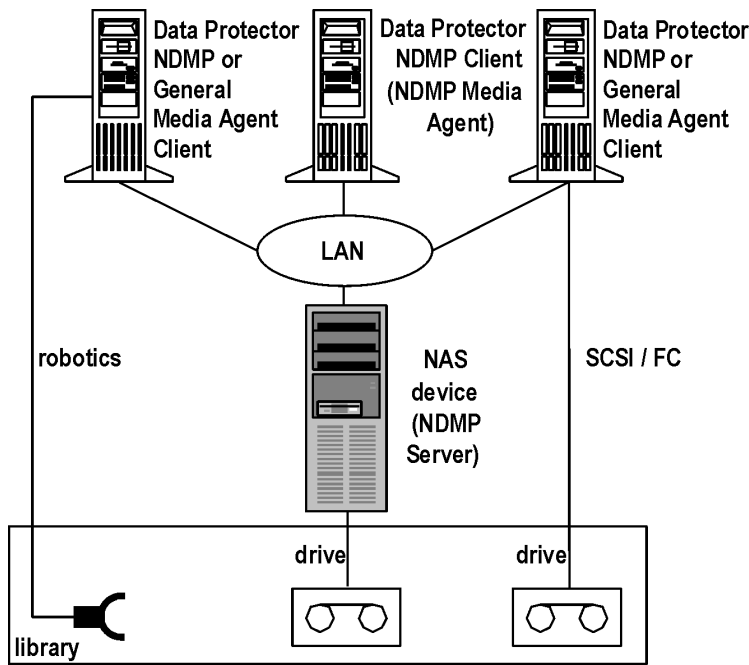


Figure 30 Library configuration 2



Several drives can be connected to the NDMP Server system.

If library robotics or drives are connected to the NDMP Server system, they can be controlled only by an NDMP client.

Library drives can be shared between multiple NDMP Server systems and general Media Agent clients, and with other applications. For more information, see the *HP Data Protector Concepts Guide*.

Limitations

- NDMP devices can only use NDMP media pools.

Configuring tape libraries

To configure a tape library with robotics connected to the NDMP Server system:

1. In the Context list, click **Devices & Media**.
2. In the Scoping Pane, right-click **Devices**, and then click **Add Device**.
3. Type a name for the device. Optionally, describe the device. See [“Configuring a library” \(page 55\)](#).

In **Device Type**, select **SCSI Library**.

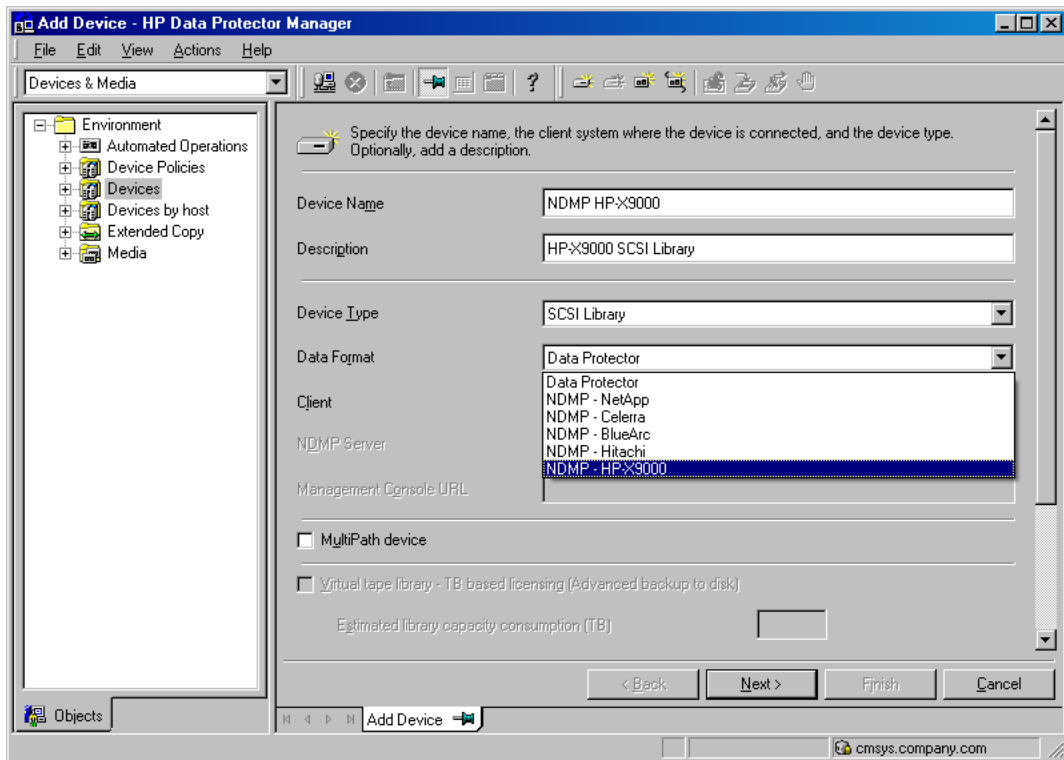
In **Interface Type**, select the NAS device used.

In **Client**, select the NDMP client that will control the library through the NDMP Server.

In **NDMP Server**, select the NDMP Server system with the library robotics connected to it.

Optionally, in **Management Console URL**, type a valid URL of the library management console. It will enable you to invoke a web browser and load the management console interface directly from the Data Protector GUI.

Figure 31 Configuring a library



Click **Next**.

4. Specify the library robotics SCSI address and the drive handling. For information, see [“Network Appliance configuration”](#) (page 57), [“EMC Celerra configuration”](#) (page 58), and [“BlueArc and Hitachi configuration”](#) (page 58)

Click **Next**.

5. Specify the slots to be used by Data Protector.

Click **Next**.

6. In the **Media Type** drop-down list, select the media type used in the library.
7. Click **Finish** and then click **Yes** to configure the drives in the library.
8. Type a name for the drive. Optionally, describe the drive.

In **Data Format**, select the NAS device used.

In **Client**, select the NDMP client that will control the library through the NDMP Server.

In **NDMP Server**, select the NDMP Server system with the library robotics connected to it.

Click **Next**.

9. Specify the SCSI address of the drive. For information, see [“Network Appliance configuration”](#) (page 57), [“EMC Celerra configuration”](#) (page 58), and [“BlueArc and Hitachi configuration”](#) (page 58).

Do not change the drive index number.

Click **Next**.

10. Specify the media pool for the NDMP media.

To specify advanced device options, click **Advanced**. For information on supported block sizes, see [“Block size”](#) (page 59).

NOTE: Multiplexing data streams is not supported by NDMP Server, limiting device concurrency to 1.

Click **Next**.

11. Select the device policies for the new drive and specify the device tag.

Click **Finish**.

12. Click **Yes** to create another drive or **NO** to finish the configuration.

For information of how to configure a tape library with robotics connected to a Data Protector NDMP or General Media Agent client and drives connected to the NDMP Server system, see the online Help index: "configuring SCSI libraries". Then configure the drives as described in [Step 8](#) through [Step 12](#).

Configuring standalone devices

To configure a standalone device:

1. In the Context List, click **Devices & Media**.
2. In the Scoping Pane, right-click **Devices**, and then click **Add Device**.
3. Type a name for the device. Optionally, describe the device.

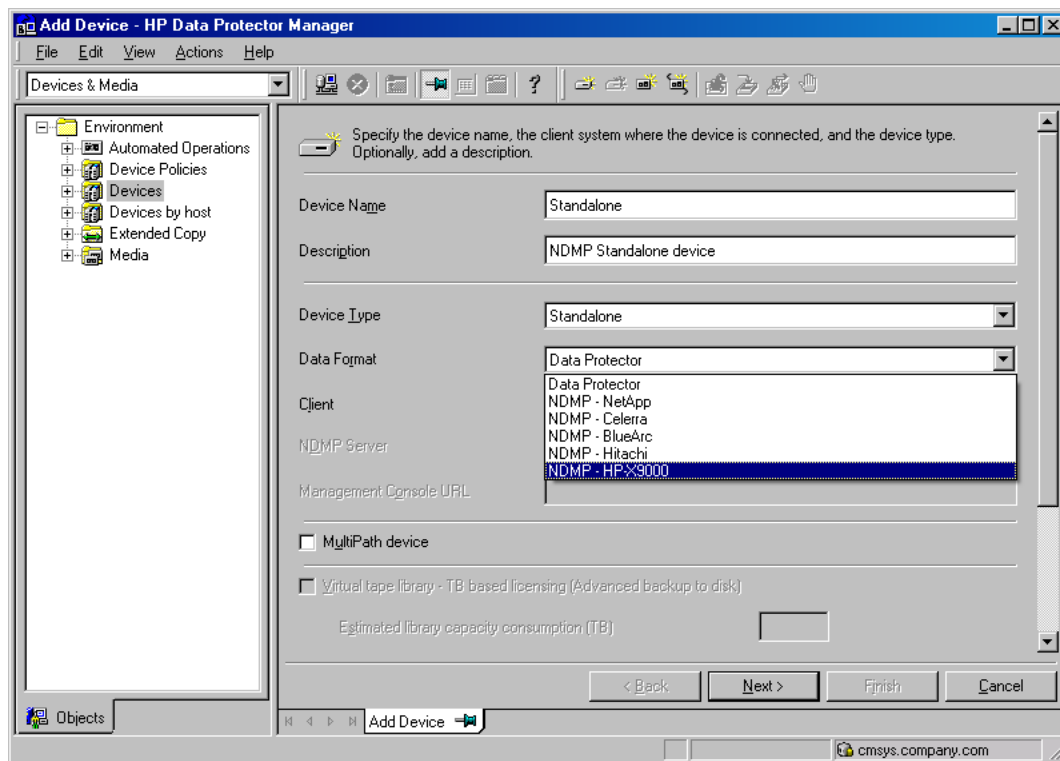
In **Device Type**, select **Standalone**.

In **Data Format**, select the NAS device used.

In **Client**, select the NDMP client that will control the device through the NDMP Server.

In **NDMP Server**, select the NDMP Server system to which the standalone device is connected.

Figure 32 Configuring a standalone device



Click **Next**.

4. Provide the SCSI address of the device. For information, see ["Network Appliance configuration"](#) (page 57), ["EMC Celerra configuration"](#) (page 58), and ["BlueArc and Hitachi configuration"](#) (page 58).

Click **Next**.

5. Specify the media pool.

To specify advanced device options, click **Advanced**. For information on supported block sizes, see “Block size” (page 59).

NOTE: Multiplexing data streams is not supported by NDMP Server, limiting device concurrency to 1.

6. Click **Finish**.

Network Appliance configuration

Before you begin

- Ensure that the NDMP Server is online.

Standalone tape devices and drives in a tape library

To get information about standalone tape devices (or drives in a tape library) connected to the NDMP Server system, run:

```
sysconfig -t
```

on the NDMP Server system. The SCSI address is written at the beginning of the output and consists of four parts. See “Analyzing the drive’s SCSI address” (page 57).

Table 11 Analyzing the drive’s SCSI address

Parts	Description
{n u}	no rewind and unload/reload respectively. ¹
rst	Raw SCSI tape (always present).
{0 1 2 ...}	Device number.
{l m h a}	Data density and compression.

¹ Data Protector supports only the no rewind devices.

Example

The output for a DLT 4000 drive is:

```
nrst0m - no rewind device, format is:42500 bpi 6.0GB
```

Library robotics

To get the SCSI address of the library robotics connected to the NDMP Server system, run:

```
sysconfig -m
```

on the NDMP Server system. The SCSI address consists of two parts. See “Analyzing the library Robotics’ SCSI address” (page 57).

Table 12 Analyzing the library Robotics’ SCSI address

Parts	Description
mc	Media changer device (always present).
{0 1 2 ...}	Device number.

Example

The output for a DLT 4000 library is:

```
mc0
```

EMC Celerra configuration

Before you begin

- Ensure that the NDMP Server is online.

SCSI devices

To get information about SCSI devices (tape drives and library robotics) connected to the EMC Celerra NAS device:

1. Log in to the Celerra control station.
2. Run:

```
server_devconfig server_name -list -scsi -all
```

Example

See “[Example of a list of SCSI devices](#)” (page 58) for an example list of SCSI devices. `c2t210` and `c2t310` are the SCSI addresses of the drives in the tape library and `c2t010` is the SCSI address of the library robotics.

Table 13 Example of a list of SCSI devices

Name	SCSI address	Device type	Information
jbox1	c2t010	jbox	ATL P1000 62200001.03
tape2	c2t310	tape	QUANTUM DLT7000 1624q\$
ttape2	c2t210	tape	QUANTUM DLT7000 1624q\$

BlueArc and Hitachi configuration

Before you begin

- Ensure that the NDMP Server is online.

Standalone tape devices and drives in a tape library

To get information about standalone tape devices (or drives in a tape library) connected to the NDMP Server system:

1. Log in to the NDMP Server system.
2. Run:

```
evs list
```

The command provides you with an EVS ID of the NDMP Server system for which you need to configure a device.

3. Run:

```
ndmp-devices-list -t tape -v VNodeID
```

The command lists all standalone tape devices (or drives in a tape library) connected to the NDMP Server system.

`VNodeID` is the EVS ID of the NDMP Server system extracted in [Step 2](#).

The SCSI address is written at the beginning of the `ndmp-device-list` output and consists of the LUN, Target and device ID number. See “[Analyzing the drive’s SCSI address](#)” (page 59).

Table 14 Analyzing the drive's SCSI address

Parts	Description
dev/mt	Tape device
d2 1 2 3...	Device ID number.

Example

The output for a standalone tape device (or a drive in a tape library) is:

```
16/dev/mt_d2|1 01YFPdba01 0x2001f29ccd2ca000:1
```

Where /dev/mt_d2|1 is the SCSI address of the tape device.

Library robotics

To get the SCSI address of the library robotics connected to the NDMP Server system:

1. Log in to the NDMP Server system.
2. Run:

```
evs list
```

The command provides you with an EVS ID of the NDMP Server system for which you need to configure a device.

3. Run:

```
ndmp-devices-list -t changer -v VNodeID
```

The command lists all library robotics connected to the NDMP Server system.

VNodeID is the EVS ID of the NDMP Server system extracted in [Step 2](#).

The SCSI address is written at the beginning of the `ndmp-device-list` output and consists of the LUN, Target and device ID number. See [“Analyzing the library Robotics’ SCSI address”](#) (page 59).

Table 15 Analyzing the library Robotics’ SCSI address

Parts	Description
dev/mc	Media changer device
d2 1 2 3...	Device ID number.

Example

The output for a media changer device of library robotics is:

```
5/dev/mc_d2|0 01YFPdba00 0x2001f29ccd2ca000:0 N/A
```

Where /dev/mc_d2|0 is the SCSI address of the media changer device.

Block size

The integration supports variable tape block sizes. Before selecting the block size for each NAS device, you should consider the following:

- Ensure that the NDMP Server is configured to support variable block size.
- The device used for restore must have the same or greater block size than the one that was used for backup.

- By NetApp, for a SMTape backup on Data ONTAP version earlier than version 8.0, you must set the **Block size** option to 240 kB. The required block size for the Data ONTAP version 8.0 is between 4 kB to 256 kB.
Note that Data Protector supports block sizes between 8 kB to 1024 kB. The recommended (default) block size is 64 kB.
- By Celerra, the block size value should not be greater than the Celerra `readWriteBlockSizeInKB` parameter.



TIP: To get the current value of the `readWriteBlockSizeInKB` parameter, run:

```
server_param server_3 -facility PAX -info
readWriteBlockSizeInKB -verbose
```

NOTE:

- If the set block size is not supported by the NAS device, and you start a backup, Data Protector displays an error and aborts the session.
 - Although the Data Protector media formatting completes successfully, that does not guarantee that the NAS device supports the set block size, and backup may still fail.
-

Backup

Limitations

- Only filesystem backup is supported.
- You cannot store an NDMP backup and a standard Data Protector backup on the same medium.
- Device concurrency is limited to 1.
- You cannot browse devices and filesystems.
- Only `Full` and `Incr1` backup types are supported.
- Object copying and object mirroring are not supported.
- Media copying is not supported for NDMP-Celerra backup sessions.
- Backing up data using the Data Protector **Reconnect broken connections** functionality is not supported.
- The `NVB` backup type enables you to only back up entire file systems. For example, you can back up `/ufs1`, but not `/ufs1/dir1`.
- The `NVB` backup type is supported on EMC Celerra DART version 5.6.46.11 or later.
- Directory direct access restore (DDAR) cannot be used with backup images created with the NDMP volume backup (`NVB`) option selected.
- The `NVB` backup type and file or directory filtering cannot be used together. If both are used, `NVB` takes precedence and the filters have no effect.
- With the `SMTape` backup type, a backup image of a volume in a particular aggregate type cannot be used for restore to a volume in a different aggregate type.
- With the `SMTape` backup type, a backup image of a volume in a regular aggregate cannot be used for restore to a volume in a larger aggregate, and the other way round.
- The `SMTape` backup type offers only full backup (level-0 backup).
- The `SMTape` backup type enables you to only back up entire file systems. For example, you can back up `/ufs1`, but not `/ufs1/dir1`.

- By default, you cannot select more than 5 million files for backup.
To enable higher values (up to 20 millions), set the OB2NDMPMEMONLY omnirc file variable to 0. For more information, see [“The NDMP specific omnirc file variables”](#) (page 67).
- Once you have selected a directory, you cannot exclude any subdirectories or files from backup. Specifically, the following options are not supported:
 - Data Protector GUI: the Trees/Filters set of options: Trees, Excludes, Skips, and Onlys.
 - Data Protector omnib command: -trees, -exclude, -skip, and -only.

Before you begin

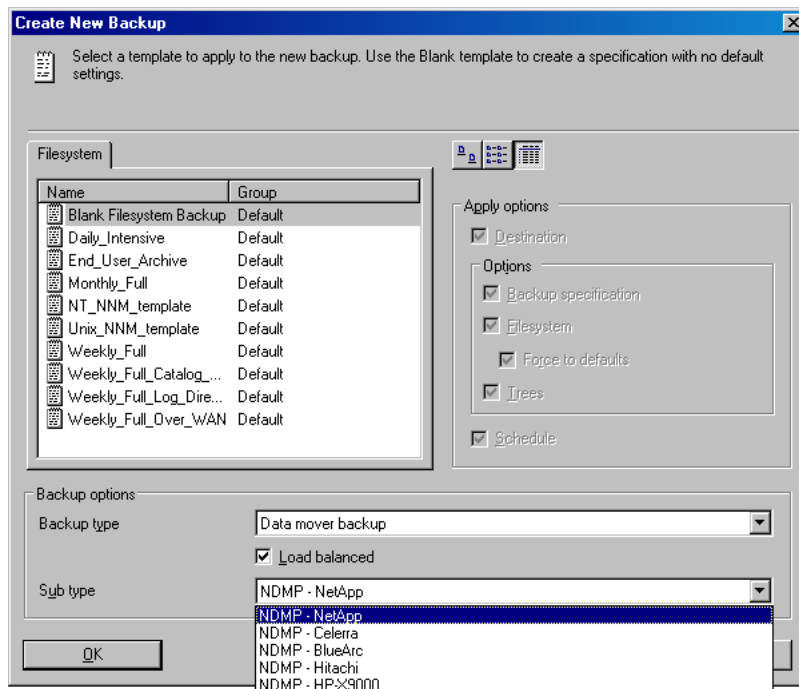
- Ensure that media to be used are formatted.
- **NetApp systems only:** Get information about filesystems exported from the NDMP Server system by running exportfs.

Creating backup specifications

Create a backup specification using the Data Protector Manager.

1. In the Context List, click **Backup**.
2. In the Scoping Pane, expand **Backup Specifications**, right-click **Filesystem**, and click **Add Backup**.
3. Select a template. In Backup type, select **Data mover backup**. In Sub type, select the NDMP Server type (for example, **NDMP-NetApp**). Optionally, select the **Load balanced** option. See [“Selecting a backup template”](#) (page 61).

Figure 33 Selecting a backup template

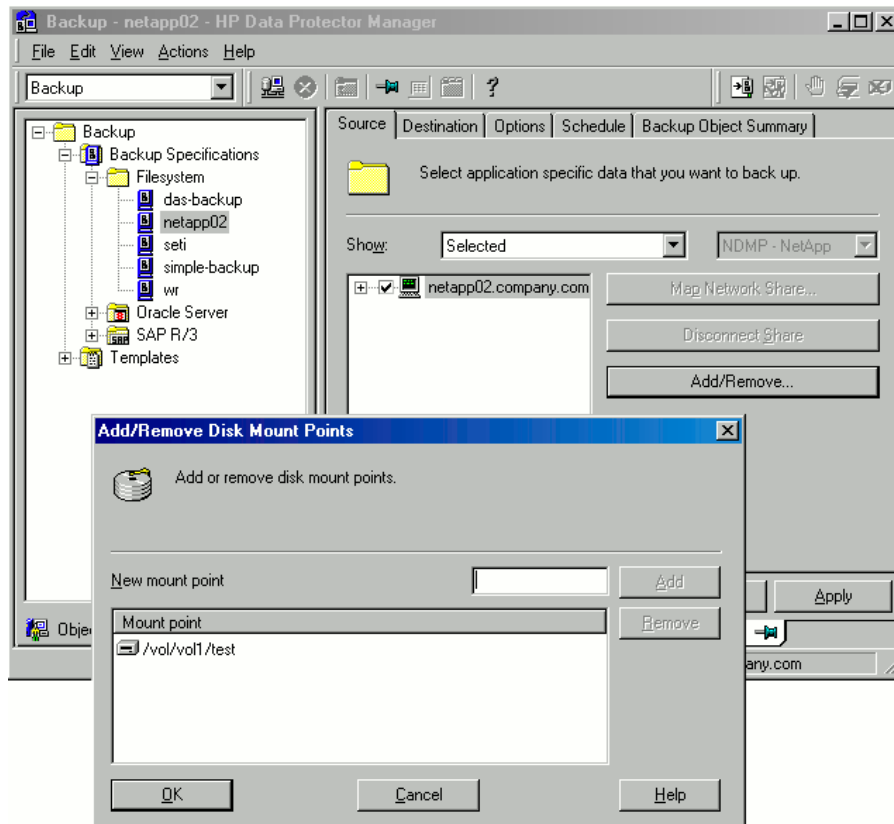


Click **OK**.

4. Select the NDMP Server system you want to back up and click **Add/Remove**.
In the Add/Remove Disk Mount Points dialog box, specify the filesystem mountpoints you want to back up: type the pathname of each directory in New mount point and click **Add**. See [“Specifying the NDMP Server mountpoints for backup \(UNIX systems\)”](#) (page 62).

Click **OK**.

Figure 34 Specifying the NDMP Server mountpoints for backup (UNIX systems)



Click **Next**.

5. Select devices to use for the backup.

To specify device options, right-click the device and click **Properties**.

Click **Next**.

6. Set backup options.

Click **Next**.

7. Optionally, schedule the backup.

Click **Next**.

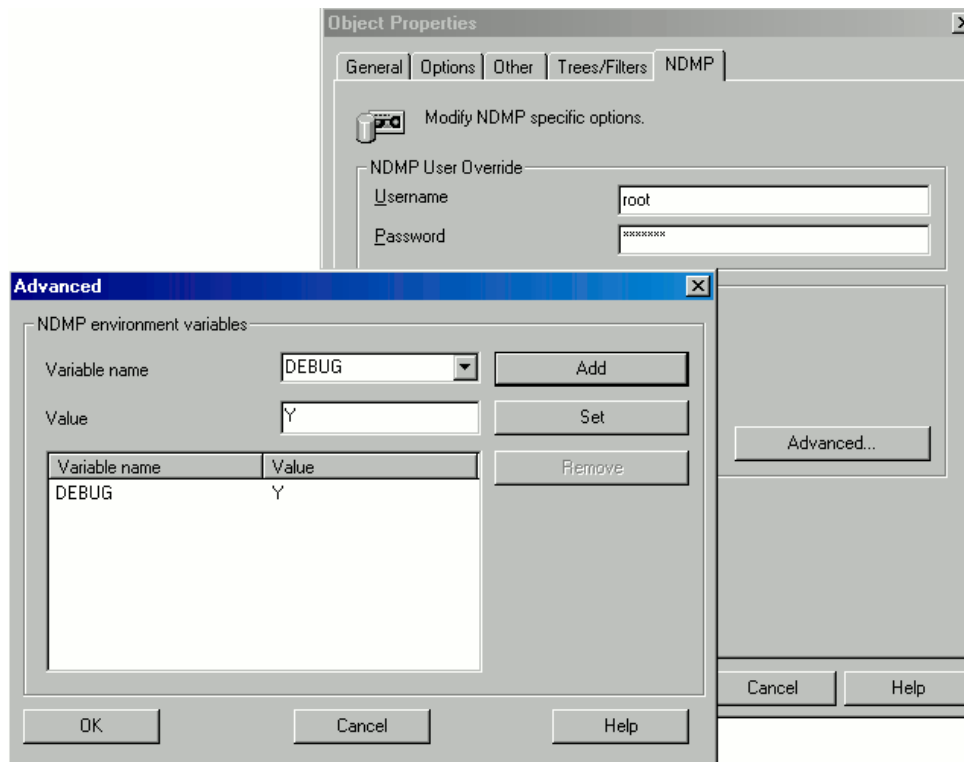
8. Review the summary of the backup specification.

To specify the NDMP options for a specific backup object, right-click the object, click **Properties**, and click the **NDMP** tab.

For each object, you can specify a new user account that will override the user account specified in the Import NDMP Host dialog box, provided that the access rights are properly set on the selected NAS device system.


To set the NDMP environment variables, click **Advanced**. See "Specifying advanced NetApp options" (page 63). For more information, see "NDMP environment variables" (page 66).

Figure 35 Specifying advanced NetApp options



For an EMC Celerra NDMP client, in **NDMP backup type**, select either **dump** or **NVB**.
For a NetApp NDMP client, in **NDMP backup type**, select either **dump** or **SMTape**.
Click **Next**.

9. Save the backup specification, specifying a name and a backup specification group.

 **TIP:** Preview backup session for your backup specification before using it. For details, see the online Help index: "previewing a backup".

Modifying backup specifications

To modify your backup specification, click its name in the Scoping Pane of the Backup context, then click the appropriate tab, and apply the changes.

Starting backup sessions

Interactive backups are run on demand. They are useful for urgent backups or for restarting failed backups. Use the Data Protector GUI.

1. In the Context List, click **Backup**.
2. In the Scoping Pane, expand Backup Specifications and then Filesystem. Right-click the backup specification you want to use and click **Start Backup**.
3. Select a Backup type and Network load. Click **OK**.

Restore

Restore filesystems using the Data Protector GUI or CLI.

Limitations

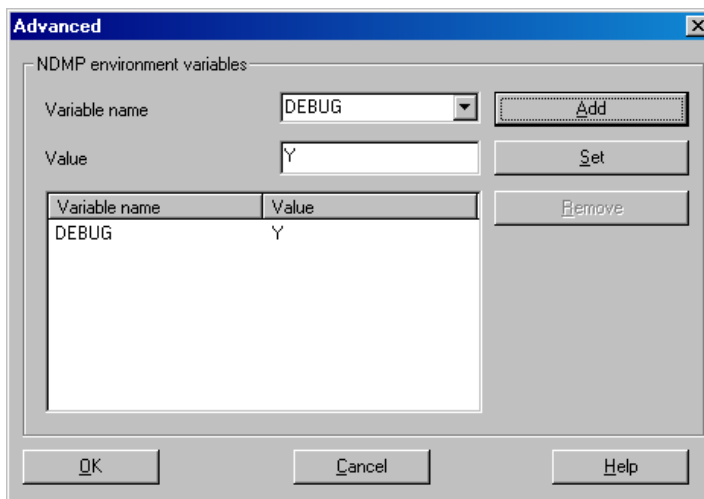
- Once you have selected a directory, you cannot exclude any subdirectories or files from restore. Specifically, the following options are not supported:
 - Data Protector GUI options: `Restore only` and `Skip`.
 - Data Protector CLI `omnir` command: `-only`, `-skip` and `-exclude`.
- The data that was backed up from an NDMP Server of a particular type (for example, NDMP-NetApp) cannot be restored to an NDMP Server of another type (for example, NDMP-Celerra).
- When restoring to another NDMP Server, the device to restore from must be connected directly to the target NDMP Server, and the device must be selected or specified as the restore device in the Data Protector GUI or CLI.
- Restore preview is not supported.
- Restoring data using the Data Protector **Restore by Query** functionality is not supported.
- Restore of data residing on more than one medium using the **List from Media** functionality is not supported. To perform such a restore, you should first import all related media.

Restoring using the Data Protector GUI

1. In the Context List, select **Restore**.
2. In the Scoping Pane, expand **Filesystem**, expand the client with the data you want to restore, and then click the object that has the data.
3. In the Source page, browse for and select the objects you want to restore.
4. In the Destination page, specify a restore target client for every selected object. By default, data is restored to the original location, from where the data was originally backed up. To restore to a new location, select **Restore to new location** and type the new path.
5. In the Options page, specify the NDMP Server system user account that will be used by Data Protector to connect to the NDMP Server system. This user must have permission to read from and write to the NDMP media.

To specify the NDMP environment variables, click **Advanced** (“NDMP advanced restore options” (page 64)). For more information, see “NDMP environment variables” (page 66).

Figure 36 NDMP advanced restore options



6. In the Devices page, select devices you want to use for the restore.
For more information, see the online Help index: “restore, selecting devices for”.

7. Optionally, in the Media page, specify the media allocation priority.
8. Optionally, in the Copies page, specify the media set to restore from.
9. Click **Restore**.
10. In the Start Restore Session dialog box, click **Next**.
11. Specify **Report level** and **Network load**.
12. Click **Finish** to start the restore.

Direct access restore

Direct access restore is an optimized data recovery operation. Backed up data is accessed directly, in the middle of a tape.

This is achieved by partitioning backed up data into segments during backup and recording their start addresses.

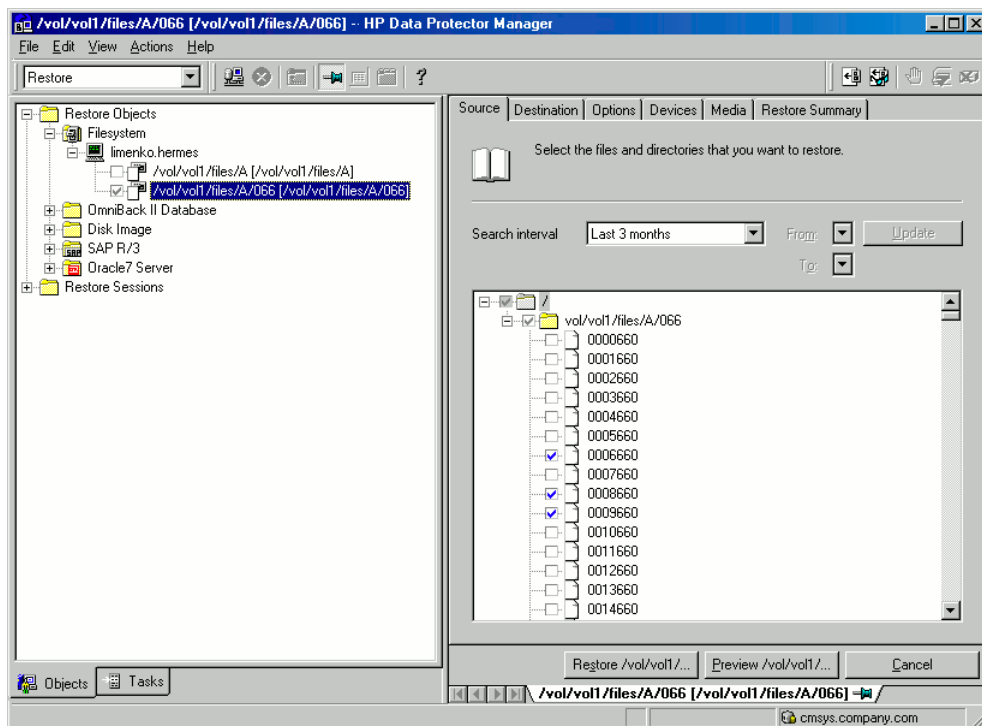
During restore, Data Protector first computes which segment contains the requested file or directory, then locates the segment, and finally starts reading through it to locate the beginning of the file or directory.

Prerequisites

File history tracking must be turned on during the backup. For information of how to enable file history tracking, see [“NDMP environment variables”](#) (page 66).

To enable direct access restore, set the NDMP environmental variable `DIRECT` to `Y`. The procedure for the direct access restore is the same as for standard restore. The only difference is that you can browse for and select individual files and directories for restore. See [“Selecting NDMP Server Data for direct access restore”](#) (page 65).

Figure 37 Selecting NDMP Server Data for direct access restore



Limitations

- **NetApp:**
 - Direct access restore (DAR) of files is supported on ONTAP version 6.1.x and later.
 - Directory direct access restore (DDAR) is supported on ONTAP version 6.4.x and later.

- Direct access restore (DAR) of files cannot be used with backup images created with the Snap mirror to tape backup (SMTape backup) option selected.
- Directory direct access restore (DDAR) cannot be used with backup images created with the Snap mirror to tape backup (SMTape backup) option selected.
- **Celerra:**
 - Directory direct access restore (DDAR) cannot be used with backup images created with the NDMP volume backup (NVB) option selected.
- Directory direct access restore (DDAR) is not supported when using BlueArc or Hitachi NAS devices.
- If you select both a directory and individual files from another directory and start the restore, only the selected files are restored. To restore both, use standard restore (set the NDMP environment variable `DIRECT` to `N`).

Restoring using another device

You can restore using a device other than that used for a backup. For more information, see the online Help index: “restore, selecting devices for”.

NDMP environment variables

Set the NDMP environment variables for the selected NAS devices using the Data Protector GUI. See “Specifying advanced NetApp options” (page 63) and “NDMP advanced restore options” (page 64).

The following tables show the supported NDMP environment variables:

Table 16 NDMP variables for NetApp NAS device

Variable	Value	Function
HIST	y/n Default: y	Turns on/off file history tracking.
DIRECT	y/n Default: y	Enables direct access restore.
LEVEL	0, 1, 2, ... 9 Default: 0 (full)	Specifies backup level.
SMTAPE_SNAPSHOT_NAME ¹	<i>Snapshot_copy_name</i> Default: Invalid	Specifies the snapshot copy name. The specified snapshot and all older snapshot copies are backed up to a tape.
SMTAPE_DELETE_SNAPSHOT	y/n Default: n	Deletes the auto snapshot copy created after the backup.
SMTAPE_BREAK_MIRROR	y/n Default: n	Disconnects the SnapMirror after the restore. NOTE: After a successful restore, the restored volume is in the restricted state and does not become writable unless the <code>SMTAPE_BREAK_MIRROR</code> variable is set to <code>y</code> .

¹ Supported only on the Data ONTAP version 8.0.7 or later.

Table 17 NDMP variables for Celerra NAS device

Variable	Value	Function
HIST	y/n Default: y	Turns on/off file history tracking.
DIRECT	y/n Default: y	Enables direct access restore.
LEVEL	0, 1, 2, ... 9 Default: 0 (full)	Specifies backup level.
BASE_DATE	<i>32bit level32bit date</i>	Incremental backup based on a specific date.
OPTIONS	LK	Follow symbolic links.
	AT	Preserve access time.
	NT	Save NT attributes.
	MI/MD/MM	Restore collision policy for localization.

Table 18 NDMP variables for BlueArc and Hitachi NAS device¹

Variable	Value	Function
HIST	y/n Default: y	Turns on/off file history tracking.
DIRECT	y/n Default: y	Enables direct access restore.
LEVEL	0, 1, 2, ... 9 Default: 0 (full)	Specifies backup level.
TYPE	dump/tar Default: dump	Specifies backup type.
UPDATE	y/n Default: y	Keeps a record of the backup time. Later incremental backups can use this backup as a base.
FILESYSTEM	<i>directory_name</i> Default: none	Specifies the directory to be backed up.
EXCLUDE	A separated list of files to be excluded from backup. Default: none	Specifies files or directories to be excluded from the backup.

¹ For information on other variables, see the vendor-specific documentation.

NOTE: You can also set some NDMP environment variables using the `omnirc` file. For more information, see [“The NDMP specific omnirc file variables”](#) (page 67).

The NDMP specific omnirc file variables

For details of how to set the `omnirc` variables, see the online Help index: [“omnirc options”](#).

NOTE: You can also set some variables using the Data Protector GUI. See “Specifying the NDMP Server mountpoints for backup (UNIX systems)” (page 62), “Specifying advanced NetApp options” (page 63), and “NDMP environment variables” (page 66).

The GUI setting overrides the setting in the `omnirc` file.

The NDMP specific `omnirc` file variables are:

- **OB2NDMPFH** (Y/N)

Default: Y

When set to Y, the NDMP Server file history tracking is turned on, which is a prerequisite for browsing and restoring individual files. However, this impacts the time needed for such a backup.

This setting overrides the file history setting on the NDMP Server every time a backup is started.

- **OB2NDMPDIRECT** (Y/N)

Default: Y

When set to Y, Data Protector uses the direct access restore functionality, provided that the NDMP Server file history tracking was turned on during the backup.

- **OB2NDMPMEMONLY** (0/1)

Default: 1

This variable defines how the NDMP Media Agent uses system resources.

When set to 1, the NDMP Media Agent uses system physical memory only.

When set to 0, the NDMP Media Agent stores part of the catalog in file history swap files.

Set the variable to 0 whenever the number of files in the backup specification exceeds 5 millions. Consequently, the NDMP Media Agent can handle backups of up to 20 million files (in one backup specification), provided the system has enough resources.

For example, to back up 20 million files, where 10% of the total number of backed up files are directories, with the average directory name consisting of 25 characters, and average filename consisting of 10 characters, you need approximately 1.9 GB of system memory and 2.8 GB of disk space.

For optimal performance, select 10 million files and directories for backup.

For more information on file history swap files, see the `OB2NDMPFHFILEOPT` variable description.

- **OB2NDMPCATQESIZE**

Default: 5

This variable sets the number of internal buffers that hold catalog information before storing it to file history swap files. By fine tuning the value, you can increase, to a certain extent, NDMP backup performance.

When set to 5, the NDMP Media Agent can process up to 20 million files (in one backup specification), provided that enough system resources are available (approximately 1.9 GB of system memory and 2.8 GB of disk space).

Set the variable to higher values if the number of files in the backup specification is less than 20 millions and enough system memory is available.

To calculate memory allocation overhead in kilobytes, multiply the variable value by 512.

- **OB2NDMPFHFILEOPT**

Defaults:

Windows systems: `Data_Protector_home\tmp, 32, 1024`

UNIX systems: /var/opt/omni/tmp, 32, 1024

This variable fine tunes file history swap files usage. It has three parameters that define the following:

1. Pathname of the directory where the file history swap files are stored.
2. Maximum number of file history swap files, created by Data Protector on the NDMP client's disk.
3. Maximum size of a file history swap file (in MB).

The parameters are separated by commas. You can specify several sets of parameters. Use a semicolon to separate them.

Example

Windows systems: C:\tmp, 32, 1024; D:\tmp\tmp_1, 10, 1024

UNIX systems: /tmp, 10, 1024; /var/tmp, 5, 60

When the files in the first directory are full, the integration writes data to the files in the next specified directory. If the allocated disk space is used up during the backup, the backup fails. File history swap files can increase in size significantly. Use the following formula to calculate approximate disk consumption:

$$EstConsumption = (NumOfFiles + NumOfDirs) \times (136 + AverageFileNameSize)$$

where NumOfFiles is the number of backed up files and NumOfDirs is the number of backed up directories.

See the calculations in “Approximate disk consumption by file history swap files” (page 69) that presume that the number of directories is up to 10% of the total number of files, the average directory name length is 25 characters, and the average file name length is 10 characters.

Table 19 Approximate disk consumption by file history swap files

Number of backed up files and directories	Approximate disk consumption by file history swap files
5 millions	0.7 GB
10 millions	1.4 GB
20 millions	2.8 GB

Media management

Data Protector media management is limited because data is backed up by NDMP Server in its specific data format.

Data Protector supports the following media management functionalities:

- Import and export of media.
- Media scan.
- Media initialization.
- Dirty drive detection.

Data Protector does not support the following media management functionalities:

- Verification of backed up data.
- Media copy for NDMP-Celerra backup sessions.

For more information, see online Help.

Troubleshooting

This section lists problems you might encounter when using the Data Protector NDMP Server integration.

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".
- For general Data Protector limitations, as well as recognized issues and workarounds, see the *HP Data Protector Product Announcements, Software Notes, and References*.
- For an up-to-date list of supported versions, platforms, and other information, see <http://www.hp.com/support/manuals>.

Problems

Problem

End of media

At the end of the backup, Data Protector starts storing the catalog to the media. The catalog size increases with the number of files backed up. Since Data Protector has no control over how much free space is left on the media, the `End of Media` error may occur during the writing of the catalog. This has no impact on future restore because the catalog is still stored in the IDB. However, the medium cannot be imported anymore.

Problem

Import of NDMP media failed

Action

Ensure that the drive used for importing NDMP media is connected to an NDMP Server system.

Problem

A tape remains in the drive after a successful drive scan

Action

Eject the tape manually and set the `OB2SCTLMOVETIMEOUT omnirc` variable on the NDMP client to a higher value (for example, 360000 or higher).

For details of how to set the `omnirc` variables, see the online Help index: "omnirc options".

Problem

Data Protector was unable to set NDMP record size

Data Protector reports:

```
DP was unable to set NDMP record size. Reason for this might be that NDMP server doesn't support specified record size. Please check the release notes in order to determine which record size is supported for your NDMP server.
```

Action

See "Block size" (page 59).

A Data Protector NetApp SnapManager solution

Introduction

This appendix describes the Data Protector NetApp SnapManager solution which, when used together with standard Data Protector functionality, enables backup and restore of NetApp SnapManager snapshots to and from Data Protector backup media.

The solution is available only on Windows systems.

Concepts

The NetApp SnapManager for Microsoft Exchange (SME) and NetApp SnapManager for Microsoft SQL Server (SMSQL) are solutions that create snapshots of the Microsoft Exchange Server and Microsoft SQL Server data on the NetApp storage system.

Data Protector supports SME and SMSQL through the `omnisnapmgr.pl` script, enabling you to archive existing NetApp SnapManager snapshots to Data Protector backup media. The `omnisnapmgr.pl` script uses the NetApp SnapDrive command line interface to perform queries, mount, and dismount volumes.

To back up SME and SMSQL snapshots to Data Protector backup media, you must create a standard Data Protector filesystem backup specification and specify the `omnisnapmgr.pl` script as a pre-and post-exec script to this backup specification.

At the start of the backup session (in the pre-exec phase), `omnisnapmgr` mounts the latest SME or SMSQL snapshots that were not archived yet, to the Windows client on which it runs. The Data Protector Disk Agent will then perform the backup of the files from the mounted volumes to the Data Protector backup device(s). At the end of the backup session (in the post-exec phase), `omnisnapmgr.pl` will dismount volumes that were mounted at the start of the backup session.

Installation

Prerequisites

- The system on which you will install the Data Protector SnapManager solution (the backup system) must have the Data Protector Disk Agent installed and must be a member of a Data Protector cell.
The Data Protector Disk Agent must be installed before the Data Protector NetApp SnapManager package, because the package must be installed in specific Data Protector directories.
- At least one Data Protector backup device must be configured in the Data Protector cell.
- NetApp SnapDrive must be installed and configured on the backup system.

Installation

To install the Data Protector NetApp SnapManager solution on the backup system:

1. Install the Data Protector Disk Agent.
2. Extract the `NetAppPackage.zip` archive to a temporary directory.
3. Copy the `omnisnapmgr.pl` script to `Data_Protector_home\bin`.
4. Rename the file `Data_Protector_home\bin\vbda.exe` to `Data_Protector_home\bin\vbda.exe.backup`.
5. Copy the following file to the directory `Data_Protector_home\bin`:

32-bit Windows Server systems: `vbda611_32bit.exe`

64-bit Windows Server systems: `vbda611_64bit.exe`

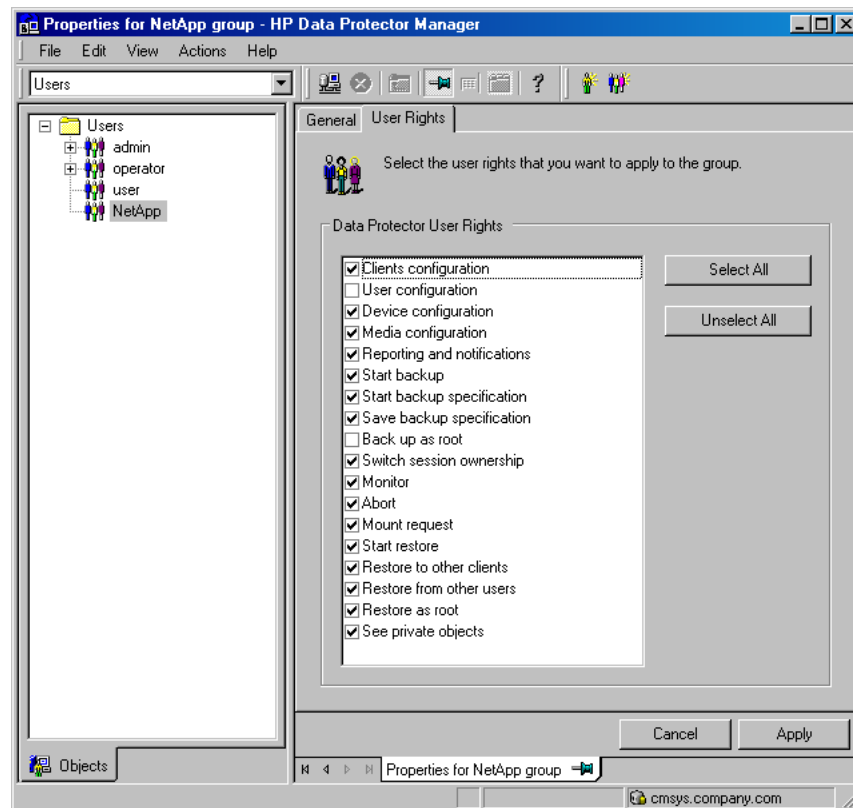
Rename `vbda611_32bit.exe` or `vbda611_64bit.exe` to `vbda.exe`.

Configuration

If the Data Protector Inet on the backup system does *not* run under the SnapDrive account, you can:

- Change the Data Protector's Inet account to that of SnapDrive. See the online Help index: "Inet, changing account".
- Configure the SnapDrive account for use with Data Protector:
 1. Create a new Data Protector user group with sufficient rights for the backup and remove the right Backup as root:

Figure 38 Setting the user rights for the new user group



2. Add the SnapDrive account to this group or, if the SnapDrive account is already in the Data Protector user list, move it to the newly created group.

Backup

Limitations

- You must back up SME and SMSQL snapshots in separate backup specifications.

Creating a backup specification

To create a NetApp SnapManager backup specification:

1. Create a filesystem backup specification for the Windows client to which Data Protector will mount the SnapManager snapshots. See the online Help index: “creating, backup specifications”.

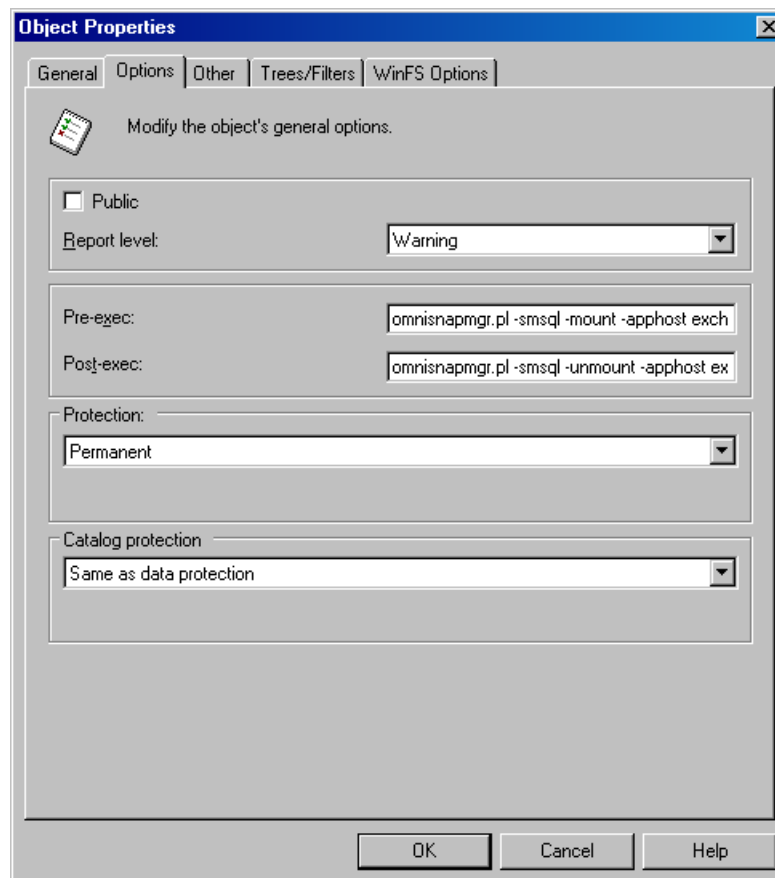
In the Source Property page, select the folder to which the Data Protector `omnisnapmgr` script will mount the volumes. This folder and all volumes mounted under it will be backed up.

NOTE: Data Protector excludes some temporary folders from being backed up, even if they are selected in the backup specification. You must select a folder that is not an operating system temporary folder or a Data Protector temporary folder or its sub folder, such as `C:\Windows\Temp` or `Data_Protector_home\tmp`. For a list of excluded folders, see the online Help index: “Windows, systems backup”.

2. Specify the `omnisnapmgr.pl` pre- and post-exec scripts:
 1. Under **Filesystem** options, click **Advanced**.
 2. In the Options pane, enter the **Pre-exec** and **Post-exec** scripts.

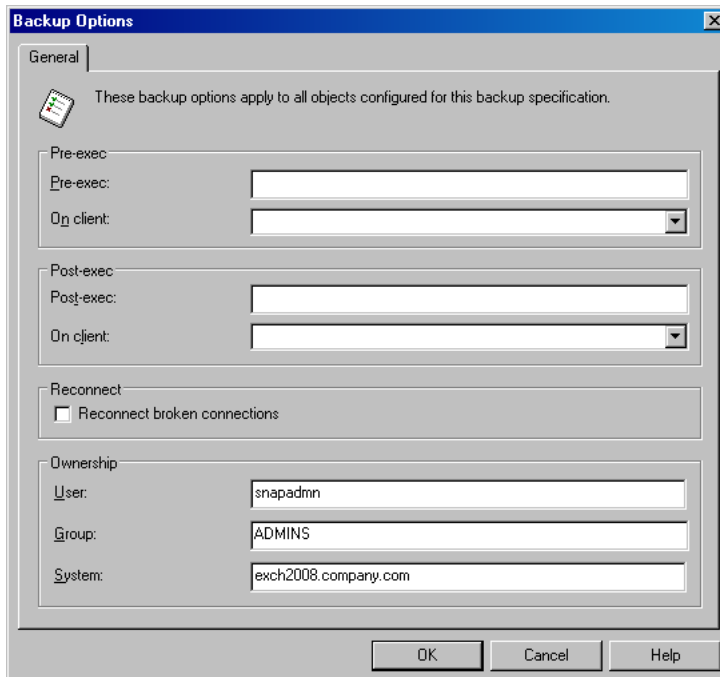
For the `omnisnapmgr.pl` syntax, available options, and examples, see the “[omnisnapmgr.pl reference page](#)” (page 78).

Figure 39 Specifying the pre- and post-exec commands



3. If the Data Protector Inet account is not running under the SnapDrive account, specify the SnapDrive account as the backup owner:
 - a. Under **Filesystem** options, click **Advanced**.
 - b. In the Backup options window, under Ownership, enter the user name, group, and the client system name.

Figure 40 Specifying the SnapDrive account



4. Save the backup specification and run or schedule the backup session.
See the online Help index: "scheduled backups".

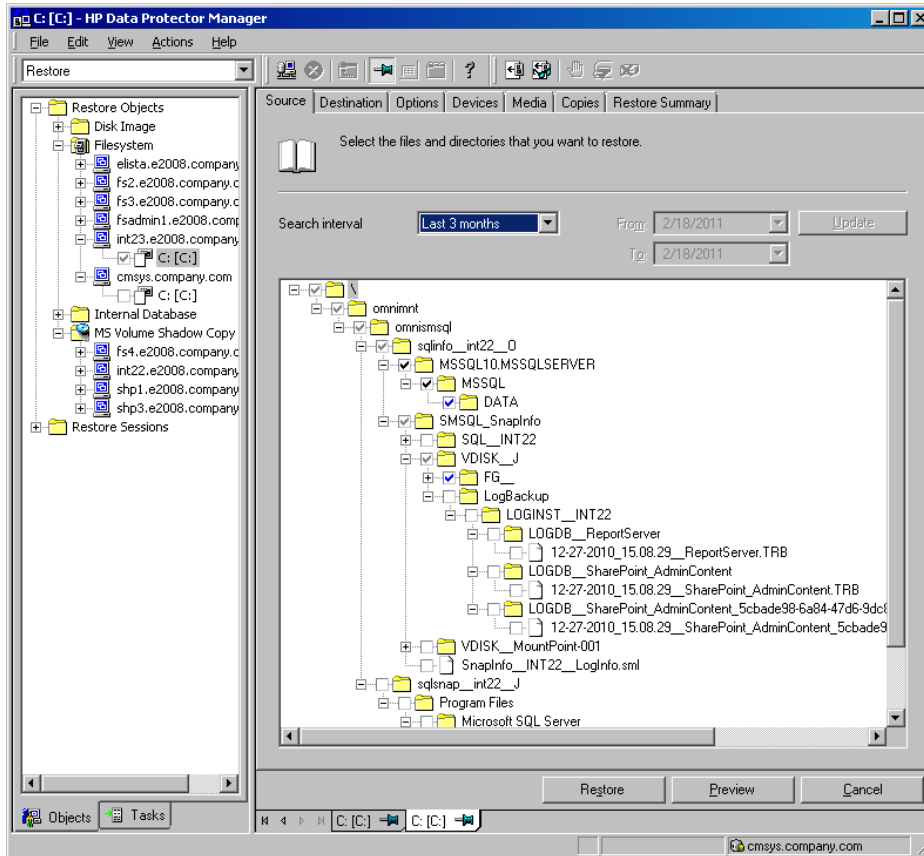
Restore

To restore SME or SMSQL data, use Data Protector and SnapManager:

1. Restore the database files and log files from Data Protector backup media to a temporary directory using the standard Data Protector restore procedure. See the online Help index: “restoring”.

For an example of the backed up SMSQL objects, see “Selecting the backed up the NetApp SnapManager objects for restore” (page 76).

Figure 41 Selecting the backed up the NetApp SnapManager objects for restore



NOTE: In case of a disaster, when your application installation is lost, you need to restore or reinstall the application to the original location first and then use the SnapManager Recovery Wizard to recover the application data.

- Use the SnapManager Recovery Wizard to recover the Microsoft Exchange Server or Microsoft SQL Server data. Select **Restore from unmanaged media** and follow the instructions. For information, see the SnapManager documentation.

Figure 42 Selecting the restore mode in SnapManager Restore Wizard

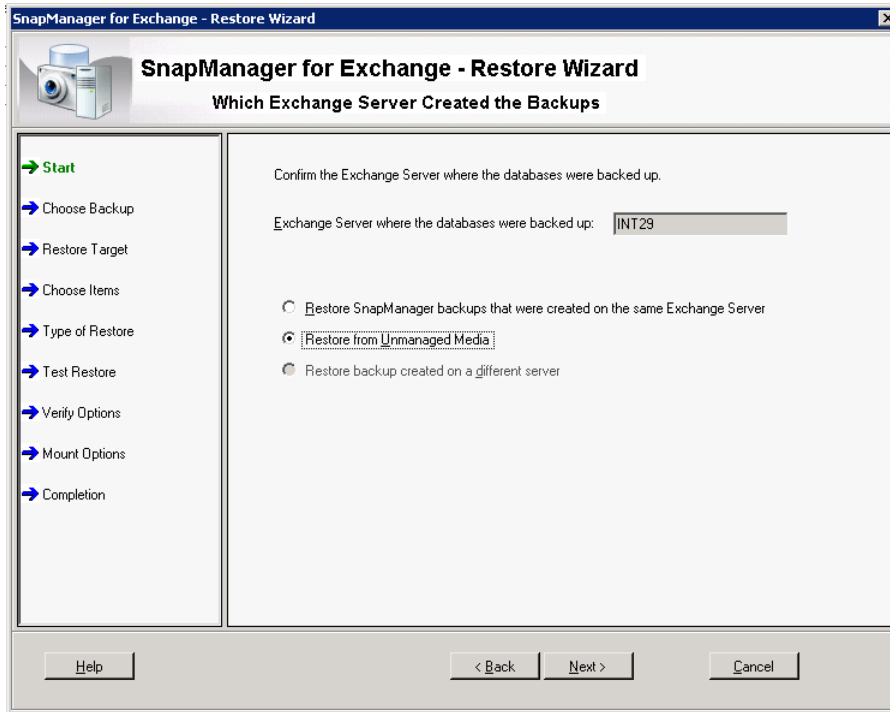
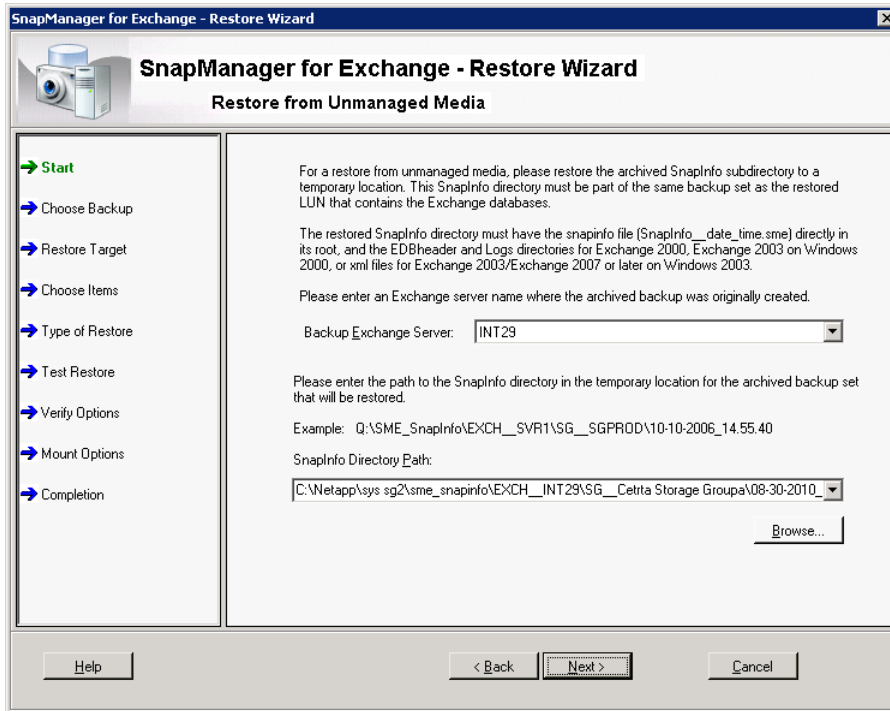


Figure 43 Specifying SnapManager Restore Wizard options



omnisnapmgr.pl reference page

SYNOPSIS

```
omnisnapmgr.pl -version | -help
omnisnapmgr.pl [-sme | -smsql] {-mount | -unmount} -apphost ClientName
[-force] [-partial] [-preview]
omnisnapmgr.pl -query
```

DESCRIPTION

The `omnisnapmgr.pl` script is used to mount or dismount the SME or SMSQL snapshots (when started as a pre- or post-exec script) or query NetApp snapshots (when run from a Command Prompt window).

OPTIONS

<code>-version</code>	Displays the Data Protector version.
<code>-help</code>	Displays the usage synopsis.
<code>-sme</code>	Specifies that SME snapshots will be backed up. If not specified, <code>omnisnapmgr</code> assumes by default that SME is backed up.
<code>-smsql</code>	Specifies that SMSQL snapshot will be backed up.
<code>-mount</code>	Mounts all volumes from the last SnapManager backup of the application system.
<code>-unmount</code>	Dismounts all volumes mounted by the <code>-mount</code> option
<code>-apphost <i>ClientName</i></code>	Specifies the application server (Exchange or SQL Server) system. If not specified, the local system is used.
<code>-force</code>	Performs a backup of the snapshots even if they were already backed up.
<code>-partial</code>	Performs a backup the SME or SMSQL snapshot even if some of the volumes cannot be mounted.
<code>-preview</code>	Displays the SnapDrive mount commands without executing them.
<code>-query</code>	Lists the snapshots and volumes contained in the last SME/SMSQL backup session.

NOTES

The `omnisnapmgr.pl` script is available on Windows systems only.

EXAMPLES

1. To back up to a SnapManager Microsoft Exchange Server snapshot to Data Protector backup media, where Microsoft Exchange Server is running on the client "exch1.company.com", specify the following two pre- and post-exec commands:

Pre-exec:

```
perl omnisnapmgr.pl -sme -mount -apphost exch1.company.com
```

Post-exec:

```
perl omnisnapmgr.pl -sme -unmount -apphost exch1.company.com
```

2. To back up a SnapManager Microsoft SQL snapshot Data Protector backup media, where Microsoft SQL Server is running on the client "sql2.company.com", even if the snapshots were backed up and to ensure that the backup is performed even if some volumes cannot be mounted, specify the following pre- and post-exec commands:

Pre-exec:

```
perl omnisnapmgr.pl -smsql -mount -apphost sql2.company.com
```

Post-exec:

```
perl omnisnapmgr.pl -smsql -unmount -apphost sql2.company.com \  
-force -partial
```

Glossary

A

access rights	See user rights.
ACSLs	<i>(StorageTek specific term)</i> The Automated Cartridge System Library Server (ACSLs) software that manages the Automated Cartridge System (ACS).
Active Directory	<i>(Windows specific term)</i> 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	<i>(ADIC/GRAU specific term)</i> Automated Mixed-Media library.
AMU	<i>(ADIC/GRAU specific term)</i> Archive Management Unit.
application agent	A component needed on a client to back up or restore online database integrations. See also Disk Agent.
application system	<i>(ZDB specific term)</i> A system the application or database runs on. The application or database data is located on source volumes. See also backup system and source volume.
archive logging	<i>(Lotus Domino Server specific term)</i> Lotus Domino Server database mode where transaction log files are overwritten only after they have been backed up.
archived redo log	<i>(Oracle specific term)</i> 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: <ul style="list-style-type: none">• ARCHIVELOG - The filled online redo log files are archived before they are reused. The database can be recovered if an instance or a disk fails. A "hot" backup can be performed only when the database is running in this mode.• NOARCHIVELOG - The filled online redo log files are not archived. See also online redo log.
ASR set	A collection of files stored on several diskettes, required for proper reconfiguration of the replacement disk (disk partitioning and logical volume configuration) and automatic recovery of the original system configuration and user data that was backed up during the full client backup. These files are stored as an ASR archive file on the Cell Manager in the directory <code>Data_Protector_program_data\Config\Server\dr\asr</code> (Windows Server 2008), <code>Data_Protector_home\Config\Server\dr\asr</code> (other Windows systems), or <code>/etc/opt/omni/server/dr/asr</code> (UNIX systems) as well as on the backup medium. After a disaster occurs, the ASR archive file is extracted to diskettes which you need to perform ASR.
audit logs	Data files to which auditing information is stored.
audit report	User-readable output of auditing information created from data stored in audit log files.
auditing information	Data about every backup session that was performed over an extended, user-defined period for the whole Data Protector cell.
autochanger	See library.
autoloader	See library.
Automatic Storage Management (ASM)	<i>(Oracle specific term)</i> A filesystem and volume manager integrated into Oracle which manages Oracle database files. It eliminates complexity associated with data and disk management and optimizes performance by providing striping and mirroring capabilities.

automigration	<i>(VLS specific term)</i> 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.
auxiliary disk	A bootable disk that has a minimal operating system with networking and Data Protector Disk Agent installed. It can be carried around and used to boot the target system in Phase 1 of Disk Delivery Disaster Recovery of UNIX clients.
B	
BACKINT	<i>(SAP R/3 specific term)</i> 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: <ul style="list-style-type: none"> • 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. The result of a backup session is a set of media, which was written to, also called the backup or media set. See also backup specification, full backup, and incremental backup.
backup set	A complete set of integration objects associated with a backup.
backup set	<i>(Oracle specific term)</i> 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	<p>(ZDB specific term) A system connected to a disk array together with one or multiple application systems. The backup system is typically connected to a disk array to create target volumes (a replica) and is used for mounting the target volumes (the replica). See also application system, target volume, and replica.</p>
backup types	See incremental backup, differential backup, transaction backup, full backup, and delta backup.
backup view	<p>Data Protector provides different views for backup specifications:</p> <p>By Type - according to the type of data available for backups/templates. Default view.</p> <p>By Group - according to the group to which backup specifications/templates belong.</p> <p>By Name - according to the name of backup specifications/templates.</p> <p>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.</p>
BC	<p>(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.</p>
BC Process	<p>(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.</p>
BCV	<p>(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.</p>
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	<p>(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.</p>
BRBACKUP	<p>(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.</p>
BRRESTORE	<p>(SAP R/3 specific term) An SAP R/3 tool that can be used to restore files of the following type:</p> <ul style="list-style-type: none">• 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 <p>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.</p>
BSM	The Data Protector Backup Session Manager controls the backup session. This process always runs on the Cell Manager system.

C

CAP	<p>(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.</p>
catalog protection	<p>Defines how long information about backed up data (such as file names and file versions) is kept in the IDB. See also data protection.</p>
CDB	<p>The Catalog Database is a part of the IDB that contains information about backup, restore, object copy, object consolidation, object verification, and media management sessions. 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.</p>
CDF file	<p>(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.</p>
cell	<p>A set of systems that are under the control of a Cell Manager. The cell typically represents the systems on a site or an organizational entity, which are connected to the same LAN or SAN. Central control is available to administer the backup and restore policies and tasks.</p>
Cell Manager	<p>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.</p>
centralized licensing	<p>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.</p>
Centralized Media Management Database (CMMDB)	<p>See CMMDB.</p>
Certificate Server	<p>A Windows Certificate Server can be installed and configured to provide certificates for clients. It provides customizable services for issuing and managing certificates for the enterprise. These services issue, revoke, and manage certificates employed in public key-based cryptography technologies.</p>
Change Journal	<p>(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.</p>
Change Log Provider	<p>(Windows specific term) A module that can be queried to determine which objects on a filesystem have been created, modified, or deleted.</p>
channel	<p>(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:</p> <ul style="list-style-type: none">• type 'disk'• type 'sbt_tape' <p>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.</p>
circular logging	<p>(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.</p>
client backup	<p>A backup of all volumes (filesystems) mounted on a Data Protector client. What is actually backed up depends on how you select objects in a backup specification:</p> <ul style="list-style-type: none">• If you select the check box next to the client system name, a single backup object of the Client System type is created. As a result, at the time of the backup, Data Protector first

detects all volumes that are mounted on the selected client and then backs them up. On Windows clients, CONFIGURATION is also backed up.

- If you individually select all volumes that are mounted on the client system, a separate backup object of the Filesystem type is created for each volume. As a result, at the time of the backup, only the selected volumes are backed up. Volumes that have been potentially mounted on the client after the backup specification was created are not backed up.

client or client system

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

cluster continuous replication

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

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

See also Exchange Replication Service and local continuous replication.

cluster-aware application

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

CMD script for Informix Server

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

CMMDB

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

See also MoM.

COM+ Class Registration Database

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

command device

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

Command 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).

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.

concurrency

See Disk Agent concurrency.

container

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

control file

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

copy set

(HP P6000 EVA Disk Array Family specific term) A pair that consists of the source volumes on a local P6000 EVA and their replica on a remote P6000 EVA.

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

CRS

The Cell Request Server process (service), which runs on the Data Protector Cell Manager, and starts and controls the backup and restore sessions. The service is started as soon as Data Protector

is installed on the Cell Manager. On Windows systems, the CRS runs under the account of the user specified at installation time. On UNIX systems, it runs under the account `root`.

CSM	The Data Protector Copy and Consolidation Session Manager process controls the object copy and object consolidation sessions and runs on the Cell Manager system.
D	
data file	<i>(Oracle and SAP R/3 specific term)</i> 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. <i>See also</i> catalog protection.
data replication (DR) group	<i>(HP P6000 EVA Disk Array Family specific term)</i> A logical grouping of HP P6000 EVA Disk Array Family virtual disks. It can contain up to eight copy sets provided they have common characteristics and share a common HP CA P6000 EVA log. <i>See also</i> copy set.
data stream	Sequence of data transferred over the communication channel.
Data_Protector_home	A reference to the directory containing Data Protector program files (on Windows Vista, Windows 7, and Windows Server 2008) or the directory containing Data Protector program files and data files (on other Windows operating systems). Its default path is <code>%ProgramFiles%\OmniBack</code> , but the path can be changed in the Data Protector Setup Wizard at installation time. <i>See also</i> Data_Protector_program_data.
Data_Protector_program_data	A reference to the directory containing Data Protector data files on Windows Vista, Windows 7, and Windows Server 2008. Its default path is <code>%ProgramData%\OmniBack</code> , but the path can be changed in the Data Protector Setup Wizard at installation time. <i>See also</i> Data_Protector_home.
database library	A Data Protector set of routines that enables data transfer between Data Protector and a server of an online database integration, for example, Oracle Server.
database parallelism	More than one database is backed up at a time if the number of available devices allows you to perform backups in parallel.
database server	A computer with a large database stored on it, such as the SAP R/3 or Microsoft SQL database. A server has a database that can be accessed by clients.
Dbobject	<i>(Informix Server specific term)</i> An Informix Server physical database object. It can be a blob space, dspace, 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 <code>dcbf</code> directory and is located on the Cell Manager in the directory <code>Data_Protector_program_data\db40</code> (Windows Server 2008), <code>Data_Protector_home\db40</code> (other Windows systems), or <code>/var/opt/omni/server/db40</code> (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 filesystem settings.
delta backup	A delta backup is a backup containing all the changes made to the database from the last backup of any type. <i>See also</i> 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	<i>(EMC Symmetrix specific term)</i> 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	<i>(Microsoft SQL Server specific term)</i> A database backup that records only the data changes made to the database after the last full database backup. See also backup types.
differential database backup	A differential database backup records only those data changes made to the database after the last full database backup.
directory junction	<i>(Windows specific term)</i> Directory junctions use the reparse point concept of Windows. An NTFS 5 directory junction allows you to redirect a directory/file request to another location.
disaster recovery	A process to restore a client's main system disk to a state close to the time when a (full) backup was performed.
disaster recovery operating system	See DR OS.
Disk Agent	A component needed on a client to back it up and restore it. The Disk Agent controls reading from and writing to a disk. During a backup session, the Disk Agent reads data from a disk and sends it to the Media Agent, which then moves it to the device. During a restore session the Disk Agent receives data from the Media Agent and writes it to the disk. During an object verification session the Disk Agent receives data from the Media Agent and performs the verification process, but no data is written to disk.
Disk Agent concurrency	The number of Disk Agents that are allowed to send data to one Media Agent concurrently.
disk group	<i>(Veritas Volume Manager specific term)</i> 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	An operating system environment in which disaster recovery runs. It provides Data Protector with a basic runtime environment (disk, network, tape, and filesystem access). It has to be installed on disk or loaded into memory and configured before the Data Protector disaster recovery can be performed. DR OS can be either temporary or active. A temporary DR OS is used exclusively as a host environment for some other operating system restore along with the target operating system configuration data. It is deleted after the target system is restored to the original system configuration. An active DR OS not only hosts the Data Protector disaster recovery process but can also be a part of the restored system because it replaces its own configuration data with the original configuration data.
drive	A physical unit that receives data from a computer system and can write it onto a magnetic medium (typically a tape drive). It can also read the data from the medium and send it to the computer system.
drive index	A number that identifies the mechanical position of a drive inside a library device. This number is used by the robotic control to access a drive.
drive-based encryption	Data Protector drive-based encryption uses the encryption functionality of the drive. While performing the backup, the drive encrypts both the data and the meta-data that is written to the medium.

E

EMC Symmetrix Agent	A Data Protector software module that prepares the EMC Symmetrix environment for backup and restore operations.
emergency boot file	<i>(Informix Server specific term)</i> The Informix Server configuration file <code>ixbar.server_id</code> that resides in the directory <code>INFORMIXDIR/etc</code> (on Windows) or <code>INFORMIXDIR\etc</code> (on UNIX). <code>INFORMIXDIR</code> is the Informix Server home directory and <code>server_id</code> is the value of the <code>SERVENUM</code> configuration parameter. Each line of the emergency boot file corresponds to one backup object.
encrypted control communication	Data Protector secure communication between the clients in the Data Protector cell is based on Secure Socket Layer (SSL) that uses SSLv3 algorithms to encrypt control communication. Control communication in a Data Protector cell is all communication between Data Protector processes, except the data transfer from Disk Agent (and Integrations) to Media Agent, and the other way round.
encryption key	A 256-bit randomly generated number used by the Data Protector encryption algorithm to encode information during backups for which AES 256-bit software encryption or drive-based encryption has been specified. The same key is used for subsequent decryption of the information. Encryption keys for a Data Protector cell are stored in a central keystore on the Cell Manager.
encryption KeyID-StoreID	Combined identifier used by the Data Protector Key Management Server to identify and administer encryption keys used by Data Protector. <code>KeyID</code> identifies the key within the keystore. <code>StoreID</code> identifies the keystore on the Cell Manager. If Data Protector has been upgraded from an earlier version with encryption functionality, there may several <code>StoreIDs</code> used on the same Cell Manager.
enhanced incremental backup	Conventional incremental backup backs up files that have changed since a previous backup, but has certain limitations in detection of changes. Unlike conventional incremental backup, enhanced incremental backup reliably detects and backs up also renamed and moved files, as well as files with changes in attributes.
enterprise backup environment	Several cells can be grouped together and managed from a central cell. The enterprise backup environment includes all clients located in several Data Protector cells which are managed and administered from a central cell using the Manager-of-Managers concept. <i>See also MoM.</i>

Event Log (Data Protector Event Log)	A central repository of all Data Protector-related notifications. By default, all notifications are sent to the Event Log. The events are logged on the Cell Manager into the file <i>Data_Protector_program_data\log\server\Ob2EventLog.txt</i> (Windows Server 2008), <i>Data_Protector_home\log\server\Ob2EventLog.txt</i> (other Windows systems), or <i>/var/opt/omni/server/log/Ob2EventLog.txt</i> (UNIX systems). The Event Log is accessible only to users of the Data Protector Admin user group and to users who are granted the Data Protector Reporting and notifications user rights. You can view or delete all events in the Event Log.
Event Logs	<i>(Windows specific term)</i> 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	<i>(Microsoft Exchange Server specific term)</i> 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)	<i>(Microsoft Exchange Server specific term)</i> A database technology used as a storage system for information exchange in Microsoft Exchange Server.
F	
failover	Transferring of the most important cluster data, called group (on Windows) 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	<i>(HP P6000 EVA Disk Array Family specific term)</i> An operation that reverses the roles of source and destination in HP Continuous Access + Business Copy (CA+BC) P6000 EVA configurations. See also HP Continuous Access + Business Copy (CA+BC) P6000 EVA.
FC bridge	See Fibre Channel bridge.
Fibre Channel	An ANSI standard for high-speed computer interconnection. Using either optical or copper cables, it allows the high speed bi-directional transmission of large data files and can be deployed between sites kilometers apart. Fibre Channel connects nodes using three physical topologies: point-to-point, loop, and switched.
Fibre Channel bridge	A Fibre Channel bridge or multiplexer provides the ability to migrate existing parallel SCSI devices, like RAID arrays, solid state disks (SSD), and tape libraries to a Fibre Channel environment. On one side of the bridge or multiplexer there is a Fibre Channel interface while on the other side there are parallel SCSI ports. The bridge or multiplexer enables SCSI packets to be moved between the Fibre Channel and parallel SCSI devices.
file depot	A file containing the data from a backup to a file library device.
file jukebox device	A device residing on disk consisting of multiple slots used to store file media.
file library device	A device which resides on a disk emulating a library with several media, hence containing multiple files, referred to as file depots.
File Replication Service (FRS)	A Windows service that replicates the domain controller store logon scripts and group policies. FRS also enables replication of Distributed File System (DFS) shares between systems and allows any server to perform replication activity.
file tree walk	<i>(Windows specific term)</i> 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	<i>(HP P9000 XP Disk Array Family specific term)</i> A mirror of an internal disk (LDEV) of a disk array of the HP P9000 XP Disk Array Family which can be further mirrored itself, producing second-level mirrors. For Data Protector zero downtime backup and instant recovery purposes, only first-level mirrors can be used. See also primary volume and mirror unit (MU) number.
flash recovery area	<i>(Oracle specific term)</i> A directory, filesystem, or Automatic Storage Management (ASM) disk group managed by Oracle that serves as a centralized storage area for files related to backup, restore, and database recovery (recovery files). See also recovery files.
fnames.dat	The <code>fnames.dat</code> 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.

G

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 <code>Data_Protector_program_data\Config\Server\Options</code> (Windows Server 2008), <code>Data_Protector_home\Config\Server\Options</code> (other Windows systems), or <code>/etc/opt/omni/server/options</code> (HP-UX, Solaris, and Linux systems).
group	<i>(Microsoft Cluster Server specific term)</i> 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.

H

hard recovery	<i>(Microsoft Exchange Server specific term)</i> 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 <i>Data_Protector_program_data\Config\Server\holidays</i> (Windows Server 2008), <i>Data_Protector_home\Config\Server\holidays</i> (other Windows systems), or <i>/etc/opt/omni/server/Holidays</i> (UNIX systems).
hosting system	A working Data Protector client used for Disk Delivery Disaster Recovery with a Data Protector Disk Agent installed.
HP Business Copy (BC) P6000 EVA	<i>(HP P6000 EVA Disk Array Family specific term)</i> A local replication software solution that enables creation of point-in-time copies (replicas) of the source volumes using the snapshot and clone capabilities of the P6000 EVA firmware. See also replica, source volume, snapshot, and HP Continuous Access + Business Copy (CA+BC) P6000 EVA.
HP Business Copy (BC) P9000 XP	<i>(HP P9000 XP Disk Array Family specific term)</i> An HP P9000 XP Disk Array Family configuration that enables creation and maintenance of internal copies of LDEVs for various purposes, such as data duplication and backup. The copies (secondary volumes or S-VOLs) can be separated from the primary volumes (P-VOLs) and connected to a different system. For Data Protector zero downtime backup purposes, P-VOLs should be available to the application system, and one of the S-VOL sets should be available to the backup system. See also LDEV, HP Continuous Access (CA) P9000 XP, Main Control Unit, application system, and backup system.
HP Command View (CV) EVA	<i>(HP P6000 EVA Disk Array Family specific term)</i> The user interface that enables you to configure, manage, and monitor your P6000 EVA storage system. It is used to perform various storage management tasks, for example, creating virtual disk families, managing storage system hardware, and creating snapshots, snapclones, and mirrorclones of virtual disks. The HP Command View EVA software runs on the HP Storage Management Appliance, and is accessed by a Web browser. See also HP StorageWorks P6000 EVA SMI-S Agent and HP StorageWorks SMI-S P6000 EVA Array provider.
HP Continuous Access (CA) P9000 XP	<i>(HP P9000 XP Disk Array Family specific term)</i> An HP P9000 XP Disk Array Family configuration that enables creation and maintenance of remote copies of LDEVs for purposes such as data duplication, backup, and disaster recovery. HP CA P9000 XP operations involve main (primary) disk array units and remote (secondary) disk array units. The main disk array units are connected to the application system and contain primary volumes (P-VOLs), which store original data. The remote disk array units are connected to the backup system and contain secondary volumes (S-VOLs). See also HP Business Copy (BC) P9000 XP, Main Control Unit, and LDEV.
HP Continuous Access + Business Copy (CA+BC) P6000 EVA	<i>(HP P6000 EVA Disk Array Family specific term)</i> An HP P6000 EVA Disk Array Family configuration that enables creation and maintenance of copies (replicas) of the source volumes on a remote P6000 EVA, and later use of these copies as the source for local replication on this remote array. See also HP Business Copy (BC) P6000 EVA, replica, and source volume.
HP SMI-S P6000 EVA Array provider	An interface used for controlling HP P6000 EVA Disk Array Family. SMI-S P6000 EVA Array provider runs as a separate service on the HP Storage Management Appliance system and acts as a gateway between incoming requests and HP Command View EVA. With the Data Protector HP P6000 EVA Disk Array Family integration, SMI-S P6000 EVA Array provider accepts standardized requests from the P6000 EVA SMI-S Agent, communicates with HP Command View EVA for information or method invocation, and returns standardized responses. See also HP StorageWorks P6000 EVA SMI-S Agent and HP Command View (CV) EVA.
HP StorageWorks P6000 EVA SMI-S Agent	A Data Protector software module that executes all tasks required for the HP P6000 EVA Disk Array Family integration. With the P6000 EVA SMI-S Agent, the control over the array is established through HP SMI-S P6000 EVA Array provider, which directs communication between incoming requests and HP CV EVA.

See also HP Command View (CV) EVA and HP SMI-S P6000 EVA Array provider.

HP StorageWorks P9000 XP Agent

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

HP 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/Operations, 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.

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. IDB is an embedded database located on the Cell Manager and keeps information regarding which data was backed up, to which media it was backed up, how backup, restore, and other sessions were run, which devices, libraries, and disk arrays are configured, and so on.

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 (re)-establish

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

incremental backup

A backup that selects only files that have changed since a previous backup. Several levels of incremental backup are available, which enables detailed control of restore chain length.
See also backup types.

incremental backup

(Microsoft Exchange Server specific term) A backup of the Microsoft Exchange Server data that has changed since the last full or incremental backup. With the incremental backup, only the transaction log files are backed up.
See also backup types.

incremental mailbox backup

An incremental mailbox backup backs up all the changes made to the mailbox after the last backup of any type.

incremental restore

(EMC Symmetrix specific term) A BCV or SRDF control operation. In BCV control operations, an incremental restore reassigns a BCV device as the next available mirror of the standard device in the pair. However, the standard devices are updated with only the data that was written to the BCV device during the time of the original pair split, and the data that was written to the standard device during the split is overwritten with data from the BCV mirror. In SRDF control operations, an incremental restore reassigns a target (R2) device as the next available mirror of the source (R1) device in the pair. However, the source (R1) devices are updated with only the data that was written to the target (R2) device during the time of the original pair split, and the

data that was written to the source (R1) device during the split is overwritten with data from the target (R2) mirror.

- incremental ZDB** A filesystem ZDB-to-tape or ZDB-to-disk+tape session in which only changes from the last protected full or incremental backup are streamed to tape.
See also full ZDB.
- incremental 1 mailbox backup** An incremental 1 mailbox backup backs up all the changes made to the mailbox after the last full backup.
- Inet** A process that runs on each UNIX system or service that runs on each Windows system in the Data Protector cell. It is responsible for communication between systems in the cell and for starting other processes needed for backup and restore. The Inet service is started as soon as Data Protector is installed on a system. The Inet process is started by the inetd daemon.
- Information Store** (*Microsoft Exchange Server specific term*) The Microsoft Exchange Server service that is responsible for storage management. Information Store in Microsoft Exchange Server manages two kinds of stores: mailbox stores and public folder stores. A mailbox store consists of mailboxes that belong to individual users. A public folder store contains public folders and messages that are shared among several users.
See also Key Management Service and Site Replication Service.
- Informix Server initializing** (*Informix Server specific term*) Refers to Informix Dynamic Server.
See formatting.
- Installation Server** A computer system that holds a repository of the Data Protector installation packages for a specific architecture. The Installation Server is used for remote installation of Data Protector clients. In mixed environments at least two Installation Servers are needed: one for UNIX systems and one for Windows systems.
- instant recovery** (*ZDB specific term*) A process in which a replica, produced by a ZDB-to-disk or a ZDB-to-disk+tape session, is used to restore the contents of the source volumes to their states at the time at which the replica was created, avoiding the need to perform a restore from tape. Depending on the application or database concerned, this may be all that is required, or other steps, such as the application of transaction log files, may be required for full recovery.
See also replica, zero downtime backup (ZDB), ZDB to disk, and ZDB to disk+tape.
- integration object** A backup object of a Data Protector integration, such as Oracle or SAP DB.
- Internet Information Services (IIS)** (*Windows specific term*) Microsoft Internet Information Services is a network file and application server that supports multiple protocols. Primarily, IIS transmits information in Hypertext Markup Language (HTML) pages by using the Hypertext Transport Protocol (HTTP).
- ISQL** (*Sybase specific term*) A Sybase utility used to perform system administration tasks on Sybase SQL Server.

J

- Java GUI Client** The Java GUI Client is a component of the Java GUI that contains only user interface related functionalities (the Cell Manager graphical user interface and the Manager-of-Managers (MoM) graphical user interface) 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".

K

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

keychain	A tool that eliminates the supply of a passphrase manually when decrypting the private key. It needs to be installed and configured on the Installation Server if you perform remote installation using secure shell.
keystore	All encryption keys are centrally stored in the keystore on the Cell Manager and administered by the Key Management Server (KMS).
KMS	Key Management Server (KMS) is a centralized service that runs on the Cell Manager and provides key management for the Data Protector encryption functionality. The service is started as soon as Data Protector is installed on the Cell Manager.
L	
LBO	<i>(EMC Symmetrix specific term)</i> A Logical Backup Object (LBO) is an object of data storage/retrieval in the EMC Symmetrix environment. It is stored/retrieved by EMC Symmetrix as one entity and can only be restored as a whole.
LDEV	<i>(HP P9000 XP Disk Array Family specific term)</i> A logical partition of a physical disk of a disk array of the HP P9000 XP Disk Array Family. An LDEV is the entity that can be replicated using the split-mirror or snapshot functionality of such disk array. See also HP Business Copy (BC) P9000 XP, HP Continuous Access (CA) P9000 XP, and replica.
library	Also called autochanger, jukebox, autoloader, or exchanger. A library contains media in repository slots. Each slot holds one medium (for example, DDS/DAT). Media are moved between slots and drives by a robotic mechanism, allowing random access to media. The library can contain multiple drives.
lights-out operation or unattended operation	A backup or restore operation that takes place outside of normal business hours without an operator. This implies that no operator personnel is present to work with the backup application or service mount requests, for example.
LISTENER.ORA	<i>(Oracle specific term)</i> 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	<i>(Microsoft Exchange Server specific term)</i> 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.
- ## M
- Magic Packet** See Wake ONLAN.
- mailbox** (*Microsoft Exchange Server specific term*) The location to which e-mail is delivered, which is set up by the administrator for each user. If a set of personal folders is designated as the e-mail delivery location, e-mail is routed from the mailbox to this location.
- mailbox store** (*Microsoft Exchange Server specific term*) A part of the Information Store that maintains information in user mailboxes. A mailbox store consists of a binary rich-text `.edb` file and a streaming native internet content `.stm` file.
- Main Control Unit (MCU)** (*HP P9000 XP Disk Array Family specific term*) An HP P9000 XP Disk Array Family unit that contains primary volumes (P-VOLs) for the HP CA P9000 XP or HP CA+BC P9000 XP configuration and acts as a master device. See also HP Business Copy (BC) P9000 XP, HP Continuous Access (CA) P9000 XP, and LDEV.

make_net_recovery	make_net_recovery is an Ignite-UX command, which allows you to create a recovery archive over the network onto the Ignite-UX server or any other specified system. The target system can be recovered across subnets after booting either from a bootable tape created by the Ignite-UX make_boot_tape command or the system boots directly from the Ignite-UX server. Booting directly from the Ignite-UX server can be automated with the Ignite-UX bootsys command or interactively specified on the boot console.
make_tape_recovery	make_tape_recovery is a command on Ignite-UX which creates a bootable recovery (installation) tape, customized for your system and enables you unattended disaster recovery by connecting the backup device directly to the target system and booting the target system from the bootable recovery tape. The backup device has to be locally connected to the client during the creation of the archive and recovery of the client.
Manager-of-Managers (MoM)	See MoM.
MAPI	(<i>Microsoft Exchange Server specific term</i>) The MAPI (Messaging Application Programming Interface) is the programming interface that lets applications and messaging clients interact with messaging and information systems.
MCU	See Main Control Unit (MCU).
Media Agent	A process that controls reading from and writing to a device, which reads from or writes to a medium (typically a tape). During a backup session, a Media Agent receives data from the Disk Agent and sends it to the device for writing it to the medium. During a restore or object verification session, a Media Agent locates data on the backup medium and sends it to the Disk Agent for processing. For a restore session, the Disk Agent then writes the data to the disk. A Media Agent also manages the robotics control of a library.
media allocation policy	Determines in which sequence media are used for backup. The Strict allocation policy directs Data Protector to prompt for a specific medium. The Loose policy directs Data Protector to prompt for any suitable medium. The Formatted First policy directs Data Protector to give preference to unknown media, even if unprotected media are available in the library.
media condition	The quality of a medium as derived from the media condition factors. Heavy usage and age result in an increased number of read and write errors with tape media. Media need to be replaced when they are marked as POOR.
media condition factors	The user-assigned age threshold and overwrite threshold used to determine the state of a medium.
media label	A user-defined identifier used to describe a medium.
media location	A user-defined physical location of a medium, such as "building 4" or "off-site storage".
media management session	A session performing some action on a medium, such as initializing, scanning the content, verifying data on a medium, or copying a medium.
media pool	A set of media of the same type (such as DDS) used and tracked as a group. Media are formatted and assigned to a media pool.
media set	The result of a backup session is data backed up on a group of media called media set. Depending on the media usage policy, several sessions can share the same media.
media type	The physical type of media, such as DDS or DLT.
media usage policy	The media usage policy controls how new backups are added to the already used media. It can be Appendable, Non-Appendable, or Appendable for incrementals only.
medium ID	A unique identifier assigned to a medium by Data Protector.
merging	This defines one mode to resolve file conflicts during restore. If the file to be restored already exists at the destination, the one with the more recent modification date is kept. Files not present on the disk are always restored. See also overwrite.
Microsoft Exchange Server	A "client-server" messaging and a workgroup system that offers a transparent connection to many different communication systems. It provides users with an electronic mail system, individual and group scheduling, online forms, and workflow automation tools. It provides a developer with a platform on which to build custom information-sharing and messaging-service applications.

Microsoft Management Console (MMC)	<i>(Windows specific term)</i> An administration model for Windows-based environments. It provides a simple, consistent, and integrated administration user interface allowing management of many applications through the same GUI, provided that the applications adhere to the MMC model.
Microsoft SQL Server	A database management system designed to meet the requirements of distributed "client-server" computing.
Microsoft Volume Shadow Copy Service (VSS)	A software service that provides a unified communication interface to coordinate backup and restore of a VSS-aware application regardless of its specific features. This service collaborates with the backup application, writers, shadow copy providers, and the operating system kernel to implement the management of volume shadow copies and shadow copy sets. See also shadow copy, shadow copy provider, replica, and writer.
mirror (EMC Symmetrix and HP P9000 XP Disk Array Family specific term)	See target volume.
mirror rotation (HP P9000 XP Disk Array Family specific term)	See replica set rotation.
mirror unit (MU) number	<i>(HP P9000 XP Disk Array Family specific term)</i> A non-negative integer number that determines a secondary volume (S-VOL) of an internal disk (LDEV) located on a disk array of the HP P9000 XP Disk Array Family. See also first-level mirror.
mirrorclone	<i>(HP P6000 EVA Disk Array Family specific term)</i> A dynamic replica of a storage volume, which is kept updated with changes made to the original storage volume via a local replication link. Replication between the original storage volume and its mirrorclone can be suspended. For each storage volume, a single mirrorclone can be created on the disk array.
MMD	The Media Management Daemon process (service) runs on the Data Protector Cell Manager and controls media management and device operations. The process is started when Data Protector is installed on the Cell Manager.
MMDB	The Media Management Database (MMDB) is a part of the IDB that contains information about media, media pools, devices, libraries, library drives, and slots configured in the cell, as well as the Data Protector media used for backup. In an enterprise backup environment, this part of the database can be common to all cells. See also CMMDB and CDB.
MoM	Several cells can be grouped together and managed from a central cell. The management system of the central cell is the Manager-of-Managers (MoM). The cells are called MoM clients. The MoM enables you to configure and manage multiple cells from a central point.
mount point	The access point in a directory structure for a disk or logical volume, for example /opt or ā : . On UNIX, the mount points are displayed using the bāf or āf command.
mount request	A screen prompt that tells you to insert a specific medium into a device. Once you respond to the mount request by providing the required medium and confirm the mount request, the session continues.
MSM	The Data Protector Media Session Manager, which runs on the Cell Manager and controls media sessions, such as copying media.
multisnapping	<i>(HP P6000 EVA Disk Array Family specific term)</i> Simultaneous creation of target volumes so that the backup data is consistent not only on each individual target volume, but also across all the volumes that constitute a snapshot. See also snapshot.
OBDR capable device	A device that can emulate a CD-ROM drive loaded with a bootable disk and can thus be used as a backup or boot device for disaster recovery purposes.
obdrindex.dat	See IDB recovery file.



object	See backup object.
object consolidation	The process of merging a restore chain of a backup object, consisting of a full backup and at least one incremental backup, into a new, consolidated version of this object. The process is a part of the synthetic backup procedure. The result is a synthetic full backup of the specified backup object.
object consolidation session	A process that merges a restore chain of a backup object, consisting of a full backup and at least one incremental backup, into a new, consolidated version of this object.
object copy	A copy of a specific object version that is created during an object copy session or a backup session with object mirroring.
object copy session	A process that creates an additional copy of the backed up data on a different media set. During an object copy session, the selected backed up objects are copied from the source to the target media.
object copying	The process of copying selected object versions to a specific media set. You can select object versions from one or several backup sessions to be copied.
object ID	<i>(Windows specific term)</i> The object IDs (OIDs) enable access to NTFS 5 files no matter where in the system the files reside. Data Protector treats the OIDs as alternate streams of the files.
object mirror	A copy of a backup object created using object mirroring. Object mirrors are often referred to as object copies.
object mirroring	The process of writing the same data to several media sets during a backup session. Data Protector enables you to mirror all or some backup objects to one or more media sets.
object verification	The process of verifying the data integrity of backup objects, from the Data Protector point of view, and the ability of Data Protector to deliver them to the required destination. The process can be used to provide a level of confidence in the ability to restore object versions created by backup, object copy, or object consolidation sessions.
object verification session	A process that verifies the data integrity of specified backup objects or object versions and the ability of selected Data Protector network components to deliver them to a specified host. Object verification sessions can be run interactively, or as specified in automated post-backup, or scheduled specifications.
offline backup	A backup during which an application database cannot be used by the application. In an offline backup session, the database is generally put into a quiescent state that allows use by the backup system, but not the application, for the time period of the data replication process. For instance, for backup to tape, until streaming of data to the tape is finished. Normal database operation is resumed before potential post-backup operations are started. See also zero downtime backup (ZDB) and online backup.
offline recovery	Offline recovery is performed if the Cell Manager is not accessible, for example, due to network problems. Only standalone and SCSI library devices can be used for offline recovery. Recovery of the Cell Manager is always offline.
offline redo log	See archived redo log.
ON-Bar	<i>(Informix Server specific term)</i> 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: <ul style="list-style-type: none"> • 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	<i>(Informix Server specific term)</i> 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 <i>INFORMIXDIR\etc</i> (on Windows) or <i>INFORMIXDIR/etc/</i> (on UNIX).

online backup	<p>A backup performed while a database application remains available for use. The database is placed into a special backup mode of operation for the time period of the data replication process. For instance, for backup to tape, until streaming of data to tape is finished. During this period, the database is fully operational, but there may be a small performance impact and log files may grow very quickly. Normal database operation is resumed before potential post-backup operations are started.</p> <p>In some cases, transaction logs may also have to be backed up to allow a consistent database to be restored.</p> <p>See also zero downtime backup (ZDB) and offline backup.</p>
online recovery	<p>Online recovery is performed when Cell Manager is accessible. In this case, most of the Data Protector] functionalities are available (Cell Manager runs the session, restore sessions are logged in the IDB, you can monitor the restore progress using the GUI, and so on).</p>
online redo log	<p>(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.</p> <p>See also archived redo log.</p>
Oracle Data Guard	<p>(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.</p>
Oracle instance	<p>(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.</p>
ORACLE_SID	<p>(Oracle specific term) A unique name for an Oracle Server instance. To switch among Oracle Servers, specify the desired <code>ORACLE_SID</code>. The <code>ORACLE_SID</code> is included in the <code>CONNECT DATA</code> parts of the connect descriptor in a <code>TNSNAMES.ORA</code> file and in the definition of the TNS listener in the <code>LISTENER.ORA</code> file.</p>
original system	<p>The system configuration backed up by Data Protector before a computer disaster hits the system.</p>
overwrite	<p>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.</p> <p>See also merging.</p>
ownership	<p>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.</p> <p>If a user starts an existing backup specification without modifying it, the backup session is not considered as interactive.</p> <p>If a modified backup specification is started by a user, the user is the owner unless the following is true:</p> <ul style="list-style-type: none"> • 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. <p>If a backup is scheduled on a UNIX Cell Manager, the session owner is root:sys unless the above conditions are true.</p> <p>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.</p> <p>When copying or consolidating objects, by default the owner is the user who starts the operation, unless a different owner is specified in the copy or consolidation specification.</p>

P

P1S file P1S file contains information on how to format and partition all disks installed in the system during Enhanced Automated Disaster Recovery (EADR). It is created during full backup and is saved on

	<p>backup medium and on Cell Manager into the directory <i>Data_Protector_program_data\Config\Server\dr\p1s</i> (Windows Server 2008), <i>Data_Protector_home\Config\Server\dr\p1s</i> (other Windows systems), or <i>/etc/opt/omni/server/dr/p1s</i> (UNIX systems) with the filename <i>recovery.p1s</i>.</p>
package	<p>(<i>MC/ServiceGuard and Veritas Cluster specific term</i>) A collection of resources (for example volume groups, application services, IP names, and addresses) that are needed to run a specific cluster-aware application.</p>
pair status	<p>(<i>HP P9000 XP Disk Array Family specific term</i>) The status of a disk pair (secondary volume and its corresponding primary volume) of a disk array of the HP P9000 XP Disk Array Family. Depending on the circumstances, the paired disks can be in various states. The following states are particularly important for the operation of the Data Protector HP StorageWorks P9000 XP Agent:</p> <ul style="list-style-type: none"> • PAIR – The secondary volume is prepared for zero downtime backup. If it is a mirror, it is completely synchronized, and if it is a volume to be used for snapshot storage, it is empty. • SUSPENDED – The link between the disks is suspended. However, the pair relationship is still maintained, and the secondary disk can be prepared for zero downtime backup again at a later time. • COPY – The disk pair is currently busy and making a transition into the PAIR state. If the secondary volume is a mirror, it is re-synchronizing with the primary volume, and if it is a volume to be used for snapshot storage, its contents are getting cleared.
parallel restore	<p>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.</p>
parallelism	<p>The concept of reading multiple data streams from an online database.</p>
phase 0 of disaster recovery	<p>Preparation for disaster recovery - the prerequisite condition for a successful disaster recovery.</p>
phase 1 of disaster recovery	<p>Installation and configuration of DR OS, establishing previous storage structure.</p>
phase 2 of disaster recovery	<p>Restoration of operating system (with all the configuration information that defines the environment) and Data Protector.</p>
phase 3 of disaster recovery	<p>Restoration of user and application data.</p>
physical device	<p>A physical unit that contains either a drive or a more complex unit such as a library.</p>
post-exec	<p>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. <i>See also</i> pre-exec.</p>
pre- and post-exec commands	<p>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.</p>
pre-exec	<p>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. <i>See also</i> post-exec.</p>
prealloc list	<p>A subset of media in a media pool that specifies the order in which media are used for backup.</p>
primary volume (P-VOL)	<p>(<i>HP P9000 XP Disk Array Family specific term</i>) An internal disk (LDEV) of a disk array of the HP P9000 XP Disk Array Family for which a secondary volume (S-VOL), either its mirror or a volume</p>

to be used for its snapshot storage, exists. In the HP CA P9000 XP and HP CA+BC P9000 XP configurations, primary volumes are located in the Main Control Unit (MCU).
See also secondary volume (S-VOL) and Main Control Unit (MCU).

protection

See data protection and also catalog protection.

public folder store

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

public/private backed up data

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

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

R

RAID

Redundant Array of Independent Disks.

RAID Manager Library

(*HP P9000 XP Disk Array Family specific term*) A software library that is used for accessing the configuration, status, and performance measurement data of a P9000 XP Array storage system, and for invoking operations on the disk array. It translates function calls into sequences of low-level SCSI commands.

See also HP StorageWorks P9000 XP Agent.

RAID Manager P9000 XP

(*HP P9000 XP Disk Array Family specific term*) A software application that provides a command-line interface to disk arrays of the HP P9000 XP Disk Array Family. It offers an extensive set of commands for reporting and controlling the status of a P9000 XP Array storage system, and for performing various operations on the disk array.

rawdisk backup

See disk image backup.

RCU

See Remote Control Unit (RCU).

RDBMS

Relational Database Management System.

RDF1/RDF2

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

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 specific files that reside in the flash recovery area: the current control file, online redo logs, archived redo logs, flashback logs, control file autobackups, datafile copies, and backup pieces.

See also flash recovery area.

Recovery Manager (RMAN)

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

RecoveryInfo	When backing up Windows configuration files, Data Protector collects the information about the current system configuration (information on disk layout, volume, and network configuration). This information is needed for disaster recovery.
recycle or unprotect	A process that removes the data protection from all backed up data on a medium, allowing Data Protector to overwrite it during one of the next backups. Data that belongs to the same session(s) but resides on other media is also unprotected. Recycling does not actually alter the data on the medium.
redo log	<i>(Oracle specific term)</i> 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)	<i>(HP P9000 XP Disk Array Family specific term)</i> An HP P9000 XP Disk Array Family unit that acts as a slave device to the Main Control Unit (MCU) in the HP CA P9000 XP or HP CA+BC P9000 XP configuration. In bidirectional configurations, the RCU can also act as an MCU.
Removable Storage Management Database	<i>(Windows specific term)</i> 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	<i>(Windows specific term)</i> 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	<i>(ZDB specific term)</i> 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	<i>(ZDB specific term)</i> A group of replicas, all created using the same backup specification. See also replica and replica set rotation.
replica set rotation	<i>(ZDB specific term)</i> 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	<i>(HP P9000 XP Disk Array Family VSS provider specific term)</i> One of two P9000 XP Array VSS hardware provider operation modes. When the P9000 XP Array provider is in the resync mode, the source volume (P-VOL) and its replica (S-VOL) are in the suspended mirror relationship after a backup. The maximum number of replicas (S-VOLs per a P-VOL) rotated is three provided that MU range is 0-2 or 0, 1, 2. Restore from a backup in such a configuration is possible only by re-synchronization of an S-VOL with its P-VOL. See also VSS compliant mode, source volume, primary volume (P-VOL), replica, secondary volume (S-VOL), mirror unit (MU) number, and replica set rotation.
RMAN (Oracle specific term)	See Recovery Manager.
RSM	The Data Protector Restore Session Manager controls restore and object verification sessions. This process always runs on the Cell Manager system.

RSM	<i>(Windows specific term)</i> Removable Storage Manager (RSM) includes a media management service that facilitates communication among applications, robotic changers, and media libraries. It enables multiple applications to share local robotic media libraries and tape or disk drives and to manage removable media.
S	
SAPDBA	<i>(SAP R/3 specific term)</i> An SAP R/3 user interface that integrates the BRBACKUP, BRARCHIVE, and BRRESTORE tools.
scanning	A function which identifies the media in a device. This synchronizes the MMDB with the media that are actually present at the selected locations (for example, slots in a library). It is useful to perform a scan and check the actual media in the device if someone has manually manipulated media without using Data Protector to eject or enter, for example.
Scheduler	A function that controls when and how often automatic backups occur. By setting up a schedule, you automate the start of backups.
secondary volume (S-VOL)	<i>(HP P9000 XP Disk Array Family specific term)</i> An internal disk (LDEV) of a disk array of the HP P9000 XP Disk Array Family which is paired with another LDEV: a primary volume (P-VOL). It can act as a mirror of the P-VOL or as a volume to be used for the P-VOL's snapshot storage. An S-VOL is assigned a SCSI address different from the one used for the P-VOL. In an HP CA P9000 XP configuration, the S-VOLs acting as mirrors can be used as failover devices in a MetroCluster configuration. See also primary volume (P-VOL) and Main Control Unit (MCU).
session	See backup session, media management session, and restore session.
session ID	An identifier of a backup, restore, object copy, object consolidation, object verification, or media management session, consisting of the date when the session ran and a unique number.
session key	This environment variable for the pre-exec and post-exec script is a Data Protector unique identification of any session, including preview sessions. The session key is not recorded in the database, and it is used for specifying options for the omnimnt, omnistat, and omniabort commands.
shadow copy	<i>(Microsoft VSS specific term)</i> 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	<i>(Microsoft VSS specific term)</i> 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	<i>(Microsoft VSS specific term)</i> 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.
Site Replication Service	<i>(Microsoft Exchange Server specific term)</i> The Microsoft Exchange Server 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.
smart copy	<i>(VLS specific term)</i> 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	<i>(VLS specific term)</i> 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.
SMB	See split mirror backup.
SMBF	The Session Messages Binary Files (SMBF) part of the IDB stores session messages generated during backup, restore, object copy, object consolidation, object verification, and media management sessions. One binary file is created per session. The files are grouped by year and month.
SMI-S Agent (SMISA)	See HP StorageWorks P6000 EVA SMI-S Agent.
snapshot	<i>(HP P6000 EVA Disk Array Family, HP P9000 XP Disk Array Family, and HP P4000 SAN Solutions specific term)</i> A type of target volumes created using a specific replication technology. Depending on the disk array model and the chosen replication technique, a range of snapshot types with different characteristics is available. Basically, each snapshot may be either a virtual copy, still reliant upon the contents of the source volume, or an independent duplicate (clone) of the source volume. See also replica and snapshot creation.
snapshot backup	See ZDB to tape, ZDB to disk, and ZDB to disk+tape.
snapshot creation	<i>(HP P6000 EVA Disk Array Family, HP P9000 XP Disk Array Family, and HP P4000 SAN Solutions specific term)</i> A replica creation process in which copies of the selected source volumes are created using storage virtualization technology. Such a replica is considered to be created at a particular point in time, and is immediately available for use. However, with certain snapshot types, a background data copying process continues to run on the disk array after the moment of the replica creation. See also snapshot.
source (R1) device	<i>(EMC Symmetrix specific term)</i> 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	<i>(ZDB specific term)</i> 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	<i>(EMC Symmetrix Disk Array and HP P9000 XP Disk Array Family specific term)</i> A type of target volumes created using a specific replication technology. A split-mirror replica provides independent duplicates (clones) of the source volumes. See also replica and split mirror creation.
split mirror backup (EMC Symmetrix specific term)	See ZDB to tape.
split mirror backup (HP P9000 XP Disk Array Family specific term)	See ZDB to tape, ZDB to disk, and ZDB to disk+tape.
split mirror creation	<i>(EMC Symmetrix and HP P9000 XP Disk Array Family specific term)</i> 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	<i>(EMC Symmetrix and HP P9000 XP Disk Array Family specific term)</i> A process in which data backed up in a ZDB-to-tape or a ZDB-to-disk+tape session is first copied from the backup media to a replica, and from the replica to the source volumes afterwards. Individual backup objects or complete sessions can be restored using this method. See also ZDB to tape, ZDB to disk+tape, and replica.

sqlhosts file or registry	<i>(Informix Server specific term)</i> 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	<i>(disaster recovery specific term)</i> A text file in the Unicode (UTF-16) format, generated during CONFIGURATION backup of a Windows or Linux system and stored on the Cell Manager. It contains system information required for installing and configuring the operating system on the target system in the case of a disaster. See also target system.
SRDF	<i>(EMC Symmetrix specific term)</i> The EMC Symmetrix Remote Data Facility is a business continuation process that enables effective, real-time data replication of SLDs between dislocated processing environments. These environments could be situated within the same root computer environment or separated by long distances.
SSE Agent (SSEA)	See HP StorageWorks P9000 XP Agent.
sst.conf file	The file <code>/usr/kernel/drv/sst.conf</code> 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 <code>/kernel/drv/st.conf</code> 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	<i>(Microsoft Exchange Server specific term)</i> A collection of mailbox stores and public folder stores that share a set of transaction log files. Exchange Server manages each storage group with a separate server process.
storage volume	<i>(ZDB specific term)</i> An object that may be presented to an operating system or some other entity (for example, a virtualization mechanism) upon which volume management systems, filesystems, or other objects may exist. The volume management systems, file systems are built on this storage. Typically, these can be created or exist within a storage system such as a disk array.
StorageTek ACS library	<i>(StorageTek specific term)</i> Automated Cartridge System is a library system (also known as Silo) consisting of one Library Management Unit (LMU) and one to 24 Library Storage Modules (LSM) connected to the unit.
switchover	See failover.
Sybase Backup Server API	<i>(Sybase specific term)</i> 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	<i>(Sybase specific term)</i> The server in the Sybase "client-server" architecture. Sybase SQL Server manages multiple databases and multiple users, keeps track of the actual location of data on disks, maintains mapping of logical data description to physical data storage, and maintains data and procedure caches in memory.
SYMA	See EMC Symmetrix Agent.
synthetic backup	A backup solution that produces a synthetic full backup, an equivalent to a conventional full backup in terms of data, without putting stress on the production servers or the network. A synthetic full backup is created from a previous full backup and any number of incremental backups.
synthetic full backup	The result of an object consolidation operation, where a restore chain of a backup objects is merged into a new, synthetic full version of this object. A synthetic full backup is equivalent to a conventional full backup in terms of restore speed.
System Backup to Tape	<i>(Oracle specific term)</i> 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	<i>(Sybase specific term)</i> The four system databases on a newly installed Sybase SQL Server are the: <ul style="list-style-type: none"> • master database (master) • temporary database (tempdb) • system procedure database (sybssystemprocs) • model database (model).
System Recovery Data file	See SRD file.
System State	<i>(Windows specific term)</i> 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	<i>(Windows specific term)</i> A shared directory that stores the server copy of the domain's public files, which are replicated among all domain controllers in the domain.
T	
tablespace	A part of a database structure. Each database is logically divided into one or more tablespaces. Each tablespace has data files or raw volumes exclusively associated with it.
tapeless backup (ZDB specific term)	See ZDB to disk.
target (R2) device	<i>(EMC Symmetrix specific term)</i> An EMC Symmetrix device that participates in SRDF operations with a source (R1) device. It resides in the remote EMC Symmetrix unit. It is paired with a source (R1) device in the local EMC Symmetrix unit and receives all write data from its mirrored pair. This device is not accessed by user applications during normal I/O operations. An R2 device must be assigned to an RDF2 group type. See also source (R1) device.
target database	<i>(Oracle specific term)</i> In RMAN, the target database is the database that you are backing up or restoring.
target system	<i>(disaster recovery specific term)</i> 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	<i>(ZDB specific term)</i> A storage volume to which data is replicated.
Terminal Services	<i>(Windows specific term)</i> 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	<i>(Microsoft SQL Server specific term)</i> 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	<i>(EMC Symmetrix specific term)</i> 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	<i>(Oracle and SAP R/3 specific term)</i> 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	<i>(Sybase and SQL specific term)</i> A backup of the transaction log providing a record of changes made since the last full or transaction backup.
transaction log backup	Transaction log backups generally use fewer resources than database backups so they can be created more frequently than database backups. By applying transaction log backups, you can recover the database to a specific point in time.
transaction log files	Files that record transactions of the database modifications, and provide fault tolerance in case of a database disaster.
transaction log table	<i>(Sybase specific term)</i> A system table in which all changes to the database are automatically recorded.
transaction logs	<i>(Data Protector specific term)</i> 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.
transportable snapshot	<i>(Microsoft VSS specific term)</i> 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	<i>(Novell NetWare specific term)</i> 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 <code>SYSDIR\SYSTEM\TSA</code> directory on the server where <code>TSANDS.NLM</code> is loaded.

U

UIProxy	The Java GUI Server (<code>UIProxy</code> 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, Windows 7, 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	<i>(Windows specific term)</i> Configuration information retained on a user basis. This information includes desktop settings, screen colors, network connections, and so on. When the user logs on, the user profile is loaded and the Windows environment is set accordingly.
user rights	User rights or access rights are the permissions needed to perform specific Data Protector tasks. Configuring a backup, starting a backup session, or starting a restore session are typical user rights. Users have the access rights of the user group to which they belong.

user_restrictions file	A file that restricts specific user actions, which are available to Data Protector user groups according to the user rights assigned to them, to be performed only on specific systems of the Data Protector cell. Such restrictions apply only to Data Protector user groups other than <i>admin</i> and <i>operator</i> .
V	
vaulting media	The process of storing media to a safe and remote place. The media are brought back to the data center when they are needed for restore or are ready for reuse in subsequent backups. The vaulting procedure depends on your company's backup strategy and policies for data protection/reliability.
verify	A function that lets you check whether the Data Protector data on a specified medium is readable. Additionally, consistency within each block can be checked if the backup was performed with the cyclic redundancy check (CRC) option ON.
Virtual Controller Software (VCS)	<i>(HP P6000 EVA Disk Array Family specific term)</i> The firmware that manages all aspects of storage system operation, including communication with HP Command View EVA through the HSV controllers. See also HP Command View (CV) EVA.
Virtual Device Interface	<i>(Microsoft SQL Server specific term)</i> This is a Microsoft SQL Server programming interface that allows fast backup and restore of large databases.
virtual disk	<i>(HP P6000 EVA Disk Array Family specific term)</i> A unit of storage allocated from a storage pool of a disk array of the HP P6000 EVA Disk Array Family. A virtual disk is the entity that can be replicated using the snapshot functionality of such disk array. See also source volume and target volume.
virtual full backup	An efficient type of synthetic backup where data is consolidated using pointers instead of being copied. It is performed if all the backups (the full backup, incremental backups, and the resulting virtual full backup) are written to a single file library that uses distributed file medium format.
Virtual Library System (VLS)	A disk-based data storage device hosting one or more virtual tape libraries (VTLs).
virtual server	A virtual machine in a cluster environment defined in a domain by a network IP name and address. Its address is cached by the cluster software and mapped to the cluster node that is currently running the virtual server resources. This way all requests for a particular virtual server are cached by a specific cluster node.
virtual tape	<i>(VLS specific term)</i> An archival storage technology that backs up data to disk drives in the same way as if it were being stored on tape. Benefits of virtual tape systems include improved backup and recovery speed and lower operating costs. See also Virtual Library System (VLS) and Virtual Tape Library (VTL).
Virtual Tape Library (VTL)	<i>(VLS specific term)</i> An emulated tape library that provides the functionality of traditional tape-based storage. See also Virtual Library System (VLS).
VMware management client	<i>(VMware (Legacy) integration specific term)</i> 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	<i>(ADIC and STK specific term)</i> A VOLume SERial number is a label on the medium to identify the physical tape used in very large libraries. A volser is a naming convention specific to ADIC/GRAU and StorageTek devices.
volume group	A unit of data storage in an LVM system. A volume group can consist of one or more physical volumes. There can be more than one volume group on the system.
volume mountpoint	<i>(Windows specific term)</i> An empty directory on a volume that can be used to mount another volume. The volume mount point acts as a gateway to the target volume. Provided that the volume is mounted, users and applications can refer to the data on the mounted volume by the full (merged) filesystem path as if both volumes are one integral part.
Volume Shadow Copy Service	See Microsoft Volume Shadow Copy Service (VSS).
VSS	See Microsoft Volume Shadow Copy Service (VSS).

VSS compliant mode	<i>(HP P9000 XP Disk Array Family VSS provider specific term)</i> One of two P9000 XP Array VSS hardware provider operation modes. When the P9000 XP Array provider is in the VSS compliant mode, the source volume (P-VOL) and its replica (S-VOL) are in simplex, unpaired state after a backup. Therefore the number of replicas (S-VOLs per a P-VOL) rotated is not limited. Restore from a backup in such a configuration is possible only by switching the disks. See also resync mode, source volume, primary volume (P-VOL), replica, secondary volume (S-VOL), and replica set rotation.
VxFS	Veritas Journal Filesystem.
VxVM (Veritas Volume Manager)	A Veritas Volume Manager is a system for managing disk space on Solaris platforms. A VxVM system consists of an arbitrary group of one or more physical volumes organized into logical disk groups.
W	
Wake ONLAN	Remote power-up support for systems running in power-save mode from some other system on the same LAN.
Web reporting	The Data Protector functionality that allows you to view reports on backup, object copy, and object consolidation status and Data Protector configuration using the Web interface.
wildcard character	A keyboard character that can be used to represent one or many characters. The asterisk (*), for example, typically represents one or more characters, and the question mark (?) typically represents a single character. Wildcard characters are often used in operating systems as a means of specifying more than one file by name.
Windows configuration backup	Data Protector allows you to back up Windows CONFIGURATION, including Windows Registry, user profiles, Event Logs, and WINS and DHCP server data (if configured on a system) in one step.
Windows Registry	A centralized database used by Windows to store configuration information for the operating system and the installed applications.
WINS server	A system running Windows Internet Name Service software that resolves Windows networking computer names to IP addresses. Data Protector can back up WINS server data as part of the Windows configuration.
writer	<i>(Microsoft VSS specific term)</i> A process that initiates change of data on the original volume. Writers are typically applications or system services that write persistent information on a volume. Writers also participate in the shadow copy synchronization process by assuring data consistency.
X	
XBSA interface	<i>(Informix Server specific term)</i> ON-Bar and Data Protector communicate with each other through the X/Open Backup Services Application Programmer's Interface (XBSA).
Z	
ZDB	See zero downtime backup (ZDB).
ZDB database	<i>(ZDB specific term)</i> A part of the IDB, storing ZDB-related information such as source volumes, replicas, and security information. The ZDB database is used in zero downtime backup, instant recovery, and split mirror restore sessions. See also zero downtime backup (ZDB).
ZDB to disk	<i>(ZDB specific term)</i> 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	<i>(ZDB specific term)</i> A form of zero downtime backup where the replica produced is kept on the disk array as a backup of the source volumes at a specific point in time, in the same way as with ZDB to disk. However, data in the replica is also streamed to a backup medium, as with ZDB to tape. If this backup method is used, data backed up in the same session can be restored using

the instant recovery process, the standard Data Protector restore from tape, or with specific disk array families, split mirror restore.

See also zero downtime backup (ZDB), ZDB to disk, ZDB to tape, instant recovery, replica, and replica set rotation.

ZDB to tape

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

See also zero downtime backup (ZDB), ZDB to disk, ZDB to disk+tape, instant recovery, and replica.

zero downtime backup (ZDB)

A backup approach in which data replication techniques, provided by a disk array, are used to minimize the impact of backup operations on an application system. A replica of the data to be backed up is created first. All subsequent backup operations are performed on the replicated data rather than the original data, while the application system can be returned to normal operation.

See also ZDB to disk, ZDB to tape, ZDB to disk+tape, and instant recovery.

Index

A

- architecture
 - NDMP integration, 48
 - Sybase integration, 15
- audience, 7

B

- backing up
 - NetApp SnapManager data, 73
- backing up NDMP, 60–63
 - backup specification, creating, 61
 - backup specification, modifying, 63
 - backup types, 48
 - starting backups, 63
- backing up NNM, 41–43
 - backup modes, 41
 - backup specifications, creating, 42
 - backup specifications, modifying, 42
 - backup templates, 42
 - backup types, 40–41
 - full backups, 41
 - incremental backups, 41
 - scheduling backups, 42
 - starting backups, 43
- backing up Sybase, 21–27
 - backup options, 24
 - backup specifications, creating, 21
 - backup specifications, modifying, 24
 - backup types, 15
 - database objects backup, 21
 - full backups, 15, 21
 - previewing backups, 25
 - scheduling backups, 24
 - scheduling backups, example, 25
 - starting backups, 26
 - transaction logs backups, 15, 21
- backup modes
 - NNM integration, 41
- backup options
 - Sybase integration, 24
- backup specifications, creating
 - NDMP integration, 61
 - NNM integration, 42
 - Sybase integration, 21
- backup specifications, modifying
 - NDMP integration, 63
 - NNM integration, 42
 - Sybase integration, 24
- backup specifications, scheduling
 - NNM integration, 42
 - Sybase integration, 24
- backup templates
 - NNM integration, 42
- backup types
 - NDMP integration, 48

- NNM integration, 40–41
 - Sybase integration, 15
- block size
 - NDMP integration, 59
 - BlueArc NAS devices
 - NDMP integration, 49, 58, 66

C

- Celerra NAS devices
 - NDMP integration, 49, 58, 60, 66
- checking configuration
 - Sybase integration, 20
- command-line interface reference
 - NetApp SnapManager solution, 78
- concepts
 - NDMP integration, 48
 - NetApp SnapManager solution, 72
 - NNM integration, 40
 - Sybase integration, 15
- configuring NDMP, 50–60
 - configuring NDMP devices, 52
 - creating media pools, 52
 - importing NDMP Servers, 51
- configuring NNM, 41
- configuring Sybase, 16–20
 - checking configuration, 20
- conventions
 - document, 12
- creating backup specifications
 - NDMP integration, 61
 - NNM integration, 42
 - Sybase integration, 21

D

- document
 - conventions, 12
 - related documentation, 7
- documentation
 - HP website, 7
 - providing feedback, 14

E

- environment variables
 - NDMP integration, 66
- examples, Sybase integration
 - restore, 35
 - scheduling backups, 25

F

- file history swap files
 - NDMP integration, 50
- full backups
 - NNM integration, 41
 - Sybase integration, 15, 21

H

help

obtaining, 13

Hitachi NAS devices

NDMP integration, 49, 58, 66

HP

technical support, 13

HP-X9000 NAS device

NDMP integration, 49

I

incremental backups

NNM integration, 41

installation

NetApp SnapManager solution, 72

interactive backups

NDMP integration, 63

NNM integration, 43

Sybase integration, 26

introduction

NDMP integration, 48

NNM integration, 40

Sybase integration, 15

M

media management

NDMP integration, 69

modifying backup specifications

NDMP integration, 63

NNM integration, 42

Sybase integration, 24

monitoring sessions

NNM integration, 43

Sybase integration, 36

N

NDMP backup, 60–63

backup specification, creating, 61

backup specification, modifying, 63

backup types, 48

starting backups, 63

NDMP configuration, 50–60

configuring NDMP devices, 52

creating media pools, 52

importing NDMP Servers, 51

NDMP integration

architecture, 48

backup, 60–63

concepts, 48

configuration, 50–60

environment variables, 66

file history swap files, 50

introduction, 48

media management, 69

omnirc file variables, 67

restore, 63–66

troubleshooting, 70–71

NDMP restore, 63–66

direct access restore, 65

using another device, 66

using GUI, 64

NDMP troubleshooting, 70–71

NetApp NAS devices

NDMP integration, 49, 57, 60, 65

NetApp SnapManager solution

backing up data, 73

command-line interface reference, 78

concepts, 72

installation, 72

restoring data, 75

NNM backup, 41–43

backup modes, 41

backup specifications, creating, 42

backup specifications, modifying, 42

backup templates, 42

backup types, 40–41

full backups, 41

incremental backups, 41

scheduling backups, 42

starting backups, 43

NNM configuration, 41

NNM integration

backup, 41–43

concepts, 40

configuration, 41

introduction, 40

monitoring sessions, 43

restore, 43

troubleshooting, 44–47

NNM restore, 43

NNM troubleshooting, 44–47

O

omnirc file variables

NDMP integration, 67

online backups

NNM integration, 41

P

previewing backups

Sybase integration, 25

R

related documentation, 7

restoring

NetApp SnapManager data, 75

restoring NDMP, 63–66

direct access restore, 65

using another device, 66

using GUI, 64

restoring NNM, 43

restoring Sybase, 27–36

examples, 35

finding information for restore, 28

using another device, 36

using the Sybase isql command, 33

running backups see starting backups see starting backups

S

- scheduling backups
 - NNM integration, 42
 - Sybase integration, 24
- starting backups
 - NDMP integration, 63
 - NNM integration, 43
 - Sybase integration, 26
- Subscriber's Choice, HP, 13
- Sybase backup, 21–27
 - backup options, 24
 - backup specifications, creating, 21
 - backup specifications, modifying, 24
 - backup types, 15
 - database objects backup, 21
 - full backups, 15, 21
 - previewing backups, 25
 - scheduling backups, 24
 - scheduling backups, example, 25
 - starting backups, 26
 - transaction logs backups, 15, 21
- Sybase configuration, 16–20
 - checking configuration, 20
- Sybase integration
 - architecture, 15
 - backup, 21–27
 - concepts, 15
 - configuration, 16–20
 - introduction, 15
 - monitoring sessions, 36
 - restore, 27–36
 - troubleshooting, 36–38
- Sybase restore, 27–36
 - examples, 35
 - finding information for restore, 28
 - using another device, 36
 - using the Sybase isql command, 33
- Sybase troubleshooting, 36–38

T

- technical support
 - HP, 13
 - service locator website, 13
- transaction logs backups
 - Sybase integration, 15, 21
- troubleshooting NDMP, 70–71
- troubleshooting NNM, 44
- troubleshooting Sybase, 36–38

W

- websites
 - HP, 13
 - HP Subscriber's Choice for Business, 13
 - product manuals, 7