HP Data Protector 8.00
Zero Downtime Backup Integration Guide
for Oracle, SAP R/3, Microsoft SQL Server, Microsoft Exchange Server, and Microsoft SharePoint Server

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

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

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

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

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

Adobe and Acrobat are trademarks of Adobe Systems Incorporated.

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

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

UNIX® is a registered trademark of The Open Group.

LiveVault® is a registered trademark of Autonomy Corporation plc.

Contents

Publication history....10
About this guide....11
Intended audience....11
Documentation set....11
Help....11
Guides....11
Documentation map....14
Abbreviations....14
Map....15
Integrations....15
Document conventions and symbols....16
Data Protector graphical user interface....17
General information....17
HP technical support....17
Subscription service....17
HP websites....18
Documentation feedback....18
1 Data Protector Oracle Server ZDB integration....19
Introduction....19
Backup and restore types....20
Integration concepts....21
Oracle backup set ZDB concepts....24
Backup process....26
Oracle proxy-copy ZDB concepts....28
Backup process....29
Configuring the integration....31
Prerequisites....31
Limitations....32
Before you begin....33
Backup set method....34
Configuring the HP P6000 EVA Disk Array Family in ASM environments....36
Configuring the HP P9000 XP Disk Array Family in ASM environments....36
Cluster-aware systems....37
Linking Oracle Server with the Data Protector MML....37
Configuring Oracle user accounts....37
Configuring Oracle operating system user accounts....37
Clusters....38
Configuring Oracle database users accounts....39
Configuring Oracle databases....39
Using the Data Protector GUI....40
Using the Data Protector CLI....42
Checking the configuration....45
Using the Data Protector GUI....46
Using the Data Protector CLI....46
Handling errors....46
Checking configuration for instant recovery....46
Setting environment variables....47
Using the Data Protector GUI....47
Using the Data Protector CLI....48
Switching between Oracle backup methods....48

Backup....49
Creating backup specifications....50
Examples of pre-exec and post-exec scripts on UNIX systems....58
Editing the Oracle RMAN script....58
Starting backup sessions....61
Considerations....61
Scheduling backup sessions....61
Running an interactive backup....62
Starting a backup using the GUI....62
Starting a backup using the CLI....63
Restore....63
Prerequisites....65
Restoring from backup media to the application system on LAN....65
Restoring Oracle using the Data Protector GUI....65
Restoring database items in a disaster recovery....65
Changing the database state....65
Restoring the recovery catalog database....66
Restoring the control file....67
Restoring Oracle database objects....68
Restoring tablespaces and datafiles....70
Duplicating an Oracle database....71
Restore, recovery, and duplicate options....73
Restore action options....73
General options....74
Duplicate options....75
Restore and recovery options....75
Restoring Oracle using RMAN....76
Preparing the Oracle database for restore....77
Connection strings used in the examples....78
SBT_LIBRARY parameter....78
Example of full database restore and recovery....78
Example of point-in-time restore....79
Example of tablespace restore and recovery....80
Example of datafile restore and recovery....82
Example of archive log restore....85
Example of database restore using a different device (with the automatic device selection functionality disabled)....86
Restoring using another device....86
Instant recovery and database recovery....87
Instant recovery using the Data Protector GUI....87
Oracle database recovery after the instant recovery....89
Oracle in Veritas Cluster instant recovery....90
Aborting sessions....91
Troubleshooting....91
Before you begin....92
Checks and verifications....92
Problems....97
2 Data Protector SAP R/3 ZDB integration....106
Introduction....106
Integration concepts....107
ZDB flow....107
Data Protector SAP R/3 configuration file....109
Setting, retrieving, listing, and deleting Data Protector SAP R/3 configuration file parameters using the CLI....111

Configuring the integration....112
Prerequisites....113
Before you begin....114
Cluster-aware clients....114
Configuring user accounts....115
Configuring SQL*Net V2 or Net8 TNS listener....116
Checking the connection....116
Authentication password file....117
Enabling archived logging....117
Sharing directories on the application system....118
UNIX application system....118
Windows application system....119
Choosing authentication mode....119
Configuring SAP R/3 databases....119
Before you begin....120
Using the Data Protector GUI....120
Using the Data Protector CLI....122
Handling errors....123
Checking the configuration....123
Using the Data Protector GUI....124
Using the Data Protector CLI....124
Configuring the SAP R/3 parameter file....124
Backup....125
Considerations....126
Creating backup specifications....126
Modifying backup specifications....132
Scheduling backup sessions....132
Scheduling example....132
Previewing backup sessions....133
Using the Data Protector GUI....133
Using the Data Protector CLI....133
What happens during the preview?....134
Starting backup sessions....134
Backup methods....134
Using the Data Protector GUI....134
Using the Data Protector CLI....134
Using the SAP BRTOOLS....134
Configuring SAP compliant ZDB sessions....136
Using the Data Protector GUI....136
Using the Data Protector CLI....137
Manual balancing....137
Restore....138
Considerations....139
Standard restore....139
Instant recovery....142
Considerations....142
Instant recovery using the Data Protector GUI....142
Database recovery options....143
Instant recovery using the Data Protector CLI....144
Instant recovery from replicas containing the control file....145
Restoring using another device....145
Using the Data Protector GUI....146
Using the Data Protector CLI or SAP commands....146
Localized SAP R/3 objects....146
Monitoring sessions....146

Troubleshooting....146
Before you begin....147
General troubleshooting....147
Verifying the prerequisites (Oracle side)....147
Verifying the prerequisites (SAP side)....148
Verifying the configuration....149
Verifying the backup configuration....150
Verifying restore....150
Configuration and backup problems....152
Restore problems....154
3 Data Protector Microsoft SQL Server ZDB integration....156
Introduction....156
Integration concepts....156
Configuring the integration....157
Prerequisites....157
Before you begin....158
Data Protector SQL Server configuration file....158
Configuring users....159
Configuring an SQL Server cluster....159
Configuring SQL Server instances....159
Using the Data Protector GUI....160
Using the Data Protector CLI....161
Changing and checking configuration....161
Using the Data Protector GUI....162
Using the Data Protector CLI....162
Backup....162
Creating ZDB specifications....163
SQL Server-specific backup options....167
Scheduling backups....168
Scheduling example....168
Starting backup sessions....168
Using the Data Protector GUI....168
Using the Data Protector CLI....169
Restore....169
Before you begin....169
Standard restore....169
Restore options....171
Restoring to a different SQL Server instance or/and different SQL Server....173
Instant recovery....173
Monitoring sessions....175
Troubleshooting....175
Before you begin....175
Checks and verifications....176
Problems....176
4 Data Protector Microsoft Exchange Server 2010 ZDB integration....181
Introduction....181
Integration concepts....182
Supported environments....182
Standalone environments....182
DAG environments....182
Configuring the integration....184
Prerequisites....184
Limitations....185
Before you begin....185

Configuring user accounts....185
Windows domain user account for backup and restore sessions....185
User account for executing Exchange Management cmdlet operations....186
Backup....186
Backup types....186
Microsoft Exchange Server backup types....186
ZDB backup types....187
VSS backup types....187
Backup parallelism....187
Replica rotation in DAG environments....188
Backup considerations....189
Object operations considerations....190
Creating backup specifications....190
Modifying backup specifications....196
Scheduling backup sessions....196
Scheduling example....196
Previewing backup sessions....197
Using the Data Protector GUI....197
Using the Data Protector CLI....197
What happens during the preview?....197
Starting backup sessions....198
Using the Data Protector GUI....198
Using the Data Protector CLI....198
Backup objects....199
Restore....199
Restore methods....199
Repair all passive copies with failed status....200
Restore to the latest state....200
Restore to a point in time....200
Restore to a new mailbox database....201
Restore files to a temporary location....201
Restore destination....201
Restoring to a standalone database....201
Restoring to an active copy....201
Restoring to a passive copy....202
Restoring data to a new database....202
Restoring data to a temporary location....202
Instant recovery in DAG environments....202
Restore chain....203
Restore chain during instant recovery....203
Restore parallelism....204
Finding information for restore....204
Using the Data Protector GUI....204
Using the Data Protector CLI....205
Standard restore....205
Restoring using the Data Protector GUI....205
Restoring using the Data Protector CLI....211
Restoring using another device....213
Instant recovery....213
Performing instant recovery using the Data Protector GUI....214
Performing instant recovery using the Data Protector CLI....219
Restore options....221
Monitoring sessions....224
Troubleshooting....224
Before you begin....225

Checks and verifications....225
Problems....225
5 Data Protector Microsoft SharePoint Server 2007/2010 VSS based solution...229
Introduction....229
Backup....229
Limitations....230
Restore....230
Installation and configuration....230
ZDB prerequisites....230
Microsoft Office SharePoint Server 2007....230
Microsoft SharePoint Server 2010....230
Licensing....231
Installing the integration....231
Configuring the integration....232
Configuring user accounts....232
Backup....232
How the command works....233
Microsoft Office SharePoint Server 2007....233
Microsoft SharePoint Server 2010....235
Considerations....235
The command syntax....236
Option description....236
Starting Windows PowerShell....238
Creating backup specifications (examples)....239
Modifying backup specifications....240
Source page....240
Destination page....240
Options page....240
Starting backup sessions (examples)....241
Scheduling backup sessions....244
Restore....244
Before you begin....245
Restoring data....245
Considerations....245
Prerequisites....246
Restoring using the Data Protector GUI....246
Restoring using the Data Protector CLI....248
Limitations....248
After the restore....248
Restoring index files on the Query system....249
Troubleshooting....249
Before you begin....249
Checks and verifications....249
After restore, you cannot connect to the Central Administration webpage....249
Backup fails with the error Failed to resume Service Windows SharePoint Services Help Search...250
After restore, a quiesce operation fails....250
After restore, you cannot connect to the FAST Search Server....251
The SharePoint_VSS_backup.ps1 script stops responding and the farm stays in read only mode...251
A Appendix....252
Reconfiguring an Oracle instance for instant recovery....252
Examples for moving the control files and redo logs to different locations 253

ZDB integrations omnirc options....254
Glossary....259
Index....288

Publication history

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

Table 1 Edition history

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

About this guide

This guide describes how to configure and use Data Protector disk array integrations with other software products.

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
- Database administration

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.

It is also recommended to read the *HP Data Protector Zero Downtime Backup Concepts Guide* for fundamentals of Data Protector integrations with disk arrays.

Documentation set

The Help and other guides provide related information.

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

Help

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

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

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

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

Windows systems: Open `DP_help.chm`.

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

Guides

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

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

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

You can also access the guides:

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

Data Protector guides are:

- *HP Data Protector Getting Started Guide*

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

- *HP Data Protector Concepts Guide*

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

- *HP Data Protector Installation and Licensing Guide*

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

- *HP Data Protector Troubleshooting Guide*

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

- *HP Data Protector Disaster Recovery Guide*

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

- *HP Data Protector Command Line Interface Reference*

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

  Windows systems: `Data_Protector_home\docs\MAN`

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

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

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

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

- *HP Data Protector Integration Guides*

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

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

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

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

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

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

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

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

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

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

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

- *HP Data Protector Integration Guide for Virtualization Environments*

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

- *HP Data Protector Zero Downtime Backup Concepts Guide*

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

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

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

- *HP Data Protector Zero Downtime Backup Integration Guide*

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

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

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

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

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

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

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

- *HP Data Protector Deduplication*

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

- *HP Data Protector Integration with Autonomy IDOL Server*

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

- *HP Data Protector Integration with Autonomy LiveVault*

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

Documentation map

Abbreviations

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

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

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

Map

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

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

Integrations

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

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

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

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

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

Document conventions and symbols

Table 2 Document conventions

Convention	Element
Blue text: "Document conventions" (page 16)	Cross-reference links and e-mail addresses
Blue, underlined text: http://www.hp.com	Website addresses
Bold text	• Keys that are pressed • Text typed into a GUI element, such as a box • GUI elements that are clicked or selected, such as menu and list items, buttons, tabs, and check boxes
Italic text	Text emphasis
`Monospace` text	• File and directory names • System output • Code • Commands, their arguments, and argument values
`Monospace, italic` text	• Code variables • Command variables
`Monospace, bold` text	Emphasized monospace text

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

IMPORTANT: Provides clarifying information or specific instructions.

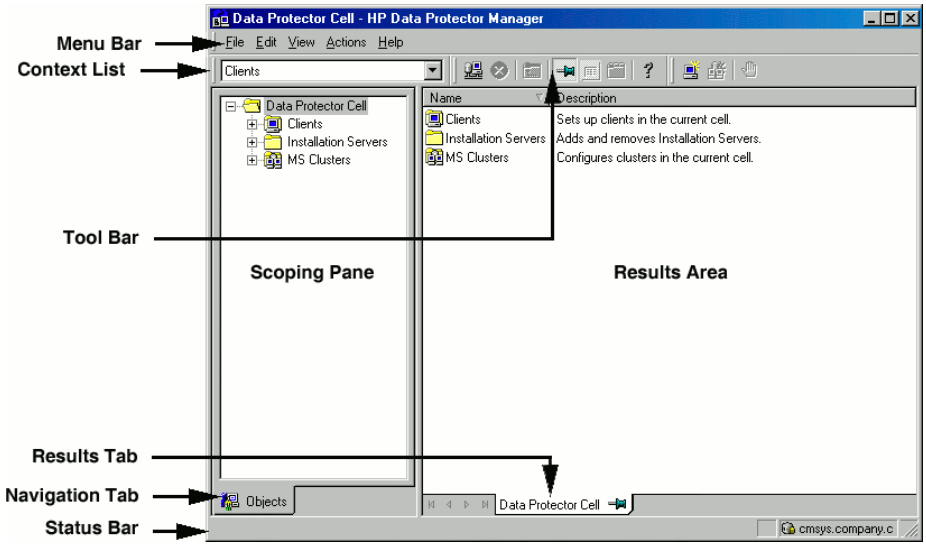
NOTE: Provides additional information.

TIP: Provides helpful hints and shortcuts.

Data Protector graphical user interface

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

Figure 1 Data Protector graphical user interface



General information

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

HP technical support

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

http://www.hp.com/support

Before contacting HP, collect the following information:

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

Subscription service

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

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

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

HP websites

For additional information, see the following HP websites:

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

Documentation feedback

HP welcomes your feedback.

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

1 Data Protector Oracle Server ZDB integration

Introduction

You can employ a variety of backup strategies to best meet your system priorities. If database availability is the highest priority, for instance, your backup strategy should include online backups that are performed frequently to minimize recovery time. This strategy limits downtime, but uses system resources more intensively. The Data Protector zero downtime backup (ZDB) functionality offers online backup capabilities with minimal degradation of the application system performance.

Supported disk arrays

The following disk arrays can be used for zero downtime backup (ZDB) of the Oracle Server data:

- HP P6000 EVA Disk Array Family (P6000 EVA Array)
- HP P9000 XP Disk Array Family (P9000 XP Array)
- EMC Symmetrix (EMC)

NOTE: With the Data Protector EMC integration, instant recovery is not supported, and ZDB to tape is the only supported ZDB form.

In Oracle Server configurations that use Automatic Storage Management (ASM), zero downtime backup is only supported with the Data Protector P6000 EVA Array and Data Protector P9000 XP Array integrations, and instant recovery is only supported with the Data Protector P9000 XP Array integration.

Advantages

The advantages of using Data Protector Oracle ZDB integration are:

- ZDB reduces the performance degradation of the application system.
- The tablespaces are in backup mode (online backup) or the database is shut down (offline backup) only during the short period required to create a **replica** (split the mirror disks or create snapshots).
- The load to the application system is significantly reduced. Following the replica creation, tape backup can be started on the copied data, at leisure, using a separate backup system.

The Data Protector Oracle ZDB integration offers online and offline backup of your Oracle Server System (application system).

The online backup concept is widely used since it enables high application availability. Offline backup requires shutting down the database while creating a replica, and therefore does not offer high availability.

ZDB methods and Oracle versions

The installation, upgrade, configuration, and parts of backup flow are different depending on the selected Oracle ZDB method. These differences are indicated where appropriate.

The procedures for configuration of backup specifications and starting or scheduling backups are the same, regardless of the Oracle ZDB method.

Backup and restore types

Backup

Using Data Protector, you can perform the following types of backup:

- Online ZDB to disk, ZDB to tape, and ZDB to disk+tape.

  During the creation of a replica, the database on the application system is in hot backup mode. If a ZDB-to-tape or a ZDB-to-disk+tape session is being performed, the streaming of the data to tape media is subsequently performed on the backup system.

- Offline ZDB to disk, ZDB to tape, and ZDB to disk+tape.

  During the creation of a replica, the database is shut down on the application system. Therefore, the database is not available during the short time that it takes to create the replica. If a ZDB-to-tape or a ZDB-to-disk+tape session is being performed, the streaming of the data to tape media is subsequently performed on the backup system.

With both online and offline ZDB to tape or ZDB to disk+tape, a standard Data Protector (non-ZDB) backup of the recovery catalog and the control file is started automatically, after the target database backup is finished on the backup system. However, you can disable this when creating a backup specification.

NOTE: Backup of the recovery catalog and control file is not performed with ZDB to disk.

The Oracle Recovery Manager utility (RMAN) is not aware of ZDB-to-disk sessions.

IMPORTANT: Backup of archived logs cannot be done with the Data Protector Oracle ZDB integration. Backup of archive logs and control file has to be done following the standard Data Protector Oracle integration backup procedure. For more information on Oracle archive log backup with Data Protector see the *HP Data Protector Integration Guide*.

NOTE: On EMC, decision support, application testing, and similar tasks are possible only if the Oracle binaries are installed on the backup system as well. In most cases, however, the Data Protector EMC integration requirement is that application binaries are installed on the application system only.

Restore

Using Data Protector and the disk array integrations, you can perform the following types of restore:

- Restoring from backup media to the application system on LAN (standard Data Protector restore) and using RMAN on the application system, you can:
  - recover a whole database
  - recover a part of a database
  - recover a whole database as it was at a specific point in time
- Using the instant recovery functionality and RMAN on the application system, you can:
  - perform a full database restore and database recovery
  - perform recovery from incremental backup (for ZDB to tape or ZDB to disk+tape)
  - perform recovery from a chain of incremental backups (for ZDB to tape or ZDB to disk+tape)
  - restore a datafile to a location other than its original one

"Oracle recovery methods" (page 21) provides an overview of recovery methods, depending on the type of backup that was performed and type of recovery required.

Table 3 Oracle recovery methods

Disk array	Backup types	Recover the whole database until		Recover a part of database until now
		Now	A point in time, logseq/thread, or SCN number	
P9000 XP, P6000 EVA, EMC	**ZDB to tape - online**	Restore	Restore	Restore
	ZDB to tape - offline	Restore	Restore[1]	Restore
P9000 XP, P6000 EVA	**ZDB to disk - online**	Instant recovery+ database recovery	Instant recovery+ database recovery	N/A
	ZDB to disk - offline	Instant recovery	Instant recovery+ database recovery[1]	N/A
	ZDB to disk+tape - online	• Restore or • Instant recovery+ database recovery	• Restore or • Instant recovery+ database recovery	Restore
	ZDB to disk+tape - offline	• Restore or • Instant recovery	• Restore or • Instant recovery+ database recovery[1]	Restore

[1] The database must be put in archive mode

Legend

Restore — Use the Data Protector GUI or RMAN scripts to restore the database from backup media to the application system on LAN.

Instant recovery + database recovery — The following three options are possible:

- Perform instant recovery followed by database recovery from the Data Protector Instant Recovery GUI context or
- Perform instant recovery first and then perform database recovery from the Data Protector Restore GUI context or
- Perform instant recovery first and then use RMAN scripts to recover the database.

Instant recovery — Perform instant recovery without database recovery.

See the *HP Data Protector Zero Downtime Backup Concepts Guide* for an overview of ZDB concepts and terminology.

Integration concepts

The Data Protector Oracle integration links the Oracle database management software with Data Protector. From the Oracle point of view, Data Protector represents a media management software. On the other hand, the Oracle database management system can be seen as a data source for backup, using media controlled by Data Protector.

Components

The software components involved in backup and restore processes are:

- The Oracle Recovery Manager (RMAN)
- The Data Protector Oracle integration software

Integration functionality overview

The Data Protector Oracle Integration agent (`ob2rman.pl`) works with RMAN to manage all aspects of the following operations on the Oracle target database:

- Database startup and shutdown
- Backups (backup and copy)
- Recovery (restore, recovery, and duplication)

How does the integration work?

`ob2rman.pl` executes RMAN, which directs the Oracle server processes on the target database to perform backup, restore and recovery. RMAN maintains the required information about the target databases in the recovery catalog, the Oracle central repository of information, and in the control file of a particular target database.

The main information which `ob2rman.pl` provides to RMAN is:

- Number of allocated RMAN channels
- RMAN channel environment parameters
- Information on the database objects to be backed up or restored

For backup, `ob2rman.pl` uses the Oracle target database views to get information on which logical (tablespaces) and physical (datafiles) target database objects are available for backup.

For restore, `ob2rman.pl` uses current control file or recovery catalog (if used) to get information on which objects are available for restore.

Using the Data Protector integration with RMAN, you can back up and restore the Oracle control files, datafiles, and archived redo logs.

The interface from the Oracle server processes to Data Protector is provided by the Data Protector Oracle integration Media Management Library (**MML**), which is a set of routines that allows the reading and writing of data to General Media Agents.

Besides handling direct interaction with the media devices, Data Protector provides scheduling, media management, network backups, monitoring, and interactive backup.

A backup that includes all datafiles and current control file that belong to an Oracle Server instance is known as a whole database backup.

These features can be used for online or offline backup of the Oracle target database. However, you must ensure that the backup objects (such as tablespaces) are switched into the appropriate state before and after a backup session. For online backup, the database instance must operate in the `ARCHIVELOG` mode; whereas for offline backup, objects need to be prepared for backup using the `Pre-exec` and `Post-exec` options in the backup specification.

The Data Protector backup specification contains information about backup options, commands for RMAN, Pre- and Post-exec commands, media, and devices.

The Data Protector backup specification allows you to configure a backup and then use the same specification several times. Furthermore, scheduled backups can only be performed using a backup specification.

Backup and restore of an Oracle target database can be performed using the Data Protector User Interface or the RMAN utility.

The heart of the Data Protector Oracle integration is MML, which enables an Oracle server process to issue commands to Data Protector for backing up or restoring parts or all of the Oracle target database files. The main purpose is to control direct interaction with media and devices.

Non-ZDB flow

A Data Protector scheduled or interactive backup is triggered by the Data Protector Backup Session Manager, which reads the backup specification and starts the `ob2rman.pl` command on the Oracle Server under the operating system user account specified in the backup specification. Further on, `ob2rman.pl` prepares the environment to start the backup, and issues the RMAN backup command. RMAN instructs the Oracle Server processes to perform the specified command.

The Oracle Server processes initialize the backup through MML, which establishes a connection to the Data Protector Backup Session Manager. The Backup Session Manager starts the General Media Agent, sets up a connection between MML and the General Media Agent, and then monitors the backup process.

The Oracle Server processes read the data from the disks and send it to the backup devices through MML and the General Media Agent.

RMAN writes information regarding the backup either to the recovery catalog (if one is used) or to the control file of the Oracle target database.

Messages from the backup session are sent to the Backup Session Manager, which writes messages and information regarding the backup session to the IDB.

The Data Protector General Media Agent writes data to the backup devices.

Restore flow

A restore session can be started using:

- Data Protector GUI
- RMAN CLI

You must specify which objects are to be restored.

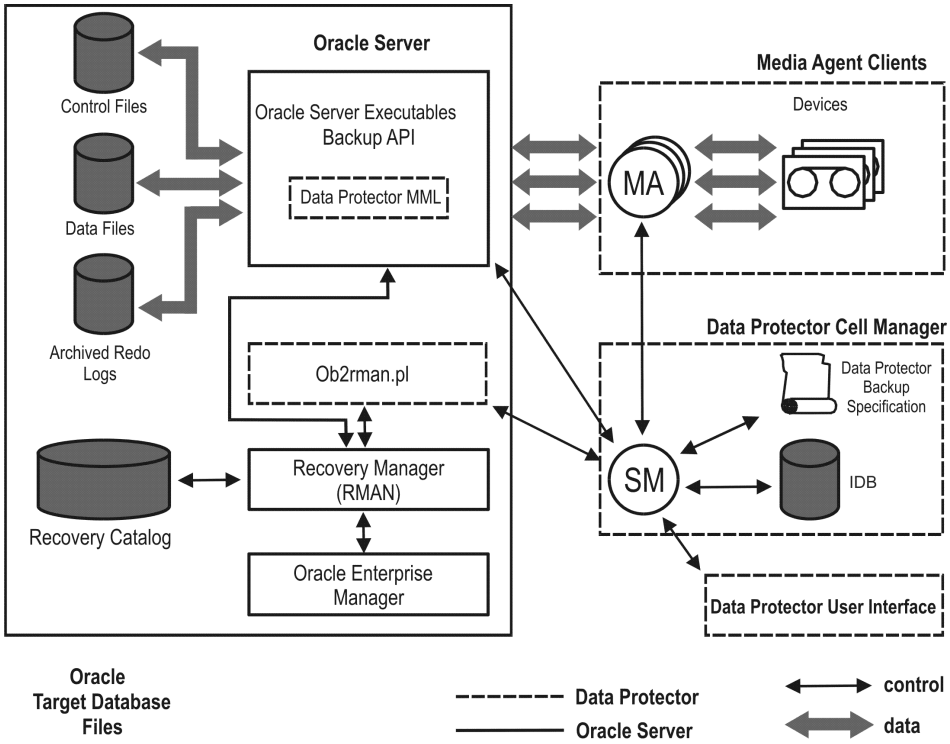
A restore from the Data Protector user interface is triggered by the Data Protector Restore Session Manager, which starts the `ob2rman.pl` command. `ob2rman.pl` prepares the environment to start the restore, and issues the RMAN restore command. RMAN checks the recovery catalog (if one is used) or the control file to gather the information about the Oracle backup objects. It also contacts the Oracle Server processes, which initialize the restore through MML. MML establishes a connection with the Restore Session Manager and passes along the information about which objects and object versions are needed.

The Restore Session Manager checks the IDB to find the appropriate devices and media, starts the General Media Agent, establishes a connection between MML and the General Media Agent, and then monitors the restore and writes messages and information regarding the restore to the IDB.

The General Media Agent reads the data from the backup devices and sends it to the Oracle Server processes through MML. The Oracle Server Processes write the data to the disks.

The concept of Oracle integration, data and the control flow are shown in "Data Protector Oracle integration concept" (page 24), and the related terms are explained in the following table.

Figure 2 Data Protector Oracle integration concept



Database files can also be managed by **Automatic Storage Management** (**ASM**).

Legend

SM	The Data Protector Session Manager, which can be the Data Protector Backup Session Manager during a backup session and the Data Protector Restore Session Manager during a restore session.
RMAN	The Oracle Recovery Manager.
Data Protector MML	The Data Protector Oracle integration Media Management Library, which is a set of routines that enables data transfer between the Oracle Server and Data Protector.
Backup API	The Oracle-defined application programming interface.
IDB	The Data Protector Internal Database where all the information about Data Protector sessions, including session messages, objects, data, and used devices and media, is written.
MA	The Data Protector General Media Agent, which reads and writes data from and to media devices.

Oracle backup set ZDB concepts

See the *HP Data Protector Zero Downtime Backup Concepts Guide* for a general description of ZDB-to-disk, ZDB-to-tape, and ZDB-to-disk+tape and instant recovery concepts.

With the Oracle backup set ZDB method, the entire data to be backed up is provided to Data Protector through the Oracle API—the data is streamed through the Data Protector Oracle integration MML.

Depending on the location of the Oracle control file, online redo log files, and SPFILE, the following two options are possible:

- Oracle control file, online redo log files, and SPFILE reside on a **different** volume group (if LVM is used) or source volume than Oracle datafiles.

  By default, instant recovery for such a configuration is enabled.

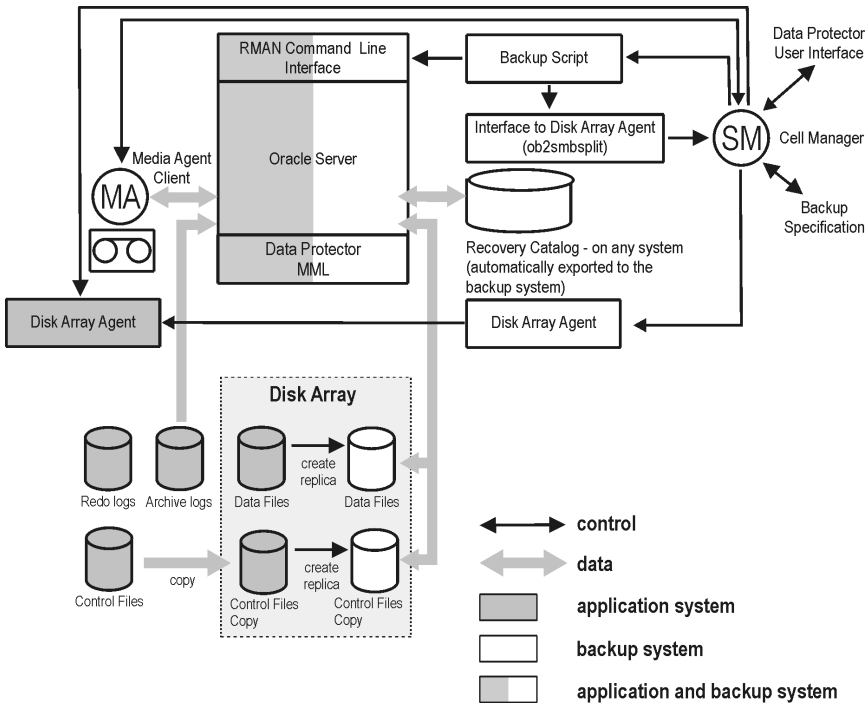
- Oracle control file, online redo log files, SPFILE reside on the **same** volume group (if LVM is used) or source volume as Oracle datafiles.

  By default, instant recovery for such a configuration is *not* enabled. You can enable instant recovery by setting the `ZDB_ORA_INCLUDE_CF_OLF`, `ZDB_ORA_INCLUDE_SPF`, and `ZDB_ORA_NO_CHECKCONF_IR` `omnirc` options to `1`. See "ZDB integrations omnirc options" (page 254).

IMPORTANT: If you enable instant recovery by setting the above mentioned options, note that the control file, SPFILE, and online redo logs are overwritten during instant recovery.

The Oracle archived redo log files do not have to reside on source volumes.

Figure 3 Oracle backup set ZDB concept



"Oracle backup set ZDB concept" (page 25) presents only the default integration behavior, where Oracle control file, online redo log files, and SPFILE reside on a different volume group (if LVM is used) or source volume than Oracle datafiles. Oracle database files can also be managed by ASM, however some limitations apply to Oracle ASM configurations. For details, see "Limitations" (page 32).

For more information on an alternative Oracle backup and restore concept, see "ZDB integrations omnirc options" (page 254).

Legend

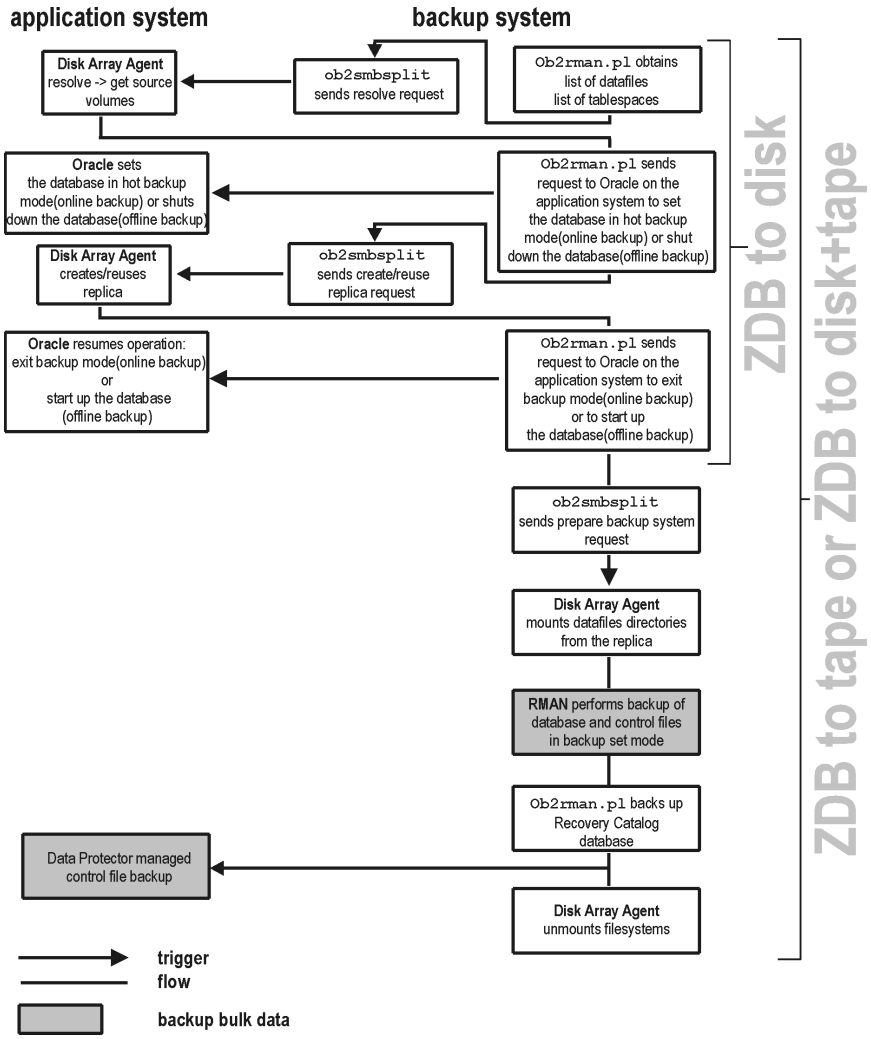
MA	The General Media Agent writes data from a replica to backup media. The General Media Agent typically resides on the backup system.
SM	The session manager controls backup and restore sessions and writes session information to the IDB.

Disk Array Agent The disk array agents (ZDB agents) are SYMA (on EMC), SSEA (on P9000 XP Array), and SMISA (on P6000 EVA Array).

Data Protector MML The Data Protector Oracle integration Media Management Library, which is a set of routines that enables data transfer between the Oracle Server and Data Protector. This is a Data Protector software library that is linked to the Oracle software.

Backup process

Figure 4 Oracle backup set ZDB flow



NOTE: ZDB agents are SYMA on EMC, SSEA on P9000 XP Array, and SMISA on P6000 EVA Array.

See the *HP Data Protector Zero Downtime Backup Concepts Guide* for a general description of ZDB and instant recovery concepts.

See the *HP Data Protector Zero Downtime Backup Administrator's Guide* for a general description of the ZDB-to-disk, ZDB-to-tape, and ZDB-to-disk+tape session flows and for the explanation of actions triggered by ZDB options.

This section provides only the information relevant to the Data Protector Oracle ZDB integration.

Operations on a replica (mounting, activating volume/disk groups,...) described below are dependent on or triggered by ZDB options. See the *HP Data Protector Zero Downtime Backup Administrator's Guide* for more information on these options.

- Data Protector executes the `ob2rman.pl` command on the backup system. This command retrieves a list of files or disk images to be backed up from the Oracle database on the application system and starts the resolving process. The list is used only to determine the source volumes to be replicated. If the location for control file copy is specified during configuration, `ob2rman.pl` makes a copy of the control file to the specified directory on the application system. This directory has to reside on a disk array source volume.
- When performing an *online* ZDB session, `ob2rman.pl` then sets the Oracle target database into backup mode by issuing the `sqlplus` command "`ALTER TABLESPACE BEGIN BACKUP`", starts the procedure to create a replica of the source volumes on which the database is installed; and after the replica is created, takes the database out of backup mode by issuing the `sqlplus` command "`ALTER TABLESPACE END BACKUP`".

  When performing an *offline* ZDB session, `ob2rman.pl` shuts down the Oracle database, starts the procedure to create a replica of the source volumes on which the database is installed; and after the replica is created, starts up the Oracle database.
- `ob2rman.pl` then starts the procedure to prepare the replica on the backup system. In this step, volume/disk groups on the backup system are enabled and, unless the database is installed on raw partitions, the mount points with the Oracle database files are mounted.
- A ZDB agent then mounts the database on the backup system to the mount points with the same names (created by Data Protector) as on the application system.

NOTE: There must be nothing already mounted on the mount point concerned on the backup system, or the resolving and backup will fail.

- If a ZDB-to-disk session is being performed, at this point the remaining ZDB options are processed and details of the session are written to the ZDB database. The session then finishes. The following steps in this description are not performed, therefore RMAN is not given any information about ZDB-to-disk session.
- If a ZDB-to-tape or a ZDB-to-disk+tape session is being performed, the processing continues as follows:
  - `ob2rman.pl` starts the Oracle backup command RMAN on the backup system, and then sends the Oracle RMAN Backup Command Script to the RMAN cmdfile (input command file).
  - RMAN contacts the Oracle database instance on the backup system, which contacts Data Protector via SBT API and initiates a backup.
  - The Oracle database instance on the backup system reads data from the replica and sends it to the Data Protector General Media Agent for writing to the backup device.
  - At the end of data transfer, the backup system is disabled (filesystems are dismounted on all platforms and volume/disk groups deactivated on UNIX systems) and links are re-established.
  - The recovery catalog and the control file are backed up automatically after the target database backup is finished on the backup system. However, you can disable this when creating a backup specification.

NOTE: A replica of the archive logs is not created; therefore, the archive logs should be backed up from the application system, following the standard Data Protector Oracle archive logs backup procedure.

Oracle proxy-copy ZDB concepts

See the *HP Data Protector Zero Downtime Backup Concepts Guide* for a general description of ZDB-to-disk, ZDB-to-tape, ZDB-to-disk+tape, and instant recovery concepts.

The Data Protector Oracle integration MML supports the Proxy Copy functionality. This enables Data Protector to perform backup using filesystem backup methods.

Depending on the location of the Oracle control file, online redo log files, and SPFILE, the following two options are possible:

- Oracle control file, online redo log files, and SPFILE reside on a **different** volume group (if LVM is used) or source volume than Oracle datafiles.

  By default, instant recovery is enabled if this option is selected in the GUI.

- Oracle control file, online redo log files, and SPFILE reside on the **same** volume group (if LVM is used) or source volume as Oracle datafiles.

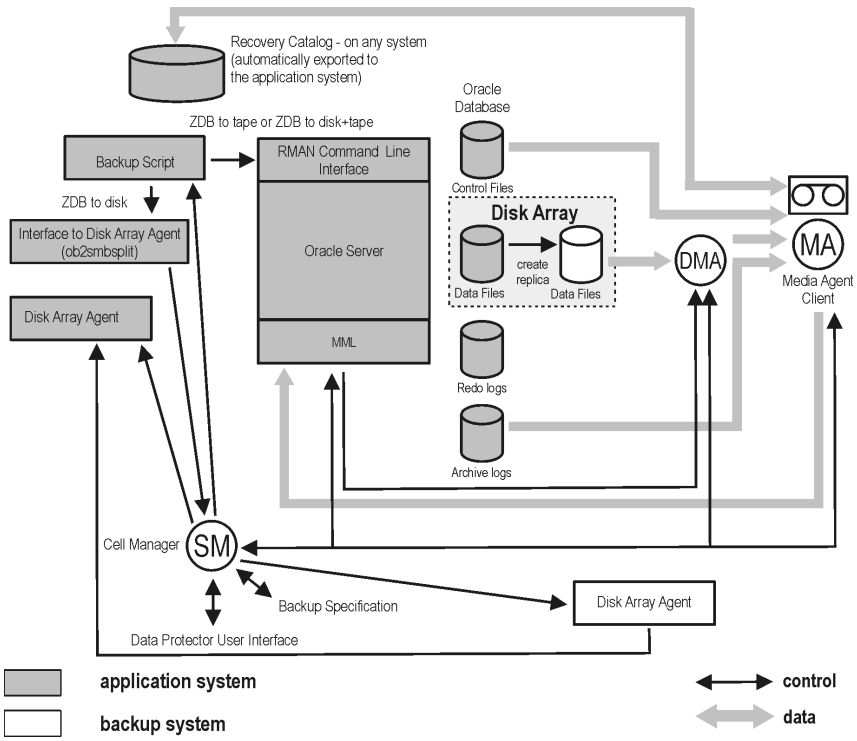
  By default, instant recovery is *not* enabled, even if this option is selected in the GUI. You can enable instant recovery by setting the `ZDB_ORA_INCLUDE_CF_OLF`, `ZDB_ORA_INCLUDE_SPF`, and `ZDB_ORA_NO_CHECKCONF_IR` `omnirc` options to `1`. See "ZDB integrations omnirc options" (page 254).

IMPORTANT: If you enable instant recovery by setting the above mentioned options, note that the control file, SPFILE, and online redo logs are overwritten during instant recovery.

The Oracle archived redo log files do not have to reside on source volumes.

"Oracle proxy-copy ZDB concept" (page 28) shows the architecture of the Data Protector Oracle ZDB integration. The figure illustrates the configuration, in which the backup is performed on the backup system. It presents the default integration behavior, where Oracle control file, online redo log files, and SPFILE reside on different disk array source volumes than the Oracle data files. For more information on alternative Oracle backup and restore concepts, see "ZDB integrations omnirc options" (page 254).

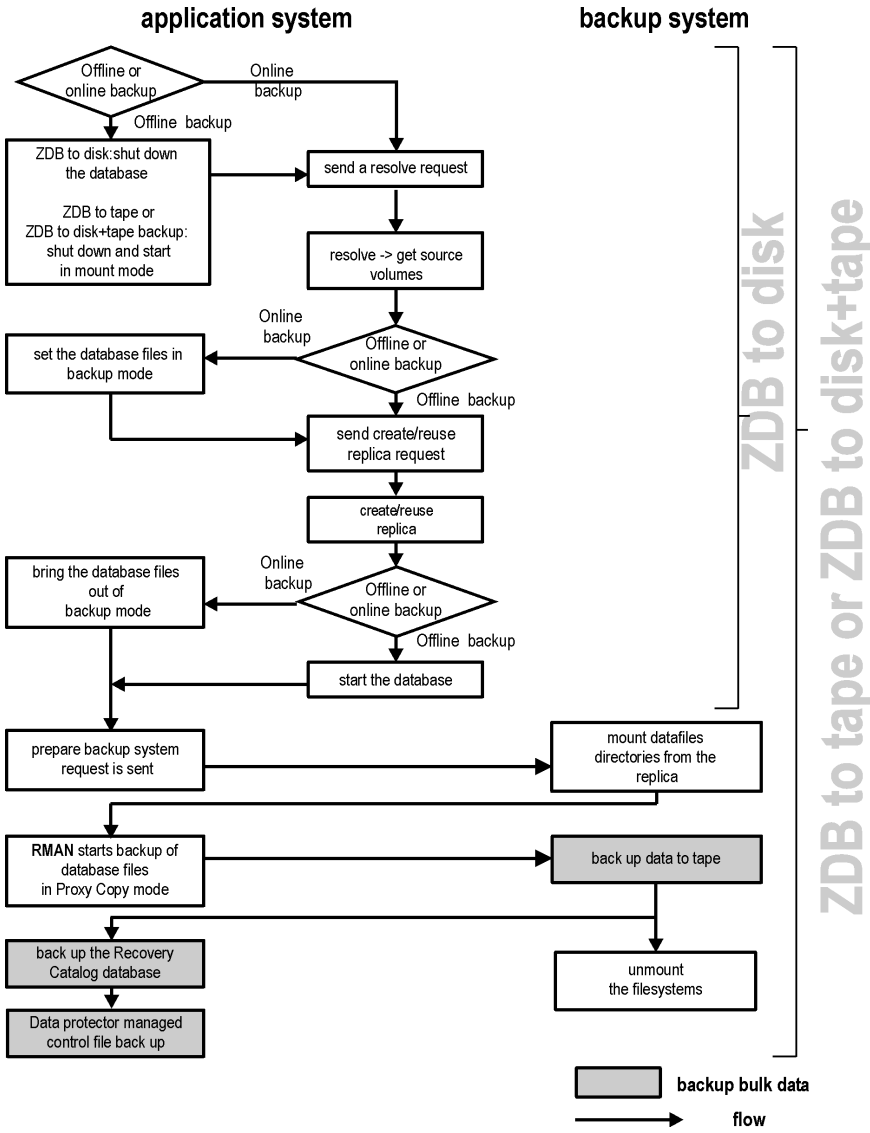
Figure 5 Oracle proxy-copy ZDB concept



MA	The General Media Agent writes data from a replica to backup media. The General Media Agent typically resides on the backup system.
SM	The session manager controls backup and restore sessions and writes the session information to the IDB.
Disk Array Agent	The disk array agents (ZDB agents) are SYMA (on EMC), SSEA (on P9000 XP Array), and SMISA (on P6000 EVA Array).
MML	The Data Protector Oracle integration Media Management Library, which is a set of routines that enables data transfer between the Oracle Server and Data Protector. This is a Data Protector software library that is linked to the Oracle software.

Backup process

Figure 6 Oracle proxy-copy ZDB flow



See the *HP Data Protector Zero Downtime Backup Administrator's Guide* for a general description of the ZDB-to-disk, ZDB-to-tape, and ZDB-to-disk+tape sessions flows and for an explanation of actions triggered by ZDB options.

This section provides only the information relevant to the Data Protector Oracle ZDB integration.

Operations on a replica (mounting, activating volume/disk groups...) described below are dependent on or triggered by ZDB options. See the *HP Data Protector Zero Downtime Backup Administrator's Guide* for more information on these options.

- In the case of an *offline* ZDB-to-disk+tape or ZDB-to-tape session, `ob2rman.pl` shuts down and opens the database instance in mount state. For both, offline and online ZDB-to-disk+tape or ZDB-to-tape sessions, Data Protector starts RMAN in proxy-copy mode.

  In the case of an *offline* ZDB-to-disk session, the database is shut down.

- Data Protector retrieves a list of files or disk images to be included in the replica creation from the Oracle database and starts the resolving process. The list is used only to determine the source volumes to be replicated.

  In the case of a *ZDB-to-disk* session, if the location for control file copy is specified during configuration, Data Protector makes a copy of the control file to the specified directory on the application system. This directory has to reside on a disk array source volume.

- In the case of an *online* backup, the Oracle target database is switched into the backup mode.
- `ob2smbsplit` or MML starts the procedure to create a replica of the source volumes on which the database is installed.
- In the case of an *online* backup, the database files are taken out of the backup mode after the replica is created.

  In the case of an *offline* backup, the Oracle `alter database open` command is sent after the replica is created.

- Data Protector (for ZDB to disk) or MML (for ZDB to tape or ZDB to disk+tape) starts the procedure to prepare the replica on the backup system. In this step, volume/disk groups on the backup system are enabled (UNIX systems) and, unless the database is installed on raw disks, the mount points containing the Oracle database files are mounted.
- A ZDB agent then mounts the database on the backup system to the mount points with the same names (created by Data Protector) as on the application system.
- If a ZDB-to-disk session is being performed, at this point the remaining ZDB options are processed and details of the session are written to the ZDB database. The session then finishes. The following steps in this description are not performed; therefore, RMAN is not given any information about the ZDB-to-disk session.
- MML on the application system sends a request to the Data Protector **data movement agent** (DMA) on the backup system to back up the datafiles to tape.
- The DMA reads data from the backup system and sends it to the General Media Agent to write the actual data to the backup device.

  DMA's role is also to disable the General Media Agent requests from accessing the application system. Thus, the database runs on the application system with greatly reduced performance degradation since the backup is performed on the backup system.

- At the end of data transfer, the backup system is disabled (filesystems are dismounted on all platforms and volume/disk groups deactivated on UNIX systems) and links are re-established.
- The recovery catalog and the control file are backed up automatically after the target database backup is finished on the backup system. However, you can disable this when creating a backup specification.

NOTE: A replica of the archive logs is not created; therefore, the archive logs should be backed up from the application system, following the standard Data Protector Oracle archive logs backup procedure.

Configuring the integration

Prerequisites

- It is assumed that you are familiar with the Oracle database administration and the basic Data Protector functionality.
- You need a license to use the Data Protector ZDB integration with Oracle. Additional licenses are required for instant recovery and for the online extension. For information on licensing, see the *HP Data Protector Installation and Licensing Guide*.
- Before you begin, ensure that you have correctly installed and configured the Oracle Server and Data Protector client systems. See the:
  - Latest support matrices at http://support.openview.hp.com/selfsolve/manuals for an up-to-date list of supported versions, platforms, devices, and other information.
  - *HP Data Protector Installation and Licensing Guide* for instructions on how to install Data Protector on various architectures and how to install a Data Protector disk array integration (EMC, P9000 XP Array, or P6000 EVA Array) with Oracle.
  - *Oracle Recovery Manager User's Guide and References* for Oracle concepts and backup/recovery strategies.
  - *Oracle Backup and Recovery Guide* for the configuration and use of Recovery Manager, as well as for Oracle backup terminology and concepts.
  - *Oracle Enterprise Manager User's Guide* for information on backup and recovery with the Oracle Enterprise Manager, as well as information about SQL*Plus.
- A Data Protector disk array integration (EMC, P9000 XP Array, or P6000 EVA Array) must be correctly installed and configured. For installation, see the *HP Data Protector Installation and Licensing Guide*. For configuration, see the *HP Data Protector Zero Downtime Backup Administrator's Guide*.
- ***Oracle Server configurations with ASM:*** The disk array must support creation of replicas with cross-volume data consistency:
  - If a disk array of the HP P6000 EVA Disk Array Family is used, it must support multisnapping.

    For configuration details, see "Configuring the HP P6000 EVA Disk Array Family in ASM environments" (page 36).
  - If a disk array of the HP P9000 XP Disk Array Family is used, it must support the atomic split operation.

    For configuration details, see "Configuring the HP P9000 XP Disk Array Family in ASM environments" (page 36).

  For details about which disk array models and disk array firmware revisions support creation of replicas with cross-volume data consistency, see the latest support matrices at http://support.openview.hp.com/selfsolve/manuals.
- The Oracle Server software must be installed on the application system and the Oracle target database must be open or mounted there.
- The Oracle recovery catalog database must be properly configured and open.
- Oracle net services must be properly configured and running (on the application system) for the Oracle target database and the recovery catalog. The net services are needed for the

Data Protector Oracle agent to be connected to the Oracle database on the application system through Oracle.

For more information about different connection options, see the *Oracle Recovery Manager User's Guide and References*.

For details on checking the prerequisites listed above, see "Troubleshooting" (page 91).

Note that the Data Protector Oracle integration uses RMAN for backup and restore. RMAN connection to a target database requires a dedicated server process. To ensure that RMAN does not connect to a dispatcher when the target database is configured for a shared server, the net service name used by RMAN must include `(SERVER_DEDICATED)` in the `CONNECT_DATA` attribute of the connection string.

- ***Oracle Real Application Clusters (RAC):*** Each node must have a dedicated disk for storing archive logs. Such disks must be NFS mounted on all other RAC nodes.

  However, if the archive logs are not on a NFS mounted disk, you must modify the archive log backup specification. See "Backup of archive logs on RAC cannot be performed" (page 101).

- ***RAC:*** With Oracle version 11.2.0.2 and later, the control file must be created on a shared disk and be accessible from all RAC nodes, and the `OB2_DPMCTL_SHRLOC` environment variable must point to this location, from where the control file is backed up.

Limitations

- The `MAXPIECESIZE` RMAN parameter option is not supported because the restore of multiple backup pieces created during a backup is not possible using the Data Protector Oracle integration.
- The Oracle recovery catalog database must be used as RMAN repository for backup and restore operations. ZDB using the Oracle control file are not supported. This is set when configuring the database. See "Configuring Oracle databases" (page 39).
- The Oracle database identifier (DBID) must be a unique in a Data Protector cell. If you clone a database you must change the DBID.
- Preview of zero downtime backup and instant recovery sessions is not available.
- Using the Oracle proxy-copy ZDB method, individual tablespaces or datafiles cannot be backed up during a ZDB-to-disk or ZDB-to-disk+tape session (instant recovery enabled), only the whole database can be backed up.
- The Oracle backup set ZDB method is supported on UNIX raw logical volumes only if these were created with LVM or VxVM.
- When using the Oracle backup set ZDB method, you must reconfigure the Oracle integration if the initialization parameter file has been changed since the last configuration execution. See "Configuring Oracle databases" (page 39).
- The single-host configuration (BC1, TF/1) is not supported for Oracle backup set ZDB sessions.
- Object copying and object mirroring is not supported for ZDB to disk.
- Recovery files residing in the **flash recovery area** cannot be backed up using ZDB.
- ***Oracle Server configurations with ASM:*** The following limitations apply:
  - Zero downtime backup (ZDB) is only supported with the HP P6000 EVA Disk Array Family and the HP P9000 XP Disk Array Family.
  - Only the backup set ZDB method is supported.

- With the HP P6000 EVA Disk Array Family, only configurations consisting of a single disk array unit are supported.
- Instant recovery is only supported with the HP P9000 XP Disk Array Family.

- ***Oracle Data Guard:*** Standby database is not supported for ZDB.
- The Data Protector Oracle integration does not support non-ASCII characters in backup specification names.

Before you begin

- Test whether the Oracle Server system and the Cell Manager communicate properly: Configure and run a Data Protector filesystem backup and restore on the Oracle Server system.
- Identify the Oracle database *user* that will be used by Data Protector for backup. This user must have the `SYSDBA` privilege granted. For example, it could be the Oracle user `sys`, which is created during database creation.

  See the Oracle documentation for more information on user privileges in Oracle.
- On Windows systems, if the Oracle target database and the Oracle recovery catalog are installed on two different systems, configure a *domain* user account that is a member of the Administrators group on both systems.

  On Windows Server 2003 systems with the Oracle target database installed, you need to restart the `Data Protector Inet` service under a Windows domain user account that has the appropriate Oracle database permissions for running backups and restores.

  For information on how to change the `Data Protector Inet` service account, see the *HP Data Protector Help* index: "Inet, changing account".

  However, for other supported Windows operating systems, you can use user impersonation instead. For details on setting accounts for the Inet service user impersonation, see the *HP Data Protector Help* index: "Inet user impersonation".
- In case of the backup set method, if the Oracle database is installed on symbolic links, create these symbolic links on the backup system, too.
- From the application system, using SQL*Plus, connect to the target database and recovery catalog by specifying the user, password, and net connect identifier. Connect to the target database as the database administrator and to the recovery catalog database as the recovery catalog owner.

  Example

  If the user name for the target database is `system`, password `manager`, net service name `PROD`, and the user name and password for the recovery catalog is `rman` and the net service name `RMANCAT`, then the commands will look like:

  ```
  sqlplus /nolog
  SQL> connect system/manager@PROD as sysdba;
  Connected.
  SQL> connect rman/rman@RMANCAT;
  Connected.
  ```
- For *online backup* only, enable the Oracle automatic log archiving:
  1. Shut down the Oracle target database instance on the application system.
  2. Back up the entire database using a filesystem backup.
  3. Select the location for archive logs:
     - If SPFILE is used:

       Run:

```
alter system set log_archive_dest=path_to_archive_logs
SCOPE=SPFILE;
```

- If the `init.ora` file is used:

  Run:

  `log_archive_start=true`

  `log_archive_dest=`*`path_to_archive_logs`*

  The default path of the file is:

  Windows systems: *`ORACLE_HOME`*`\database\init`*`DB_NAME`*`.ora`

  UNIX systems: *`ORACLE_HOME`*`/dbs/init`*`DB_NAME`*`.ora`

  where *`DB_NAME`* is the name of the Oracle database instance.

4. Mount the target database and to enable the archive log mode, start SQL*Plus and type:

   ```
   startup mount
   alter database archivelog;
   alter database open;
   ```

   Example

   If the user name for the target database is `system`, password `manager`, instance name `PROD`, and the user name and password for the recovery catalog is `rman`, then the commands will look like:

   ```
   sqlplus /nolog
   SQL> connect system/manager@PROD as sysdba;
   Connected.
   SQL> startup mount;
   SQL> alter database archivelog;
   Statement processed.
   SQL> archive log start;
   Statement processed.
   SQL> alter database open;
   ```

5. Back up the entire database.

Backup set method

For backup set method:

- Ensure that the Oracle software on the backup system and application system have the same directory structure. That means that `ORACLE_HOME` for both Oracle installations has to be identical.
- Ensure that the following files are the same on the application system and the backup system. Check also that the permissions are identical as on the application system:

  - `names.ora`

    Default path: *`ORACLE_HOME`*`/network/admin/names.ora`

  - `init`*`DB_NAME`*`.ora`

    Default path: *`ORACLE_HOME`*`/dbs/init`*`DB_NAME`*`.ora`.

  - `orapw`*`DB_NAME`*

    Default path: *`ORACLE_HOME`*`/dbs/orapw`*`DB_NAME`*

  - `admin/`*`DB_NAME`*

    Default path: *`ORACLE_BASE`*`/admin/`*`DB_NAME`*

Ensure that the Oracle net services on the application system and the backup system have the same directory structure. This can be accomplished by either NFS sharing of the files, manually copying the files from the application system to the backup system, or by using the UNIX `rdist` or `tar` commands to distribute the files from the application system.

- Test whether the Oracle user can log in to the Oracle target database as the Oracle database administrator and to the Oracle recovery catalog database as the Oracle recovery catalog owner from the backup system:
  1. Export `ORACLE_HOME`, `DB_NAME`, and on UNIX systems also `SHLIB_PATH` variables.
  2. Using SQL*Plus, connect to the Oracle recovery catalog database by specifying the user (recovery catalog owner), password, and net connect identifier.
  3. Connect to the Oracle target database locally using the Oracle Net software as the Oracle database administrator with the `SYSDBA` role.

     Example

     If the `DB_NAME` of the target database is `PROD`, the `DB_NAME` of the Oracle recovery catalog database is `RMANCAT`, and *`ORACLE_HOME`* is `/oracle/PROD`, then the commands will look like:

```
su - ora
id
uid=101(ora) gid=101(dba)

export DB_NAME=PROD
oracle/PROD/bin/sqlplus
SQL> connect rman/rman@RMANCAT
Connected.

SQL> connect system/manager as sysdba
SQL> connect system/manager@PROD as sysdba;
Connected.
```

- Test whether the user `root` and the Oracle administrator (for example, the user `oracle`) can connect to the target database and the recovery catalog database using the RMAN command on the backup system:
  1. Log on as the Oracle database administrator to the backup system (for example, the user `oracle`).
  2. Execute the RMAN command and connect to the target database and the recovery catalog database.

Example

If the `DB_NAME` of the target database is `PROD`, the `DB_NAME` of the Oracle recovery catalog database is `RMANCAT`, and *`ORACLE_HOME`* is `/oracle/PROD`, then the commands will look like:

```
su - ora
id
uid=101(ora) gid=101(dba)
export DB_NAME=PROD

rman target system/manager catalog rman/rman
Recovery Manager: Release 10.1.0.2.0 - Production
RMAN-06005: connected to target database: PROD
RMAN-06008: connected to recovery catalog database
RMAN> exit
Recovery Manager completed.
```

Configuring the HP P6000 EVA Disk Array Family in ASM environments

Zero downtime backup with the HP P6000 EVA Disk Array Family is supported for ASM configurations, provided that the P6000 EVA Array supports multisnapping. Additionally, to enable zero downtime backup, the following prerequisites must be fulfilled:

- The ASM-managed files that will be backed up must reside on raw disks, not on raw logical volumes.

Note that the maximum number of source disks that can be involved in multisnapping depends on the firmware revision of the P6000 EVA Array that will be used and the installed Command View (CV) version. If the number of source disks selected for a zero downtime backup session exceeds this limitation, the session is aborted. For limitation details, see the HP P6000 EVA Disk Array Family documentation.

Configuring the HP P9000 XP Disk Array Family in ASM environments

In Oracle Server configurations that use Automatic Storage Management (ASM), both ZDB and instant recovery are supported with the HP P9000 XP Disk Array Family, provided that the following prerequisites are met:

- Data files, control files, and redo log files must reside on separate storage volumes (LUNs). This configuration is needed if you plan to perform instant recovery.
- The disk arrays must support the atomic split operation:
  - Each storage volume (LUN) must be composed of a single LDEV.
  - The storage volumes on which the ASM-managed files reside must belong to consistency groups (CTG) that have unique and non-zero IDs. Storage volumes that belong to the same CTG must be selected together in a backup specification. Otherwise, the backup session will fail. If you plan to back up datafiles, control files and log files in separate sessions, the corresponding storage volumes must reside in separate consistency groups.

    Depending on your environment, set the following `omnirc` options on the application system:

    - `SSEA_ATOMIC_SPLIT`
    - `SSEA_ATOMIC_SPLIT_MULTIPLE_CTGROUPS`
    - `SSEA_ATOMIC_SPLIT_MIXED_CONFIG`

    At least one option must be set to enable the atomic split operation. For details, see the online Help index: “omnirc options”.
- If the ASM instance name differs from `+ASM`, specify the correct name by setting the Data Protector `omnirc` option `ORA_ASM_LCL_INSTANCE` on the application system.
- Additional requirements for instant recovery:
  - In a cluster environment, on the active cluster node, set the Data Protector `omnirc` option `ORA_ASM_LCL_INSTANCE` to the name of the ASM instance running on that node.
  - If an Oracle ASM instance manages files of more than one database, you must reconfigure Oracle Server to use a separate ASM disk group for each database.
  - The names of the ASM disk groups should not be changed after the backup.
  - The autoextend feature of the Oracle Server ASM must be disabled.

Cluster-aware systems

In cluster environment, if you intend to use the Data Protector CLI, set the Data Protector environment variable `OB2BARHOSTNAME` to the virtual server name. Set the variable on the Oracle Server system as follows:

Windows systems: `set OB2BARHOSTNAME=virtual_server_name`

UNIX systems: `export OB2BARHOSTNAME=virtual_server_name`

HP-UX with RAC: To enable instant recovery, create an MC/ServiceGuard package containing *only* the virtual IP and the virtual hostname parameters and distribute it among the RAC nodes.

Linking Oracle Server with the Data Protector MML

To use the Data Protector Oracle integration, the Oracle Server software needs to be linked with the Data Protector Oracle integration **Media Management Library** (**MML**) on every system on which an Oracle instance is running.

You do not need to link Oracle Server with the Data Protector MML manually. When you start backups or restores using the Data Protector GUI or CLI, Data Protector automatically links Oracle Server with the correct platform–specific Data Protector MML. However, for testing purposes, you can override this automatic selection. You can manually specify which platform–specific Data Protector MML should be used by setting the Data Protector `SBT_LIBRARY` parameter. On how to set the parameter, see the `util_cmd` man page. The parameter is saved in the Data Protector Oracle instance configuration file.

MML is invoked by the Oracle server when it needs to write to or read from devices using Data Protector.

Configuring Oracle user accounts

Decide under which user accounts you want backups to run. Data Protector requires the following user accounts:

- Oracle operating system user account

  For details, see "Configuring Oracle operating system user accounts" (page 37).
- Oracle database user accounts

  For details, see "Configuring Oracle database users accounts" (page 39).

Configuring Oracle operating system user accounts

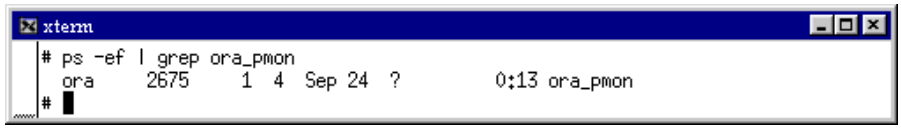
For each Oracle database, Data Protector requires an operating system user account that has Oracle rights to back up the database. This user account usually belongs to the `DBA` user group (**OSDBA user**). The user account under which the Oracle database is running has these rights. For example, to find such a user on UNIX systems, run:

`ps -ef|grep ora_pmon_DB_NAME`

or

`ps -ef|grep ora_lgwr_DB_NAME`

Figure 7 Finding the Oracle user



The following table explains how to configure users on different operating systems:

Client system	Description
UNIX system	Ensure that the Oracle user `oracle` from the Oracle Inventory group (`oinstall`) has been added to the Data Protector `admin` user group. For details on adding users, see the *HP Data Protector Help* index: "adding users". Add the OSDBA user account and `root` user account from both the application system and backup system to the Data Protector `admin` or `operator` user group. The OSDBA user on the backup system must have the same numerical user ID and group ID as the OSDBA user on the application system (for example, `uid=101(ora) gid=101(dba)`). **TIP:** To find the user ID, connect to a system under this user account and run: `#id`
Windows system	On Windows systems, Data Protector connects to the Oracle database using the Data Protector `Inet` service on the related system. By default, the service runs under the `Local System account`, which is automatically added to the Data Protector `admin` user group. However, if you have restarted the Data Protector `Inet` service on the application system and backup system under OSDBA user accounts, you need to add the new users to the Data Protector `admin` or `operator` user group.

For information on adding users to Data Protector user groups, see the *HP Data Protector Help* index: "adding users".

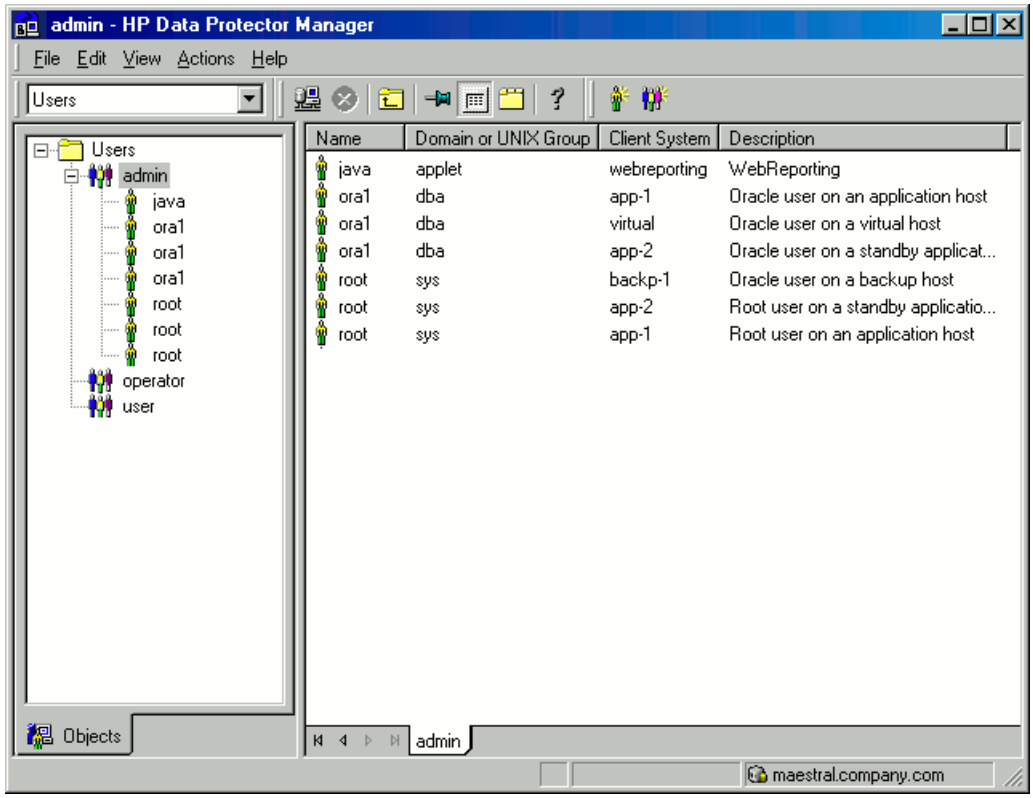
NOTE: The OSDBA user account for the backup system needs to be added to a Data Protector user group only if you plan to use the Oracle backup set ZDB method.

Clusters

In cluster environments, ensure to add he following users to the Data Protector `admin` or `operator` user group:

- OSDBA user for all physical nodes
- OSDBA user for the virtual server (applicable for MC/ServiceGuard clusters)
- **UNIX systems:** `root` user for all physical nodes

Figure 8 Example user configuration in a cluster environment



Configuring Oracle database users accounts

Identify or create the following Oracle database user accounts. You need to provide these user accounts when you configure the Oracle database as described in "Configuring Oracle databases" (page 39).

Table 4 Oracle database user accounts

User	Description
Primary database user	Required to log in to the primary database.
Recovery catalog user	The owner of the recovery catalog (for example, `rman`). Required to log in to the catalog database. Needed if you use the recovery catalog. If you are using Oracle 11g R2 or later, ensure that the owner of the Oracle recovery catalog: • is granted the CREATE ANY DIRECTORY and the DROP ANY DIRECTORY system privileges, which are required to use the Data Pump Export (`expdp`) and the Data Pump Import (`impdp`) utilities. • has SELECT permissions on `sys.v$instance` view. Start SQL*Plus and type: `grant select on v_$instance to recovery_catatalog_user;`
Standby database user	Required to log in to the standby database. Applicable only in Oracle Data Guard environments. Needed to back up the standby database.

Configuring Oracle databases

Configuration of an Oracle database consists of providing Data Protector with the following data:

- Oracle Server home directory
- Login information to the target database
- Optionally, login information to the recovery catalog database
- Optionally, login information to the standby database

- Optionally, ASM-related information.
- Backup method to be used and the related options

During the configuration, the `util_oracle8.pl` command, which is started on the application system, saves the specified parameters in the Data Protector Oracle database specific configuration file on the Cell Manager.

Ensure that the database is open during the configuration procedure and that you are able to connect to the database.

To configure an Oracle database, you can use the Data Protector GUI or the Data Protector CLI.

NOTE: With Oracle Server configurations using ASM, to be able to perform instant recovery, the Oracle database must be configured using the Data Protector CLI. This is because the ASM-related parameters cannot be set using the Data Protector GUI. However, if you plan to perform ZDB sessions only, without instant recovery, the database can also be configured using the Data Protector GUI.

Using the Data Protector GUI

Configure an Oracle database when you create the first ZDB backup specification for the database. Start with the procedure described in "Creating backup specifications" (page 50) and at Step 6 proceed as follows:

1. In the **Configure Oracle** dialog box and in the **General** page, specify the pathname of the Oracle Server home directory.

Figure 9 Configuring Oracle - General (Windows)

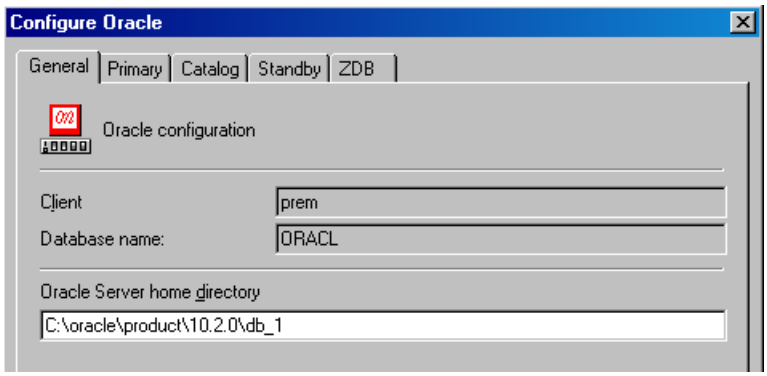
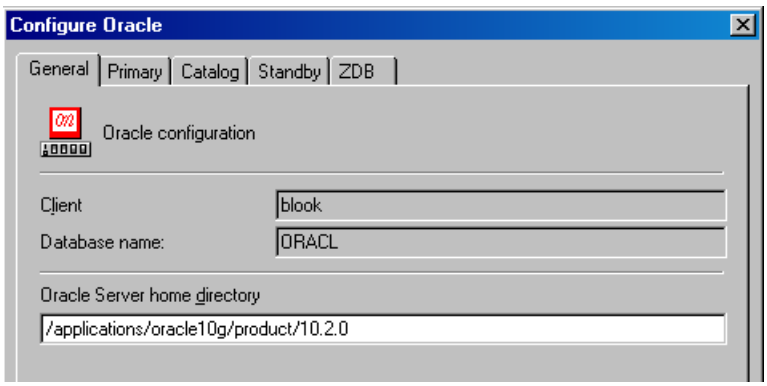


Figure 10 Configuring Oracle - General (UNIX)



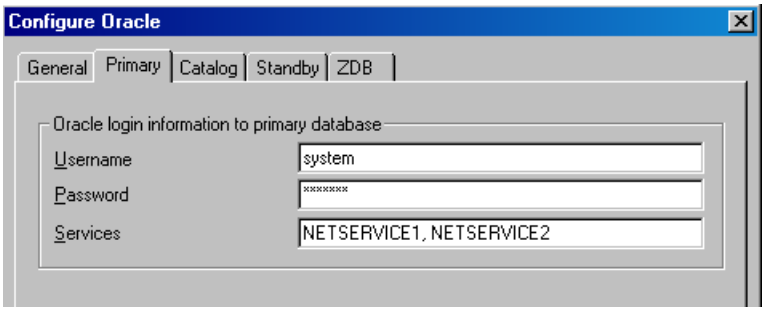
2. In the **Primary** page, specify the login information to the primary database.

   Note that the user must have the `SYSDBA` privilege granted.

   In **Services**, type the net service name for the primary database instance. The backup will be performed on the system where this database instance resides.

RAC: List all net services names for the primary database separated by a comma.

Figure 11 Configuring Oracle - Primary



3. In the **Catalog** page, select **Use target database control file instead of recovery catalog** to use the primary database control file.

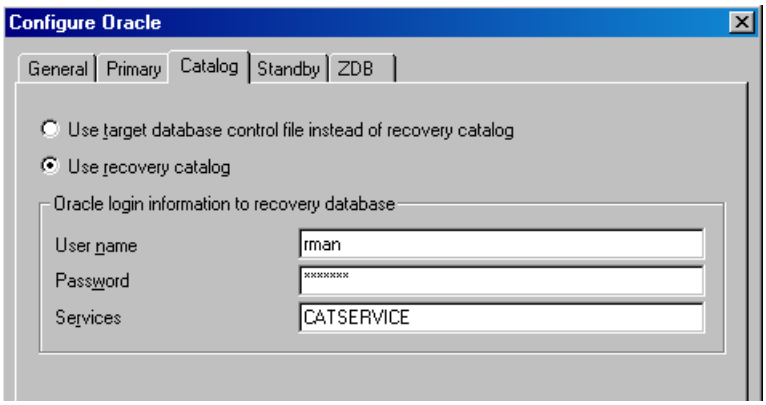
   To use the recovery database catalog as an RMAN repository for backup history, select **Use recovery catalog** and specify the login information to the recovery catalog.

   Note that for ZDB, you must use the recovery catalog.

   The user specified must be the owner of the recovery catalog.

   In **Services**, type the net service name for the recovery catalog.

Figure 12 Configuring Oracle - Catalog



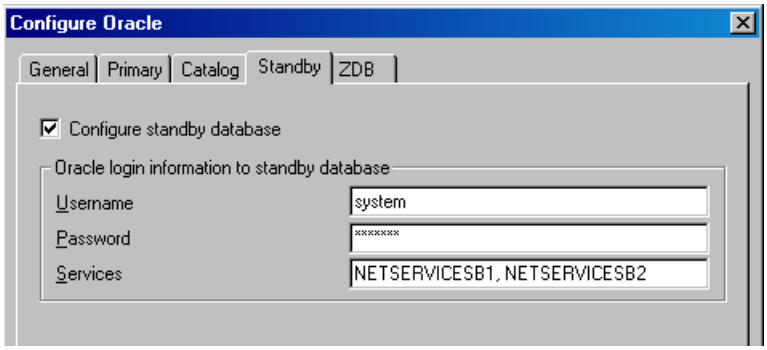
4. If you have Oracle Data Guard configuration for *non-ZDB sessions* and if you intend to back up a standby database, configure also the standby database:

   In the **Standby** page, select **Configure standby database** and specify the login information to the standby database.

   In **Services**, type the net service name for the standby database instance.

   RAC: List all net services names for the standby database separated by a comma.

Figure 13 Configuring Oracle - Standby



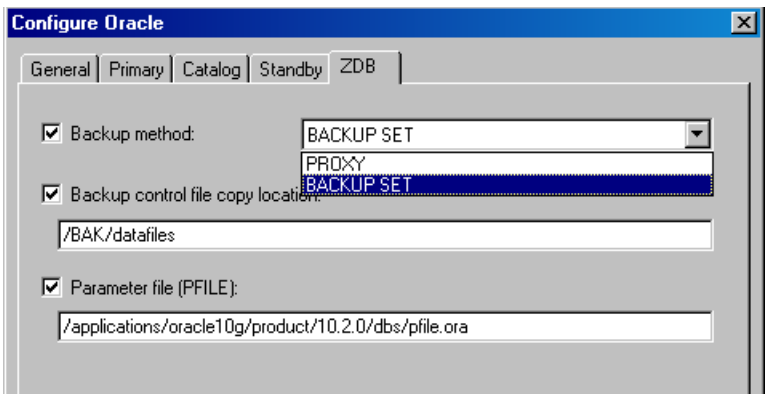
5. In the **ZDB** page, select **Backup method** and then select **PROXY** or **BACKUP SET** in the drop-down list.

   In **Backup control file copy location**, you can specify the location on the source volumes where a backup copy of the current control file will be made during ZDB to disk.

   If you do not specify the location, `ob2rman.pl` will copy the copy of the control file from the application system to the backup system when it is needed. Thus, you do not need to create an additional disk for this location if you do not need the control file copy on a replica.

   If your backup method is *backup set* and if your database instance uses PFILE (and not SPFILE), select the **Parameter file (PFILE)** option and specify the pathname of `PFILE` residing on the application system.

Figure 14 Configuring Oracle - ZDB



   Click **OK**.

The Oracle database is configured. Exit the GUI or proceed with creating the backup specification at Step 7.

Using the Data Protector CLI

1. On UNIX systems, log on to the Oracle Server system with an OSDBA user account.
2. On the Oracle Server system, execute:

   Windows systems:

   ```
   perl -I..\lib\perl util_oracle8.pl -config -dbname DB_NAME -orahome
   ORACLE_HOME PRIMARY_DB_LOGIN [CATALOG_DB_LOGIN] [STANDBY_DB_LOGIN]
   [ZDB_OPTIONS] [ASM_OPTIONS] [-client CLIENT_NAME]
   ```

   UNIX systems:

   ```
   util_oracle8.pl -config -dbname DB_NAME -orahome ORACLE_HOME
   PRIMARY_DB_LOGIN [CATALOG_DB_LOGIN] [STANDBY_DB_LOGIN] [ZDB_OPTIONS]
   [ASM_OPTIONS] [-client CLIENT_NAME]
   ```

where:

PRIMARY_DB_LOGIN is:

-prmuser *PRIMARY_USERNAME*

-prmpasswd *PRIMARY_PASSWORD*

-prmservice *PRIMARY_NET_SERVICE_NAME_1*[,*PRIMARY_NET_SERVICE_NAME_2 ...*]

CATALOG_DB_LOGIN is:

-rcuser *CATALOG_USERNAME*

-rcpasswd *CATALOG_PASSWORD*

-rcservice *CATALOG_NET_SERVICE_NAME*

STANDBY_DB_LOGIN is:

-stbuser *STANDBY_USERNAME*

-stbpasswd *STANDBY_PASSWORD*

-stbservice *STANDBY_NET_SERVICE_NAME_1*[,*STANDBY_NET_SERVICE_NAME_2 ...*]

ZDB_OPTIONS are:

-zdb_method {PROXY | BACKUP_SET}

[-ctlcp_location *BACKUP_CONTROL_FILE_COPY_LOCATION*]

[-pfile *PARAMETER_FILE*]

[-bkphost *BACKUP_SYSTEM*]

ASM_OPTIONS are:

[-asmhome *ASM_HOME*]

[-asmuser *ASM_USER* -asmpasswd *ASM_PASSWORD* -asmservice *ASM_NET_SERVICE_NAME_1*[,*ASM_NET_SERVICE_NAME_2 ...*]]

If you have Oracle Data Guard configuration for *non-ZDB sessions* and if you intend to back up a standby database, you must provide the *STANDBY_DB_LOGIN* information.

To configure an Oracle database for ZDB, you must provide the *ZDB_OPTIONS* information. If your ZDB method is *backup set*, you must also provide the *BACKUP_SYSTEM* information.

The *ASM_OPTIONS* options are needed for instant recovery in Oracle Server configurations that use Automatic Storage Management (ASM).

Parameter description

CLIENT_NAME

Name of the Oracle Server system with the database to be configured. It must be specified in a cluster environment or if the ZDB configuration is run on the backup system.

RAC: The virtual server of the Oracle resource group.

Oracle Data Guard: Name of either a primary system or secondary (standby) system.

DB_NAME

Name of the database to be configured.

ORACLE_HOME

Pathname of the Oracle Server home directory.

PRIMARY_USERNAME PRIMARY_PASSWORD

Username and password for login to the target or primary database. Note that the user must have the SYSDBA privilege granted.

PRIMARY_NET_SERVICE_NAME_1 [,*PRIMARY_NET_SERVICE_NAME_2, ...*]

Net services names for the primary database.

RAC: Each net service name must resolve into a specific database instance.

CATALOG_USERNAME CATALOG_PASSWORD

Username and password for login to the recovery catalog. This is optional and is used only if you use the recovery catalog database as an RMAN repository for backup history.

CATALOG_NET_SERVICE_NAME

Net service name for the recovery catalog.

STANDBY_USERNAME STANDBY_PASSWORD

This is used in Oracle Data Guard environment for backing up a standby database. Username and password for login to the standby database.

STANDBY_NET_SERVICE_NAME_1 [,*STANDBY_NET_SERVICE_NAME_2, ...*]

Net services names for the standby database.

BACKUP_CONTROL_FILE_COPY_LOCATION

A location on a source volume where a copy of the current control file is made before a ZDB to disk. This is optional and if not specified, `ob2rman.pl` will copy the copy of the control file from the application system to the backup system when it is needed. Thus, you do not need to create an additional disk for this location if you do not need the control file copy on a replica.

PARAMETER_FILE

Full pathname of the PFILE residing on the application system. This is optional and used if backup method is backup set and the database instance uses PFILE (and not SPFILE).

BACKUP_SYSTEM

Name of the backup system. It must be specified for a ZDB backup set configuration.

ASM_HOME

Home directory of the ASM instance in an Oracle ASM configuration. Specify this option if the value differs from the home directory of the Oracle database instance.

ASM_USERNAME ASM_PASSWORD

User name and password (authentication credentials) used by the Data Protector Oracle integration agent to connect to the ASM database.

ASM_NET_SERVICE_NAME_1[,*ASM_NET_SERVICE_NAME_2 ...*]

Name of the net service to be used to access the ASM database. For Oracle environments involving multiple net services, multiple names can be specified.

The message `*RETVAL*0` indicates successful configuration, even if followed by additional messages.

NOTE: If you need to export some variables before starting SQL*Plus, these variables must be defined in the `Environment` section of the Data Protector Oracle global configuration file or using the Data Protector GUI.

Example

The following example represents configuration on a UNIX system of an Oracle database and its recovery catalog with the backup set method used and the parameter file location specified.

The following names are used in the example:

- database name: `oracle`
- Oracle Server home directory: `/app10g/oracle10g/product/10.1.0`
- primary user name: `system`
- primary password: `manager`
- primary net service name 1: `netservice1`
- primary net service name 2: `netservice2`

- recovery catalog user name: `rman`
- recovery catalog password: `manager`
- recovery catalog net service name: `catservice`
- backup system name: `bcksys`

Syntax

```
/opt/omni/lbin/util_oracle8.pl -config -dbname oracle -orahome
/app10g/oracle10g/product/10.1.0 -prmuser system -prmpasswd manager
-prmservice netservice1,netservice2 -rcuser rman -rcpasswd manager
-rcservice catservice -zdb_method BACKUP_SET -pfile
/app10g/oracle10g/product/10.1.0/dbs/pfile.ora -bkphost bcksys
```

Example

The following example shows how to configure an Oracle database in a cluster environment. The database files are managed by ASM. The configuration enables instant recovery in ASM environments:

- Database name: `SUN`
- Oracle Server home directory: `/orahome/ora/app/oracle/product/11.2.0/dbhome_1`
- Primary user name: `sys`
- Primary password: `oracle`
- Primary net service name 1: `SUN1`
- Primary net service name 2: `SUN2`
- Recovery catalog user name: `rman`
- Recovery catalog password: `manager`
- Recovery catalog net service name: `RECO`
- ZDB method: Backup set
- Oracle Server system (cluster virtual system): `cluster.company.com`
- Backup system: `backup.company.com`
- ASM home directory: `/oracle/crshome/crshome/crs/app/11.2.0/grid`
- ASM user: `sys`
- ASM user password: `oracle`
- ASM net service name 1: `ASMSRV1`
- ASM net service name 2: `ASMSRV2`

To configure the database, execute:

```
opt/omni/lbin/util_oracle8.pl -config -dbname SUN -orahome
/orahome/ora/app/oracle/product/11.2.0/dbhome_1 -prmuser sys -prmpasswd
oracle -prmservice SUN1,SUN2 -rcuser rman -rcpasswd manager -rcservice
RECO -zdb_method BACKUP_SET -bkphost backup.company.com -client
cluster.company.com -asmhome /crshome/crs/app/11.2.0/grid –asmuser sys
–asmpasswd oracle –asmservice ASMSRV1, ASMSRV2
```

Checking the configuration

You can check the configuration of an Oracle database after you have created at least one backup specification for the database. If you use the Data Protector CLI, a backup specification is not needed.

Using the Data Protector GUI

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

IMPORTANT: Data Protector does not check if the specified user has appropriate Oracle backup permissions.

Using the Data Protector CLI

1. On UNIX systems, log on to the application system with an OSDBA user account.
2. Execute:

   Windows systems:

   ```
   perl -I..\lib\perl util_oracle8.pl -chkconf_smb -dbname DB_NAME
   ```

   UNIX systems:

   ```
   util_oracle8.pl -chkconf_smb -dbname DB_NAME
   ```

Handling errors

If an error occurs, the error number is displayed in the form `*RETVAL*error_number`.

To get the error description, on the Cell Manager, execute:

Windows systems: `Data_Protector_home\bin\omnigetmsg 12 error_number`

UNIX systems: `/opt/omni/lbin/omnigetmsg 12 error_number`

IMPORTANT: On UNIX systems, it is possible that although you receive `*RETVAL*0`, backup still fails because Data Protector does not check if the specified user has appropriate Oracle backup permissions.

Checking configuration for instant recovery

Check if the Oracle configuration is suitable for instant recovery.

On the application system, execute:

Windows systems:

```
perl util_oracle8.pl -chkconf_ir -dbname DB_NAME
```

UNIX systems:

```
util_oracle8.pl -chkconf_ir -dbname DB_NAME
```

If the control files, SPFILE, and online redo logs are on the same volume group (if LVM is used) or source volume as datafiles, a warning is displayed stating that instant recovery is not possible. You can either:

- Reconfigure the Oracle database instance. See "Reconfiguring an Oracle instance for instant recovery" (page 252) on how to move the control files and redo logs to source volumes that are not replicated.

  Or:

- Set the `ZDB_ORA_INCLUDE_CF_OLF`, `ZDB_ORA_INCLUDE_SPF`, and `ZDB_ORA_NO_CHECKCONF_IR` `omnirc` options and ignore the warning. However, note that the control file, SPFILE, and online redo logs are overwritten during instant recovery. See "ZDB integrations omnirc options" (page 254) on how to set the `omnirc` options.

Setting environment variables

Use environment variables to modify backup environment to suit your needs. Environment variables are Oracle database specific. It means that they can be set differently for different Oracle databases. Once specified, they are saved to related Data Protector Oracle database configuration files.

For details of how environment variables affect your environment, see Table 5 (page 47).

NOTE: Environment variables are not supported on HP OpenVMS systems.

Table 5 Environment variables

Environment variable	Default value	Description
OB2_RMAN_COMMAND_TIMEOUT	300 s	This variable is applicable when Data Protector tries to connect to a target or catalog database. It specifies how long (in seconds) Data Protector waits for RMAN to respond that the connection succeeded. If RMAN does not respond within the specified time, Data Protector aborts the current session.
OB2_SQLP_SCRIPT_TIMEOUT	300 s	This variable is applicable when Data Protector issues an SQL*Plus query. It specifies how long Data Protector waits for SQL*Plus to respond that the query completed successfully. If SQL*Plus does not respond within the specified time, Data Protector aborts the current session.
OB2_DPMCTL_SHRLOC	N/A	Defines the location at which the control file is created and from where it is backed up in Data Protector managed control file backup. Data Protector copies the control file to the directory /var/opt/omni/tmp (UNIX systems) or *Data_Protector_program_data*\tmp (Windows systems) by default. This variable overrides the default directory with a customer-specified directory. In an Oracle Real Application Clusters (RAC) environments with Oracle version 11.2.0.2 or later, to enable Data Protector managed control file backups and the corresponding restore sessions, ensure this directory resides on a shared disk that all RAC nodes can access.

To set environment variables, use the Data Protector GUI or CLI.

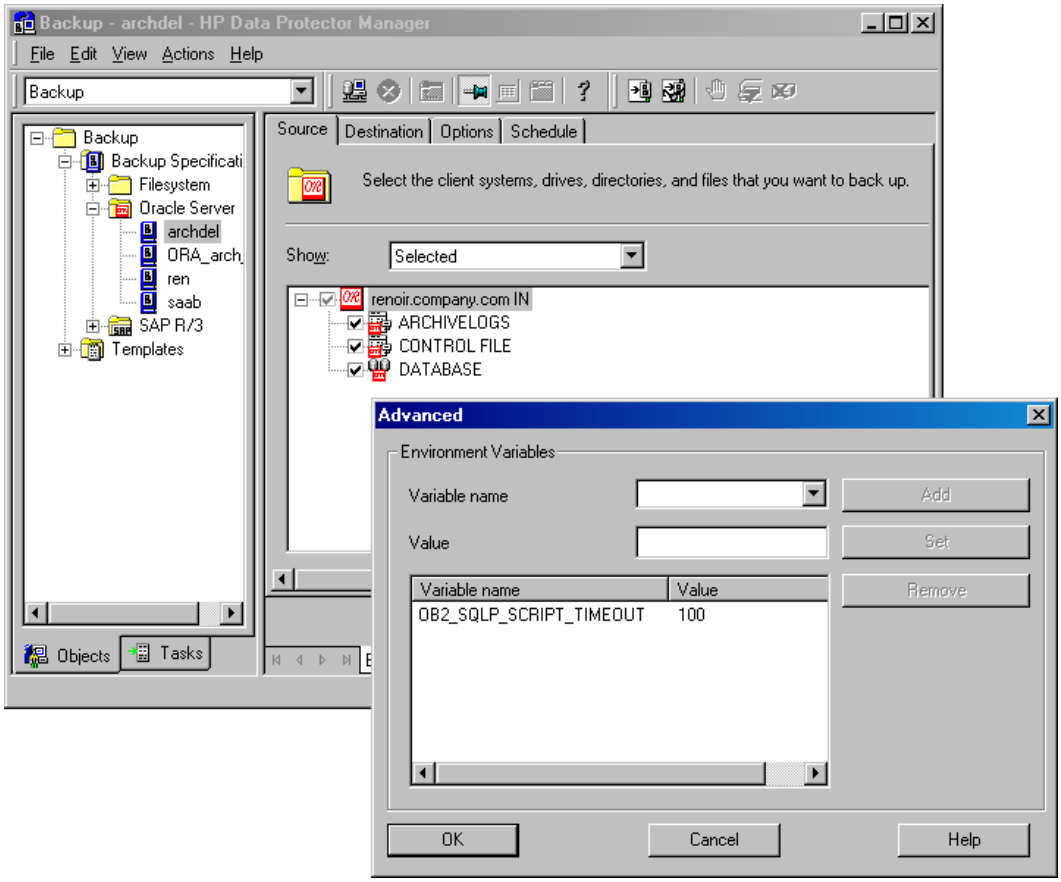
Using the Data Protector GUI

You can set a variable when you create a backup specification or modify an existing one:

1. In the Source page of the backup specification, right-click the Oracle database at the top and click **Set Environment Variables**.

2. In the Advanced dialog box, specify the variable name, its value, and click **Add**. See Figure 15 (page 48).

Figure 15 Setting environment variables



Click **OK**.

Using the Data Protector CLI

Execute:

```
util_cmd -putopt Oracle8 DatabaseName Variable Value -sublist Environment
```

For details, see the `util_cmd` man page or the *HP Data Protector Command Line Interface Reference*.

Example

To set the environment variable `OB2_RMAN_COMMAND_TIMEOUT` to `100` seconds for the Oracle database `INST2`, execute:

```
util_cmd -putopt Oracle8 INST2 OB2_RMAN_COMMAND_TIMEOUT 100 -sublist
Environment
```

Switching between Oracle backup methods

You can switch between the Oracle backup methods by reconfiguring the Data Protector Oracle integration for each database. It is *not* possible to select the method during the backup specification creation.

IMPORTANT: When switching between the Oracle backup set and proxy-copy methods, you must carefully follow the instructions given bellow to ensure a successful switch between both methods and to ensure that during a restore or recovery RMAN does not select backup objects backed up using different methods in one restore session. If such a mixed set is used, the restore procedure will fail.

To switch between the backup methods:

1. Successfully back up the entire database using the *currently* selected method.
2. To avoid selecting backup specifications with a backup method different than the current backup method, you may remove or move all ZDB backup specifications belonging to the selected database instance. The backup specifications are located on the Cell Manager in:

   Windows systems:
   `Data_Protector_program_data\Config\Server\BarLists\Oracle8`

   UNIX systems: `/etc/opt/omni/server/barlists/oracle8`
3. Re-configure the database with the n*ew method* selected while creating a new Oracle ZDB specification.
4. Optionally, if you switch *from backup set to proxy-copy*, you may:
   a. On the Cell Manager, remove the file:

      Windows systems: `Data_Protector_program_data\Config\Server\Integ\Config\Oracle8\client_name%initDB_NAME_bckp.ora`

      UNIX systems: `/etc/opt/omni/server/integ/config/Oracle8/client_name%initDB_NAME_bckp.ora`

   b. Remove the Oracle software from the backup system.
5. Perform ZDB of the entire database.

IMPORTANT: If you need to perform a restore from a time between the start and the end of the first backup of the entire database using the new backup method, RMAN may try to use backup files from old method through a channel allocated for the files from the old method and the restore will fail. See "Problem" (page 99) on how to restore such a backup.

Backup

To configure an Oracle ZDB, perform the following steps:

1. Configure the devices you plan to use for a backup. For instructions, see the *HP Data Protector Help* index: "configuring devices".
2. Configure media pools and media for a backup. For instructions, see the *HP Data Protector Help* index: "creating media pools".
3. Ensure you are able to connect to the database.
4. Configure a non-ZDB backup specification and run the backup of Oracle data on the application system to verify that you have properly configured the Oracle environment. On how to create a non-ZDB backup specification, see the *HP Data Protector Integration Guide for Oracle and SAP*.
5. Create a Data Protector Oracle ZDB backup specification. See "Creating backup specifications" (page 50).

Creating backup specifications

Online ZDB

To perform an online ZDB of an Oracle database, the database has to run in the ARCHIVELOG mode.

Offline ZDB

To perform an offline ZDB, create only a ZDB backup specification.

Cluster-aware systems

Before you perform an *offline* ZDB in a cluster environment, take the Oracle Database resource offline and bring it back online after the replica is created. This can be done using the Oracle `fscmd` command line interface commands in the `Pre-exec` and `Post-exec` commands for the client system in a particular backup specification, or by using the Cluster Administrator.

You cannot perform a ZDB of the archived redo log files. Therefore, you need to create two backup specifications:

- ZDB backup specification for backing up database files
- standard Data Protector Oracle integration backup specification for backing up the application system archived log files

Procedure

To create an Oracle ZDB backup specification:

1. In the Context List, click **Backup**.
2. In the Scoping Pane, expand **Backup Specifications**, right-click **Oracle Server**, and click **Add Backup**.
3. In the Create New Backup dialog box, select the following:

Backup set method

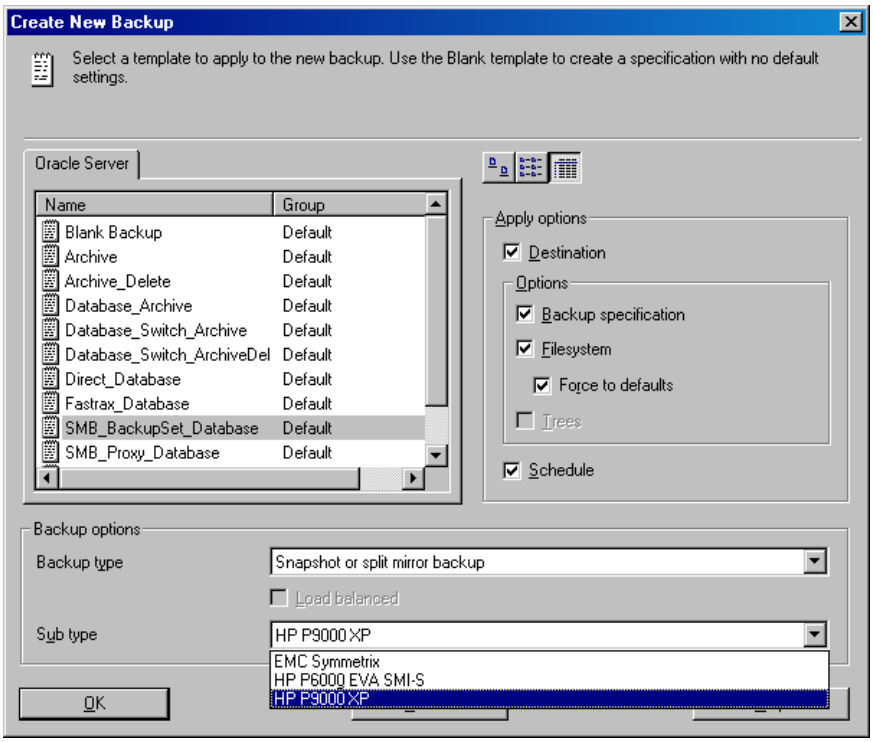
To perform a ZDB of the entire database using the backup set method, select the **SMB_BackupSet_Database** template.

Proxy-copy method

To perform a ZDB of the entire database using the proxy-copy method, select the **SMB_Proxy_Database** template.

From the **Backup type** drop-down list, select **Snapshot or split mirror backup**, and from the **Sub type** drop-down list, select the appropriate disk array agent. The agent must be installed on the application system and the backup system. See "Selecting an Oracle backup template and the snapshot or split mirror backup" (page 51).

Figure 16 Selecting an Oracle backup template and the snapshot or split mirror backup



Click **OK**.

4. In **Application system**, select the Data Protector Oracle integration client. In a non-RAC cluster environment, select the virtual server.

   RAC: Select the virtual server of the Oracle resource group.

   In **Backup system**, select the backup system.

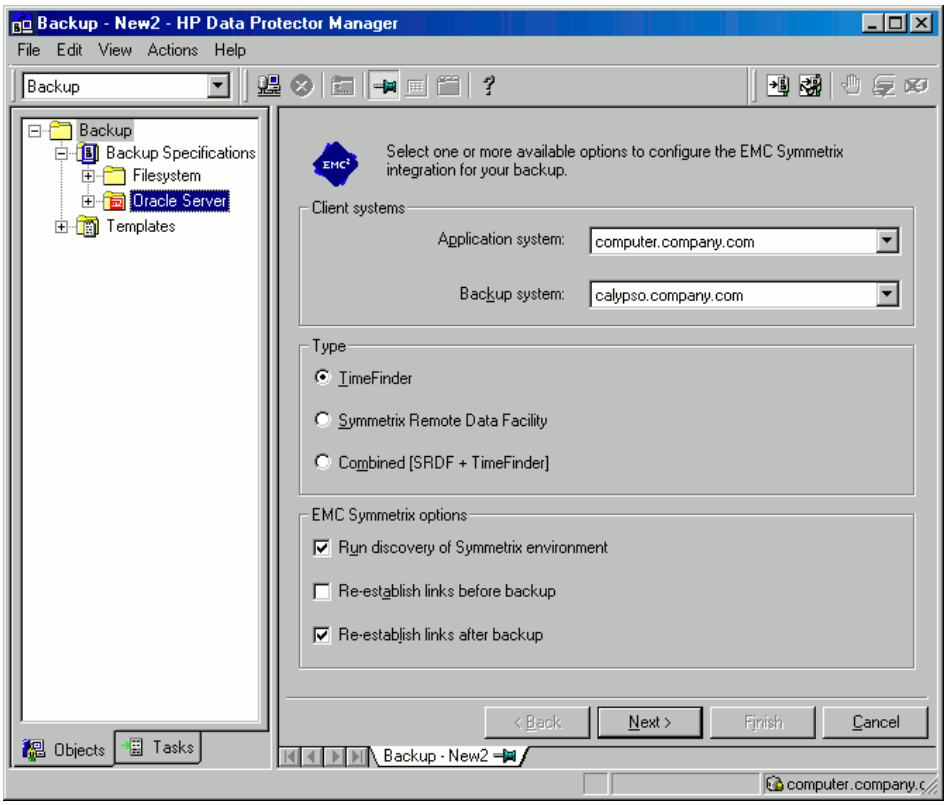
   Select other disk array-specific backup options (see "EMC backup options" (page 52) for EMC, "P9000 XP Array backup options" (page 52) for P9000 XP Array, or "P6000 EVA Array backup options" (page 53) for P6000 EVA Array. For detailed information on the backup options, press **F1**.

EMC GeoSpan specifics

In the EMC GeoSpan for Microsoft Cluster Service environment, select the backup system for the active node and specify the TimeFinder configuration.

After a failover in EMC GeoSpan for MSCS, select the backup system for the currently active node and save the backup specification.

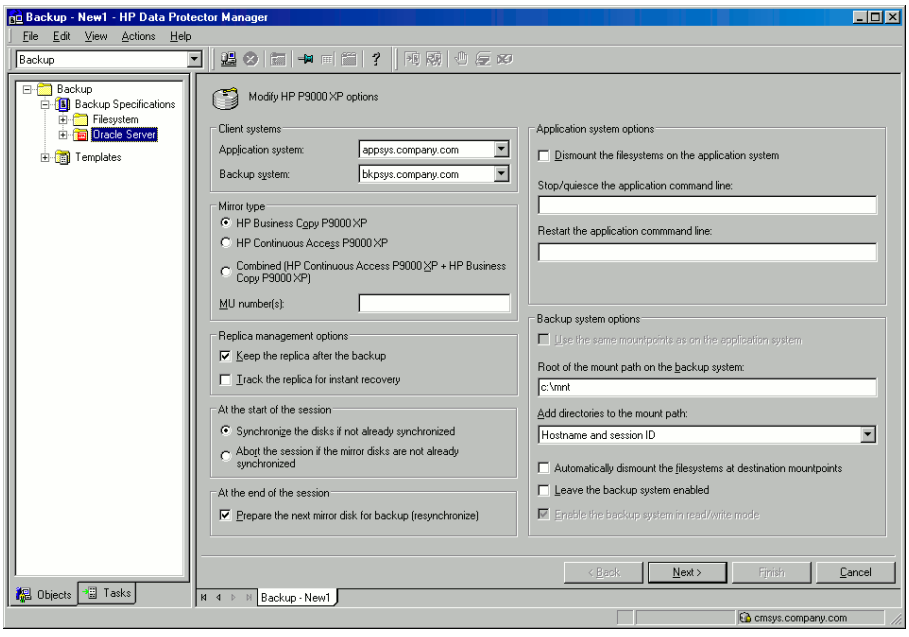
Figure 17 EMC backup options



P9000 XP Array specifics

To enable instant recovery, leave the **Track the replica for instant recovery** option selected. It is not possible to run instant recovery with Data Protector if this option is cleared.

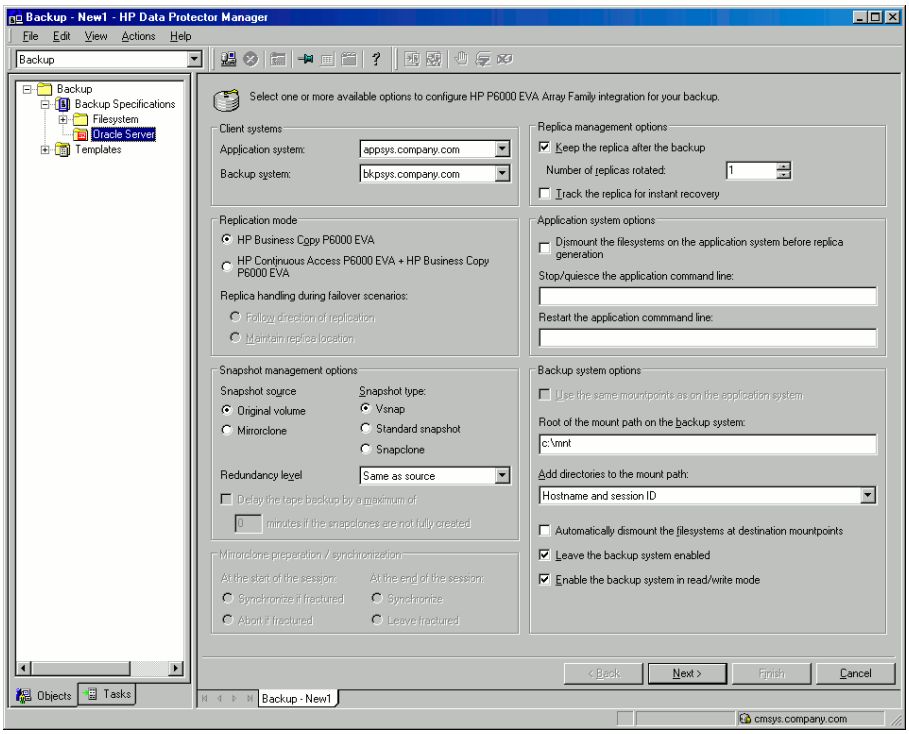
Figure 18 P9000 XP Array backup options



P6000 EVA Array specifics

To enable instant recovery, select the **Track the replica for instant recovery** option.

Figure 19 P6000 EVA Array backup options



Click **Next**.

5. In **Application database**, type the name of the database to be backed up.

   The database name can be obtained using SQL*Plus:

   ```
   SQL>select name from v$database;
   ```

   NOTE: In a single-instance configuration, the database name is usually the same as its instance name. In this case, the instance name can be also used. The instance name can be obtained as follows:

   ```
   SQL>select instance_name from v$instance;
   ```

   Specify the **User and group/domain** options, which are available on UNIX and Windows Server 2008 systems, as follows:

   - ***UNIX systems:*** In **Username** and **Group/Domain name**, specify the OSDBA user account under which you want the backup to start (for example, the user name `ora`, group `DBA`). This user must be configured as described in "Configuring Oracle user accounts" (page 37).
   - ***Windows Server 2008 systems:*** It is not mandatory to specify these options and if they are not specified, the backup runs under the Local System Account.

     In **Username** and **Group/Domain name**, specify the operating system user account under which you want the backup session to run (for example, the user name `Administrator`, domain `DP`). This user must be set up for the `Data Protector Inet` service user impersonation.

     For details on setting accounts for the Inet service user impersonation, see the *HP Data Protector Help* index: "Inet user impersonation".

   Ensure that this user has been added to the Data Protector `admin` or `operator` user group and has the Oracle database backup rights. This user becomes the backup owner.

   NOTE: If this is not your first backup specification, Data Protector fills in **Username** and **Group/Domain name** for you, providing the values of the last configured Oracle database.

Figure 20 Specifying an Oracle Server system (Windows)

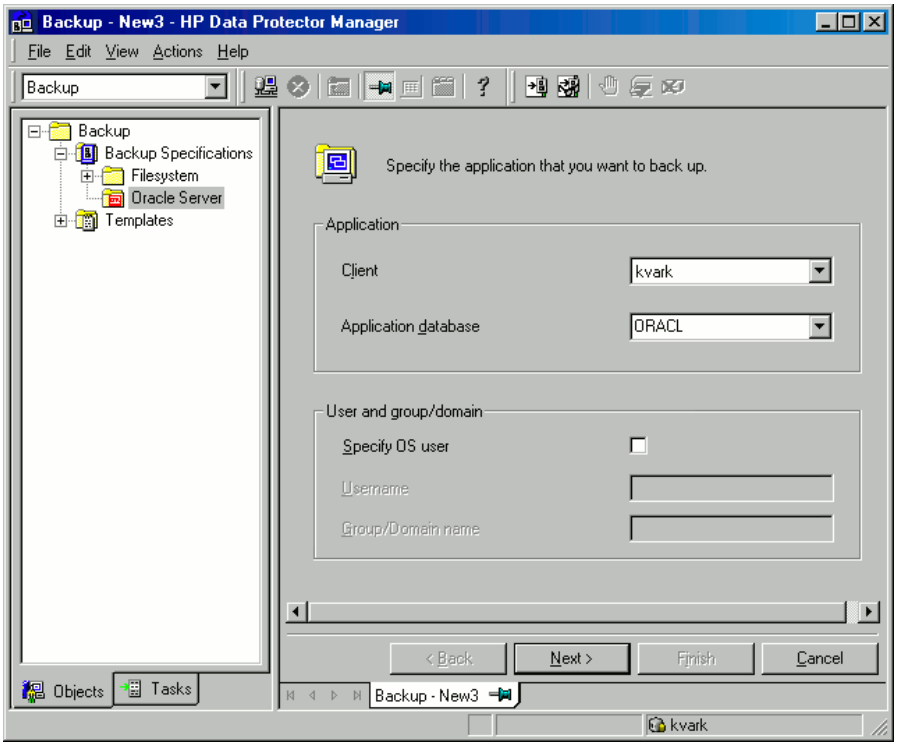
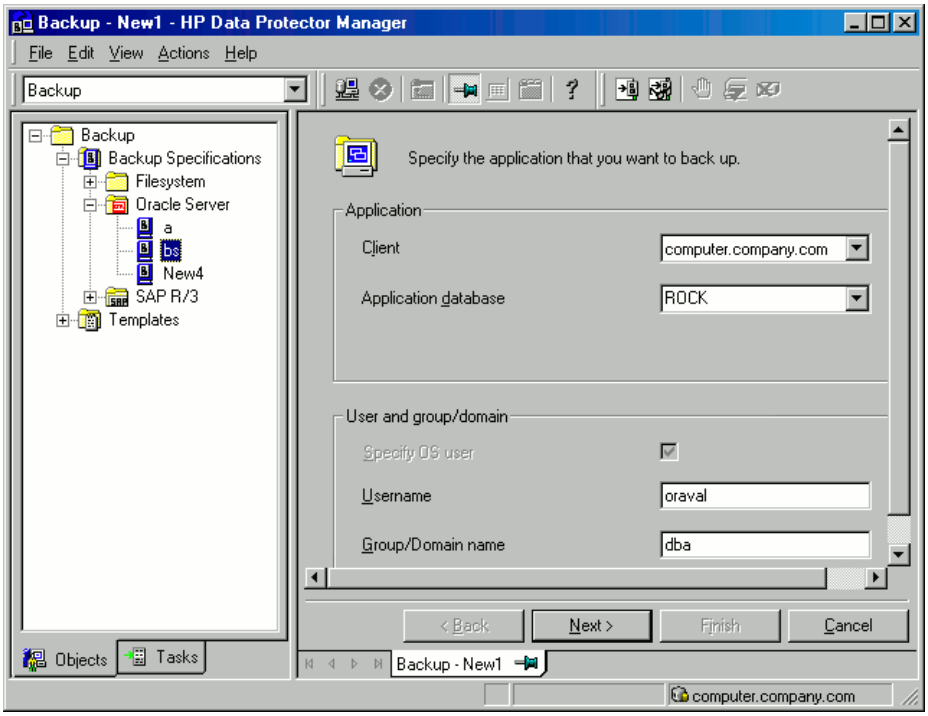


Figure 21 Specifying an Oracle Server system (UNIX)



Click **Next**.

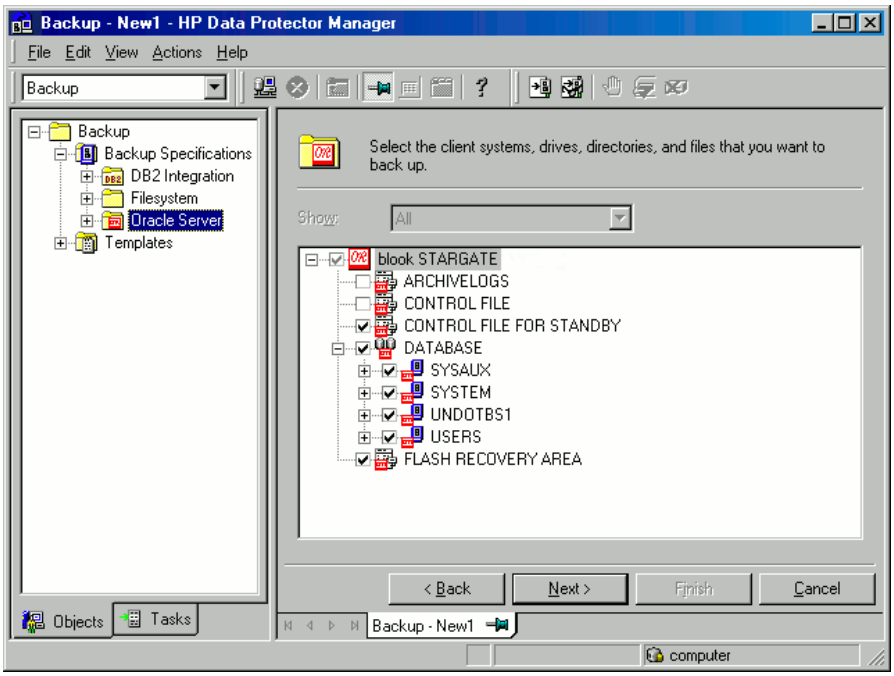
NOTE: When you click **Next**, Data Protector performs a configuration check.

UNIX systems: The check is started under the specified OSDBA user account. If it completes successfully, the OSDBA user and group are also saved in both the Oracle database specific configuration file and Oracle system global configuration file, overriding previous values if they exist.

6. If the Oracle database is not configured yet for use with Data Protector, the Configure Oracle dialog box is displayed. Configure the Oracle database for use with Data Protector as described in "Configuring Oracle databases" (page 39).
7. Select the Oracle database objects to be backed up.

NOTE: Since temporary tablespaces do not contain permanent database objects, RMAN and Data Protector do not back them up. For more information, see the Oracle documentation.

Figure 22 Selecting backup objects



Click **Next**.

If the backup method configured for this instance does not correspond to the method in the backup specification, Data Protector will display a warning and abort the configuration.

8. Select the device(s) you want to use for the backup. Click **Properties** to set the device concurrency, media pool, and preallocation policy. For more information on these options, click **Help**.

   You can also specify whether you want to create additional copies (mirrors) of the backup during the backup session. Specify the desired number of mirrors by clicking the **Add mirror** and **Remove mirror** buttons. Select separate devices for the backup and for each mirror.

   For detailed information on the object mirror functionality, see the *HP Data Protector Help* index: "object mirroring".

NOTE: Object mirroring is not supported for ZDB to disk.

Click **Next** to proceed.

9. Set the backup options.

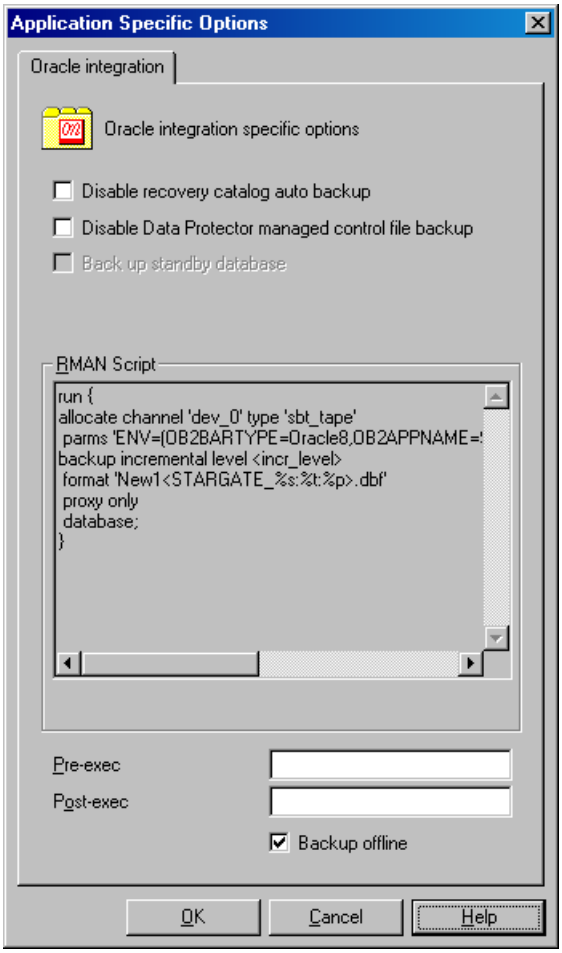
   For information on other the Backup Specification Options and Common Application Options, press **F1**.

Offline ZDB

To perform an offline ZDB, select the **Backup offline** option in the Application Specific Options dialog box. This option stops the database before creating a replica, and restarts it after the replica is created. Note that if a ZDB-to-tape or ZDB-to-disk+tape session is being performed,

the database is not offline during the actual backup to tape. See “Backup offline option ” (page 56).

Figure 23 Backup offline option



For information on other Application Specific Options, see “Oracle backup options” (page 57) or press **F1**.

Click **Next**.

10. Optionally, schedule the backup. For more details, see “Scheduling backup sessions” (page 61).

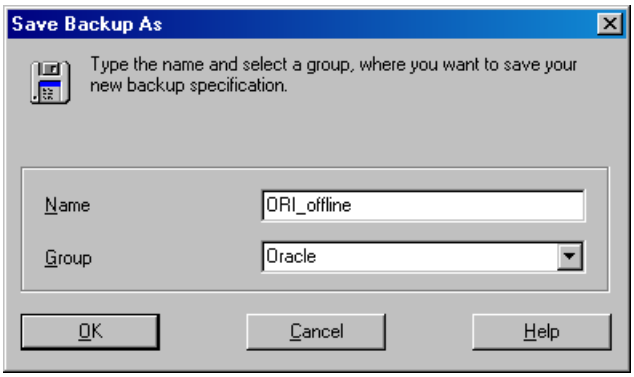
    Note that only the **Full** backup type is supported.

    Click **Next**.

11. Save the backup specification. It is recommended that you save all Oracle backup specifications in the **Oracle** group.

IMPORTANT: The word `DEFAULT` is a reserved word and therefore must not be used for backup specification names or labels of any kind. Therefore, do not use a punctuation in the names of backup specifications, since the Oracle channel format is created from the backup specification name.

Figure 24 Saving the backup specification



Click **OK**.

To start the backup, see "Starting backup sessions" (page 61).

12. For **online backup**, create also a standard Data Protector Oracle integration backup specification for backing up the application system archived log files. See the *HP Data Protector Integration Guide*.

TIP: The backup specification for the backup of archived log files can be either triggered by the **Post-Exec** command defined in the ZDB backup specification for the backup of database files (recommended), or started manually after the ZDB backup specification has been started. See the *HP Data Protector Help* index: "pre- and post-exec commands" for more information on configuring the **Pre-Exec** and **Post-Exec** commands.

Table 6 Oracle backup options

Disable recovery catalog auto backup	By default, Data Protector backs up the recovery catalog after every ZDB to tape or ZDB to disk+tape. Select this option to disable backup of the recovery catalog.
Disable Data Protector managed control file backup	By default, Data Protector backs up the Data Protector managed control file after every ZDB to tape or ZDB to disk+tape. Select this option to disable backup of the Data Protector managed control file.
Back up standby database	This option is ignored for ZDB.
RMAN Script	You can edit the Oracle RMAN script section of the Data Protector Oracle backup specification. The script is created by Data Protector during the creation of a backup specification and reflects the backup specification's selections and settings. You can edit the script only after the backup specification has been saved. For information on how to edit the RMAN script section, see "Editing the Oracle RMAN script" (page 58).
Pre-exec, Post-exec	Specify a command or RMAN script that will be started by `ob2rman.pl` on the Oracle Server system before the backup (`pre-exec`) or after it (`post-exec`). RMAN scripts must have the `.rman` extension. Do not use double quotes. For example, you can provide scripts to shut down and start up an Oracle instance. For examples of shut-downing and starting an Oracle instance on a UNIX system, see "Examples of pre-exec and post-exec scripts on UNIX systems" (page 58). Provide the pathname of the command or RMAN script.
Backup offline	Select this option to perform an offline ZDB session. This option stops the database before creating a replica, and restarts it after the replica is created. See "Backup offline option " (page 56).

Examples of pre-exec and post-exec scripts on UNIX systems

Pre-exec example

The following is an example of a script that *shuts down* an Oracle instance:

```
#!/bin/sh
export ORACLE_HOME=$2
export ORACLE_SQLNET_NAME=$1
if [ -f $ORACLE_HOME/bin/sqlplus ]; then
$ORACLE_HOME/bin/sqlplus << EOF
connect sys/manager@$ORACLE_SQLNET_NAME as sysdba
shutdown
EOF
echo "Oracle database \"$DB_NAME\" shut down."
exit 0
else
echo "Cannot find Oracle SQLPLUS ($ORACLE_HOME/bin/sqlplus)."
exit 1
fi
```

Post-exec example

The following is an example of a script that *starts* an Oracle instance:

```
#!/bin/sh
export ORACLE_HOME=$2
export ORACLE_SQLNET_NAME=$1
if [ -f $ORACLE_HOME/bin/sqlplus ]; then
$ORACLE_HOME/bin/sqlplus << EOF
connect sys/manager@$ORACLE_SQLNET_NAME as sysdba
startup
EOF
echo "Oracle database \"$DB_NAME\" started."
exit 0
else
echo "Cannot find Oracle SQLPLUS ($ORACLE_HOME/bin/sqlplus)."
exit 1
fi
```

Editing the Oracle RMAN script

The RMAN script is used when the Data Protector backup specification is started to perform a backup of the Oracle objects.

The RMAN script section is not written to the backup specification until the backup specification is either saved or manually edited by clicking the **Edit** button.

You can edit the RMAN script section of only after the Data Protector Oracle backup specification has been saved.

Limitations

When editing the RMAN script sections of the Data Protector backup specifications, consider the following limitations:

- The Oracle manual configuration convention must be used and not the Oracle automatic configuration convention.
- Double quotes (") must not be used - single quotes should be used instead.
- By default, RMAN scripts created by Data Protector contain instructions for backing up one or more of the following objects:
  - Databases, tablespaces, or datafiles (the first backup command)
  - Archive logs (the second backup command)
  - Control files (the last backup command)

  The RMAN scripts with all combinations of the above listed backup objects are recognized by Data Protector as its own scripts and it is possible to modify the selection of objects that will be backed up in the **Source** tab of the Results Area.

  If the RMAN script contains *additional* manually entered backup commands, for example a second backup command for backing up a database that is already listed in the first backup command, the object selection is disabled and it is only possible to browse the **Source** tab.

To edit an Oracle RMAN script, click **Edit** in the **Application Specific Options** window (see "Recovery catalog settings dialog" (page 66)), edit the script, and then click **Save** to save the changes to the script.

See the *Oracle Recovery Manager User's Guide and References* for more information on Oracle RMAN commands.

Data Protector RMAN script structure

The RMAN script created by Data Protector consists of the following parts:

- **The Oracle channel allocation** together with the Oracle environment parameters' definition for every allocated channel.

  For all backup specifications except for Oracle proxy-copy ZDB backup specifications, the number of allocated channels is the same as the sum of concurrency numbers for all devices selected for backup.

  NOTE: Once the backup specification has been saved, changing the concurrency number does not change the number of allocated channels in the RMAN script. This has to be done manually by editing the RMAN script.

  IMPORTANT: On Windows systems, a maximum of 32 or 64 (if device is local) channels can be allocated. If the calculated number exceeds this limitation, you have to manually edit the RMAN script and reduce the number of allocated channels.

  When an Oracle channel is manually defined by editing the RMAN script, the environment parameters must be added in the following format:

  ```
  parms 'ENV=(OB2BARTYPE=Oracle8, OB2APPNAME=DB_NAME,
  OB2BARLIST=Backup_Specification_Name)';
  ```

Proxy-copy

For Oracle proxy-copy ZDB backup sessions, Data Protector allocates *one* channel.

For Oracle proxy-copy ZDB, the `OB2SMB` parameter must be set to 1. If you use the `Blank Oracle Backup` template, the number of concurrently running DMA (`OB2DMAP`) is

automatically calculated as the sum of all device concurrences; for example, if there are 4 devices with concurrency set to 3 then OB2DMAP will be set to 12.

If you use the Oracle_SMB template, the OB2DMAP parameter is set to 1. To improve the backup and restore performance, you may want to increase the value of this parameter. The environment parameters must be added in the following format:

```
parms 'ENV=(OB2BARTYPE=Oracle8, OB2APPNAME=DB_NAME,
OB2BARLIST=Backup_Specification_Name, OB2SMB=1,
OB2DMAP=Concurrent_DMAs)';
```

NOTE: The OB2DMAP parameter does not change after it has been calculated, even if you adjust the device concurrency. To change OB2DMAP, you have to manually edit the RMAN script.

- Depending on the backup objects selection, **an RMAN backup statement for the backup of the whole database instance, and/or for any combination of RMAN commands to back up tablespaces and datafile**. The backup statement consists of the following:
  - The Oracle format of the backup file in the following format:

    ```
    format 'Backup_Specification_Name<DB_NAME_%s:%t:%p>.dbf' database;
    ```

    NOTE: When an Oracle format of the backup file is manually defined or changed by editing the RMAN script, any user-defined combination of the Oracle substitution variables can be *added* to the %s:%t:%p substitution variables and *DB_NAME*, which are obligatory.

  - In case of an Oracle proxy-copy ZDB-to-disk+tape or ZDB-to-tape session, the PROXY ONLY option is required. Only one BACKUP command with the proxy only option is permitted and only one additional backup command for backing up the control file is permitted.
  - The RMAN datafile *tablespace_name***datafile_name* command.
- If the archived redo logs were selected for a backup, **an RMAN backup statement for the backup of Oracle archive logs**.

  The backup statement consists of the Oracle format of the backup file:

  ```
  format 'Backup_Specification_Name<DB_NAME_%s:%t:%p>.dbf'
  ```

  NOTE: When an Oracle format of the backup file is manually defined or changed by editing the RMAN script, any user-defined combination of the Oracle substitution variables can be *added* to the obligatory %s:%t:%p substitution variables and *DB_NAME*.

- If the control file was selected for a backup, **an RMAN backup statement for the backup of Oracle control files**. The backup statement consists of the following:
  - The Oracle format of the backup file in the following format:

    ```
    format 'Backup_Specification_Name<DB_NAME_%s:%t:%p>.dbf' current
    controlfile;
    ```

    NOTE: When an Oracle format of the backup file is manually defined or changed by editing the RMAN script, any user-defined combination of the Oracle substitution variables can be *added* to the %s:%t:%p substitution variables and *DB_NAME*, which are obligatory.

  - The RMAN current controlfile command.

  For Oracle proxy-copy ZDB to disk or disk+tape, it is not possible to select only the control file. You must also select either a DATABASE, TABLESPACE, or DATAFILE object.

Example of the Oracle proxy-copy ZDB to disk+tape RMAN script

The following is an example of the RMAN script section as created by Data Protector based on the `Oracle SMB_Proxy_Database` template, after the whole database selection:

```
run {
allocate channel 'dev_0' type 'sbt_tape' parms
 'ENV=(OB2BARTYPE=Oracle8,OB2APPNAME=DIPSI,OB2BARLIST=New1,
OB2SMB=1,OB2DMAP=1)';
backup incremental level <incr_level>
format 'New1<DIPSI_%s:%t:%p>.dbf'
proxy only
database
;
backup format 'New1<DIPSI_%s:%t:%p>.dbf' controlfile;
}
```

Starting backup sessions

To run a ZDB-to-disk, ZDB-to-tape, or ZDB-to-disk+tape backup session of an Oracle database, use any of the following methods:

Backup methods

- Schedule a backup of an existing Oracle ZDB backup specification using the Data Protector Scheduler. See "Scheduling backup sessions" (page 61).
- Start an interactive backup of an existing Oracle ZDB backup specification using the Data Protector GUI or the Data Protector CLI. See "Running an interactive backup" (page 62).

Considerations

Before running an Oracle ZDB session, consider the following:

- It is not possible to start a ZDB, restore, or instant recovery sessions using the same source volume on the application system at the same time. A ZDB, restore, or instant recovery session must be started only after the preceding session that is using the same source volume on the application system has finished the ZDB session or restore; otherwise, the session will fail.
- For the backup set method, if the Oracle database is installed on symbolic links, then these symbolic links have to be also created on the backup system.
- On P9000 XP Array, if the LVM mirroring configuration is used, Data Protector displays a warning during a backup because the volume group source volumes on the application system do not have their HP BC P9000 XP pairs assigned. This message should be ignored.
- If the control file, SPILE, or online redo logs are on the same source volumes as the datafiles and the **Track the replica for instant recovery** option is selected, the backup session will be aborted. In this case, you need to either reconfigure the database or set the `ZDB_ORA_INCLUDE_CF_OLF`, `ZDB_ORA_INCLUDE_SPF`, and `ZDB_ORA_NO_CHECKCONF_IR` `omnirc` options. See "Reconfiguring an Oracle instance for instant recovery" (page 252) or "ZDB integrations omnirc options" (page 254).

Scheduling backup sessions

Scheduling a backup session means setting the time, date, and type of a backup that starts unattended once the scheduling options are defined and saved in the backup specification.

For more information on scheduling, see the *HP Data Protector Help* index: "scheduled backups".

To schedule an Oracle ZDB backup specification, proceed as follows:

1. In the Data Protector Manager, switch to the **Backup** context.
2. In the **Scoping Pane**, expand **Backup Specifications** and then **Oracle Server**.
3. Double-click the backup specification you want to schedule and click the **Schedule** tab.

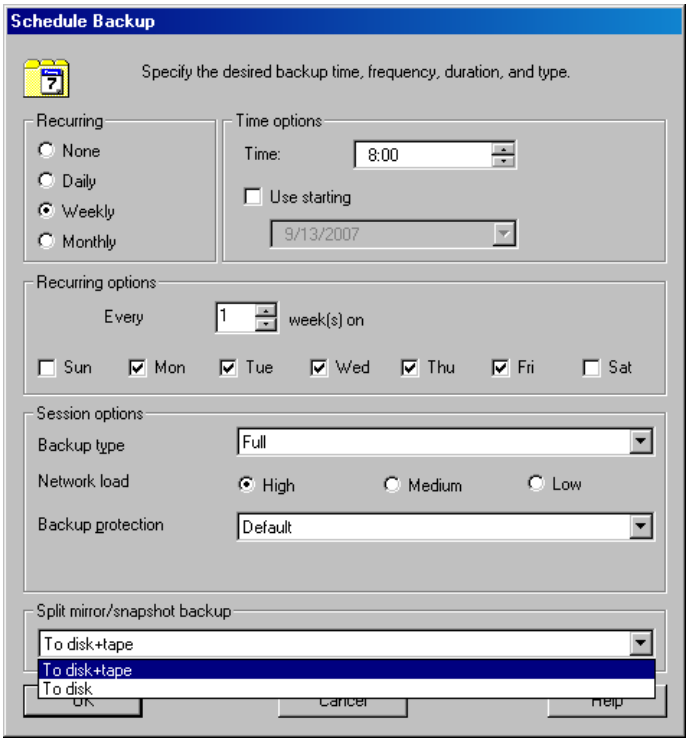
4. In the **Schedule** page, select a date in the calendar and click **Add** to open the **Schedule Backup** dialog box.
5. Specify **Recurring**, **Time options**, **Recurring options**, and **Session options**.

   Note that only the `Full` backup type is supported.

   In the case of a ZDB-to-disk or a ZDB-to-disk+tape session, specify the **Split mirror/snapshot backup** option. See "Selecting ZDB to disk or ZDB to disk+tape session using the Data Protector scheduler" (page 62).

NOTE: You can run a ZDB-to-disk or a ZDB-to-disk+tape session only if the **Track the replica for instant recovery** option is selected in the backup specification.

Figure 25 Selecting ZDB to disk or ZDB to disk+tape session using the Data Protector scheduler



Click **OK** and then **Apply** to save the changes.

Running an interactive backup

An interactive backup can be performed any time after a backup specification has been created and saved. You can use the Data Protector GUI or CLI.

Starting a backup using the GUI

To start an interactive ZDB session of an Oracle database using the Data Protector GUI, proceed as follows:

1. In the Context List, click **Backup** context.
2. In the Scoping Pane, expand **Backup Specifications** and then **Oracle Server**. Right-click the backup specification you want to use and click **Start Backup**.

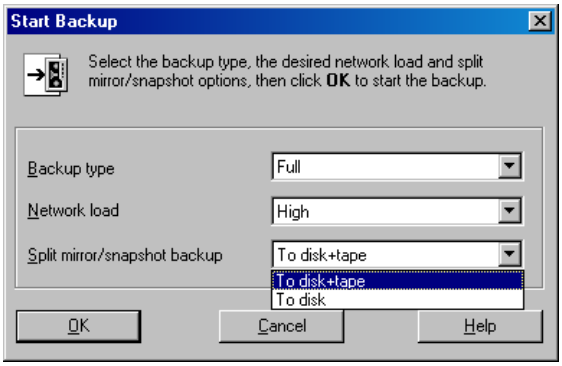
3. In the **Start Backup** dialog box, select the **Network load** option. For information on network load, click **Help**.

   Note that only the `Full` backup type is supported.

   In the case of a ZDB-to-disk or a ZDB-to-disk+tape session, specify the **Split mirror/snapshot backup** option. See "Selecting ZDB to disk or ZDB to disk+tape session when starting an interactive backup" (page 63).

NOTE: You can run a ZDB-to-disk or a ZDB-to-disk+tape session only if the **Track the replica for instant recovery** option is selected in the backup specification.

Figure 26 Selecting ZDB to disk or ZDB to disk+tape session when starting an interactive backup



   Click **OK**.

Starting a backup using the CLI

To start an Oracle **ZDB-to-tape** or **ZDB-to-disk+tape** session using the Data Protector CLI, execute:

```
omnib -oracle8_list Name
```

To start an Oracle **ZDB-to-disk** session using the Data Protector CLI, execute:

```
omnib -oracle8_list Name -disk_only
```

where *Name* is the name of the backup specification. For more information on the `omnib` command, see its man page or the *HP Data Protector Command Line Interface Reference*.

NOTE: It is not possible to run a ZDB-to-disk or a ZDB-to-disk+tape session if the **Track the replica for instant recovery** backup option is not selected in the backup specification.

Restore

You can restore the following database objects using both the Data Protector GUI or RMAN:

- Control files
- Datafiles
- Tablespaces
- Databases
- Recovery Catalog Databases

Using the Data Protector GUI, you can also **duplicate** a production database. See "Duplicating an Oracle database" (page 71).

The following are the available methods in Data Protector for restoring database objects:

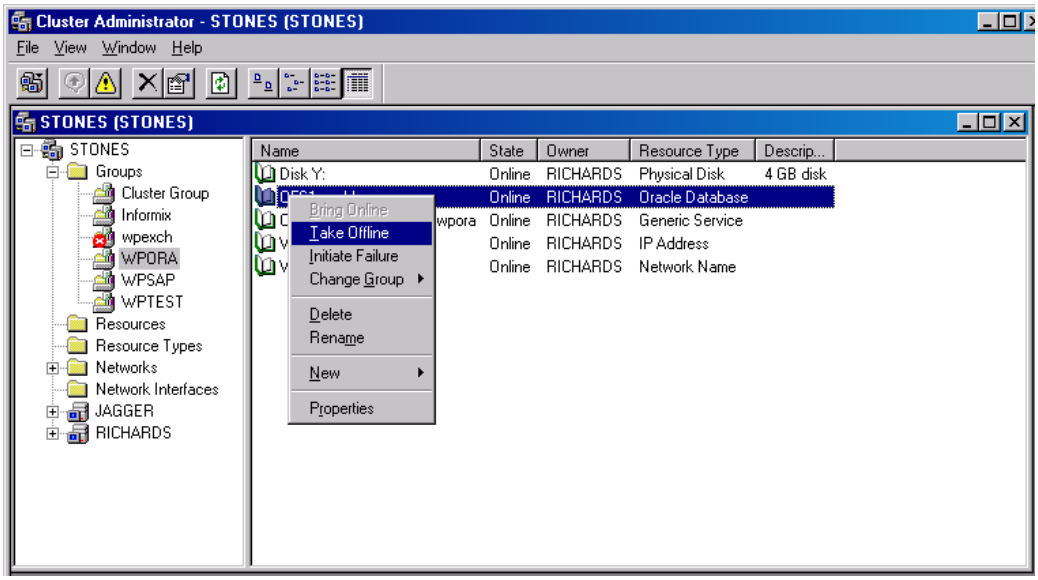
- Standard restore from backup media to the application system on LAN. See "Restoring from backup media to the application system on LAN" (page 65).
- Instant recovery. See "Instant recovery and database recovery" (page 87).

See also "Oracle recovery methods" (page 21) for an overview of recovery methods depending on the backup type and type of recovery.

Microsoft Cluster Server systems

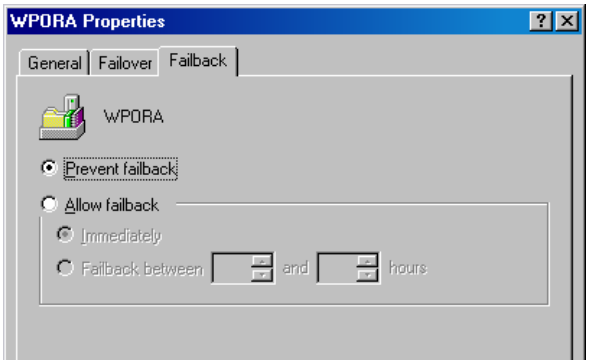
Before you start restoring a cluster-aware Oracle server, take the Oracle Database resource offline using, for example, the Cluster Administrator utility. See "Taking the Oracle resource group offline" (page 64).

Figure 27 Taking the Oracle resource group offline



Verify that you have set the **Prevent Fallback** option for the Oracle resource group and **Do not restart** for the *DB_NAME*.world resource, which is an Oracle Database resource.

Figure 28 Checking properties



MC/ServiceGuard systems

When restoring the database from a backup performed on a virtual host, you should set OB2BARHOSTNAME environment variable in the RMAN script. For example:

```
run {
allocate channel dev1 type 'sbt_tape' parms
 'SBT_LIBRARY=Path_to_Data_Protector_MML,
  ENV=(OB2BARHOSTNAME=virtual.domain.com)';
restore datafile '/opt/ora10g/oradata/MAKI/example02.dbf';
release channel dev1;
}
```

Prerequisites

- An instance of Oracle must be created on the system to which you want to restore or duplicate the database.
- The database must be in the `Mount` state if the whole database is being restored, or in the `NoMount` state if the control file is being restored or a database duplication is performed.
- You must be able to connect to the database.

  One way of achieving this is by configuring static service information for your Oracle listener. For details, see the Oracle documentation. You can find an example of static service information configuration in the troubleshooting "Instant recovery of an Oracle database fails" (page 103).
- On Windows systems, when performing a restore from backup using the Oracle backup set ZDB method, set the `omnirc` option `ZDB_SMISA_AUTOMOUNTING` on the application system to `2`, in order to enable automatic volume mounting on the local system.

Restoring from backup media to the application system on LAN

You can restore the database objects using one of the following tools within Data Protector:

- Data Protector GUI. See "Restoring Oracle using the Data Protector GUI" (page 65).
- RMAN. See "Restoring Oracle using RMAN" (page 76).

Restoring Oracle using the Data Protector GUI

For restore, RMAN scripts are generated with necessary commands, depending on selections made in the GUI. To use additional commands, use them manually from RMAN itself. You can also use the workaround described in "How to modify the RMAN restore script" (page 102).

Restoring database items in a disaster recovery

In a disaster recovery situation, database objects must be restored in a certain order. The following list shows you in which order database items must be restored. Under normal conditions it is possible to restore database items in any order.

1. Restore the recovery catalog database (if it was lost)
2. Restore the control file
3. Restore the entire database or data items

Changing the database state

Before you restore any database item or you perform a duplication of a database, ensure that the database is in the correct state:

Table 7 Required database states

Item to restore	Database state
Control file, duplicating a database	`NoMount` (started)
All other items[1]	`Mount`

[1] When restoring only a few tablespaces or datafiles, then the database can be open with the tablespaces or datafiles to be restored offline.

To put the database into the correct state, execute:

```
sqlplus /nolog
SQL>connect user/password@service as sysdba;
SQL>shutdown immediate;
```

To put the database into `NoMount` state, execute:

```
SQL>startup nomount;
```

To put the database into `Mount` state, execute:

```
SQL>startup mount;
```

Restoring the recovery catalog database

The Oracle recovery catalog database is exported using the Oracle export utility to a binary file and backed up by Data Protector. This file has to be restored back to the disk and then imported into the Oracle database using the Oracle import utility. Data Protector provides a facility to do this automatically using the Oracle integration.

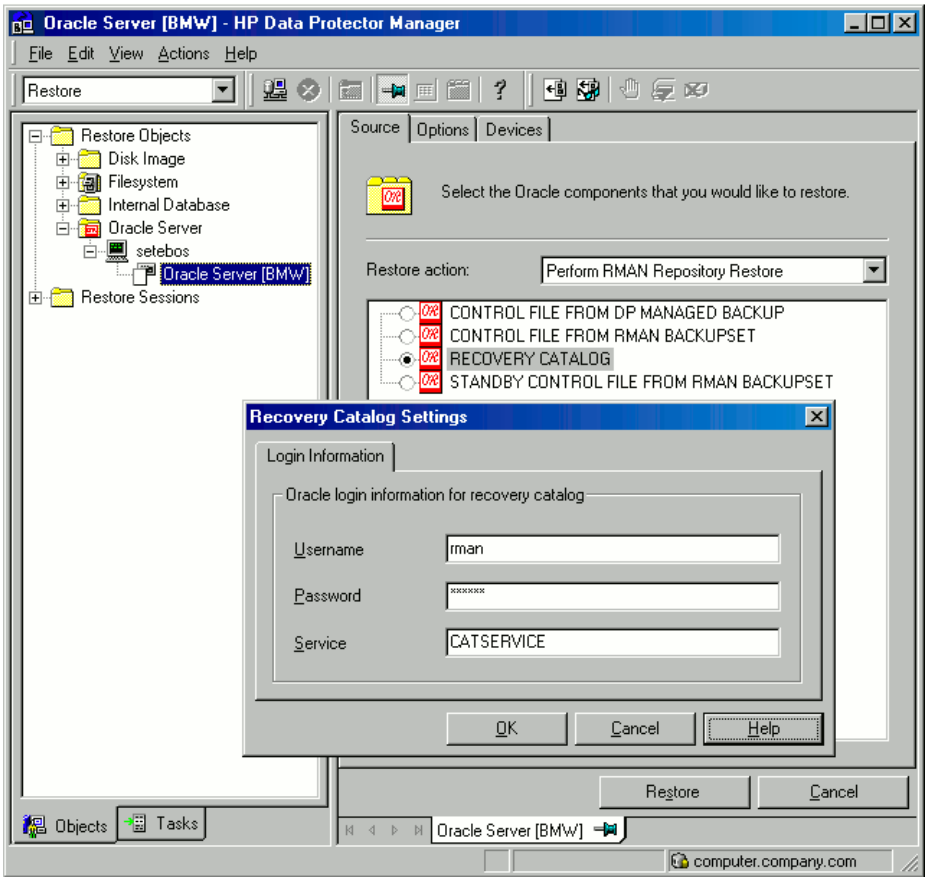
To restore the recovery catalog database:

1. Ensure that the recovery catalog database is in the **Open** state.
2. Remove the recovery catalog from the database (if it exists), using the RMAN command `DROP CATALOG`.
3. In the Data Protector GUI, switch to the **Restore** context.
4. Under **Restore Objects**, expand **Oracle Server**, expand the system on which the database, for which you want to restore the recovery catalog, resides, and then click the database.
5. In the **Restore action** drop-down list, select **Perform RMAN Repository Restore**.

   In the Results Area, select **RECOVERY CATALOG**.

   If you want to change the recovery catalog login information, right-click **RECOVERY CATALOG** and click **Properties**. In **Recovery Catalog Settings**, specify the login information for recovery catalog.

Figure 29 Recovery catalog settings dialog



6. In the **Options** page:

   In **User name** and **User group**, specify the user name and password to the recovery catalog database.

   From the **Session ID** drop-down list, select the Session ID.

   For further information, see "Restore, recovery, and duplicate options" (page 73).

7. Click **Restore**.

Proceed to restore the control file.

Restoring the control file

The control file contains all the information about the database structure. If the control file has been lost, you must restore it before you restore any other part of the database. The database should be in the `NoMount` state.

Depending on the type of the control file backup, the following types of restore are possible when restoring the control file:

- Restoring from Data Protector managed control file backup (`CONTROLFILE FROM DP MANAGED BACKUP`)

  The control file was backed up automatically by `ob2rman.pl` at the end of a backup session, unless the option `Disable Data Protector managed control file backup` was selected.

  The recovery catalog is *not* required for this restore option.

  The control files (`ctrl`*`DB_NAME`*`.dbf`) are restored to:

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

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

  NOTE: In Oracle Real Application Clusters (RAC) environments with Oracle versions 11.2.0.2 and later, the control files are created at, backed up from, and restored to the location defined by the `OB2_DPMCTL_SHRLOC` variable. This directory must reside on a shared disk and be accessible from all RAC nodes in order for restore sessions to succeed.

  After the restore, execute the following script:

  ```
  run {
  allocate channel 'dev0' type disk;
  restore controlfile from 'TMP_FILENAME';
  release channel 'dev0';
  }
  ```

  Where *`TMP_FILENAME`* is the location to which the file was restored.

- Restoring from RMAN backup set (`CONTROLFILE FROM RMAN BACKUPSET`)

  The recovery catalog *is* required.

A backup session can contain more than one type of the control file backup.

To restore the control file:

1. Open the `sqlplus` window and put the database in the nomount state. See "Changing the database state" (page 65).
2. In the Data Protector GUI, switch to the **Restore** context.
3. Under **Restore Objects**, expand **Oracle Server**, expand the system on which the database, for which you want to restore the control file, resides, and then click the database.
4. In the **Restore Action** drop-down list, select **Perform RMAN Repository Restore**.

   In the Results area, select the control file for restore.

5. In the **Options** page, from the **Client** drop-down list, select the system on which the Data Protector Oracle integration agent (`ob2rman.pl`) will be started. To restore the control file to a different database than it is selected, click **Settings** and specify the login information for the target database.

   Set the other restore options. For information, see "Restore, recovery, and duplicate options" (page 73).

6. Click **Restore**.

Proceed with restoring the Oracle database objects.

Restoring Oracle database objects

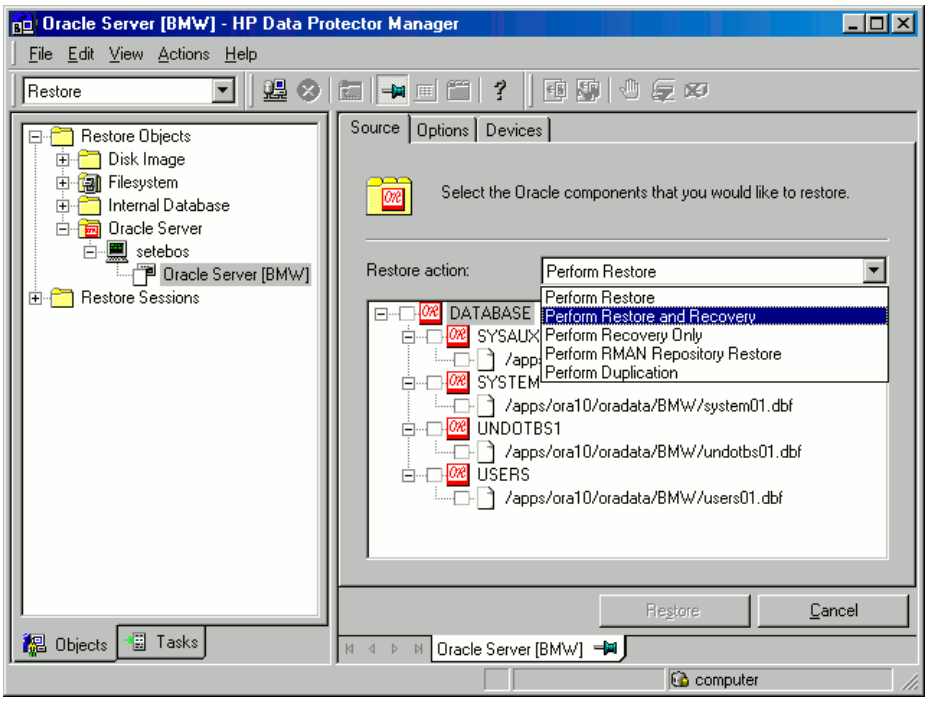
Before you restore Oracle database objects, ensure that you have an up-to-date version of the recovery catalog database and the control file. They contain the database structure information. If you do not have up-to-date versions of these files, restore them as described in "Restoring the recovery catalog database" (page 66) and "Restoring the control file" (page 67).

To restore Oracle database objects:

1. Put the database in the mount state. See "Changing the database state" (page 65).
2. In the Data Protector GUI, switch to the **Restore** context.
3. Under **Restore Objects**, expand **Oracle Server**, expand the system on which the database, for which you restore the database objects, resides, and then click the database.
4. In the **Restore action** drop-down list, select the type of restore you wish to perform. For information on the options, see "Restore, recovery, and duplicate options" (page 73).

IMPORTANT: If you do not select **Perform Restore and Recovery** or **Perform Recovery Only**, you will have to recover the database objects manually using RMAN. For information, see "Restoring Oracle using RMAN" (page 76).

Figure 30 Source page



5. In the Results Area, select objects for restore.

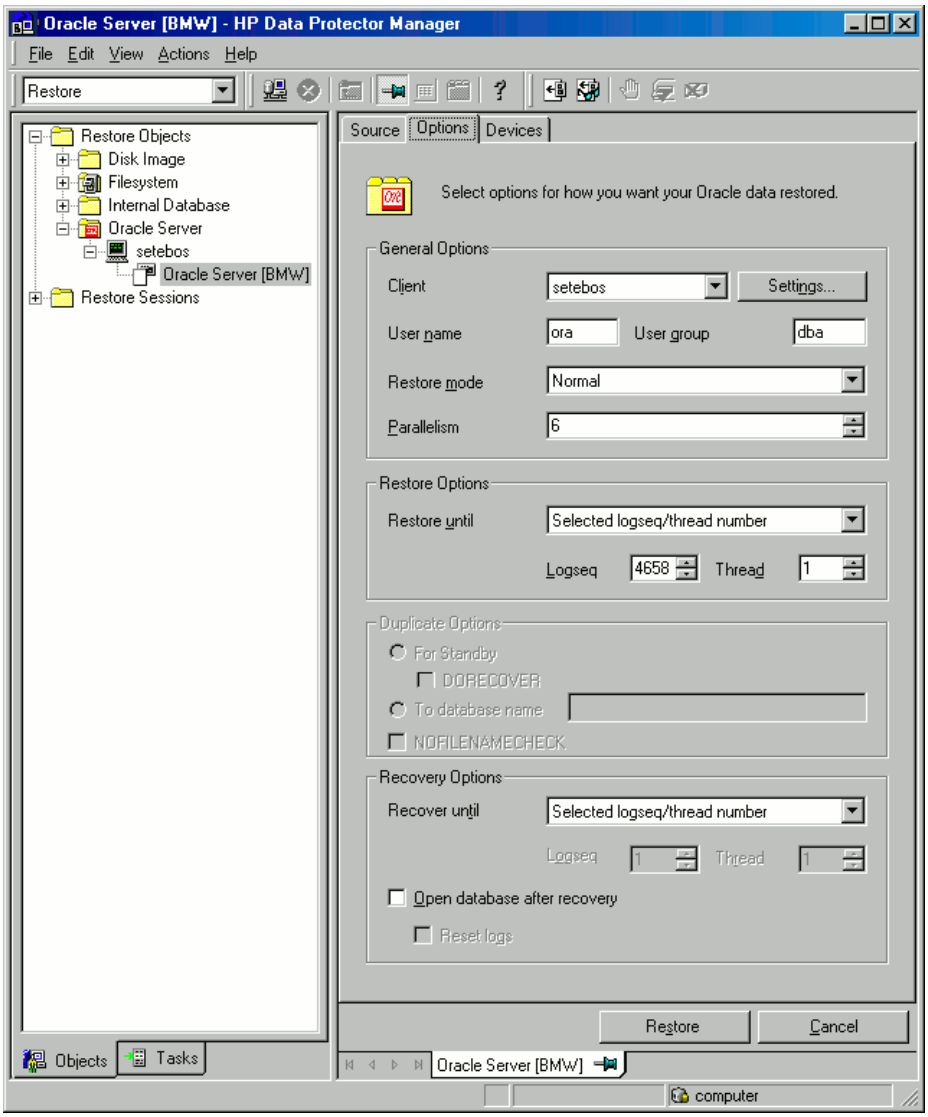
   If you are restoring datafiles, you can restore the files to a new location. Right-click the database object, click **Restore As**, and in the **Restore As** dialog box, specify the new datafile location.

NOTE: When restoring to a new location, current datafiles will be switched to the restored datafile copies only if you have selected **Perform Restore and Recovery** from the **Restore action** drop-down list.

6. In the **Options** page, from the **Client** drop-down list, select the system on which the Data Protector Oracle integration agent will be started. To restore the database objects to a different database than it is selected, click **Settings** and specify the login information for the target database.

   Set the other restore options. For information, see "Restore, recovery, and duplicate options" (page 73).

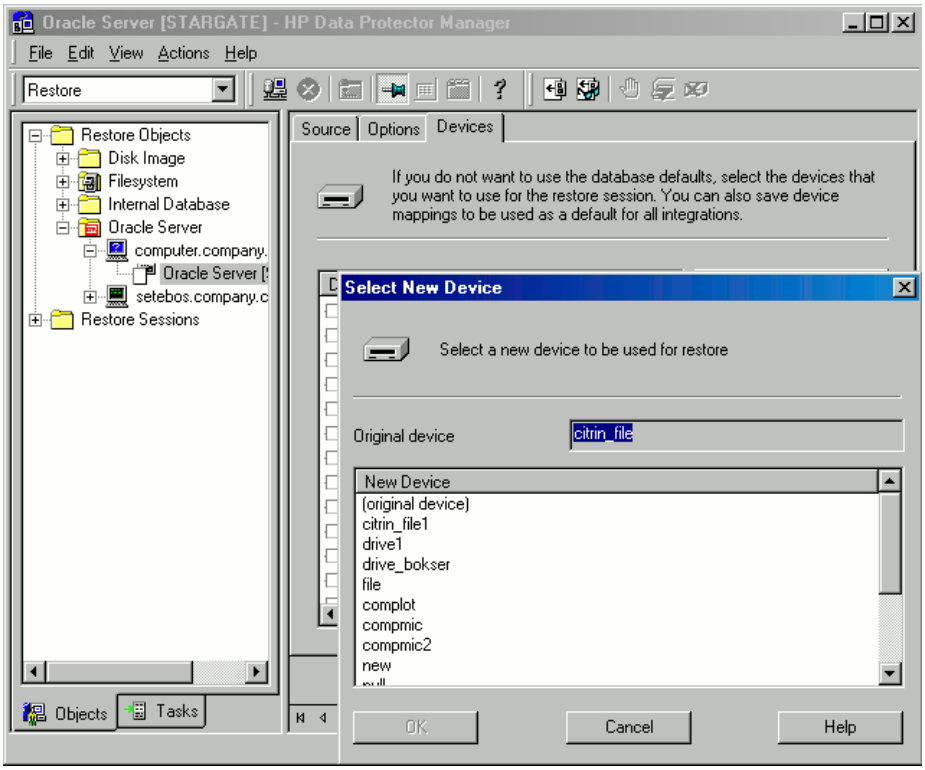
Figure 31 Options page



7. In the **Devices** page, select the devices to be used for the restore.

   For more information on how to specify devices for a restore, see the *HP Data Protector Help* index: "restore, selecting devices for".

Figure 32 Devices page



8. Click **Restore**.

After the restore:

1. Put the database in the correct state.

   If you selected **Perform Restore and Recovery** or **Perform Recovery Only** in the **Source** page, then the database is automatically put into **Open** state by Data Protector.

2. If you performed an Oracle database restore and recovery until point in time, and the session has finished successfully, reset the database to register the new incarnation of database in the recovery catalog.

   Connect to the target and recovery catalog database using RMAN and reset the database:

   ```
   rman target Target_Database_Login catalog Recovery_Catalog_Login
   RMAN> RESET DATABASE;
   RMAN> exit
   ```

3. If you did not choose to use Data Protector to recover the database objects and if you have all archived redo logs on disk, perform the following after the database is restored:

   Open a command line window and enter the following commands:

   ```
   sqlplus /nolog
   SQL>recover database;
   SQL>connect user/password@service as sysdba;
   SQL>alter database open;
   ```

Restoring tablespaces and datafiles

To restore tablespaces and datafiles:

1. Open a command line window and enter the following commands if you have the database in the Open state:

   ```
   sqlplus /nolog
   SQL>connect user/password@service as sysdba;
   SQL>alter database datafile 'datafile name' offline;
   ```

   If you are restoring a tablespace enter:

   ```
   SQL>alter tablespace tablespace_name offline;
   ```

2. When the restore has been completed put the datafiles and tablespaces back online with the following procedures:

   Open a command line window and enter the following commands:

   ```
   sqlplus /nolog
   SQL>connect user/password@service as sysdba
   ```

   If you are restoring a datafile enter:

   ```
   SQL>alter database datafile 'datafile_name' online;
   ```

   If you are restoring a tablespace enter:

   ```
   SQL>alter tablespace tablespace_name online;
   ```

Duplicating an Oracle database

Perform a production database duplication to create:

- A standby database which has the same DBID as the production (primary) database. With this, you can:
  - Create a new standby database.
  - Re-create a standby database after:
    - Loss of entire standby database
    - Primary database control file was restored or recreated
    - Database point-in-time recovery was performed on the primary database
    - Switchover or failover of database roles occurred
- An independent copy, with a unique DBID, which can be used for data mining or testing purposes.

Prerequisites

- The whole primary database with the archived logs must be backed up.
- Archive logs, which have not been backed up to tape since the last full backup and are required for duplication must be available on the duplicate system with the same path names as on the target system (system with the production database to be duplicated).
- Net service name for the auxiliary instance must be configured.
- When duplicating a database on the same system on which the target database resides, set all *_PATH, *_DEST, DB_FILE_NAME_CONVERT, and LOG_FILE_NAME_CONVERT initialization parameters appropriately. Thus, the target database files will not be overwritten by the duplicate database files.

Limitations

- Database duplication is not supported using proxy copy backups of the primary database.
- If you perform duplication of a database (not for standby) on the same system on which the target or production database resides, note that you cannot use the same database name for the target and duplicate databases when the duplicate database resides in the same Oracle home directory as the target database. Note also that if the duplicate database resides in a different Oracle home directory than the target database, then the duplicate database name has to differ from other database names in that same Oracle home directory.

To duplicate a production database:

1. On the system where the selected database will be duplicated, put the Oracle auxiliary database instance in the nomount state. See "Changing the database state" (page 65).
2. In the Context List of the Data Protector GUI, click **Restore**.
3. Under **Restore Objects**, expand **Oracle Server**, expand the system on which the production database resides, and then click the production database which you want to duplicate. If there are several such systems, select the system on which you want the Data Protector Oracle integration agent (`ob2rman.pl`) to be started.
4. In the **Restore Action** drop-down list, select **Perform Duplication**.
5. In the **Options** page, from the **Client** drop-down list, select the system on which the Data Protector Oracle integration agent (`ob2rman.pl`) will be started.

   Click **Settings** to specify the login information (a user name, password, and net services name) for the auxiliary database. If you do not provide the login information, the duplication session will fail.

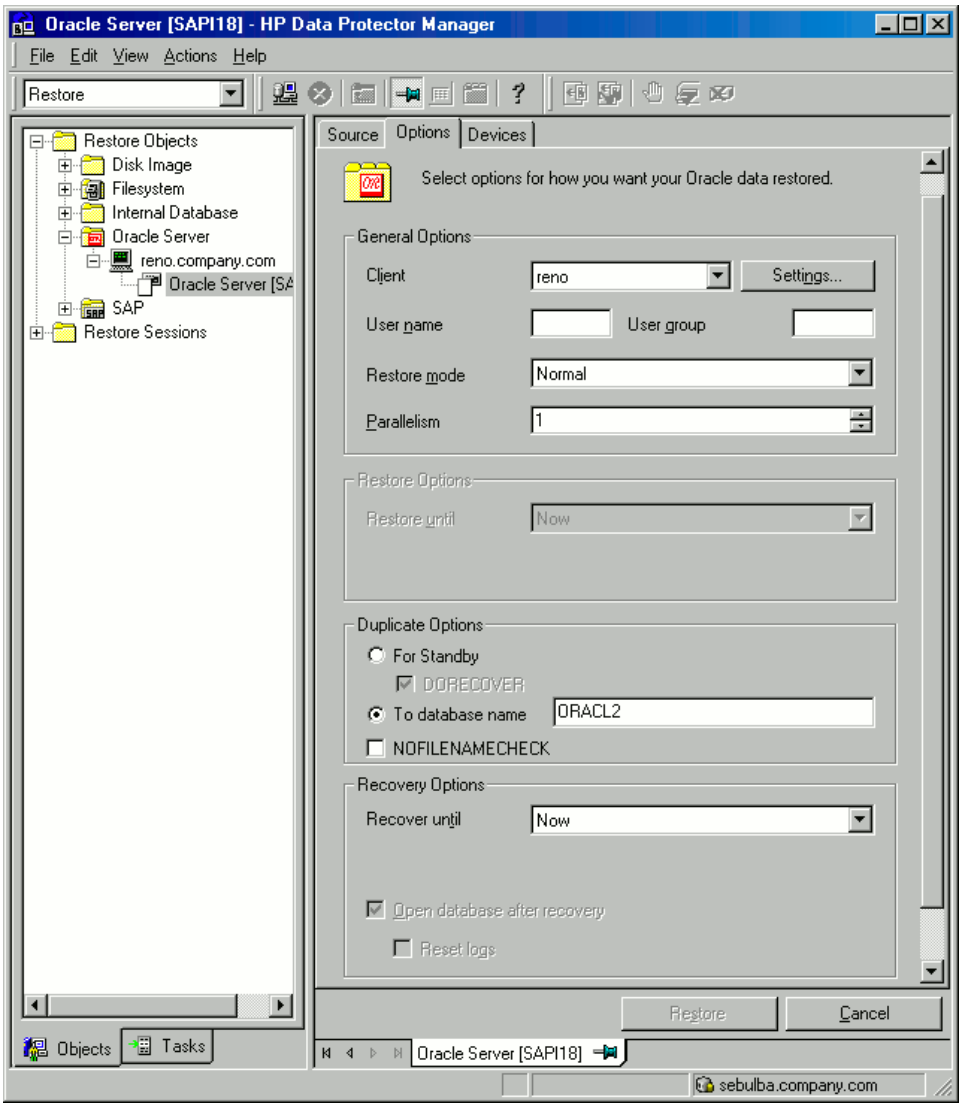
   In **User name** and **User group**, specify the user name and group for the `OSDBA` account, which will be used by the Data Protector Oracle integration agent.

   In **Parallelism**, specify the number of RMAN auxiliary channels to be allocated for database duplication.

   Set duplicate options. For information, see "Duplicate options" (page 75) or press **F1**.

   If you are creating a new database copy (not for standby), specify also the **Recover until** option to recover the duplicated database until a specified point in time.

Figure 33 Oracle duplicate options



6. Click **Restore**.

When the standby database is created, it is left mounted. Start the managed recovery process (log apply services) manually.

For information on how to use the RMAN commands to duplicate a database, see the Oracle documentation.

Restore, recovery, and duplicate options

Restore action options

The following describes each of the options in the **Source** page. This page is used to define the combination of restore and recovery you would like to perform using the GUI.

In the context of Data Protector, “restore” means to restore the datafiles. You can select which database, tablespace, or datafiles they would like to restore and up to which point in time they would like them to be restored. “Recover” means applying the redo logs. You can select which redo logs to apply according to SCN number, logseq, or you can apply all the redo logs to the time of the last backup.

Perform Restore

Use this option to only restore (but not recover) the database objects using Data Protector. After restore, recover the database manually using RMAN. For information on recovering the database using RMAN, see "Restoring Oracle using RMAN" (page 76).

Perform Restore and Recovery

Use this option to perform both the restore and recovery of the database objects using Data Protector.

Perform Recovery Only

Use this option to only recover the database. This action can only be performed on the whole database.

Perform RMAN Repository Restore

Use this option to restore the recovery catalog or the control file when the database objects are not available in the **Source** page.

Perform Duplication

This option is used to perform duplication of a production database. This action can only be performed on the whole database.

General options

Client

This option specifies the system on which the Data Protector Oracle integration agent (`ob2rman.pl`) will be started.

Settings

Click **Settings** to specify the login information (user name, password, and net service name) for the target database (in case of restore and recovery) or auxiliary database (in case of duplication) where you want the selected database objects to be restored or duplicated.

If this is not specified in the case of restore or recovery, the login information of the selected database that resides on the selected system will be used.

If this is not specified in the case of duplication, the duplication session will fail.

User name, User group (UNIX systems only)

Specify the operating system user account under which you want the restore to start.

Ensure that this user has Oracle rights to restore the database (for example, it is in the `DBA` user group). The user must also be in the Data Protector `admin` or `operator` user group (actually, the `Start restore` and `See private objects` user rights suffice).

Restore mode

This drop-down list allows you to specify which type of restore you would like perform. The options are:

- Normal

  This option should be used when a conventional backup or ZDB using the backup set method was performed.

- Proxy copy

  This option should be used when the original Oracle backup was made using the Oracle RMAN proxy-copy method.

This option is disabled when you perform recovery only.

Parallelism

This field is used to specify the number of concurrent data streams that can read from the backup device. The default value is one.

In case of `Normal` restore mode, to optimize restore performance, specify the same number of data streams as were used during the backup. For example, if you set the backup concurrency to 3, set the number of parallel data streams to 3 as well. Note that if a very high number of parallel data streams is specified this may result in a resource problem because too much memory is being used.

For Oracle proxy-copy ZDB sessions, this option is disabled and Data Protector sets the number of concurrent data streams to the value that was used at backup. If you are restoring a backup created using a previous version of Data Protector, parallelism is set to the number of devices that were used for backup, regardless of the concurrency numbers for these devices.

Duplicate options

Available if **Perform Duplication** was selected.

For Standby

Select this option to create a standby database.

Default: selected.

DORECOVER

Available if **For Standby** was selected.

Select this option if you want RMAN to recover the database after creating it.

To database name

Select this option to create a new database copy. In the text box, specify its name. The name should match the name in the initialization parameter file that was used to start the auxiliary database instance. By default, the database name is set to the database name of the currently selected target database.

NOFILENAMECHECK

Select this option to disable RMAN to check whether the target datafiles share the same names with the duplicated datafiles.

Select this option when the target datafiles and duplicated datafiles have the same names, but reside on different systems.

Default: not selected.

Restore and recovery options

Restore until

The options in this drop-down list allow you to limit the selection to those backups that are suitable for an incomplete recovery to the specified time.

- **Now**

  Use this option to restore the most recent full backup. By default, this option is selected.

- **Selected time**

  Use this option to specify an exact time to which you wish the database to be restored. Data Protector restores the backup that can be used in recovery to the specified time.

- **Selected logseq/thread number**

  A logseq number is a redo log sequence number. Use this option to specify a particular redo log sequence and a thread number which will act as an upper limit of redo logs to restore. Data Protector restores the backup that can be used in recovery to the specified log sequence number.

- **Selected SCN number**

Use this option to specify the SCN number to which you wish the database to be restored. Data Protector restores the backup that can be used in recovery to the specified SCN number.

Recover until

The options in this drop-down list allow you to specify to which point in time you would like the recovery to be performed.

- **Now**

  Data Protector starts RMAN to recover the database to the most recent time possible by applying all archived redo logs. By default, this option is selected.

- **Selected time**

  Use this option to specify an exact time to which the archive logs are applied.

- **Selected logseq/thread numbe**r

  A logseq number is a redo log sequence number. Use this option to specify a particular redo log sequence and a thread number which will act as an upper limit of redo logs to recover.

- **Selected SCN number**

  Use this option to specify the SCN number to which you perform the recovery.

If you reset the logs, also reset the database; otherwise, Oracle will during the next backup try to use the logs that were already reset and the backup will fail. Login to the target and recovery catalog database and execute:

```
rman target Target_Database_Login catalog Recovery_Catalog_Login
RMAN> RESET DATABASE;
RMAN> exit
```

Open database after recovery

Opens the database after a recovery is performed.

Reset logs

Resets the archive logs after the database is opened.

Always reset the logs:

- After an incomplete recovery (not **Recover until now**).
- If a backup of a control file is used in recovery or restore and recovery.

Do not reset the logs:

- After a complete recovery (**Recover until now**) when the backup of a control file was not used in recovery or restore and recovery.
- On the primary database, if the archive logs are used for a standby database. However, if you must reset the archive logs, you will need to recreate the standby database.

If you reset the logs when the **Recover until** option is set to **Now**, a warning is displayed, stating that you should reset the logs only if you use an older control file for restore.

NOTE: Oracle recommends that you perform a complete backup immediately after a database was opened with the **Reset Logs** option.

Restoring Oracle using RMAN

Data Protector acts as a media management software for the Oracle system, therefore RMAN can be used for a restore.

This section only describes *examples* of how you can perform a restore. The examples provided do not apply to all situations where a restore is needed.

See the *Oracle Recovery Manager User's Guide and References* for detailed information on how to perform:

- Restore and recovery of the database, tablespace, control file, and datafile.
- Duplication of a database.

The following examples of restore are given:

- "Example of full database restore and recovery" (page 78)
- "Example of point-in-time restore" (page 79)
- "Example of tablespace restore and recovery" (page 80)
- "Example of datafile restore and recovery" (page 82)
- "Example of archive log restore" (page 85)

The restore and recovery procedure of Oracle control files is a very delicate operation, which depends on the version of the Oracle database you are using. For detailed steps on how to perform the restore of control files, see the *Recovery Manager User's Guide and References*.

Preparing the Oracle database for restore

The restore of an Oracle database can be performed when the database is in mount mode. However, when you are performing the restore of tablespaces or datafiles, only a part of the Oracle database can be put offline.

Prerequisites

The following requirements must be met before you start a restore of an Oracle database:

- Make sure that the recovery catalog database is open. If the recovery catalog database cannot be brought online, you will probably need to restore the recovery catalog database. See "Restore" (page 63) for details of how to restore the recovery catalog database.
- Check which ZDB method (proxy-copy or backup set) was used for the backup session that you plan to restore.
- Control files must be available. If the control files are not available, you must restore them. See the *Oracle Recovery Manager User's Guide and References* for more details.

  If you have to perform a restore of the recovery catalog database, you must perform this restore first. Only then can you perform a restore of other parts of the Oracle database.

  When you are sure that the recovery catalog database files are in place, start the recovery catalog database.

- Make sure that the following environment variables are set:
  - `ORACLE_BASE`
  - `ORACLE_HOME`
  - `ORACLE_TERM`
  - `DB NAME`
  - `PATH`
  - `NLS_LANG`
  - `NLS_DATE_FORMAT`

Windows systems example

`ORACLE_BASE=`*`Oracle_home`*

```
ORACLE_HOME=Oracle_home\product\10.1.0
ORACLE_TERM=HP
DB_NAME=PROD
PATH=$PATH:Oracle_home\product\10.1.0\bin
NLS_LANG=american
NLS_DATE_FORMAT='Mon DD YYYY HH24:MI:SS'
```

UNIX systems example

```
ORACLE_BASE=/opt/oracle
ORACLE_HOME=/opt/oracle/product/10.1.0
ORACLE_TERM=HP
DB_NAME=PROD
PATH=$PATH:/opt/oracle/product/10.1.0/bin
NLS_LANG=american
NLS_DATE_FORMAT='Mon DD YYYY HH24:MI:SS'
```

- Check that the `/etc/oratab` file has the following line:

  Windows systems: `PROD:Oracle_home\product\10.1.0:N`

  UNIX systems: `PROD:/opt/oracle/product/10.1.0:N`

  The last letter determines whether the database will automatically start upon boot-up (Y) or not (N).

Connection strings used in the examples

In the examples below, the following connection strings are used:

- Target connection string for target database:

  `sys/manager@PROD`

  where `sys` is the username, `manager` is the password and `PROD` is a net service name.

- Recovery catalog connection string for recovery catalog database:

  `rman/rman@CATAL`

  where `rman` is the username and password and `CATAL` is a net service name.

SBT_LIBRARY parameter

On Windows and UNIX systems, set the `SBT_LIBRARY` RMAN script parameter to point to the correct platform-specific Data Protector MML. The parameter must be specified for each RMAN channel separately. For details on the Data Protector MML location, see the *HP Data Protector Integration Guide for Oracle and SAP*.

In the following examples, the `SBT_LIBRARY` parameter is set to `/opt/omni/lib/libob2oracle8.so`, which is the correct path for 32-bit Solaris systems.

Example of full database restore and recovery

To perform a full database restore and recovery, you also need to restore and apply all the archive logs. To perform a full database restore and recovery:

1. Log in to the Oracle RMAN:

   Windows systems: *ORACLE_HOME*\bin\rman target sys/manager@PROD catalog rman/rman@CATAL

   UNIX systems: *ORACLE_HOME*/bin/rman target sys/manager@PROD catalog rman/rman@CATAL

2. Start the full database restore and recovery:

   For a non-ZDB or ZDB backup set session:

```
run{
allocate channel 'dev1' type 'sbt_tape' parms
 'SBT_LIBRARY=/opt/omni/lib/libob2oracle8.so,
 ENV=(OB2BARTYPE=Oracle8,OB2APPNAME=DB_NAME)';
restore database;
recover database;
sql 'alter database open';
release channel 'dev1';
}
```

   For a ZDB proxy-copy session:

```
run{
allocate channel 'dev1' type 'sbt_tape' parms
 'SBT_LIBRARY=/opt/omni/lib/libob2oracle8.so,
  ENV=(OB2BARTYPE=Oracle8,OB2PROXYCOPY=1, OB2APPNAME=DB_NAME)';
restore database;
recover database;
sql 'alter database open';
release channel 'dev1';
}
```

You can also save the script into a file and perform a full database restore using the saved files. The procedure in such cases is as follows:

1. Create a file `restore_database` in the `/var/opt/omni/tmp` (UNIX systems) or *Data_Protector_home*\tmp (Windows systems) directory.
2. Start the full database restore:

   Windows systems: *ORACLE_HOME*\bin\rman target sys/manager@PROD catalog rman/rman@CATAL cmdfile=*Data_Protector_home*\tmp\restore_datafile

   UNIX systems: *ORACLE_HOME*/bin/rman target sys/manager@PROD catalog rman/rman@CATAL cmdfile=/var/opt/omni/tmp/restore_datafile

Example of point-in-time restore

To perform a point-in-time restore, you also need to restore and apply the archive logs to the specified point in time. To perform a point-in-time database restore and recovery:

1. Log in to the Oracle RMAN:

   Windows systems: *ORACLE_HOME*\bin\rman target sys/manager@PROD catalog rman/rman@CATAL

   UNIX systems: *ORACLE_HOME*/bin/rman target sys/manager@PROD catalog rman/rman@CATAL

2. Start the point-in-time restore:

   For a non-ZDB or ZDB backup set session:

```
run{
allocate channel 'dev1' type 'sbt_tape' parms
 'SBT_LIBRARY=/opt/omni/lib/libob2oracle8.so,
  ENV=(OB2BARTYPE=Oracle8,OB2APPNAME=DB_NAME)';
set until time 'Mar 14 2004 11:40:00';
restore database;
```

```
recover database;
sql 'alter database open';
release channel 'dev1';
}
```

For a ZDB proxy-copy session, allocate one channel for restoring proxy-copy sessions and one channel for database recovery. Release the proxy-copy channel before the recovery:

```
run{
allocate channel 'dev1' type 'sbt_tape' parms
 'SBT_LIBRARY=/opt/omni/lib/libob2oracle8.so,
  ENV=(OB2BARTYPE=Oracle8,OB2PROXYCOPY=1, OB2APPNAME=DB_NAME)';
allocate channel 'dev2' type 'sbt_tape' parms
 'SBT_LIBRARY=/opt/omni/lib/libob2oracle8.so,
  ENV=(OB2BARTYPE=Oracle8, OB2APPNAME=DB_NAME)';
set until time 'Mar 14 2006 11:40:00';
restore database;
release channel 'dev1';
recover database;
sql 'alter database open';
release channel 'dev2';
}
```

3. After you have performed a point-in-time restore, reset the database in the Recovery Catalog.

You can also save the script into a file and perform a point-in-time restore using the saved files:

1. Create a file `restore_PIT` in the `/var/opt/omni/tmp` or *`Data_Protector_home`*`\tmp` directory.
2. Start the point-in-time restore:

   Windows systems: *`ORACLE_HOME`*`\bin\rman target sys/manager@PROD catalog rman/rman@CATAL cmdfile=`*`Data_Protector_home`*`\tmp\restore_PIT`

   UNIX systems: *`ORACLE_HOME`*`/bin/rman target sys/manager@PROD catalog rman/rman@CATAL cmdfile=/var/opt/omni/tmp/restore_PIT`

Example of tablespace restore and recovery

If a table is missing or corrupted, you need to perform a restore and recovery of the entire tablespace. To restore a tablespace, you may take only a part of the database offline, so that the database does not have to be in the mount mode. You can use either a recovery catalog database or control files to perform a tablespace restore and recovery. Follow the steps below:

1. Log in to the Oracle RMAN:

   Windows systems: *`ORACLE_HOME`*`\bin\rman target sys/manager@PROD catalog rman/rman@CATAL`

   UNIX systems: *`ORACLE_HOME`*`/bin/rman target sys/manager@PROD catalog rman/rman@CATAL`

2. Start the tablespace restore and recovery.
   - If the database is in the open state, the script to restore and recover the tablespace should have the following format:

     For a non-ZDB or ZDB backup set session:

     ```
     run{
     allocate channel dev1 type 'sbt_tape' parms
      'SBT_LIBRARY=/opt/omni/lib/libob2oracle8.so,
       ENV=(OB2BARTYPE=Oracle8,OB2APPNAME=DB_NAME)';
     sql 'alter tablespace TEMP offline immediate';
     restore tablespace TEMP;
     recover tablespace TEMP;
     sql 'alter tablespace TEMP online';
     release channel dev1;
     }
     ```

     For a ZDB proxy-copy session, allocate one channel for restoring proxy-copy sessions and one channel for database recovery. Release the proxy-copy channel before the recovery:

     ```
     run{
     allocate channel 'dev1' type 'sbt_tape' parms
      'SBT_LIBRARY=/opt/omni/lib/libob2oracle8.so,
       ENV=(OB2BARTYPE=Oracle8,OB2PROXYCOPY=1, OB2APPNAME=DB_NAME)';
     allocate channel 'dev2' type 'sbt_tape' parms
      'SBT_LIBRARY=/opt/omni/lib/libob2oracle8.so,
       ENV=(OB2BARTYPE=Oracle8, OB2APPNAME=DB_NAME)';
     sql 'alter tablespace TEMP offline immediate';
     restore tablespace TEMP;
     release channel 'dev1';
     recover tablespace TEMP;
     sql 'alter tablespace TEMP online';
     release channel 'dev2';
     }
     ```

   - If the database is in the mount state, the script to restore and recover the tablespace should have the following format:

     For a non-ZDB or ZDB backup set session:

     ```
     run{
     allocate channel dev1 type 'sbt_tape' parms
      'SBT_LIBRARY=/opt/omni/lib/libob2oracle8.so,
       ENV=(OB2BARTYPE=Oracle8,OB2APPNAME=DB_NAME)';
     restore tablespace 'TEMP';
     recover tablespace 'TEMP';
     release channel dev1;
     }
     ```

     For a ZDB proxy-copy session, allocate one channel for restoring proxy-copy sessions and one channel for database recovery. Release the proxy-copy channel before the recovery:

     ```
     run{
     allocate channel 'dev1' type 'sbt_tape' parms
      'SBT_LIBRARY=/opt/omni/lib/libob2oracle8.so,
       ENV=(OB2BARTYPE=Oracle8,OB2PROXYCOPY=1, OB2APPNAME=DB_NAME)';
     allocate channel 'dev2' type 'sbt_tape' parms
      'SBT_LIBRARY=/opt/omni/lib/libob2oracle8.so,
       ENV=(OB2BARTYPE=Oracle8, OB2APPNAME=DB_NAME)';
     restore tablespace 'TEMP';
     release channel 'dev1';
     recover tablespace 'TEMP';
     release channel 'dev2';
     }
     ```

You can also save the script into a file and perform a tablespace restore using the saved files:

1. Create a file `restore_TAB` in the `/var/opt/omni/tmp` (UNIX systems) or *`Data_Protector_home`*`\tmp` (Windows systems) directory.
2. Start the tablespace restore.

   Windows systems: *`ORACLE_HOME`*`\bin\rman target sys/manager@PROD catalog rman/rman@CATAL cmdfile=`*`Data_Protector_home`*`\tmp\restore_TAB`

   UNIX systems: *`ORACLE_HOME`*`/bin/rman target sys/manager@PROD catalog rman/rman@CATAL cmdfile=/var/opt/omni/tmp/restore_TAB`

Example of datafile restore and recovery

To restore and recover a datafile, you may take only a part of the database offline.

To restore and recover a datafile:

1. Log in to the Oracle RMAN.

   Windows systems: *`ORACLE_HOME`*`\bin\rman target sys/manager@PROD catalog rman/rman@CATAL`

   UNIX systems: *`ORACLE_HOME`*`/bin/rman target sys/manager@PROD catalog rman/rman@CATAL`

2. Start the datafile restore and recovery:
   - If the database is in an open state, the script to restore the datafile should have the following format:

     ### UNIX systems

     For a non-ZDB or ZDB backup set session:

```
run{
allocate channel dev1 type 'sbt_tape' parms
 'SBT_LIBRARY=/opt/omni/lib/libob2oracle8.so,
  ENV=(OB2BARTYPE=Oracle8,OB2APPNAME=DB_NAME)';
sql "alter database datafile
 ''/opt/oracle/data/oradata/DATA/temp01.dbf'' offline";
restore datafile
 '/opt/oracle/data/oradata/DATA/temp01.dbf';
recover datafile
 '/opt/oracle/data/oradata/DATA/temp01.dbf';
sql "alter database datafile
 '/opt/oracle/data/oradata/DATA/temp01.dbf' online";
release channel dev1;
}
```

For a ZDB proxy-copy session, allocate one channel for restoring proxy-copy sessions and one channel for database recovery. Release the proxy-copy channel before the recovery:

```
run{
allocate channel dev1 type 'sbt_tape' parms
 'SBT_LIBRARY=/opt/omni/lib/libob2oracle8.so,
  ENV=(OB2BARTYPE=Oracle8,OB2APPNAME=DB_NAME)';
allocate channel dev2 type 'sbt_tape' parms
 'SBT_LIBRARY=/opt/omni/lib/libob2oracle8.so,
  ENV=(OB2BARTYPE=Oracle8,OB2APPNAME=DB_NAME, OB2PROXYCOPY=1)';
sql "alter database datafile
 ''/opt/oracle/data/oradata/DATA/temp01.dbf'' offline";
restore datafile
 '/opt/oracle/data/oradata/DATA/temp01.dbf';
release channel dev2;
recover datafile
 '/opt/oracle/data/oradata/DATA/temp01.dbf';
sql "alter database datafile
 '/opt/oracle/data/oradata/DATA/temp01.dbf' online";
release channel dev1;
}
```

Windows systems

For a non-ZDB or ZDB backup set session:

```
run{
allocate channel dev1 type 'sbt_tape' parms
 'SBT_LIBRARY=Data_Protector_home\bin\orasbt.dll,
  ENV=(OB2BARTYPE=Oracle8,OB2APPNAME=DB_NAME)';
sql "alter database datafile
 ''C:\oracle\data\oradata\DATA\temp01.dbf'' offline";
restore datafile
 'C:\oracle\data\oradata\DATA\temp01.dbf';
recover datafile
 'C:\oracle\data\oradata\DATA\temp01.dbf';
sql "alter database datafile
 ''C:\oracle\data\oradata\DATA\temp01.dbf'' online";
release channel dev1;
}
```

For a ZDB proxy-copy session, allocate one channel for restoring proxy-copy sessions and one channel for the recovery process. Release the proxy-copy channel before the recovery:

```
run{
allocate channel dev1 type 'sbt_tape' parms
 'SBT_LIBRARY=Data_Protector_home\bin\orasbt.dll,
  ENV=(OB2BARTYPE=Oracle8,OB2APPNAME=DB_NAME)';
allocate channel dev2 type 'sbt_tape' parms
 'SBT_LIBRARY=Data_Protector_home\bin\orasbt.dll,
  ENV=(OB2BARTYPE=Oracle8,OB2APPNAME=DB_NAME, OB2PROXYCOPY=1)';
sql "alter database datafile
 ''Oracle_home\data\oradata\DATA\temp01.dbf'' offline";
restore datafile
 'Oracle_home\data\oradata\DATA\temp01.dbf';
release channel dev2;
recover datafile
 'Oracle_home\data\oradata\DATA\temp01.dbf';
sql "alter database datafile
 ''Oracle_home\data\oradata\DATA\temp01.dbf'' online";
release channel dev1;
}
```

- If the database is in a mount state, the script to restore and recover the datafile should have the following format:

  ### UNIX system

  For a non-ZDB or ZDB backup set session:

  ```
  run{
  allocate channel dev1 type 'sbt_tape' parms
   'SBT_LIBRARY=/opt/omni/lib/libob2oracle8.so,
    ENV=(OB2BARTYPE=Oracle8,OB2APPNAME=DB_NAME)';
  restore datafile
   '/opt/oracle/data/oradata/DATA/temp01.dbf';
  recover datafile
   '/opt/oracle/data/oradata/DATA/temp01.dbf';
  release channel dev1;
  }
  ```

  For a ZDB proxy-copy session, allocate one channel for restoring proxy-copy sessions and one channel for the recovery process. Release the proxy-copy channel before the recovery:

  ```
  run{
  allocate channel dev1 type 'sbt_tape' parms
   'SBT_LIBRARY=/opt/omni/lib/libob2oracle8.so,
    ENV=(OB2BARTYPE=Oracle8,OB2APPNAME=DB_NAME)';
  allocate channel dev2 type 'sbt_tape' parms
   'SBT_LIBRARY=/opt/omni/lib/libob2oracle8.so,
    ENV=(OB2BARTYPE=Oracle8,OB2APPNAME=DB_NAME, OB2PROXYCOPY=1)';
  restore datafile
   '/opt/oracle/data/oradata/DATA/temp01.dbf';
  release channel dev2;
  recover datafile
   '/opt/oracle/data/oradata/DATA/temp01.dbf';
  release channel dev1;
  }
  ```

Windows system

For a non-ZDB or ZDB backup set session:

```
run{
allocate channel dev1 type 'sbt_tape' parms
 'SBT_LIBRARY=Data_Protector_home\bin\orasbt.dll,
  ENV=(OB2BARTYPE=Oracle8,OB2APPNAME=DB_NAME)';
restore datafile
 'Oracle_home\data\oradata\DATA\temp01.dbf';
recover datafile
 'Oracle_home\data\oradata\DATA\temp01.dbf';
release channel dev1;
}
```

For a ZDB proxy-copy session, allocate one channel for restoring proxy-copy sessions and one channel for the recovery process. Release the proxy-copy channel before the recovery:

```
run{
allocate channel dev1 type 'sbt_tape' parms
 'SBT_LIBRARY=Data_Protector_home\bin\orasbt.dll,
  ENV=(OB2BARTYPE=Oracle8,OB2APPNAME=DB_NAME)';
allocate channel dev2 type 'sbt_tape' parms
 'SBT_LIBRARY=Data_Protector_home\bin\orasbt.dll,
  ENV=(OB2BARTYPE=Oracle8,OB2APPNAME=DB_NAME, OB2PROXYCOPY=1)';
restore datafile
 'Oracle_home\data\oradata\DATA\temp01.dbf';
release channel dev2;
recover datafile
 'Oracle_home\data\oradata\DATA\temp01.dbf';
release channel dev1;
}
```

You can also save the script into a file and perform a datafile restore using the saved files:

1. Create a file `restore_dbf` in the `/var/opt/omni/tmp` (UNIX systems) or *`Data_Protector_home`*`\tmp` (Windows systems) directory.
2. Start the datafile restore:

   Windows systems: *`ORACLE_HOME`*`/bin/rman target sys/manager@PROD catalog rman/rman@CATAL cmdfile=/var/opt/omni/tmp/restore_dbf`

   UNIX systems: *`ORACLE_HOME`*`\bin\rman target sys/manager@PROD catalog rman/rman@CATAL cmdfile=`*`Data_Protector_home`*`\tmp\restore_dbf`

Example of archive log restore

To restore an archive log:

1. Log in to the Oracle RMAN:

   Windows systems: *`ORACLE_HOME`*`\bin\rman target sys/manager@PROD catalog rman/rman@CATAL`

   UNIX systems: *`ORACLE_HOME`*`/bin/rman target sys/manager@PROD catalog rman/rman@CATAL`

2. Start the archive log restore:

   ```
   run{
   allocate channel dev1 type 'sbt_tape' parms
   'SBT_LIBRARY=/opt/omni/lib/libob2oracle8.so,
    ENV=(OB2BARTYPE=Oracle8,OB2APPNAME=DB_NAME)';
   restore archivelog all;
   release channel dev1;}
   ```

You can also save the script into a file and perform an archive log restore using the saved files:

1. Create a file `restore_arch` in the `/var/opt/omni/tmp` (UNIX systems) or *`Data_Protector_home`*`\tmp` (Windows systems) directory.
2. Start the archive log restore:

   Windows systems: *`ORACLE_HOME`*`\bin\rman target sys/manager@PROD catalog rman/rman@CATAL cmdfile=`*`Data_Protector_home`*`\tmp\restore_arch`

   UNIX systems: *`ORACLE_HOME`*`/bin/rman target sys/manager@PROD catalog rman/rman@CATAL cmdfile=/var/opt/omni/tmp/restore_arch`

Example of database restore using a different device (with the automatic device selection functionality disabled)

Suppose a database was backed up with the device `dev1`. To restore the database with the device `dev2`, add the line `send device type 'sbt_tape' 'CHDEV=dev1>dev2';` to the RMAN script:

1. Log in to the Oracle RMAN:

   Windows systems: *`ORACLE_HOME`*`\bin\rman target sys/manager@TIN`

   UNIX systems: *`ORACLE_HOME`*`/bin/rman target sys/manager@TIN`

2. Execute:

```
run {
allocate channel 'dev_0' type 'sbt_tape'
 parms 'SBT_LIBRARY=C:/PROGRA~1/OmniBack/bin/orasbt.dll,
ENV=(OB2BARTYPE=Oracle8,OB2APPNAME=CAN,OB2BARLIST=test)';
allocate channel 'dev_1' type 'sbt_tape'
 parms 'SBT_LIBRARY=C:/PROGRA~1/OmniBack/bin/orasbt.dll,
ENV=(OB2BARTYPE=Oracle8,OB2APPNAME=CAN,OB2BARLIST=test)';
allocate channel 'dev_2' type 'sbt_tape'
 parms 'SBT_LIBRARY=C:/PROGRA~1/OmniBack/bin/orasbt.dll,
ENV=(OB2BARTYPE=Oracle8,OB2APPNAME=CAN,OB2BARLIST=test)';
send device type 'sbt_tape' 'NO_AUTO_DEVICE_SELECTION=1';
send device type 'sbt_tape' 'CHDEV=dev1>dev2';
restore database;
}
```

NOTE: The line `device type 'sbt_tape' 'NO_AUTO_DEVICE_SELECTION=1';` disables the automatic device selection.

Restoring using another device

Data Protector supports the restore of Oracle database objects from devices other than those on which the database objects were backed up.

Specify these devices in the `/etc/opt/omni/server/cell/restoredev` (UNIX systems) or *`Data_Protector_program_data`*`\Config\server\Cell\restoredev` (Windows systems) file in the following format:

`"DEV 1" "DEV 2"`

where

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

On Windows systems, this file must be in the Unicode format.

Note that this file should be deleted after it is used.

Example

Suppose you have Oracle objects backed up on a device called `DAT1`. To restore them from a device named `DAT2`, specify the following in the **`restoredev`** file:

`"DAT1" "DAT2"`

Instant recovery and database recovery

For general information on instant recovery, see the *HP Data Protector Zero Downtime Backup Concepts Guide* and the *HP Data Protector Zero Downtime Backup Administrator's Guide*. For information on instant recovery in cluster environment (Cluster File System (CFS), MC/ServiceGuard, and Microsoft Cluster Server), see the *HP Data Protector Zero Downtime Backup Administrator's Guide*.

The Data Protector instant recovery functionality is used only to restore the target volumes on which the database files are located. The database recovery part is performed after instant recovery by the RMAN utility. During database recovery, incremental backups and archive log backups performed after ZDB to disk or ZDB to disk+tape are restored from tape. Only those archive logs that do not reside on the target volumes are restored.

IMPORTANT: If the Oracle control file, online redo logs, and SPFILE are on the same source volumes as datafiles and you enable instant recovery by setting the `omnirc` options, note that the control file, SPFILE, and online redo logs are overwritten during the instant recovery.

Prerequisites

- The control file that reflects the internal database structure at the time of backup must be available on the application system. If necessary, restore the appropriate control file from a tape backup.
- The recovery catalog must be open.

Limitations

- For ZDB-to-disk sessions, only archived redo logs can be used for a database recovery after an instant recovery.
- The recovery process will fail if the log entry with the specified logseq number or SCN number was created before the target volume.

RAC preparation steps

In case of RAC, set the following option in the `omnirc` file:

```
ZDB_IR_VGCHANGE=vgchange -a s
```

The instant recovery procedure is the same as without RAC.

However, if instant recovery is to be performed to some other node than the one that was backed up, the following procedure must be performed before the standard instant recovery procedure:

1. Make sure that the MC/SG virtual package is running on the target node.
2. Set the `OB2BARHOSTNAME` environment variable as the virtual hostname before running the configuration from the command line:

   ```
   export OB2BARHOSTNAME=virtual_hostname
   ```

Instant recovery using the Data Protector GUI

To perform an instant recovery:

1. Shut down the Oracle database instance using `sqlplus`. In case of RAC, shut down all instances.

   For example:

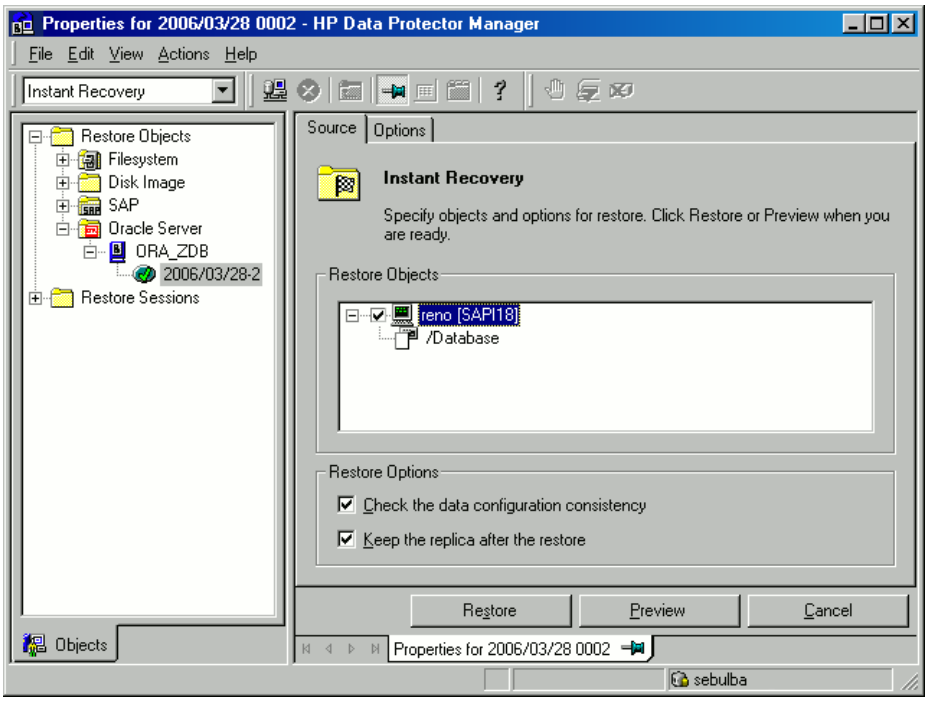
   ```
   sqlplus
   sql> shutdown immediate
   sql> exit
   ```

2. In the Context List, click **Instant Recovery**.

3. Expand **Oracle Server** and select the ZDB-to-disk or ZDB-to-disk+tape session from which you want to perform the restore.
4. In the **Source** tab, select the objects to recover. Only whole databases can be selected. With HP P9000 XP Disk Array Family, it is recommended to leave the **Keep the replica after the restore** option set to enable a restart of an instant recovery session. With HP P6000 EVA Disk Array Family, replica is kept on the disk array only if the **Copy replica data to the source location** is selected.

   Set other HP P6000 EVA Disk Array Family or HP P9000 XP Disk Array Family options. For details, press **F1**.

Figure 34 Selecting backup sessions (P9000 XP Array example)

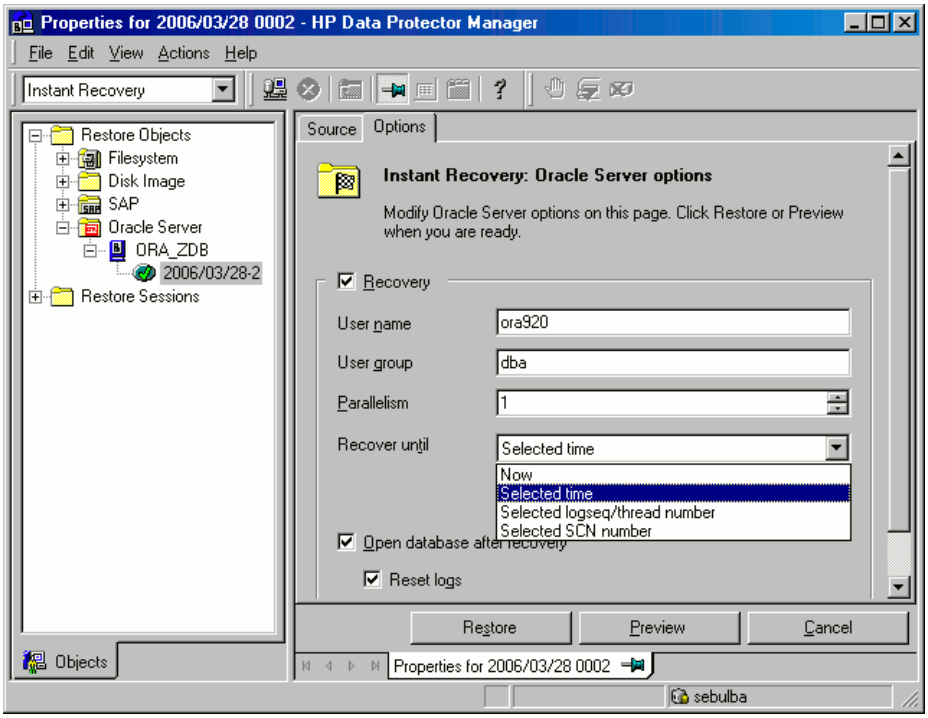


5. At this point, you can decide whether to perform a database recovery immediately after an instant recovery or not:
   - To perform only an instant recovery, click **Restore**.

     NOTE: You can perform a database recovery at a later time either from the Data Protector Manager Restore Context or manually using the RMAN CLI. See "Oracle database recovery after the instant recovery" (page 89).

   - To perform a database recovery immediately after an instant recovery, click on the **Options** tab, select **Recovery** and then select the database recovery options. For a recovery until a selected time, logseq/thread number, or SCN number, it is recommended to reset the log files. See "Oracle recovery options " (page 89) and "Restore, recovery, and duplicate options" (page 73) for details on available options.

Figure 35 Oracle recovery options



6. Click **Restore** or **Preview**. Note that preview only checks if the replica can be restored. It does not check if the database recovery will be successful.

Data Protector recovers the database after performing instant recovery by switching the database to a mount state, restoring the necessary incremental backups and archived redo logs from tape, and applying the redo logs.

If you reset the logs, reset the database; otherwise, Oracle will during the next backup try to use the logs that were already reset and the backup will fail. Login to the target and recovery catalog database and execute:

```
rman target Target_Database_Login catalog Recovery_Catalog_Login
RMAN> RESET DATABASE;
RMAN> exit
```

Oracle database recovery after the instant recovery

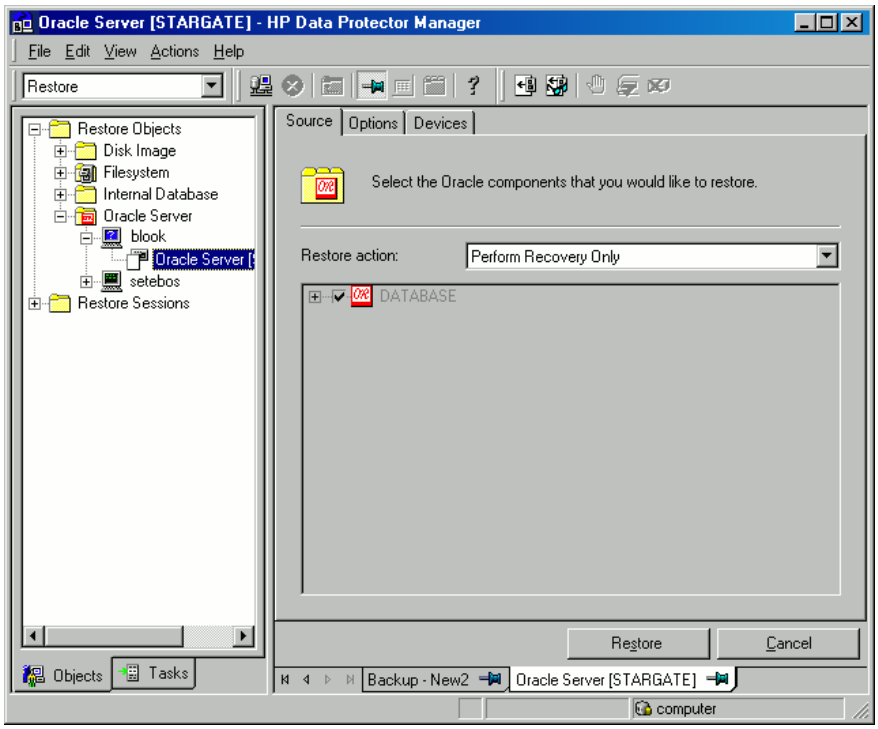
To recover the Oracle database after the instant recovery has been performed, perform the following steps:

1. Put the Oracle database in a mount state by connecting to the target database from the `sqlplus` and then running the following command:

   ```
   startup mount
   ```

2. To recover the database, the following two options are available:
   - Perform a recovery from the Data Protector Manager Restore Context:
     a. Expand **Oracle Server** and select the database to recover. In the **Source** tab, under **Restore action**, select **Perform recovery only**.

Figure 36 Selecting the database for recovery



     b. In the **Options** tab, select the recovery options. For details, see "Restore, recovery, and duplicate options" (page 73).
     c. Click **Restore**.
   - Perform a manual database recovery using RMAN.

     Run the following RMAN script to recover the database:

```
run {
    allocate channel dev1 type 'sbt_tape' parms
     'SBT_LIBRARY=/opt/omni/lib/libob2oracle8.so,
      ENV=(OB2BARTYPE=Oracle8,OB2APPNAME=DB_NAME)';
   recover database;
   sql 'alter database open';
   release channel dev1;
}
```

     For additional examples on how to recover the database after an instant recovery, see "Restoring Oracle using RMAN" (page 76).

Oracle in Veritas Cluster instant recovery

If Oracle on the application system runs in a Veritas Cluster, the following two Veritas Cluster resources must be disabled before instant recovery is performed, and enabled after instant recovery has finished to prevent the failover of the Oracle Veritas Cluster Service Group:

- Veritas Cluster application resource for the Oracle application and
- Veritas Cluster mountpoint resource for the Oracle database files.

Follow the steps below to perform an instant recovery to the application system with Oracle in a Veritas Cluster:

1. On the application system, enter the following commands to disable the two Veritas Cluster resources:
   a. `hares -offline application_resource_name -sys system`

      where *application_resource_name* is the name of the Veritas Cluster application resource for the Oracle application and *system* is the name of the active node.

      `hares -offline mountpoint_resource_name -sys system`

      where *mountpoint_resource_name* is the name of the Veritas Cluster mountpoint resource for the Oracle database files and *system* is the name of the active node.

   b. `hares -modify application_resource_name Enabled 0`

      where *application_resource_name* is the name of the Veritas Cluster application resource for the Oracle application.

      `hares -modify mountpoint_resource_name Enabled 0`

      where *mountpoint_resource_name* is the name of the Veritas Cluster mountpoint resource for the Oracle database files.
2. Perform an instant recovery.
3. If you performed only an instant recovery without the database recovery, use RMAN as described in "Oracle database recovery after the instant recovery" (page 89) to bring the Oracle database to a consistent state.
4. On the application system, enter the following commands to enable the two Veritas Cluster resources:
   a. `hares -modify mountpoint_resource_name Enabled 1`

      where *mountpoint_resource_name* is the name of the Veritas Cluster mountpoint resource for the Oracle database files.

      `hares -modify application_resource_name Enabled 1`

      where *application_resource_name* is the name of the Veritas Cluster application resource for the Oracle application.

   b. `hares -online application_resource_name -sys system`

      where *application_resource_name* is the name of the Veritas Cluster application resource for the Oracle application and *system* is the name of the active node.

      `hares -online mountpoint_resource_name -sys system`

      where *mountpoint_resource_name* is the name of the Veritas Cluster mountpoint resource for the Oracle database files and *system* is the name of the active node.

Aborting sessions

You can abort currently running sessions by clicking the abort button.

If, during a session, RMAN or SQL*Plus do not respond when requested, Data Protector automatically aborts the session. By default, Data Protector waits for the response for 5 minutes. Using `omnirc` options or environment variables `OB2_RMAN_COMMAND_TIMEOUT` and `OB2_SQLP_SCRIPT_TIMEOUT`, you can modify this time interval.

For details of how to set environment variables, see "Setting environment variables" (page 47). For details of how to set the corresponding `omnirc` options, see the *HP Data Protector Help* index: "omnirc option". Note that environment variables override omnirc options.

Troubleshooting

This section contains a list of general checks and verifications and a list of problems you might encounter when using the Data Protector Oracle integration. You can start at "Problems" (page 97) and if you cannot find a solution there, perform general checks and verifications.

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

For general ZDB, restore, and instant recovery troubleshooting information, see the troubleshooting sections in the *HP Data Protector Zero Downtime Backup Administrator's Guide*.

Before you begin

- Ensure that the latest official Data Protector patches are installed. See the *HP Data Protector 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://support.openview.hp.com/selfsolve/manuals for an up-to-date list of supported versions, platforms, and other information.

Checks and verifications

For more detailed information on performing any of the following procedures, see the Oracle documentation.

If your configuration, backup, or restore failed:

- On the application system, verify that you can access the Oracle target database and that it is opened:
  1. Perform the following:

     Windows systems: Set the *ORACLE_HOME* and *DB_NAME* variables.

     UNIX systems: Export the *ORACLE_HOME* and *DB_NAME* variables as follows:

     - If you are using an `sh`-like shell, enter the following commands:

       ```
       ORACLE_HOME="ORACLE_HOME"
       export ORACLE_HOME
       DB_NAME="DB_NAME"
       export DB_NAME
       ```

     - If you are using a `csh`-like shell, enter the following commands:

       ```
       setenv ORACLE_HOME "ORACLE_HOME"
       setenv DB_NAME "DB_NAME"
       ```

  2. Start SQL*Plus from the `bin` directory in the *ORACLE_HOME* directory:

     ```
     sqlplus /nolog
     ```

  3. Start SQL*Plus and type:

     ```
     connect user_name/password@service as sysdba;
     select * from dba_tablespaces;
     exit
     ```

     If this fails, open the Oracle target database.

- On the application system, verify that you can access the recovery catalog (if used) and that it is opened as follows:
  1. Export or set the *ORACLE_HOME* and *DB_NAME* variables as described in Step 1.
  2. Start SQL*Plus from the `bin` directory in the *ORACLE_HOME* directory:

     ```
     sqlplus /nolog
     ```

3. Start SQL*Plus and type:

   ```
   connect Recovery_Catalog_Login
   select * from rcver;
   exit
   ```

   If this fails, open the recovery catalog.

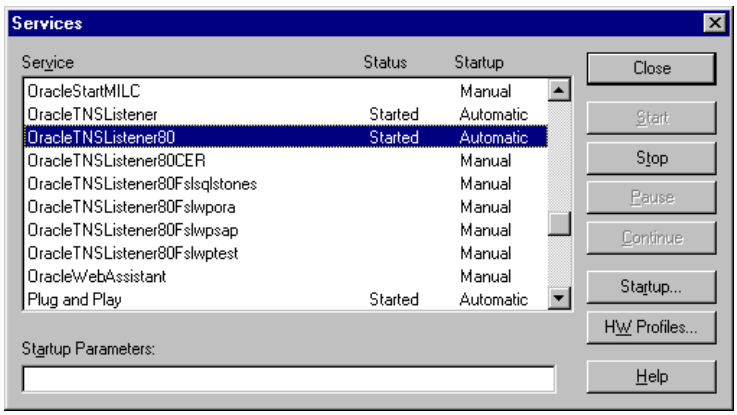
- Verify that the listener is correctly configured for the Oracle target database and the recovery catalog database. This is required to properly establish network connections:
  1. Export or set the *ORACLE_HOME* variable as described in Step 1.
  2. Start the listener from the `bin` directory in the *ORACLE_HOME* directory:

     ```
     lsnrctl status service
     ```

     If this fails, startup the listener process and see the Oracle documentation for instructions on how to create a configuration file (`LISTENER.ORA`).

     On Windows, the listener process can be started in the `Control Panel` > `Administrative Tools` > `Services`.

     Figure 37 Checking the status of the Oracle listener

     The status of the respective listener service in the **`Services`** window should be **`Started`**, otherwise you must start it manually.

  3. Start SQL*Plus from the `bin` directory in the *ORACLE_HOME* directory:

     ```
     sqlplus /nolog
     ```

  4. Start SQL*Plus and type:

     ```
     connect Target_Database_Login
     exit
     ```

     and then

     ```
     connect Recovery_Catalog_Login
     exit
     ```

     If this fails, see the Oracle documentation for instructions on how to create a configuration file (`NAMES.ORA`).

- From the application system, verify that the target database and recovery catalog database are configured to allow remote connections with the system privileges and to allow backup:
  - If you use the recovery catalog database:

    Export or set the *ORACLE_HOME* and *DB_NAME* variables as described in Step 1.

    ```
    SQL> connect login_to_recovery_catalog_or_target_database as sysdba;
    ```

```
> exit
ORACLE_HOME/bin/rman target login_to_target database catalog
login_to_Recovery_Catalog
```

- If you do not use the recovery catalog database:

  Export or set the *ORACLE_HOME* and *DB_NAME* variables as described in Step 1.

  ```
  ORACLE_HOME/bin/rman target login_to_target_database nocatalog
  ```

  See the Oracle documentation for how to set up a password file and parameters in the `initDB_NAME.ora` file and how to add system privileges for a user.

  For information, see the section "Recovery Manager Connection Options" in the *Oracle Backup and Recovery Guide*.

- If you use the recovery catalog database, verify that the target database is registered in the recovery catalog:
  1. Export or set the *ORACLE_HOME* variable as described in Step 1.
  2. Start SQL*Plus from the `bin` directory in the *ORACLE_HOME;* directory:

     ```
     sqlplus /nolog
     ```

  3. Start SQL*Plus and type:

     ```
     connect Recovery_Catalog_Login;
     select * from rc_database;
     exit
     ```

  If this fails, start the configuration using Data Protector on the application system, or see the Oracle documentation for information on how to register an Oracle target database in the recovery catalog database.
- On the application system, verify backup and restore directly to disk using an RMAN channel type disk:

  If you use the recovery catalog:
  1. Export or set the *ORACLE_HOME* variable as described in Step 1.
  2. Start RMAN from the `bin` directory in the *ORACLE_HOME* directory:

     ```
     rman target Target_Database_Login catalog Recovery_Catalog_Login
     ```

  If you do not use the recovery catalog:
  1. Export or set the *ORACLE_HOME* variable as described in Step 1.
  2. Start RMAN from the `bin` directory in the *ORACLE_HOME* directory:

     ```
     rman target Target_Database_Login nocatalog
     ```

  An example of the RMAN backup script is presented below:

  ```
  run {
  allocate channel 'dev0' type disk;
  backup tablespace tablespace_name format
   'ORACLE_HOME/tmp/datafile_name';
  }
  ```

  After a successful backup, try to restore the backed up tablespace by running the following restore script:

  ```
  run {
  allocate channel 'dev0' type disk;
  sql 'alter tablespace tablespace_name offline immediate';
  restore tablespace tablespace_name;
  recover tablespace tablespace_name;
  sql 'alter tablespace tablespace_name online';
  }
  ```

If this fails, see the Oracle documentation for details of how to execute a backup and restore directly to disk using RMAN.

Additionally, if your configuration or backup failed:

- Verify that the Data Protector software has been installed properly.

  For details, see the *HP Data Protector Installation and Licensing Guide*.
- Check if the `SYSDBA` privilege is granted to the Oracle administrator.
- If you have special Oracle environment settings, ensure that they are entered in the Data Protector Oracle configuration files on the Cell Manager. For information on setting the variables in the Data Protector Oracle configuration files, see the `util_cmd` man page or the *HP Data Protector Command Line Interface Reference*.
- Perform a filesystem backup (non-ZDB) of the Oracle Server system so that you can eliminate any potential communication problems between the Oracle Server and the Data Protector Cell Manager system.

  For details on performing filesystem backups, see the *HP Data Protector Help* index: "standard backup procedure".

  Ensure that the hostname defined in the backup specification as a system to be backed up is the name of the application system.
- ***Windows systems:*** Check the `Data Protector Inet` service startup parameters on the Oracle Server system:

  Go to **Control Panel** > **Administrative Tools** > **Services** > **Data Protector Inet**.

  The service must run under a specified user account. Make sure that the same user is also added to the Data Protector `admin` or `user` group.
- Examine the system errors reported in the following file on the application system (Oracle proxy-copy ZDB method) or backup system (Oracle backup set ZDB method):

  Windows systems: *`Data_Protector_program_data`*`\log\debug.log`

  UNIX systems: `/var/opt/omni/log/debug.log`

Additionally, if your backup or restore failed:

- Test the Data Protector internal data transfer using the `testbar2` utility:
  1. Verify that the Cell Manager name is correctly defined on the Oracle Server system. Check the following file, which contains the name of the Cell Manager system:

     Windows systems:
     `Data_Protector_program_data``\Config\client\cell_server`

     UNIX systems: `/etc/opt/omni/client/cell_server`
  2. From the `bin` directory in the *`ORACLE_HOME`* directory, run:

     If backup failed:

     `testbar2 -type:Oracle8 -appname:`*`DB_NAME`*`-perform:backup -bar:`*`backup_specification_name`*

     If restore failed:

     `testbar2 -type:Oracle8 -appname:`*`DB_NAME`*`-perform:restore`

     The hostname should not be specified in the `object` option. It is automatically provided by `testbar2`.
  3. You should see only `NORMAL` messages displayed on your screen, otherwise examine the errors reported by the `testbar2` utility by clicking the **Details** button in the Data Protector **Monitor** context.

  If the messages indicate problems on the Data Protector side of the integration, proceed as follows:

  - Check if the user under which the backup or restore session was started has appropriate Oracle permissions (for example, belongs to the `DBA` group). This user must also be in the Data Protector `operator` or `admin` user group.
  - Check that the respective Data Protector user group has the `See private objects` user right enabled.
  - ***If backup failed:*** Create an Oracle backup specification to back up to a null device or file. If the backup succeeds, the problem may be related to the backup devices. See the *HP Data Protector Troubleshooting Guide* for instructions on troubleshooting devices.
  - ***If restore failed:*** Run the `omnidb` command to see objects in the database.

  If the test fails again, call a support representative for assistance.

Additionally, if your restore failed:

- Verify that an object exists on the backup media.

  This can be done by running the following command on the Oracle server system from the `bin` directory in the *`ORACLE_HOME;`* directory:

  `omnidb -oracle8 "`*`object_name`*`" -session "`*`Session_ID`*`" -media`

  The output of the command lists detailed information about the specified Oracle object, as well as the session IDs of the backup sessions containing this object and a list of the media used. For detailed syntax of the `omnidb` command, see its man page.
- Ensure that the database is in the correct state.

  If you are trying to restore a database item using the Data Protector GUI and the GUI stops responding, try one of the following:

  - If you are restoring the control file, the database should be in the `NoMount` state.

    Open a command window and enter the following:

    `sqlplus/nolog`

```
SQL>connect user/password@service as sysdba
SQL>shutdown immediate
SQL>startup nomount
```

- If you are restoring datafiles, the database should be in the `Mount` state.

  Open a command window and enter the following:

  ```
  sqlplus/nolog
  SQL>connect user/password@service as sysdba
  SQL>shutdown immediate
  SQL>startup mount
  ```

- If there is a problem you cannot resolve while you are trying to restore a database item using the Data Protector GUI, try using the RMAN CLI to restore the database items.

  For information, see "Restoring Oracle using RMAN" (page 76).

- Try putting the database into the Open state manually after using the Data Protector GUI to recover and restore a backup session.

  If you have used the Data Protector GUI to recover and restore a backup session and you see the following error message:

  ```
  Oracle Error: ORA-1589: must use RESETLOGS or NORESETLOGS option
  for database open.
  ```

  Open a SQLplus window and use the following command:

  ```
  sqlplus/nolog
  SQL>connect user/password@service as sysdba
  SQL>alter database open noresetlogs;
  ```

  If this does not work, try using the following command:

  ```
  SQL>alter database open resetlogs;
  ```

Problems

Problem

SQL*Plus is unable to connect to destination

Action

Check if the Oracle listener process is up and running. Check if there are any environment variables you need to enter (for example, `TNS_ADMIN`). Enter these variables in the Data Protector Oracle configuration files on the Cell Manager. For information, see the `util_cmd` man page.

Problem

The following error is displayed: ORA-12532: : invalid argument

If this is reported by SQL*Plus in the Data Protector monitor, the application system may be low on resources (CPU, memory, and so on).

Action

Try to configure the application system in such a way that it consumes as little resources as possible. This error can be reproduced without using Data Protector by starting SQL*Plus on the application system, and connecting to the target database on the application system.

Problem

Backup set ZDB is aborted after 10 minutes

While performing a backup set ZDB, the following warning is displayed for each database datafile:

```
RMAN-06554: WARNING: file n is in backup mode
```

The ZDB session then aborts with the following message:

```
Bar backup session was started but no client connected in 600 seconds.
```

Action

Increase the value of the following global options (by default, these options are set to 10):

- If you upgraded Data Protector from a previous version of Data Protector:

  `SmWaitForFirstClient=minutes`

- If you performed a clean installation:

  `SmWaitForFirstBackupClient=minutes`

For more information about the global options, see the *HP Data Protector Troubleshooting Guide*.

Problem

Backup set ZDB fails after changing the physical schema of the Database

Backup fails after you have modified the physical schema of a database, for example, if you added or dropped a tablespace, added a new datafile, or added or dropped a rollback segment. Depending on the performed modification, different error messages are displayed, for example:

```
RMAN-06056: could not access datafile datafile
```

The problem occurs because the physical schema of target database is not updated in the recovery catalog.

Action

Manually re-synchronize the recovery catalog database with the current control file.

Problem

On UNIX systems, a backup set ZDB-to-disk+tape session fails

While performing a backup set ZDB to disk+tape, the session fails with the following error when Oracle Server attempts to start up an instance on the backup system:

```
[Major] From: ob2rman@computer.company.com DB_NAME Time: Date Time
The database reported error while performing requested operation.
```

This problem occurs when either the user ID or the group ID number of the Oracle operating system user account on the application and backup systems do not match. Under such circumstances, Oracle Server is unable to start up the instance on the backup system due to missing privileges.

Action

Configure the user accounts as described in "Configuring Oracle operating system user accounts" (page 37), and restart the session.

Problem

Proxy copy restore fails

Proxy copy restore fails with the following error:

```
RMAN-10035: exception raised in RPC: ORA-27197: skgfprs: sbtpcrestore
returned error
```

```
RMAN-10031: ORA-27197 occurred during call to
DBMS_BACKUP_RESTORE.PROXYRESTOREDATAFILE
```

Action

Check the IDB for the session and the objects of the latest backup. You might check if a more recent session exists in the recovery catalog. Connect to the RMAN prompt:

`rman target user/password@TGT_DB catalog user/password@CDB`

At the `RMAN>` prompt, enter

```
list backup;
```

to display a list of the objects in the recovery catalog. Check the list of Proxy Copy sessions, listed at the end.

To synchronize the recovery catalog and the IDB, run the RMAN command:

```
resync catalog;
```

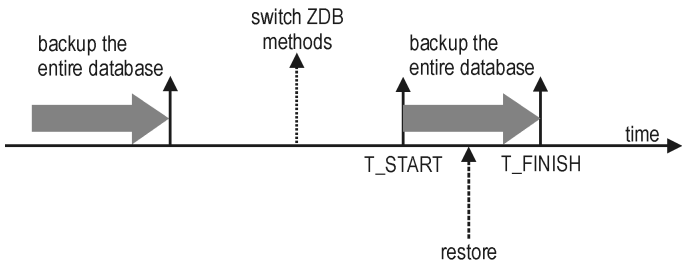
After the synchronization is performed, restore should be possible.

Problem

Restore after a switch between ZDB methods fails

If you perform a restore to a specified time (`T_RESTORE`) that lies in the time interval between the start of the first backup of the entire database using the new method (`T_START`), and before this backup is finished (`T_FINISH`), RMAN may try to restore the backup files made with the new method using a channel allocated for backup files made using the previous method. As a result, the restore procedure fails.

Figure 38 Restore after a switch between ZDB methods fails



Action

Restore the backup session manually using RMAN scripts. Add the required parameter to the allocated channels, that is `OB2PROXYCOPY=1` for the channel which will be used for restoring the backup made using the proxy-copy ZDB method. Then restore the backup files using the correct channels.

For example, if you switched from the backup set to the proxy-copy ZDB method, the script may look similar to the following one:

```
run {
ALOCATE CHANNEL 'dev_0' TYPE 'sbt_tape'
PARMS 'SBT_LIBRARY=Path_to_Data_Protector_MML,
  ENV(OB2BARTYPE=Oracle8,OB2APPNAME=DB_NAME)';
ALOCATE CHANNEL 'dev_1' TYPE 'sbt_tape'
PARMS 'SBT_LIBRARY=Path_to_Data_Protector_MML,
  ENV(OB2BARTYPE=Oracle8,OB2APPNAME=DB_NAME,
OB2PROXYCOPY=1)';
RESTORE DATAFILE list_of_backup_set_backups UNTIL
 T_RESTORE CHANNEL 'dev_0';
RESTORE DATAFILE list_of_proxy-copy_backups UNTIL
 T_RESTORE CHANNEL 'dev_1';
RELEASE 'dev_0';
```

```
RECOVER DATABASE UNTIL T_RECOVER ...
RELEASE 'dev_1';
}
```

Where:

T_RESTORE specifies the time to which to restore and *T_RECOVER* the time to which to apply the transactions.

list_of_backup_set_backups is a list of backups of the entire database using the backup set ZDB method.

list_of_proxy_copy_backups is a list of datafile backups completed after the start of the backup of the entire database (T_START) and before *T_RESTORE*.

Problem

Data Protector reports errors when calling SYS.LT_EXPORT_PKG.schema_inf_exp during Oracle backup

The following errors are listed in the Data Protector monitor:

```
EXP-00008: ORACLE error 6550 encountered
ORA-06550: line 1, column 13:
PLS-00201: identifier 'SYS.LT_EXPORT_PKG' must be declared
ORA-06550: line 1, column 7:
PL/SQL: Statement ignored
EXP-00083: The previous problem occurred when calling
SYS.LT_EXPORT_PKG.schema_info_exp
. exporting statistics
Export terminated successfully with warnings.
[Major] From: ob2rman.pl@machine "MAKI"  Time: 10/01/01 16:07:53
Export of the Recovery Catalog Database failed.
```

Action

Start SQL*Plus and grant the execute permission to the LT_EXPORT_PKG as follows (make sure that the user sys has the SYSDBA privilege granted beforehand):

```
sqlplus 'sys/password@CDB as sysdba'
SQL> grant execute on sys.lt_export_pkg to public;
```

Restart the failed backup session.

Problem

On a UNIX system, Data Protector reports "Cannot allocate/attach shared memory"

Backup fails and the following error message is displayed:

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

Action

Set the OB2SHMEM_IPCGLOBAL omnirc option to 1 to use the memory windowing properly, and restart the failed backup session. See the *HP Data Protector Troubleshooting Guide* for details on using the omnirc file.

Problem

Backup fails after a point in time restore and recovery

The following error is displayed:

```
RMAN-06004: ORACLE error from recovery catalog database: RMAN-20003:
target database incarnation not found in recovery catalog
```

Action

Connect to the target and recovery catalog database using RMAN and reset the database to register the new incarnation of database in the recovery catalog:

```
rman target Target_Database_Login catalog Recovery_Catalog_Login
RMAN> RESET DATABASE;
RMAN> exit
```

Problem

Oracle online backup fails with the following error:

```
RMAN-06004: ORACLE error from recovery catalog database: RMAN-20220:
controlfile copy not found in the recovery catalog
```

When running an online backup, Data Protector adds the filename of the *controlfilecopy* to the RMAN backup script. This filename has to be cataloged to the RMAN catalog prior to the backup command.

Action

To catalog the *controlfilecopy* to the RMAN catalog:

1. Connect to RMAN on the application system.
2. Run the following command:

   ```
   RMAN> catalog controlfilecopy 'CONTROL_FILE_LOCATION/ctrlDB_NAME.ctl'
   ```

Problem

Backup of archive logs on RAC cannot be performed

On RAC, the archive logs are not installed on a NFS mounted disk. Backup of archive logs cannot be performed.

Action

Edit the archive logs backup specification:

- Add an additional `allocate channel` command for *each* node.
- Add a command to connect to each instance. The connection parameters should be given as *username/passwd@INSTANCE*.

For example, if you are using two nodes, the backup specification might look as follows:

```
run {
allocate channel 'dev_0' type 'sbt_tape' parms
 'SBT_LIBRARY=Path_to_Data_Protector_MML,
  ENV=(OB2BARTYPE=Oracle8,OB2APPNAME=DB_NAME,OB2BARLIST=RAC_arch)'
 connect username/passwd@INSTANCE_1;
allocate channel 'dev_2' type 'sbt_tape' parms
 'SBT_LIBRARY=Path_to_Data_Protector_MML,
  ENV=(OB2BARTYPE=Oracle8,OB2APPNAME=DB_NAME,OB2BARLIST=RAC_arch)'
connect username/passwd@INSTANCE_2;
backup
 format 'RAC_arch<QU_%s:%t:%p>.dbf'
 archivelog all;
}
```

Problem

The Recovery Catalog was lost and the control file cannot be restored from Data Protector managed backup

The Recovery Catalog was not used, the RMAN autobackup feature was not used, and the control file cannot be restored from Data Protector managed backup. A valid control file backup exists on tape.

Action

Restore the control file from RMAN backup set, mount and restore the database, and perform database recovery:

```
run {
allocate channel 'dev_0' type 'sbt_tape' parms
 'SBT_LIBRARY=Path_to_Data_Protector_MML';
restore controlfile from 'backup piece handle';
sql 'alter database mount';
set until time 'MMM DD YY HH24:MM:SS';
restore database;
recover database;
sql 'alter database open resetlogs';
release channel 'dev_0';
}
```

At this point you must manually register any backups made after the control file backup that was restored. After that, continue with the restore procedure.

For the *backup piece handle* search the Data Protector Internal Database and session outputs of previous backup sessions.

Problem

How to modify the RMAN restore script

When you start a restore of an Oracle database using the Data Protector GUI or CLI, an RMAN restore script is created, which is instantly run, so you cannot edit it first.

Action

To edit the script before it is run, set the Data Protector `omnirc` option `OB2RMANSAVE` to point to an existing directory. When the variable is set and you start a restore, the RMAN restore script, which is created at run time, is saved to the specified location under the name `RMAN_restore_`*`backup_specification_name`*`.rman`, and the actual restore is skipped. Then you can edit the script and run it manually afterwards. On how to set the `omnirc` options, see the *HP Data Protector Help* index: "omnirc options".

To start a restore using Data Protector again, clear the `OB2RMANSAVE` option by deleting its content or commenting or removing the whole option. If you comment or remove the option on a Windows system, restart the Data Protector `Inet` service for the settings to take effect.

Problem

Instant recovery session for an Oracle database fails

On a Windows Server 2008 x64 system, when you run an instant recovery from a backed up Oracle 11g application database that resides on a disk array of the HP P6000 EVA Disk Array Family, the session may fail with the following error messages:

```
[Major] From: SMISA@appsystem.company.com "SMISA"
    Time: 5/17/2010 5:00:50 AM
        A filesystem could not be mounted.
        Filesystem name :
        Mount point : I:\
[Critical] From: SMISA@appsystem.company.com "SMISA"
    Time: 5/17/2010 5:00:50 AM
        Failed to resume the application system.
[Critical] From: SMISA@appsystem.company.com "SMISA"
    Time: 5/17/2010 5:00:50 AM
        Instant Recovery failed.
```

Such an instant recovery failure occurs when the “copy-back” instant recovery method (the default) is chosen and the following instant recovery options are selected in the Source and Options panes of the Data Protector GUI:

- Wait for the replica to complete (with the default waiting period used)
- Retain source for forensics
- Check the data configuration consistency
- Force the removal of all replica presentations
- Recovery
- Open database after recovery

Action

On the application system and the backup system, set the values of the `omnirc` options `ZDB_DELAY_BEFORE_RESCAN` and `ZDB_DELAY_AFTER_RESCAN` to `300` and restart the instant recovery session.

Problem

Instant recovery of an Oracle database fails

An instant recovery session for an Oracle database fails with a message similar to the following:

```
[Normal] From: ob2rman@x64-node1.x64ring.com "testdb"  Time:
 2/7/2008 10:48:19 AM
 Starting target database instant recovery.

 Net service name: testdb.
 Instance status: .
 Instance name: .
 Database DBID = .
 Database control file type: .
 Database log mode: .


[Major] From: ob2rman@x64-node1.x64ring.com "testdb"  Time:
 2/7/2008 10:48:20 AM
 The database reported error while performing requested operation.
```

Note that the database parameters are empty, which happens when Data Protector is not able to connect to the Oracle database.

Action

Data Protector must be able to connect to the Oracle database even when the database is in the `Mount` or `Nomount` state. One way of achieving this is by configuring static service information for your Oracle listener. For details, see the Oracle documentation.

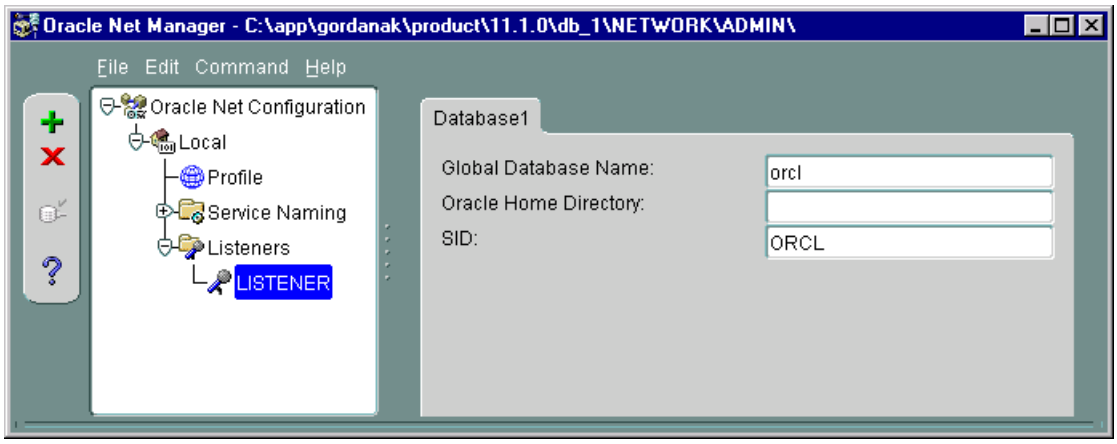
The following example shows how static service information is configured using the Oracle Net Manager.

Suppose you have the following environment:

Listener name: `LISTENER`
Global database name: `orcl`
Oracle SID: `ORCL`

To configure static service information for the listener, open the Oracle Net Manager, select the listener, go to the **Database Services** context, add a database and specify the Oracle database parameters.

Figure 39 Configuring an Oracle listener



As a result, the `listener.ora` file gets updated with the `SID_LIST_LISTENER` section.

```
SID_LIST_LISTENER =
  (SID_LIST =
    (SID_DESC =
      (GLOBAL_DBNAME = orcl)
      (SID_NAME = ORCL)
    )
  )
```

At the end, restart the Oracle listener service to apply the changes.

Problem

"IPC Invalid Hostname or IP Address" error message is displayed when browsing Oracle restore sessions

The following error message is displayed when browsing the Oracle database for restore sessions in the Data Protector GUI Restore context:

```
IPC Invalid Hostname or IP Address
```

The problem can appear in the following cases:

- When restoring database items to a different client.
- When importing Data Protector media containing backups of Oracle database from another Data Protector cell.
- When restoring 64-bit Oracle version 10.2.0.4 in the RAC environment, on HP-UX 11.23 PA-RISC systems. If `util_orarest` is present on the system, this error can mean that the `util_orarest` agent ends abnormally while trying to load the 32-bit OCI library from the *`ORACLE_HOME`*`/lib32` directory.

Actions

- To successfully restore database items to a different client, make sure that the system on which the Data Protector Oracle integration agent will be started is configured as Data Protector Oracle database instance (*`ORACLE_SID`*).

  To verify, check if it is listed in the **Client** drop-down list in the **Options** page.

  Select the system and proceed with Step 6 of the "Restoring Oracle database objects" (page 68) procedure.

- When restoring 64-bit Oracle database in RAC environment, on HP-UX 11.23, resolve the problem as follows:

  In the directory *`ORACLE_HOME`*`/lib` remove the soft link `libclntsh.sl`, which points to the 64-bit OCI library *`ORACLE_HOME`*`/lib/liblntsh.sl.10.1`.

Problem

When editing the RMAN script section of a backup specification using the Data Protector GUI, an RMAN backup script error is displayed

In the Data Protector GUI, when you edit the RMAN script section of a Data Protector backup specification, the following error message may display:

```
Cannot proceed, invalid RMAN backup script.
```

The error is displayed if you have specified an Oracle RMAN parameter, which has not been recognized by the Data Protector parser or a parsing error has occurred.

Action

Disable Oracle RMAN script parsing in the Data Protector GUI by setting the Data Protector `NoGUIRMANScriptParsing` global option to `1`.

For details of how to set the option, see the *HP Data Protector Help* index: "global options".

2 Data Protector SAP R/3 ZDB integration

Introduction

This chapter explains how to configure and use the Data Protector SAP R/3 ZDB integration (**SAP R/3 ZDB integration**). It describes concepts and methods you need to understand to back up and restore the following files of the SAP R/3 database environment (**SAP R/3 objects**):

- Data files
- Control files
- Online redo logs
- Offline (archived) redo logs
- SAP R/3 logs and parameter files

Data Protector supports offline and online backups. During an online backup, the SAP R/3 application is actively used.

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

- ZDB to disk
- ZDB to tape
- ZDB to disk+tape

Data Protector supports only a filesystem restore. You can restore SAP R/3 files:

- To the original location
- To another client
- To another directory

"Backup and restore sessions" (page 106) shows which restore methods are available, depending on the ZDB session you restore from.

Table 8 Backup and restore sessions

ZDB type	Restore methods
ZDB to tape	Standard restore
ZDB to disk	Instant recovery
ZDB to disk+tape	Standard restore, instant recovery

When the instant recovery completes, you can recover the database to a specific point in time using the SAP BRTOOLS interface.

Table 9 Supported disk arrays and array configurations

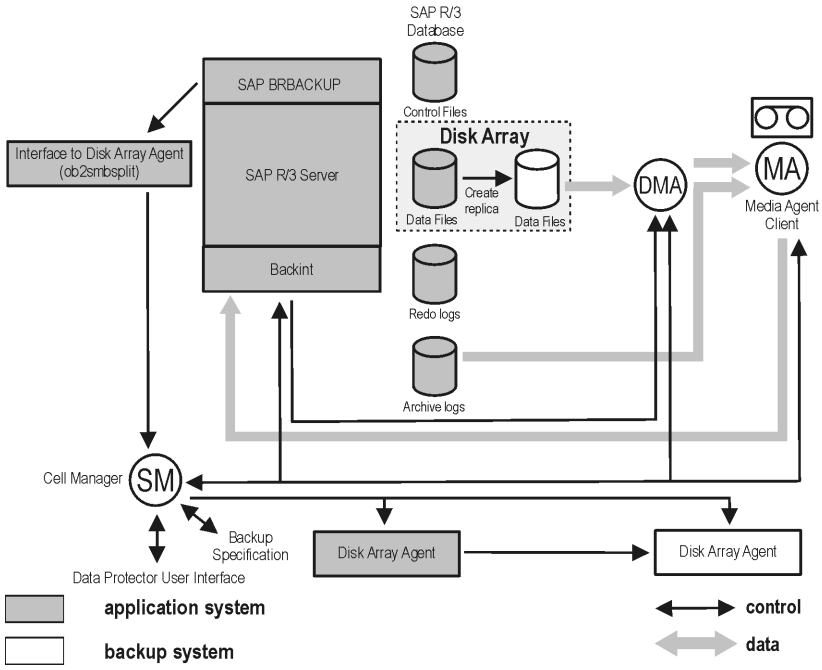
Supported array	Supported configurations
EMC Symmetrix (EMC)	TimeFinder, SRDF, combined SRDF+TimeFinder
HP P9000 XP Disk Array Family (P9000 XP Array)	HP BC P9000 XP, HP CA P9000 XP, combined HP CA+BC P9000 XP
HP P6000 EVA Disk Array Family (P6000 EVA Array)	HP BC P6000 EVA, combined HP CA+BC P6000 EVA

This chapter provides information specific to the Data Protector SAP R/3 ZDB integration. For general Data Protector procedures and options, see the *HP Data Protector Help*. For details on ZDB terminology, ZDB types, advantages of offline and online backups, and instant recovery concepts, see the *HP Data Protector Zero Downtime Backup Concepts Guide*.

Integration concepts

"SAP R/3 integration architecture" (page 107) shows the architecture of the Data Protector SAP R/3 ZDB integration. The figure illustrates the preferred configuration, in which the Oracle control file, online redo log files, and Oracle SPFILE reside on a different volume group than the Oracle data files.

Figure 40 SAP R/3 integration architecture

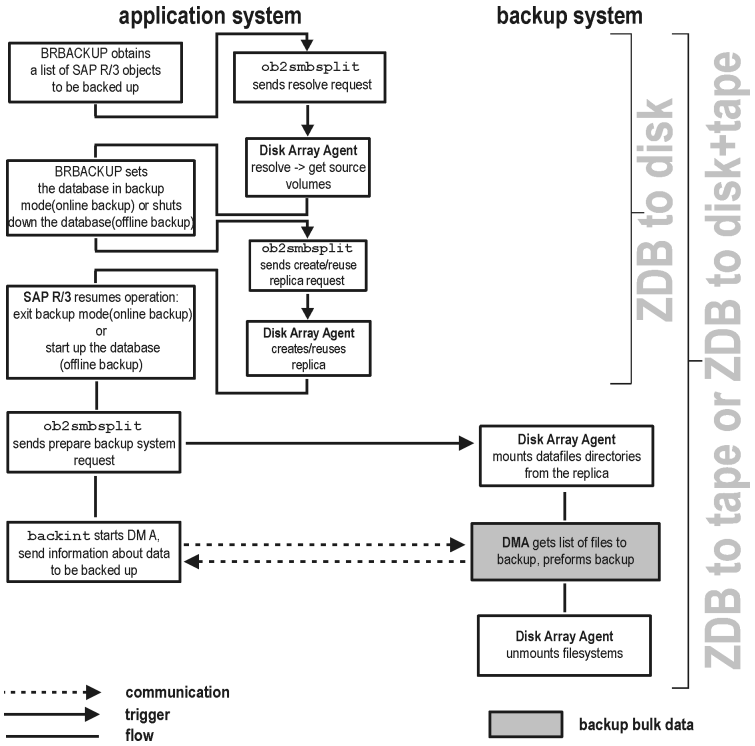


For other supported configurations, see "ZDB integrations omnirc options" (page 254).

ZDB flow

For details of how ZDB options affect the ZDB flow, including mounting, activating volume or disk groups and so on, see the *HP Data Protector Zero Downtime Backup Administrator's Guide*.

Figure 41 SAP R/3 ZDB session flow (BRBACKUP started on the application system)



1. The SAP R/3 backup specification is read and the Data Protector `omnisap.exe` program is started on the application system.
2. `Omnisap.exe` starts BRBACKUP, which switches the database to the backup mode (online backup) or shuts down the database (offline backup), and starts the split command on the application system, with the list of files to be included in the replica creation.

   The database is put out of the backup mode (online backup) or is restarted (offline backup) after the replica is created.

   NOTE: Data Protector can use the `splitint` interface (if BRTOOLS supports it) to reduce the time during which the database is in the backup mode.

3. The Data Protector `ob2smbsplit` command resolves the backup configuration, creates a replica, and preparing the replica for backup.

   The mountpoints for the backed up object are created on the backup system.

   The backup volume/disk groups are activated and the filesystems are mounted on the backup system.

4. **ZDB to disk:** The remaining ZDB options are processed and the details on the session are written to the ZDB database. The session then finishes.
5. ***ZDB to tape, ZDB to disk+tape:*** BRBACKUP starts the Data Protector `backint` program, which starts establishing a connection between the Data Protector Data Movement Agents (DMA) on the backup system and the General Media Agents (MA). The process is coordinated by the Data Protector Backup Session Manager (BSM). When the connection is established, the data specified for backup is streamed to tape.

   NOTE: You can configure SAP to use a third-party `backint` tool to perform ZDB-to-disk+tape backup sessions. To enable this feature, set the `OB2_3RD_PARTY_BACKINT` environment variable to `1` and copy the `backint` you want to use to the SAP BRTOOLS directory. In case of a ZDB-to-disk+tape backup session, a `disk_only` backup object is created in the Data Protector IDB. The third-party `backint` starts after the split and is responsible for backing up the needed files.

6. When the data transfer completes, the backup system is disabled (filesystems are dismounted on all platforms and volume/disk groups deactivated on UNIX).
7. ***EMC and P9000 XP Array:*** Links are re-established, depending on how ZDB options are specified.

Data Protector SAP R/3 configuration file

Data Protector stores the integration parameters for every configured SAP R/3 database in the following file on the Cell Manager:

Windows systems:

Data_Protector_program_data\Config\Server\Integ\Config\Sap*ClientName%ORACLE_SID*

UNIX systems: /etc/opt/omni/server/integ/config/SAP/*ClientName%ORACLE_SID*

The parameters stored are:

- Oracle home directory
- encoded connection string to the target database
- BRTOOLS home directory
- the variables which need to be exported prior to starting a backup
- SAPDATA home directory
- user name and user group
- temporary directory used for the copy of the control file or redo logs
- list of control files and redo logs that will be copied to a safe location
- character set (ORA_NLS_CHARACTERSET)
- speed parameters (time needed for a specific file to back up - in seconds)
- manual balancing parameters

The configuration parameters are written to the Data Protector SAP R/3 configuration file:

- during configuration of the integration
- during creation of a backup specification
- when the configuration parameters are changed

IMPORTANT: To avoid problems with your backups, take extra care to ensure the syntax and punctuation of your configuration file match the examples.

NOTE: You can set up the parameters in the `Environment` section (sublist) of the file by referring to other environment variables in the following way:

```
SAPDATA_HOME=${ORACLE_HOME}/data
```

Syntax

The syntax of the Data Protector SAP R/3 configuration file is as follows:

```
ORACLE_HOME='ORACLE_HOME';
ConnStr='ENCODED_CONNECTION_STRING_TO_THE_TARGET_DATABASE';
BR_directory='BRTOOLS_HOME';
SAPDATA_HOME='SAPDATA_HOME';
ORA_NLS_CHARACTERSET='CHARACTER_SET';
OSUSER='USER_NAME';
OSGROUP='USER_GROUP';
Environment={
[ENV_var1='value1';]
[ENV_var2='value2';
  ...]
```

```
}
SAP_Parameters={backup_spec_name=('-concurrency #_of_concurrency
' | '-time_balance' | '-load_balance' | '-manual_balance');
}
speed={
AVERAGE=1;
'filename'=#_of_seconds_needed_to_back_up_this_file;
}
compression={'filename'=size_of_the_file_in_bytes_after_the
_compression;
}
manual_balance={backup_specification_name={
'filename'=device_number;
 }
 }
```

The ORA_NLS_CHARACTERSET parameter is set automatically by Data Protector during SAP R/3 database configuration. For details of how to configure SAP R/3 database for use with Data Protector, see "Configuring SAP R/3 databases" (page 119).

Example

This is an example of the file:

```
ORACLE_HOME='/app/oracle805/product';
ConnStr='EIBBKIBBEIBBFIBBGHBBOHBB
QDBBOFBBCFBBPFBBCFBBIFBBGFBBDGBBBFBBCFBBDFBBCFBB';
BR_directory='/usr/sap/ABA/SYS/exe/run';
SAPDATA_HOME='/sap';
ORA_NLS_CHARACTERSET='USASCII7';
OSUSER='orasid';
OSGROUP='dba';


Environment={   }
 SAP_Parameters={
  sap_weekly_offline=('-concurrency 1','-no_balance');
  sap_daily_online=('-concurrency 3','-load_balance');
  sap_daily_manual=('-concurrency 3','-manual_balance');
 }
 speed={
  AVERAGE=203971;
'/file1'=138186;
'/file2'=269756;
 }
 compression={
'/file1'=1234;
'/file2'=5678;
 }
 manual_balance={
  sap_daily_manual={
'/file1'=1; /* file 1 is backed up by the first sapback */
'/file2'=2; /* file 2 is backed up by the second sapback */
'/file3'=1; /* file 3 is backed up by the first sapback */
'/file4'=1;
  }
 }
```

Setting, retrieving, listing, and deleting Data Protector SAP R/3 configuration file parameters using the CLI

The Data Protector SAP R/3 configuration file parameters are normally written to the Data Protector SAP R/3 configuration file after:

- the Data Protector configuration of the Oracle instance that is run by SAP R/3 is completed.
- a new backup specification is created.
- a backup that uses balancing by time algorithm is completed.

The `util_cmd` command

You can set, retrieve, list, or delete the Data Protector SAP R/3 configuration file parameters using the `util_cmd -putopt` (setting a parameter), `util_cmd -getopt` (retrieving a parameter), or `util_cmd -getconf` (listing all parameters) command on the Data Protector SAP R/3 client.

Cluster-aware clients

In a cluster environment, the environment variable `OB2BARHOSTNAME` must be defined as the virtual hostname before executing the `util_cmd` command from the command line (on the client). The `OB2BARHOSTNAME` variable is set as follows:

Windows systems: `set OB2BARHOSTNAME=virtual_hostname`

UNIX systems: `export OB2BARHOSTNAME=virtual_hostname`

The `util_cmd` synopsis

The syntax of the `util_cmd` command is as follows:

```
util_cmd -getconf[ig] SAP oracle_instance [-local filename]
util_cmd -getopt[ion] [SAP oracle_instance] option_name [-sub[list] sublist_name] [-local filename]
util_cmd -putopt[ion] [SAP oracle_instance] option_name [option_value] [-sub[list] sublist_name] [-local filename]
```

where:

`option_name` is the name of the parameter

`option_value` is the value for the parameter

`[-sub[list] sublist_name]` specifies the sublist in the configuration file to which a parameter is written to or taken from.

`[-local filename]` specifies one of the following:

- When it is used with the `-getconf[ig]` option, it specifies the filename for the output of the command to be written to. If the `-local` option is not specified, the output is written to the standard output.
- When it is used with the `-getopt[ion]`, it specifies the filename of the file from which the parameter and its value are to be taken and then written to the standard output. If the `-local` option is not specified, the parameter and its value are taken from the Data Protector SAP R/3 configuration file and then written to the standard output.
- When it is used with the `-putopt[ion]` option, it specifies the filename for the output of the command to be written to. If the `-local` option is not specified, the output is written to the Data Protector SAP R/3 configuration file.

NOTE: If you are setting the *`option_value`* parameter as a number, the number must be put in single quotes, surrounded by double quotes.

Return values

The `util_cmd` command displays a short status message after each operation (writes it to the standard error):

- `Configuration read/write operation successful.`

  This message is displayed when all the requested operations have been completed successfully.

- `Configuration option/file not found.`

  This message is displayed when either an option with the specified name does not exist in the configuration, or the file specified as the `-local` parameter does not exist.

- `Configuration read/write operation failed.`

  This message is displayed if any fatal errors occurred, for example: the Cell Manager is unavailable, the Data Protector SAP R/3 configuration file is missing on the Cell Manager, and so on.

Setting parameters

To set the Data Protector `OB2OPTS` and the Oracle `BR_TRACE` parameters for the Oracle instance `ICE` that is run by SAP R/3, use the following commands on the Data Protector SAP R/3 client:

Windows, HP-UX, Solaris systems

```
util_cmd -putopt SAP ICE OB2OPTS '-debug 1-200 debug.txt' -sublist
Environment
util_cmd -putopt SAP ICE BR_TRACE "'10'" -sublist Environment
```

Retrieving parameters

To retrieve the value of the `OB2OPTS` parameter for the Oracle instance `ICE`, use the following command on the Data Protector SAP R/3 client:

```
util_cmd -getopt SAP ICE OB2OPTS -sublist Environment
```

Listing parameters

To list all the Data Protector SAP R/3 configuration file parameters for the Oracle instance `ICE`, use the following command on the Data Protector SAP R/3 client:

```
util_cmd -getconf SAP ICE
```

Deleting parameters

To remove the value of the `OB2OPTS` parameter for the Oracle instance `ICE`, use the following command on the Data Protector SAP R/3 client:

```
util_cmd -putopt SAP ICE OB2OPTS "" –sublist Environment
```

Configuring the integration

To configure the integration:

1. Configure the required user accounts. See "Configuring user accounts" (page 115).
2. Configure SQL*Net V2 or Net8 TNS listener. See "Configuring SQL*Net V2 or Net8 TNS listener" (page 116).
3. Check the connection to the Oracle database from the application system. See "Checking the connection" (page 116).
4. Enable the use of the authentication password file. See "Authentication password file" (page 117).
5. Optionally, set the archived logging mode to enable online backups. See "Enabling archived logging" (page 117).

6. Share directories on the application system. See "Sharing directories on the application system" (page 118).
7. Configure every SAP R/3 database you intend to back up from or restore to. See "Configuring SAP R/3 databases" (page 119).
8. Configure the SAP R/3 parameter file. See "Configuring the SAP R/3 parameter file" (page 124).

Prerequisites

- Ensure that you have correctly installed and configured the SAP R/3 application. The database used by the SAP R/3 application must be an Oracle database. If any other database is used, you can back it up using the corresponding Data Protector integration. It is assumed that you are familiar with the SAP R/3 application and Oracle database administration.
  - For supported versions, platforms, devices, and other information, see the latest support matrices at http://support.openview.hp.com/selfsolve/manuals.
  - For information on installing, configuring, and using the SAP R/3 application and the SAP backup and restore tools (BRBACKUP, BRRESTORE, and BRARCHIVE), see the SAP R/3 application documentation.
- Ensure that you have a license to use the Data Protector SAP R/3 ZDB integration. For information, see the *HP Data Protector Installation and Licensing Guide*.
- Ensure that you have correctly installed Data Protector.
  - For information on how to install the Data Protector disk array integration (P6000 EVA Array, P9000 XP Array, or EMC) with SAP R/3 in various architectures, see the *HP Data Protector Installation and Licensing Guide*.
  - On how to configure the Data Protector ZDB integration (EMC, P9000 XP Array, or P6000 EVA Array), see the *HP Data Protector Zero Downtime Backup Administrator's Guide*.
  - For information on the Data Protector Cell Manager package configuration in the MC/SG cluster, see the *HP Data Protector Help* index: "MC/ServiceGuard integration".

  NOTE: You cannot run ZDB sessions in the RMAN mode.
- The SAP R/3 directories `SAPBACKUP`, `SAPARCH`, `SAPREORG`, `SAPCHECK`, and `SAPTRACE` must not reside on the same disk array source volumes as the data files. Otherwise, the BRTOOLS data needed for complete recovery of a database is overwritten during instant recovery. You can set the locations for these directories in the `init`*`DBSID`*`.sap` file.

Before you begin

- Configure devices and media for use with Data Protector.
- To test whether the SAP R/3 system and the Cell Manager communicate properly, configure and run a Data Protector filesystem backup and restore.
- ***Windows systems:***
  - On Windows Server 2003 system, you need to restart the `Data Protector Inet` service under the Oracle operating system user account described in "Configuring user accounts" (page 115).

    For information on changing the user account under which the `Data Protector Inet` service is running, see the *HP Data Protector Help* index: "Inet, changing account".
  - On other Windows operating systems, configure the `Data Protector Inet` service user impersonation for the user that has the appropriate SAP R/3 permissions for running backups and restores.

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

  If there are several SAP R/3 instances running on the same system with different SAP administrator accounts configured for each instance, create an additional, common SAP administrator account. Configure the `Data Protector Inet` service to use this account as the service startup account.

Cluster-aware clients

- Configure SAP R/3 databases only on one cluster node, since the configuration files reside on the Cell Manager.

  Windows systems: During the configuration, Data Protector copies the Data Protector `backint` and `ob2smbsplit.exe` programs (the latter only if `splitint` is supported by BRTOOLS) from *`Data_Protector_home`*`\bin` to the directory that stores the SAP backup tools and renames `ob2smbsplit.exe` to `splitint.exe`. This is done only on the currently active node. On the other node, do it manually.

  UNIX systems: During the configuration, Data Protector creates a link to the Data Protector `backint` and `splitint` programs on the currently active node. On all the other nodes, do it manually. Execute:

  ```
  ln -s /opt/omni/lbin/backint \ /usr/sap/ORACLE_SID/sys/exe/run
  ```

  If `splitint` is supported by BRTOOLS, also execute:

  ```
  ln -s /opt/omni/lbin/ob2smbsplit \
  /usr/sap/ORACLE_SID/sys/exe/run/splitint
  ```

- If you intend to use the Data Protector CLI, set the Data Protector environment variable `OB2BARHOSTNAME` to the virtual server name as follows:

  Windows systems: `set OB2BARHOSTNAME=`*`virtual_server_name`*

  UNIX systems: `export OB2BARHOSTNAME=`*`virtual_server_name`*

NOTE: SAP recommends to install SAP backup utilites on all cluster nodes.

Configuring user accounts

To enable backup and restore of SAP R/3 database files, you need to configure or create several user accounts.

Oracle operating system user account	Operating system user account that is added to the following user groups: ***Windows systems:*** `ORA_DBA` and `ORA_SID_DBA` local groups ***UNIX systems:*** `dba` and `sapsys` For example, user `oraSID`. ***UNIX systems:*** Ensure that this user is the owner of the filesystem or of the raw logical volume on which the database is mounted. The minimum permissions should be 740.
User account `root` (UNIX systems only)	Default operating system administrator's user account added to the `dba` user group.
Oracle database user account	Database user account granted at least the following Oracle roles: • `sysdba` • `sysoper` For example, user `system`. Do not configure the Oracle SYS user for backing up SAP R/3 objects. When backing up using the SYS user account, the SAP backup fails with the error `ORA-28009: connection as SYS should be as SYSDBA or SYSOPER.`

Add the following user accounts to the Data Protector `admin` or `operator` user group:

- Oracle operating system user account

  (if you are using backup set method, add this user on the application as well as on backup system)
- ***UNIX systems:*** User account `root` (for both the application system and backup system)

In cluster environments, add these user accounts to the Data Protector `admin` or `operator` user group for the following clients:

- virtual server
- every node in the cluster

For information on adding Data Protector users, see the *HP Data Protector Help* index: “adding users”.

Configuring SQL*Net V2 or Net8 TNS listener

1. Ensure that the `listener.ora` and `tnsnames.ora` files on the application system are configured as shown in the following example. The files are located in:

   UNIX systems: *`ORACLE_HOME`*`/network/admin`

   Windows systems: *`ORACLE_HOME`*`\network\admin`

   ### Example

   Oracle instance: `PRO`

   Application system: `alpha.hp.com`

`listener.ora`	`LISTENER =`
	`  (DESCRIPTION_LIST =`
	`  (DESCRIPTION =`
	`  (ADDRESS =`
	`  (PROTOCOL = TCP) (HOST = alpha.hp.com)`
	`  (PORT = 1522)`
	`  )`
	`  )`
	`  )`
	
	`SID_LIST_LISTENER =`
	`  (SID_LIST =`
	`  (SID_DESC =`
	`  (GLOBAL_DBNAME = PRO)`
	`  (SID_NAME = PRO)`
	`  (ORACLE_HOME = /app/oracle815/product)`
	`  )`
	`  )`

`tnsnames.ora`	`PRO =`
	`  (DESCRIPTION =`
	`  (ADDRESS_LIST =`
	`  (ADDRESS = (PROTOCOL = TCP)`
	`  (HOST = alpha.hp.com) (PORT = 1522))`
	`  )`
	`  (CONNECT_DATA =  (SERVICE_NAME = PRO)`
	`  )`
	`  )`

2. Start the SQL*Net V2 or Net8 TNS listener by executing the following on the Oracle Server system:

   UNIX systems: *`ORACLE_HOME`*`/bin/lsnrctl start`

   Windows systems: *`ORACLE_HOME`*`\bin\lsnrctl start`

Checking the connection

To check the connection to the Oracle instance from the application system:

1. Log in to the application system as the Oracle OS user.
2. Export/set the *`ORACLE_HOME`* and *`ORACLE_SID`* variables.
3. Start `sqlplus`.
4. Connect to the Oracle target database as the Oracle database user, first with the `sysdba` role and then with the `sysoper` role.

Example

For the following configuration:

Oracle instance: `PRO` `ORACLE_HOME: /app/oracle816/product`

execute:

```
id
uid=102(oraprod) gid=101(dba)
export ORACLE_SID=PRO
export ORACLE_HOME=/app/oracle816/product
export SHLIB_PATH=/app/oracle816/product/lib:/opt/omni/lbin
sqlplus /nolog
SQLPLUS> connect system/manager@PRO as sysdba;
Connected.
SQLPLUS> connect system/manager@PRO as sysoper;
Connected.
```

Authentication password file

Enable the use of the authentication password file for the database administrator:

1. Shut down the Oracle target database on the application system.
2. In the `init`*`ORACLE_SID`*`.ora` file, specify:

   ```
   remote_login_passwordfile = exclusive
   ```

For instructions on how to set up the password file, see the Oracle documentation.

Enabling archived logging

When you set the database to the archived logging mode, you protect the unsaved online redo logs from being overwritten. Online backup of data files is useless without the related redo logs because you cannot recover the database to a consistent state.

TIP: Archive the redo log files generated during the online backup immediately after BRBACKUP completes.

To protect the archive directory from overflowing, clear the directory regularly.

To enable archived logging:

1. In the `init`*`ORACLE_SID`*`.ora` file, set

   ```
   log_archive_start = true
   ```

   and specify the `log_archive_dest` option.

   ### Example

   This is an example of the `init`*`ORACLE_SID`*`.ora` file for the Oracle instance `PRO`:

   ```
   # @(#)initSID.ora    20.4.6.1    SAP    98/03/30
   ######################################################
   #  (c)Copyright SAP AG, Walldorf
   ######################################################
   . . . .
   . . . . . . . . . .
   . . . . . . . .
   . . . . . . . .
   ### ORACLE Authentication Password File
   remote_login_passwordfile = exclusive
   ### ORACLE archiving
   log_archive_dest = /oracle/PRO/saparch/PROarch
   log_archive_start  = true
   . . . .
   ```

2. Mount the Oracle database and start the archived logging mode using the Oracle Server Manager. Execute:

```
startup mount
alter database archivelog;
archive log start;
alter database open;
```

Example

For the Oracle instance `PRO`, execute:

Windows systems: `set ORACLE_SID=PRO`

UNIX systems: `export ORACLE_SID=PRO`

Any operating system:

```
sqlplus /nolog
SQLPLUS> connect user/passwd@PRO;
Connected.
SQLPLUS> startup mount
ORACLE instance started.
Total System Global Area       6060224 bytes
Fixed Size                       47296 bytes
Variable Size                  4292608 bytes
Database Buffers               1638400 bytes
Redo Buffers                     81920 bytes
Database mounted.
SQLPLUS> alter database archivelog;
Statement processed.
SQLPLUS> archive log start;
Statement processed.
SQLPLUS> alter database open;
```

Sharing directories on the application system

The following directories on the application system must be accessible:

- `sapbackup`
- `sapreorg`
- Oracle home directory
- BR*Tools home directory

NOTE: The `sapreorg` and BR*Tools home directories must be accessible only if you want to run SAP compliant ZDB sessions (BRBACKUP is started on the backup system and not on the application system).

UNIX application system

1. Share the directories on the application system through NFS with root permissions.

   For example, suppose that the `sapbackup` directory on the application system points to `/oracle/SID/sapbackup` and the backup system is `backup.company.com`. To share the `sapbackup` directory:

   HP-UX systems: In the file `/etc/exports` on the application system, add the line:

   `/oracle/SID/sapbackup -root=backup.company.com`

   Solaris systems: In the file `/etc/dfs/dfstab` on the application system, add the line:

   `share -F nfs -o root=backup.company.com /oracle/SID/sapbackup`

2. Mount the directories on the backup system. Ensure that you have the same directory structure on both the application and backup system.

   For example, suppose that you have an HP-UX application system `app.company.com`. To mount the `/oracle/SID/sapbackup` directory on the backup system, add the following line to the file `/etc/fstab` on the backup system:

   ```
   app.company.com:/oracle/SID/sapbackup
   /oracle/SID/sapbackup nfs     defaults 0 0
   ```

Windows application system

- On the application system, find the location of the `sapbackup` and `sapreorg` directories. If they reside inside the SAP data home directory, share this directory under any name you want. Then, on the backup system, create the `HKEY_LOCAL_MACHINE\SOFTWARE\SAP\ORACLE_SID\Environment\SAPDATA_HOME` Windows registry key, specifying the SAP data home directory path as seen from the backup system.

  For example, suppose your application system is `mycomputer.company.com` and the SAP data home is `K:\oracle\my_instance`, which you share under the name `my_SAPinstance`. Then, the `SAPDATA_HOME` Windows registry key on the backup system must have the value `\\mycomputer.company.com\my_SAPinstance`.

  If the `sapbackup` and `sapreorg` directories do not reside together, share each directory separately and also create a separate Windows registry key on the backup system (`SAPBACKUP`, `SAPREORG`).

- Share the Oracle home directory on the application system and specify its path in the `ORACLE_HOME` Windows registry key on the backup system, similarly as described above.
- Ensure that the BR*Tools home directory on the application system is accessible from the backup system as follows:

  `\\application_system\sapmnt\SAP_SID\SYS\exe\run`

TIP:

Instead of creating registry keys, you can also set the Data Protector SAP R/3 integration environment variables (`ORACLE_HOME`, `SAPDATA_HOME`, `SAPBACKUP`, `SAPREORG`).

Choosing authentication mode

Data Protector SAP R/3 ZDB integration supports two authentication modes for accessing Oracle databases that are used by SAP R/3:

- database authentication mode
- operating system authentication mode

With database authentication mode, you need to re-configure the SAP R/3 integration for an SAP R/3 database with the new Oracle login information each time the corresponding Oracle database user account changes. Such a reconfiguration is not needed if operating system authentication mode is used.

You select the preferred authentication mode when you configure a particular SAP R/3 database.

Configuring SAP R/3 databases

You need to provide Data Protector with the following configuration parameters:

- Oracle Server home directory
- SAP R/3 data home directory

- Optionally, if you choose database authentication mode, Oracle database user account. The user account is used by BRBACKUP and BRARCHIVE during backup.
- Directory in which the SAP backup utilities are stored

Data Protector then creates the configuration file for the SAP R/3 database on the Cell Manager and verifies the connection to the database. On UNIX systems, Data Protector also creates a soft link for the `backint` program from the directory that stores the SAP backup utilities to `/opt/omni/lbin`.

On Windows systems, Data Protector copies the `backint` and programs (the latter only if `splitint` is supported by BR*Tools) from *`Data_Protector_home`*`\bin` to the directory that stores the SAP backup tools and renames `ob2smbsplit.exe` to `splitint.exe`.

To configure an SAP R/3 database, use the Data Protector GUI or CLI.

Before you begin

- Ensure that the SAP R/3 database is open.

Using the Data Protector GUI

1. In the Context List, click **Backup**.
2. In the Scoping Pane, expand **Backup Specifications**, right-click **SAP R/3**, and click **Add Backup**.
3. In the **Create New Backup** dialog box, select the template.

   From the **Backup type** drop-down list, select the **Snapshot or split mirror backup** option, and from the **Sub type** drop-down list, select the appropriate disk array agent. The agent must be installed on the application system and the backup system.

   Click **OK**.
4. In **Application system**, select the SAP R/3 client to be backed up. In cluster environments, select the virtual server.

   In **Backup system**, select the backup system.

   Specify other disk array specific backup options (see "EMC backup options" (page 128) for EMC, "P9000 XP Array backup options" (page 128) for P9000 XP Array, or "P6000 EVA Array backup options" (page 129) for P6000 EVA Array). For details on the options, press **F1**.

   NOTE: ***P9000 XP Array and P6000 EVA Array:*** To enable instant recovery, select **Track the replica for instant recovery**.
5. In **Application database**, type the Oracle instance name (`ORACLE_SID`).

   Specify the **User and group/domain** options, which are available on UNIX and Windows Server 2008 clients, as follows:

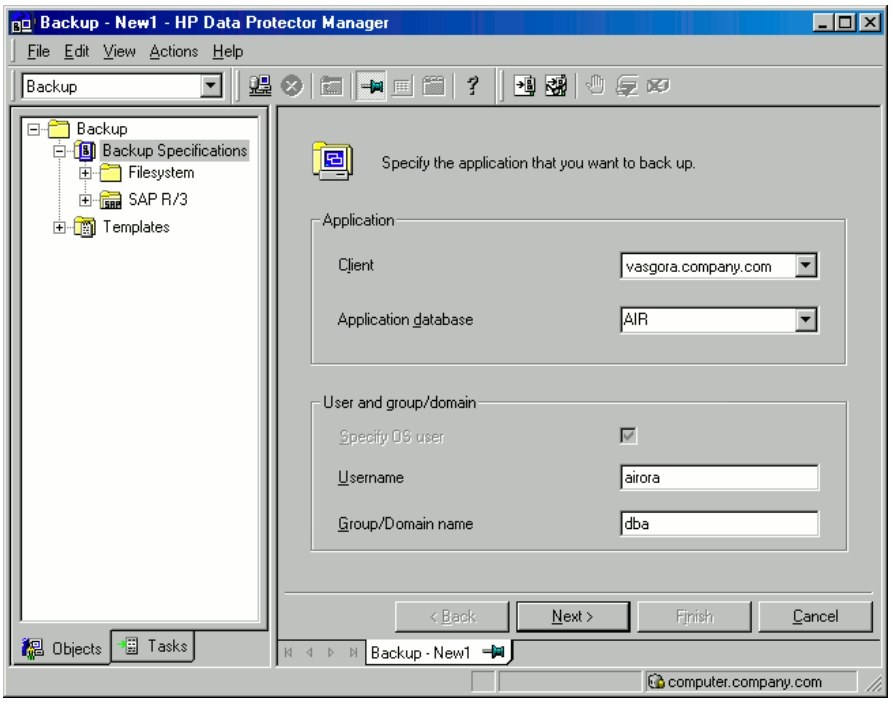
   Windows Server 2008: In **Username** and **Group/Domain name**, specify the operating system user account under which you want the backup session to run (for example, the user name `Administrator`, domain `DP`).

   UNIX systems: In **Username**, type the Oracle OS user described in "Configuring user accounts" (page 115). In **Group/Domain name**, type `dba`.

   Ensure that this user has been added to the Data Protector `admin` or `operator` user group, has the SAP R/3 backup rights, and has been set up for the `Data Protector Inet` service user impersonation. This user becomes the backup owner.

   For details on setting accounts for the Inet service user impersonation, see the *HP Data Protector Help* index: "Inet user impersonation".

Figure 42 Specifying an SAP R/3 system and Oracle instance



Click **Next**.

6. In the **Configure SAP** dialog box, specify the pathname of the Oracle Server home directory and SAP R/3 data home directory. If you leave the fields empty, the default *ORACLE_HOME* directory is used.

   Under **Oracle login information to target database**, specify the following:

   - For the database authentication mode, specify **Username**, **Password**, and **Service**.
   - For the local operating system authentication mode, leave **Username**, **Password**, and **Service** empty.
   - For the remote operating system authentication mode, specify only **Service** (leave **Username** and **Password** empty).

   The following are the option descriptions:

   - **Username** and **Password**: Specify the user name and password of the Oracle database user account described in "Configuring user accounts" (page 115).
   - **Service**: Specify the Oracle service name.

   In **Backup and restore executables directory**, specify the pathname of the directory in which the SAP backup utilities reside. By default, the utilities reside in:

   Windows systems: `\\SAP_system\sapmnt\ORACLE_SID\sys\exe\run`

   UNIX systems: `/usr/sap/ORACLE_SID/SYS/exe/run`

Figure 43 Configuring an SAP R/3 database on a UNIX system (operating system authentication mode)

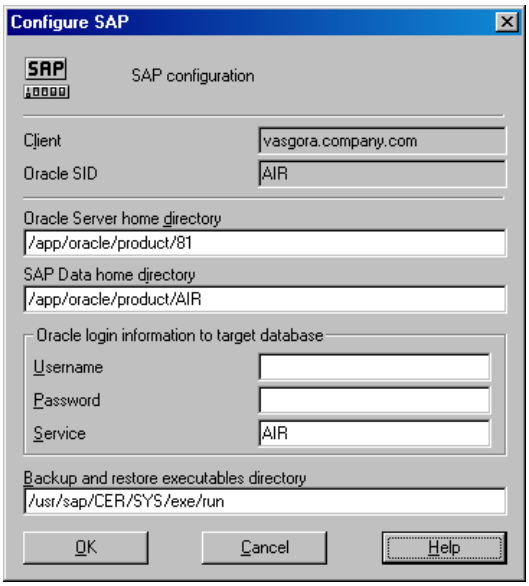
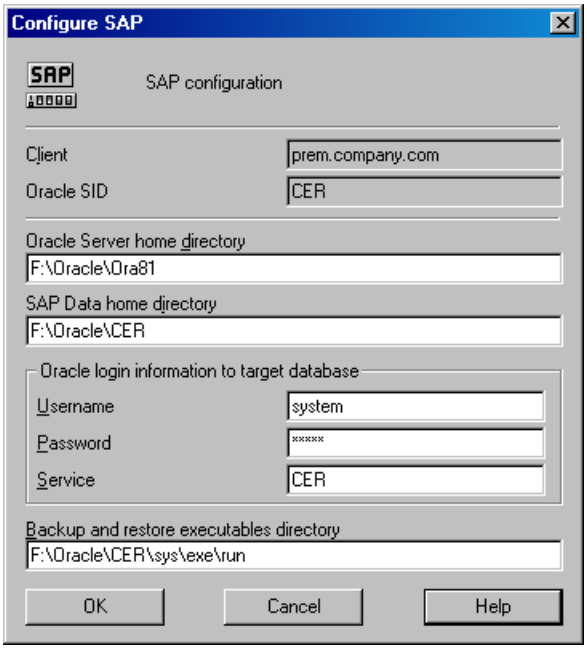


Figure 44 Configuring an SAP R/3 database on a Windows system (database authentication mode)



Click **OK**.

7. The SAP R/3 database is configured. Exit the GUI or proceed with creating the backup specification at Step 7.

Using the Data Protector CLI

1. Log in to the SAP R/3 system using the Oracle operating system user account.
2. At the command prompt, change current directory to the following directory:

   Windows systems: `Data_Protector_home\bin`

HP-UX, Solaris systems: `/opt/omni/lbin`

3. Execute:

```
util_sap.exe -CONFIG ORACLE_SID ORACLE_HOME
targetdb_connection_string SAPTOOLS_DIR [SAPDATA_HOME][SQL_PATH]
```

Parameter description

ORACLE_SID
Oracle instance name.

ORACLE_HOME
Pathname of the Oracle Server home directory.

targetdb_connection_string
This argument value determines the authentication mode used for accessing the Oracle database:

- To select the database authentication mode, specify the login information to the target database in the format *user_name/password@Oracle_service*.
- To select the local operating system authentication mode, specify only the character `/`.
- To select the remote operating system authentication mode, specify the login information to the target database in the format */@Oracle_service*.

SAPTOOLS_DIR
Pathname of the directory that stores the SAP backup utilities.

SAPDATA_HOME
Pathname of the directory where the SAP R/3 data files are installed. By default, this parameter is set to *ORACLE_HOME*.

The message `*RETVAL*0` indicates successful configuration.

Handling errors

If you receive the message `*RETVAL*`*error_number* where *error_number* is different than zero, an error occurred.

To get the error description, execute:

Windows systems:

Data_Protector_home`\bin\omnigetmsg 12` *error_number*

HP-UX systems:

`/opt/omni/lbin/omnigetmsg 12` *error_number*

TIP: To get a list of Oracle instances that are used by the SAP R/3 application, execute:

```
util_sap.exe -APP
```

To get a list of tablespaces of an Oracle instance, execute:

```
util_sap.exe -OBJS0 ORACLE_SID
```

To get a list of database files of a tablespace, execute:

```
util_sap.exe -OBJS1 ORACLE_SID TABLESPACE
```

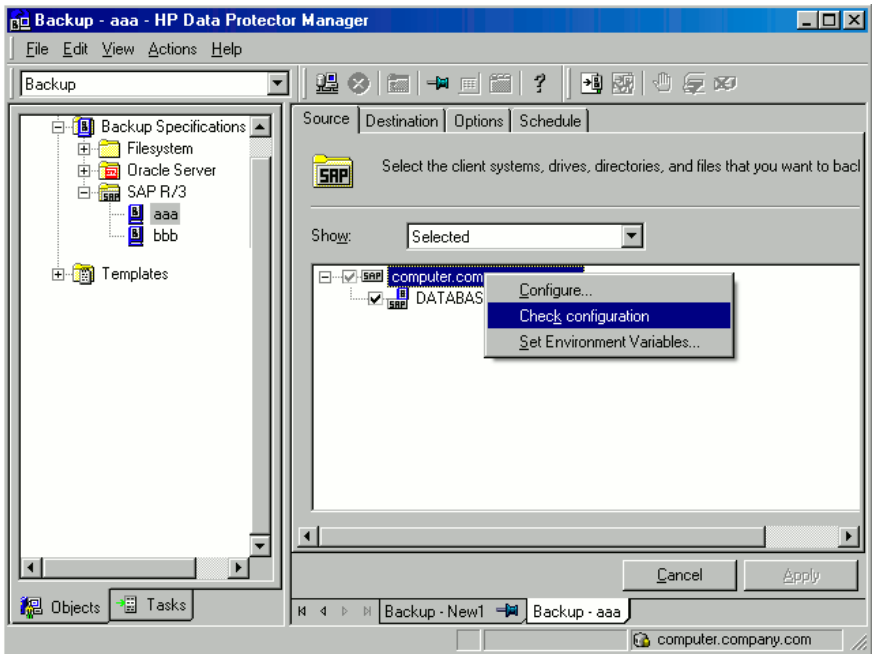
Checking the configuration

You can check the configuration of an SAP R/3 database after you have created at least one backup specification for this database. Use the Data Protector GUI or CLI.

Using the Data Protector GUI

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

Figure 45 Checking the SAP R/3 configuration



Using the Data Protector CLI

Log in to the SAP R/3 system as the Oracle OS user and execute:

`util_sap.exe -CHKCONF` *`ORACLE_SID`*

where *`ORACLE_SID`* is the name of the Oracle instance.

A successful configuration check displays the message `*RETVAL*0`.

If you receive the message `*RETVAL*`*`error_number`* where *`error_number`* is different than zero, an error occurred. On how to get the error description, see "Handling errors" (page 123).

To check if the SAP R/3 configuration is suitable for instant recovery, execute:

`util_sap.exe -CHKCONF_IR` *`ORACLE_SID`* `[-verbose]`

The `-verbose` option creates a file with a list of control files and redo log files that are on the same source volumes as the database files. If this list in not empty, a warning is displayed, stating that instant recovery is impossible. On how to solve this problem, see "Reconfiguring an Oracle instance for instant recovery" (page 252).

Configuring the SAP R/3 parameter file

To configure the integration, you need to set some parameters in the SAP R/3 parameter file on both the application system and backup system. The file template is located in:

UNIX systems: *`ORACLE_HOME`*`/dbs/init`*`ORACLE_SID`*`.sap`

Windows systems: *`ORACLE_HOME`*`\database\init`*`ORACLE_SID`*`.sap`

Table 10 SAP parameter file settings

Parameter	Value/Description
`split_cmd`	On the application system: ***UNIX systems:*** `"/opt/omni/lbin/ob2smbsplit $"` ***Windows systems:*** `"Data_Protector_home\bin\ob2smbsplit $"` On the backup system, you do not need to set the parameter. BRBACKUP uses this parameter to trigger the replica creation. At run time, the optional sign "$" is replaced with the name of the text file containing the names of files to be backed up. ***Windows systems:*** If the pathname contains spaces, use Windows short names instead.
`primary_db`	On the application system: `LOCAL` On the backup system: name of the service used for connecting to the Oracle database. This parameter defines the service name of the Oracle database to link the backup system to the application system.

Backup

The integration provides online and offline database backups of the following types:

- ZDB to disk
- ZDB to tape
- ZDB to disk+tape

To configure a backup, create a ZDB backup specification.

Archived logs can only be backed up in a ZDB to disk+tape, ZDB to tape, or non-ZDB (standard backup) session. If you try to back up archived logs in a ZDB to disk session, the session fails.

TIP: Create a separate (non-ZDB) backup specification for backing up archived logs.

What is backed up depends on your selection in the backup specification. For details, see "What is backed up" (page 125).

Table 11 What is backed up

Selected items	Backed up files
ARCHIVELOGS	• offline (archived) redo logs • control files
DATABASE or individual tablespaces	• data files • control files • SAP R/3 logs and parameter files • online redo logs (only during offline backups)

You can specify SAP R/3 backup options in two different ways:

- Using the BRBACKUP options.
- Using the SAP parameter file.

NOTE: The BRBACKUP options override the settings in the SAP parameter file.

You can specify BRBACKUP options when you create a backup specification. If no options are specified, the SAP R/3 application refers to the current settings in the SAP parameter file. In such a case, before running a backup, ensure that the SAP parameter file is correctly configured.

TIP: When you create a backup specification, select a backup template that already contains the desired BRBACKUP options.

Considerations

- Before you start a backup, ensure that the SAP R/3 database is in the `open` or `shutdown` mode.
- Before you start a backup, ensure the `primary_db` parameter is set to `LOCAL` in the SAP R/3 parameter file. For more information on setting the SAP R/3 parameter file, see "Configuring the SAP R/3 parameter file" (page 124).
- ZDB, restore, and instant recovery sessions that use the same source volume on the application system cannot run simultaneously.
- You cannot start a ZDB to disk session if another session is backing up the archived logs, even if the Oracle data files and the archived logs reside on different source volumes.
- ***P9000 XP Array:*** If the LVM Mirroring configuration is used, Data Protector displays a warning during a backup because the volume group source volumes on the application system do not have their BC pairs assigned. The message should be ignored.
- ***ZDB to disk:*** Archived logs cannot be backed up. To back up archived logs, create a non-ZDB (standard) SAP R/3 backup specification. For information, see the *HP Data Protector Integration Guide for Oracle and SAP*.
- Configurable backup modes are supported only by using templates.
- By default, Data Protector supports all BRTOOL options, except `-a` and `-b`. To enable support for `-a` and `-b`, set the `OB2BRTNOSECU` `omnirc` option to `1`. On how to set the `omnirc` options, see the *HP Data Protector Help* index: "omnirc options".

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 **SAP R/3**, and click **Add Backup**.
3. In the **Create New Backup** dialog box, select a template ("Selecting a template" (page 127)) and click **OK**.

Figure 46 Selecting a template

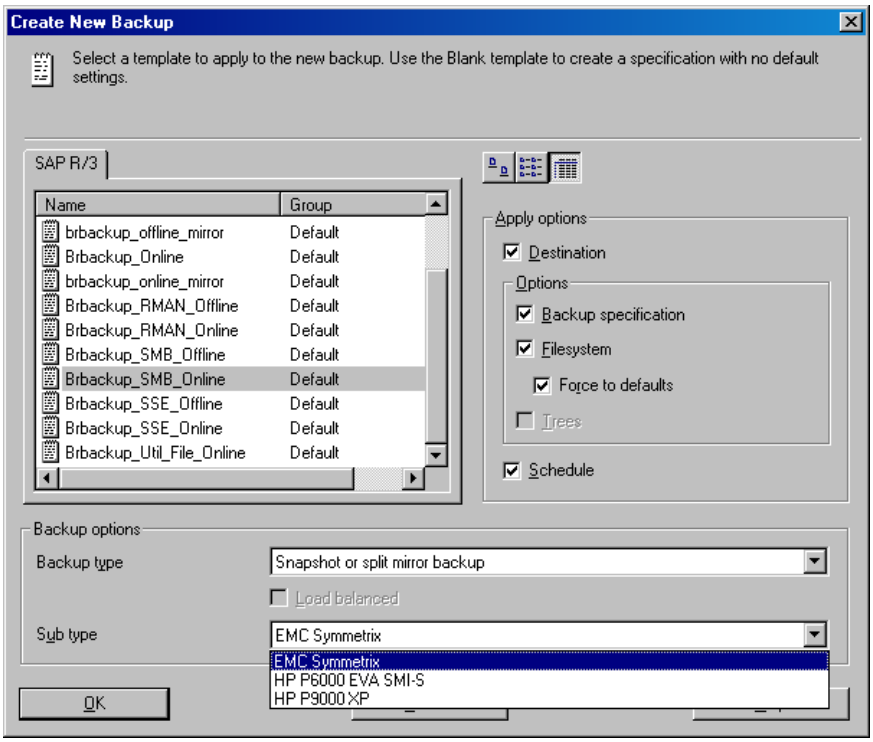


Table 12 Backup templates available for zero downtime backup

Blank SAP Backup	No predefined options.
Brbackup_offline_mirror	Used for an offline ZDB (split mirror or snapshot backup) using `splitint`. The database is stopped during the creation of a replica. The database is offline for a shorter period of time than if Brbackup_SMB_Offline was used, but `splitint` must be supported by BRTOOLS.
Brbackup_online_mirror	Used for an online ZDB (split mirror or snapshot backup) using `splitint`. The database is active during the creation of a replica. The database is in the backup mode for a shorter period of time than if Brbackup_SMB_Online was used, but `splitint` must be supported by BRTOOLS.
Brbackup_SMB_Offline	Used for an offline ZDB (split mirror or snapshot backup). The database is stopped during the creation of a replica.
Brbackup_SMB_Online	Used for an online ZDB (split mirror or snapshot backup). The database is active during the creation of a replica.

From the **Backup type** drop-down list, select **Snapshot or split mirror backup**.

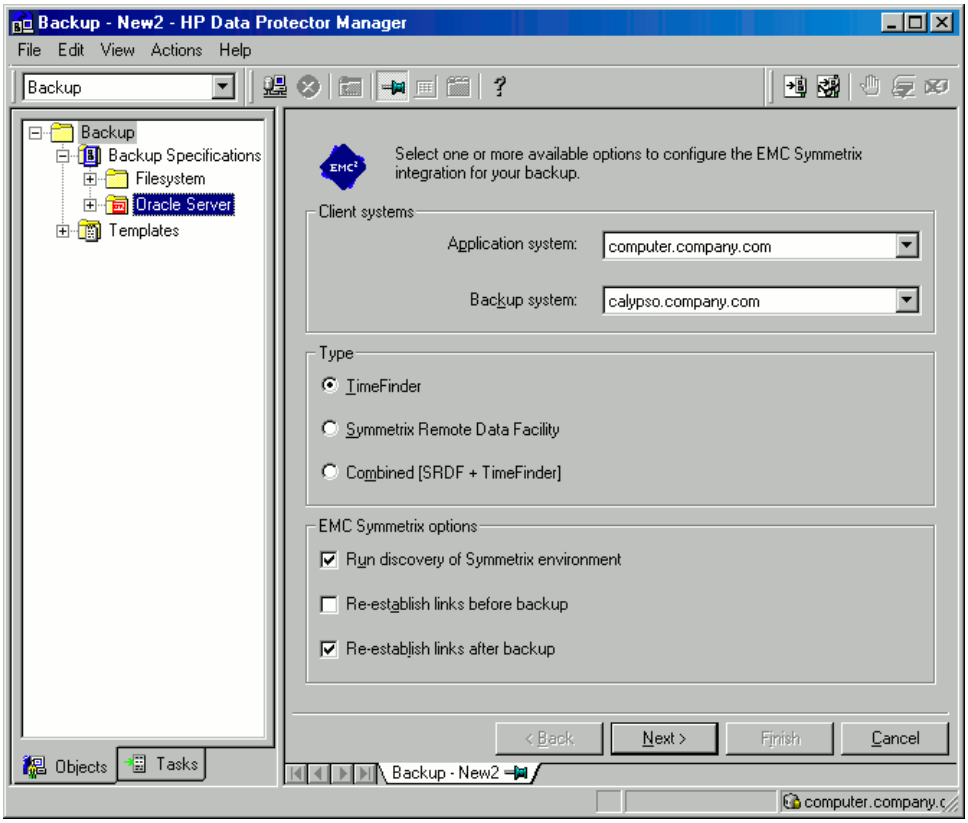
From the **Sub type** drop-down list, select the appropriate disk array agent. The agent must be installed on the application system and the backup system.

4. In **Application system**, select the SAP R/3 client to be backed up. In cluster environments, select the virtual server.

   In **Backup system**, select the backup system.

   Select other disk array-specific backup options (see "EMC backup options" (page 128) for EMC, "P9000 XP Array backup options" (page 128) for P9000 XP Array, or "P6000 EVA Array backup options" (page 129) for P6000 EVA Array). For detailed information on the backup options, press **F1**.

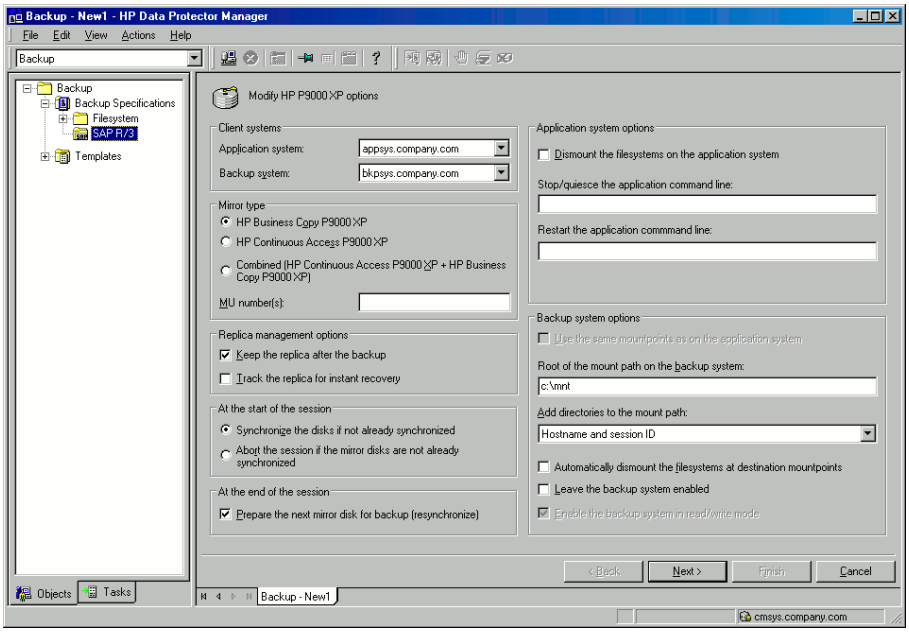
Figure 47 EMC backup options



P9000 XP Array specifics

To enable instant recovery, leave the **Track the replica for instant recovery** option selected. It is not possible to run instant recovery with Data Protector if this option is cleared.

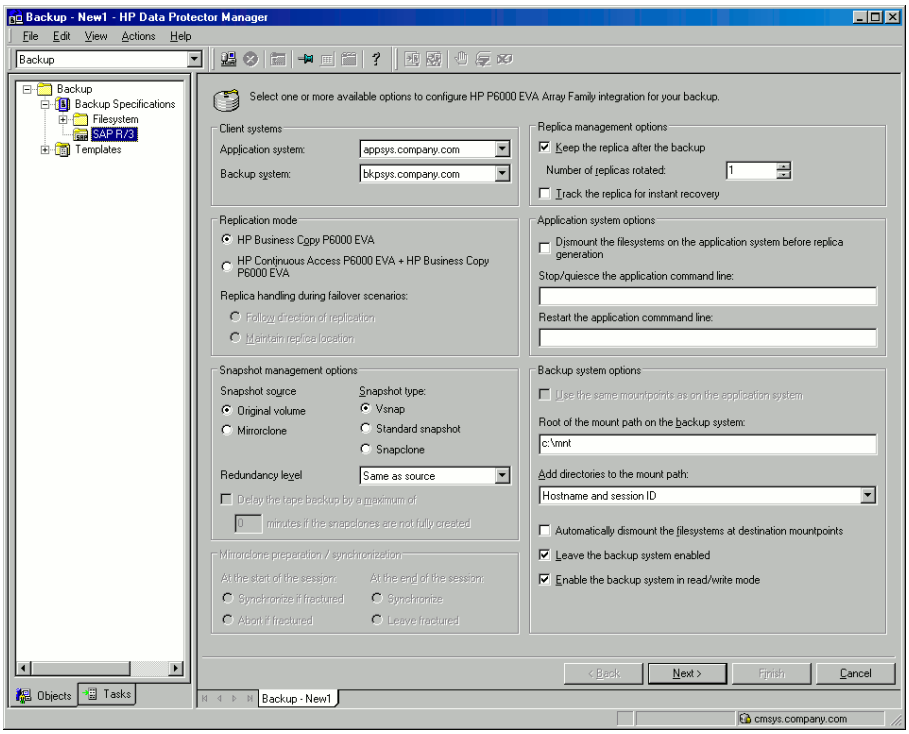
Figure 48 P9000 XP Array backup options



P6000 EVA Array specifics

To enable instant recovery, select the **Track the replica for instant recovery** option.

Figure 49 P6000 EVA Array backup options



Click **Next**.

5. In **Application database**, select the Oracle instance (`ORACLE_SID`) to be backed up.

   Specify the **User and group/domain** options, which are available on UNIX and Windows Server 2008 clients, as follows:

   Windows Server 2008: In **Username** and **Group/Domain name**, specify the operating system user account under which you want the backup session to run (for example, the user name `Administrator`, domain `DP`).

   UNIX systems: In **Username**, type the Oracle OS user described in "Configuring user accounts" (page 115). In **Group/Domain name**, type `dba`.

   Ensure that this user has been added to the Data Protector `admin` or `operator` user group, has the SAP R/3 backup rights, and has been set up for the `Data Protector Inet` service user impersonation. This user becomes the backup owner.

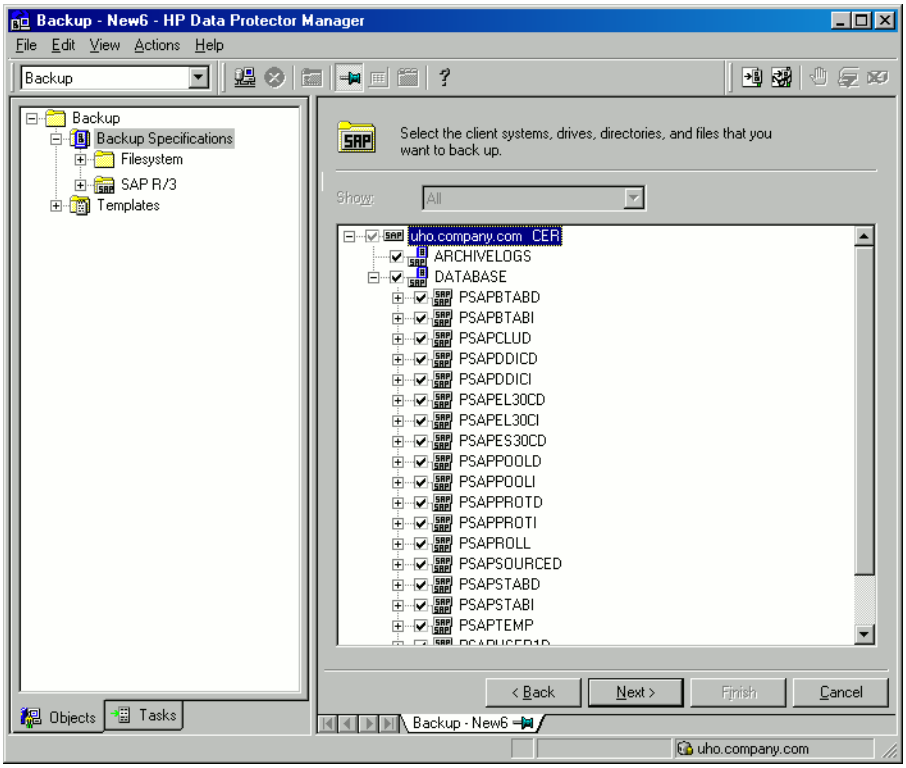
   For details on setting accounts for the Inet service user impersonation, see the *HP Data Protector Help* index: "Inet user impersonation".

   Click **Next**.

6. If the SAP R/3 database is not configured yet for use with Data Protector, the **Configure SAP** dialog box is displayed. Configure it as described in "Configuring SAP R/3 databases" (page 119).
7. Select SAP R/3 objects to be backed up. You can select individual tablespaces, data files, or archived logs.

   NOTE: If you plan to do instant recovery, select the whole **DATABASE** item.

Figure 50 Selecting backup objects



Click **Next**.

8. Select devices to use for the backup.

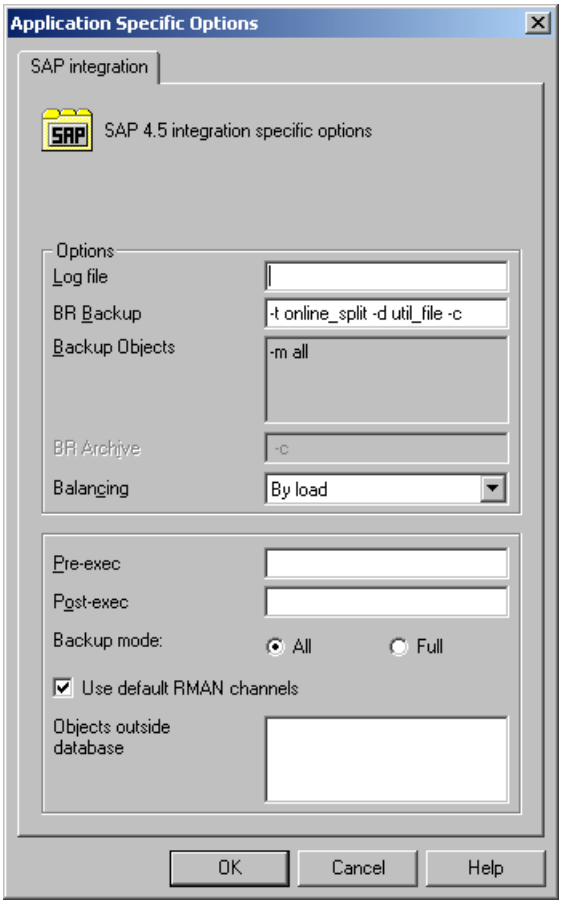
   To specify device options, right-click the device and click **Properties**. Specify the number of parallel backup streams in the **Concurrency** tab and the media pool.

   NOTE: Parallelism (the number of streams your SAP R/3 database is backed up with) is set automatically. If load balancing is used, the number of streams equals the sum of concurrencies of the selected devices.

   Click **Next**.

9. Set backup options. For information on the application-specific options, see "SAP R/3 backup options" (page 131).

Figure 51 Application-specific options



Click **Next**.

10. Optionally, schedule the backup. See "Scheduling backup sessions" (page 132).
    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 133).

Table 13 SAP R/3 backup options

Option	Description
Log file	If you want to create a backint log file during backup, specify a pathname for the file. By default, this file is not created because Data Protector stores all relevant information about backup sessions in the database.
BR Backup	Specifies BRBACKUP options. For example, for online backup using the `splitint` interface, type `-t online_mirror`. If `splitint` is not supported by BRTOOLS, type `-t online_split`. To run BRBACKUP under a different Oracle database user than the one specified during the configuration, type `-u user_name`.
Backup Objects	Lists BRBACKUP options passed by `omnisap.exe`. The list is displayed after you save the backup specification.
BR Archive	Specifies BRARCHIVE options. Not applicable for ZDB to disk.

Table 13 SAP R/3 backup options *(continued)*

Option	Description
Balancing: By Load	Groups files into subsets of approximately equal sizes. The subsets are then backed up concurrently by Data Protector `sapback` programs. If your backup devices use hardware compression, the sizes of the original and backed up files differ. To inform Data Protector of this, specify the original sizes of the backed up files in the `compression` section of the Data Protector SAP R/3 configuration file. See "Data Protector SAP R/3 configuration file" (page 109).
Balancing: By Time	Groups files into subsets that are backed up in approximately equal periods of time. The duration depends on the file types, speed of the backup devices, and external influences (such as mount prompts). This option is best for environments with large libraries of the same quality. The subsets are backed up concurrently by Data Protector `sapback` programs. Data Protector automatically stores backup speed information in the `speed` section of the Data Protector SAP R/3 configuration file. It uses this information to optimize the backup time. This type of balancing may lead to non-optimal grouping of files in the case of an online backup or if the speed of backup devices varies significantly.
Balancing: Manual	Groups files into subsets as specified in the manual balancing section of the Data Protector SAP R/3 configuration file. For more information, see "Manual balancing" (page 137). Not applicable for ZDB to disk.
Balancing: None	No balancing is used. The files are backed up in the same order as they are listed in the internal Oracle database structure. To check the order, use the Oracle Server Manager SQL command: `select * from dba_data_files`
Pre-exec, **Post-exec**	The command specified here is started by `omnisap.exe` on the SAP R/3 system before the backup (`pre-exec`) or after it (`post-exec`). Do not use double quotes. Provide only the name. The command must reside in the directory: ***Windows systems:*** *`Data_Protector_home`*`\bin` ***HP-UX, Solaris:*** `/opt/omni/bin`
Backup mode	Not applicable for ZDB.
Use default RMAN channels	Not applicable for ZDB.
Objects outside database	Specifies non-database files of the Oracle SAP R/3 environment to be saved. Save these files in a separate backup session.

NOTE: The total number of sapback processes started in one session using Data Protector is limited to 256.

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 sessions

You can run unattended backups at specific times or periodically. For details on scheduling, see the *HP Data Protector Help* index: "scheduled backups".

Scheduling example

To schedule ZDB to disk+tape at 8:00, 13:00, and 18:00 during week days:

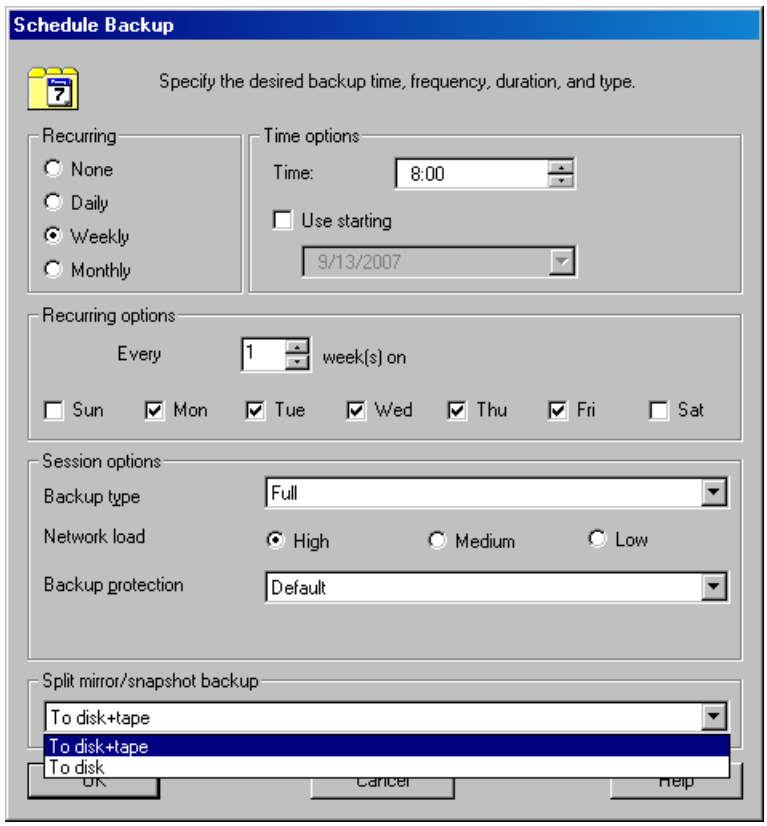
1. In the **Schedule** property page, select the starting date in the calendar and click **Add** to open the **Schedule Backup** dialog box.

2. Under **Recurring**, select **Weekly**. Under **Time options**, select **8:00**. Under **Recurring Options**, select **Mon**, **Tue**, **Wed**, **Thu**, and **Fri**.

   From the **Split mirror/snapshot backup** drop-down list, select **To disk+tape**. See "Scheduling backup sessions" (page 133).

   Click **OK**.
3. Repeat Step 1 and Step 2 to schedule backups at 13:00 and 18:00.
4. Click **Apply** to save the changes.

Figure 52 Scheduling backup sessions



Previewing backup sessions

Preview the backup session to test it. You can 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 **SAP R/3**. Right-click the backup specification you want to preview and click **Preview Backup**.
3. Specify **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

Execute:

```
omnib -sap_list backup_specification_name -test_bar
```

What happens during the preview?

The `omnisap.exe` command is started, which starts the Data Protector `testbar` command to test the following:

- The syntax of the backup specification
- If devices are correctly specified
- If the necessary media are in the devices

Starting backup sessions

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

Backup methods

Start a backup of SAP R/3 objects in any of the following ways:

- Using the Data Protector GUI.
- Using the Data Protector CLI.
- Using the SAP BR*Tools.

Using the Data Protector GUI

1. In the Context List, click **Backup**.
2. In the Scoping Pane, expand **Backup Specifications**, and then **SAP R/3**. Right-click the backup specification you want to use and click **Start Backup**.
3. Specify Click **OK**.

   NOTE: Only the `Full` backup type is supported.

   ZDB to disk, ZDB to disk+tape: Specify the **Split mirror/snapshot backup** option.

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

Using the Data Protector CLI

Execute:

ZDB to tape, ZDB to disk+tape:

`omnib -sap_list` *`backup_specification_name`*

ZDB to disk:

`omnib -sap_list` *`backup_specification_name`* `-disk_only`

For details, see the `omnib` man page or the *HP Data Protector Command Line Interface Reference*.

Using the SAP BRTOOLS

1. Log in to the SAP R/3 backup system or SAP R/3 application system as the Oracle OS user.
2. Export/set the following environment variables:

   `ORACLE_SID=`*`SAP_instance_name`*

   `ORACLE_HOME=`*`Oracle_software_home_directory`*

   `[SAPBACKUP_TYPE=OFFLINE]`

   Default is `ONLINE`.

`SAPDATA_HOME=`*`database_files_directory`*

`SAPBACKUP=`*`BRTOOLS_logs_and_control_file_copy_directory`*

`SAPREORG=`*`BRSPACE_logs_directory`*

`OB2BARLIST=`*`backup_specification_name`*

The backup specification is needed only to specify which Data Protector devices should be used for backup. Other information from the backup specification, like SAP R/3 objects to be backed up or the BRBACKUP options, is ignored and has to be specified manually at run time.

`[OB2_3RD_PARTY_BACKINT=1]`

Specifies usage of a third-party `backint` tool to perform ZDB-to-disk+tape backup sessions. After setting the variable, copy the `backint` you want to use to the SAP BRTOOLS directory.

`[OB2BARHOSTNAME=`*`application_system_name`*`]`

Required if you are logged in to the backup system. Optional if you want to specify a virtual server name in cluster environments.

`[OB2BACKUPHOSTNAME=`*`backup_system_name`*`]`

Required if you are logged in to the application system.

`OB2SMB=1`

Specifies a ZDB session.

`[OB2SMBIR=1]`

Specifies tracking replica for instant recovery.

`[ZDB_ORA_INCLUDE_CF_OLF=1]`

Required if you are logged in to the backup system. For details, see "ZDB integrations omnirc options" (page 254).

`[OB2DISKONLY=1]`

Specifies a ZDB-to-disk session.

If you are logged on to the backup system, ensure that the `NLS_LANG` environment variable is set to the same value as the `NLS_LANG` environment variable on the application system.

Alternatively, these variables can be specified in the backint parameter file. If this is required, the location of the file must be specified in the SAP configuration file using the *`util_par_file`* parameter:

`util_par_file = `*`path\filename`*

If you do not supply the path, the system searches for the parameter file in the directory:

Windows systems: *`SAPDATA_HOME`*`\database`

UNIX systems: *`ORACLE_HOME`*`/dbs`

3. Run the BRBACKUP command. The command syntax depends on whether you are logged in to the application system or backup system:

   Application system:

   ```
   brbackup -t {online_split | offline_split | online_mirror | \
   offline_mirror} [-q split] -d \ util_file -m all -c -u user/password
   ```

   Backup system:

   ```
   brbackup -t {online_mirror | offline_mirror} [-q split] -d util_file
   -m all -c -u user/password
   ```

   The `-q split` option is required if `OB2DISKONLY` is set to `1`.

Configuring SAP compliant ZDB sessions

SAP R/3 standards recommend that, in ZDB sessions that use the `splitint` backup interface, BRBACKUP is started on the backup system and not on the application system. You can configure Data Protector to comply with these standards by setting the Data Protector `OB2_MIRROR_COMP` environment variable to `1`. The variable is saved in the Data Protector SAP R/3 instance configuration file. Consequently, in all `splitint` ZDB sessions for this SAP R/3 instance, BRBACKUP will be started on the backup system. By default, BRBACKUP is started on the application system.

Set the `OB2_MIRROR_COMP` environment variable using the Data Protector GUI or CLI.

NOTE: If no backup specification for the related SAP R/3 instance exists, you cannot use the Data Protector CLI to set the `OB2_MIRROR_COMP` variable.

Using the Data Protector GUI

You can set the `OB2_MIRROR_COMP` variable when you create a backup specification or modify an existing one:

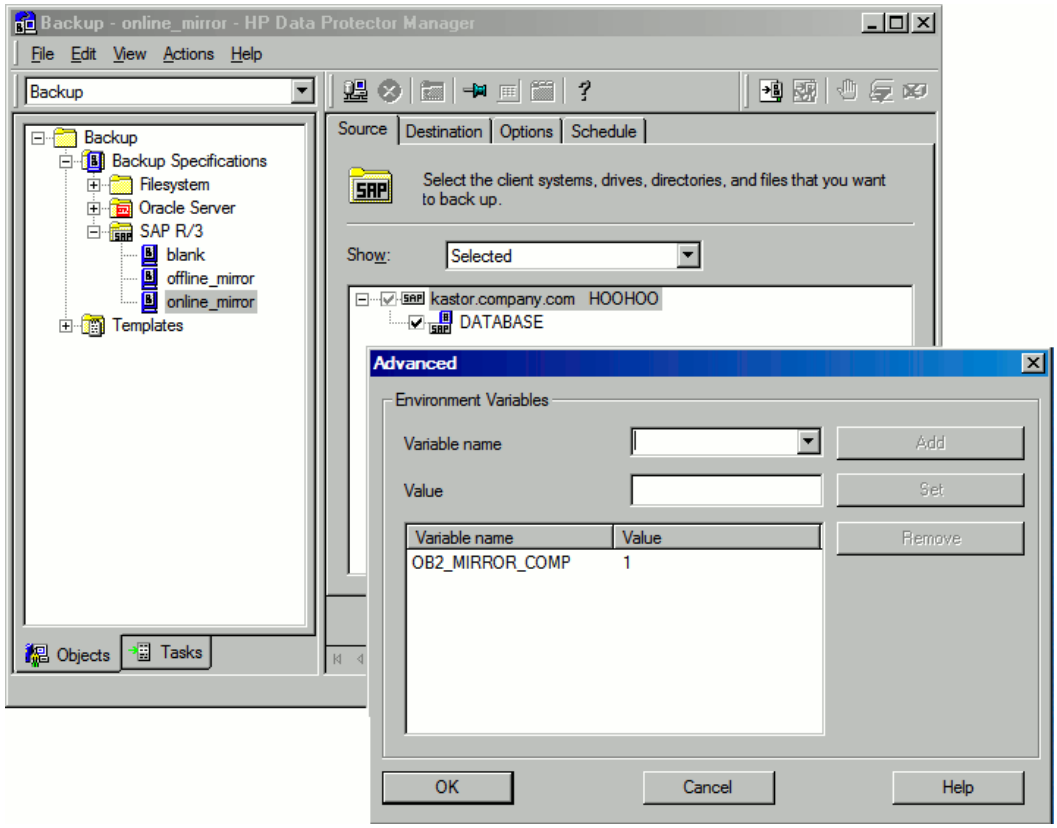
1. Proceed to the Source page of the backup specification.

   NOTE: In environments in which the control file and datafiles reside on the same source disk, Data Protector does not let you proceed to the Source page if the **Track the replica for instant recovery** option is selected. Specifically, the Data Protector instant recovery check fails. In such a case, clear the option first. You can select the option later if needed, when the `OB2_MIRROR_COMP` variable is already set and, consequently, the instant recovery check is no longer performed.

   Right click the SAP R/3 instance at the top and click **Set Environment Variables**.
2. In the Advanced dialog box, set `OB2_MIRROR_COMP` to `1`. See " Setting environment variables" (page 137).

   Click **OK**.

Figure 53 Setting environment variables



Using the Data Protector CLI

Execute the following command:

```
util_cmd -putopt SAP instance_name OB2_MIRROR_COMP 1 -sublist Environment
```

Manual balancing

Manual balancing means that you manually group files into subsets, which are then backed up in parallel. To group files into subsets, add the `manual_balance` section to the Data Protector SAP R/3 configuration file as described in the following example.

Example

Suppose that we have a backup specification named `SAP-R3` with the following files to be backed up: `fileA`, `fileB`, `fileC`, `fileD`. To group the files into three subsets (`0={fileA, fileC}`, `1={fileB}`, `2={fileD}`), add the following lines to the Data Protector SAP R/3 configuration file:

```
manual_balance={
        SAP-R3={
  fileA=0;
  fileB=1;
  fileC=0;fileD=2;}}
```

When you group files into subsets, consider the following:

- Use only one file from the same hard disk at a time.
- The number of files in a subset must be equal to or smaller than the sum of the concurrencies of all devices specified for backup.
- If the backup specification contains files that are not allocated to any subset, Data Protector automatically adds these files to the list of files to be backed up using the load balancing principle. Before the backup, this list is logged in:

  Windows systems: *SAPDATA_HOME*\sapbackup*.lst

  UNIX systems: *ORACLE_HOME*/sapbackup/.*.lst

Restore

You can restore SAP R/3 objects using any of the following methods:

- **Standard restore:** Data is restored from backup media created in ZDB to tape, ZDB to disk+tape, and non-ZDB (standard backup) sessions. See "Standard restore" (page 139).
- **Instant recovery:** Data is restored from a replica created in *online* ZDB–to–disk or ZDB–to–disk+tape sessions. See "Instant recovery" (page 142).

After the restore, you can recover the database to a specific point in time using the SAP BRTOOLS interface. Instant recovery method enables you to restore and recover the database within the same session. However, you can only restore (and recover) the whole database. To restore only a part of the database or the archived logs, use the standard restore method.

"SAP recovery methods" (page 138) shows which restore methods are available, depending on the backup session you restore from.

Table 14 SAP recovery methods

Disk array	Backup types	Recovery of the whole database		Recovery of a part of the database
		Until now	To a point in time, logseq/thread or SCN number	
P9000 XP, P6000 EVA, EMC	ZDB to tape - online	Restore	Restore	Restore
	ZDB to tape - offline	Restore	Restore	Restore
P9000 XP, P6000 EVA	ZDB to disk - online	Instant recovery + database recovery	Instant recovery + database recovery	N/A
	ZDB to disk - offline	N/A	N/A	N/A
	ZDB to disk+tape - online	• Instant recovery + database recovery or • Restore	• Instant recovery + database recovery or • Restore	Restore
	ZDB to disk+tape - offline	Restore	Restore	Restore

Table 15 Legend

Restore	You can do a standard restore from the Data Protector media using the Data Protector GUI or the SAP BRTOOLS. After the restore, you can recover the database using the SAP BRTOOLS.
Instant recovery + database recovery	You can do an instant recovery. You can include database recovery in the instant recovery session or do it afterwards, using the SAP BRTOOLS.
N/A	Not available.

Considerations

- SAP R/3 tablespaces located on raw partitions cannot be restored using the Data Protector GUI. Workaround: Use SAP restore commands (for example, `brrestore`).
- If your Oracle database is localized, you may need to set the appropriate Data Protector encoding before you start a restore. For details, see "Localized SAP R/3 objects" (page 146).
- Restore preview is not supported.

Standard restore

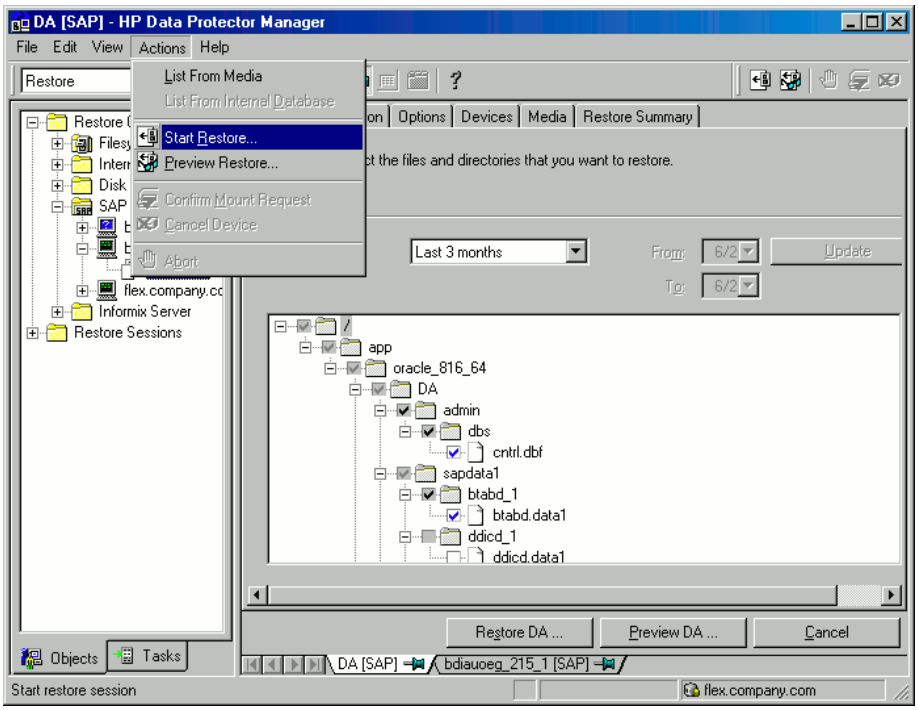
Restore SAP R/3 objects using the Data Protector Manager.

1. In the Context List, click **Restore**.
2. In the Scoping Pane, expand **SAP R/3**, expand the client (backup system) from which the data was backed up, and then click the Oracle instance you want to restore.
3. In the **Source** page, select SAP R/3 files to be restored.

   To restore a file under a different name or to a different directory, right-click the file and click **Restore As/Into**.

   To restore a file from a specific backup session, right-click the file and click **Restore Version**.

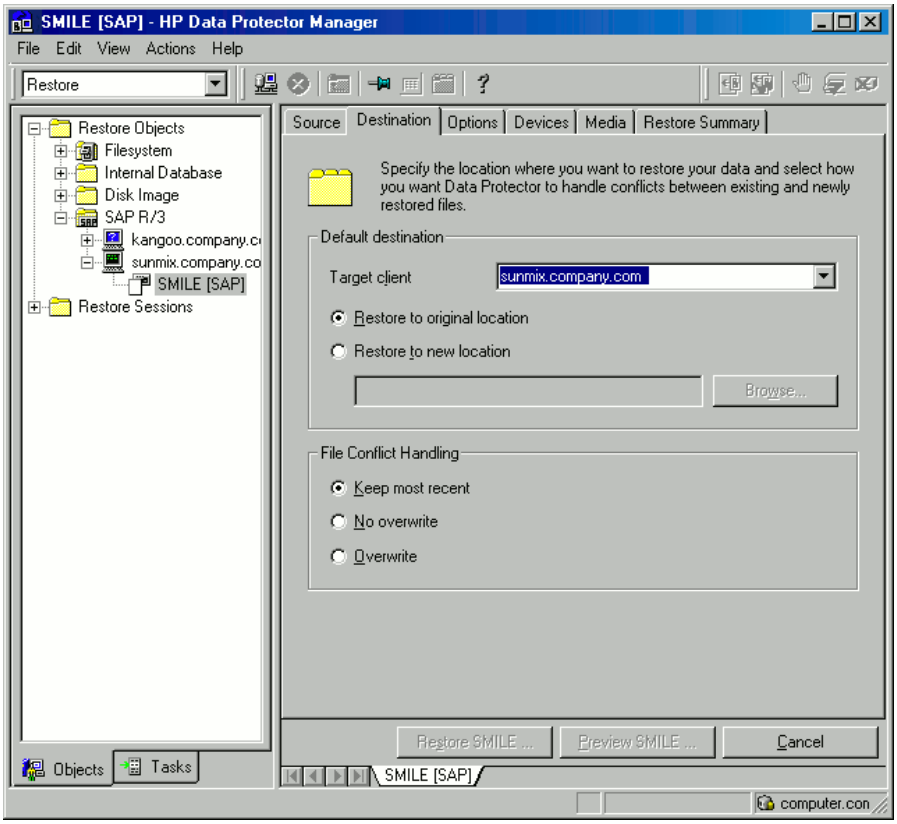
Figure 54 Selecting objects for restore



4. In the **Destination** tab, select the client to restore to (**Target client**). By default, this is the application system. See "Selecting the target client" (page 140).

   For details on options, press **F1**.

Figure 55 Selecting the target client



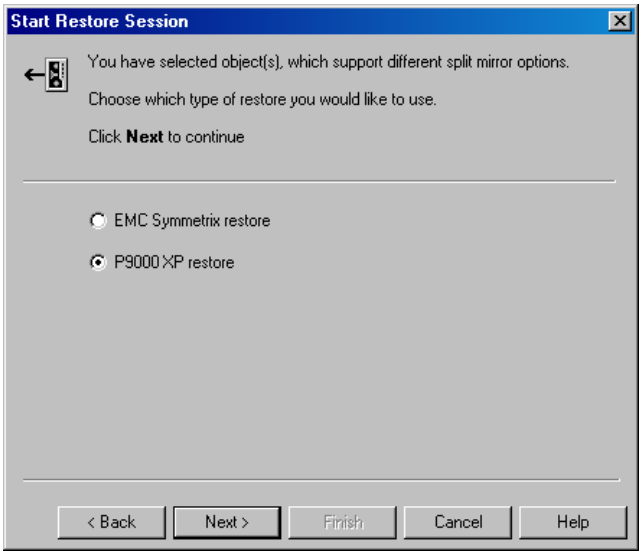
5. In the **Options** page, set the restore options. For information, press **F1**.
6. In the **Devices** page, select the devices to be used for the restore.

   For more information on how to select devices for a restore, see the *HP Data Protector Help* index: "restore, selecting devices for".
7. Click **Restore**.
8. In the **Start Restore Session** dialog box, click **Next**.
9. Specify **Report level** and **Network load**.
10. ***EMC and P9000 XP Array:*** This step is relevant only if you have both the `EMC Symmetrix Agent` and `HP P9000 XP Agent` components installed on the application system.

    EMC: Select `EMC Symmetrix restore`.

    P9000 XP Array: Select `P9000 XP restore`. See "Selecting the P9000 XP restore" (page 141).

Figure 56 Selecting the P9000 XP restore



Click **Next**.

11. ***EMC and P9000 XP Array:*** From the `EMC Symmetrix mode` or `Mirror mode` drop-down list, select **Disabled**. This sets the restore from backup media to the application system directly. See "EMC – Selecting restore to the application system directly" (page 141).

Figure 57 EMC – Selecting restore to the application system directly

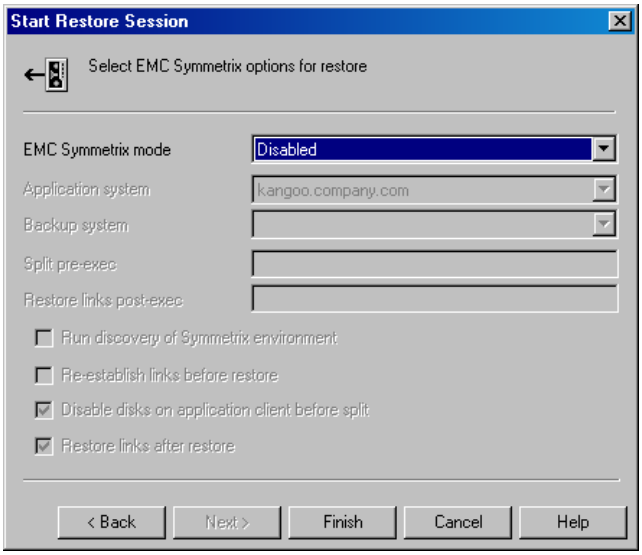
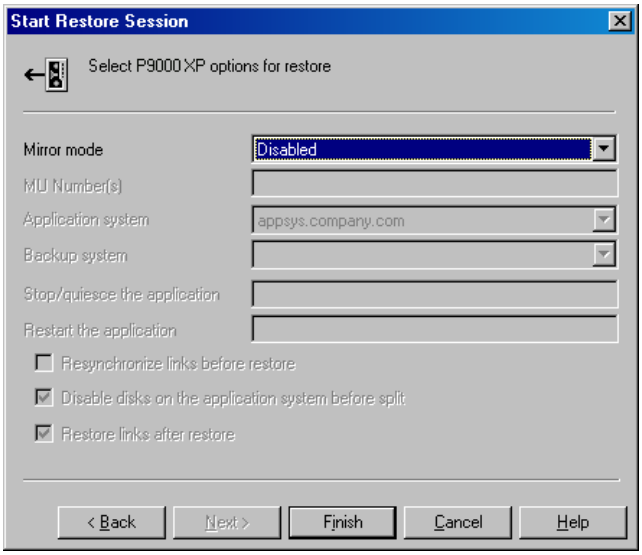


Figure 58 P9000 XP Array – Selecting restore to the application system directly



12. Click **Finish** to start the restore.

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

Instant recovery

For general information on instant recovery, see the *HP Data Protector Zero Downtime Backup Concepts Guide* and *HP Data Protector Zero Downtime Backup Administrator's Guide*. For information on instant recovery in cluster environment (Cluster File System (CFS), MC/ServiceGuard, and Microsoft Cluster Server), see the *HP Data Protector Zero Downtime Backup Administrator's Guide*.

You can start an instant recovery using the Data Protector GUI or CLI.

Considerations

- The database recovery part is performed after the instant recovery procedure. During database recovery, archive log backups performed after the ZDB are restored from tape by the SAP BR*Tools utilities. If selected, the logs are reset and the database is opened.
- If the replica to be used for instant recovery contains the control file, first see "Instant recovery from replicas containing the control file" (page 145).

Instant recovery using the Data Protector GUI

To perform an instant recovery:

1. Shut down the Oracle database using `sqlplus`:

   For example:

   ```
   sqlplus
   sqlplus> shutdown immediate
   sqlplus> exit
   ```

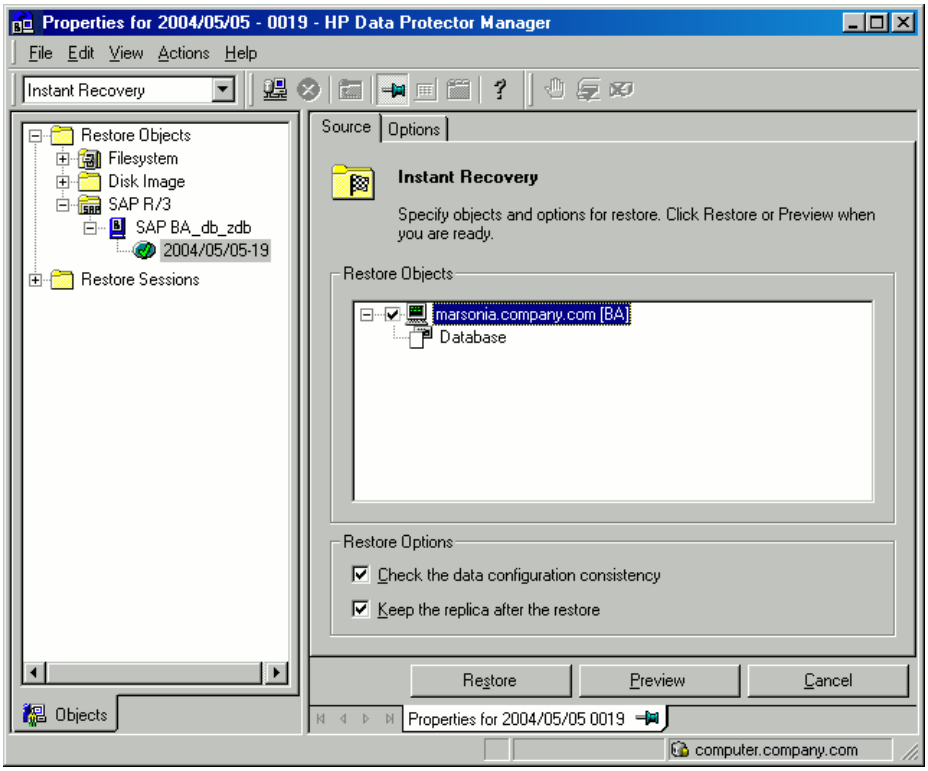
2. In the Data Protector Manager Context List, select **Instant Recovery**.
3. Expand **SAP R/3** and select the ZDB-to-disk or ZDB-to-disk+tape session from which you want to perform the restore.
4. In the **Source** tab, select the objects to recover. Only whole databases can be selected.

   For HP P9000 XP Disk Array Family, it is recommended to leave the **Keep the replica after the restore** option selected to enable a restart of an instant recovery session. The option is selected by default, except for an offline backup where the database was in NOARCHIVELOG

mode during the backup. With HP P6000 EVA Disk Array Family, replica is kept on the disk array only if the **Copy replica data to the source location** is selected.

Set other HP P6000 EVA Disk Array Family or HP P9000 XP Disk Array Family options. For details, press **F1**.

Figure 59 SAP R/3 source options



5. At this point, you can decide whether to perform a database recovery immediately after an instant recovery or not:
   - To perform only an instant recovery, click **Restore**.
   - To automatically perform a database recovery after an instant recovery, select the recovery options. For details, see "Database recovery options" (page 143).

     Click **Restore**.

     Data Protector recovers the database after performing instant recovery by switching the database to mount state, restoring the necessary archive redo logs from tape, and applying the redo logs.

Database recovery options

User name (UNIX systems only)	Specifies the user name under which the instant recovery is performed. The user needs to be a member of the DBA group.
User group (UNIX systems only)	Specifies the user group the user in the **User name** field belongs to. **NOTE:** The **User name** and the **User group** must be the same as defined in the backup ownership.
Recovery	Enables database recovery after instant recovery.
Recover until	The options in this drop-down list enables you to specify to which point in time you would like the recovery to be performed. The following options are available:

Now: All existing archive logs are applied.

Selected time: Only archive logs until the specified time are applied.

Selected logseq/ thread number: Specifies an incomplete recovery. Only archive logs with a lower or equal number than the specified log sequence or thread number are applied.

Selected SCN number: Only archive logs until the specified SCN number are applied.

Open database after recovery

Opens the database after the recovery was performed.

Reset logs

Resets the archive logs after the database is opened. This option is by default not selected if the **Recover until** option is set to **Now**.

The following are Oracle recommendations on when to reset the logs:

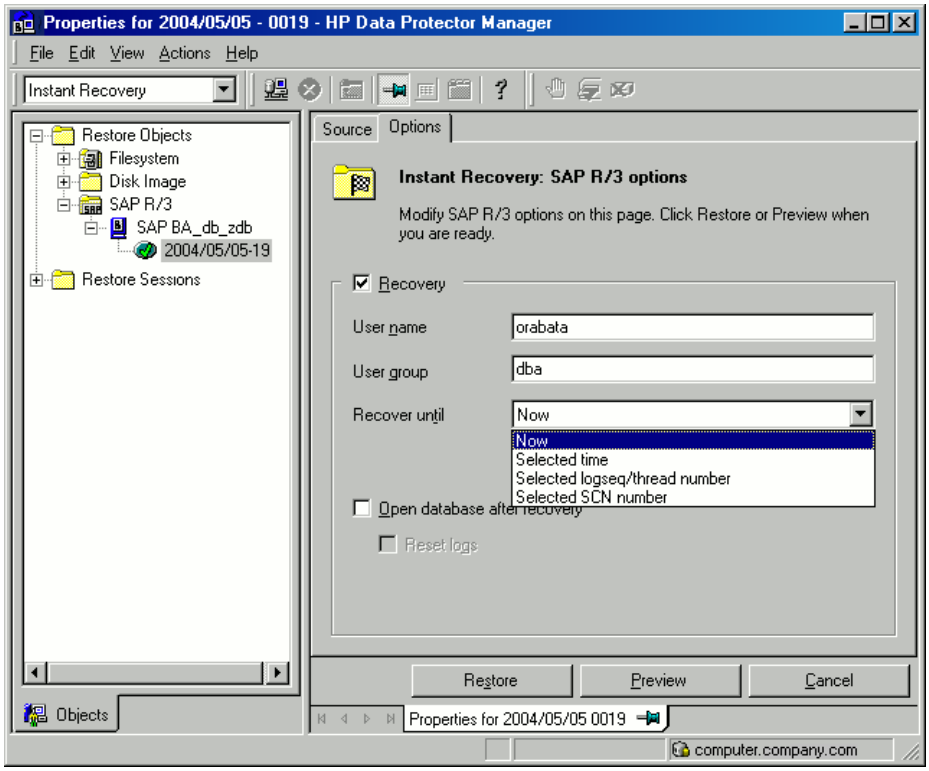
Always reset the logs:

- After an incomplete recovery, that is, if not all archive redo logs are applied.
- If a backup of the control file is used for recovery.

Do not reset the logs:

- After a complete recovery, when the control file is not used.
- If the archive logs are used for a standby database. However, if you must reset the archive logs, recreate the standby database.

Figure 60 SAP R/3 recovery options



Instant recovery using the Data Protector CLI

Execute:

```
omnir
-host ClientName
```

```
-session SessionID
-instant_restore
[P9000_DISK_ARRAY_XP_OPTIONS | P6000_ENTERPRISE_VIRTUAL_ARRAY_OPTIONS]
-sap
-user UserName -group GroupName
-recover {now | time MM/DD/YY hh:mm:ss | logseq LogSeqNumber thread
ThreadNumber | SCN Number} [-open [-resetlogs]]
-appname ApplicationDatabaseName
```

The order of options is important. On Windows clients, the user name and group name options are not required. For a detailed description of the options, see the *HP Data Protector Command Line Interface Reference*.

Instant recovery from replicas containing the control file

During an instant recovery from a replica that contains the control file, the current control file and, possibly, online redo logs get overwritten. Therefore, before you start the session, copy the current control file and online redo logs to a safe location to be able to do a database recovery afterwards.

A replica contains the control file if it is created in any of the following sessions:

- *Online* ZDB session with the `omnirc` option `ZDB_ORA_INCLUDE_CF_OLF` set to `1`
- *Online* SAP compliant ZDB session
- *Offline* ZDB session (any configuration)

NOTE: An *offline* ZDB session also contains online redo logs. You can use such a session to restore the SAP R/3 database to a point in time at which the backup was performed. In this case, you do not need to follow the steps below.

To restore and recover the database:

1. Copy the current control files and online redo logs to a safe location.
2. Perform instant recovery (without database recovery). Use the Data Protector GUI or CLI.
3. Copy the current control files and online redo logs back to their original location.
4. Mount the target database.
5. Restore missing archived redo logs required for database recovery.

   Example:

   ```
   # sqlplus user/password@net_service_name
   SQL> select SEQUENCE#, NAME from V$ARCHIVED_LOG  where
   (NEXT_TIME>to_date('2010/10/03','YYY/MM/DD') and (FIRST_CHANGE#<='1000');
   # brrestore -a log_no,... -d util_file -c force -u user/password
   ```

6. Recover the target database.

   Example:

   ```
   # rman target user/password@net_service_name
   RMAN> run{
      2> allocate channel dbrec type disk;
      3> recover database until scn 1000;
      4> release channel dbrec;
      5> }
   ```

Restoring using another device

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

Using the Data Protector GUI

For information on how to select another device for a restore using the Data Protector GUI, see the *HP Data Protector Help* index: "restore, selecting devices for".

Using the Data Protector CLI or SAP commands

If you are restoring using the Data Protector CLI or SAP R/3 commands, specify the new device in the file:

Windows systems: *Data_Protector_program_data*\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 systems, use the Unicode format for the file.

Localized SAP R/3 objects

Oracle Server uses its own encoding, which may differ from the encoding used by the filesystem. In the Backup context, Data Protector displays the logical structure of the Oracle database (with Oracle names) and in the Restore context, the filesystem structure of the Oracle database. Therefore, to display non-ASCII characters correctly, ensure that the Data Protector encoding matches with the Oracle Server encoding during backup and with the filesystem encoding during restore. However, the incorrect display does not impact the restore.

Windows systems: If the current values of DBCS and the default Windows character set for non-Unicode programs do not match, problems arise. See ZDB, restore, or instant recovery sessions fail due to invalid characters in filenames.

UNIX systems: To be able to switch between the Data Protector encodings, start the GUI in UTF-8 locale.

Monitoring sessions

You can monitor currently running sessions in the Data Protector GUI. When you run an interactive backup or a 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 *HP Data Protector Help* index: "viewing currently running sessions".

System messages generated during backups are sent to both the SAP R/3 and the Data Protector monitor. However, mount requests are sent only to the Data Protector monitor.

Troubleshooting

This section lists general checks and verifications plus problems you might encounter when using the Data Protector SAP R/3 integration.

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

For general ZDB, restore, and instant recovery related troubleshooting, see the troubleshooting sections in the *HP Data Protector Zero Downtime Backup Administrator's Guide*.

See also the troubleshooting section in the SAP R/3 chapter of the *HP Data Protector Integration Guide*.

Before you begin

- Ensure that the latest official Data Protector patches are installed. See the *HP Data Protector 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.
- For an up-to-date list of supported versions, platforms, and other information, see the latest support matrices at http://support.openview.hp.com/selfsolve/manuals.

General troubleshooting

Problem

Configuration fails due to a database operation failure

During configuration of an SAP R/3 database, Data Protector reports the following error:

```
Integration cannot be configured.
The database reported error while performing requested operation.
```

Action

Review user group membership for the user account which is used in Oracle database access authentication. For details, see "Configuring user accounts" (page 115).

Verifying the prerequisites (Oracle side)

Perform the following verification steps, in numerical order, to verify that Oracle is installed properly:

1. On the application system, verify that the target database is online, as follows:

   UNIX systems:

   ```
   export ORACLE_SID=Oracle_SID
   export ORACLE_HOME=Oracle_home_path
   $ORACLE_HOME/bin/sqlplus
   ```

   Windows systems:

   ```
   set ORACLE_SID=Oracle_SID
   set ORACLE_HOME=Oracle_home_path
   %ORACLE_HOME%\bin\sqlplus
   ```

   At the SQLPlus prompt, type:

   ```
   connect user/passwd@service
   select * from dba_tablespaces
   exit;
   ```

   Try starting the target database.

2. In order to establish the TNS network connection, verify that Net8 software is configured correctly for the target database, as follows:
   - On the application system, perform the following:

     UNIX systems:

     `$ORACLE_HOME/bin/lsnrctl status service`

     Windows systems:

     `%ORACLE_HOME%\bin\lsnrctl status service`

     If it fails, either start the TNS listener process or see the Oracle documentation on how to create the TNS configuration file (LISTENER.ORA).
   - On the application system, perform the following. Use `sqlplus`:

     UNIX systems:

     `export ORACLE_SID=Oracle_SID`

     `export ORACLE_HOME=Oracle_home_path`

     `$ORACLE_HOME/bin/sqlplus`

     Windows systems:

     `set ORACLE_SID=Oracle_SID`

     `set ORACLE_HOME=Oracle_home_path`

     `%ORACLE_HOME%\bin\sqlplus`

     At the SQLPlus prompt, type:

     `connect user/passwd@service;`

     `exit;`

     If it fails, see the Oracle documentation on how to create the TNS configuration file (TSNAMES.ORA).

Verifying the prerequisites (SAP side)

Before you begin the steps in this section, be sure you have completed all the steps in "Verifying the prerequisites (Oracle side)" (page 147).

Perform the following verification steps, in numerical order, to verify that SAP is installed properly:

1. On the application system, verify a backup directly to disk, as follows:

   `brbackup -d disk -u user/password`

   If it fails, see the *SAP Online Help* for instructions on how to execute a backup to disk using the SAP backup utility.
2. On the application system, verify a restore from the disk, as follows:

   `brrestore -d disk -u user/password`

   If it fails, see the *SAP Online Help* for instructions on how to execute a restore to disk using the SAP restore utility.

3. On the application system, verify that SAP is configured properly, as follows:

   Move the original `backint`. Create a test script with the name `backint` in the directory with the SAP backup utility, with the following entries:

   ```
   #!/usr/bin/sh
   echo "Test backint called as follows:"
   echo "$0 $*"
   echo "exiting 3 for a failure"
   exit 3
   ```

   Export all environment variables required by the SAP (SAPDATA_HOME, SAPBACKUP...) and then start the command with the backup owner user:

   `brbackup -t offline_split -d util_file -u` *`user/password`* `-c`

   or, if Data Protector uses `splitint`:

   `brbackup -t offline_mirror -d util_file -u` *`user/password`* `-c`

   If you receive arguments from `backint`, that means SAP is properly configured for backup using `backint`. Otherwise, you should reconfigure SAP.

Verifying the configuration

Before you begin this section, be sure that you completed all the steps provided in the sections "Verifying the prerequisites (Oracle side)" (page 147) and "Verifying the prerequisites (SAP side)" (page 148).

Perform the following verification steps, in numerical order, to verify that Data Protector is configured properly:

1. On the application system, verify a Data Protector filesystem backup of the SAP Database Server:

   Perform a filesystem backup of the Oracle Server system so that you can eliminate any potential communication problems between the Oracle Server and the Data Protector Cell Manager system.

   See the *HP Data Protector Help* index "standard backup procedure" for details about how to do a filesystem backup.

   If it fails, see the *HP Data Protector Troubleshooting Guide* for help with troubleshooting a filesystem backup.

2. Verify the environment variable on the application system:

   If you have to export some variables before starting the SAP backup utilities, Oracle Server Manager, or the TNS listener, set these environment variables using the Data Protector GUI.

3. Verify the permissions of the SAP user on application system:

   SAP user permissions must be set to enable you to perform an SAP backup or restore with Data Protector. See "Configuring user accounts" (page 115). Use the `testbar2` to check the permissions:

   - Login in as an SAP user
   - Execute `/opt/omni/bin/testbar2 -perform:checkuser`

   If the user account has all the required permissions, you will see only the usual messages displayed on the screen.

4. Examine the system errors:

   System errors are reported in the following file on the Oracle Server:

   `/var/opt/omni/log/debug.log`

Verifying the backup configuration

Before you begin this section, be sure that you completed all the steps provided in the sections "Verifying the prerequisites (Oracle side)" (page 147) and "Verifying the prerequisites (SAP side)" (page 148).

Perform the following verification steps, in numerical order, to verify that Data Protector is configured properly:

1. Verify the Data Protector SAP ZDB configuration on the application system:

   Execute the following command:

   HP-UX and Solaris systems:`/opt/omni/lbin/util_sap -CHKCONF ORACLE_SID`

   Windows systems:`Data_Protector_home\bin\util_sap.exe -CHKCONF ORACLE_SID`

   If an error occurs, the error number is displayed in the form `*RETVAL*error_number`.

   To get the error description, on the Cell Manager, execute:

   Windows systems:: `Data_Protector_home\bin\omnigetmsg 12 error_number`

   which is located on the Cell Manager.

   HP-UX and Linux systems: `/opt/omni/lbin/omnigetmsg 12 error_number`

2. Verify the SAP user.

   Check that the respective user group has the `See Private Objects` user right selected. See also "Configuring user accounts" (page 115).

3. On the application system, verify the backup using `testbar2`:

   Execute the following to ensure that communication within Data Protector is established:

   - Create a non-ZDB backup specification on the application system.
   - Execute:

     ```
     /opt/omni/bin/testbar2 -type:SAP -appname:ORACLE_SID \
     -perform:backup -file:file_name -bar barlist_name
     ```

   If it fails, check the errors and try to fix them or call a support representative for assistance.

4. On the application system, verify the backup using backint:

   Execute the following command to ensure that communication within Data Protector is established and that a backup of files can be performed:

   - Create a non-ZDB backup specification on the backup system.
   - ```
     export OB2BARLIST=barlist_name
     export OB2APPNAME=ORACLE_SID
     /opt/omni/lbin/backint -f backup -t file -u ORACLE_SID -i \
     input_file
     ```

     where `input_file` is the file containing the full pathnames for backup.

   If it fails, check the errors and try to fix them or call a support representative for assistance.

Verifying restore

Before you begin this section, be sure that you completed all the steps provided in the sections "Verifying the prerequisites (Oracle side)" (page 147) and "Verifying the prerequisites (SAP side)" (page 148).

Perform the following verification steps, in numerical order, to verify that Data Protector is configured properly:
     ```

1. Verify the user for the restore

   Verify that the user specified for the restore session is the user of the backup session and that they belong to the Data Protector operator or admin group. Check that the respective user group has the `See private objects` user right selected.
2. Verify that files are backed up and in the Data Protector database:
   - Using the `omnidb` command;

     See the appropriate man page on using the `omnidb` command.
   - Using `backint`;

     SAP tools also use this command to make a query.

     `/opt/omni/lbin/backint -f inquiry -u ORACLE_SID -i input_file`

     where *`input_file`* is what will be queried. `Backint` expects a list of files in the following format:

     `backint_ID_1 pathName_1`

     `backint_ID_2 pathName_2`

     `backint_ID_3 pathName_3`

     To retrieve the *`backint_ID`* numbers, enter the following command:

     `echo "#NULL #NULL" | backint -f inquiry -u ORACLE_SID`

     or, alternatively, you can just specify `#NULL` as *`backint_ID_1`* in the *`input_file`*. In this case, the latest backup session for the file is used for the restore.

   If it fails, proceed as follows:
   - Check the backup session - was it successful?
   - Check the user rights. Was the query started under the correct SAP user account?
   - Call a support representative for assistance.
3. Verify the restore using Data Protector or CLI:

   If it fails, proceed as follows:
   - Check the backup session - was it successful?
   - Check that the files are in the Data Protector database.
   - Check the user rights. Was the restore started under the correct SAP user account?
   - Call a support representative for assistance.
4. Verify the restore using `testbar2`:

   Execute the following to ensure that restore is possible:

   ```
   /opt/omni/bin/testbar2 -type:SAP -appname:ORACLE_SID \
   -perform:restore -file:file_name -bar barlist_name -object objectName
   ```

   If it fails, proceed as follows:
   - Check the backup session - was it successful?
   - Check that the files are in the Data Protector database.
   - Check the user rights. Was the a restore started under the correct SAP user account
   - Call a support representative for assistance.

5. Verify the restore using `backint`:

   `backint` is the same command used by the SAP backup utility.

   ```
   /opt/omni/lbin/backint -f restore -u ORACLE_SID -i input_file
   ```

   where *`input_file`* specifies what will be restored; `backint` expects the list of files in the following format:

   ```
   backint_ID_1 pathName_1 [targetDirectory_1]
   backint_ID_2 pathName_2 [targetDirectory_2]
   backint_ID_3 pathName_3 [targetDirectory_3]
   ```

   To retrieve the *`backint_ID`* numbers, enter the following command:

   ```
   echo "#NULL #NULL" | backint -f inquiry -u ORACLE_SID
   ```

   or, alternatively, you can just specify `#NULL` as *`backint_ID_1`* in the *`input_file`*. In this case, the latest backup session for the file is used for the restore.

   If it fails, proceed as follows:

   - Check the backup session - was it successful?
   - Check that the files are in the Data Protector database.
   - Check the user rights. Was the restore started under the correct SAP user account?
   - Call a support representative for assistance.

Configuration and backup problems

The following list gives a description of problems and actions to be taken to resolve them:

- **The Server Manager is unable to connect to the destination**

  Check whether the Oracle TNS listener process is up and running. Check whether there are any environment variables required for a successful remote connection to the target database; for example, *`TNS_ADMIN`* and *`SHLIB_PATH`*. Set these environment variables using the Data Protector GUI.

  For more information on the Data Protector SAP configuration file, see "Data Protector SAP R/3 configuration file" (page 109).

- **Configuration procedure fails**

  Check whether the Oracle Server is up and running.

  Check the login information for the target from the application system using Oracle Server Manager. If you cannot log in, then perform the following actions:

  Check whether `sysoper` and `sysdba` rights are set for the Oracle administrator user.

  Examine system errors reported in:

  UNIX systems:

  ```
  /var/opt/omni/log/debug.log
  /var/opt/omni/log/sap.log
  /var/opt/omni/log/oracle8.log
  ```

  Windows systems:

  ```
  Data_Protector_program_data\log\debug.log,
  Data_Protector_program_data\log\sap.log
  Data_Protector_program_data\log\oracle8.log
  ```

  If you have special Oracle environment settings, ensure that they are registered in the `Environment` sublist of the Data Protector SAP configuration file:

`/etc/opt/omni/server/integ/config/SAP/client_name%ORACLE_SID` (UNIX Cell Manager), or `Data_Protector_program_data\Config\server\integ\config\sap\client_name%ORACLE_SID` (Windows Cell Manager).

For more information on the Data Protector SAP configuration file, "Data Protector SAP R/3 configuration file" (page 109).

- **Starting the backup fails**

  On UNIX systems, check the output of the following command on the application system:

  `/opt/omni/lbin/util_sap.exe -CHKCONF ORACLE_SID`

  In case of an error, the error number is displayed in the form:

  `*RETVAL*Error_number`

  To get the error description, start the following command on the application system:

  `/opt/omni/lbin/omnigetmsg 12 Error_number`

  On Windows systems, perform the following procedure using the Data Protector GUI:

  1. In the Context List, select **Backup**.
  2. In the Scoping Pane, expand **Backup**, **Backup Specifications**, and then **SAP R/3**. A list of SAP backup specifications is displayed.
  3. In the Scoping Pane, select the failed backup specification and right-click on the SAP R/3 server item in the Results Pane to display a pop-up menu.
  4. From the pop-up menu, select **Check Configuration**.

  A short description of the problems and how to resolve them is displayed.

- **Backup does not work**

  - Check whether the Cell Manager is correctly set on the application system. The file `/etc/opt/omni/client/cell_server` (UNIX systems) or `HKEY_LOCAL_MACHINE\SOFTWARE\Hewlett-Packard\OpenView\OmniBackII\Site\CellServer` (Windows systems) must contain the name of the Cell Manager.
  - Check that the `primary_db` parameter in the `initORACLE_SID.sap` file on the application system is set to `LOCAL`.
  - On UNIX systems, check whether the users are properly configured in user groups. Both the UNIX Oracle administrator (`oraORACLE_SID`) and UNIX SAP administrator (`ORACLE_SIDadm`) have to be in the Data Protector operator class.
  - On UNIX systems, check whether the permissions of the `SAPDATA_HOME/sapbackup/` directory are set to 755.
  - On Windows systems, check that the user account that started the Data Protector Inet service is added in the Data Protector operator class.

- **Backup fails with "Connect to database instance failed"**

  If you start a backup while the database instance is in the `unmount` or `mount` mode, the session fails with a message similar to the following:

  ```
  BR0301E SQL error -1033 at location BrDbConnect-2
  ORA-01033: ORACLE initialization or shutdown in progress
  BR0310E Connect to database instance HOOHOO failed
  ```

  Before you start a backup, ensure that the database instance is the `open` or `shutdown` mode.

Problem

Configuration fails due to a script failure

During configuration of an SAP R/3 database, Data Protector reports the following error:

```
Integration cannot be configured.
Script failed. Cannot get information from remote host.
```

Action

If the SAP R/3 database is located on a Windows system, check the environment settings and ensure Data Protector Inet is running under a user account which has the required privileges. For details, see "Before you begin" (page 114).

If the SAP R/3 database is located on a UNIX system, resolve the problem by reviewing the user account configuration. For details, see "Configuring user accounts" (page 115).

Problem

Backup using backint fails on Solaris and HP-UX

A backup using backint fails on a Solaris and HP-UX systems with the following error:

```
[Major] From: OB2BAR_DMA@computer.company.com "SAP" Time: 4/29/09 3:55:52
PM

Cannot open file '/saphome/SAP/sapbackup/cntrlSAP.dbf'. Error: 13
```

Action

Share the directories on the application system through NFS with root permissions. On the application system, add the following line in the file `/etc/dfs/dfstab`:

Solaris systems:

```
share -F nfs -o anon=0 /usr/src
```

HP-UX systems:

```
share -F nfs -o anon=0,rw -d "" SAPHOME
```

Problem

A ZDB session fails after reporting connections errors

A ZDB session reports the following critical errors and completes with failures:

```
Connection with DMA was reset
Signal SIGABRT (6) received from BRtools
```

Action

In the SAP parameter file on the application system, set the parameter `primary_db` to `LOCAL` and restart the session.

For details, see "Configuring the SAP R/3 parameter file" (page 124).

Restore problems

Problem

ZDB, restore, or instant recovery sessions fail due to invalid characters in filenames

On Windows systems, where the Oracle Database Character Set (DBCS) is not set to the same value as the default Windows character set for non-Unicode programs, and where SAP tools are used to create Oracle datafiles, ZDB, restore, and instant recovery fail if the datafiles contain non-ASCII or non-Latin 1 characters.

Actions

Use any of the following solutions:

- For new Oracle installations, set the DBCS to UTF-8.
- If you do not use other non-Unicode programs, set the language for non-Unicode programs to the same value as DBCS.
- Do not use non-ASCII or non-Latin 1 characters for filenames.

Problem

Restore of SAP R/3 tablespaces located on raw partitions fails

When restoring SAP tablespaces that are located on raw partitions using the Data Protector GUI, the restore fails with a message similar to the following:

```
[Major] From: VRDA@joca.company.com "SAP" Time: 5/9/06 3:33:51 PM
/dev/sapdata/rsapdata Cannot restore -> rawdisk section ![Warning] From:
VRDA@joca.company.com "SAP" Time: 5/9/06 3:42:45 PM Nothing restored.
```

Action

Use SAP commands (for example, `brrestore`) to restore these tablespaces.

3 Data Protector Microsoft SQL Server ZDB integration

Introduction

This chapter explains how to configure and use the Data Protector Microsoft SQL Server ZDB integration. It describes the concepts and methods you need to understand to back up and restore the Microsoft SQL Server (**SQL Server**) database objects.

During the backup, an SQL Server snapshot is made (the database files are frozen and any transactions to them are cached), so the database is highly available (*online* backup). The I/O to it is suspended during the time it takes to create a **replica** (split the mirror disks or create snapshots).

NOTE: SQL Server snapshot is an SQL Server related term and does not mean the same as a disk array snapshot.

The following disk arrays and array configurations are supported:

Supported array	Supported configurations
EMC Symmetrix (EMC)	Dual-host TimeFinder
HP P9000 XP Disk Array Family (P9000 XP Array)	HP BC P9000 XP, HP CA P9000 XP, combined HP CA+BC P9000 XP
HP P6000 EVA Disk Array Family (P6000 EVA Array)	HP BC P6000 EVA, combined HP CA+BC P6000 EVA

All ZDB types (ZDB to tape, ZDB to disk, and ZDB to disk+tape) are supported by this integration. For ZDB types description, see the *HP Data Protector Zero Downtime Backup Concepts Guide* and the *HP Data Protector Help*.

Using Data Protector, you can restore your SQL Server data:

- From backup media to the application system on LAN (standard restore).
- Using the instant recovery functionality.

The following table gives an overview of SQL Server recovery methods:

ZDB type	Recovery method
ZDB to tape	Standard restore
ZDB to disk	Instant recovery
ZDB to disk+tape	Standard restore, instant recovery

For a description of ZDB and instant recovery (IR) concepts, see the *HP Data Protector Zero Downtime Backup Concepts Guide*.

ZDB and IR do not support an SQL Server availability group configuration.

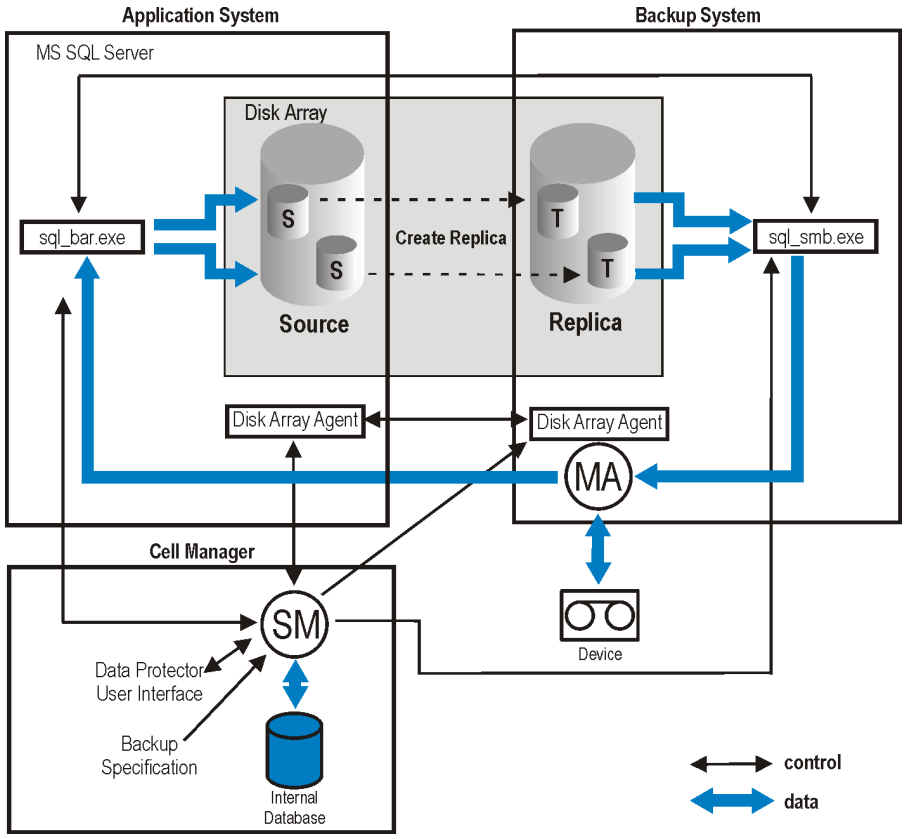
Integration concepts

Data Protector integrates with SQL Server through the Data Protector `sql_bar.exe` executable, installed on SQL Server. During backup, `sql_bar.exe`, started on the application system, connects to SQL Server to find the locations of the database files. The integration then backs up SQL Server database(s), which are replicated within a disk array.

During restore, `sql_bar.exe` connects to SQL Server to receive the restore data, which is then written to disks.

ZDB process depends on whether you replicate your data in a split mirror or snapshot replication and on the selected ZDB type. Restore process depends on the restore type - standard restore or instant recovery. See the *HP Data Protector Zero Downtime Backup Concepts Guide* for a detailed description of replication techniques and ZDB and restore processes.

Figure 61 Backup and restore concepts



Configuring the integration

Prerequisites

- You need a license to use the SQL Server ZDB integration. For information, see the *HP Data Protector Installation and Licensing Guide*.
- Make sure that you correctly installed and configured SQL Server.
  - For supported versions, platforms, devices, and other information, see the latest support matrices at http://support.openview.hp.com/selfsolve/manuals.
  - For information on installing, configuring, and using SQL Server, see the SQL Server documentation.
- Make sure that you correctly installed Data Protector. For information on installing Data Protector in various architectures and installing a Data Protector disk array integration (P6000

EVA Array, P9000 XP Array, or EMC) with SQL Server, see the *HP Data Protector Installation and Licensing Guide*.

Every SQL Server to be used with Data Protector must have the `MS SQL Integration` component installed.

- Install SQL Server on the application system. Install user databases on the disk array source volumes (system databases can be installed anywhere). If the system databases are also installed on a disk array, they *must* reside on *different* source volumes than user databases.

  If SQL Server is installed on the backup system as well, its databases *must* reside on source volumes *different* from the source volumes used for this integration. Drive letters/mount points assigned to those volumes must also be different from the drive letters/mount points assigned to the volumes used for this integration.

Before you begin

- Configure devices and media for use with Data Protector. For instructions, see the *HP Data Protector Help* index: "configuring devices" and "creating media pools".
- On Windows Server 2003 systems, if you plan to use **Integrated authentication** to connect to an SQL Server instance, you need to restart the `Data Protector Inet` service under a Windows domain user account that has the appropriate SQL Server permissions for running backup and restore sessions. For information on changing the user account under which the `Data Protector Inet` service is running, see the *HP Data Protector Help* index: "Inet, changing account".

  However, for other supported Windows operating systems, you can use user impersonation instead. For details on setting accounts for the Inet service user impersonation, see the *HP Data Protector Help* index: "Inet user impersonation".
- Using the SQL Server Management Studio, add the user account which you will use for backing up and restoring SQL Server data to the fixed server role `sysadmin`. For instructions, see the SQL Server documentation.
- To test whether SQL Server and Cell Manager communicate properly, configure and run a Data Protector filesystem ZDB and restore. For instructions, see the *HP Data Protector Help*.

Data Protector SQL Server configuration file

Data Protector stores integration parameters for every configured SQL Server on the Cell Manager in:

HP-UX and Linux systems:

`/etc/opt/omni/server/integ/config/MSSQL/`*`ClientName%InstanceName`*

Windows systems:

`Data_Protector_program_data`
`\Config\Server\Integ\Config\MSSQL\`*`ClientName%InstanceName`*

Configuration parameters are the username and password of the SQL Server user, who must have permissions to run backups and restores within SQL Server (assuming the standard security is used). They are written to the Data Protector SQL Server configuration file during configuration of the integration.

The content of the configuration file is:

```
Login='user';
Password='encoded_password';
Domain='domain';
Port='PortNumber';
```

IMPORTANT: To avoid backup problems, make sure that the syntax of your configuration file matches the examples.

Examples

- ***SQL Server authentication:***

```
Login='sa';
Domain='';
Password='jsk74yh80fh43kdf';
```

- ***Windows authentication:***

```
Login='Administrator';
Domain='IPR';
Password='dsjf08m80fh43kdf';
```

- ***Integrated authentication:***

```
Login='';
Domain='';
Password='kf8u3hdgtfh43kdf';
```

Configuring users

On Windows Server 2003 system, if you have restarted the `Data Protector Inet` service on the SQL Server system under a different user account, add this user to the Data Protector `admin` or `operator` Data Protector user group.

For information on adding users to the Data Protector groups, see the *HP Data Protector Help* index: "adding users".

Configuring an SQL Server cluster

In a cluster, all the nodes must be installed as Data Protector cluster-aware clients and the `Data Protector Inet` service on all nodes must run under a Windows domain user account that has also cluster administrator rights.

You must configure the `Data Protector Inet` service user impersonation for all cluster nodes. The Windows domain user account that is used must be given the following Windows operating system Security Policy privileges:

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

For more information, see the *HP Data Protector Help* index: "cluster-aware client", "Inet user impersonation", and the SQL Server cluster documentation.

Configuring SQL Server instances

An SQL Server instance is configured during the creation of the first backup specification. The configuration consists of setting the user account that Data Protector should use to connect to the SQL Server instance. The specified login information is saved to the Data Protector SQL Server instance configuration file on the Cell Manager.

NOTE: Make sure that the user account to be used has appropriate SQL Server permissions for running backups and restores. Check the permissions using SQL Server Enterprise Manager.

You can change configuration by following instructions described in "Changing and checking configuration" (page 161).

Prerequisites

- SQL Server must be online during configuration.
- Make sure that the SQL Server Browser service is running.
- Configuration must be performed for every SQL Server instance separately.

Using the Data Protector GUI

1. In the Context List, click **Backup**.
2. In the Scoping Pane, expand **Backup Specifications**, right-click **MS SQL Server**, and click **Add Backup**.
3. In the **Create New Backup** dialog box, select the **Blank Microsoft SQL Server Backup** template and specify backup type. For details, see Step 3.

   Click **OK**.
4. Specify the ZDB-specific options. For details, see Step 4.
5. In **Application database**, select or specify the name of the SQL Server instance.

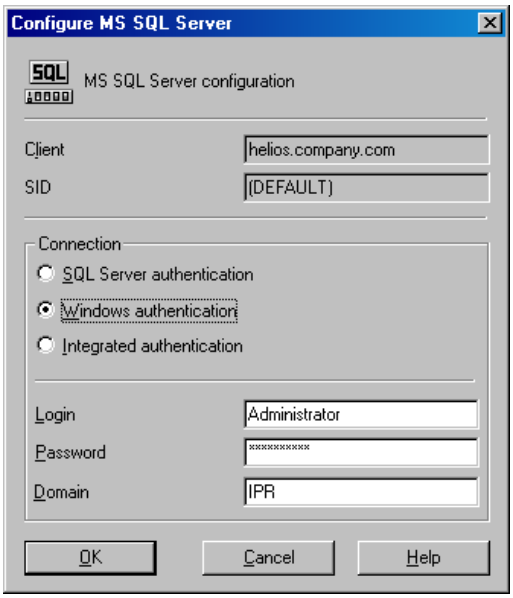
   Windows Server 2008: If you intend to use **Integrated authentication** and you want that the backup session runs under the specified operating system user account, specify the **Specify OS user** option. For information on the **User and group/domain** options, press **F1**.

   Click **Next**.
6. In the Configure MS SQL Server dialog box, specify the user account that Data Protector should use to connect to the SQL Server instance.
   - **SQL Server authentication**: SQL Server user account. Specify a username and password.
   - **Windows authentication**: Windows domain user account (preferred option). Specify a username, password, and the domain.
   - **Integrated authentication**: Select this option to enable Data Protector to connect to the SQL Server instance with the following Windows domain user account:
     - ***Windows Server 2008:*** The account specified in the **User and group/domain** options in the previous step or in the Client selection page.
     - ***Other Windows systems:*** The account under which the `Data Protector Inet` service on the SQL Server system is running.

   Make sure that the user account you specify has the appropriate permissions for backing up and restoring the SQL Server databases.

   See "Configuring SQL Server" (page 161).

Figure 62 Configuring SQL Server



NOTE: It is recommended that the SQL Server system administrator configures the integration.

For details about security, see the SQL Server documentation.

Click **OK** to confirm the configuration.

7. The SQL Server instance is configured. Exit the GUI or proceed with creating the backup specification at "Creating ZDB specifications" (page 163).

Using the Data Protector CLI

Execute:

```
sql_bar config [-appsrv:SQLServerClient] [-instance:InstanceName]
[-dbuser:SQLServerUser -password:password | -dbuser:WindowsUser
-password:password -domain:domain]
```

Parameter description

`-appsrv:SQLServerClient`

The client system on which the SQL Server instance is running. This option is not required if you run the command locally.

`-instance:InstanceName`

The SQL Server instance name. If you omit this option, the default SQL Server instance is configured.

`-dbuser:SQLServerUser -password:password`

The SQL Server user account (**SQL Server authentication**)

`-dbuser:WindowsUser -password:password -domain:domain`

The Windows domain user account (**Windows authentication**)

NOTE: If no user account is specified, Data Protector uses **Integrated authentication**.

The message `*RETVAL*0` indicates successful configuration.

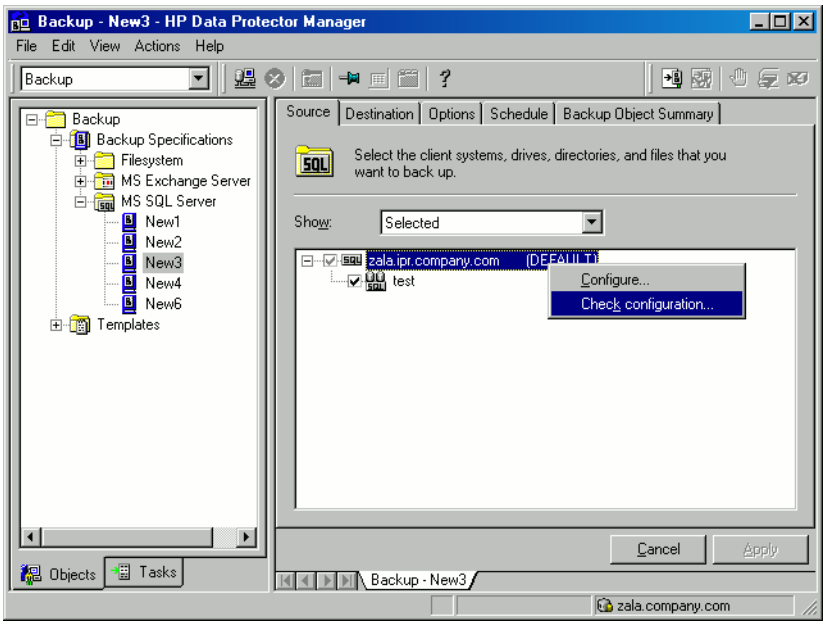
Changing and checking configuration

You can check and change configuration using 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 **MS SQL Server**. Click a backup specification for which you want to change the configuration.
3. In the **Source** property page, right-click the SQL Server name and select **Configure**.
4. Configure SQL Server as described in "Configuring SQL Server instances" (page 159).
5. Right-click SQL Server and select **Check Configuration**. See "Checking configuration" (page 162).

Figure 63 Checking configuration



Using the Data Protector CLI

To change the configuration, run the command for configuring SQL Server instances again, entering different data.

To check configuration , run:

```
sql_bar chkconf [-instance:InstanceName]
```

If the optional parameter `-instance:`*`InstanceName`* is not specified, the default instance is checked.

If the integration is not properly configured, the command returns:

```
*RETVAL*8523
```

To get the information about the existing configuration , run:

```
sql_bar getconf [-instance:InstanceName]
```

If `-instance:`*`InstanceName`* is not specified, Data Protector returns configuration for the default instance.

Backup

To run ZDB of an existing SQL Server ZDB specification:

- Schedule a backup using the Data Protector Scheduler.
- Start an interactive backup using the Data Protector GUI or CLI.

Prerequisites

- In case of nested mount points, the same drive letters, on which the source volumes to be replicated reside on the application system, must exist on the backup system to enable successful mounting of the target volumes. If the same drive letters do not exist on the backup system, the backup fails.

Considerations

Your session will fail if:

- You start ZDB, restore, or instant recovery using the same source volume on the application system at the same time. A session must be started only after the preceding session using the same source volume on the application system finishes.
- SQL Server services are not running when the backup starts.

To configure a ZDB, create a Data Protector SQL Server ZDB specification.

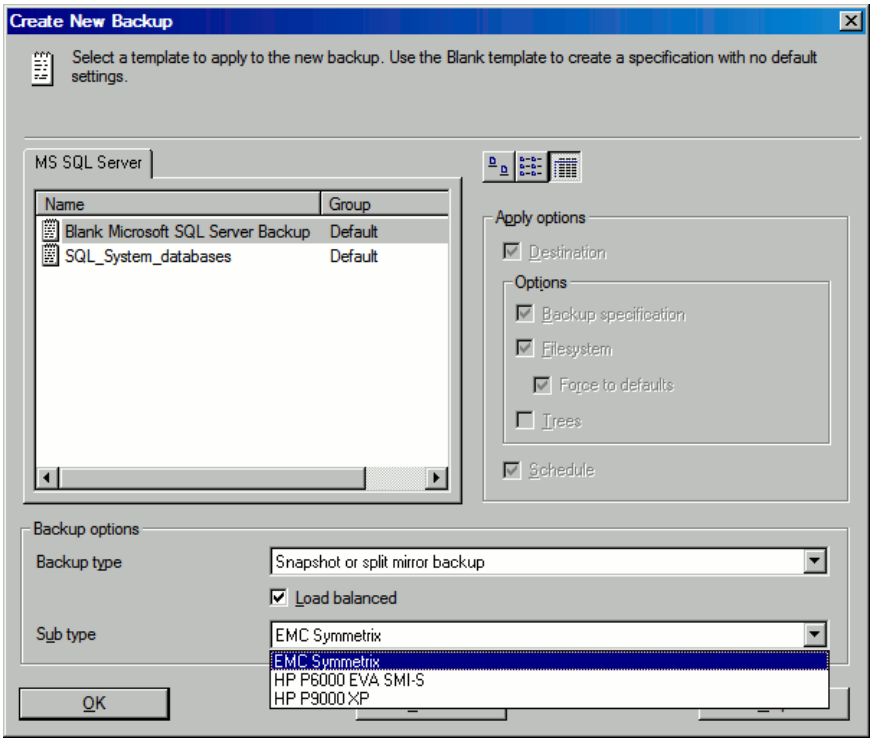
Creating ZDB specifications

Create a ZDB specification, using the Data Protector Manager.

1. In the Context List, click **Backup**.
2. In the Scoping Pane, expand **Backup Specifications**, right-click **MS SQL Server**, and click **Add Backup**.
3. In the **Create New Backup** dialog box, select the **Blank Microsoft SQL Server Backup** template.

   From the **Backup type** drop-down list, select **Snapshot or split mirror backup**, and from the **Sub type** drop-down list, select the appropriate disk array agent. The agent must be installed on the application system and the backup system. See "Selecting a Microsoft SQL Server backup template and the snapshot or split mirror backup" (page 163).

Figure 64 Selecting a Microsoft SQL Server backup template and the snapshot or split mirror backup



Click **OK**.

4. Under **Client systems**, select the SQL Server system. In cluster environments, select the virtual server of the SQL Server resource group.

   In the **Backup system** drop-down list, select the backup system.

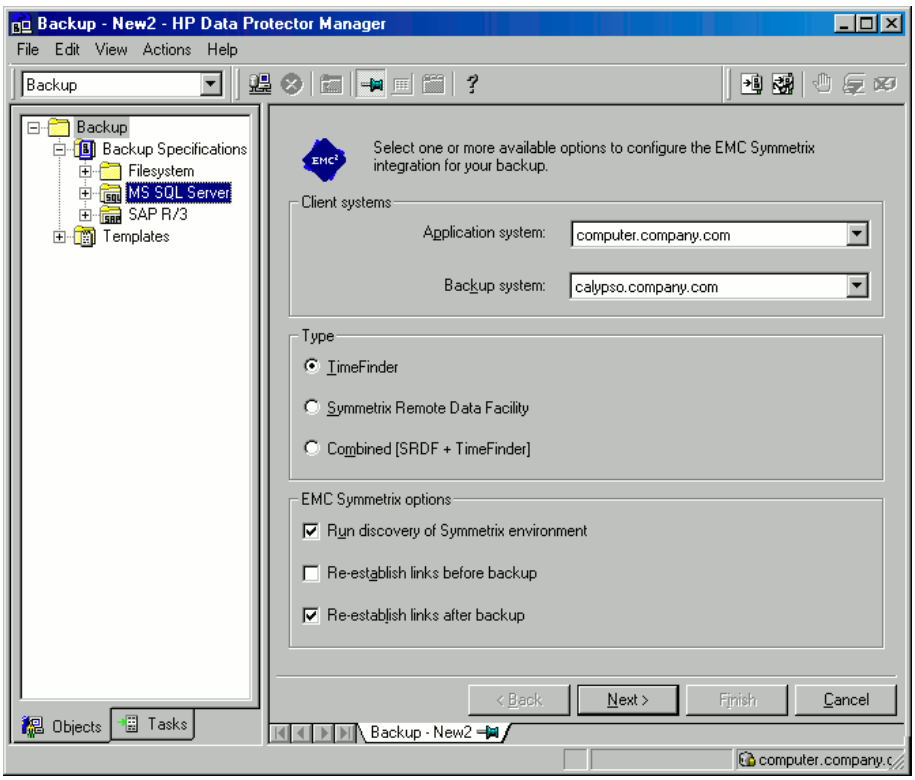
   Select other disk array-specific backup options (see for EMC, "P9000 XP Array backup options" (page 165) for P9000 XP Array, or "P6000 EVA Array backup options" (page 165) for P6000 EVA Array). For detailed information on the backup options, press **F1**.

   EMC:

   In the EMC GeoSpan for Microsoft Cluster Service environment, select the backup system for the active node and specify the TimeFinder configuration.

   After a failover in EMC GeoSpan for MSCS, select the backup system for the currently active node and save the backup specification.

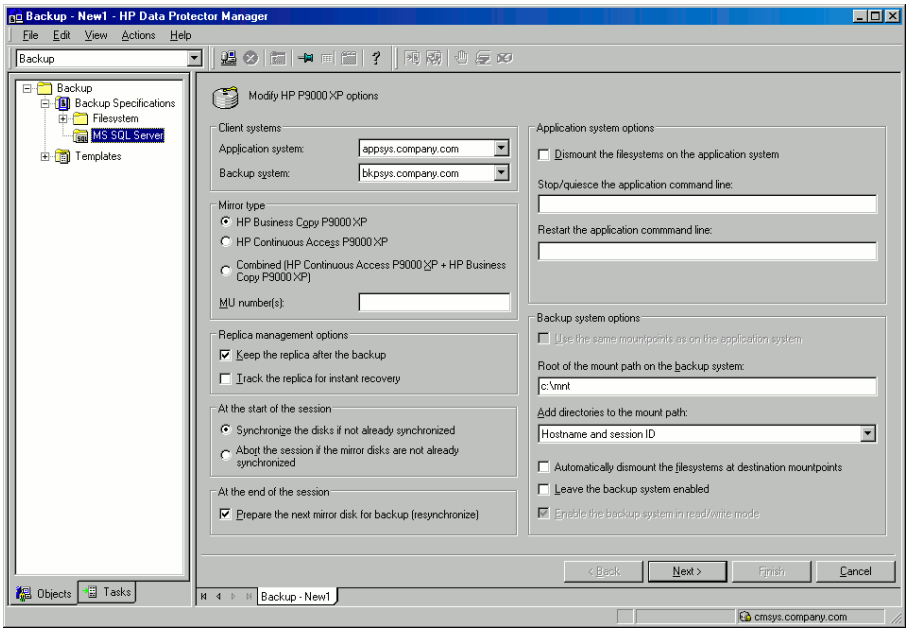
Figure 65 EMC backup options



P9000 XP Array:

To enable instant recovery, leave **Track the replica for instant recovery** selected.

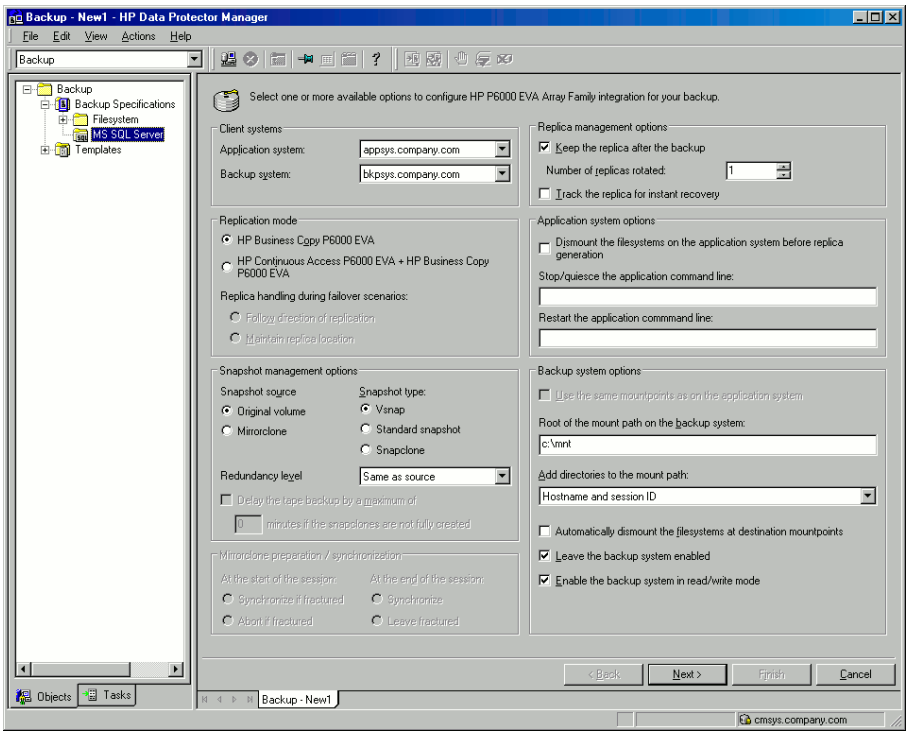
Figure 66 P9000 XP Array backup options



P6000 EVA Array:

To enable instant recovery, select **Track the replica for instant recovery**.

Figure 67 P6000 EVA Array backup options



Click **Next**.

5. In **Application database**, specify the name of the SQL Server instance.

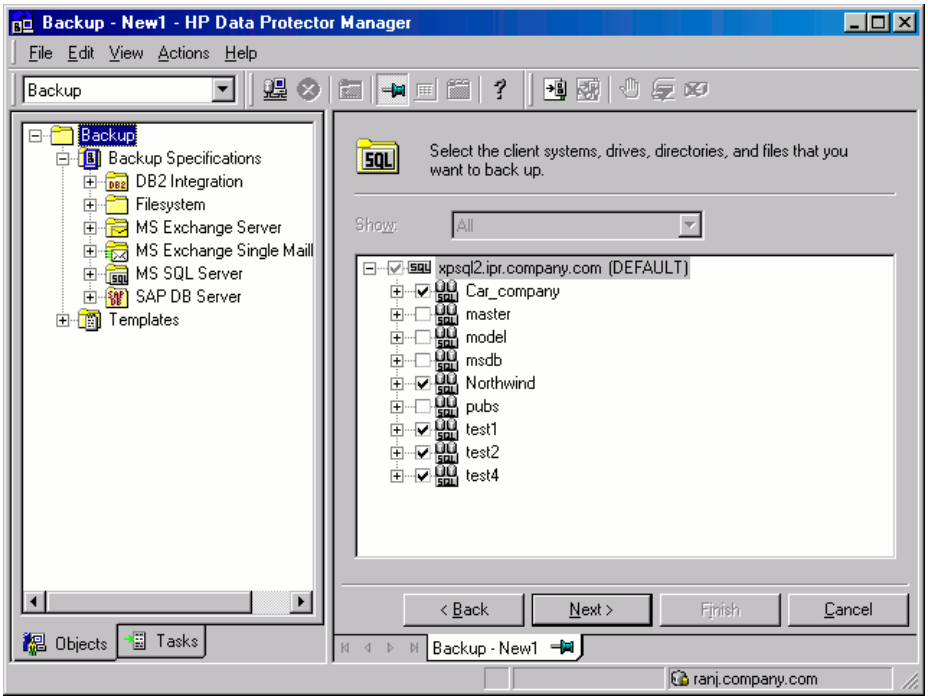
   Windows Server 2008: If you intend to use **Integrated authentication** and you want that the backup session runs under the specified operating system user account, specify the **Specify OS user** option. For information on the **User and group/domain** options, press **F1**.

   Click **Next**.

6. If the client is not configured, the **Configure MS SQL Server** dialog box appears. Configure it as described in "Configuring SQL Server instances" (page 159).
7. Select the databases to be backed up.

IMPORTANT: To enable instant recovery, create different backup specifications for user and system databases.

Figure 68 Selecting user databases



Click **Next**.

8. Select the devices. Click **Properties** to set the media pool and preallocation policy. The device concurrency is set to 1 and cannot be changed. For more information on options, press **F1**.

   To create additional backup copies (mirrors), specify the desired number by clicking **Add mirror**/**Remove mirror**. Select separate devices for each mirror. The minimum number of devices for mirroring equals the number of devices used for backup.

   For more information on object mirroring, see the *HP Data Protector Help*.

   NOTE: Object mirroring is not supported for ZDB to disk.

   Click **Next**.
9. Select backup options.

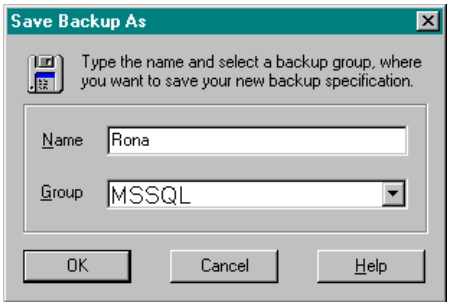
   For information on **Backup Specification Options** and **Common Application Options**, see the *HP Data Protector Help*.

   For information on **Application Specific Option**, see "SQL Server-specific backup options" (page 167).

   Click **Next**.
10. Optionally, schedule the backup. For information on scheduler, press **F1**.

    Note that only **Full** backup is performed.
11. Save the backup specification, specifying a name and backup specification group. You start the backup specification by clicking **Start Backup**.

Figure 69 Saving a backup specification



SQL Server-specific backup options

Specify SQL Server-specific backup options by clicking **Advanced** in the **Application Specific Options** group box page.

Figure 70 Application-specific options

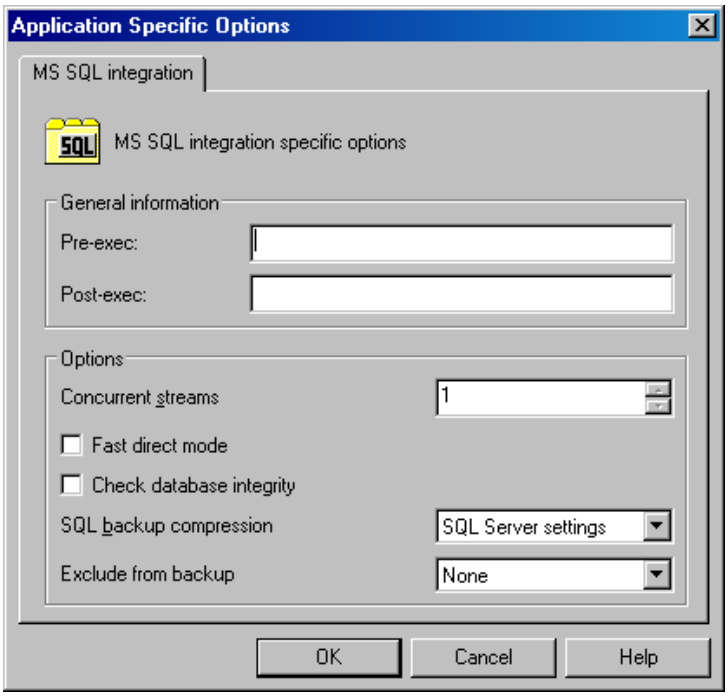


Table 16 SQL Server backup options

Pre-exec	Specifies a command with arguments or a script started by `sql_bar.exe` on SQL Server before backup. Resides in the *`Data_Protector_home`*`\bin` directory. Only the filename must be provided in the backup specification.
Post-exec	Specifies a command with arguments or a script started by `sql_bar.exe` on SQL Server after backup. Resides in the *`Data_Protector_home`*`\bin` directory. Only the filename must be provided in the backup specification.
Concurrent streams	Sets the number of concurrent streams used to back up SQL Server databases from the replica to tape. Applicable for ZDB–to–tape and ZDB–to–disk+tape sessions.
Fast direct mode	Ignored for ZDB sessions.
Check database integrity	Performs data integrity validation before backup. If the check fails, the session completes with warnings.
SQL backup compression	Specify how Data Protector should handle the Microsoft SQL Server backup compression.

Table 16 SQL Server backup options *(continued)*

	SQL Server settings (default)	Handles the backup compression according to the Microsoft SQL Server settings.
	Enable	Executes the backup compression regardless of the Microsoft SQL Server settings.
	Disable	Specifies that the backup compression should not be executed regardless of the Microsoft SQL Server settings.
Exclude from backup *(available for standalone instance backup only)*	Excludes specific databases from backup.	
	Availability Group Databases	Excludes databases belonging to any availability group from backup.
	Standalone databases	Excludes all standalone databases from backup.
	None (default)	Does not exclude any database from backup.

NOTE: Do not use double quotes (" ") in object-specific pre-exec and post-exec commands.

Scheduling backups

You can run unattended ZDB at specific times or periodically. For details on scheduling, see the *HP Data Protector Help* index: "scheduled backups".

NOTE: You cannot run ZDB to disk or ZDB to disk+tape if **Track the replica for instant recovery** is not selected in the backup specification.

Scheduling example

To schedule a database ZDB 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**.

   Click **OK**.
3. Repeat Step 1 and Step 2 to schedule backups at 13:00 and 18:00.
4. Click **Apply** to save the changes.

NOTE: For ZDB sessions, the backup type is set to **Full**.

Starting backup sessions

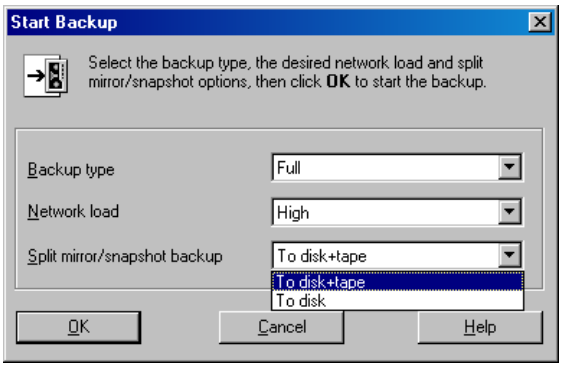
Interactive backups are run on demand. They are useful for urgent backups or restarting failed backups.

Using the Data Protector GUI

1. In the Context List, click **Backup**.
2. In the Scoping Pane, expand **Backup Specifications**, and then **MS SQL Server**. Right-click the backup specification you want to use and select **Start Backup**.

3. Select **Network load**. For information on network load, click **Help**. Click **OK**.
   For ZDB sessions, the backup type is set to **Full**.
   For ZDB to disk or ZDB to disk+tape, specify the **Split mirror/snapshot backup** option.

Figure 71 Starting interactive backups



Using the Data Protector CLI

To start ZDB to tape or ZDB to disk+tape, execute:

```
omnib -mssql_list ListName
```

To start ZDB to disk, execute:

```
omnib -mssql_list ListName -disk_only
```

where *ListName* is the name of the backup specification. For more information on `omnib`, see its man page.

Restore

Data Protector offers restore from backup media to the application system on LAN (standard restore), where you can select various restore options depending on your restore scenario, and instant recovery. For more information, see the following sections.

Before you begin

- Verify that the databases to be restored are not being in use.

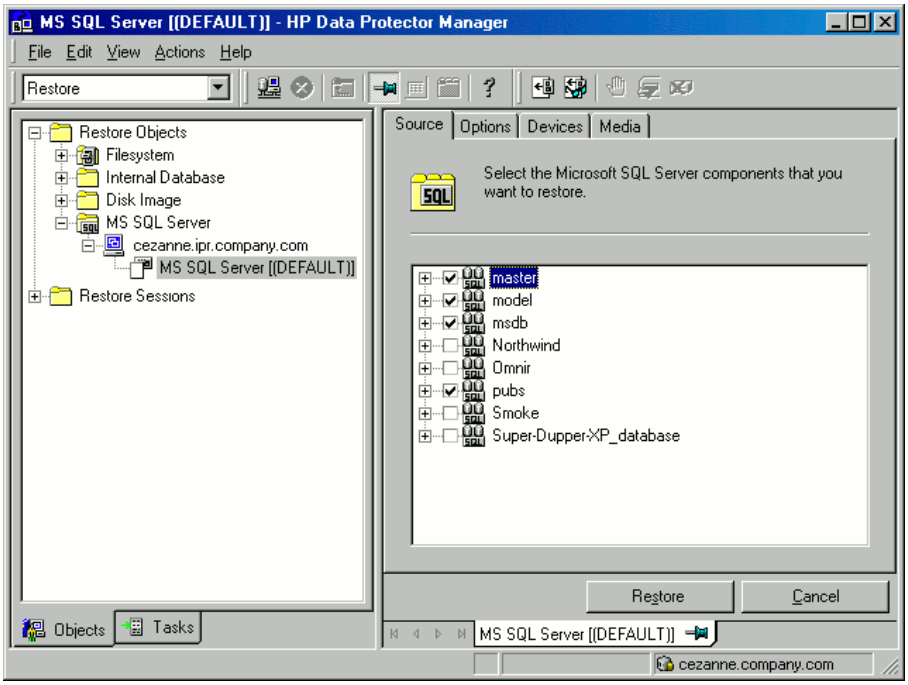
Standard restore

NOTE: There is no need to create an empty database before restore, because the database and its files are generated automatically by SQL Server.

Proceed as follows using the Data Protector Manager:

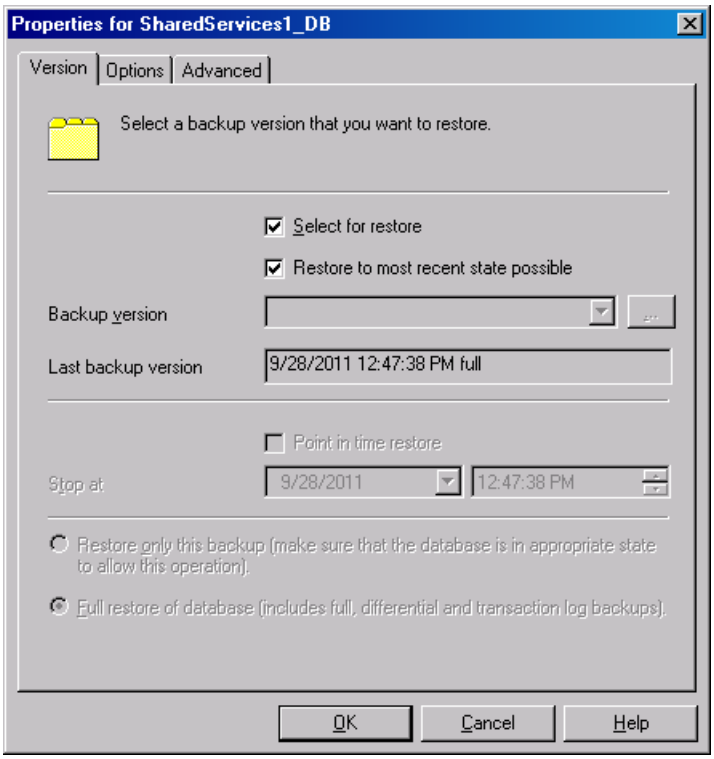
1. In the Context List, click **Restore**.
2. In the Scoping Pane, expand **Restore Objects**, **MS SQL Server**, and then select the client (backup system) from which you want to restore. A list of backed up objects is displayed in the Results Area.
3. Select the SQL Server objects that you want to restore. See "Selecting backup objects for restore" (page 170).

Figure 72 Selecting backup objects for restore



To select backup object-specific options, right-click the object and select **Properties**.

Figure 73 Selecting object-specific options



In the Version tab, select the backup version (backup date) which you want to use for restore.

Select other restore options as appropriate. Note that some options are not available for restore of data files. See "Restore options" (page 171) for details.

Click **OK**.

4. In the **Options** property page, specify new locations for the databases, if you want to restore your data to a different client or instance.

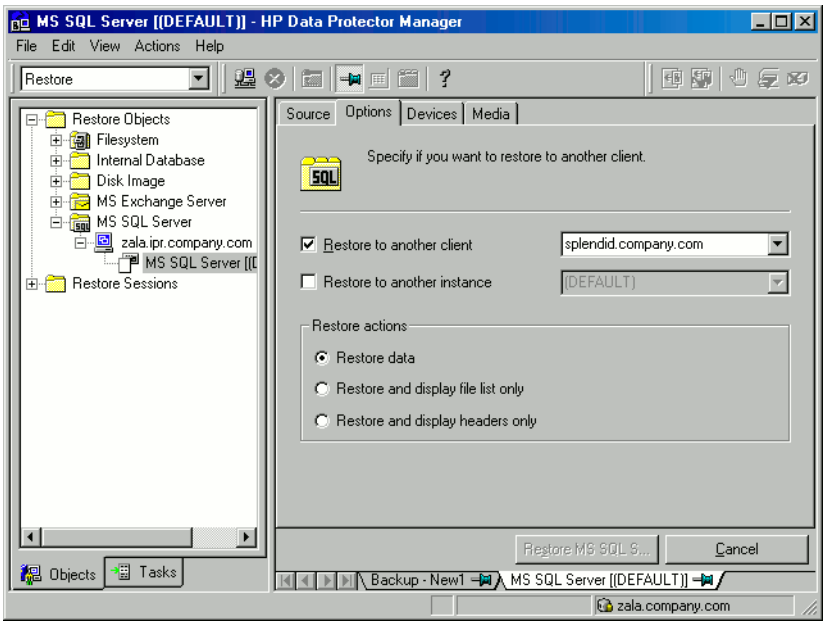
IMPORTANT:

- When you click **Options**, the cell is browsed for running SQL Server instances that can become target instances for restore. If no instances are found, **Restore to another instance** is disabled and the message **There are no instances on this client system** is displayed.
- Make sure that the specified SQL Server instance exists on the target client. Otherwise, restore fails.

Select one of the following **Restore actions**:

- **Restore data**. Select to restore the whole database. This option is selected by default.
- **Restore and display file list only**. Select if you do not know the original filenames. In this case, the files backed up in a particular session are displayed.
- **Restore and display headers only**. Select if you need specific details about backup. SQL Server header information is displayed.

Figure 74 Restore options



5. In the **Devices** page, select the devices to be used for the restore.

   For more information of how to select devices for a restore, see the *HP Data Protector Help* index: "restore, selecting devices for".

6. Click **Restore MS SQL Server** and then **Next** to select **Report level** and **Network load**.

   Click **Finish** to start restore.

Restore options

Table 17 Microsoft SQL Server database restore options

Option	Description
Backup version	Specifies the backup session from which the selected objects will be restored.
Point-in-time restore	This option is only available for database objects. Specifies a point in time to which the database state will be restored (you also need to select **Backup version** and set **Stop at**). After recovery, the database is in the state it was at the specified date and time.

Table 17 Microsoft SQL Server database restore options *(continued)*

Option	Description
	Only transaction logs written before the specified date and time are applied to the database.
Stop at	This option is only available for database objects. Specifies the exact time when the rollforward of transactions will be stopped. Therefore, to enable database recovery to a particular point in time, backup you restore from must be a transaction log backup. You cannot use this option with **NORECOVERY** or **STANDBY**. If you specify **Stop at** time that is after the end of **RESTORE LOG** operation, the database is left in a non-recovered state (as if **RESTORE LOG** is run with **NORECOVERY**).
Restore only this backup	If you restored a database version and left it in a non-operational or standby state, you can subsequently restore differential or transaction log backups one by one, leaving each version non-operational to restore additional backups.
Full restore of the database	All necessary versions are restored, including the latest full backup, the latest differential backup (if one exists), and all transaction log backups from the last differential up to the selected version.
Force restore over the existing database	Select this option if a database with the same name but a different internal structure already exists at the target Microsoft SQL Server instance. If this option is not selected, the Microsoft SQL Server does not let you overwrite the existing database - the restore will fail. If you are restoring a data file from the PRIMARY group to an existing database, you must specify the option at the data file level. When using this option, make sure that the most recent logs are backed up before the restore.
Put database in single user mode - log off all users	Disconnects all users that are connected to the target Microsoft SQL Server database and puts the database in the single user mode. Note that if the database is not in the simple recovery mode, the **Force restore over the existing database** option should also be selected.
Recovery completion state	Enables selecting the database state after recovery. You may select from: • Leaving the database operational. Once the last transaction log is restored and the recovery completed, the database becomes operational. • Leaving the database non-operational after the last transaction log is restored. You may restore additional transaction logs one by one. • Leaving the database in read-only mode. You may restore additional transaction logs before the database is set to read-write mode. This selection is only available for database objects.
Restore database with a new name	This option is only available for database objects. Restores the database under a different name. Specify the database logical filename and the destination filename (suboptions of **Restore files to new locations**).
Restore files to new locations	Restores files to a new location. Specify the database logical filename and a destination target filename for the specified logical filename. Use this option to restore data to a different client, a different instance, or to make a database copy on the same client.

TIP: To allow different restore scenarios, you can combine general restore options, such as **Restore database to another Microsoft SQL Server** and **Restore using a different device**, with object-specific restore options, such as **Point-in-time restore**, **Recovery completion state**, **Force restore over the existing database**.

Restoring to a different SQL Server instance or/and different SQL Server

Prerequisites

- Both SQL Servers must have the same local settings (code page and sort order). This information is displayed in the session monitor for each backup.
- The target SQL Server must be configured and reside in the same Data Protector cell as the original SQL Server. For the configuration procedure, see "Creating ZDB specifications" (page 163).

Procedure

1. Select the databases you want to restore and their versions.
2. Select the following:
   - To restore to a different SQL Server client, select **Restore to another client** and the target client from the drop-down list.
   - To restore to a different SQL Server instance, select **Restore to another instance**. If there are no instances in the drop-down list, enter the instance name by yourself.

   IMPORTANT: Make sure that the specified SQL Server instance exists on the target client. Otherwise, restore fails.
3. Specify new database locations.
4. Start restore. See "Restore" (page 169).

Instant recovery

See the *HP Data Protector Zero Downtime Backup Concepts Guide* and *HP Data Protector Zero Downtime Backup Administrator's Guide* for general information on instant recovery.

Prerequisites

- If you restore user databases, put the databases offline:
  1. Start SQL Server Enterprise Manager.
  2. Selecting the database and click **Action**.
  3. Select all tasks and take them offline.
- If you restore system databases, put SQL Server offline by starting SQL Server Enterprise Manager, right-clicking SQL Server, and clicking **Stop**.

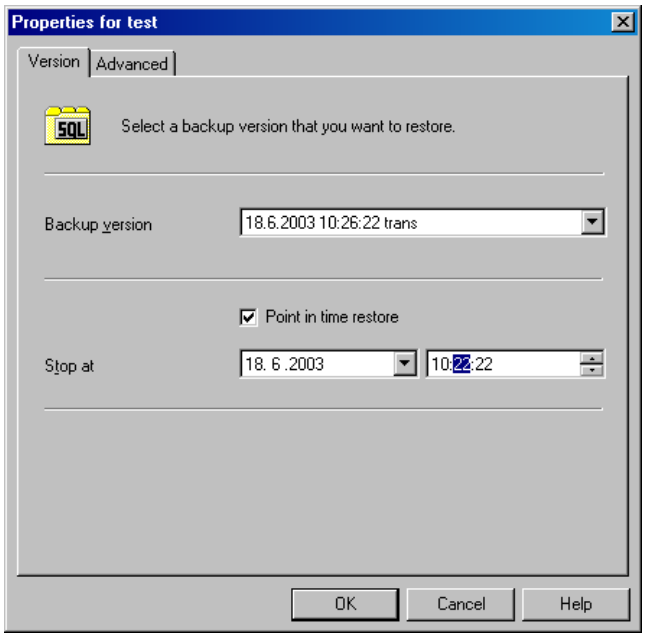
Perform instant recovery using the Data Protector Manager:

1. In the Context List, click **Instant Recovery**.
2. Expand **MS SQL Server** and select the backup session (replica) from which you want to restore. By default, the database will be recovered until the last backed up transaction.

3. To recover user databases to a specific point in time:
   a. In the **Source** property page, under **Restore Objects**, right-click a database and click **Properties**.
   b. In the **Backup version** drop-down list, select the required replica. The latest version is selected by default.

      Select **Point in time restore**. From the **Stop at** drop-down list, select the point in time to which the transactions should be applied, and click **OK**. If no transaction logs are available, this option is disabled.

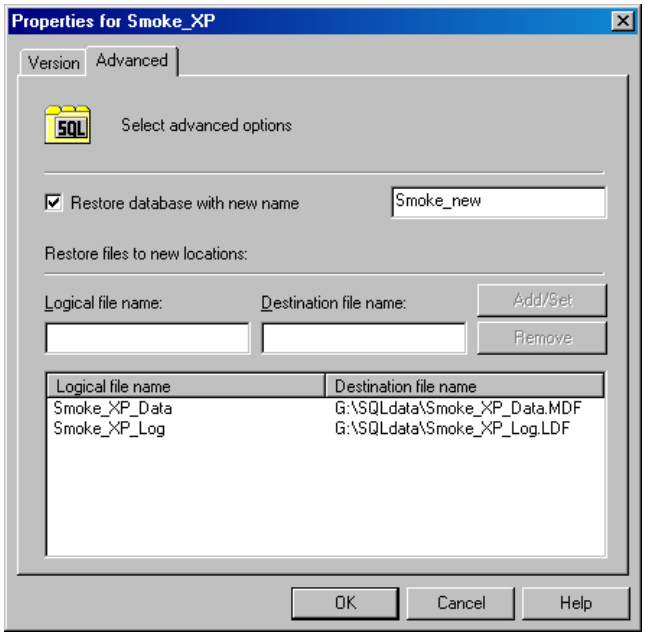
Figure 75 Point-in-Time restore



To restore the database under a different name, click **Advanced** and select **Restore database with new name**. See "Restoring database with a new name" (page 175).

IMPORTANT: If the logical filename and physical filename are not listed, add them to the list. Specify the same names as used for ZDB; otherwise, instant recovery fails.

Figure 76 Restoring database with a new name



4. Click **Restore MS SQL Server**.

   If you restore system databases, SQL Server displays errors because its services are offline. Therefore, when restore completes, start SQL Server manually using SQL Server Enterprise Manager.

Monitoring sessions

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

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

For information on monitoring sessions, see the *HP Data Protector Help* index: "viewing currently running sessions" and "viewing finished sessions".

Troubleshooting

This section lists general checks and verifications, plus problems you might encounter when using the Data Protector SQL Server integration. Start at "Problems" (page 176). If you cannot find a solution there, perform general checks and verifications.

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

For general ZDB, restore, and instant recovery related troubleshooting, see the *HP Data Protector Zero Downtime Backup Administrator's Guide*.

Before you begin

- Make sure that the latest official Data Protector patches are installed. For details of how to verify this, see the *HP Data Protector Help* index: "patches".
- 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://support.openview.hp.com/selfsolve/manuals for an up-to-date list of supported versions, platforms, and other information.

Checks and verifications

If your configuration, backup, or restore failed:

- Check that SQL Server services are running.
- Examine system errors reported in *Data_Protector_program_data*\log\debug.log on the SQL Server client.

  Additionally, check errorlog and VDI.log files in the *MSSQL*\log directory.
- Make a test filesystem backup and restore of the problematic client. For information, see the *HP Data Protector Help*.
- Check that every SQL Server used with Data Protector has the MS SQL Integration component installed.
- Connect to SQL Server via SQL Server Enterprise Manager using the same login ID as you specified in the Data Protector **Configuration** dialog box.
- Perform a database backup using SQL Server Enterprise Manager. If the backup fails, fix any SQL Server problems, and then perform a backup using Data Protector.

Additionally, if your backup failed:

- Verify the configuration file to check if the Cell Manager is correctly set on SQL Server.
- If you do not see the SQL Server instance as the application database when creating a backup specification, enter the instance name yourself. When “not-named instance” is not displayed, insert the DEFAULT string.
- If Data Protector reports that the integration is properly configured, verify that the SQL Server user has appropriate rights to access the required databases.

During master database restore, the following error occurs when executing an SQL statement:

```
Error has occurred while executing an SQL statement.
Error message: 'SQLSTATE:[42000] CODE:(3108) MESSAGE:[Microsoft]
[ODBC SQL Server Driver][SQL Server]To restore the master database,
the server must be running in single user mode. For information on
starting in single user mode, see "How to: Start an Instance of SQL
Server (sqlservr.exe)" in Books Online.
```

Note that this behavior is expected when the master database is not restored in single user mode.

Problems

Problem

The integration is properly configured but the database backup fails after a timeout

- With an error similar to:

  ```
  [Warning] From: OB2BAR@computer.company.com "SQLSRV"
  Time: 7/29/2011 8:19:22 PM
  Error has occurred while executing SQL statement.
  [Microsoft][ODBC SQL Server Driver][SQL Server]Backup or restore
  operation terminating abnormally.'
  [Critical] From: OB2BAR@computer.company.com "SQLSRV"
  Time: 7/29/11 8:19:24 PM
  Received ABORT request from SM => aborting
  ```

- SQL Server error log contains an entry similar to:

  ```
  2011-07-29 20:19:21.62 kernel
  BackupVirtualDeviceSet::Initialize: Open failure on backup
  ```

```
device 'Data_Protector_master'.
Operating system error -2147024891(Access is denied.).
```

- SQL Server `VDI.LOG` file contains an entry similar to:

```
2011/07/30 13:19:31 pid(2112)
Error at BuildSecurityAttributes: SetSecurityDescriptorDacl
Status Code: 1338, x53A Explanation: The security descriptor
structure is invalid.
```

SQL Server service and `Data Protector Inet` are running under different accounts. The integration cannot access SQL Server due to security problems.

Action

Restart the `Data Protector Inet` service under the same account as the SQL Server service is running.

Problem

Backup fails with "The object was not open"

When backing up Microsoft SQL Server databases, the session fails with an error similar to the following:

```
[Critical]From : OB2BAR_Main@wemaoldb2dr "Aolins" Time:11/12/2011
02:01:34 AM Microsoft SQL Server reported the following error during
login : The object was not open
```

The error may appear if the SQL Server Browser service is not running.

Action

Proceed as follows:

1. Start the SQL Server Browser service.
2. Start a new backup session.

Problem

Backup fails if the appropriate drive letter on the backup system does not exist

Backup fails with an error, similar to:

```
[Major] From: SSEA@computer1.com ""  Time: 02-Feb-11 14:07:54
 Filesystem \\.\Volume{ef58fe0e-b2b8-11db-aa08-000802804af6} could not be mounted
 to Q:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\DATA\.
 ([87] The parameter is incorrect. ).
```

Backup fails because SSE agent tries to mount the filesystem to the drive letter which does not exist on the backup system. The drive letter must be the same as on the application system. SSE or SMI-S agents always mount the filesystems to the same drive letters on the backup systems as if the `ZDB_PRESERVE_MOUNTPOINTS` `omnirc` option is set to `1`.

Action

For source volumes to be successfully replicated, create the same drive letters on the backup system as they are used on the application system for mounting the source volumes.

Problem

Database is left in unrecovered state after "Invalid value specified for STOPAT parameter" is reported

The database remains in an unrecovered state as if the `RESTORE LOG` operation was run with **Leave the database non-operational**.

Action

Recover the database to the latest point in time using SQL Query Analyzer:

`RESTORE DATABASE database_name WITH RECOVERY`

After the recovery, additional transaction logs cannot be applied.

Problem

Transaction logs cannot be restored from tape

The recovery completed successfully and the database was put in `norecovery` state, but transaction logs cannot be restored from tape.

Action

Recover the database to the state of ZDB to disk using the SQL Query Analyzer:

`RESTORE DATABASE database name WITH RECOVERY`

After the recovery, additional transaction logs cannot be applied.

Problem

Instant recovery of SQL Server databases fails

If the SQL Server service is offline prior to the instant recovery, instant recovery of the SQL Server databases fails.

The following errors are displayed:

```
[Critical] From: computer@company.com "(DEFAULT)" Time: 4/9/2011 7:01:42 PM
Microsoft SQL Server reported the following error during login:
The object was not open.
[Warning] From: computer@company.com "(DEFAULT)" Time: 4/9/2011 7:01:42 PM [152:9208] Data Protector is probably
 not configured for use with SQL Server on this host.
```

Action

Perform one of the following:

- Set the Data Protector `omnirc` option `OB2_SQLRESTORE_STARTSRV`, which starts the SQL Server service prior to the recovery of SQL databases, to `1`.

  During the master database restore, the following error is displayed:

  `RESTORE master with SNAPSHOT is not supported.`

  Note that this behavior is expected. No further steps are needed after the instant recovery.
- Restart SQL Server instance services after instant recovery completes. If restarting services does not automatically start the recovery of all system databases, start the SQL Server instance in single user mode and manually start the recovery of the master database. Follow the same procedure for other system databases. At the end, restart SQL Server instance services.

Problem

Restore to another client in the Data Protector cell not configured for use with SQL Server fails

Action

Configure the SQL integration on this client (see "Configuring the integration" (page 157)).

Problem

Database is left in unrecovered state after restore completed successfully

If you set the time for `Stop at` beyond the end of the `RESTORE LOG` operation, the database remains in the unrecovered state as if the `RESTORE LOG` operation was run with `Leave the database non-operational`.

Action

Recover the database to the latest point in time by using the SQL Query Analyzer:

`RESTORE DATABASE database_name WITH RECOVERY`

After the recovery, additional transaction logs cannot be applied.

Problem

Instant recovery of a Microsoft SQL Server database configured on a Microsoft Cluster Server system fails with "The physical filename may be incorrect"

Instant recovery of the Microsoft SQL Server data in an HP Business Copy P9000 XP configuration on a Microsoft Cluster Server system fails with the following error:

```
[Microsoft][ODBC SQL Server Driver][SQL Server]Device activation error.
The physical file name '<Data/Log filename>' may be incorrect.
```

Action

Perform the following steps:

1. Using Microsoft SQL Server Enterprise Manager, detach the Microsoft SQL Server database that you want to recover.
2. Using Cluster Administrator, take the Microsoft SQL Server Disk resource offline.
3. On the application system, configure the `ZDB_TAKE_CLUSRES_ONLINE` `omnirc` option.

   For details, see "ZDB integrations omnirc options" (page 254).
4. Start instant recovery.
5. When the message `Please, take MS SQL cluster resources online` appears in the Data Protector GUI, bring the Microsoft SQL Server cluster resources online using Cluster Administrator.

Problem

Restoring a Microsoft SQL Server 2005 instance to an alternate location when full-text indexing is enabled fails

When the Use full-text indexing option is enabled for a particular database in a Microsoft SQL Server 2005 instance, the restore session does not complete successfully, since restore of the full-text catalog of the SQL database fails. The session report contains warning messages about the full-text catalog file being used by the affected database.

Action

To solve the problem:

1. In the HP Data Protector Manager, switch to the **Restore** context.
2. In the Scoping Pane, expand **Restore Objects** and then **MS SQL Server**. Select name of the Microsoft SQL Server for which you want to perform restore.
3. In the Results Area, double-click the bar name corresponding to the particular Microsoft SQL Server instance. A list of backed up objects gets displayed.
4. Select the desired Microsoft SQL Server database, right-click it, and click **Properties**.
5. In the Properties window, click the **Advanced** tab.
6. Select the **Restore database with new name** option, and enter the new database name in the text box.
7. For all logical file names that are already present on the list, update contents of the Destination file name column accordingly.
8. Add the full-text catalog to the list.

   In the Logical file name text box, enter the string `sysft_Full-Text_Catalog_Name`. In the Destination file name text box, enter the corresponding physical location.

   NOTE: The full-text catalog is always restored to its original location, regardless of the specified physical location.

9. Click **Add/Set**.
10. In the Version and Options property pages, specify the appropriate options. For details, see "Standard restore" (page 169).
11. Click **OK** to close the Properties window.
12. In the Options, Devices, and Media property pages, specify the appropriate options. For details, see "Standard restore" (page 169).
13. Click **Restore** and then **Next** to select the Report level and Network load.
14. Click **Finish** to start the restore session.

Problem

Database restore fails

The restore session aborts with a major error similar to:

```
Error has occurred while executing a SQL statement.Error message:
'SQLSTATE:[42000] CODE:(3159) MESSAGE:[Microsoft][ODBC SQL Server
Driver][SQL Server]The tail of the log for the database "test2" has not
been backed up. Use BACKUP LOG WITH NORECOVERY to backup the log if it
contains work you do not want to lose. Use the WITH REPLACE or WITH
STOPAT clause of the RESTORE statement to just overwrite the contents
of the log. SQLSTATE:[42000] CODE:(3013) MESSAGE:[Microsoft][ODBC SQL
Server Driver][SQL Server]RESTORE DATABASE is terminating abnormally.
```

Action

To solve the problem perform a transaction log backup to obtain the most recent transaction logs.

4 Data Protector Microsoft Exchange Server 2010 ZDB integration

Introduction

This chapter explains how to configure and use the Data Protector Microsoft Exchange Server 2010 ZDB integration, where Data Protector integrates with Microsoft Exchange Server 2010 or Microsoft Exchange Server 2013 (hereinafter, both Exchange Servers are called **Microsoft Exchange Server**, unless differences are pointed out). It describes concepts and methods you need to understand to back up and restore Microsoft Exchange Server 2010 mailbox and public folder databases or Microsoft Exchange Server 2013 mailbox databases (**databases**).

Both standalone environments and Database Availability Group (**DAG**) environments are supported.

The Data Protector Microsoft Exchange Server 2010 integration is based on the Volume Shadow Copy Service (**VSS**) technology. For details on VSS concepts, see the *HP Data Protector Integration Guide for Microsoft Volume Shadow Copy Service*.

Backup

During backup, databases can be used actively (**online backup**). In DAG environments, you can back up active and/or passive database copies.

As Microsoft Exchange Server, ZDB disk array, and VSS are involved, you can specify different kinds of backup types:

- Microsoft Exchange Server backup types
- VSS backup types
- ZDB backup types

You can select among the following Microsoft Exchange Server backup types:

- Full
- Copy
- Incremental
- Differential

You can select among the following ZDB backup types:

- ZDB-to-disk
- ZDB-to-disk+tape
- ZDB-to-tape

You can select among the following VSS backup types:

- Local or network backup
- VSS transportable

For details on the backup types, see "Backup types" (page 186).

Restore

You can restore Microsoft Exchange Server databases using standard restore or instant recovery.

During restore, each database can be restored using a different restore method. The following methods are available:

- Repair all passive copies with failed status
- Restore to the latest state

- Restore to a point in time
- Restore to a new mailbox database
- Restore files to a temporary location

This chapter provides information specific to the Microsoft Exchange Server 2010 integration. For additional limitations, see the *HP Data Protector Product Announcements, Software Notes, and References*. For general Data Protector procedures and options, see the *HP Data Protector Help*.

Integration concepts

Data Protector integrates with Microsoft Exchange Server through the Data Protector Microsoft Exchange Server integration agent, which channels communication between the Data Protector Session Manager and the clients in the Microsoft Exchange Server environment. The agent communicates with Microsoft Exchange Server through the Microsoft Exchange Management Shell and uses VSS to back up data.

Supported environments

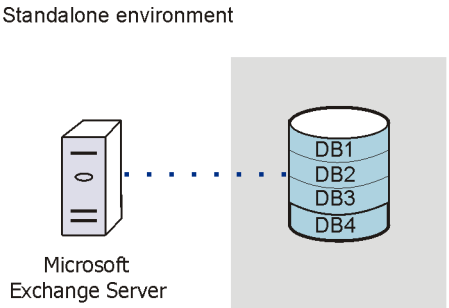
Data Protector supports Microsoft Exchange Server Database Availability Group environments (**DAG environments**) as well as environments with standalone Microsoft Exchange Server systems (**standalone environments**).

Standalone environments

In a standalone Microsoft Exchange Server environment, each Microsoft Exchange Server system stands on its own.

In one session, you can back up databases from only one Microsoft Exchange Server system. Data Protector sends backup and restore requests directly to the Microsoft Exchange Server system.

Figure 77 Standalone environment (example)

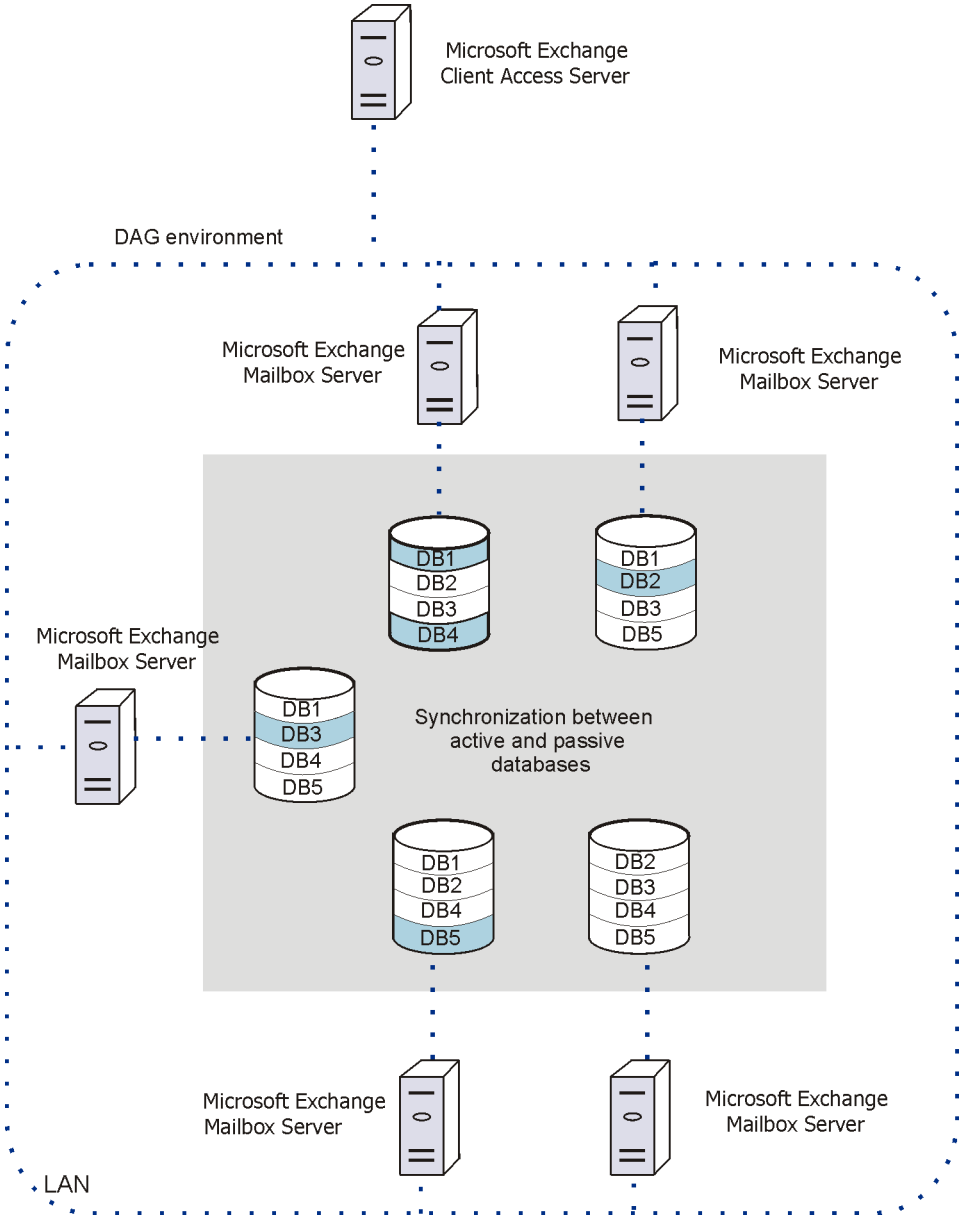


DAG environments

In a DAG environment, Data Protector communicates with the DAG using one of the Microsoft Exchange Server systems (the one that is currently active in the environment). All backup and restore requests are sent there.

In one session, you can back up active and/or passive database copies from different Microsoft Exchange Server systems that belong to the same DAG.

Figure 78 DAG environment (example)



In Figure 78 (page 183), active databases are shaded in blue.

If a database has multiple passive copies, you can specify which particular passive copy you want to back up, using one of the following backup policies:

- minimize the number of hosts
- lowest activation preference
- highest activation preference
- shortest replay lag time
- longest replay lag time
- longest truncation lag time

You can also specify from which Microsoft Exchange Server systems database copies should not be backed up.

For a brief description of the activation preference number, replay lag time, and the truncation lag time, see " Microsoft Exchange Server parameters in DAG environments" (page 184).

Table 18 Microsoft Exchange Server parameters in DAG environments

Parameter	Description
Activation preference number	The activation preference number determines which passive copy is activated if multiple passive copies meet the same criteria; the copy assigned the lowest activation preference number is activated.
Replay lag time	The `ReplayLagTime` parameter plays a role when synchronizing a passive copy with the active copy. As soon as a log file at the active copy side is filled up, it is copied to the passive copy side. By default, the newly copied log is also applied to the passive copy database files. However, if the passive copy `ReplayLagTime` parameter is set to a value greater than `0`, the log is applied with a lag, creating a lagged database copy. The maximum value is `14` days.
Truncation lag time	The `TruncationLagTime` parameter specifies how long the Microsoft Exchange Replication service waits before truncating log files that have already been applied to the database files. The maximum value is `14` days.

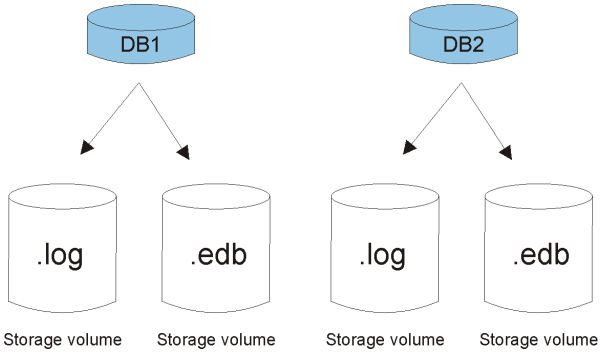
Configuring the integration

Prerequisites

- Ensure that you have correctly installed and configured the Microsoft Exchange Server environment.
  - For supported versions, platforms, devices, and other information, see the latest support matrices at http://support.openview.hp.com/selfsolve/manuals.
  - For information on installing, configuring, and using Microsoft Exchange Server, see the Microsoft Exchange Server documentation.
  - In the Microsoft Exchange Server 2010 environment, if you intend to use the restore method **Restore to a point in time**, make sure that you have the Microsoft Exchange Server 2010 SP1 installed.
- If you intend to run Incremental and Differential backup sessions, make sure that circular logging is disabled.
- If you plan to run instant recovery sessions, it is advisable to keep Microsoft Exchange Server databases on separate storage volumes. Also, keep a database's files (`.edb` and `.log`) on separate storage volumes. See Figure 79 (page 184). Such a configuration provides better restore granularity.

  Ensure that storage volumes on different Microsoft Exchange Server systems are the same size. Otherwise, you may experience problems during copy-backup instant recovery sessions.

Figure 79 Where to keep database files



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

  Ensure that the following Data Protector components are installed on all Microsoft Exchange Server systems:

  - `MS Exchange Server 2010/2013 2010+ Integration`
  - `MS Volume Shadow Copy Integration`
  - The appropriate Data Protector disk array agent

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

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

- For limitations, see "Limitations and recommendations" in the *HP Data Protector Product Announcements, Software Notes, and References*.

Limitations

- Due to incompatibility between Microsoft Exchange Server versions, backup objects belonging to a particular Exchange Server version cannot be restored to Data Protector clients on which a different Exchange Server version is installed.

Before you begin

- Configure devices and media for use with Data Protector.
- To test whether a Microsoft Exchange Server system and the Cell Manager communicate properly, configure and run a Data Protector filesystem backup and restore on every Microsoft Exchange Server client in your environment.

Configuring user accounts

Windows domain user account for backup and restore sessions

Backup and restore sessions are started by the `Data Protector Inet` service, which by default runs under the Windows local user account `SYSTEM`. Consequently, a backup or restore session is performed using the same user account.

However, you can specify that the `Data Protector Inet` service should use a different Windows domain user account to start a session:

- To perform a backup session under a different user account, specify the **Specify OS user** option (see "Specifying view type" (page 191)) when creating a backup specification.
- To perform a restore session under a different user account, specify the **User name** and **Group/Domain name** options in the Options page (when performing standard restore, see "Restore options" (page 210)) or Advanced page (when performing instant recovery, see "Instant recovery – advanced" (page 219)).

Before you specify a different Windows domain user account, configure the user account as follows:

1. Grant the user appropriate permissions to back up and restore Microsoft Exchange Server databases.
2. Add the user to the Data Protector `admin` or `operator` user group. For details on adding users, see the *HP Data Protector Help* index: "adding users".

3. Save the user and its password to a Windows Registry on the Microsoft Exchange Server system on which you plan to start the integration agent (`e2010_bar.exe`). To save the user account, use the Data Protector `omniinetpasswd` or `omnicc` command.

   NOTE: The user account saved in the Windows Registry will be used by the `Data Protector Inet` service when needed.

   For details on setting accounts for the Inet service user impersonation, see the *HP Data Protector Help* index: "Inet user impersonation".

   Example

   To save the user `jane` from the domain `HP` and with the password `mysecret` to a Windows Registry, log on to the Microsoft Exchange Server system and execute the following command:

   ```
   omniinetpasswd -add jane@HP mysecret
   ```

User account for executing Exchange Management cmdlet operations

In the Microsoft Exchange Server 2013 environment, you need user credentials with specific Exchange Management Roles assigned to create a remote runspace for executing the Exchange Management cmdlet operations remotely. These operations are executed as part of Microsoft Exchange Server backup and restore operations.

Configure a valid Exchange domain user account, when creating a backup specification. The user account is saved in the user credentials specific configuration file located in the `Data_Protector_program_data\Config\Server\Integ\Config\E2010` directory and named by the domain name. The saved user credentials will be used by Data Protector when needed.

For details, see "Specifying view type" (page 191).

For information on the Exchange Management cmdlet operations, see the Microsoft Exchange Server documentation.

Backup

When you back up a Microsoft Exchange Server database, the following files are automatically backed up:

- database files (`.edb`)
- transaction logs (`.log`)
- checkpoint files (`.chk`)

However, depending on the Microsoft Exchange Server backup type you select, not all files are always backed up. For details, see "Microsoft Exchange Server backup types" (page 186).

Backup types

As Microsoft Exchange Server, ZDB disk array, and VSS are involved, you can specify different kinds of backup types:

- Microsoft Exchange Server backup types
- ZDB backup types
- VSS backup types

Microsoft Exchange Server backup types

You can select among the following Microsoft Exchange Server backup types:

Table 19 Backup types

Full	Backs up the database files (`.edb`), transaction logs (`.log`), and checkpoint files (`.chk`), and then truncates the transaction logs. ***DAG environments:*** If multiple copies of a database are selected for backup, Data Protector first performs a Full backup of the passive copy that has the fewest logs applied to the database file, and then performs a Copy backup of all the remaining copies, with the active copy being backed up last. The copies are backed up sequentially due to a Microsoft Exchange Server VSS writers limitation.
Copy	Backs up the database files (`.edb`), transaction logs (`.log`), and checkpoint files (`.chk`), without truncating the transaction logs.
Incremental	Backs up the transaction logs (`.log`) that have been created since the last Full or Incremental backup, and then truncates the transaction logs. *DAG environments:* If multiple copies of a database are selected for backup, Data Protector backs up the transaction logs of only one copy (one of the passive copies is selected).
Differential	Backs up the transaction logs (`.log`) that have been created since the last Full backup, without truncating the transaction logs.

NOTE:
An incremental or differential backup of a database cannot be performed:

- If a full backup has not been performed.
- If an incremental backup is started just after a differential backup has been performed, or the other way around.
- If Microsoft Exchange Server circular logging is enabled.

ZDB backup types

You can select among the following ZDB backup types:

- ZDB-to-disk
- ZDB-to-disk+tape
- ZDB-to-tape

NOTE: For Microsoft Exchange Server Incremental and Differential backup types, only the ZDB-to-tape backup type is available.

VSS backup types

You can select among the following VSS backup types:

- Local or network backup
- VSS transportable

For details, see the *HP Data Protector Integration Guide for Microsoft Volume Shadow Copy Service*.

Backup parallelism

- During a backup session, copies of different databases are backed up in parallel, however, copies of the same database are not, due to a Microsoft Exchange Server VSS writers limitation.
- If multiple backup sessions that intend to back up the same database are started in parallel, only the session that first locks the database can back up the database; the other sessions cannot. In DAG environments, this also applies if backup sessions intend to back up different copies of the same database; only the session that first locks the database (that is, all its copies) can back up the database copies; the other sessions cannot.

NOTE: This behavior ensures that the construction of a restore chain is valid. For example, suppose that several Full backup sessions that intend to back up the same database are started in parallel. If all the sessions backed up the database, it might happen that the session given the latest SessionID is not the one that backed up the database last. For details on restore chains, see "Restore chain" (page 203).

Replica rotation in DAG environments

Data Protector Microsoft Exchange Server 2010 integration enables you to perform ZDB sessions in multi-system environments (DAG environments). This brings some changes to the existing replica rotation functionality.

In standalone environments, the replica rotation functionality works as it used to; it limits the number of backups that are kept in the Data Protector IDB database for instant recovery purposes. For example, if the **Number of replicas rotated** option is set to `1`, only one backup session is available for instant recovery at a time. If you start another backup session (with the same backup specification), backup storage volumes created in the previous backup session are deleted before new ones are created and the previous session is removed from the Instant Recovery context.

In DAG environments, a database can be backed up from different systems in different sessions. This introduces the changes. For example, you want to back up the database `DB1`, which is active on `node1.company.com`, and the database `DB2`, which is active on `node2.company.com`. Suppose the **Number of replicas rotated** option is set to `1` and your backup policy is such that the active copy is always backed up. After the backup, the Data Protector VSSDB database contains the following entries:

Backup 1 (`2013/10/05-1`):

- `2013/10/05-1:node1.company.com` (containing `DB1`)
- `2013/10/05-1:node2.company.com` (containing `DB2`)

Suppose that a failover occurs and the database `DB1` becomes active on `node2.company.com`. You start another backup session. Now both databases are backed up from `node2.company.com`. As a result, the VSSDB database contains the following entries:

Backup 2 (`2013/10/05-2`):

- `2013/10/05-1:node1.company.com` (containing `DB1`)
- `2013/10/05-2:node2.company.com` (containing `DB1` and `DB2`)

The entry `2013/10/05-1:node2.company.com` is no longer in the VSSDB database as it has been rotated out (the corresponding backup storage volumes have been deleted) due to the replica rotation functionality.

NOTE: Entries are rotated per system and not per session. As a result, entries that are created in the same session can be rotated out at different points in time (that is, in different sessions).

Now another failover occurs and both databases become active on `node1.company.com`. You start another session and both databases are backed up from `node1.company.com`. As a result, the VSSDB database contains the following entries:

Backup 3 (`2013/10/05-3`):

- `2013/10/05-3:node1.company.com` (containing `DB1` and `DB2`)
- `2013/10/05-2:node2.company.com` (containing `DB1` and `DB2`)

Note that the entry `2013/10/05-1:node1.company.com` has been rotated out as well. Since both parts created in the session `2013/10/05-1` have been rotated out, the session `2013/10/05-1` can no longer be used for instant recovery (it is removed from the Instant Recovery context).

If you go to the Instant Recovery context and select the session created in Backup 1 after you have performed Backup 2, the source page incorrectly shows that both databases can be restored. The entry `2013/10/05-1:node2.company.com` (containing `DB2`) has been rotated out in Backup 2. If you select `DB2` for restore and start instant recovery, the session fails. Therefore, make sure to restore databases from sessions for which the necessary entries in the VSSDB database still exist.

Backup considerations

- *Backup strategy:*

  Choose one of the following strategies to back up your data:

  - Full
  - Full, Incremental, Incremental, ...
  - Full, Differential, Differential, ...
  - Full, Copy, Incremental, ..., Copy, Incremental, ...

IMPORTANT: An Incremental backup session cannot be followed by a Differential backup session, nor the other way around. You must first run a Full backup session.

- *Active copies as opposed to passive copies:*

  There is no difference between the active and passive copy, except in the currently active log file (at the active copy side), which is not copied to the passive copy side until the file is filled up (that is, reaches 1 MB). Consequently, if you back up a passive copy, the transactions in the currently active log file are not included.

- *Lagged database copies:*

  Backing up a lagged database copy is equivalent to backing up a non-lagged database copy. If you restore from the backup of a lagged database copy, files are not only restored, but logs are also applied to the database file, returning the database to its most recent state. However, restoring the logs and applying them to the database file is time-consuming and, therefore prolongs the restore session. Also note that you need enough disk space to restore all the necessary logs.

  On the other hand, restoring from the backup of a lagged database copy enables you to restore the database to a point in time before the backup was taken. Restore the database without performing database recovery and mounting. Then remove unwanted logs, and finally recover and mount the database.

- *Public folders*:

  In the Microsoft Exchange Server 2010 environment, backup of Microsoft Exchange Server public folders with activated replication is not supported.

- *Concurrent backup sessions:*

  Backup sessions that back up the same database cannot run in parallel.

Object operations considerations

- Object copy and object verification

  When copying or verifying Microsoft Exchange Server objects you need to select all Data Protector backup objects created in the same session. To make sure that you do not select only a few objects from the session, the Data Protector GUI does not list Microsoft Exchange Server backup objects for interactive object copy or object verification sessions in the Objects scope of the Object Operations context.

  Use the Session or the Media scope instead.

Creating backup specifications

Create a backup specification using the Data Protector GUI (**Data Protector Manager**).

1. In the Context List, click **Backup**.
2. In the Scoping Pane, expand **Backup Specifications**, right-click **MS Exchange 2010+ Server**, and click **Add Backup**.
3. In the Create New Backup dialog box, specify **Backup type** (VSS backup type). For details, press **F1**. Click **OK**.
4. In **Application system**, select the Microsoft Exchange Server system that you want to back up. In a DAG environment, select the DAG virtual system or a Microsoft Exchange Server system.

   NOTE: The **Application system** drop-down list contains all clients that have the Data Protector `MS Exchange Server 2010/2013 2010+ Integration` component installed. In a DAG environment, the list contains also the DAG virtual system (host).

   The backup session (that is, the integration agent `e2010_bar.exe`) will be started on the client that you specify here. If you select a DAG virtual system, the integration agent is started on the currently active Microsoft Exchange Server node. To find out which node is currently active, see "Tip" (page 224).

   NOTE: In the Microsoft Exchange Server 2010 environment, to back up public folders residing on a Microsoft Exchange Server system that is a part of a DAG environment, select the Microsoft Exchange Server system and not the DAG virtual system (host). If you select the DAG virtual system, you can back up only databases that belong to the DAG. The Microsoft Exchange Server public folders database is not the part of it.

   Depending on the VSS backup type you selected, specify the following:

   - If you selected **Local or network backup**, in **Provider**, select **Use hardware provider**.
   - If you selected **VSS transportable backup**, specify **Backup system**.

   Specify ZDB-specific options.

   For details, press **F1** or see the *HP Data Protector Integration Guide for Microsoft Volume Shadow Copy Service*.

   NOTE: In an HP P9000 XP Disk Array Family resync mode environment, the maximum number of replica storage volumes (S-VOL) that can be created for a given storage volume (P-VOL) is limited by the hardware provider configuration — MU range (maximum is 3). To enable performing of incremental and differential sessions, the **Number of replicas rotated** option in the backup specification must be set to one less than the MU range. Thus, one replica storage volume is kept free for incremental and differential backup sessions.

   Click **Next**.
5. If you selected the DAG virtual system (host), specify **View Type** to define how Microsoft Exchange Server databases should be organized in the next page (source page):

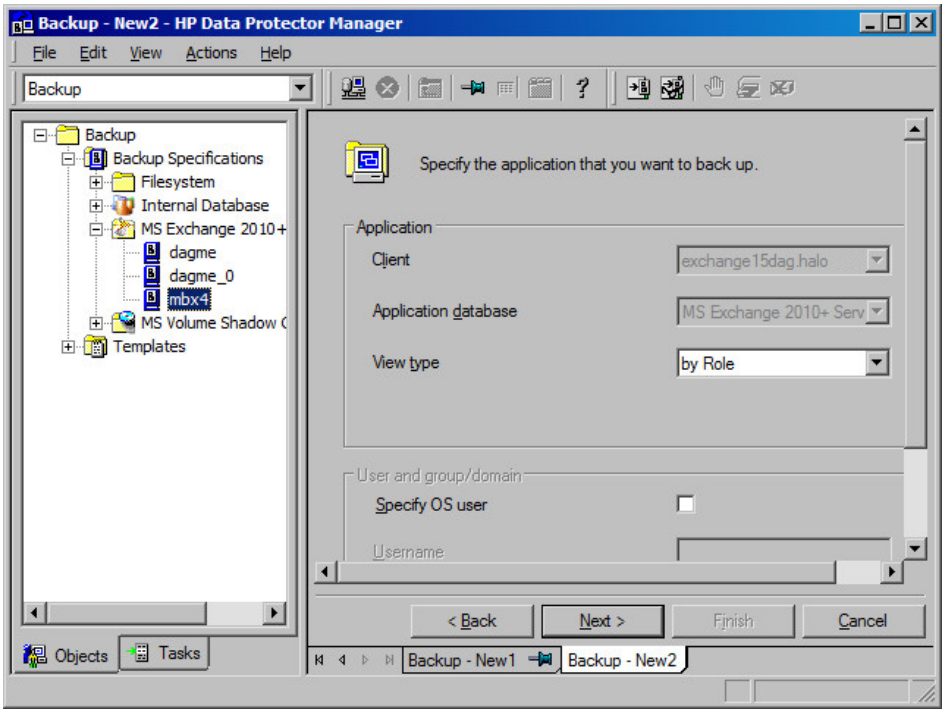
By Role

All databases in the DAG are displayed.

By Client

All clients in the DAG are displayed, together with all the databases (active or passive) residing on them. Active databases have the label `(active)` appended at the end. Passive databases have no label.

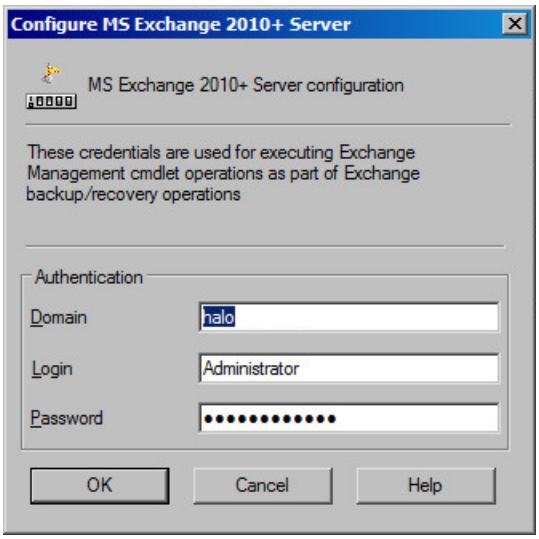
Figure 80 Specifying view type



For information on the **User and group/domain** options, press **F1**.

NOTE: If no valid user credentials for executing the Exchange Management cmdlet operations remotely are specified, the Microsoft Exchange Server configuration dialog box is displayed. Enter the required user credentials and click **OK**.

Figure 81 User credentials for executing Exchange Management cmdlet operations



Click **Next**.

6. Select which Microsoft Exchange Server databases to back up.

NOTE: ***DAG environments:***

In a single session, you can back up one of the following:

- multiple databases, but only one copy of each
- a single database, but multiple copies of it

Figure 82 Selecting databases (DAG environment – by role)

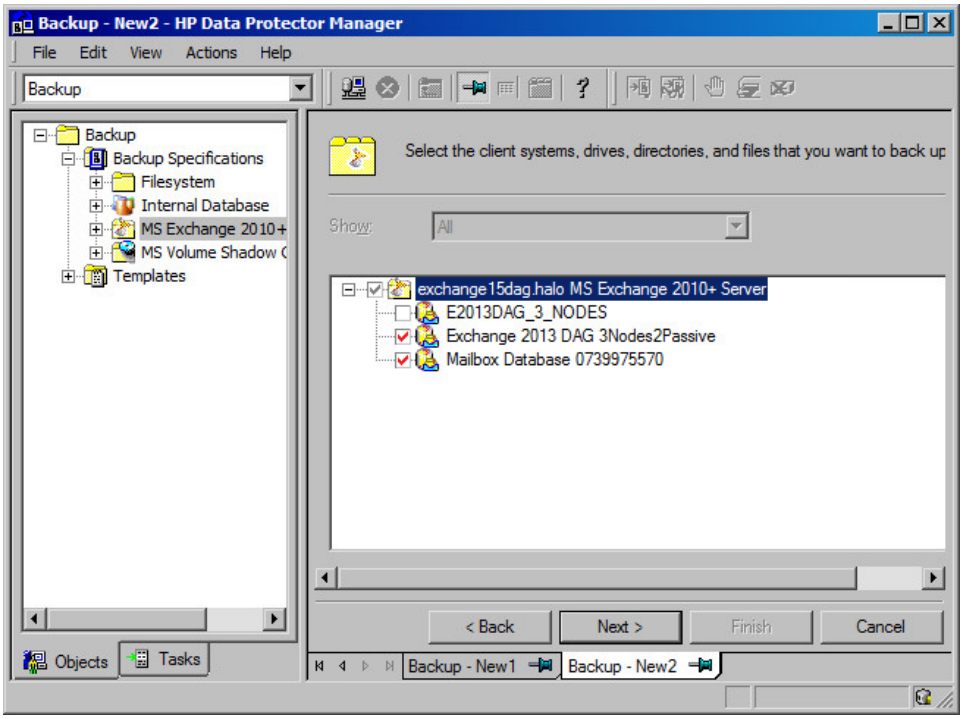


Figure 83 Selecting databases (DAG environment – by client)

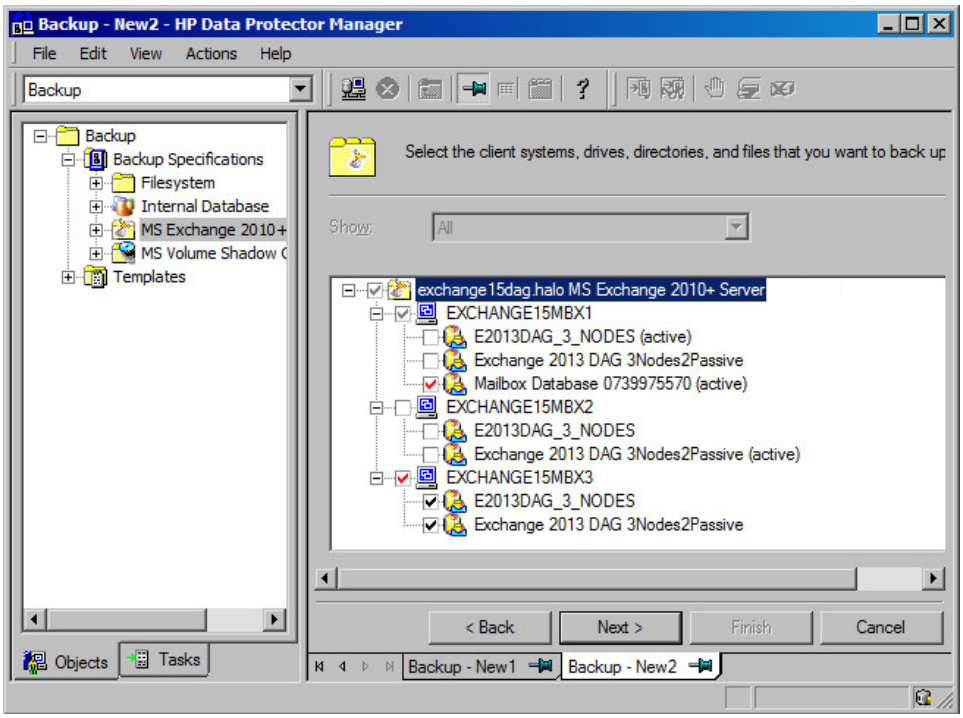
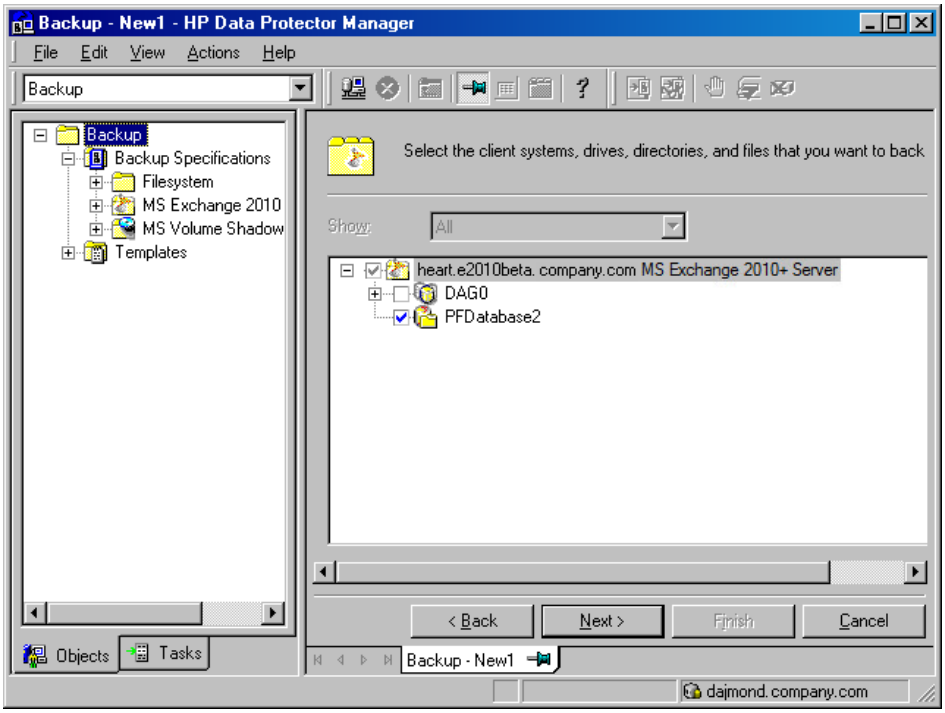
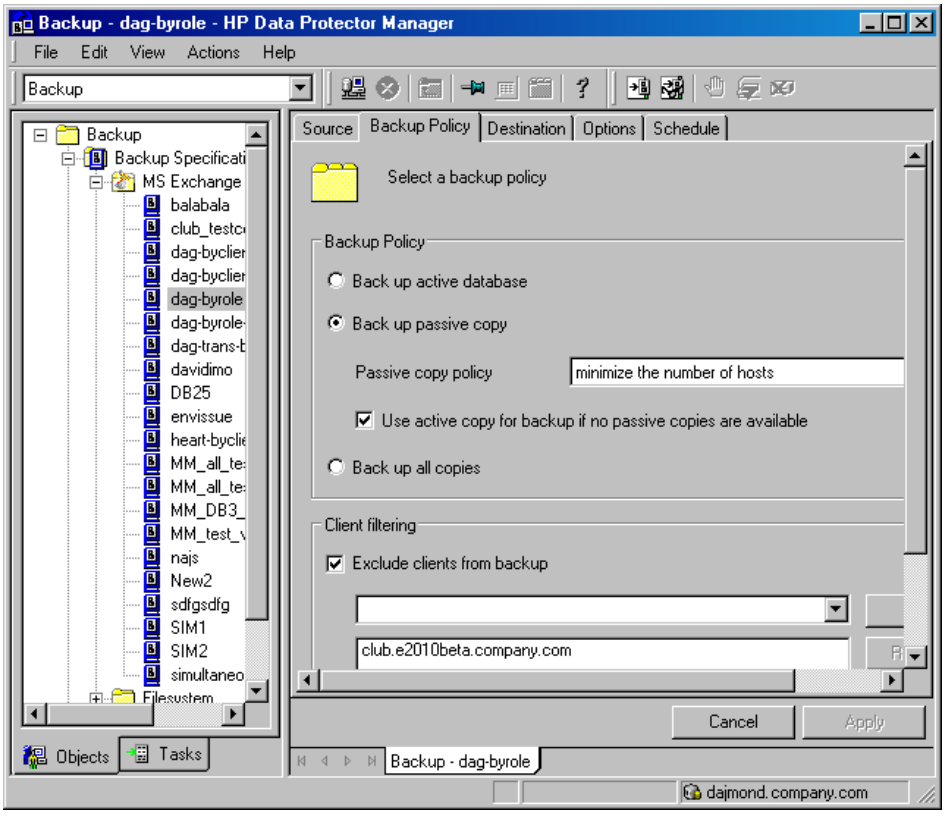


Figure 84 Selecting databases (standalone environment)



7. The following applies in DAG environments if you selected the **By Role** view type. Specify the backup policy options.

Figure 85 Backup policy options



For details, see "Backup policy options" (page 194).

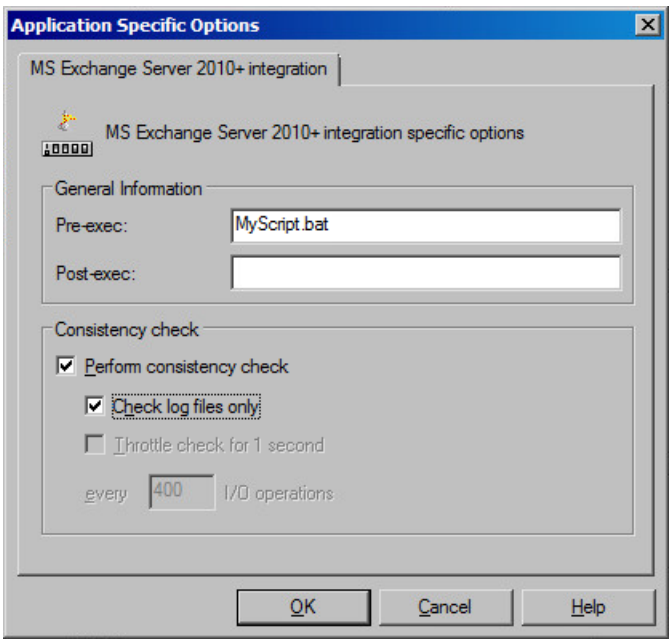
8. Select which devices to use for the backup.

   To specify device options, right-click the device and click **Properties**. Specify the number of parallel backup streams in the **Concurrency** tab and which media pool to use.

   Click **Next**.

9. Set backup options.

Figure 86 Application-specific option



   For information on application-specific backup options, see "Application-specific backup options" (page 195).

   Click **Next**.

10. Optionally, schedule the backup. See "Scheduling backup sessions" (page 196).

    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 197).

Table 20 Backup policy options

Options	Description	
Back up active database	If this option is selected, the active copy is backed up.	
Back up passive copy	If this option is selected, a passive copy is backed up. If a database has multiple passive copies, specify which particular copy you want to back up, using one of the following policies:	
	minimize the number of hosts (default)	If this option is selected, the minimum number of clients is involved in the backup. For example, if databases to be backed up have each a passive copy residing on the same client, they are all backed up from this client (and not one database from one client and another database from another client).
	lowest/highest activation preference	If this option is selected, the database copy with the lowest/highest activation preference number is backed up.

Table 20 Backup policy options *(continued)*

Options	Description	
	shortest/longest replay lag time	If this option is selected, the database copy with the shortest/longest replay lag time is backed up.
	longest truncation lag time	If this option is selected, the database copy with the longest truncation lag time is backed up.
	For a brief description of the activation preference number, replay lag time and transaction lag time parameters, see " Microsoft Exchange Server parameters in DAG environments" (page 184). For details, see the Microsoft Exchange Server documentation.	
	Use active copy for backup if no passive copies are available	Available if **Back up passive copy** is selected. If this option is selected, the active copy is backed up when no passive copy is available.
Back up all copies	Available if only one database is selected for backup. If this option is selected, all copies (active and passive) are backed up. This is useful when you create `ZDB-to-disk` or `ZDB-to-disk+tape` backups (that is, backups that can be used for instant recovery). If multiple copies are backed up, during instant recovery, multiple copies can be restored, as each copy has its own replica storage volumes to be restored from. For details, see "Instant recovery in DAG environments" (page 202). When you create a `ZDB-to-tape` backup, it is enough that a single copy is backed up; you can restore different copies of a database from the `ZDB-to-tape` backup of a single copy.	
Exclude clients from backup	Creates a list of clients. The database copies that reside on these clients are not backed up.	

Table 21 Application-specific backup options

Options	Description
Pre-exec, **Post-exec**	Specifies which command line to run on a Microsoft Exchange Server system before (`pre-exec`) or after (`post-exec`) the backup. The command line is executed only on the Microsoft Exchange Server system on which the backup session is started (that is the system on which the Data Protector Microsoft Exchange Server integration agent `e2010_bar.exe` is started). Type only the name of the command and ensure that the command is located in the *`Data_Protector_home`*`\bin` directory on the same system. Do not use double quotes. *DAG environment only:* If you selected the DAG virtual system (host) in the **Application system** option, ensure that the command is located on the currently active node. To find out which Microsoft Exchange Server node is currently active, see "Tip" (page 224).

Perform consistency check
`[-exch_check`
`[-exch_throttle` *`Value`*`] |`
`-exch_checklogs]`
	If this option is selected, Microsoft Exchange Server checks the consistency of a database's backup data. If this option is not selected, the session finishes earlier, but the backup data consistency is not guaranteed.
	The check is performed on the replica storage volumes after the backup data is created. If the data is found corrupt, the replica storage volumes are discarded and the database backup fails.
	Default: selected
	If the **Check log files only** option is selected, only the backup data of the log files is checked, which is enough for Microsoft Exchange Server to guarantee data consistency.
	Default: selected
	By default, the consistency check is I/O intensive, which can negatively affect disk performance. The **Throttle check for 1 second** option throttles down the consistency check of the database file `.edb` to lessen impact on the disk performance. Specify after how many input/output operations the check should stop for one second.

Table 21 Application-specific backup options *(continued)*

Options	Description
	This option is not available if only the log files are checked. Default: not selected

Modifying backup specifications

To modify your backup specification, click its name in the Scoping Pane of the Backup context.

In the Microsoft Exchange Server 2013 environment, in the Source page, you can change the Exchange domain user credentials for executing the Exchange Management cmdlet operations remotely by right-clicking the selected backup object and clicking **Configure**. You can also validate your configuration by clicking **Check configuration**.

Click other desired tabs, and apply the changes.

NOTE: To see all databases in the source page, not just those you selected, select **All** in the **Show** option. In a DAG environment, this not only shows all databases, but also updates the current status of databases (active or passive).

Scheduling backup sessions

You can schedule a backup session to start automatically at specific times or periodically. For details on scheduling, see the *HP Data Protector Help* index: "scheduled backups".

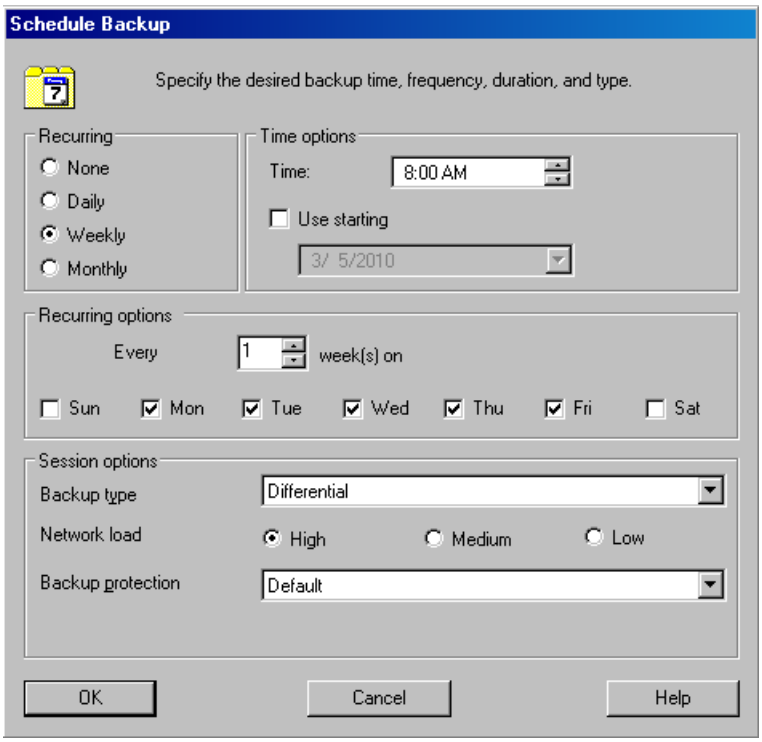
Scheduling example

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

1. In the **Schedule** property page of the backup specification, 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 backup sessions" (page 197). Under **Session options**, select **Differential** from the **Backup type** drop-down list.

   Click **OK**.
3. Repeat Step 1 and Step 2 to schedule Differential backups at 13:00 and 18:00.
4. Click **Apply** to save the changes.

Figure 87 Scheduling backup sessions



Previewing backup sessions

Preview the backup session to test it. You can 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 **MS Exchange 2010+ Server**. Right-click the backup specification you want to preview and click **Preview Backup**.
3. Specify **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

1. Log in to the Cell Manager or to any client with the Data Protector `User Interface` component installed, under a user account that is configured as described in "Configuring user accounts" (page 185).
2. Execute the following command:

```
omnib -e2010_list BackupSpecificationName -test_bar
```

What happens during the preview?

The following are tested:

- Communication between the Microsoft Exchange Server system on which the backup session is started and the Cell Manager
- If each selected database has at least one copy available for backup after the **Backup policy** options and **Client filtering** options have been applied (this applies to backup specifications that contain backup policy options)
- If the selected databases are ready to be backed up (that is, they should not be dismounted, suspended, or in a failed state)

Starting backup sessions

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

To start a backup, 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 **MS Exchange 2010+ Server**. Right-click the backup specification you want to use and click **Start Backup**.
3. Specify **Backup type** and **Network load**. Click **OK**.

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

Using the Data Protector CLI

1. Log in to the Cell Manager or to any client that has the Data Protector `User Interface` component installed under a user account that is configured as described in "Configuring user accounts" (page 185).
2. Execute the following command:

   `omnib -e2010_list` *`BackupSpecificationName`* `[-barmode` *`E2010Mode`*`] [`*`LIST_OPTIONS`*`]`

   where *`E2010Mode`* is one of the following:

   `full|copy|incr|diff`

   The default is `full`.

   For *`ListOptions`*, see the `omnib` man page or the *HP Data Protector Command Line Interface Reference*.

Examples

To start a Full backup using the backup specification `MyDatabases`, execute:

```
omnib -e2010_list MyDatabases -barmode full
```

To start a Differential backup using the same backup specification, execute:

```
omnib -e2010_list MyDatabases -barmode diff
```

Backup objects

For each database (copy), Data Protector creates the following backup objects:

- *Database file object*
  - *ClientName*:/Microsoft Exchange Writer (Exchange Information Store)/Microsoft Information Store/*DBID*/File [MSVSSW-APP]

    (standalone database or active copy)
  - *ClientName*:/Microsoft Exchange Writer (Exchange Replication Service)/Microsoft Information Store/*DBID*/File [MSVSSW-APP]

    (passive copy)
- *Log file object*
  - *ClientName*:/Microsoft Exchange Writer (Exchange Information Store)/Microsoft Information Store/*DBID*/Logs [MSVSSW-APP]

    (standalone database or active copy)
  - *ClientName*:/Microsoft Exchange Writer (Exchange Replication Service)/Microsoft Information Store/*DBID*/Logs [MSVSSW-APP]

    (passive copy)
- *Database object*

  ClientName:/*DBID*/*DBName* [E2010]

  The database object contains information needed to construct the restore chain. For details on restore chains, see "Restore chain" (page 203).
- *VSS metadata object*

  /BackupSession/Metadata [MSVSSW-APP]

Information on whether the objects were successfully backed up or not is saved in the Data Protector IDB. On how to retrieve the information from the IDB, see "Finding information for restore" (page 204).

Restore

You can restore Microsoft Exchange Server data by performing a standard restore or instant recovery session. For details, see "Standard restore" (page 205) and "Instant recovery" (page 213).

IMPORTANT: After you have restored a database, start a Full backup session for the database. Otherwise, the subsequent Incremental and Differential backup sessions will fail.

Considerations

- A Microsoft Exchange Server database that was backed up using the Data Protector Microsoft Volume Shadow Copy Service integration cannot be restored using the Data Protector Microsoft Exchange Server 2010 integration, nor the other way round.

Restore methods

There are various reasons for restoring a Microsoft Exchange Server database. Here are some examples:

- The database has become corrupt.
- The synchronization between an active and passive database copy is broken, but you want to avoid reseeding the passive copy, or simply the resume operation does not work.

- The database needs to be restored to a different point in time.
- The database's backup data needs to be restored for investigation purposes.
- The database's backup data needs to be restored to a recovery database in order to extract individual mailboxes or mailbox files.
- The database's backup data needs to be restored to a dial tone database.

To suit your needs, Data Protector offers different restore methods. You can choose among the following:

- **Repair all passive copies with failed status**
- **Restore to the latest state**
- **Restore to a point in time**
- **Restore to a new mailbox database**
- **Restore to a temporary location**

You can specify different restore methods for different databases in the same session.

NOTE: The first three methods restore backup data to the original database and are therefore only available if the original database still exists. The last two methods restore backup data to a new location.

Repair all passive copies with failed status

This method is available only for databases that are part of a DAG. It is useful if some of a database's passive copies become corrupt, acquiring the status `Failed` or `FailedAndSuspended`. The method automatically restores all the corrupt passive copies from the backup created in the last backup session (and the corresponding restore chain). After the data is restored, the copies are synchronized with the active copy, provided that the **Resume database replication** option is selected.

Restore to the latest state

This method is used to restore a corrupt database to the latest possible point in time. Data Protector restores the database from the backup created in the last backup session (and the corresponding restore chain). For details, see "Restore chain" (page 203).

Once the files are restored, all the logs (not only those restored from the backup, but also any existing logs) are replayed to the database file.

NOTE: ***DAG environments:***

When a passive copy is restored, Microsoft Exchange Server ensures that the logs are replayed to the database file in accordance with the `ReplayLagTime` parameter setting.

Restore to a point in time

This method is used to restore a database to a specific point in time.

NOTE: ***Standard restore:***

When you restore a standalone database or active copy, the existing `.log` and `.chk` files are renamed (a `.keep` extension is added to their names). This feature is useful when you restore files without performing database recovery. It enables you to apply additional logs to the database file; just delete the `.keep` extension of the log files that you also want to be applied and start a database recovery manually. In this way, you can fine-tune the point in time the database is restored to.

When you restore a passive copy, the existing files are deleted.

Once the files are restored, the logs are replayed to the database file (`.edb`) if the **Perform database recovery** option is selected.

NOTE: ***DAG environments:***

- When a passive copy is restored, Microsoft Exchange Server ensures that the logs are replayed to the database file in accordance with the `ReplayLagTime` parameter setting.
- For passive copies that are not restored, a full reseed is required once the restore session completes.

Restore to a new mailbox database

This method is used to restore data to a different database, either because the original database no longer exists or in order to move the data elsewhere.

Using it, you can restore data also to a Microsoft Exchange Server recovery database.

NOTE: ***Instant recovery:***

This option is not available for replica types whose data can only be restored to the original storage volumes.

Restore files to a temporary location

Using this method, you can restore database files to a location of your choice.

- When you restore from a Differential or Incremental backup session, you can restore the complete restore chain or only the files (`.log`) backed up in the selected session.
- When you restore data from a Full backup session, you have an option to restore only the database file (`.edb`).

NOTE: ***Instant recovery:***

This option is not available for replica types whose data can only be restored to the original storage volumes.

Restore destination

Backup data can be restored:

- to an existing database (standalone database, active copy, passive copy),
- to a new database,
- to a temporary location.

Restoring to a standalone database

Restore to the original standalone database (standalone environment) progresses as follows:

1. The database is dismounted.
2. Backup data is restored.
3. Optionally, the newly-restored logs (and pre-existing ones if you are performing the **Restore to the latest state** method) are replayed to the database file `.edb` and the database is mounted.

To restore to the original standalone database, use one of the following restore methods:

- **Restore to the latest state**
- **Restore to a point in time**

Restoring to an active copy

Restore to the active copy (DAG environment) progresses as follows:

1. The database is dismounted.

2. All replications are suspended.
3. Backup data is restored.
4. Optionally, the newly-restored logs (and pre-existing ones if you are performing the **Restore to the latest state** method) are replayed to the database file `.edb` and the database is mounted.

To restore to the active copy, use one of the following restore methods:

- **Restore to the latest state**
- **Restore to a point in time**

Restoring to a passive copy

Restore to a passive copy (DAG environment) progresses as follows:

1. The replication is suspended.
2. Backup data is restored.
3. Optionally, the replication with the active copy is resumed.

To restore to a passive copy, use one of the following restore methods:

- **Restore all passive copies with failed status**
- **Restore to the latest state**
- **Restore to a point in time**

Restoring data to a new database

Restore to a new database progresses as follows:

1. A new mailbox database is created.
2. Backup data is restored to the new database.

NOTE: If you restore to a recovery database, first the backup data is restored and then a recovery database is created.

To restore data to a new mailbox database or recovery database, use the **Restore to a new mailbox database** restore method.

Restoring data to a temporary location

You can restore the database file (`.edb` and/or `.log` and/or `.chk`) to a client and directory of your choice. Select the **Restore files to a temporary location** restore method.

Instant recovery in DAG environments

When you back up a database in a DAG environment, you can decide whether to back up all its copies or only a single copy. If all copies are backed up, during instant recovery, all copies can be restored, as each copy has its own replica storage volumes to be restored from. If only a single copy is backed up, note the following:

- In most cases, only one database copy can be restored from the backup of a single database copy. Some replica types are directly connected with the source (*dependent* replica types) while others are *independent*, allowing the data to be restored to a different location. With the latter, you can restore either the original or a different database copy.

  NOTE: The following replica types are independent:

  - HP P9000 XP Disk Array Family (split mirror replica type in the VSS compliant mode)
  - HP P6000 EVA Disk Array Family (snapclone replica type)

For dependent replica types, Data Protector automatically grays out those clients in the **Target Nodes** option whose database copies were not backed up, because these copies cannot be restored.

- The only replica type that enables you to restore multiple database copies from the backup of a single database copy is snapclone (only with the HP P6000 EVA Disk Array Family). However, you must also ensure that both the **Restore using HP P6000 EVA SMI-S** and **Copy replica data to the source volumes** instant recovery options are selected, in which case data from the replica storage volumes is sequentially copied to multiple locations, restoring one database copy after the other.

Restore chain

By default, when you select a Differential or Incremental backup session for restore, Data Protector restores not only the logs (`.log`) backed up in the selected session but also files backed up in preceding sessions (**restore chain**):

- If a Differential backup session is selected, Data Protector restores:
  1. The `.edb` file and `.log` files backed up in the most recent Full or Copy backup session.
  2. The `.log` files backed up in the selected Differential backup session.
- If an Incremental backup session is selected, Data Protector restores:
  1. The `.edb` file and `.log` files backed up in the most recent Full or Copy backup session.
  2. The `.log` files backed up in all subsequent Incremental backup sessions, up to the selected Incremental backup session.
- If a Full or Copy backup session is selected, Data Protector restores the `.edb` file and `.log` files backed up in the selected session.

NOTE:

- If the **Restore to the latest state** method is used, `.log` files from the Full or Copy backup session are not restored.
- The only method that enables you to restore only `.log` files backed up in the selected Incremental or Differential session is **Restore to a temporary location**.

Restore chain during instant recovery

During an instant recovery session, you first select which:

- Full (ZDB-to-disk or ZDB-to-disk+tape) session or
- Copy (ZDB-to-disk or ZDB-to-disk+tape) session

to use for instant recovery. From database specific options you then specify whether additional logs should also be restored, by selecting a subsequent Incremental or Differential session in the **Restore additional logs until** option.

In an instant recovery session Data Protector restores:

1. The `.edb` file and `.log` files backed up in the selected Full or Copy backup session.
2. The `.log` files backed up in the selected Differential backup session or in all subsequent Incremental backup sessions, up to the selected Incremental backup session.

Restore parallelism

If device concurrency allows, database copies are restored in parallel, except in the following cases:

- If database copies were backed up from the same client, but are now restored to different clients.
- If backup data of the same database copy is used as a restore source for multiple database copies.

Finding information for restore

You can retrieve information about backup sessions (such as information on the backup type and media used, and the messages reported during the backup) from the Data Protector IDB.

To retrieve information, use the Data Protector GUI or CLI.

Using the Data Protector GUI

1. In the Context List, click **Internal Database**.
2. In the Scoping pane, expand **Objects** or **Sessions**.

   If you expand **Objects**, backup objects are sorted according to the Microsoft Exchange Server databases for which they were created.

   NOTE: The backup object name contains the database GUID. To find out which GUID belongs to which database, see the *database object* `/DB_GUID/DB_Name`.

   For example, the *database object* for the database `DB1` with the GUID `08bca794-c544-4e27-87e8-533fb81fd517` is:

   ```
   /08bca794-c544-4e27-87e8-533fb81fd517/DB1
   ```

If you expand **Sessions**, backup objects are sorted according to the sessions in which they were created. For example, backup objects created in the session `2013/02/7–7` are listed under `2013/02/7–7`.

To view details on a backup object, right-click the backup object and click **Properties**.

TIP: To view the messages reported during the session, click the **Messages** tab.

Using the Data Protector CLI

1. Log in to the Cell Manager or to any Microsoft Exchange Server client with the Data Protector `User Interface` component installed under a user account that is configured as described in "Configuring user accounts" (page 185).
2. Get a list of Microsoft Exchange Server backup objects created in a backup session:

   ```
   omnidb -session SessionID
   ```
3. Get details on a backup object:

   ```
   omnidb -e2010 BackupObjectName -session SessionID -catalog
   ```

   Here is one example of a backup object name:

   ```
   devy.company.com:/08bca794-c544-4e27-87e8-533fb81fd517/DB1
   ```

For details, see the `omnidb` man page or the *HP Data Protector Command Line Interface Reference*.

Standard restore

Standard restore is restore from backup data residing on Data Protector media (for example, a tape). Such data is created in ZDB-to-disk+tape and ZDB-to-tape sessions.

You can restore multiple Microsoft Exchange Server databases in the same standard restore session, specifying a different restore method for each database. For details, see "Restore methods" (page 199).

To perform a standard restore, use the Data Protector GUI or CLI.

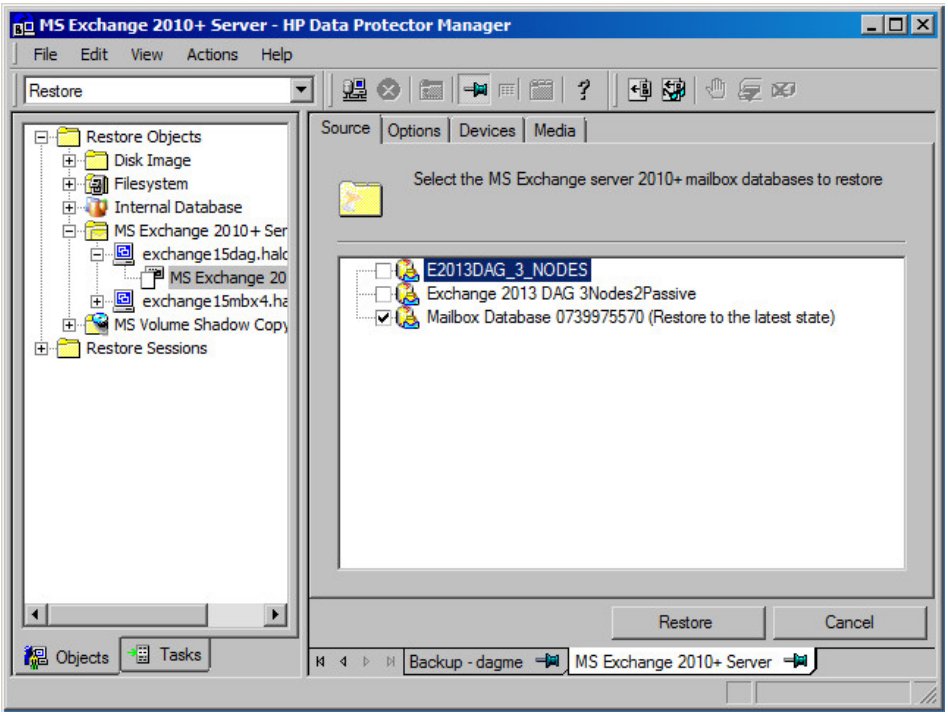
Restoring using the Data Protector GUI

1. In the Context List, click **Restore**.
2. In the Scoping Pane, expand **MS Exchange 2010+ Server**, expand the DAG virtual system or standalone Microsoft Exchange Server system and click **MS Exchange 2010+ Server**.
3. In the Source page, Data Protector displays all Microsoft Exchange Server databases backed up from the selected DAG or standalone environment.

   Select which Microsoft Exchange Server databases to restore.

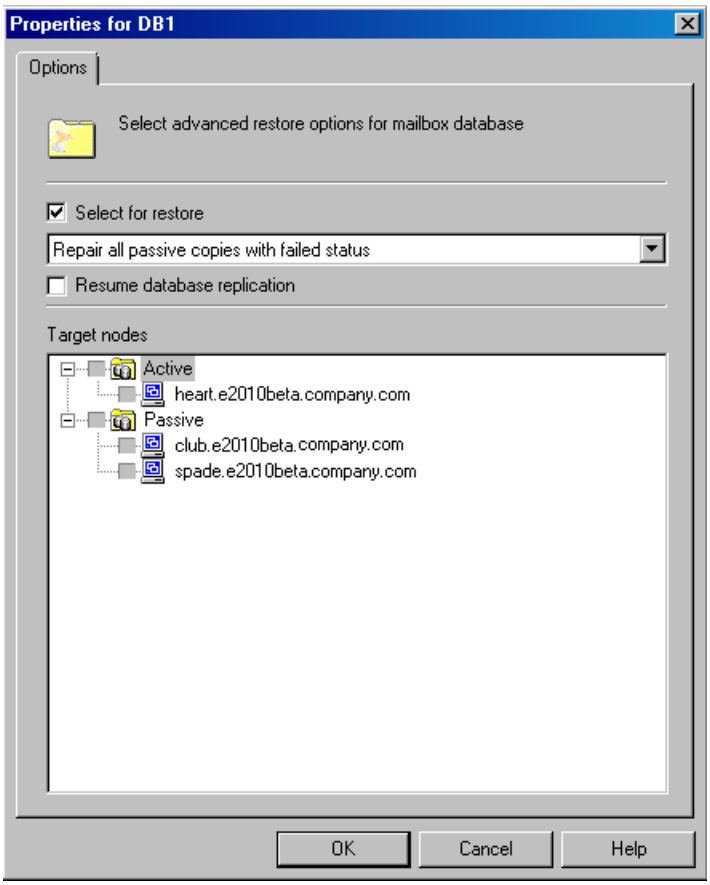
   When you select a database, the Properties for Database dialog box is displayed automatically. Specify a restore method and click **OK**. For databases that are part of a DAG, the default restore method is **Repair all passive copies with failed status**. For standalone databases, the default is **Restore to the latest state**.

Figure 88 Selecting databases for restore



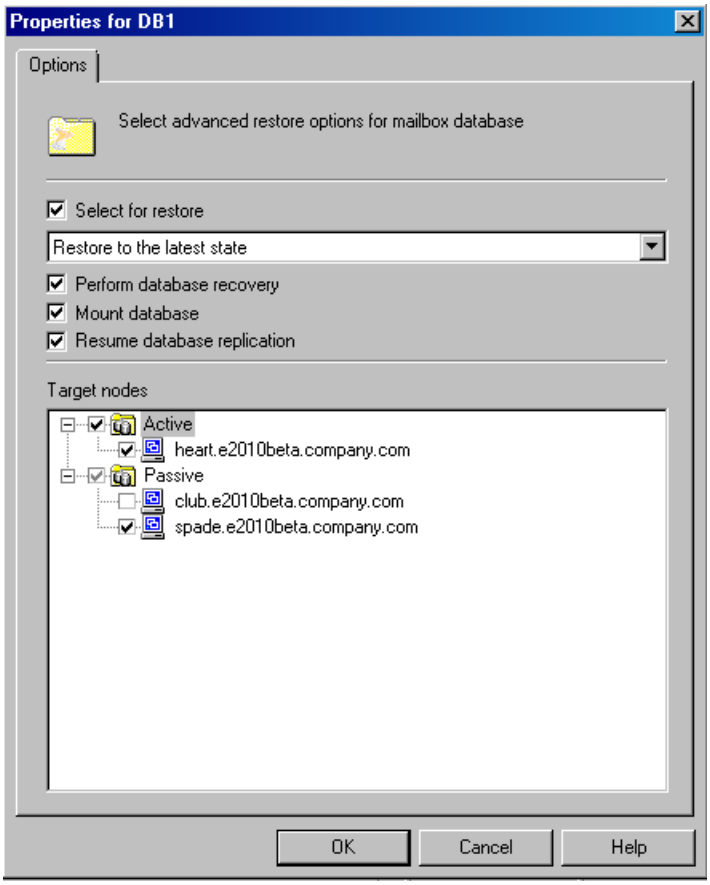
To change the restore method, right-click the database and click **Properties**.

Figure 89 Repair all passive copies with failed status



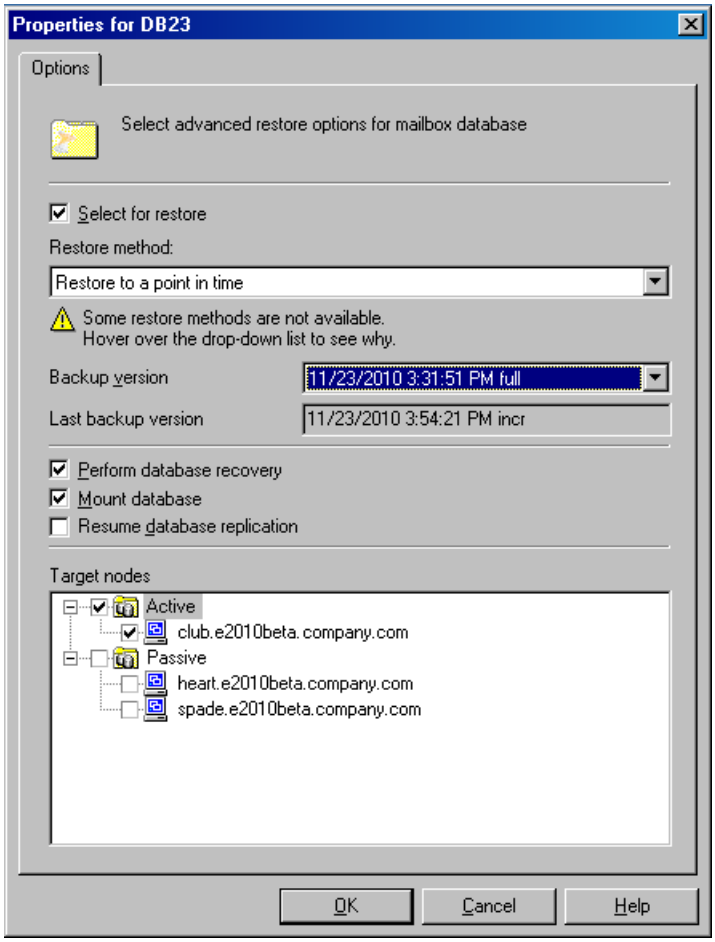
For details, see "Repair all passive copies with failed status" (page 221).

Figure 90 Restore to the latest state



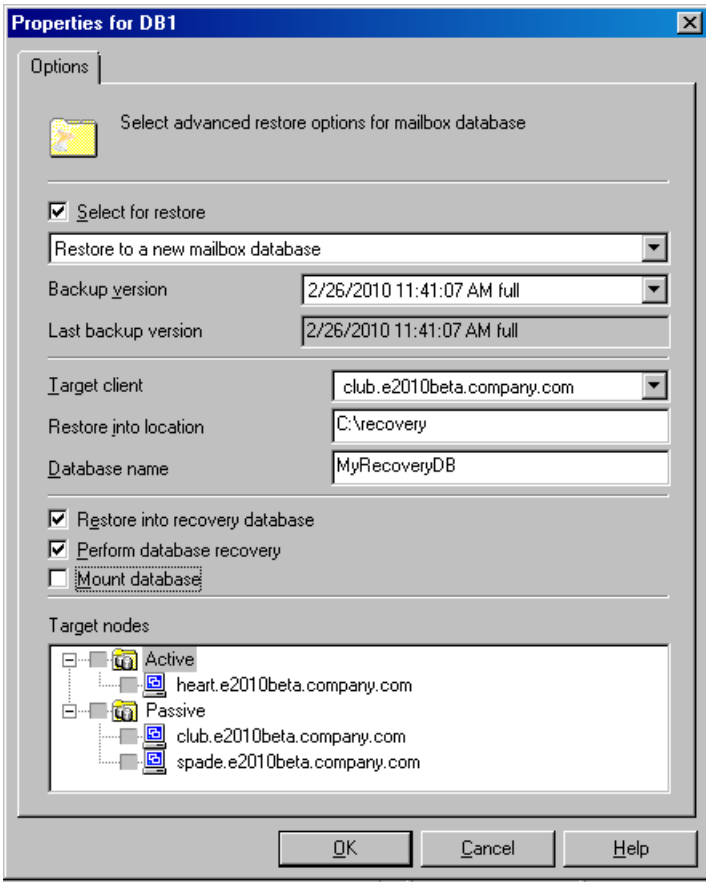
For details, see “Restore to the latest state” (page 200).

Figure 91 Restore to a point in time



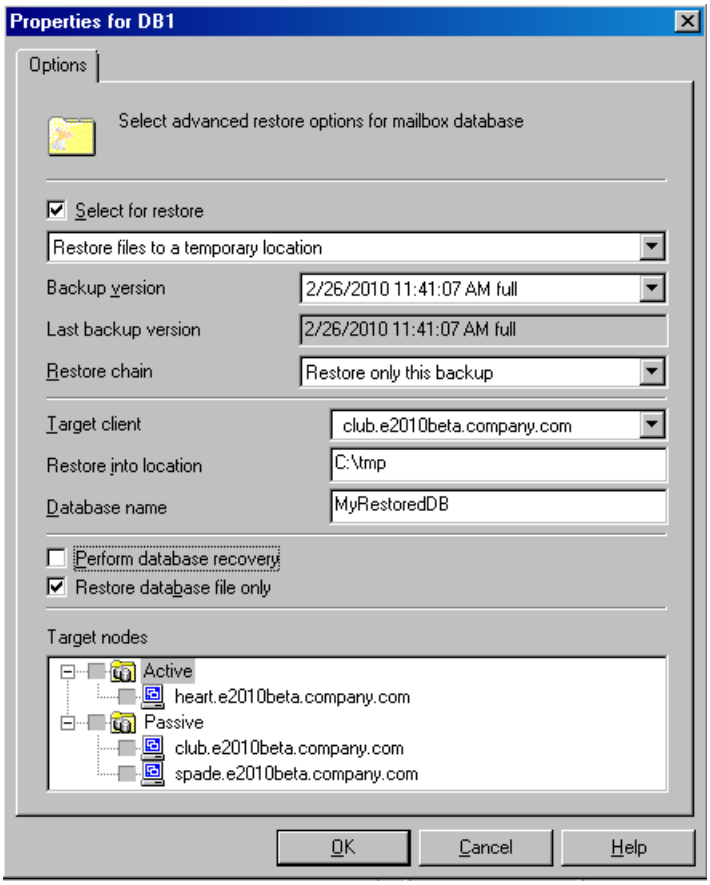
For details, see "Restore to a point in time" (page 200).

Figure 92 Restore to a recovery database



For details, see "Restore to a new mailbox database" (page 201).

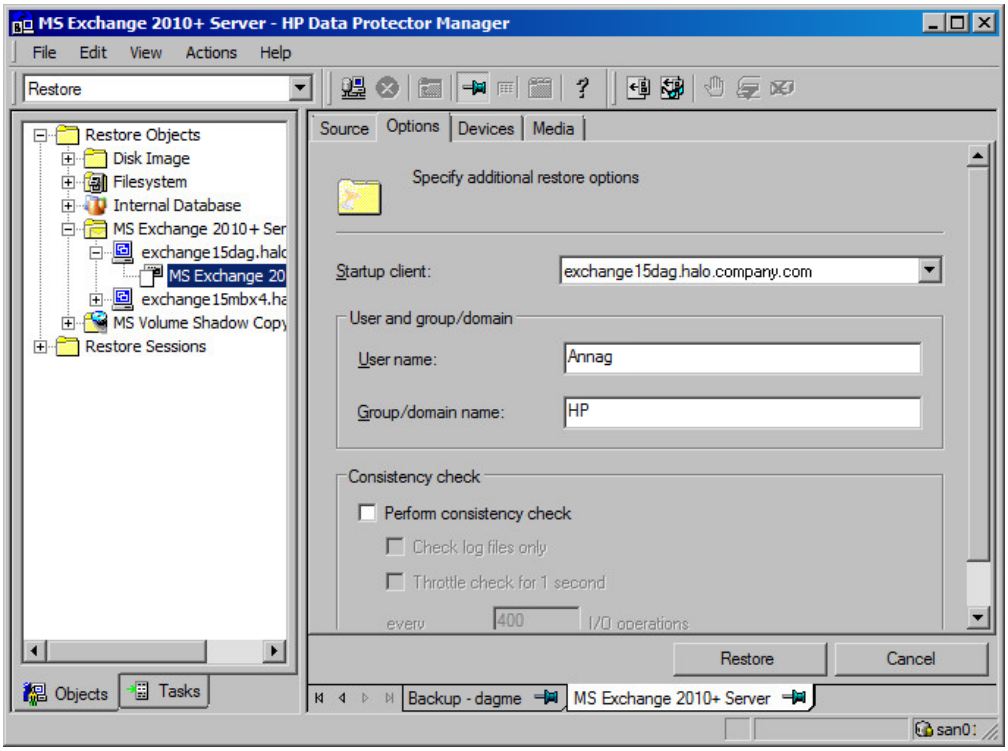
Figure 93 Restore files to a temporary location



For details, see "Restore files to a temporary location" (page 201).

4. In the **Options** page, specify the Data Protector Microsoft Exchange Server 2010 integration restore options. For details, see Table 27 (page 223).

Figure 94 Restore options



5. In the **Devices** page, select which devices to use for restore.

   For details on how to select devices to be used for restore, see the *HP Data Protector Help* index: "restore, selecting devices for".
6. Click **Restore**.
7. In the **Start Restore Session** dialog box, click **Next**.
8. Specify **Report level** and **Network load**.

   Click **Finish** to start the restore.

   If the session succeeds, the message `Session completed successfully` is displayed at the end.

Restoring using the Data Protector CLI

1. Log in to the Cell Manager or to any Microsoft Exchange Server client with the `User Interface` component installed under a user account that is configured as described in "Configuring user accounts" (page 185).
2. Execute the following:

```
omnir -e2010
-barhost ClientName
[VSS_EXCHANGE_SPECIFIC_OPTIONS]
Database [Database …]
[-user User:Domain]
[GENERAL_OPTIONS]

Database
{-db_name SourceDatabaseName | -db_guid SourceDatabaseGUID }
[-source SourceClientName]
{-repair | -latest | -pit | -new | -temp} E2010_METHOD_OPTIONS

E2010_REPAIR_METHOD_OPTIONS
[-no_resume_replication]

E2010_LATEST_METHOD_OPTIONS
[-node TargetNode … | -all]
[-no_resume_replication]
[-no_recover]
[-no_mount]

E2010_PIT_METHOD_OPTIONS
-session BackupID
[-node TargetNode … | -all]
[-no_resume_replication]
[-no_recover]
[-no_mount]
```

```
E2010_NEW_METHOD_OPTIONS
-session BackupID
-client TargetClientName
-location TargetDatabasePath
-name TargetDatabaseName
[-recoverydb]
[-no_recover]
[-no_mount]

E2010_TEMP_METHOD_OPTIONS
-session BackupID
-client TargetClientName
-location TargetDatabasePath
[-no_chain]
[-edb_only]
[-no_recover]
```

For a brief description of the options, see "Restore options" (page 221). For details, see the `omnir` man page or the *HP Data Protector Command Line Interface Reference*.

NOTE: A backup ID is a point in time. All objects (backup data) created in a backup session have the same backup ID, which is the same as the session ID of the backup session.

Mirrored objects and objects created in an object copy session have the same backup ID as objects created in the original backup session. Suppose the media set created in the original backup session no longer exists, but the media set created in an object copy session still exists. To restore the objects, you must specify the session ID of the original *backup* session (that is, the backup ID) and not the session ID of the *object copy* session.

The omnir syntax does not let you specify from which object copy to restore if several copies of the same object exist. This is only possible using the Data Protector GUI by setting the media allocation priority list.

Example (Restore method – repair)

DAG environment

To restore all corrupt passive copies of the database `DB1`, which was backed up from a DAG whose virtual system name was `dag0.company.com`, and to ensure that the integration agent (`e2010_bar.exe`) is started on the client `exchange2.company.com`, execute:

```
omnir -e2010 -barhost exchange2.company.com –db_name DB1 –source
dag0.company.com -repair
```

Example (Restore method – latest)

Standalone environment

To restore the corrupt standalone database `DB1`, which resides on the client `exchange1.company.com`, to the latest possible point in time, and to ensure that the integration agent (`e2010_bar.exe`) is started on the client `exchange2.company.com`, execute:

```
omnir -e2010 -barhost exchange2.company.com –db_name DB1 –source
exchange1.company.com –latest
```

DAG environment

Suppose you want to restore the active copy of the database `DB1`, which resides on the client `exchange1.company.com`, and the passive copies of the database that reside on the clients `exchange2.company.com` and `exchange3.company.com`. Suppose the database `DB1` is part of a DAG whose virtual system name is `dag0.company.com`, and that you want the integration agent (`e2010_bar.exe`) to be started on the client `exchange2.company.com`. Execute the following command:

```
omnir -e2010 -barhost exchange2.company.com –db_name DB1 –source
dag0.company.com –latest –node exchange1.company.com –node
exchange2.company.com –node exchange3.company.com
```

Example (Restore method – pit)

Standalone environment

Suppose you want to restore the corrupt standalone database `DB1`, which resides on the client `exchange1.company.com`, using the backup data created in the session `2013/5/14-1`. Suppose you want the integration agent (`e2010_bar.exe`) to be started on the client `exchange1.company.com`. Execute the following command:

```
omnir -e2010 -barhost exchange1.company.com –db_name DB1 -pit –session
2013/5/14-1
```

NOTE: The `–source` option is not specified, in which case Data Protector assumes that the database was backed up from the client specified with the `–barhost` option.

Example (Restore method – new)

DAG environment

Suppose you want to restore the backup of the database `DB1` to a recovery database that should be created on the client `exchange2.company.com` and named `Recovery1`, with the files in the `C:\Recovery1Folder` directory. Suppose the database `DB1` was backed up in the session `2013/5/14-1` from a DAG whose virtual system name was `dag0.company.com`. To also ensure that the integration agent (`e2010_bar.exe`) is started on the client `exchange1.company.com`, execute the following command:

```
omnir -e2010 -barhost exchange1.company.com –db_name DB1 –source
dag0.company.com –new –session 2013/5/14-1 –client exchange2.company.com
-location C:\Recovery1Folder –name Recovery1 –recoverydb
```

Example (Restore method – temp)

Standalone environment

Suppose you want to restore the transaction logs of the database `DB1`, which resides on the client `exchange2.company.com`. The logs were backed up in the Incremental backup session `2013/5/14-1`. To restore the logs to the client `exchange2.company.com` to the directory `C:\DB1TransactionLogFolder` without performing database recovery, and to ensure that the integration agent (`e2010_bar.exe`) is started on the client `exchange1.company.com`, execute the following command:

```
omnir -e2010 -barhost exchange1.company.com –db_name DB1 –source
exchange2.company.com –temp –session 2013/5/14-1 –client
exchange2.company.com –location C:\DB1TransactionLogFolder -no_chain
–no_recover
```

Restoring using another device

You can restore using a device other than that used for a backup. For details, see the *HP Data Protector Help* index: “restore, selecting devices for”.

Instant recovery

To be able to perform an instant recovery session, you need backup data that is stored on replica storage volumes. Such backup data is created in ZDB-to-disk and ZDB-to-disk+tape sessions.

You can restore multiple Microsoft Exchange Server databases in the same instant recovery session, specifying a different restore method for each database. For details, see “Restore methods” (page 199).

To start an instant recovery session, use the Data Protector GUI or CLI.

Performing instant recovery using the Data Protector GUI

To perform an instant recovery session:

1. In the Context List, click **Instant Recovery**.
2. Expand **Exchange 2010+ Server** and select which ZDB-to-disk or ZDB-to-disk+tape session to use for instant recovery. The sessions are sorted according to the backup specifications used.
3. In the **Source** page, select which Microsoft Exchange Server databases to restore.

   When you select a database, the Properties for Database dialog box is displayed automatically. Specify a restore method and click **OK**. For databases that are part of a DAG, the default restore method is **Repair all passive copies with failed status**. For standalone databases, the default is **Restore to the latest state**. To change the restore method, right-click the database and click **Properties**.

   For details on **Configuration check mode**, press **F1**.

Figure 95 Selecting databases for instant recovery

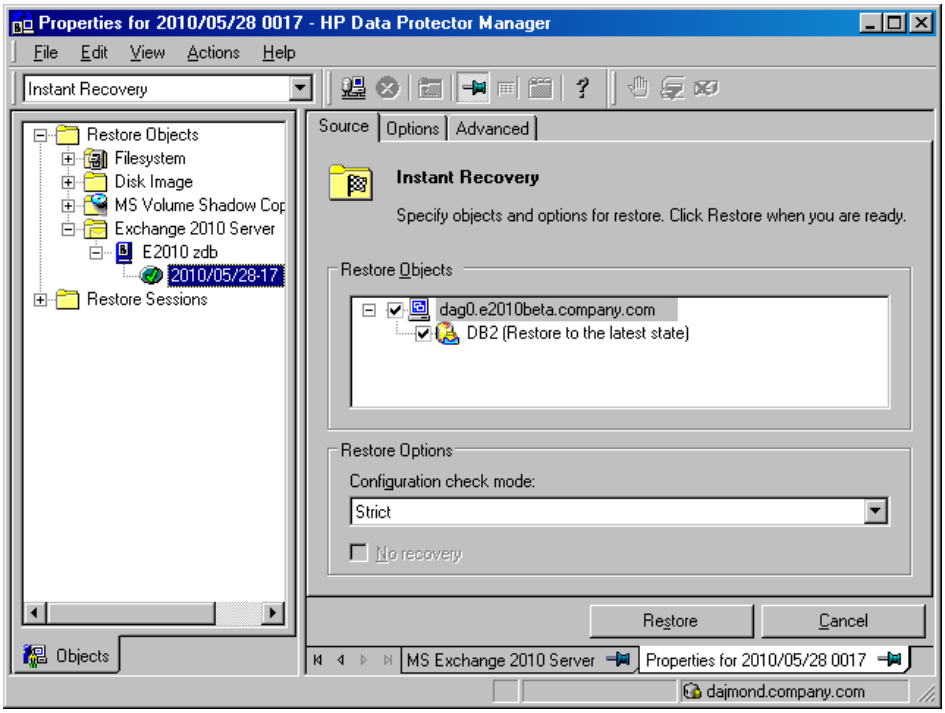
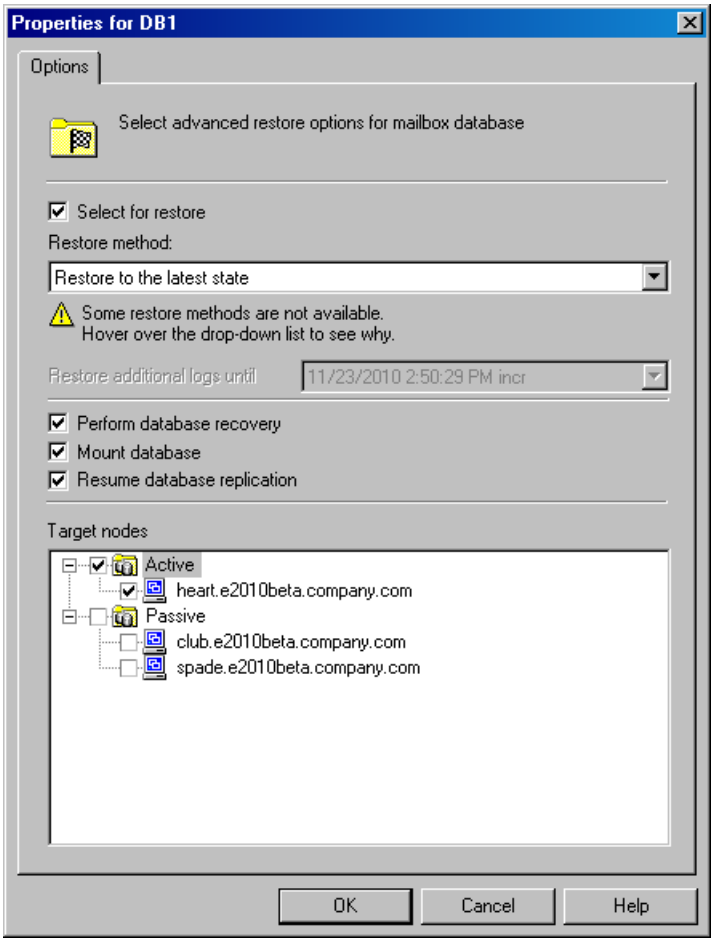
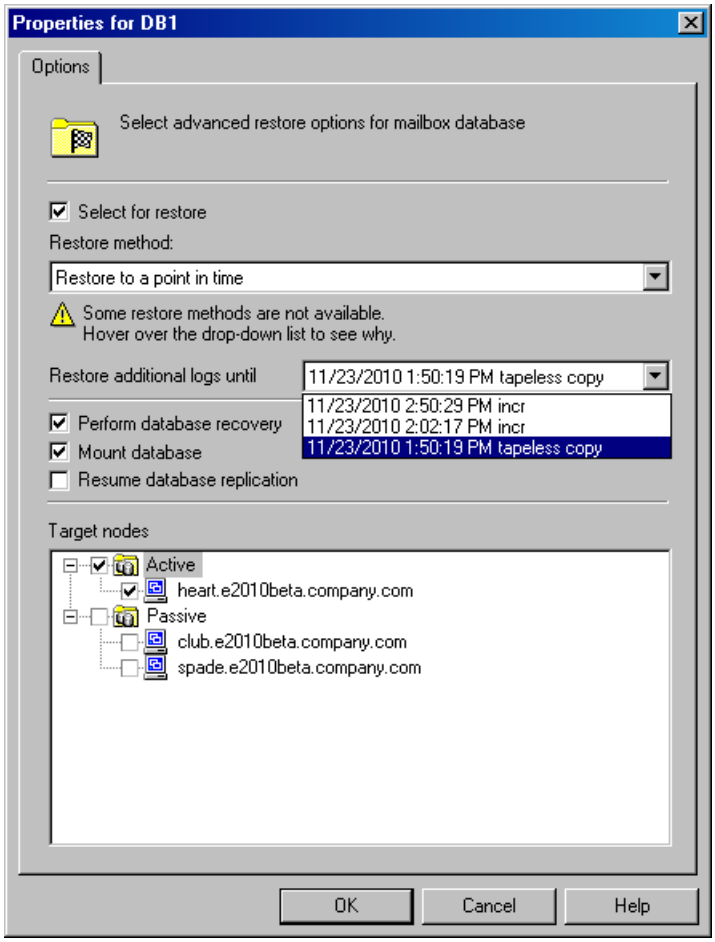


Figure 96 Restore to the latest state



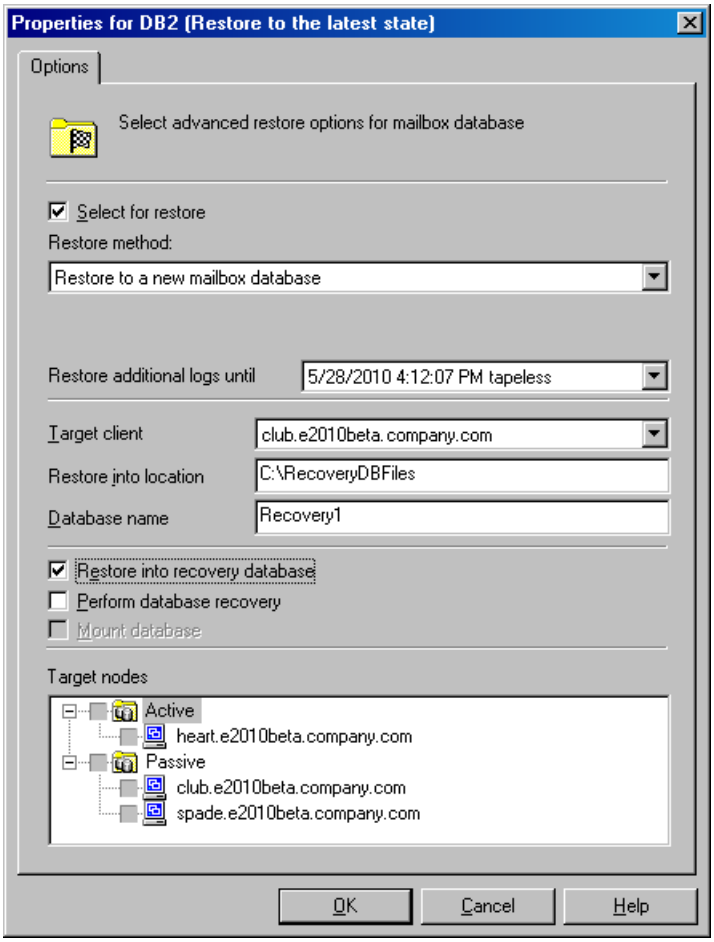
For details, see " Restore to a point in time" (page 221).

Figure 97 Restore to a point in time



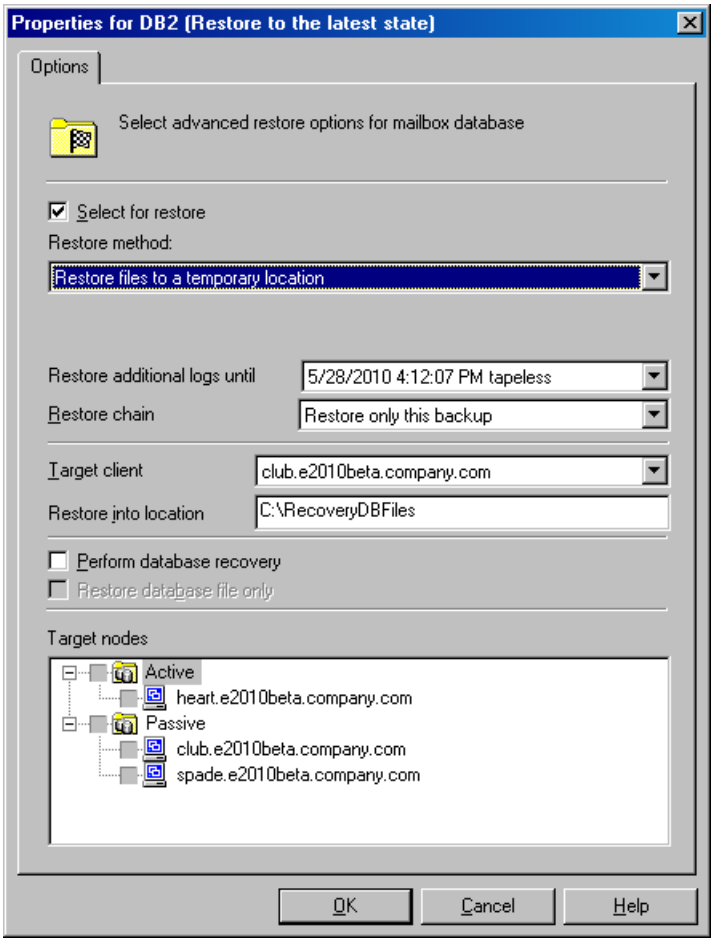
For details, see " Restore to a point in time" (page 221).

Figure 98 Restore to a new mailbox database



For details, see "Restore to a new mailbox database" (page 201).

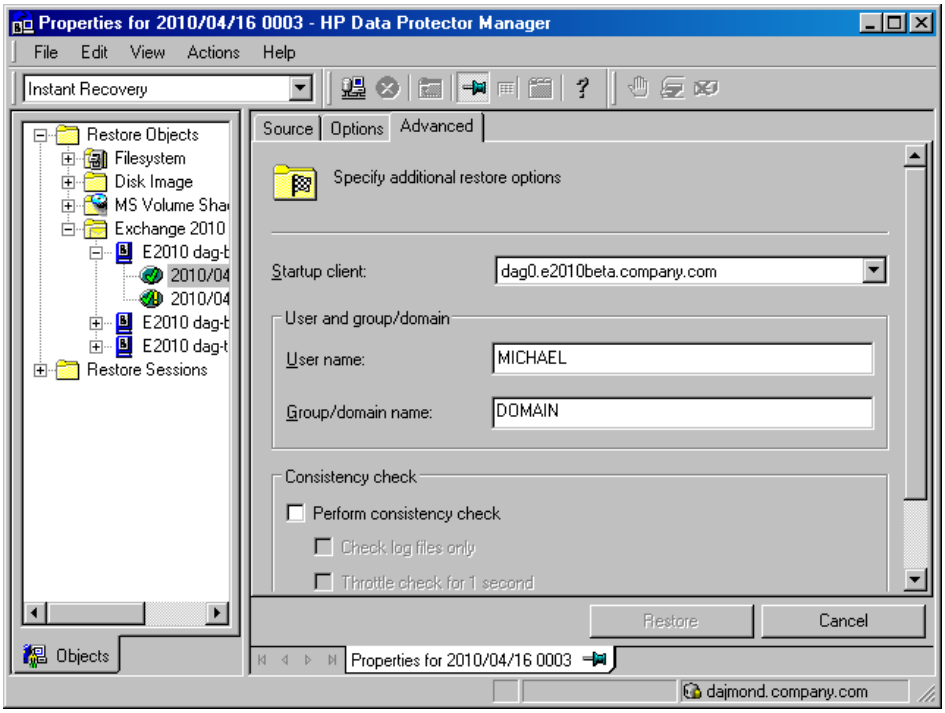
Figure 99 Restore files to a temporary location



For details, see "Restore files to a temporary location" (page 201).

4. In the **Options** page, specify ZDB-specific options. For details, press **F1**.
5. In the **Advanced** page, specify the Data Protector Microsoft Exchange Server 2010 integration instant recovery options. For details, see **"General restore options" (page 223)**.

Figure 100 Instant recovery – advanced



6. Click **Restore**.

Performing instant recovery using the Data Protector CLI

1. Log in to the Data Protector Cell Manager or to any Microsoft Exchange Server client under a user account as described in "Configuring user accounts" (page 185).
2. Execute the following:

```
omnir -e2010
      -barhost ClientName
      -instant_restore
     [VSS_INSTANT_RECOVERY_OPTIONS]
      [VSS_EXCHANGE_SPECIFIC_OPTIONS]
       Database [Database ...]
      [-user User:Domain]
      [GENERAL_OPTIONS]

Database
{-db_name SourceDatabaseName | -db_guid SourceDatabaseGUID}
[-source SourceClientName]
{-repair | -latest | -pit | -new | -temp} E2010_METHOD_OPTIONS

E2010_REPAIR_METHOD_OPTIONS
[-no_resume_replication]
```

```
E2010_LATEST_METHOD_OPTIONS
[-node TargetNode … | -all]
[-no_resume_replication]
[-no_recover]
[-no_mount]
[E2010_IR_SPECIFIC_OPTIONS]

E2010_PIT_METHOD_OPTIONS
-session SessionID
[-node TargetNode … | -all]
[-no_resume_replication]
[-no_recover]
[-no_mount]
[E2010_IR_SPECIFIC_OPTIONS]

E2010_NEW_METHOD_OPTIONS
-session SessionID
-client TargetClientName
-location TargetDatabasePath
-name TargetDatabaseName
[-recoverydb]
[-no_recover]
[-no_mount]
[E2010_IR_SPECIFIC_OPTIONS]

E2010_TEMP_METHOD_OPTIONS
-session SessionID
-client TargetClientName
-location TargetDatabasePath
[-no_chain]
[-edb_only]
[-no_recover]
[E2010_IR_SPECIFIC_OPTIONS]

E2010_IR_SPECIFIC_OPTIONS
[-from_session SessionID]
```

For brief description of the options, see the section "Restore options" (page 221).

For details on the options, see the *HP Data Protector Command Line Interface Reference* or the `omnir` man page.

Example (Restore method – latest)

Standalone environment

Suppose you want to restore the corrupt standalone database `DB1`, which resides on the client `exchange1.company.com`. To ensure the integration agent (`e2010_bar.exe`) is started on the client `exchange1.company.com`, and that the database is restored to the latest state, execute:

```
omnir -e2010 -barhost exchange1.company.com –instant_restore –copy_back
–db_name DB1 -latest
```

Example (Restore method – temp)

DAG environment

Suppose you want to restore the database `DB1`, which was part of a DAG whose DAG virtual system (host) name was `dag0.company.com`. The database was backed up in the session `2013/5/14-1`. To restore the database to a temporary location on the client `exchange1.company.com` to the directory `C:\BackupDatabase`, and to ensure that the integration agent (`e2010_bar.exe`) is started on the client `exchange1.company.com`, execute:

```
omnir -e2010 -barhost exchange1.company.com –instant_restore –copy_back
–db_name DB1 –source dag0.company.com –temp –session 2013/5/14-1 –client
exchange1.company.com –location C:\BackupDatabase
```

Restore options

Table 22 Repair all passive copies with failed status

Option GUI / CLI	Description
Resume database replication / `-no_resume_replication`	Available in DAG environments. Resumes the replication between the active and passive copies after the copies are restored. Note that the CLI option `-no_resume_replication` has the opposite meaning. If it is specified, the replication in not resumed.
Restore additional logs until `-session`	This is an instant recovery-specific option. Not available.
Target nodes	Not available. The clients (that is, copies) that have the status `Failed` or `FailedAndSuspended` are automatically selected.

Table 23 Restore to the latest state

Option GUI / CLI	Description
Select for restore	Specifies whether the database should be restored.
Restore additional logs until `-session`	This is an instant recovery-specific option. Not available.
Perform database recovery / `-no_recover`	Available when restoring a standalone database (standalone environment) or an active copy (DAG environment). Applies the logs to the database file (`.edb`) after the restore completes. Note that the CLI option `-no_recover` has the opposite meaning. If it is specified, the database recovery in not performed.
Mount database / `-no_mount`	Available when restoring a standalone database (standalone environment) or an active copy (DAG environment). Mounts the database after the database recovery completes. This option is available only if **Perform database recovery** is selected. Note that the CLI option `-no_mount` has the opposite meaning. If it is specified, the database is not mounted.
Resume database replication / `-no_resume_replication`	Available when restoring passive copies (DAG environment). Resumes the replication between the active and passive copies after the copies are restored. Note that the CLI option `-no_resume_replication` has the opposite meaning. If it is specified, the replication is not resumed.
Target nodes `-node | –all`	Available only in DAG environments. Specifies which clients (that is, database copies) to restore.

Table 24 Restore to a point in time

Option GUI/CLI	Description
Select for restore	See the description in “ Restore to the latest state” (page 221).
Backup version / `-session`	This is a standard restore-specific option. It specifies from which backup data to restore. Select a backup ID.

Table 24 Restore to a point in time *(continued)*

Option GUI/CLI	Description
	If a Differential backup session is selected, the `.log` files backed up in the selected Differential backup session are restored. If an Incremental backup session is selected, the `.log` files backed up in all subsequent Incremental backup sessions, up to the selected Incremental backup session, are restored.
Last backup version	This is a standard restore-specific option. It shows the session in which the database was last backed up.
Restore additional logs until `-session`	This is an instant recovery-specific option. If a Differential backup session is selected, the `.log` files backed up in the selected Differential backup session are restored. If an Incremental backup session is selected, the `.log` files backed up in all subsequent Incremental backup sessions, up to the selected Incremental backup session, are restored.
Perform database recovery / `-no_recover`	See the description in " Restore to the latest state" (page 221).
Mount database / `-no_mount`	
Resume database replication / `-no_resume_replication`	
Target nodes / `-node | -all`	See the description in " Restore to the latest state" (page 221). The node (client) hosting the active copy is automatically selected for restore.

Table 25 Restore to a new mailbox database

Option GUI/CLI	Description
Select for restore	See the description in " Restore to the latest state" (page 221).
Restore additional logs until `-session`	This is an instant recovery-specific option. See the description in Table 24 (page 221).
Target client / `-client`	Specifies the client to restore to.
Restore into location / `-location`	Specifies the directory to restore to (standard restore) or the directory to mount the replica storage volumes to (instant recovery).
Database name / `-name`	Specifies the name to be used for the new database. If another database with the same name already exists, the restore fails.
Restore into Recovery database / `-recoverydb`	Restores the data to a Microsoft Exchange Server recovery database. Although multiple recovery databases can exist in parallel, only one recovery database can be mounted to the Microsoft Exchange Server at a time.
Backup version / `-session`	See the description in Table 24 (page 221).
Last backup version	
Perform database recovery / `-no_recover`	See the description in " Restore to the latest state" (page 221).

Table 25 Restore to a new mailbox database *(continued)*

Option GUI/CLI	Description
Mount database / `-no_mount`	
Target nodes	Not available.

Table 26 Restore files to a temporary location

Option GUI/CLI	Description
Select for restore	See the description in " Restore to the latest state" (page 221).
Restore additional logs until `-session`	This is an instant recovery-specific option. See the description in Table 24 (page 221).
Restore chain	If this option is set to **Restore only this backup**, only files backed up in the selected session are restored. If this option is set to **Full restore (full, incr, diff backups)**, the complete chain is restored.
Target client / `-client`	See the description in " Restore to a new mailbox database" (page 222).
Restore into location / `-location`	
Backup version / `-session`	See the description in " Restore to a point in time" (page 221).
Last backup version	
Restore database files only / `-edb_only`	Restores only the database files (`.edb`). The logs (`.log`) and checkpoint files (`.chk`) are not restored.
Perform database recovery / `-no_recover`	See the description in " Restore to the latest state" (page 221).
Target nodes	Not available.

Table 27 General restore options

Option GUI / CLI	Description
Startup client / `-barhost`	Specifies the client on which the integration agent (`e2010_bar.exe`) should be started. If the DAG virtual client (host) is selected, the integration agent is started on the currently active node. To find out which node is currently active, see "Tip" (page 224). Default: The same client that was specified for the backup session. If the DAG virtual client was specified, this client is now selected. However, note that the integration agent may not be started on the same physical node as during the backup session; it depends which node is currently active.
Username **Group/Domain name** / `-user`	Specifies which Windows domain user account to use for the restore session. Ensure that the user is configured as described in "Configuring user accounts" (page 185).

Table 27 General restore options *(continued)*

Option GUI / CLI	Description
	If these options are not specified, the restore session is started under the user account under which the `Data Protector Inet` service is running.
Perform consistency check / `[-exch_check [-exch_throttle Value] | -exch_checklogs]`	If this option is selected, Microsoft Exchange Server checks the consistency of a database's backup data. If this option is not selected, the session finishes earlier, but the backup data consistency is not guaranteed. The check is performed on the source storage volumes after the backup data is restored. You do not need to perform the consistency check if it was already performed at the time of backup. Default: not selected If the **Check log files only** option is selected, only the log file backup data is checked, which is enough for Microsoft Exchange Server to guarantee data consistency. Default: not selected By default, the consistency check is I/O intensive, which can negatively affect disk performance. The **Throttle check for 1 second** option throttles down the consistency check of the database file `.edb` to lessen impact on the disk performance. Specify after how many input/output operations the check should stop for one second. This option is not available if only the log files are checked. Default: not selected

TIP: To find out which Microsoft Exchange Server node is currently active, connect to one of the nodes and run:

```
cluster group
```

Example

```
C:\Users\administrator.E2010BETA>cluster group
Listing status for all available resource groups:

Group                Node            Status
-------------------- --------------- ------
Available Storage    spade           Offline
Cluster Group        club            Online
```

The currently active node has the status `Online`. In the example, this is `club`.

Monitoring sessions

You can monitor currently running sessions in the Data Protector GUI. When you run a backup or restore session, a monitor window shows 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.

To monitor a session, see the *HP Data Protector Help* index: "viewing currently running sessions".

Troubleshooting

This section lists general checks and verifications, plus problems you might encounter when using the Data Protector Microsoft Exchange Server 2010 integration.

Because the Data Protector Microsoft Exchange Server 2010 integration is based on the Data Protector Microsoft Volume Shadow Copy Service integration, also see troubleshooting information in the *HP Data Protector Integration Guide for Microsoft Volume Shadow Copy Service*.

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. On how to verify this, see the *HP Data Protector Help* index: "patches".
- 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://support.openview.hp.com/selfsolve/manuals for an up-to-date list of supported versions, platforms, and other information.

Checks and verifications

If your browsing, backup, or restore failed:

- Examine system errors reported in the `debug.log` file.
- Check if you can do a filesystem backup and restore on the problematic client. For information, see the *HP Data Protector Help*.

Problems

Problem

It takes a long time to display Microsoft Exchange Server topology in the Data Protector GUI

When you open the Data Protector GUI and try to display the source page, either in the Backup or Restore context, you must wait a long time.

This may happen if there is an unresponsive system in the same domain (for example, a system that is shut down). The problem occurs even if the unresponsive system is not part of your backup environment. This is due to Microsoft Exchange Server problems with execution of Microsoft Exchange Server Shell commands.

Action

Remove the system from the domain or fix the problem.

Problem

A database backup cannot be performed

When you start a backup session for a database, the database is not backed up, appearing to be locked by other session, though there are no other backup sessions currently running. A message similar to the following is displayed:

```
[Minor] From: OB2BAR_E2010_BAR@exch03.e2010.company.com "MS Exchange
 Server"  Time: 1/17/2013 3:07:13 PM
[170:313]  One or more copies of database DEMAR are already being
backed up in a different session.
```

This may happen if the integration agent (`e2010_bar.exe`) was terminated by force while a previous backup session was in progress, either because the Microsoft Exchange Server system was restarted or for some other reason, so the lock remains.

Action

Execute the following command:

```
omnidbutil -free_cell_resources
```

NOTE: This command line removes all existing locks, so ensure that none of the existing locks is still needed.

Problem

Restore fails

When you try to restore a database, the session fails.

This may happen if a database has been restored before (probably unsuccessfully), and during that previous restore session, the Microsoft Exchange Server created an `.env` file in the database directory. This file now prevents the database from being restored again.

Action

Delete the `.env` file and start a new restore session.

Problem

Restore from an object copy fails in a DAG environment

When restoring a database from a media set created in an object copy session, as the media set created in the original backup session no longer exists, the session fails with an error similar to the following:

```
[Critical] From: OB2BAR_E2010_BAR@computer1.company.com "MS Exchange
2010 Server" Time: 28/02/2013 16:08:12 No mailbox database copy can be
selected for restore/instant recovery.
```

Action

1. Verify that the media set created in the object copy session still exists.
2. On all Microsoft Exchange Server system nodes, set the environment variable `OB2BARHOSTNAME` to the name of the DAG virtual system and restart the Data Protector Inet service.
3. Start a new restore session.

Problem

Restore to the latest state fails

When you try to restore a database all of whose log files were lost, using the restore method **Restore to the latest state** with the **Perform database recovery** option selected, the database recovery fails.

This may happen if a database is restored from a Full backup (that is, the restore chain consists of only the Full backup session). Since in the **Restore to the latest state** session, only the `.edb` file is restored from the Full backup (see "Restore chain" (page 203)), when the database recovery is started, there are no logs to be applied to the database file, and the database recovery fails.

Action

Restore the database using the restore method **Restore to a point in time**. For details, see "Restore to a point in time" (page 200).

Problem

After instant recovery to a point in time, passive copies remain in the Failed state

When you start an instant recovery session in a DAG environment to restore active and passive copies of the same database, using the restore method **Restore to a point in time**, the data is successfully restored, but the synchronization between the active copy and passive copies fails, leaving the passive copies in the `Failed` state.

This problem occurs if, after the data is restored, the passive copy has extra log files, which are not present at the active copy side, and so synchronization cannot be established. This can happen if, during a Full backup session, multiple copies of a database are selected for backup. Data Protector first performs a Full backup of the passive copy that has the fewest logs applied to the database file, and then performs a Copy backup of all the remaining copies, with the active copy being backed up last. While the backup session is in progress, a new log may be created at the active copy side, so when the active copy is backed up, the newly created log is also backed up. If, further on in time, a failover occurs (one of the passive copies becomes the active copy) and you perform a **Restore to a point in time** instant recovery, each copy is restored from its own replica storage volumes. This results in the active copy (which was passive at the time of backup) having fewer logs than the passive copy (which was active at the time of backup). Consequently, synchronization cannot be established.

Action

Perform a full reseed for all `Failed` passive copies.

Problem

In a DAG, a copy-back instant recovery fails when restoring a non-original database copy

Suppose you backed up a database copy by creating a snapclone replica (HP P6000 EVA Disk Array Family). Using the copy-back method, this replica can be used to restore the original database copy and/or the related database copies that reside on different Microsoft Exchange Server systems in the DAG. If the size of the source storage volumes on those Microsoft Exchange Server systems differs from the size of the source storage volumes that were backed up, the instant recovery session fails.

If the **Retain source for forensics** option is selected, a message similar to the following is displayed:

```
[Warning] From: SMISA@dizzy.e2008.company.com "SMISA"  Time:
 1/17/2013 2:51:08 PM
[236:8001] This pair of source and target storage volumes are
not the same size.
Source storage volume : 50014380025B4860\\Virtual Disks\VSS\
FizzyDizzy\DAG\dizzy\dizzy-DB1-data\ACTIVE
Source size : 4 GB
Target storage volume : 50014380025B4860\\Virtual Disks\VSS\
```

```
FizzyDizzy\DAG\fizzy\hpVSS-LUN-06Jul10 02.23.27\ACTIVE
Target size : 3 GB

[Major] From: OB2BAR_VSSBAR@dizzy.e2008.company.com "MS Exchange
 Server"  Time: 1/17/2013 3:11:16 PM
The system failed to refresh symbolic links in kernel object namespace.
```

If the **Retain source for forensics** option is not selected, a message similar to the following is displayed:

```
[Major] From: SMISA@dizzy.e2008.company.com "SMISA"  Time:
 1/17/2013 2:51:08 PM
[236:8001]      This pair of source and target storage volumes are not
the same size.
        Source storage volume : 50014380025B4860\\Virtual Disks\VSS\
FizzyDizzy\DAG\dizzy\dizzy-DB1-data\ACTIVE
        Source size : 4 GB
        Target storage volume : 50014380025B4860\\Virtual Disks\VSS\
FizzyDizzy\DAG\fizzy\hpVSS-LUN-06Jul10 02.23.27\ACTIVE
        Target size : 3 GB
```

Action

Ensure that storage volumes on different Microsoft Exchange Server systems are the same size.

5 Data Protector Microsoft SharePoint Server 2007/2010 VSS based solution

Introduction

This chapter explains how to configure and use the Data Protector Microsoft SharePoint Server 2007/2010 VSS based solution (**VSS based solution**). In reality, the solution is based on the Data Protector Microsoft Volume Shadow Copy Service integration (**VSS integration**). For details on the VSS integration, see the *HP Data Protector Integration Guide for Microsoft Volume Shadow Copy Service*.

The chapter describes concepts and methods you need to understand to back up and restore Microsoft Office SharePoint Server 2007 and Microsoft SharePoint Server 2010 data that is stored in Microsoft SQL Server databases. For example:

- The configuration database (`SharePoint_Config`)
- Content databases (`SharePoint_AdminContent_Label`, `WSS_Content_Label`,...)
- Shared Services Provider databases (`SSP_DB`) (Microsoft Office SharePoint Server 2007)
- SharePoint Service Applications databases (`SSA_DB`) (Microsoft SharePoint Server 2010)
- Search databases (`SSP_Search_DB`)
- The Single Sign-On database (`SSO`)

In addition, you can also back up and restore Microsoft SharePoint Server search index files.

From now on, both Microsoft SharePoint Server versions are called **Microsoft SharePoint Server**, unless the differences are pointed out.

Backup

Microsoft SharePoint Server data that is stored in Microsoft SQL Server databases is backed up using one of the following Microsoft SQL Server VSS writers:

- `MSDE writer` (for Microsoft SQL Server 2000 databases)
- `SqlServerWriter` (for Microsoft SQL Server 2005/2008 databases)

Microsoft Office SharePoint Server 2007 search index files are backed up using the following VSS writers:

- `OSearch VSS writer`
- `SPSearch VSS writer`

Microsoft SharePoint Server 2010 search index files are backed up using the following VSS writers:

- `OSearch14 VSS writer`
- `SPSearch4 VSS writer`

Microsoft FAST Search Server 2010 search index files are backed up:

- using the Data Protector Disk Agent (in case of the standard filesystem backup with VSS enabled)
- using the Data Protector VSS integration (in case of the ZDB filesystem backup)

You can create and run backup specifications using the Data Protector PowerShell command which is described in "Backup" (page 232).

Limitations

- The only supported way to start backup sessions is using the Data Protector PowerShell command. Starting the backup sessions using the Data Protector GUI or CLI is not supported.
- With VSS based solution, the FAST Search index files can also be backed up incrementally when using the Data Protector Disk Agent. For all other Microsoft SharePoint Server data only `Full` backup type is supported.

Restore

Restore can be started using the Data Protector GUI or CLI as described in "Restore" (page 244).

Installation and configuration

ZDB prerequisites

If you plan to run ZDB and instant recovery (IR) sessions, ensure that the SPSearch and OSearch index files of each SSP or SSA, and the FAST Search index files reside on a disk array.

Microsoft Office SharePoint Server 2007

The default location for the SPSearch index files is:

```
C:\Program Files\Microsoft Office Servers\12.0\Data\Applications
```

The default location for the OSearch index files is:

```
C:\Program Files\Microsoft Office Servers\12.0\Data\Office Server\
Applications
```

To move the index files to the disk array:

1. Open the Command Prompt and change the directory to:

   ```
   C:\Program Files\Common Files\Microsoft Shared\Web Server
   Extensions\12\BIN>
   ```

2. To move the SPSearch index files, execute:

   ```
   stsadm -o spsearch -indexlocation PathToNewLocation
   ```

3. To move the OSearch index files, execute:

   ```
   stsadm -o editssp –title SSPname -indexlocation PathToNewLocation
   ```

Microsoft SharePoint Server 2010

The default location for the SPSearch index files is:

```
C:\Program Files\Microsoft Office Servers\14.0\Data\Applications
```

The default location for the OSearch index files is:

```
C:\Program Files\Microsoft Office Servers\14.0\Data\Office Server\
Applications
```

To move the index files to the disk array:

1. Open the Command Prompt and change the directory to:

   ```
   C:\Program Files\Common Files\Microsoft Shared\Web Server
   Extensions\14\BIN>
   ```

2. To move the SPSearch index files, execute:

   ```
   stsadm -o spsearch -indexlocation PathToNewLocation
   ```

3. To move the OSearch index files use the Central Administration (modify farm topology).

The FASTSearch home folder must be installed to the disk array during the FAST Search Server 2010 system installation. In case of a multiple FAST Search Server system farm, ensure that the FASTSearch home folders on all the systems have the same path (drive and path name).

Licensing

The Data Protector VSS based solution requires one online-extension license per each Microsoft SharePoint Server client participating in the backup and restore process. This means one online-extension license for each system on which the Data Protector MS Volume Shadow Copy Integration component is installed.

Installing the integration

For details on how to install a Data Protector cell, see the *HP Data Protector Installation and Licensing Guide*.

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

- Service Pack 2 (Windows SharePoint Services 3.0 and Microsoft Office SharePoint Server 2007)
- Windows PowerShell 2.0 and the Data Protector User Interface component on the Microsoft SharePoint Server system on which you plan to execute the Data Protector commands and on which you install the Data Protector MS Volume Shadow Copy Integration component. See the next bullet.

  If not already available on your Windows system, you can download Windows PowerShell from the Microsoft webpage.
- The Data Protector MS Volume Shadow Copy Integration component on the Microsoft SQL Server system and the Microsoft SharePoint Server systems that have at least one of the following services enabled:

  Microsoft Office SharePoint Server 2007

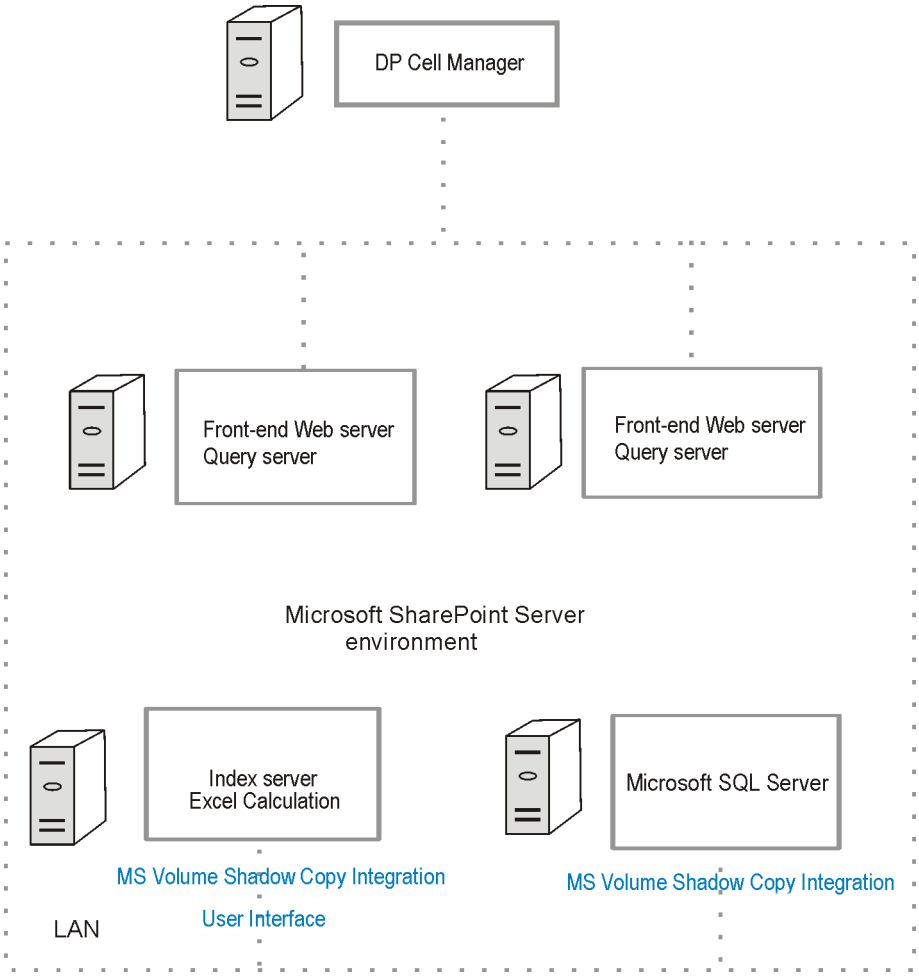
  - Windows SharePoint Services Database
  - Windows SharePoint Services Help Search
  - Office SharePoint Server Search

  Microsoft SharePoint Server 2010

  - SharePoint Foundation Database
  - SharePoint Foundation Help Search
  - SharePoint Server Search
  - FAST Search Server 2010 for SharePoint
- The Data Protector Disk Agent component on each Microsoft FAST Search Server 2010 system for SharePoint (Microsoft SharePoint Server 2010, in case of the mixed filesystem + ZDB environment)

Ensure that the Volume Shadow Copy service is started on all these clients.

Figure 101 Installing a medium farm (example)



In Figure 101 (page 232), the Data Protector components that you need to install are colored blue.

Configuring the integration

For details on how to configure the Data Protector VSS integration, see the *HP Data Protector Integration Guide for Microsoft Volume Shadow Copy Service*.

Configuring user accounts

Create or identify a Windows domain user account that has Windows administrative rights on the Microsoft SharePoint Server system on which you plan to execute the Data Protector commands. This user must also be granted Microsoft SharePoint Server administrative rights and must be added to the Data Protector `admin` user group.

Backup

To back up Microsoft SharePoint Server data, create backup specifications and start backup sessions using the Data Protector PowerShell command `SharePoint_VSS_backup.ps1`.

Prerequisites

- The Windows Remote Management service (which is used for starting and stopping Windows services remotely, and suspending and resuming FAST for Microsoft SharePoint Server 2010) must be configured on all systems.

  To configure and analyze the WinRM service, execute the `winrm quickconfig` command.

For more information, see the Windows Remote Management service documentation.

- In case of Microsoft SharePoint Server 2010 which uses Microsoft SQL Server 2008 for storing data, and Remote BLOB Storage (RBS) is used with the FILESTREAM provider, ensure that FILESTREAM access level is set to `Full access enabled` or `Transact-SQL access enabled`.

  For details of how to configure RBS and FILESTREAM, see the Microsoft SQL Server 2008 documentation.

Limitations

- The only supported way to start backup sessions is using the Data Protector PowerShell command. Starting the backup sessions using the Data Protector GUI or CLI is not supported.
- With VSS based solution, the FAST Search index files can also be backed up incrementally when using the Data Protector Disk Agent. For all other Microsoft SharePoint Server data only `Full` backup type is supported.

Recommendations

- Use the Data Protector PowerShell command to create backup specifications and not the Data Protector GUI.
- Use the Data Protector GUI to modify backup specifications (for example, to add backup devices).
- Use the simple mode for the SQL Server databases. In case you want to use the full mode anyway, ensure that you truncate the transaction logs. Otherwise, you may run out of disk space.
- Whenever you change the farm configuration, perform a new backup.
- In case you want to back up the Single Sign-On database, do not forget to back up the encryption key as described in: http://technet.microsoft.com/en-us/library/cc262932.aspx#Section32.

  Otherwise, you will not be able to restore the database.

How the command works

When you execute the Data Protector PowerShell command `SharePoint_VSS_backup.ps1`, Data Protector first queries for information about the Microsoft SharePoint Server environment. Then it creates backup specifications.

The newly created backup specifications are named `SharePoint_VSS_backup_`*`ClientName`* and have the same backup device specified for use (the one that you specified at command runtime).

Once the backup specifications are created, the command starts backup sessions (one session for each backup specification).

Microsoft Office SharePoint Server 2007

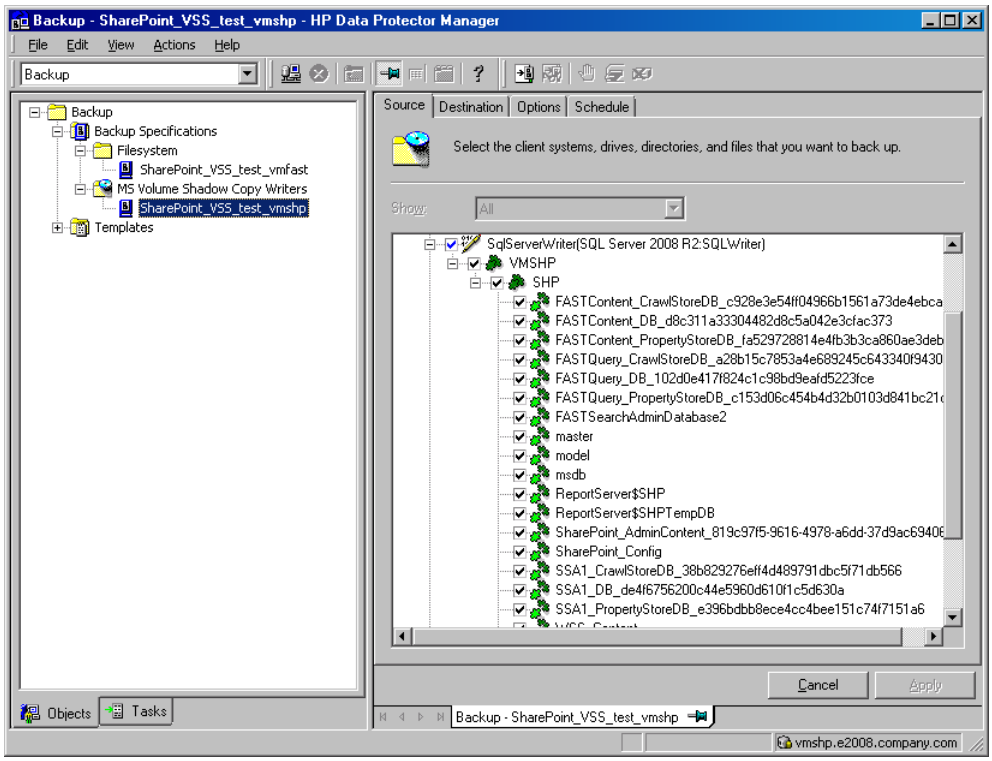
In a Microsoft Office SharePoint Server 2007 environment, the command creates a separate backup specification for each Microsoft Office SharePoint Server 2007 system that has at least one of the following services enabled:

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

For a system with the `Windows SharePoint Services Database` service enabled, the command creates a backup specification that has the `SqlServerWriter` (Microsoft SQL Server

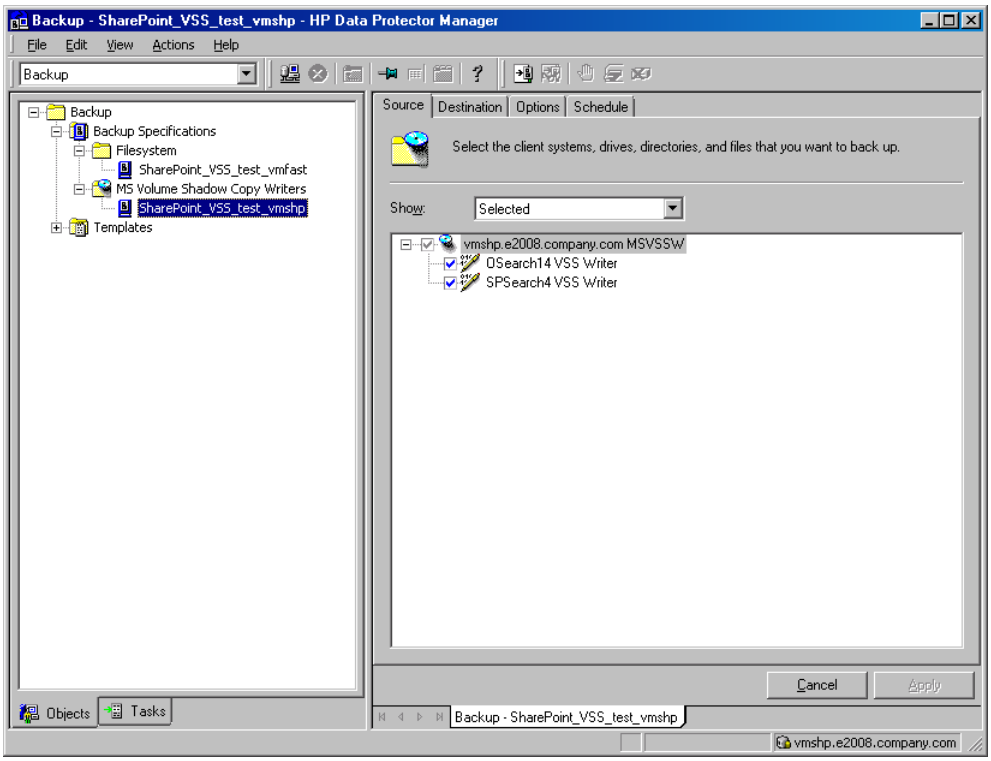
2005/2008) or `MSDE writer` (Microsoft SQL Server 2000) object selected (Figure 102 (page 234)).

Figure 102 Selection of Microsoft Office SharePoint Server 2007 databases



For a system with the `Windows SharePoint Services Help Search` and `Office SharePoint Server Search` services enabled, the command creates a backup specification that has the `SPSearch VSS Writer` and `OSearch VSS Writer` objects selected (Figure 103 (page 235)).

Figure 103 Selecting Microsoft Office SharePoint Server 2007 search index files



Microsoft SharePoint Server 2010

In a Microsoft SharePoint Server 2010 environment, the command creates a separate backup specification for each Microsoft SharePoint Server 2010 system that has at least one of the following services enabled:

- `SharePoint Foundation Database`
- `SharePoint Foundation Help Search`
- `SharePoint Server Search 14`
- `FAST Search Server 2010 for SharePoint (FAST Search)`

For a system with the `SharePoint Foundation Database` service enabled, the command creates a backup specification that has the `SqlServerWriter` (Microsoft SQL Server 2005/2008) object selected.

For a system with the `SharePoint Foundation Help Search` and `SharePoint Server Search` services enabled, the command creates a backup specification that has the `SPSearch4 VSS Writer` and `OSearch14 VSS Writer` objects selected.

For a system with the `FAST Search Server 2010` service enabled, the command with the `-hardware` option specified creates a VSS backup specification that has the complete `FASTSearch` home folder (including `bin` and `lib`) selected.

Considerations

- ***Microsoft Office SharePoint Server 2007:*** If the `Office SharePoint Server Search` service is enabled on two separate Microsoft SharePoint Server systems so that one is assigned the Query and the other the Indexing role, the command creates a backup specification only for the system with the `Indexing` role. It is not created for the one with the `Query` role. To restore index files on the `Query` system, copy the files from the `Indexing` system to the

`Query` system after the restore. For details, see the section "Restoring index files on the Query system" (page 249)".

- The command options enable you to split the process into two parts: first you create the backup specifications and then you start backup sessions. In this way, you can manually modify the newly-created backup specifications in the Data Protector GUI before the backup is actually started.
- If Microsoft SQL Server instances are used not only by Microsoft SharePoint Server but also by other database applications, modify the backup specifications so that only the databases that belong to Microsoft SharePoint Server are selected for backup. See the section "Modifying backup specifications" (page 240).
- If you have Microsoft SQL Server database mirroring enabled, a failover can occur and so a different Microsoft SQL Server system becomes active. Since the command creates backup specifications only for the currently active Microsoft SQL Server systems, it is advisable to update (recreate) the backup specifications before the backup is started.

The command syntax

```
SharePoint_VSS_backup.ps1 -help |-version
SharePoint_VSS_backup.ps1 -createonly CreateOptions
SharePoint_VSS_backup.ps1 -backuponly BackupOptions
SharePoint_VSS_backup.ps1 -resumefarm [-preview] | -resumecert

CreateOptions
{-device DevName | -hardware {no_keep|keep|ir} [-device DevName]}
[-overwrite]
[-prefix PrefixName]
[-excludeindex]

BackupOptions
[-outfile PathToFile]
[-prefix PrefixName]
[-preview]
[-snapshot {diskonly | disktape | tapeonly}]
[-reduce]
[-mode {full | incremental | incremental1 ... | incremental9}]
[-timeout Timeout]
```

IMPORTANT:

- The command must be executed from the *Data_Protector_home*\bin directory on the front-end Web Server system. Ensure that you are logged in under a user account that is configured as described in "Configuring user accounts" (page 232) and that you open the command prompt with administrative rights.
- Do not close the PowerShell console while the backup session is in progress. If you close the console during the backup, some actions are not performed: the backup sessions started do finish, but the farm does not resume the original state. To resume the farm, first execute the command with the `-resumefarm` option and then unquiesce the farm manually using the Microsoft SharePoint Server Central Administration or `stsadm`.

Option description

`-help`

Displays the `SharePoint_VSS_backup.ps1` command usage.

`-version`

Displays the `SharePoint_VSS_backup.ps1` version.

`-createonly`

If this option is specified, Data Protector only creates backup specifications. Backup is not started.

`-backuponly`

If this option is specified, Data Protector only starts backup sessions using the existing backup specifications. The `-device` option is not required.

`-device` *`DevName`*

Specifies which Data Protector device to use for backup. You can specify only one device.

IMPORTANT: If only one device is used to back up a multi-system farm, the corresponding backup sessions cannot run in parallel. This prolongs the time during which the farm is in read-only mode. Specifically, the farm is in read-only mode from the moment when the backup sessions are started up until all VSS snapshots are created.

To enable backup sessions to run in parallel, select different or additional devices in each backup specification before the backup is started. See the section "Modifying backup specifications" (page 240).

`-hardware {no_keep|keep|ir}`

Specifies that the hardware provider should be used (instead of the software provider with `-device` option specified) and, consequently, ZDB options set. The default values for ZDB options are as follows:

- Keep the replica for instant recovery: selected if `ir` is specified.
- Keep the replica after the backup: selected if `ir` or `keep` is specified.
- Configuration check mode: Strict
- Replica type: Mirror/Clone (Plex)
- Numbers of replica rotated: 3

The default ZDB backup types are as follows (provided a device is also specified):

- `no_keep`: ZDB-to-tape
- `keep`: ZDB-to-disk+tape
- `ir`: ZDB-to-disk+tape

`-overwrite`

By default, Data Protector does not create backup specifications if they already exist. If this option is specified, Data Protector overwrites the existing backup specifications with the newly-created ones. Not applicable if `-backuponly` is specified.

`-prefix` *`PrefixName`*

With this option specified, the backup specifications are created under a different name: `SharePoint_VSS_backup_`*`PrefixName`*`_`*`ClientName`*.

In case of backup, this option specifies which backup specifications to use: those which name contains *`PrefixName`*.

Non-ASCII characters in *`PrefixName`* are not supported.

`-outfile` *`PathToFile`*

If this option is specified, backup specification names, errors, sessions outputs, and `omnir` restore commands are written to the specified file.

`-preview`

If this option is specified, Data Protector displays information about the Microsoft SharePoint Server environment and describes the related actions without actually performing them.

`-snapshot {diskonly|disktape|tapeonly}`

Applicable when starting ZDB backup sessions (that is, sessions that use backup specifications in which a hardware provider is specified for use). Performs a ZDB-to-disk (`diskonly`), ZDB-to-tape (`tapeonly`) or ZDB-to-disk+tape (`disktape`) session.

`-reduce`

Applicable only to Microsoft SharePoint Server 2010. If this option is specified, the command excludes mirrored query components from backup to reduce the backup size.

`-excludeindex`

Applicable only to a Data Protector standard filesystem backup of the FAST Search index files (Microsoft SharePoint Server 2010). If this option is specified, Data Protector excludes `data_index` folder contained in the `FASTSearch` home folder from backup specification. This way, the backup is faster, but the restore is more time consuming. The option enables balancing between a backup size and a time to recovery.

`-mode {full|incremental|incremental1... |incremental9}`

Applicable only to a Data Protector standard filesystem backup of the FAST Search index files (Microsoft SharePoint Server 2010). With this option specified, either a `Full` or `Incremental` or leveled incremental backup can be started. By default, the `Full` backup is performed.

When the `incremental` option is specified and the `Full` backup does not exist, the option is ignored and the `Full` filesystem backup of the FAST Search index files is started.

`-resumecert`

Applicable only to Microsoft FAST Search Server 2010. If this option is specified, the FAST Search certificates for the content and the query connectors are reinstalled.

IMPORTANT: The `SharePoint_VSS_backup.ps1 -resumecert` command must be started on the Microsoft SharePoint Server system where the `SharePoint Server Search 14` service is enabled.

`-resumefarm`

To be used after restore. This option returns the farm to a working state by resuming all background activities and crawling, unlocking sites, and starting Microsoft SharePoint Server services.

IMPORTANT: The command with the `-resumefarm` option specified uses the WMI (Windows Management Instrumentation) to remotely start any stopped SharePoint services. To ensure its proper operation, an exception must be added to the Windows Default Firewall for `Remote administration`, which adds the WMI ports, or for the WMI directly. For details, see: http://support.microsoft.com/kb/154596.

`-timeout` *`Timeout`*

This option sets the timeout in minutes after which the crawl of the FAST Search index files is aborted and the farm is resumed. If not specified, the default timeout is 15 minutes.

Starting Windows PowerShell

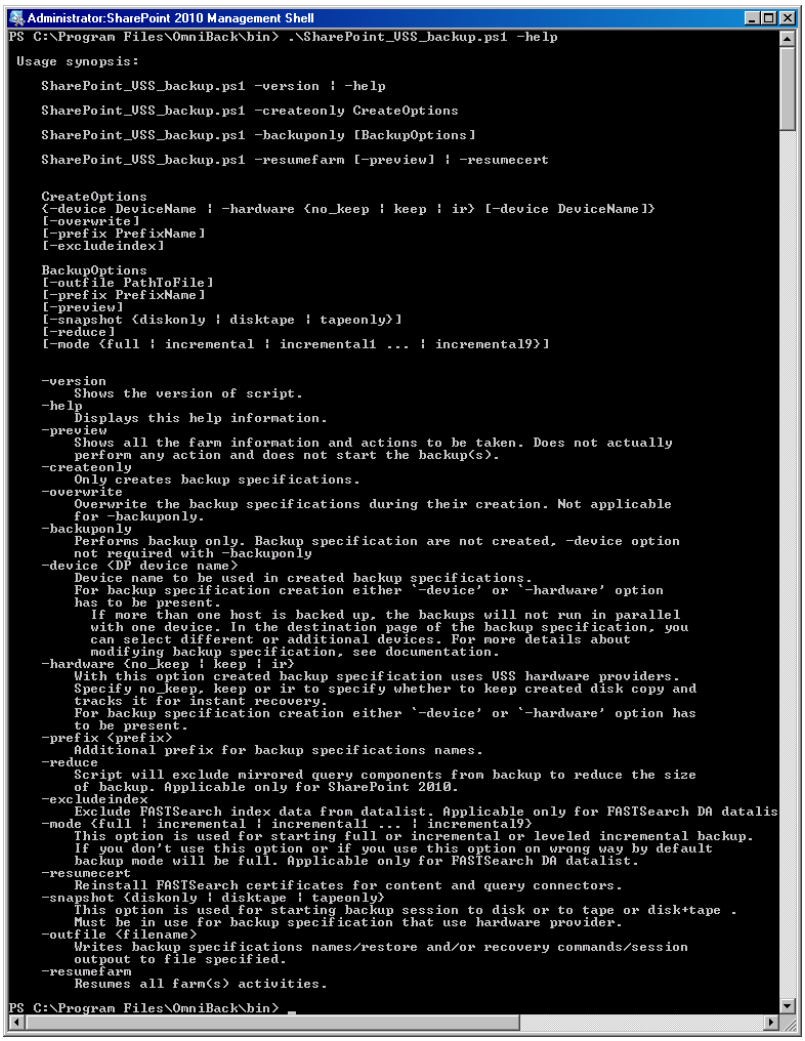
1. Log in to the Microsoft SharePoint Server system where Windows PowerShell and `User Interface` component are installed, under a user account that is configured as described in "Configuring user accounts" (page 232).
2. Open the Windows PowerShell CLI. For example:

   Start > **Programs** > **Accessories** > **Windows PowerShell** > **Windows PowerShell**
3. In case you have Windows User Account Control (UAC) enabled, ensure that you open the CLI with administrative rights. Otherwise, you will not be able to run the Data Protector PowerShell command.

4. Ensure that the Windows PowerShell execution policy is set to `RemoteSigned` or `Unrestricted`.

   "Displaying the Data Protector PowerShell command syntax" (page 239) shows how the Windows PowerShell execution policy is set to `Unrestricted` and how the Data Protector PowerShell command syntax is displayed.

Figure 104 Displaying the Data Protector PowerShell command syntax



Creating backup specifications (examples)

1. To create backup specifications in which the backup device `filelib_writer1` is specified for use, execute:

   ```
   SharePoint_VSS_backup.ps1 -createonly -device filelib_writer1
   ```

2. To create backup specifications with the label `weekly` in their names and in which the backup device `dev1` is specified for use, execute:

   ```
   SharePoint_VSS_backup.ps1 -createonly -device dev1 -prefix weekly
   ```

3. To create ZDB backup specifications in which the backup device `dev1` and the hardware provider (ZDB disk array) are specified for use, and in which the ZDB option Keep the replica for instant recovery is enabled, execute:

   ```
   SharePoint_VSS_backup.ps1 -createonly -hardware ir -device dev1
   ```

4. Applicable only to a Data Protector standard filesystem backup of the FAST Search index files (Microsoft SharePoint Server 2010).

   To create filesystem backup specifications in which the backup device `dev1` is specified for use and with the `data_index` folder, contained in the `FASTSearch` home folder, excluded from the backup of the FAST Search index files, execute:

   ```
   SharePoint_VSS_backup.ps1 -createonly -device dev1 -excludeindex
   ```

Modifying backup specifications

To modify a backup specification, open the Data Protector GUI. In the Context list, select **Backup** and, under **MS Volume Shadow Copy Writers** or under **Filesystem** (if performing a standard filesystem backup of the FAST Search index files), click the name of the backup specification that you want to modify (see Figure 102 (page 234)).

Source page

If you want to modify the Source page of the backup specification (for example, you want to back up individual Microsoft SharePoint Server databases), consider the following:

- The configuration database and the Central Administration content database must both be backed up during the same time period which starts with the suspend of the Microsoft SharePoint Server (SharePoint farm) and ends with the resume of the SharePoint farm to ensure the data consistency.
- **Microsoft Office SharePoint Server 2007**: The Shared Services Provider database (SSP_DB), Search database (`SSP_Search_DB`), and the associated search index files must all be backed up during the same time period which starts with the suspend of the Microsoft SharePoint Server (SharePoint farm) and ends with the resume of the SharePoint farm to ensure the data consistency.
- **Microsoft SharePoint Server 2010**:
  - The SharePoint Service Applications, Search database (`SSA_Search_DB`), and the associated search index files must all be backed up during the same time period which starts with the suspend of the Microsoft SharePoint Server (SharePoint farm) and ends with the resume of the SharePoint farm to ensure the data consistency.
  - The FAST search index files and the FAST Content SSA crawl components must all be backed up during the same time period which starts with the suspend of the Microsoft SharePoint Server (SharePoint farm) and ends with the resume of the SharePoint farm to ensure the data consistency.
- The Help Search database and the associated index files must all be backed up during the same time period which starts with the suspend of the Microsoft SharePoint Server (SharePoint farm) and ends with the resume of the SharePoint farm to ensure the data consistency.

Otherwise, after restore, the Microsoft SharePoint Server data may not be consistent.

Destination page

In the Destination page of the backup specification, you can select different or additional devices and set the device and media options.

Options page

In the Options page of the backup specification, you can modify backup options. For the standard filesystem backup of the FAST search index files leave the **Use Shadow Copy** option specified to enable the use of the VSS. To modify ZDB options, click **Advanced** in the Backup Specifications field and then, in the Backup Options dialog box, click the **Advanced backup options** tab.

Starting backup sessions (examples)

1. To preview the actions that are performed when a backup session is started, execute:
   `SharePoint_VSS_backup.ps1 -backuponly -prefix dev -preview`
   The following output is from a Microsoft Office SharePoint Server 2007 environment:

```
==============================
 Starting MOSS backup command
 02/10/2011 03:16:30
==============================
------------------------------
List of hosts and their services
------------------------------
 virtual20
 Application Server
   Windows SharePoint Services Help Search
   Windows SharePoint Services Database
   Information Management Policy Configuration Service
   Office SharePoint Server Search
   Shared Services Timer
   Office SharePoint Server Search Admin Web Service
   Excel Calculation Services
   Single Sign-on Service
   SSP Job Control Service
   Portal Service
   Office SharePoint Server Search
   Document Conversions Launcher Service
   Document Conversions Load Balancer Service
   Windows SharePoint Services Web Application
   Central Administration
   Windows SharePoint Services Incoming E-Mail
   Windows SharePoint Services Administration
   Windows SharePoint Services Timer

VIRTUAL21
 Application Server
   Windows SharePoint Services Help Search
   Office SharePoint Server Search
   Shared Services Timer
   Office SharePoint Server Search Admin Web Service
   Single Sign-on Service
   SSP Job Control Service
   Portal Service
   Office SharePoint Server Search
   Windows SharePoint Services Web Application
   Windows SharePoint Services Administration
   Windows SharePoint Services Help Search
   Windows SharePoint Services Timer
```

```
VIRTUAL23
 Application Server
   Windows SharePoint Services Help Search
   Office SharePoint Server Search
   Shared Services Timer
   Office SharePoint Server Search Admin Web Service
   Single Sign-on Service
   SSP Job Control Service
   Portal Service
   Office SharePoint Server Search
   Windows SharePoint Services Web Application
   Windows SharePoint Services Administration
   Windows SharePoint Services Help Search
   Windows SharePoint Services Timer
--------------------------------
SQL hosts list
 virtual20

Index hosts list
 virtual20
 VIRTUAL21
 VIRTUAL23

Help search hosts list
 VIRTUAL21
 VIRTUAL23
-------------------
SUSPENDING FARM
02/10/2011 03:16:43
-------------------
Farm SharePoint_Config

Service Windows SharePoint Services Help Search on host VIRTUAL21
-> Pausing background activity ...
   ... background activity paused.

Service Windows SharePoint Services Help Search on host VIRTUAL23
-> Pausing background activity ...
   ... background activity paused.

Web applications:
 Display name:  Recovery Web Application
 Alternate URL: http://virtual20:999

 Display name:  SharePoint - 123
 Alternate URL: http://virtual20:123
  Web site URL: http://virtual20:123/ssp/admin
  Root title:   Shared Services Administration: SSP1
  -> Setting lock state to readonly
   Crawled by:   , id
   Crawl status:
  -> Pausing background activity
...
Quiesce status is: Quiesced
-------------------
SUSPENDING END
02/10/2011 03:18:28
-------------------
```

```
-> Starting backups...

Starting backup:  omnib -msvssw_list SharePoint_VSS_backup_dev_virtual20 \ -barmode full
Starting backup:  omnib -msvssw_list SharePoint_VSS_backup_dev_VIRTUAL21 \ -barmode full
Starting backup:  omnib -msvssw_list SharePoint_VSS_backup_dev_VIRTUAL23 \ -barmode full

Waiting while VSS creates Volume Shadow Copies ...
       Please wait. DO NOT close PowerShell console!
       After shadow copies are created, the command will resume farm
       and display Data Protector backup session(s) output(s).
  SUCCESS: Volume Shadow Copy successfully created.
           Host   : virtual20
  SUCCESS: Volume Shadow Copy successfully created.
           Host   : VIRTUAL21
  SUCCESS: Volume Shadow Copy successfully created.
           Host   : VIRTUAL23

------------------
RESUMING FARM
02/10/2011 03:18:28
------------------
Service Windows SharePoint Services Help Search on host VIRTUAL21
-> Resuming background activity ...
   ... background activity resumed

Service Windows SharePoint Services Help Search on host VIRTUAL23
-> Resuming background activity ...
   ... background activity resumed

Web site URL: http://virtual20:123/ssp/admin
Root title:  Shared Services Administration: SSP1
 -> Reverting lock for site http://virtual20:123/ssp/admin to none
 -> Resuming background activity
...
--------------------
RESUMING END
02/10/2010 03:19:18
------------------
==============================
 MOSS backup command finished
 02/10/2011 03:19:18
 Running time 00:02:48.3336122
==============================
```

2. To start backup sessions using the existing backup specifications that have no prefix in their names, execute:

   ```
   SharePoint_VSS_backup.ps1 –backuponly
   ```

3. To start backup sessions using the existing backup specifications that have the prefix `weekly` in their names, execute:

   ```
   SharePoint_VSS_backup.ps1 –backuponly –prefix weekly
   ```

4. To start backup sessions using the existing backup specifications that have no prefix in their names and to save the output of the sessions and the associated restore commands to the file `c:\logs\shp.log`, execute:

   ```
   SharePoint_VSS_backup.ps1 –backuponly –outfile C:\logs\shp.log
   ```

5. To start ZDB-to-disk backup sessions using the existing ZDB backup specifications that have no prefix in their names, execute:

   ```
   SharePoint_VSS_backup.ps1 –backuponly -snapshot diskonly
   ```

6. To start `incremental` filesystem backup sessions of the FAST Search index files (Microsoft SharePoint Server 2010), execute:

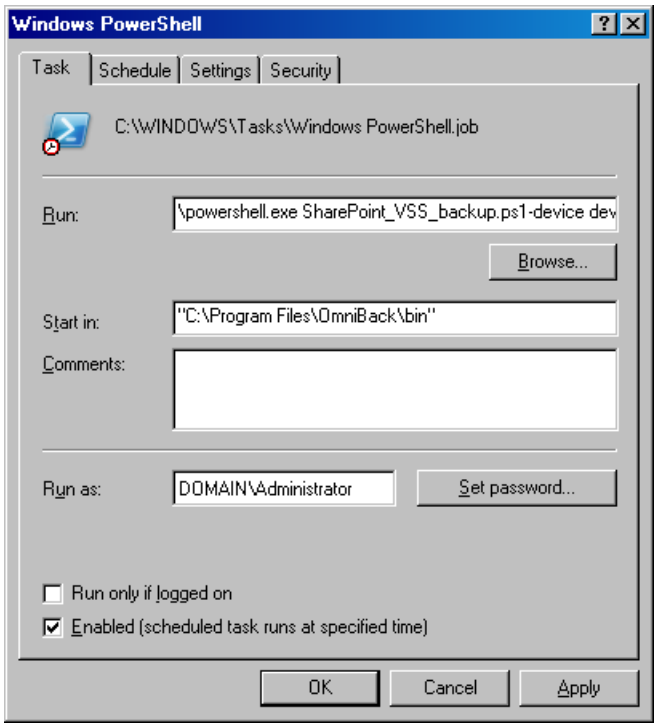
   ```
   SharePoint_VSS_backup.ps1 -backuponly -mode incremental
   ```

Scheduling backup sessions

You can schedule backup sessions using the Windows system scheduler.

1. On the front-end Web server system, create a Windows PowerShell scheduled task. Go to:
   Start > **Settings** > **Control Panel** > **Scheduled Tasks** > **Add Scheduled Task**
2. Open advanced properties for the task.

Figure 105 Scheduling a backup session using the Windows scheduler



In **Run**, type:

Windows_PowerShell_home\powershell.exe SharePoint_VSS_backup.ps1[Options]

For details on `Options`, see "The command syntax" (page 236).

In **Start in**, type:

Data_Protector_home\bin

In **Run as**, type a Windows domain user account `DOMAIN\UserName` that is configured as described in "Configuring user accounts" (page 232).

Restore

To restore Microsoft SharePoint Server data:

- Stop Microsoft SharePoint Server services
- Restore the data.
- Return the farm to a working state.

For details, see the following sections.

Before you begin

- Stop and disable the following services:
  - `IIS Admin Service` (Only for Internet Information Services 6.0 on Windows Server 2003, when the whole farm is restored)
  - `Office SharePoint Server Search` (Microsoft Office SharePoint Server 2007)
  - `SharePoint Server Search 14` (Microsoft SharePoint Server 2010)

In addition, stop the following services:

- Microsoft Office SharePoint Server 2007
  - `Windows SharePoint Services Administration`
  - `Windows SharePoint Services Search`
  - `Windows SharePoint Services Timer`
- Microsoft SharePoint Server 2010
  - `SharePoint 2010 Administration`
  - `SharePoint Foundation Search V4`
  - `SharePoint 2010 Timer`
  - `SharePoint 2010 Tracing`
  - `FAST Search for SharePoint`
  - `FAST Search for SharePoint Monitoring`
- Put the Microsoft SQL Server instance offline if you plan to restore one of the following Microsoft SQL Server databases:
  - `master`
  - `model`
  - `msdb`
  - a database for which Microsoft SQL Server mirroring is enabled

NOTE:

- If you use `SqlServerWriter`, you can restore the `model` and `msdb` databases also when the Microsoft SQL Server instance is online. This is one advantage over `MSDE writer`.
- *Microsoft SQL Server mirroring*: If the original and mirror database reside in separate Microsoft SQL Server instances, put offline both Microsoft SQL Server instances.

Restoring data

You can restore Microsoft SharePoint Server data using the Data Protector GUI or CLI.

Considerations

- The configuration database and the Central Administration content database must both be restored using backups from the same point in time (the backups performed in the same period in which the Microsoft SharePoint Server (SharePoint farm) was in suspended mode) to ensure the data consistency. Since the configuration database and the Central Administration content

database contain system-specific information, you can restore them only to the original environment or to an environment that has precisely the same configuration, software updates, server names, and number of servers.

- **Microsoft Office SharePoint Server 2007**: The Shared Services Provider database (`SSP_DB`), Search database (`SSP_Search_DB`), and the associated search index files must all be restored using backups from the same point in time (the backups performed in the same period in which the Microsoft SharePoint Server (SharePoint farm) was in suspended mode) to ensure the data consistency.
- **Microsoft SharePoint Server 2010**:
  - The SharePoint Service Applications, Search database (`SSA_Search_DB`), and the associated search index files must all be restored using backups from the same point in time (the backups performed in the same period in which the Microsoft SharePoint Server (SharePoint farm) was in suspended mode) to ensure the data consistency.
  - Since the FAST configuration database and the `FAST Search` home folder contain system-specific information, you can restore them only to the original environment or to an environment that has precisely the same configuration, software updates, server names, and number of servers.
  - The FAST Search index files and the FAST Content SSA crawl components must all be restored using backups from the same point in time (the backups performed in the same period in which the Microsoft SharePoint Server (SharePoint farm) was in suspended mode) to ensure the data consistency.
- The Help Search database and the associated index files must all be restored using backups from the same point in time (the backups performed in the same period in which the Microsoft SharePoint Server (SharePoint farm) was in suspended mode) to ensure the data consistency.
- The following table shows which VSS restore modes are supported for which writers:

Table 28 VSS supported restore modes and writers

Writers	VSS restore modes	
	Restore to another client	**Restore files to temporary location**
MSDE writer SqlServerWriter	No	Yes (manual attach needed)
OSearch VSS writer OSearch14 VSS writer	Yes	No
SPSearch VSS writer SPSearch4 VSS writer	Yes	No

Prerequisites

- Applicable only to a Data Protector filesystem restore of the FAST Search index files (Microsoft SharePoint Server 2010). Before restoring the FAST Search index files, the **Overwrite** option must remain selected to ensure the data consistency. It is selected by default.

Restoring using the Data Protector GUI

1. In the Context List, click **Restore**.

2. In the Scoping Pane, expand **MS Volume Shadow Copy Writers**, expand the client which data you want to restore, and then click **MS Volume Shadow Copy Writers**.

   If performing a filesystem restore of the FAST Search index files (Microsoft SharePoint Server 2010), expand **Filesystem**, expand the client which data you want to restore, and then click the filesystem object.

3. In the Source page, select the data that you want to restore.

Figure 106 Selecting Microsoft Office SharePoint Server 2007 databases for restore

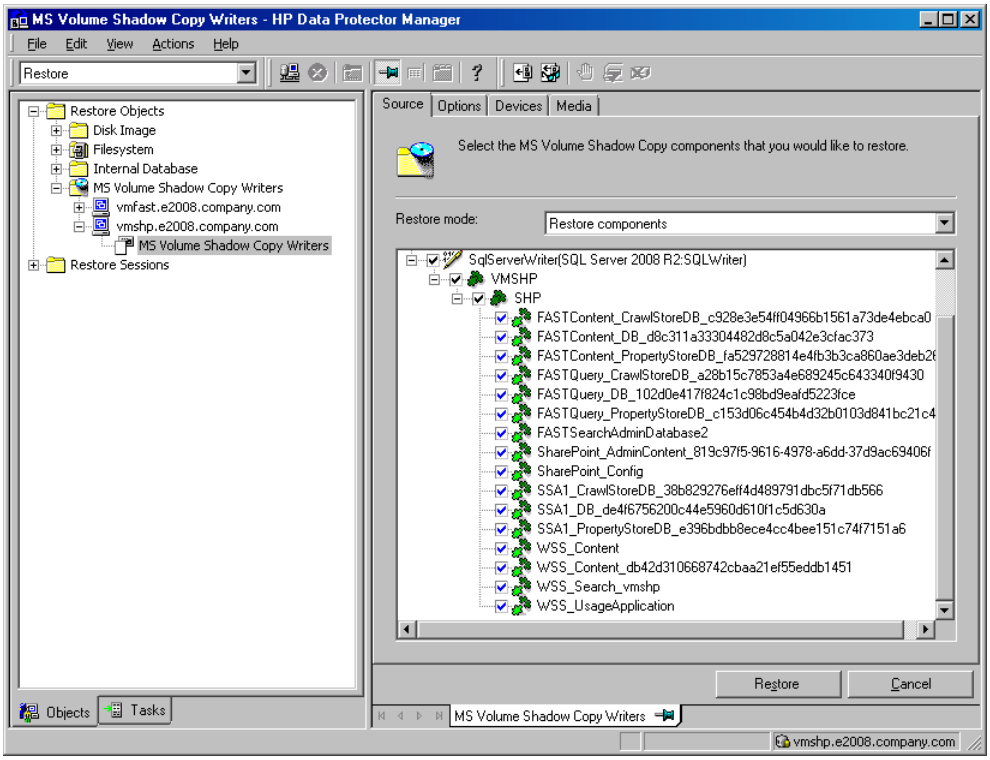
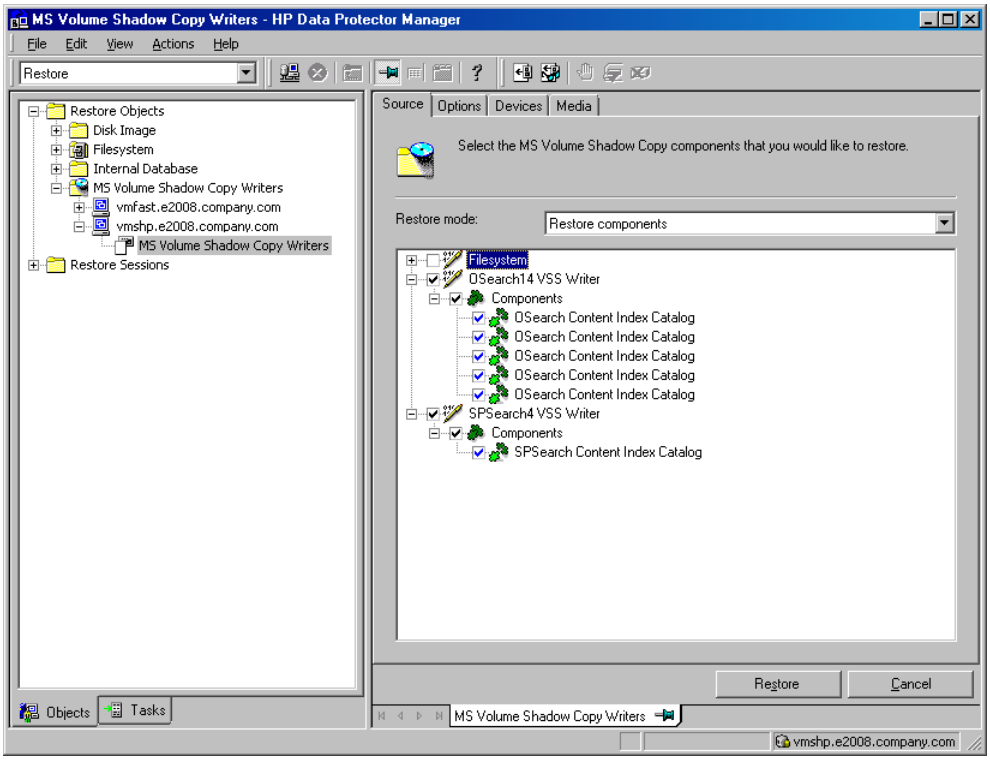


Figure 107 Selecting Microsoft Office SharePoint Server 2007 Search index files for restore



4. In the Options page, specify the restore options.
5. In the Devices page, select devices to use for restore.
6. Click **Restore**, review your selection, and click **Finish**.

Restoring using the Data Protector CLI

You can restore Microsoft SharePoint Server data using the Data Protector `omnir` command. For details, see the `omnir` man page or the *HP Data Protector Command Line Interface Reference*.

If you specified the `-outfile` option when you ran backup sessions, you can find the necessary `omnir` commands in the specified file. The following is an example of the `omnir` command from such a file.

```
 omnir -vss -barhost SHP-APP
-session 2011/09/25-13
-tree "/SqlServerWriter(SQL Server 2005:SQLWriter)/SHP-APP/master"
-session 2011/09/25-13
-tree "/SqlServerWriter(SQL Server2005:SQLWriter)/SHP-APP/model"
-session 2011/09/25-13
-tree "/SqlServerWriter(SQL Server 2005:SQLWriter/SHP-APP/msdb"
-session 2011/09/25-13
-tree "/SqlServerWriter(SQL Server 2005:SQLWriter)/SHP-APP/
WSS_Content_SSPAdminAccounting"
-session 2011/09/25-13
-tree "/SqlServerWriter(SQL Server 2005:SQLWriter)/SHP-APP/SSP_Accounting"
-session 2011/09/25-13
-tree "/SqlServerWriter(SQL Server 2005:SQLWriter)/
SHP-APP/SSP_Accounting_Search"
```

Limitations

The `omnir` command syntax should not contain more than 8191 characters. If you have so many `-tree` objects that the syntax exceeds 8191 characters, split the objects and run two separate sessions.

After the restore

After the restore:

1. Enable and start the service `IIS Admin Service` (only for IIS 6 on Windows Server 2003, when the whole farm was restored)
2. Enable the service `Office SharePoint Server Search or SharePoint Server Search 14`.
3. Bring the Microsoft SQL Server instances online (if offline).
4. Return the farm to a working state (that is, resume background activities and crawling, unlock sites, and start the Microsoft SharePoint Server services) by executing:

   `SharePoint_VSS_backup.ps1 -resumefarm`

NOTE:

- The command uses the WMI (Windows Management Instrumentation) to remotely start any stopped SharePoint services. Ensure its proper operation by adding an exception to the Windows Default Firewall for `Remote administration`, which adds the WMI ports, or for the WMI directly. For details, see: http://support.microsoft.com/kb/154596.
- If the FAST Search certificates for the content and query connectors are out of sync, you can reinstall them by executing:

  `SharePoint_VSS_backup.ps1 -resumecert`

  Start the command on the Microsoft SharePoint Server system where the `SharePoint Server Search 14` service is enabled.

Restoring index files on the Query system

This section is applicable for Microsoft Office SharePoint Server 2007 only. The `Office SharePoint Server Search` service is enabled on two separate Microsoft Office SharePoint Server 2007 systems, so that one is assigned the `Indexing` and the other the `Query` role.

To copy the newly restored index files from the `Indexing` system to the `Query` system, perform the following steps (depending on which Microsoft Office SharePoint Server 2007 and Windows Shared Services service pack you have):

- **Service Pack 1**
  1. On the `Query` system, stop and disable the service `Office SharePoint Server Search`.
  2. Copy the index files from the `Indexing` to the `Query` system.

     By default, index files are located in the `C:\Program Files\Microsoft Office Servers\12.0\Data\Office Server\Applications` directory.
  3. On the `Query` system, enable and start the service `Office SharePoint Server Search`.
- **Service Pack 2**

  On the `Query` system, execute:

  `stsadm -o search -reprovisionindex -ssp` *`SSPName`*

  for each Shared Services Provider separately.

Troubleshooting

This section lists general checks and verifications, plus problems you might encounter when using the Data Protector Microsoft SharePoint Server VSS based solution.

For Microsoft Volume Shadow Copy troubleshooting information, see the troubleshooting chapter in the *HP Data Protector Integration Guide for Microsoft Volume Shadow Copy Service*.

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. On how to verify this, see the *HP Data Protector 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://support.openview.hp.com/selfsolve/manuals.

Checks and verifications

If your browsing, backup, or restore failed:

- Examine system errors reported in the `debug.log` file.
- Check if you can do a filesystem backup and restore on the problematic client. For information, see the *HP Data Protector Help*.

After restore, you cannot connect to the Central Administration webpage

Problem

After restore, when you try to connect to the Microsoft SharePoint Central Administration webpage, an error similar to the following is displayed in your web browser:

Windows Internet Explorer:

```
Retrieving the COM class factory for component with CLSID
(BDEADEE2-C265-11D0-BCED-00A0C90AB50F) failed due to the following error
800703fa.
```

Mozilla Firefox:

```
An unexpected error has occurred.
```

Action

1. Restart Microsoft SharePoint Server services on all clients in the farm.
2. Open the Internet Information Services (IIS) Manager and restart all application pools.
3. In case an application pool fails to be restarted with the following error:

   ```
   Cannot Restore Application Pool. There was an error while performing
   this operation.
   ```

   wait for a few seconds and then restart the operation.
4. Delete browsing history in your web browser.
5. Log in to the Central Administration webpage.

Backup fails with the error Failed to resume Service Windows SharePoint Services Help Search

Problem

When you start backup sessions, an error similar to the following is displayed:

```
Service Windows SharePoint Services Help Search on host
MOSS07-INDEX
-> Resuming background activity ...
ERROR: Failed to resume Service Windows SharePoint Services Help Search
on host MOSS07-INDEX
Web site URL: http://moss07-web:2001
Root title: as
-> Resuming background activity
```

Action

Execute:

```
SharePoint_VSS_backup.ps1-resumefarm
```

After restore, a quiesce operation fails

Problem

After you have restored the configuration database and executed `SharePoint_VSS_backup.ps1-resumefarm`, the data in the Microsoft SharePoint Server file system caches on front-end Web Server systems is not consistent with the data in the newly-restored configuration database. When you try to quiesce the farm, the operation fails with the following error:

```
An unhandled exception occurred in the user interface. Exception
Information: An update conflict has occurred, and you must re-try
this action. The object SessionStateService Parent=SPFarm Name=<
farm_config_database_name > is being updated by < domain\username
>, in the w3wp process, on machine < servername >. View the tracing
 log for more information about the conflict.
```

Action

Clear the Microsoft Office SharePoint Server file system cache on all server systems in the farm. For details, see:

http://support.microsoft.com/kb/939308.

After restore, you cannot connect to the FAST Search Server

Problem

After restore, when you try to connect to the Microsoft FAST Search Server 2010 system for SharePoint, the operation fails.

FAST Query SSA search operations display an error similar to the following:

```
The search request was unable to connect to the Search Service.
```

Action

Execute:

```
SharePoint_VSS_backup.ps1 -resumecert
```

NOTE: The VSS based solution copies the FAST Search certificate `FASTSearchCert.pfx` from the FAST Admin Server system to the SharePoint Server system and installs it. Also, the SharePoint certificate is copied and installed to each FAST Search Server system. For details, see: http://technet.microsoft.com/en-us/library/ff381244.aspx.

The SharePoint_VSS_backup.ps1 script stops responding and the farm stays in read only mode

Problem

When starting a back up, the `SharePoint_VSS_backup.ps1` script stops responding when a crawl of the Microsoft SharePoint Server is being performed. The issue can appear due to external conditions such as a corrupted SSA index, the need to reissue the certificate manually and so on.

As a result, the farm stays in read-only mode.

Action

Normally, the crawl should be aborted automatically after 15 minutes. If this does not happen:

1. Abort the script by pressing **Ctrl-C**.
2. Manually resume the farm.

You can specify a different timeout after which the crawl is aborted and the farm is resumed by using the `-timeout` option.

A Appendix

This appendix contains information on the following topics:

- Reconfiguring an Oracle instance for instant recovery
- ZDB integrations omnirc options

Reconfiguring an Oracle instance for instant recovery

If the control files or redo logs are located on the same volume group (if LVM is used) or source volume as the database files, the control files and online redo logs are overwritten during instant recovery. In such case, you may want to reconfigure the Oracle instance. For details on the required configuration, see "Oracle backup set ZDB concepts" (page 24) and to "Oracle proxy-copy ZDB concepts" (page 28). For additional examples on how to move the redo logs and control files, see "Examples for moving the control files and redo logs to different locations " (page 253).

Moving online redo logs

To move the *online redo log files* from the source volumes to be replicated, to other locations:

1. List the online redo log files:

   ```
   $ sqlplus
   SQL> select member from v$logfile;
   ```

2. Shut down the database:

   ```
   SQL> connect user/password@service as sysdba;
   SQL> shutdown
   SQL> exit
   ```

3. Move the log files to a different location using operating system tools.
4. Start the database in mount mode:

   ```
   $ sqlplus
   SQL> connect user/password@service as sysdba;
   SQL> startup mount;
   ```

5. Register the new locations for each moved file:

   ```
   SQL> alter database rename file 'OldPathName' to 'NewPathName';
   ```

   where *OldPathName* and *NewPathName* are full paths to the log file.

6. Open the database in normal mode:

   ```
   SQL> alter database open;
   ```

Moving control files

To move the *control files* from the source volumes to be replicated, to other locations:

1. Determine if the database uses the SPFILE parameter:

   ```
   SQL> show parameter SPFILE
   ```

2. If the database does not use SPFILE:
   a. Shut down the database.

      ```
      SQL> shutdown
      ```

   b. Move the control files to a different location using operating system tools.

c. Edit the CONTROL_FILES parameter in the database's initialization parameter file (usually located in the $ORACLE_HOME/dbs/init*SID*.ora directory) to change the existing control file names:

```
control_files = ("NewPathName", ...)
```

d. Restart the database:

```
SQL> startup
```

If the database uses SPFILE:

a. Specify the new location for control files by running the following command:

```
SQL> alter system set control_files='NewPathName1',
'NewPathName2',..., scope=spfile
```

b. Shut down the database.

```
SQL> shutdown
```

c. Move the control files to a different location.

d. Restart the database:

```
SQL> startup
```

Examples for moving the control files and redo logs to different locations

Example - moving online redo logs

In the following example for Oracle10g on HP-UX, the data files are on the same source volume as the control files and redo logs, which is /opt/oracle/product/10.2.0.

To move the *online redo log files* from /opt/oracle/product/10.2.0 to /oracle/logs (which is not replicated):

1. List the online redo log files:

```
$ sqlplus
SQL> select member from v$logfile;
/opt/oracle/product/10.2.0/oradata/redo01.log
/opt/oracle/product/10.2.0/oradata/redo02.log
/opt/oracle/product/10.2.0/oradata/redo03.log
```

List the filenames and tablespaces to check whether they are on the same source volumes as the control files:

```
SQL> select FILE_NAME,TABLESPACE_NAME,BYTES from dba_data_files;
FILE_NAME
------------------------------------------------------------
TABLESPACE_NAME                BYTES
------------------------------ ----------
/opt/oracle/product/10.2.0/oradata/system01.dbf
SYSTEM                         419430400
/opt/oracle/product/10.2.0/oradata/undotbs01.dbf
UNDOTBS1                       377487360
/opt/oracle/product/10.2.0/oradata/cwmlite01.dbf
CWMLITE                         20971520
```

2. Shut down the database:

```
SQL> connect user/password@service as sysdba;
SQL> shutdown
SQL> exit
```

3. Move the log files to a different location.

```
$ mv /opt/oracle/product/10.2.0/oradata/redo* /oracle/logs
```

4. Start the database in mount mode:

```
$ sqlplus
SQL> connect user/ password@service as sysdba;
SQL> startup mount;
```

5. Rename the new locations for each moved file:

```
alter database rename file
'/opt/oracle/product/10.2.0/oradata/redo01.log' to
'/oracle/logs/redo01.log';
Database altered.
alter database rename file
'/opt/oracle/product/10.2.0/oradata/redo02.log' to
'/oracle/logs/redo01.log';
Database altered.
alter database rename file
'/opt/oracle/product/10.2.0/oradata/redo03.log' to
'/oracle/logs/redo01.log';
Database altered.
```

6. Open the database in normal mode:

```
SQL> alter database open;
```

Example - moving control files for Oracle 10g

In the following example, the Oracle 10g database uses SPFILE. To move the control files from `/opt/oracle/product/10.2.0/` to `/oracle/oractl`:

1. Determine if the database uses the SPFILE parameter:

```
SQL> show parameter spfile;
NAME                         TYPE             VALUE
---------------------------- ---------- -------------------
spfile                       string       ?/dbs/spfile@.ora
```

2. Specify the new location for the control files by running the following command (in a single line and without the "\" characters):

```
SQL> alter system setcontrol_files='/oracle/logs/RCVCAT \
/control01.ctl','/oracle/logs/RCVCAT/control02','/oracle \
/logs/RCVCAT/control03.ctl' scope=spfile;
```

3. Shut down the database:

```
SQL> shutdown
```

4. Move the control files to the new location:

```
mv /opt/oracle/product/10.2.0/oradata/control* /oracle/oractl
```

5. Restart the database:

```
SQL> startup
```

ZDB integrations omnirc options

The Data Protector ZDB integrations use options, which can be set in the `/opt/omni/.omnirc` (on UNIX systems) or *`Data_Protector_home`*`\omnirc` file (on Windows systems), on both the application and backup systems. These options are used for Data Protector ZDB integrations customizing. See the *HP Data Protector Help* index: "omnirc options" for information on how to use the `omnirc` file.

For information on Data Protector ZDB agents omnirc file options, see the *HP Data Protector Zero Downtime Backup Administrator's Guide*.

This section explains the omnirc file options that can be set for the Data Protector ZDB integrations.

ZDB_ORA_INCLUDE_CF_OLF: Data Protector Oracle Server integration and Data Protector SAP R/3 integration-related options.

NOTE: This option is not supported on EMC.

The default value is `0`. Possible values are `0` and `1`.

If an offline backup is performed using the Data Protector SAP R/3 integration, the option is ignored and the integration behaves as if the option was set to `1`.

Instant recovery

The instant recovery process depends on whether the control file and redo logs reside on the same disk array source volume as datafiles or not:

- If this option is set to `0` (default), during a ZDB session, Data Protector creates target volumes only for the source volumes containing Oracle datafiles. Target volumes for source volumes containing Oracle control file and Oracle online redo logs are not created.

  For Oracle proxy-copy or backup set ZDB and restore concepts when this option is set to `0`, see "Oracle backup set ZDB concepts" (page 24) and "Oracle proxy-copy ZDB concepts" (page 28). For SAP R/3 backup and restore concept when this option is set to `0`, see "Integration concepts" (page 107).

- If this option is set to `1`, Data Protector creates target volumes for all source volumes containing Oracle datafiles, Oracle control file, and if Oracle integration is used, Oracle online redo logs.

IMPORTANT: If the `ZDB_ORA_INCLUDE_CF_OLF` option is set to `1` the control files and redo logs are overwritten during instant recovery.

Opening the database on the backup system

To successfully open the database on the backup system for *other* purposes than Data Protector, note:

- With Oracle proxy-copy ZDB method, set this option to `1`.
- With Oracle backup set ZDB method, used with the Oracle integration, you can always open the database on the backup system.

Prerequisites

The prerequisites for this option to be set to `1` are:

- Data Protector Oracle Server integration: Oracle datafiles, Oracle control file, and Oracle online redo logs must be installed on a disk array.
- Data Protector SAP R/3 integration: Oracle datafiles and Oracle control file must be installed on a disk array.

See "Oracle proxy-copy ZDB and restore concepts when the ZDB_ORA_INCLUDE_CF_OLF option is set to 1" (page 256) and "Oracle backup set ZDB and restore concept when the ZDB_ORA_INCLUDE_CF_OLF option is set to 1 " (page 256) for Oracle backup and restore concepts when this option is set to `1`. See "SAP R/3 backup and restore concept when the ZDB_ORA_INCLUDE_CF_OLF option is set to 1 with online backup, or in case of offline backup" (page 257) for SAP R/3 backup and restore concepts when this option is set to `1`.

Figure 108 Oracle proxy-copy ZDB and restore concepts when the ZDB_ORA_INCLUDE_CF_OLF option is set to 1

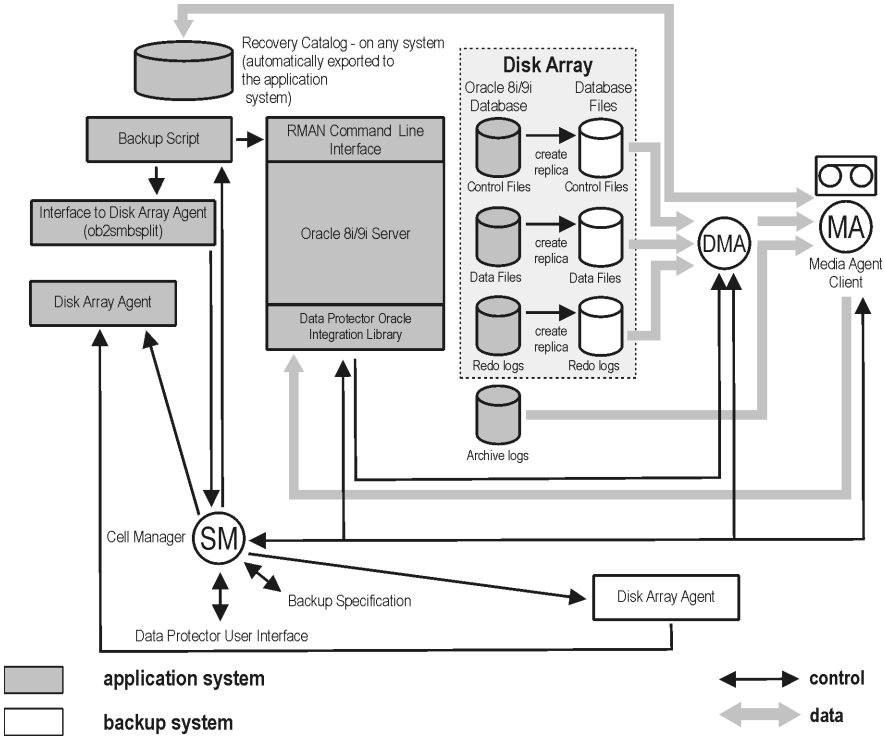


Figure 109 Oracle backup set ZDB and restore concept when the ZDB_ORA_INCLUDE_CF_OLF option is set to 1

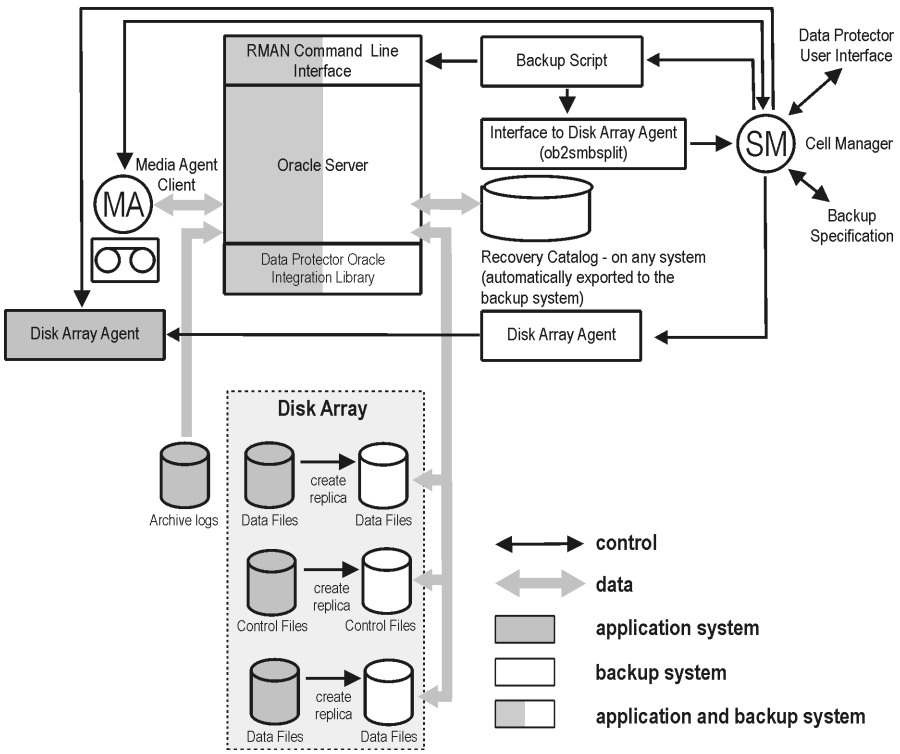
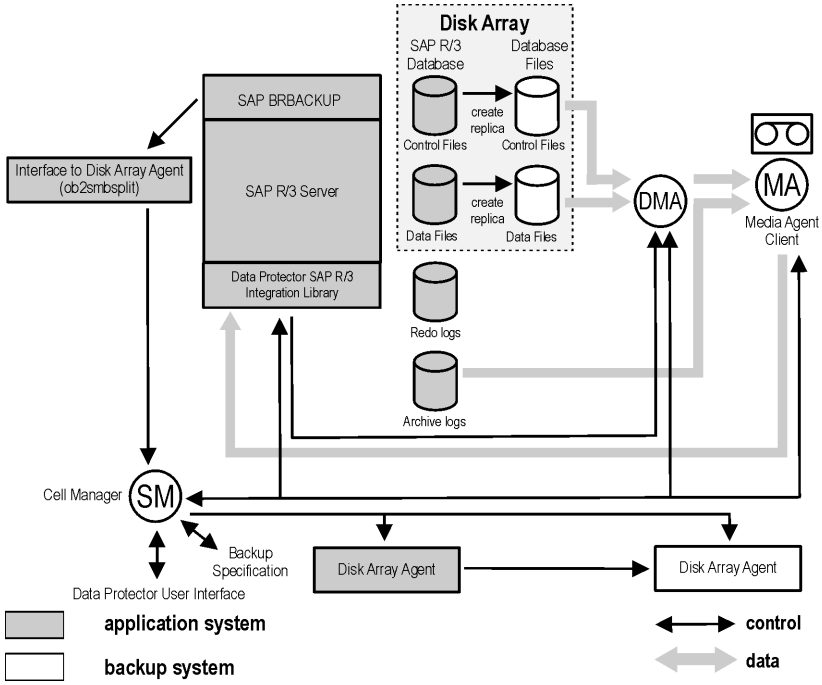


Figure 110 SAP R/3 backup and restore concept when the ZDB_ORA_INCLUDE_CF_OLF option is set to 1 with online backup, or in case of offline backup



ZDB_ORA_INCLUDE_SPF: Data Protector Oracle Server integration-related options.

The default value is `0`. Possible values are `0` and `1`.

The option is ignored and the integration behaves as if the option was set to `1` if offline backup is performed using the Data Protector SAP R/3 integration.

If this option is set to `0`, during ZDB sessions, Data Protector checks if Oracle Server datafiles and the Oracle Server SPFILE are located on the same source volume. If the datafiles and the SPFILE are located on the same volume and instant recovery is enabled in the backup specification, the ZDB session fails. If this option is set to `1`, Data Protector skips the check. To enable instant recovery, leave this option set to the default value.

△ **CAUTION:** If this option is set to `1` and the datafiles are located on the same volume as the SPFILE, the SPFILE is overwritten during instant recovery, potentially resulting in a data loss.

ZDB_ORA_NO_CHECKCONF_IR: Data Protector Oracle Server integration-related option.

The default value is `0`. Possible values are `0` and `1`.

By default, the Oracle Server configuration is checked whether it is instant recovery-enabled or not (whether the Oracle control file, the Oracle Server SPFILE, and the Oracle Server online redo logs are located on volumes of a different volume group than Oracle Server datafiles or not). For Oracle Server configuration check, the Data Protector command `omniresolve` is used internally. On UNIX systems, the `omniresolve` file must have the `setuid` bit set. When this option is set to `1`, the configuration check is omitted.

△ **CAUTION:** Checking the Oracle Server configuration for instant recovery suitability is an essential step to ensure the instant recovery session does not result in a data loss. It is therefore not recommended to set this option to 1 unless you ensure that the Oracle Server is and remains configured appropriately for instant recovery.

OB2MARAWREAD_KB: This option sets the read block size for Oracle and SAP R/3 ZDB integrations on UNIX systems with Oracle tablespaces or datafiles installed on disk images and when using the proxy-copy method (when using DMA).

The default value is 64 kB. The specified value must be in the range between 1 kB and 1 MB.

The specified size is automatically adjusted to a size which is a multiple of the block size. The values above 256 kB could cause the DMA to fail.

ZDB_TAKE_CLUSRES_ONLINE: This option specifies how many times Data Protector tries to connect to Microsoft SQL Server in case the first connection fails. A reconnection is triggered every 30 seconds. This means that Data Protector waits up to *ZDB_TAKE_CLUSRES_ONLINE* x 30 seconds for the Microsoft SQL Server resources to start up.

SSEA_ATOMIC_SPLIT: Determines if the Data Protector HP P9000 XP Agent should use the atomic split configuration of a disk array of the HP P9000 XP Disk Array Family to ensure data consistency of replicas of the Oracle Server data in configurations where Automatic Storage Management (ASM) is used.

Default: 0 (disabled). Possible: 0| 1.

Glossary

A

access rights — *See* user rights.

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

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

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

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

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

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

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

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

archived log files — *(Data Protector specific term)* Files that keep track of changes made to the Data Protector Internal Database (IDB). They are used for online and offline IDB restore and recovery where the IDB needs to be recreated either in its latest possible state, beyond the time of the most recent IDB backup session, or in a state between the times of two consecutive IDB backup sessions.

archived redo log — *(Oracle specific term)* Also called offline redo log. If the Oracle database operates in the ARCHIVELOG mode, as each online redo log is filled, it is copied to an archived log destination. This copy is the archived redo log. The presence or absence of an archived redo log is determined by the mode the database is using:

- ARCHIVELOG - The filled online redo log files are archived before they are reused. The database can be recovered if an instance or a disk fails. A "hot" backup can be performed only when the database is running in this mode.
- NOARCHIVELOG - The filled online redo log files are not archived.

See also online redo log.

ASR set — A collection of files stored on several diskettes, required for proper reconfiguration of the replacement disk (disk partitioning and logical volume configuration) and automatic recovery of the original system configuration and user data that was backed up during the full client backup. These files are stored as an ASR archive file on the Cell Manager in the directory *Data_Protector_program_data*`\Config\Server\dr\asr` (Windows systems) or `/etc/opt/omni/server/dr/asr` (UNIX systems) as well as on the backup medium. After a disaster occurs, the ASR archive file is extracted to diskettes which you need to perform ASR.

audit logs — Data files to which auditing information is stored.

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

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

autochanger — *See* library.

autoloader — *See* library.

Automatic Storage Management (ASM) *(Oracle specific term)* A filesystem and volume manager integrated into Oracle which manages Oracle database files. It eliminates complexity associated with data and disk management and optimizes performance by providing striping and mirroring capabilities.

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

B

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

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

backup chain *See* restore chain.

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

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

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

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

A backup object is defined by:

- Client name: Hostname of the Data Protector client where the backup object resides.
- Mount point: For filesystem objects — the access point in a directory structure on the client where the backup object is located (drive on Windows systems and mount point on UNIX systems). For integration objects — backup stream identification, indicating the backed up database/application items.
- Description: For filesystem objects — uniquely defines objects with identical client name and mount point. For integration objects — displays the integration type (for example, SAP or Lotus).
- Type: Backup object type. For filesystem objects — filesystem type (for example, WinFS). For integration objects — "Bar".

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

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

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

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

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

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

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

backup view Data Protector provides different views for backup specifications:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

C

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

Catalog Database (CDB) A part of the Data Protector Internal Database (IDB) that contains information about backup, restore, object copy, object consolidation, object verification, and media management sessions. This part of the IDB is always local to the cell. It is stored in the embedded database.
See also MMDB.

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

CDB *See* Catalog Database (CDB).

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

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

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

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

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

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

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

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

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

- type 'disk'
- type 'sbt_tape'

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

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

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

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

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

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

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

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

See also Exchange Replication Service and local continuous replication.

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

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

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

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

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

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

concurrency *See* Disk Agent concurrency.

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

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

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

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

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

D

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

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

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

data stream Sequence of data transferred over the communication channel.

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

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

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

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

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

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

DC directory A directory that contains DC binary files, one for each configured Data Protector backup medium. DC directories constitute the Detail Catalog Binary Files part of the Data Protector Internal Database.
See also Detail Catalog Binary Files (DBCF) and Internal Database (IDB).

DCBF *See* Detail Catalog Binary Files (DCBF).

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

Detail Catalog Binary Files (DCBF) A part of the Data Protector Internal Database that stores names, versions, and metadata of the backed up items. It consists of DC directories with DC binary files.
See also DC directory and Internal Database (IDB).

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

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

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

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

	to the tape is less or equal the data rate which can be delivered to the device by the computer system, then the device is streaming. Streaming significantly improves the performance of the device and use of space.
DHCP server	A system running the Dynamic Host Configuration Protocol (DHCP) providing dynamic IP address assignment and network configuration for DHCP clients.
differential backup	An incremental backup that backs up changes made since the last full backup. To perform this type of backup, specify the Incr1 backup type. *See also* incremental backup.
differential backup	*(Microsoft SQL Server specific term)* A database backup that records only the data changes made to the database after the last full database backup. *See also* backup types.
differential database backup	A differential database backup records only those data changes made to the database after the last full database backup.
directory junction	*(Windows specific term)* Directory junctions use the reparse point concept of Windows. An NTFS 5 directory junction allows you to redirect a directory/file request to another location.
disaster recovery	A process to restore a client's main system disk to a state close to the time when a (full) backup was performed.
disaster recovery operating system	*See* DR OS.
Disk Agent	A component needed on a client to back it up and restore it. The Disk Agent controls reading from and writing to a disk. During a backup session, the Disk Agent reads data from a disk and sends it to the Media Agent, which then moves it to the device. During a restore session the Disk Agent receives data from the Media Agent and writes it to the disk. During an object verification session the Disk Agent receives data from the Media Agent and performs the verification process, but no data is written to disk.
Disk Agent concurrency	The number of Disk Agents that are allowed to send data to one Media Agent concurrently.
disk group	*(Veritas Volume Manager specific term)* The basic unit of data storage in VxVM system. A disk group can consist of one or more physical volumes. There can be more than one disk group on the system.
disk image backup	A high-speed backup where Data Protector backs up files as bitmap images. A disk image backup does not track the files and directory structure stored on the disk, but stores a disk image structure on byte level. You can perform a disk image backup of either specific disk sections or a complete disk.
disk quota	A concept to manage disk space consumption for all or a subset of users on a computer system. This concept is used by several operating system platforms.
disk staging	The process of backing up data in several phases to improve the performance of backups and restores, reduce costs of storing the backed up data, and increase the data availability and accessibility for restore. The backup stages consist of backing up data to one media type first (for example disk) and later copying it to a different media type (for example tape).
distributed file media format	A media format, available with the file library, which supports a space efficient type of synthetic backup called virtual full backup. Using this format is a prerequisite for virtual full backup. *See also* virtual full backup.
Distributed File System (DFS)	A service that connects file shares into a single namespace. The file shares can reside on the same or on different computers. DFS provides client access to the resources in a location-transparent manner.
DMZ	The Demilitarized Zone (DMZ) is a network inserted as a "neutral zone" between a company's private network (intranet) and the outside public network (Internet). It prevents outside users from getting direct access to company servers in the intranet.
DNS server	In the DNS client-server model, this is the server containing information about a portion of the DNS database that makes computer names available to client resolvers querying for name resolution across the Internet.

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

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

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

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

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

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

E

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

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

encrypted control communication Data Protector secure communication between the clients in the Data Protector cell is based on Secure Socket Layer (SSL) that uses SSLv3 algorithms to encrypt control communication. Control communication in a Data Protector cell is all communication between Data Protector processes, except the data transfer from Disk Agent (and Integrations) to Media Agent, and the other way round.

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

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

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

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

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

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

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

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

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

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

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

F

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

failover *(HP P6000 EVA Disk Array Family specific term)* An operation that reverses the roles of source and destination in HP Continuous Access + Business Copy (CA+BC) P6000 EVA configurations.
See also HP Continuous Access + Business Copy (CA+BC) P6000 EVA.

FC bridge *See* Fibre Channel bridge.

Fibre Channel An ANSI standard for high-speed computer interconnection. Using either optical or copper cables, it allows the high speed bi-directional transmission of large data files and can be deployed between sites kilometers apart. Fibre Channel connects nodes using three physical topologies: point-to-point, loop, and switched.

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

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

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

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

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

file tree walk *(Windows specific term)* The process of traversing a filesystem to determine which objects have been created, modified, or deleted.

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

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

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

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

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

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

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

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

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

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

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

G

global options A set of options that define behavior of the entire Data Protector cell. The options are stored in a plain text file on the Cell Manager

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

GUI A graphical user interface provided by Data Protector for easy access to all configuration, administration, and operation tasks. It is available for Microsoft Windows operating systems.

H

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

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

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

Holidays file A file that contains information about holidays. You can set different holidays by editing the Holidays file on the Cell Manager in the directory `Data_Protector_program_data\Config\Server\holidays` (Windows systems), or `/etc/opt/omni/server/Holidays` (UNIX systems).

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

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

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

HP Business Copy (BC) P9000 XP

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

HP Command View (CV) EVA

(HP P6000 EVA Disk Array Family specific term) The user interface that enables you to configure, manage, and monitor your P6000 EVA storage system. It is used to perform various storage management tasks, for example, creating virtual disk families, managing storage system hardware, and creating snapshots, snapclones, and mirrorclones of virtual disks. The HP Command View EVA software runs on the HP Storage Management Appliance, and is accessed by a Web browser.
See also HP P6000 / HP 3PAR SMI-S Agent and HP SMI-S P6000 EVA Array provider.

HP Continuous Access (CA) P9000 XP

(HP P9000 XP Disk Array Family specific term) An HP P9000 XP Disk Array Family configuration that enables creation and maintenance of remote copies of LDEVs for purposes such as data duplication, backup, and disaster recovery. HP CA P9000 XP operations involve main (primary) disk array units and remote (secondary) disk array units. The main disk array units are connected to the application system and contain primary volumes (P-VOLs), which store original data. The remote disk array units are connected to the backup system and contain secondary volumes (S-VOLs).
See also HP Business Copy (BC) P9000 XP, Main Control Unit, and LDEV.

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

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

HP P6000 / HP 3PAR SMI-S Agent

A Data Protector software module that executes all tasks required for the HP P6000 EVA Disk Array Family integration. With the HP P6000 / HP 3PAR SMI-S Agent, the control over the array is established through an appropriate SMI-S provider, which directs communication between incoming requests and the storage system's native interface.
See also HP Command View (CV) EVA and HP SMI-S P6000 EVA Array provider.

HP P9000 XP Agent

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

HP SMI-S P6000 EVA Array provider

An interface used for controlling HP P6000 EVA Disk Array Family. SMI-S P6000 EVA Array provider runs as a separate service on the HP Storage Management Appliance system and acts as a gateway between incoming requests and HP Command View EVA. With the Data Protector HP P6000 EVA Disk Array Family integration, SMI-S P6000 EVA Array provider accepts standardized requests from the HP P6000 / HP 3PAR SMI-S Agent, communicates with HP Command View EVA for information or method invocation, and returns standardized responses.
See also HP P6000 / HP 3PAR SMI-S Agent and HP Command View (CV) EVA.

I

ICDA

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

IDB

See Internal Database (IDB).

IDB recovery file

A file that maintains information about completed IDB backup sessions and the backup media and backup devices used in them. If available, it significantly simplifies and speeds up offline recovery of the Internal Database in case of a Cell Manager disaster. Its filename is `obdrindex.dat`.

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

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

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

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

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

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

incremental ZDB A filesystem ZDB-to-tape or ZDB-to-disk+tape session in which only changes from the last protected full or incremental backup are streamed to tape.
See also full ZDB.

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

Inet A process that runs on each UNIX system or service that runs on each Windows system in the Data Protector cell. It is responsible for communication between systems in the cell and for starting other processes needed for backup and restore. The Inet service is started as soon as Data Protector is installed on a system. The Inet process is started by the inetd daemon.

Information Store *(Microsoft Exchange Server specific term)* The Microsoft Exchange Server service that is responsible for storage management. Information Store in Microsoft Exchange Server manages two kinds of stores: mailbox stores and public folder stores. A mailbox store consists of mailboxes that belong to individual users. A public folder store contains public folders and messages that are shared among several users.
See also Key Management Service and Site Replication Service.

Informix Server *(Informix Server specific term)* Refers to Informix Dynamic Server.

initializing *See* formatting.

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

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

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

Internal Database (IDB) An entity in Data Protector that keeps information regarding which data was backed up, to which media it was backed up, how and when backup, restore, and other sessions were run, which devices, libraries, and disk arrays are configured, and so on. It stores its data in an embedded database and a collection of proprietary data files which reside on the Cell Manager.
See also DC directory and Detail Catalog Binary Files (DBCF).

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

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

J

jukebox *See* library.

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

K

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

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

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

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

L

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

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

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

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

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

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

for each object in the backup specification. Data Protector will access the devices in the specified order.

local and remote recovery

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

local continuous replication

(Microsoft Exchange Server specific term) Local continuous replication (LCR) is a single-server solution that creates and maintains an exact copy (LCR copy) of a storage group. An LCR copy is located on the same server as the original storage group. When an LCR copy is created, it is kept up to date through change propagation (log replay) technology. The replication feature in LCR guarantees that logs that have not been replicated are not deleted. The implication of this behavior is that running backups in a mode that deletes logs may not actually free space if replication is sufficiently far behind in its log copying.

An LCR copy is used for disaster recovery because you can switch to the LCR copy in a few seconds. If an LCR copy is used for backup and if it is located on a different disk than the original data, then the I/O load on a production database is minimal.

A replicated storage group is represented as a new instance of Exchange writer called Exchange Replication Service and can be backed up (using VSS) as a normal storage group.

See also cluster continuous replication and Exchange Replication Service.

lock name

You can configure the same physical device several times with different characteristics, by using different device names. The lock name is a user specified string that is used for locking all such device configurations to prevent collision if several such devices (device names) are used concurrently. Use an identical lock name for all device definitions which use the same physical device.

log_full shell script

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

logging level

An option that determines the amount of details on files and directories written to the IDB during backup, object copying, or object consolidation. You can always restore your data, regardless of the logging level used during backup. Data Protector provides four logging levels: Log All, Log Directories, Log Files, and No Log. The different logging level settings mainly influence the IDB growth and the convenience of browsing data for restore.

logical-log files

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

login ID

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

login information to the Oracle Target Database

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

- *`user_name`* is the name by which a user is known to Oracle Server and to other users. Every user name is associated with a password and both have to be entered to connect to an Oracle Target Database. This user must have Oracle SYSDBA or SYSOPER rights.
- *`password`* must be the same as the password specified in the Oracle password file (`orapwd`), which is used for authentication of users performing database administration.
- *`service`* is the name used to identify an SQL*Net server process for the target database.

login information to the Recovery Catalog Database

(Oracle specific term) The format of the login information to the Recovery (Oracle) Catalog Database is *`user_name`*`/`*`password`*`@`*`service`*, where the description of the user name, password, and service name is the same as in the Oracle SQL*Net V2 login information to the

Oracle target database. In this case, *service* is the name of the service to the Recovery Catalog Database, not the Oracle target database.

Note that the Oracle user specified here must be the owner of the Oracle Recovery Catalog.

Lotus C API *(Lotus Domino Server specific term)* An interface for the exchange of backup and recovery information between Lotus Domino Server and a backup solution, like Data Protector.

LVM A Logical Volume Manager is a subsystem for structuring and mapping physical disk space to logical volumes on UNIX systems. An LVM system consists of several volume groups, where each volume group has several volumes.

M

Magic Packet *See* Wake ONLAN.

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

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

Main Control Unit (MCU) *(HP P9000 XP Disk Array Family specific term)* An HP P9000 XP Disk Array Family unit that contains primary volumes (P-VOLs) for the HP CA P9000 XP or HP CA+BC P9000 XP configuration and acts as a master device.
See also HP Business Copy (BC) P9000 XP, HP Continuous Access (CA) P9000 XP, and LDEV.

maintenance mode An operating mode you can initiate on the Cell Manager to prevent changes in the Internal Database. It enables you to perform various maintenance tasks, such as upgrading and patching the Data Protector installation.

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

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

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

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

MCU *See* Main Control Unit (MCU).

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

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

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

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

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

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

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

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

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

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

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

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

merging This defines one mode to resolve file conflicts during restore. If the file to be restored already exists at the destination, the one with the more recent modification date is kept. Files not present on the disk are always restored.
See also overwrite.

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

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

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

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

mirror *(EMC Symmetrix and HP P9000 XP Disk Array Family specific term)* *See* target volume.

mirror rotation *(HP P9000 XP Disk Array Family specific term)* *See* replica set rotation.

mirror unit (MU) number *(HP P9000 XP Disk Array Family specific term)* A non-negative integer number that determines a secondary volume (S-VOL) of an internal disk (LDEV) located on a disk array of the HP P9000 XP Disk Array Family.
See also first-level mirror.

mirrorclone *(HP P6000 EVA Disk Array Family specific term)* A dynamic replica of a storage volume, which is kept updated with changes made to the original storage volume via a local replication link. Replication between the original storage volume and its mirrorclone can be suspended. For each storage volume, a single mirrorclone can be created on the disk array.

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

MMDB The Media Management Database (MMDB) is a part of the IDB that contains information about media, media pools, devices, libraries, library drives, and slots configured in the cell, as well as the Data Protector media used for backup. In an enterprise backup environment, this part of the database can be common to all cells.
See also CMMDB and Catalog Database (CDB).

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

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

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

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

multisnapping *(HP P6000 EVA Disk Array Family specific term)* Simultaneous creation of target volumes so that the backup data is consistent not only on each individual target volume, but also across all the volumes that constitute a snapshot.
See also snapshot.

O

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

obdrindex.dat *See* IDB recovery file.

object *See* backup object.

object consolidation The process of merging a restore chain of a backup object, consisting of a full backup and at least one incremental backup, into a new, consolidated version of this object. The process is a part of the synthetic backup procedure. The result is a synthetic full backup of the specified backup object.

object consolidation session A process that merges a restore chain of a backup object, consisting of a full backup and at least one incremental backup, into a new, consolidated version of this object.

object copy A copy of a specific object version that is created during an object copy session or a backup session with object mirroring.

object copy session A process that creates an additional copy of the backed up data on a different media set. During an object copy session, the selected backed up objects are copied from the source to the target media.

object copying The process of copying selected object versions to a specific media set. You can select object versions from one or several backup sessions to be copied.

object ID *(Windows specific term)* The object IDs (OIDs) enable access to NTFS 5 files no matter where in the system the files reside. Data Protector treats the OIDs as alternate streams of the files.

object mirror A copy of a backup object created using object mirroring. Object mirrors are often referred to as object copies.

object mirroring The process of writing the same data to several media sets during a backup session. Data Protector enables you to mirror all or some backup objects to one or more media sets.

object verification The process of verifying the data integrity of backup objects, from the Data Protector point of view, and the ability of Data Protector to deliver them to the required destination. The process can be used to provide a level of confidence in the ability to restore object versions created by backup, object copy, or object consolidation sessions.

object verification session A process that verifies the data integrity of specified backup objects or object versions and the ability of selected Data Protector network components to deliver them to a specified host. Object verification sessions can be run interactively, or as specified in automated post-backup, or scheduled specifications.

offline backup A backup during which an application database cannot be used by the application. In an offline backup session, the database is generally put into a quiescent state that allows use by the backup system, but not the application, for the time period of the data replication process. For instance, for backup to tape, until streaming of data to the tape is finished. Normal database operation is resumed before potential post-backup operations are started.
See also zero downtime backup (ZDB) and online backup.

offline recovery Offline recovery is performed if the Cell Manager is not accessible, for example, due to network problems. Only standalone and SCSI library devices can be used for offline recovery. Cell Manager can only be recovered offline.

offline redo log *See* archived redo log.

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

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

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

online backup A backup performed while a database application remains available for use. The database is placed into a special backup mode of operation for the time period of the data replication process. For instance, for backup to tape, until streaming of data to tape is finished. During this period, the database is fully operational, but there may be a small performance impact and log files may grow very quickly. Normal database operation is resumed before potential post-backup operations are started.

In some cases, transaction logs may also have to be backed up to allow a consistent database to be restored.

See also zero downtime backup (ZDB) and offline backup.

online recovery A type of the Internal Database recovery that you can use when the Cell Manager is accessible. In this case, the Cell Manager runs sessions, the sessions are logged into the IDB, and you can monitor the session progress using the GUI.

online redo log *(Oracle specific term)* Redo logs that have not been archived, but are either available to the instance for recording database activity or are filled and waiting to be archived or reused.
See also archived redo log.

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

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

ORACLE_SID *(Oracle specific term)* A unique name for an Oracle Server instance. To switch among Oracle Servers, specify the desired *`ORACLE_SID`*. The *`ORACLE_SID`* is included in the CONNECT DATA

parts of the connect descriptor in a `TNSNAMES.ORA` file and in the definition of the TNS listener in the `LISTENER.ORA` file.

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

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

ownership Backup ownership affects the ability of users to see and restore data. Each backup session and all the data backed up within it is assigned an owner. The owner can be the user that starts an interactive backup, the account under which the CRS process is running, or the user specified as the owner in the backup specification options.

If a user starts an existing backup specification without modifying it, the backup session is not considered as interactive.

If a modified backup specification is started by a user, the user is the owner unless the following is true:

- The user has the Switch Session Ownership user right.
- The backup session owner is explicitly defined in the backup specification, where the username, group or domain name, and the system name are specified.

If a backup is scheduled on a UNIX Cell Manager, the session owner is root:sys unless the above conditions are true.

If a backup is scheduled on a Windows Cell Manager, the session owner is the user specified during the installation, unless the above conditions are true.

When copying or consolidating backup objects, the owner of the resulting objects is the user who started the original backup session.

P

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

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

pair status *(HP P9000 XP Disk Array Family specific term)* The status of a disk pair (secondary volume and its corresponding primary volume) of a disk array of the HP P9000 XP Disk Array Family. Depending on the circumstances, the paired disks can be in various states. The following states are particularly important for the operation of the Data Protector HP P9000 XP Agent:

- PAIR – The secondary volume is prepared for zero downtime backup. If it is a mirror, it is completely synchronized, and if it is a volume to be used for snapshot storage, it is empty.
- SUSPENDED – The link between the disks is suspended. However, the pair relationship is still maintained, and the secondary disk can be prepared for zero downtime backup again at a later time.
- COPY – The disk pair is currently busy and making a transition into the PAIR state. If the secondary volume is a mirror, it is re-synchronizing with the primary volume, and if it is a volume to be used for snapshot storage, its contents are getting cleared.

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

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

phase 0 of disaster recovery Preparation for disaster recovery - the prerequisite condition for a successful disaster recovery.

phase 1 of disaster recovery Installation and configuration of DR OS, establishing previous storage structure.

phase 2 of disaster recovery Restoration of operating system (with all the configuration information that defines the environment) and Data Protector.

phase 3 of disaster recovery Restoration of user and application data.

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

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

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

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

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

primary volume (P-VOL) *(HP P9000 XP Disk Array Family specific term)* An internal disk (LDEV) of a disk array of the HP P9000 XP Disk Array Family for which a secondary volume (S-VOL), either its mirror or a volume to be used for its snapshot storage, exists. In the HP CA P9000 XP and HP CA+BC P9000 XP configurations, primary volumes are located in the Main Control Unit (MCU).
See also secondary volume (S-VOL) and Main Control Unit (MCU).

protection *See* data protection and also catalog protection.

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

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

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

R

RAID Redundant Array of Independent Disks.

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

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

rawdisk backup *See* disk image backup.

RCU *See* Remote Control Unit (RCU).

RDBMS Relational Database Management System.

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

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

- The physical schema of the Oracle target database
- Data file and archived log backup sets
- Data file copies
- Archived redo Logs
- Stored scripts

Recovery Catalog Database *(Oracle specific term)* An Oracle database that contains a recovery catalog schema. You should not store the recovery catalog in your target database.

recovery files *(Oracle specific term)* Recovery files are Oracle specific files that reside in the flash recovery area: the current control file, online redo logs, archived redo logs, flashback logs, control file autobackups, datafile copies, and backup pieces.
See also flash recovery area.

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

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

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

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

Remote Control Unit (RCU) *(HP P9000 XP Disk Array Family specific term)* An HP P9000 XP Disk Array Family unit that acts as a slave device to the Main Control Unit (MCU) in the HP CA P9000 XP or HP CA+BC P9000 XP configuration. In bidirectional configurations, the RCU can also act as an MCU.

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

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

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

See also snapshot, snapshot creation, split mirror, and split mirror creation.

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

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

restore chain Backup images that are needed to restore a backed up object to the state it was in at the selected point in time. In general, a restore chain of an object consists of its full backup image and one or more related incremental backup images.

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

resync mode *(HP P9000 XP Disk Array Family VSS provider specific term)* One of two P9000 XP Array VSS hardware provider operation modes. When the P9000 XP Array provider is in the resync mode, the source volume (P-VOL) and its replica (S-VOL) are in the suspended mirror relationship after a backup. The maximum number of replicas (S-VOLs per a P-VOL) rotated is three provided that MU range is 0-2 or 0, 1, 2. Restore from a backup in such a configuration is possible only by re-synchronization of an S-VOL with its P-VOL.
See also VSS compliant mode, source volume, primary volume (P-VOL), replica, secondary volume (S-VOL), mirror unit (MU) number, and replica set rotation.

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

RSM The Data Protector Restore Session Manager controls restore and object verification sessions. This process always runs on the Cell Manager system.

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

S

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

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

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

secondary volume (S-VOL) *(HP P9000 XP Disk Array Family specific term)* An internal disk (LDEV) of a disk array of the HP P9000 XP Disk Array Family which is paired with another LDEV: a primary volume (P-VOL). It can act as a mirror of the P-VOL or as a volume to be used for the P-VOL's snapshot storage. An S-VOL is assigned a SCSI address different from the one used for the P-VOL. In an HP CA P9000 XP configuration, the S-VOLs acting as mirrors can be used as failover devices in a MetroCluster configuration.
See also primary volume (P-VOL) and Main Control Unit (MCU).

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

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

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

shadow copy *(Microsoft VSS specific term)* A volume that represents a duplicate of the original volume at a certain point in time. The data is then backed up from the shadow copy and not from the original

volume. The original volume continues to change as the backup process continues, but the shadow copy of the volume remains constant.
See also Microsoft Volume Shadow Copy Service and replica.

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

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

shared disks A Windows disk on another system that has been made available to other users on the network. Systems with shared disks can be backed up without a Data Protector Disk Agent installed.

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

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

SMB *See* split mirror backup.

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

SMI-S Agent (SMISA) *See* HP P6000 / HP 3PAR SMI-S Agent.

snapshot *(HP P4000 SAN Solutions, HP P6000 EVA Disk Array Family, HP P9000 XP Disk Array Family, and HP 3PAR StoreServ Storage specific term)* A type of target volumes created using a specific replication technology. Depending on the disk array model and the chosen replication technique, a range of snapshot types with different characteristics is available. Basically, each snapshot may be either a virtual copy, still reliant upon the contents of the source volume, or an independent duplicate (clone) of the source volume.
See also replica and snapshot creation.

snapshot backup *See* ZDB to tape, ZDB to disk, and ZDB to disk+tape.

snapshot creation *(HP P4000 SAN Solutions, HP P6000 EVA Disk Array Family, HP P9000 XP Disk Array Family, and HP 3PAR StoreServ Storage specific term)* A replica creation process in which copies of the selected source volumes are created using storage virtualization technology. Such a replica is considered to be created at a particular point in time, and is immediately available for use. However, with certain snapshot types, a background data copying process continues to run on the disk array after the moment of the replica creation.
See also snapshot.

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

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

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

split mirror *(EMC Symmetrix Disk Array and HP P9000 XP Disk Array Family specific term)* A type of target volumes created using a specific replication technology. A split-mirror replica provides independent duplicates (clones) of the source volumes.
See also replica and split mirror creation.

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

split mirror backup *(HP P9000 XP Disk Array Family specific term)* *See* ZDB to tape, ZDB to disk, and ZDB to disk+tape.

split mirror creation *(EMC Symmetrix and HP P9000 XP Disk Array Family specific term)* A replica creation technique, in which a pre-configured set of target volumes (a mirror) is kept synchronized with a set of source volumes until the time at which a replica of the contents of the source volumes is required. Then, the synchronization is stopped (the mirror is split) and a split mirror replica of the source volumes at the time of the split remains in the target volumes.
See also split mirror.

split mirror restore *(EMC Symmetrix and HP P9000 XP Disk Array Family specific term)* A process in which data backed up in a ZDB-to-tape or a ZDB-to-disk+tape session is first copied from the backup media to a replica, and from the replica to the source volumes afterwards. Individual backup objects or complete sessions can be restored using this method.
See also ZDB to tape, ZDB to disk+tape, and replica.

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

SRD file *(disaster recovery specific term)* A text file in the Unicode (UTF-16) format, generated during CONFIGURATION backup of a Windows or Linux system and stored on the Cell Manager. It contains system information required for installing and configuring the operating system on the target system in the case of a disaster.
See also target system.

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

SSE Agent (SSEA) *See* HP P9000 XP Agent.

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

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

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

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

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

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

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

switchover *See* failover.

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

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

SYMA *See* EMC Symmetrix Agent.

synthetic backup A backup solution that produces a synthetic full backup, an equivalent to a conventional full backup in terms of data, without putting stress on the production servers or the network. A synthetic full backup is created from a previous full backup and any number of incremental backups.

synthetic full backup The result of an object consolidation operation, where a restore chain of a backup objects is merged into a new, synthetic full version of this object. A synthetic full backup is equivalent to a conventional full backup in terms of restore speed.

System Backup to Tape *(Oracle specific term)* An Oracle interface that handles the actions required to load, label, and unload correct backup devices when Oracle issues a backup or restore request.

system databases *(Sybase specific term)* The four system databases on a newly installed Sybase SQL Server are the:

- master database (master)
- temporary database (tempdb)
- system procedure database (sybsystemprocs)
- model database (model).

System Recovery Data file *See* SRD file.

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

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

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

T

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

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

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

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

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

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

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

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

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

TLU Tape Library Unit.

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

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

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

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

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

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

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

transportable snapshot *(Microsoft VSS specific term)* A shadow copy that is created on the application system and can be presented to the backup system where a backup can be performed.
See also Microsoft Volume Shadow Copy Service (VSS).

U

unattended operation *See* lights-out operation.

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

User Account Control (UAC) A security component in Windows Vista, Windows 7, Windows 8, Windows Server 2008, and Windows Server 2012 that limits application software to standard user privileges until an administrator authorizes an increase in privilege level.

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

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

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

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

user_restrictions file A file that restricts specific user actions, which are available to Data Protector user groups according to the user rights assigned to them, to be performed only on specific systems of the Data Protector cell. Such restrictions apply only to Data Protector user groups other than *admin* and *operator*.

V

vaulting media The process of storing media to a safe and remote place. The media are brought back to the data center when they are needed for restore or are ready for reuse in subsequent backups. The vaulting procedure depends on your company's backup strategy and policies for data protection/reliability.

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

Virtual Controller Software (VCS) *(HP P6000 EVA Disk Array Family specific term)* The firmware that manages all aspects of storage system operation, including communication with HP Command View EVA through the HSV controllers.
See also HP Command View (CV) EVA.

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

virtual disk *(HP P6000 EVA Disk Array Family specific term)* A unit of storage allocated from a storage pool of a disk array of the HP P6000 EVA Disk Array Family. A virtual disk is the entity that can be replicated using the snapshot functionality of such disk array.
See also source volume and target volume.

virtual full backup An efficient type of synthetic backup where data is consolidated using pointers instead of being copied. It is performed if all the backups (the full backup, incremental backups, and the resulting virtual full backup) are written to a single file library that uses distributed file medium format.

Virtual Library System (VLS) A disk-based data storage device hosting one or more virtual tape libraries (VTLs).

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

virtual tape *(VLS specific term)* An archival storage technology that backs up data to disk drives in the same way as if it were being stored on tape. Benefits of virtual tape systems include improved backup and recovery speed and lower operating costs.
See also Virtual Library System (VLS) and virtual tape library (VTL).

virtual tape library (VTL) *(VLS specific term)* An emulated tape library that provides the functionality of traditional tape-based storage.
See also Virtual Library System (VLS).

VMware management client *(VMware (Legacy) integration specific term)* The client that Data Protector uses to communicate with VMware Virtual Infrastructure. This can be a VirtualCenter Server system (VirtualCenter environment) or an ESX Server system (standalone ESX Server environment).

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

volume group A unit of data storage in an LVM system. A volume group can consist of one or more physical volumes. There can be more than one volume group on the system.

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

Volume Shadow Copy Service *See* Microsoft Volume Shadow Copy Service (VSS).

VSS *See* Microsoft Volume Shadow Copy Service (VSS).

VSS compliant mode *(HP P9000 XP Disk Array Family VSS provider specific term)* One of two P9000 XP Array VSS hardware provider operation modes. When the P9000 XP Array provider is in the VSS compliant mode, the source volume (P-VOL) and its replica (S-VOL) are in simplex, unpaired state after a backup. Therefore the number of replicas (S-VOLs per a P-VOL) rotated is not limited. Restore from a backup in such a configuration is possible only by switching the disks.
See also resync mode, source volume, primary volume (P-VOL), replica, secondary volume (S-VOL), and replica set rotation.

VxFS Veritas Journal Filesystem.

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

W

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

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

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

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

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

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

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

X

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

Z

ZDB *See* zero downtime backup (ZDB).

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

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

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

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

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

Index

A

advantages
  Oracle integration, 19
architecture
  MS Exchange 2010 Server integration, 182
audience, 11

B

backing up Microsoft Exchange Server
  backup options, 195–196
backing up Microsoft SQL Server, 162, 169
  backup options, 167
  backup specifications, creating, 163
  scheduling backups, 168
backing up MS Exchange Server 2010/2013, 186–199
  backup specification, modifying, 196
  backup specifications, creating, 190
  backup types, 186
  copy backups, 187
  differential backups, 187
  full backups, 187
  incremental backups, 187
  previewing backups, 197
  scheduling backups, 196
  scheduling backups, example, 196
  starting backups, 198
backing up Oracle, 61–63
  backup options, 57
  backup set ZDB concepts, 24–27
  backup set ZDB session flow, 26–27
  backup specifications, creating, 50
  backup types, 20
  proxy-copy ZDB concepts, 28–30
  proxy-copy ZDB session flow, 29–30
  scheduling backups, 61
  starting backups, 62–63
  starting backups, using CLI, 63
  starting backups, using GUI, 62
backing up SAP R/3 , 125–138
  backup options, 132
  backup specification, modifying, 132
  backup specifications, creating, 126
  backup templates, 127
  backup types, 106, 125
  manual balancing, 132, 137
  previewing backups, 133
  SAP compliant ZDB, 136
  scheduling backups, 132
  scheduling backups, example, 132
  starting backups, 134
  verifying backups, 150
  ZDB concepts, 107–109
  ZDB flow, 107
backup flow
  SAP R/3 integration, 107
backup flow, Oracle integration, 23
  backup set ZDB session flow, 26–27
  proxy-copy ZDB session flow, 29–30
backup options
  Microsoft Exchange Server 2010 integration, 195–196
  Microsoft SQL Server integration, 167
  Oracle integration, 57
  SAP R/3 integration, 132
backup sessions, scheduling
  Microsoft SQL Server integration, 168
  MS Exchange 2010 Server integration, 196
  Oracle integration, 61
  SAP R/3 integration, 132
backup specifications, creating
  Microsoft SQL Server integration, 163
  MS Exchange 2010 Server integration, 190
  Oracle integration, 50
  SAP R/3 integration, 126
backup specifications, modifying
  MS Exchange 2010 Server integration, 196
  SAP R/3 integration, 132
backup templates
  SAP R/3 integration, 127
backup types
  MS Exchange 2010 Server integration, 186
  Oracle integration, 20
  SAP R/3 integration, 106, 125
BRBACKUP, 108

C

checking configuration
  Microsoft SQL Server integration, 161
  Oracle integration, 45
  SAP R/3 integration, 123
concepts
  Microsoft SQL Server integration, 156–157
  MS Exchange 2010 Server integration, 182
  Oracle integration, 21
  Oracle integration, backup set ZDB concepts, 24–27
  Oracle integration, proxy-copy ZDB concepts, 28–30
concepts, ZDB
  SAP R/3 integration, 107–109
configuration file
  SAP R/3 integration, 109
configuration files
  Microsoft SQL Server integration, 158
configuring Microsoft SQL Server, 157, 162
  checking configuration, 161
  configuration files, 158
configuring MS Exchange Server 2010/2013, 184–186
configuring Oracle, 31–49
  backup methods, 48
  checking configuration, 45
  example, CLI, 44–45
  prerequisites, 33
configuring SAP R/3, 109–125

authentication modes, 119
checking configuration, 123
configuration file, 109
listener, configuring, 116
SAP R/3 parameter file, 124
verifying configuration, 149
control files, Oracle integration
restore, 67
conventions
document, 16
copy backups
MS Exchange 2010 Server integration, 187
creating backup specifications
Microsoft SQL Server integration, 163
MS Exchange 2010 Server integration, 190
Oracle integration, 50
SAP R/3 integration, 126

D

Data Guard, Oracle integration
limitations, 33
database recovery
Oracle integration, after instant recovery, 87
Oracle integration, options, 73
SAP R/3 integration, 142
database recovery options
SAP R/3 integration, 143
differential backups
MS Exchange 2010 Server integration, 187
disaster recovery
Oracle integration, 65
document
conventions, 16
related documentation, 11
documentation
HP website, 11
providing feedback, 18

E

examples
SAP R/3 integration, starting interactive backups, 134
examples, MS Exchange 2010 Server integration
scheduling backups, 196
starting interactive backups, 198
examples, Oracle integration
restoring using RMAN, 76
examples, scheduling backups
SAP R/3 integration, 132

F

full backups
MS Exchange 2010 Server integration, 187

H

help
obtaining, 17
HP
technical support, 17

I

incremental backups
MS Exchange 2010 Server integration, 187
Informix backup
backup specifications, creating, 126
instant recovery
Microsoft SQL Server integration, 173, 175
Oracle integration, 87, 91
Oracle integration, database recovery after, 89
RAC preparation steps, 87
reconfiguring an Oracle instance, 252
SAP R/3 integration, 142
instant recovery options
SAP R/3 integration, 143
integrated authentication, Microsoft SQL Server integration, 160
interactive backups
MS Exchange 2010 Server integration, 198
Oracle integration, 62
SAP R/3 integration, 134
introduction
Microsoft SQL Server integration, 156
MS Exchange 2010 Server integration, 181
Oracle integration, 19
SAP R/3 integration, 106

M

manual balancing
SAP R/3 integration, 132, 137
Media Management Library *see* MML
Microsoft Exchange Server backup
backup options, 195–196
Microsoft SQL Server backup, 162, 169
availability group level, 162
backup options, 167
backup specifications, creating, 163
instance level, 162
scheduling backups, 168
Microsoft SQL Server configuration, 157, 162
checking configuration, 161
configuration files, 158
Microsoft SQL Server integration
backup, 162, 169
concepts, 156–157
configuration, 157, 162
introduction, 156
monitoring sessions, 175
restore, 169, 175
troubleshooting, 175, 180
Microsoft SQL Server restore, 169, 175
instant recovery, 173, 175
restore options, 171–172
restoring, tail log backup, 169
Microsoft SQL Server troubleshooting, 175, 180
MML (Data Protector Media Management Library)
linking with Oracle, UNIX, 37
modifying backup specifications
MS Exchange 2010 Server integration, 196
SAP R/3 integration, 132

monitoring sessions
Microsoft SQL Server integration, 175
MS Exchange 2010 Server integration, 224
SAP R/3 integration, 146
MS Exchange 2010 Server integration
architecture, 182
backup, 186–199
concepts, 182
configuration, 184–186
introduction, 181
monitoring sessions, 224
restore, 199–224
troubleshooting, 224–228
MS Exchange Server 2010/2013 backup, 186–199
backup specification, modifying, 196
backup specifications, creating, 190
backup types, 186
copy backups, 187
differential backups, 187
full backups, 187
incremental backups, 187
previewing backups, 197
scheduling backups, 196
scheduling backups, example, 196
starting backups, 198
MS Exchange Server 2010/2013 configuration, 184–186
MS Exchange Server 2010/2013 restore, 199–224
finding information, 204
restore options, 224
using another device, 213
using CLI, 211
using GUI, 205
MS Exchange Server 2010/2013 troubleshooting, 224–228

O

OB2_MIRROR_COMP, SAP R/3 integration, 136
OB2RMANSAVE, Oracle integration, 102
omnirc options, 254–258
online backups
MS Exchange 2010 Server integration, 181
Oracle backup, 61–63
backup concepts, scheme, 24
backup set ZDB concepts, 24–27
backup set ZDB session flow, 26–27
backup specifications, creating, 50
backup types, 20
proxy-copy concepts, 28–30
proxy-copy ZDB session flow, 29–30
scheduling backups, 61
starting backups, 62–63
starting backups, using CLI, 63
starting backups, using GUI, 62
Oracle configuration
backup methods, 48
checking configuration, 45
example, CLI, 44–45
prerequisites, 33
Oracle integration
advantages, 19
backup, 61–63
backup set ZDB concepts, 24–27
concepts, 21
configuration, 31–49
instant recovery, 87–91
introduction, 19
proxy-copy ZDB concepts, 28–30
troubleshooting, 91–105
Oracle restore
control files, 67
database items, 63
database objects, 68
database recovery after instant recovery, 87
editing RMAN scripts, 102
examples, using RMAN, 76
instant recovery, 87–91
preparing databases for restore, 77
recovery catalog, 66
restorable items, 63
restore flow, 23
restore options, 73
restore types, 20
standard restore procedure, 63–86
tablespaces and datafiles, 70
to the application system, 65
using another device, 86
using GUI, 65
using RMAN, 76
Oracle RMAN script, 58
Oracle troubleshooting, 91–105

P

prerequisites, verifying Oracle side
SAP R/3 integration, 147
prerequisites, verifying SAP side
SAP R/3 integration, 148
previewing backups
MS Exchange 2010 Server integration, 197
SAP R/3 integration, 133

R

RAC
preparing for instant recovery, 87
RAC, configuring Oracle Servers
on HP-UX, 37
on other UNIX systems, 37
reconfiguring an Oracle instance for instant recovery , 252
recovery
Oracle database after instant recovery, 87
Oracle integration, options, 73
SAP R/3 integration, 142
recovery catalog, Oracle integration
restore, 66
recovery options
SAP R/3 integration, 143
related documentation, 11

restore methods
SAP R/3 integration, 138
restore options
Informix integration, 172
Microsoft SQL Server integration, 171
MS Exchange 2010 Server integration, 224
restore types
Oracle integration, 20
restoring Informix
restore options, 172
restoring Microsoft SQL Server, 169, 175
instant recovery, 173, 175
restore options, 171
restoring, availability group, 169
restoring, tail log backup, 169
restoring MS Exchange Server 2010/2013, 199–224
finding information, 204
restore options, 224
using another device, 213
using CLI, 211
using GUI, 205
restoring Oracle
control files, 67
database objects, 68
database recovery after instant recovery, 87
editing RMAN scripts, 102
instant recovery, 87–91
recovery catalog, 66
restore flow, 23
restore types, 20
standard restore procedure, 63–86
tablespaces and datafiles, 70
to the application system, 65
using another device, 86
using GUI, 65
using RMAN, 76
restoring SAP R/3, 138–144
database recovery, 142
instant recovery, 142
restore methods, 138
standard restore, 139
using another device, 145
verifying restores, 150
RMAN, Oracle integration
restore, 76
running backups *see* starting backups

S

SAP compliant ZDB
SAP R/3 integration, 136
SAP R/3 backup, 125–138
backup options, 132
backup specification, modifying, 132
backup templates, 127
backup types, 106, 125
manual balancing, 132, 137
previewing backups, 133
SAP compliant ZDB, 136
scheduling backups, 132
scheduling backups, example, 132
starting backups, 134
verifying backups, 150
ZDB concepts, 107–109
ZDB flow, 107
SAP R/3 configuration, 109–125
authentication modes, 119
checking configuration, 123
configuration file, 109
listener, configuring, 116
SAP R/3 parameter file, 124
verifying configuration, 149
SAP R/3 integration
backup, 125–138
configuration, 109–125
introduction, 106
monitoring sessions, 146
restore, 138–144
troubleshooting, 146–155
ZDB concepts, 107–109
SAP R/3 restore, 138–144
database recovery, 142
instant recovery, 142
restore methods, 138
standard restore, 139
using another device, 145
verifying restores, 150
SAP R/3 troubleshooting, 146–155
verifying backups, 150
verifying configuration, 149
verifying prerequisites on Oracle side, 147
verifying prerequisites on SAP side, 148
verifying restores, 150
SBT_LIBRARY, Oracle integration, 37, 78
scheduling backups
Microsoft SQL Server integration, 168
MS Exchange 2010 Server integration, 196
Oracle integration, 61
SAP R/3 integration, 132
SQL Server authentication, Microsoft SQL Server integration, 160
starting backups
MS Exchange 2010 Server integration, 198
SAP R/3 integration, 134
starting backups, Oracle integration, 62–63
using CLI, 63
using GUI, 62
Subscriber's Choice, HP, 17

T

technical support
HP, 17
service locator website, 18
troubleshooting Microsoft SQL Server, 175, 180
troubleshooting MS Exchange Server 2010/2013, 224–228
troubleshooting Oracle, 91–105
troubleshooting SAP R/3 , 146–155
verifying backups, 150

verifying configuration, 149
verifying prerequisites on Oracle side, 147
verifying prerequisites on SAP side, 148
verifying restores, 150

U

users, configuring
Oracle integration, 37

V

verifying backups
SAP R/3 integration, 150
verifying configuration
SAP R/3 integration, 149
verifying prerequisites, Oracle side
SAP R/3 integration, 147
verifying prerequisites, SAP side
SAP R/3 integration, 148
verifying restores
SAP R/3 integration, 150

W

websites
HP, 18
HP Subscriber's Choice for Business, 17
product manuals, 11
Windows authentication, Microsoft SQL Server integration, 160

Z

ZDB flow
SAP R/3 integration, 107
ZDB session flow
Oracle integration, backup set, 26–27
Oracle integration, proxy-copy, 29–30