HP Data Protector A.06.11

Integration guide for Microsoft applications

SQL Server, SharePoint Portal Server, Exchange Server, and Volume Shadow Copy Service

B 6 9 6 0 - 9 0 1 5 7

Part number: B6960-90157
First edition: September 2009

Legal and notice information

Printed in the US

Contents

Publication history 13

About this guide 15

- Intended audience 15
- Documentation set 15
  - Guides 15
  - Online Help 18
  - Documentation map 19
    - Abbreviations 19
    - Map 20
    - Integrations 21
- Document conventions and symbols 23
- Data Protector graphical user interface 24
- General information 25
- HP technical support 25
- Subscription service 26
- HP websites 26
- Documentation feedback 26

1 Integrating Microsoft SQL Server and Data Protector 27

- Introduction 27
- Integration concepts 28
  - Parallelism 29
- Configuring the integration 30
  - Prerequisites 30
  - Before you begin 31
  - Data Protector SQL Server configuration file 31
  - Configuring users 32
  - Configuring SQL Server instances 32
    - Using the Data Protector GUI 33
    - Using the Data Protector CLI 36
  - Changing and checking configuration 37
    - Using the Data Protector GUI 37

Using the Data Protector CLI 38
Backup 39
Creating backup specifications 39
SQL Server Specific Backup Options 42
Object specific options 44
Scheduling backups 45
Scheduling example 45
Starting backup sessions 46
Using the Data Protector GUI 46
Restore 46
Restore methods 46
Before you begin 47
Restoring using the Data Protector GUI 47
Restore options 51
Restoring to another SQL Server instance or/and another SQL Server 53
Restoring using the Data Protector CLI 54
Disaster recovery 55
Recovering the master database 56
Recovering user databases 57
Performance tuning 58
Monitoring sessions 62
Troubleshooting 63
Before you begin 63
Checks and verifications 63
Problems 64

2 Integrating Microsoft SharePoint Portal Server and Data Protector 69
Introduction 69
Integration concepts 70
Backup and restore flow 73
Configuring the integration 73
Prerequisites 74
Before you begin 74
Configuring SPS users 74
Configuring SPS farms 74
Checking the configuration 77
Backup 77
Before you begin 78
Creating backup specifications 78
Modifying backup specifications 81
Scheduling backup specifications 81

Scheduling example 81
Previewing backup sessions 82
Using the Data Protector GUI 82
Using the Data Protector CLI 83
What happens during the preview? 83
Starting backup sessions 83
Before you begin 83
Using the Data Protector GUI 83
Using the Data Protector CLI 84
Preparing for disaster recovery 84
Restore 85
Before you begin 85
Considerations 85
Restoring using the Data Protector GUI 85
Restoring using the Data Protector CLI 90
Restoring using another device 92
Using the Data Protector GUI 92
Using the Data Protector CLI 92
Disaster recovery 93
Monitoring sessions 93
Troubleshooting 93
Before you begin 94
Checks and verifications 94
Problems 94

3 Integrating Microsoft Exchange Server and Data Protector 97
Introduction 97
Integration concepts 98
Configuring the integration 99
Prerequisites 99
Limitations 100
Before you begin 100
Backup 101
Configuring Exchange Server Backup 102
Creating backup specifications 102
Exchange Server specific backup options 107
Scheduling backups 108
Scheduling example 108
Starting backup sessions 108
Using the Data Protector GUI 108
Restore 109
Restoring using the GUI 110

Restoring to another client 115
Restoring using the CLI 116
Troubleshooting 117
Before you begin 117
Checks and verifications 117
Problems 119

4 Integrating Microsoft Exchange Single Mailbox and Data Protector 123
Introduction 123
Integration concepts 124
Configuring the integration 125
Prerequisites 125
Limitations 126
Before you begin 126
Cluster-aware clients 126
Configuring Exchange Server users 126
Configuring Exchange servers 126
Checking the configuration 127
Backup 128
Creating backup specifications 128
Modifying backup specifications 132
Scheduling backup specifications 132
Scheduling example 132
Previewing backup sessions 133
Using the Data Protector GUI 133
Using the Data Protector CLI 134
What happens during the preview? 134
Starting backup sessions 134
Using the Data Protector GUI 134
Using the Data Protector CLI 135
Restore 135
Before you begin 135
Restoring using the Data Protector GUI 135
Restoring using the Data Protector CLI 142
Restore examples 144
Monitoring sessions 145
Performance tuning 145
Troubleshooting 147
Before you begin 147
Checks and verifications 147
Problems 148

5 Integrating Microsoft Volume Shadow Copy Service with Data Protector 153
Introduction 153
Volume Shadow Copy Service 153
Integration concepts 156
Backup 156
Data consistency 158
Restore 158
Restoring components 158
Restoring files 159
VSS database 159
Querying the VSSDB 160
Deleting backup sessions 160
Microsoft Exchange Server 2007 writer concepts 161
Backup 161
Restore 161
Microsoft Hyper-V VSS writer concepts 162
Prerequisites 162
Microsoft SharePoint Services VSS writer concepts 162
Prerequisites and limitations 163
Prerequisites 164
Limitations 164
Configuring the integration 164
Microsoft Exchange Server writer specific configuration 165
Prerequisites 165
Writers specifics 165
Backing up writers data 170
Overview 170
Creating backup specifications using GUI 170
VSS specific backup options 175
Microsoft Exchange Server writer backup specifics 175
Microsoft Data Protection Manager 2006 writer specifics 179
Microsoft Hyper-V VSS writer backup specifics 181
Microsoft SharePoint Services VSS writer backup specifics 183
Scheduling the backup 184
Running an interactive backup 185
Restoring writers data 186
Restore procedure 186
Restore options 191
MSDE writer restore specifics 191
Microsoft Exchange Server writer restore specifics 193
Rollforward recovery from the loss of one or more databases 193

Point-in-time restore after loss of a log file 194
Microsoft Exchange Server 2007 writer restore specifics 195
Microsoft Data Protection Manager 2006 writer restore specifics 198
Restore the DPM server first 198
Restore the DPM clients directly 201
Microsoft Hyper-V VSS writer restore specifics 201
Restore from a physical cluster node 201
Microsoft SharePoint Services VSS writer restore specifics 202
Monitoring a VSS backup and restore 203
Monitoring current sessions 203
Viewing previous sessions 204
Troubleshooting 205
Before you begin 206
Checks and verifications 206
Backup problems 206
Restore problems 208

Glossary 211

Index 269

Figures

1 Data Protector graphical user interface ... 25

2 Data Protector SQL Server integration architecture ... 29

3 Database parallelism = 4, Overall Concurrency = 10 ... 30

4 SQL Server users ... 33

5 Configuring SQL Server ... 35

6 Checking configuration ... 38

7 Selecting a blank template ... 40

8 Selecting backup objects ... 41

9 Saving a backup specification ... 42

10 Application specific options ... 43

11 Object properties ... 45

12 Restore objects ... 48

13 Selecting object specific options ... 49

14 Restore options ... 50

15 Adjusted local device ... 60

16 Advanced options ... 61

17 Block sizes not adjusted ... 62

18 SPS integration architecture ... 71

19 Selecting a front-end Web server system ... 76

20 Configuring an SPS farm ... 77

21 Selecting SPS objects ... 79

22 Application specific options ... 80

23 Scheduling a backup specification ... 82

24 Selecting SPS objects for restore ... 86

25 Specifying the restore destination for an SQL Server database 87
26 Specifying the restore destination for an index server 88
27 SPS restore options 89
28 Data Protector Exchange Server integration architecture 99
29 Path system variable 101
30 Selecting a blank template 103
31 Client name and application database 104
32 Backup objects 105
33 Backup devices 106
34 Application specific options 107
35 Unmounting a database 110
36 Restore objects 112
37 Selecting a backup version 113
38 Restore options 115
39 Exchange Single Mailbox integration architecture 124
40 Configuring the Exchange Server 127
41 Selecting a template 129
42 Selecting Exchange items for backup 130
43 Exchange Single Mailbox specific backup options 131
44 Scheduling a backup specification 133
45 Selecting Exchange items for restore 136
46 Version properties 137
47 Advanced properties 138
48 Selecting the destination Exchange Server system 139
49 Restored mailbox and public folders content with the restore to new folder option selected. 140
50 Example of backup with concurrency 1 146
51 Example of backup with concurrency 2 146
52 Specifying the Exchange Server administrator's mailbox 150

53 Actors of the traditional backup model 155
54 Actors of the Data Protector VSS integration backup model 155
55 Local VSS backup 158
56 Selecting Microsoft Exchange Server 2007 CCR copy backup objects 172
57 Selecting Microsoft Hyper–V VSS writer backup objects 173
58 Additional options for Microsoft Exchange Server 2007 in a CCR environment 174
59 Selecting Microsoft Exchange Server 2003 storage groups 177
60 Selecting a replicated Microsoft Exchange Server 2007 storage group 178
61 Selecting Microsoft Data Protection Manager database and replicas 181
62 Selecting Microsoft SharePoint Services writer and the corresponding search writers 184
63 Scheduling a backup 185
64 Restore objects 188
65 Restore to different location options (Exchange Server 2007 Writer) 190
66 MSDE writer 192
67 Selecting Microsoft Exchange Server 2007 stores for rollforward recovery 194
68 Selecting Microsoft Exchange Server 2003 stores for point-in-time restore 195
69 Restoring the Microsoft Data Protection Manager 2006 client 200
70 Selecting Microsoft SharePoint Services writer and the corresponding search writers for restore 203
71 Monitoring a current session 204
72 Viewing a previous session 205

Tables

1 Edition history ... 13
2 Document conventions ... 23
3 SQL Server online backup types ... 27
4 Legend ... 29
5 SQL Server backup options ... 43
6 Object specific options ... 45
7 SQL Server restore options ... 51
8 Backup types ... 69
9 Legend ... 71
10 SPS objects ... 72
11 Backup types ... 78
12 SPS backup options ... 81
13 What must be backed up ... 84
14 SPS restore options ... 90
15 Exchange Server online backup types ... 97
16 Legend ... 99
17 Application specific options ... 107
18 Exchange Server restore options ... 114
19 Exchange Single Mailbox backup types ... 123
20 Exchange Single Mailbox backup types ... 128
21 Exchange Single Mailbox specific backup options ... 132
22 Exchange Single Mailbox restore options ... 140
23 Writer description ... 166
24 VSS specific backup options ... 175

Publication history

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

Table 1 Edition history

Part number	Guide edition	Product
B6960-90108	October 2004	Data Protector Release A.05.50
B6960-96007	July 2006	Data Protector Release A.06.00
B6960-96041	November 2008	Data Protector Release A.06.10
B6960-90157	September 2009	Data Protector Release A.06.11

About this guide

This guide describes how to configure and use Data Protector with Microsoft applications.

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.

Documentation set

Other documents and online Help provide related information.

Guides

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

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

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

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

- *HP Data Protector concepts guide*

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

- *HP Data Protector installation and licensing guide*

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

- *HP Data Protector troubleshooting guide*

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

- *HP Data Protector disaster recovery guide*

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

- *HP Data Protector integration guides*

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

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

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

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

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

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

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

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

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

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

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

- *HP Data Protector integration guide for HP Reporter*

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

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

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

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

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

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

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

- *HP Data Protector zero downtime backup concepts guide*

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

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

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

- *HP Data Protector zero downtime backup integration guide*

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

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

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

- *HP Data Protector Media Operations user guide*

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

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

  This guide gives a description of new features of HP Data Protector A.06.11. It also provides information on installation requirements, required patches, and limitations, as well as known issues and workarounds.

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

  This guide fulfills a similar function for the listed integrations.

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

  This guide fulfills a similar function for Media Operations.

- *HP Data Protector command line interface reference*

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

Online Help

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

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

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

Documentation map

Abbreviations

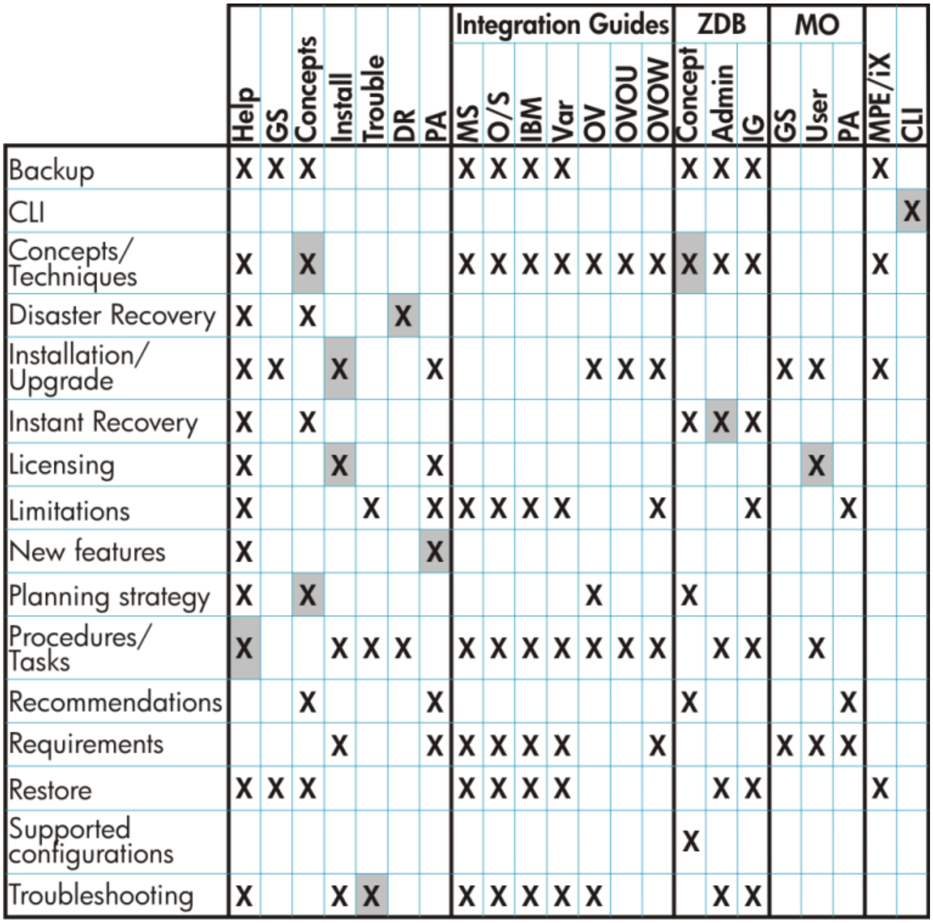
Abbreviations in the documentation map that follows are explained below. The guide titles are all preceded by the words “HP Data Protector”.

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

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

Map

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



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

Integrations

Look in these guides for details of the following integrations:

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

Integration	Guide
HP Reporter	IG-R
HP Service Information Portal	IG-SIP
HP StorageWorks Disk Array XP	all ZDB
HP StorageWorks Enterprise Virtual Array (EVA)	all ZDB
HP StorageWorks Virtual Array (VA)	all ZDB
IBM DB2 UDB	IG-IBM
Informix	IG-IBM
Lotus Notes/Domino	IG-IBM
Media Operations	MO User
MPE/iX system	MPE/iX
Microsoft Exchange Server	IG-MS, ZDB IG
Microsoft Exchange Single Mailbox	IG-MS
Microsoft SQL Server	IG-MS, ZDB IG
Microsoft Volume Shadow Copy Service (VSS)	IG-MS, ZDB IG
NDMP Server	IG-Var
Network Node Manager (NNM)	IG-Var
Oracle	IG-O/S
Oracle ZDB	ZDB IG
SAP DB	IG-O/S
SAP R/3	IG-O/S, ZDB IG

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

Document conventions and symbols

Table 2 Document conventions

Convention	Element
Blue text: Table 2 on page 23	Cross-reference links and e-mail addresses
Blue, underlined text: http://www.hp.com	Website addresses
Italic text	Text emphasis
`Monospace` text	- File and directory names - System output - Code - Commands, their arguments, and argument values
`Monospace, italic` text	- Code variables - Command variables
`Monospace, bold` text	Emphasized monospace text

△ CAUTION:

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

IMPORTANT:

Provides clarifying information or specific instructions.

📝 NOTE:

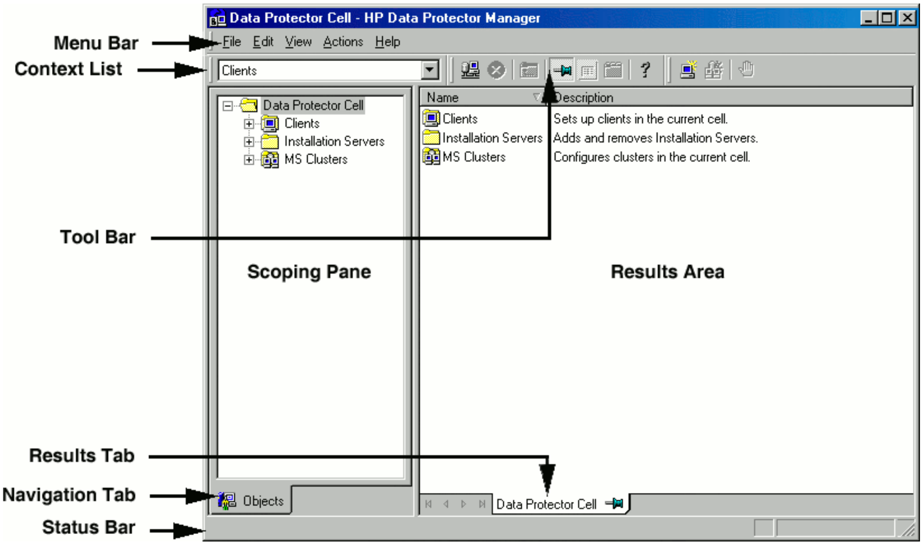
Provides additional information.

💡 TIP:

Provides helpful hints and shortcuts.

Data Protector graphical user interface

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



Name	Description
Clients	Sets up clients in the current cell.
Installation Servers	Adds and removes Installation Servers.
MS Clusters	Configures clusters in the current cell.

Figure 1 Data Protector graphical user interface

General information

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

HP technical support

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

http://www.hp.com/support

Before contacting HP, collect the following information:

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

Subscription service

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

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

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

HP websites

For additional information, see the following HP websites:

- http://www.hp.com
- http://www.hp.com/go/software
- http://www.hp.com/support/manuals
- http://h20230.www2.hp.com/selfsolve/manuals
- http://www.hp.com/support/downloads

Documentation feedback

HP welcomes your feedback.

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

1 Integrating Microsoft SQL Server and Data Protector

Introduction

This chapter explains how to configure and use the Data Protector Microsoft SQL Server integration. It describes the concepts and methods you need to understand to back up and restore the Microsoft SQL Server (**SQL Server**) database objects.

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

Table 3 SQL Server online backup types

Full database backup	Includes all data regardless of the changes made after the last backup.
Transaction log backup	Uses fewer resources than database backups, so can be created more frequently. By applying transaction log backups, you can recover the database to a specific point in time.
Differential database backup	Records only changes made to the database since the last full database backup. By creating differential backups more frequently than full database backups, you can conserve the media used for backup.

Data Protector offers different restore types, depending on your needs. You can select point-in-time restore, full database restore, as well as restore your SQL Server data to a new location, to another SQL Server, or another SQL Server instance. For detailed information, see "Restore options" on page 51.

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

Integration concepts

Data Protector integrates with SQL Server through the Data Protector `sql_bar.exe` executable, installed on SQL Server. It implements multiple virtual devices for backup and restore and transforms SQL Server Virtual Device Interface (VDI) commands from SQL Server into Data Protector backup or restore streams.

The VDI architecture allows the Data Protector General Media Agent to access data directly in the SQL Server memory, provided the devices are directly attached to SQL Server. Therefore, high backup and restore speed is achieved.

You can perform interactive and scheduled full database backups, differential database backups, and transaction log backups. Full and differential backups, combined with regular transaction log backups, prevent data loss if a disk failure occurs. Furthermore, transaction log backups are needed to perform point-in-time restore.

You can back up the whole server or particular databases listed below:

User databases	Contain user data.
Master	Controls user databases and the SQL Server operation. Keeps track of user accounts, configurable environment variables, and system error messages.
Model	Provides a template or prototype for new user databases.
Distribution	A system database used by SQL Server replication components, such as Distribution Agent, to store data, including transactions, snapshot jobs, synchronization status, and replication history information.
Msdb	Provides storage for scheduling and backup information.

For more information about system databases, see the SQL Server documentation.

Data Protector restores databases so that the last differential backup is applied to the most recent full backup. Then the transaction log backups are applied according to the specified restore options.

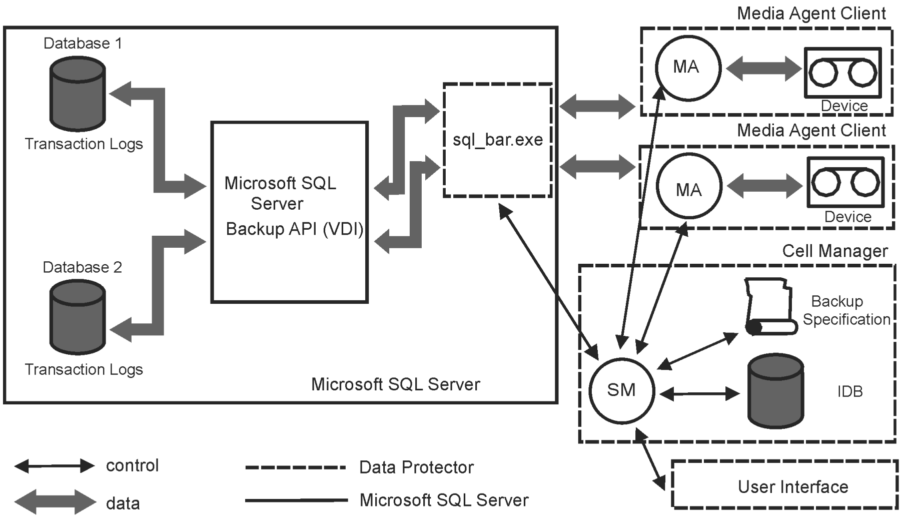


Figure 2 Data Protector SQL Server integration architecture

Table 4 Legend

SM	Data Protector Session Manager: Backup Session Manager during backup and Restore Session Manager during restore.
Backup API or VDI	SQL Server VDI, the backup interface introduced with SQL Server 7.0.
MA	Data Protector General Media Agent.

Parallelism

You can back up more than one SQL Server database at a time or back up a single database using multiple streams.

Parallelism types used with SQL Server are:

- Database parallelism

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

  The allocation of streams to available devices is done automatically.

- Number of concurrent streams

This is the number of devices used to back up a particular database or a server. Can be specified by the user or calculated automatically.

NOTE:

SQL Server cannot back up multiple streams to one device.

Figure 3 on page 30 shows a session in which each SQL Server database is backed up using a different number of concurrent streams.

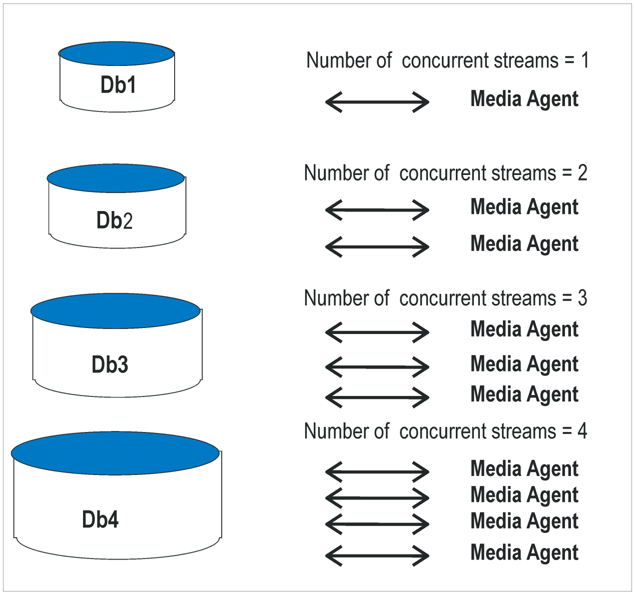

Db1
Number of concurrent streams = 1
Media Agent
Db2
Number of concurrent streams = 2
Media Agent
Media Agent
Db3
Number of concurrent streams = 3
Media Agent
Media Agent
Media Agent
Db4
Number of concurrent streams = 4
Media Agent
Media Agent
Media Agent
Media Agent

Figure 3 Database parallelism = 4, Overall Concurrency = 10

Configuring the integration

Prerequisites

- You need a license to use the SQL Server integration. See the *HP Data Protector installation and licensing guide* for information.
- Ensure that you correctly installed and configured SQL Server.
  - For supported versions, platforms, devices, and other information, see the latest support matrices at http://www.hp.com/support/manuals.

    - For information on installing, configuring, and using SQL Server, see the SQL Server documentation.
- Ensure that you correctly installed Data Protector. For information on installing Data Protector in various architectures and installing the Data Protector SQL Server integration, 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.

Before you begin

- Configure devices and media for use with Data Protector. See the online Help index: "configuring devices" and "creating media pools" for instructions. See also "Performance tuning" on page 58 for advanced options.
- 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 backups and restores. On Windows Server 2008, this is not required.

  For information on changing the user account under which the Data Protector `Inet` service is running, see the online Help index: "Inet, changing account".
- To test whether SQL Server and Cell Manager communicate properly, configure and run a Data Protector filesystem backup and restore. See the online Help for instructions.

Data Protector SQL Server configuration file

Data Protector stores integration parameters for every configured SQL Server on the Cell Manager in:

HP-UX, Solaris:

`/etc/opt/omni/server/integ/config/MSSQL/`*`client_name%instance_name`*

Windows:

`Data_Protector_home``\Config\Server\Integ\Config\MSSQL\`*`client_name%instance_name`*

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';
```

IMPORTANT:

To avoid backup problems, ensure 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

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 online Help index: “adding users”.

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.

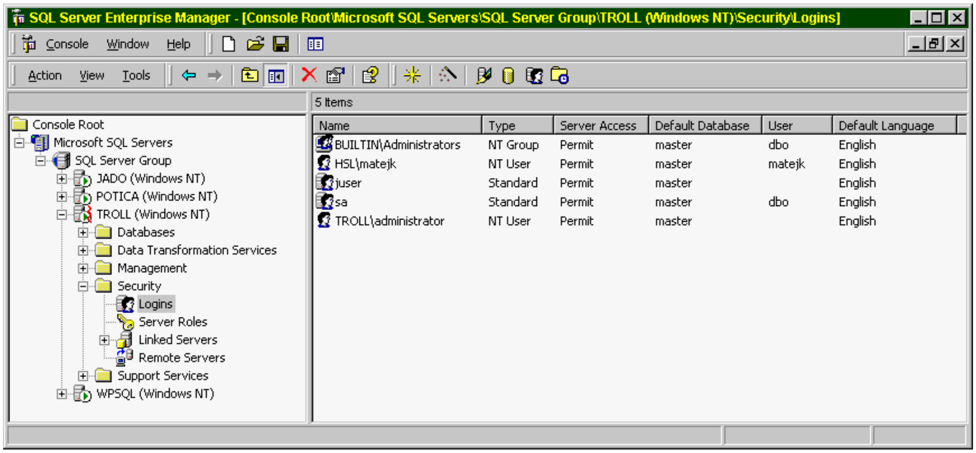
NOTE:

Ensure 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" on page 37.

Prerequisites

- SQL Server must be online during configuration.
- Configuration must be performed for every SQL Server instance separately.



SQL Server Enterprise Manager - [Console Root\Microsoft SQL Servers\SQL Server Group\TROLL (Windows NT)\Security\Logins]

5 Items

Name	Type	Server Access	Default Database	User	Default Language
BUILTIN\Administrators	NT Group	Permit	master	dbo	English
HSL\matejk	NT User	Permit	master	matejk	English
juser	Standard	Permit	master		English
sa	Standard	Permit	master	dbo	English
TROLL\administrator	NT User	Permit	master		English

Figure 4 SQL Server users

Configure SQL Server instances 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**, 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.

   Click **OK**.

4. In **Client**, select the SQL Server system. For cluster environments, select the virtual server of the SQL Server resource group.

   In **Application database**, select or specify the name of the SQL Server instance.

   Windows Server 2008 only: If you intend to use the **Integrated authentication** option, specify the **User and group/domain** options. For information on the options, press **F1**.

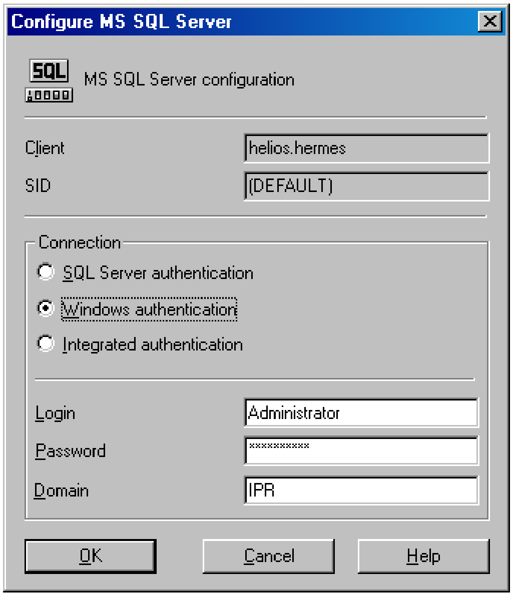
   Click **Next**.

5. 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.

   Ensure that the user account you specify has the appropriate permissions for backing up and restoring the SQL Server databases.

   See Figure 5 on page 35.



Configure MS SQL Server

MS SQL Server configuration

Client: helios.hermes

SID: (DEFAULT)

Connection

○ SQL Server authentication

● Windows authentication

○ Integrated authentication

Login: Administrator

Password: **********

Domain: IPR

Figure 5 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.

6. The SQL Server instance is configured. Exit the GUI or proceed with creating the backup specification at Step 6 on page 41.

Using the Data Protector CLI

From the *Data_Protector_home*\bin directory, run:

```
sql_bar config [-appsrv:SQL_Server_client]
[-instance:instance_name] [-dbuser:SQL_Server_user
-password:password | -dbuser:Windows_user -password:password
-domain:domain]
```

Parameter description

`-appsrv:SQL_Server_client`

Client system on which the SQL Server instance is running. This option is not required if you run the command locally.

`-instance:instance_name`

SQL Server instance name. If you omit this option, the default SQL Server instance is configured.

`-dbuser:SQL_Server_user -password:password`

SQL Server user account (**SQL Server authentication**)

`-dbuser:Windows_user -password:password -domain:domain`

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.

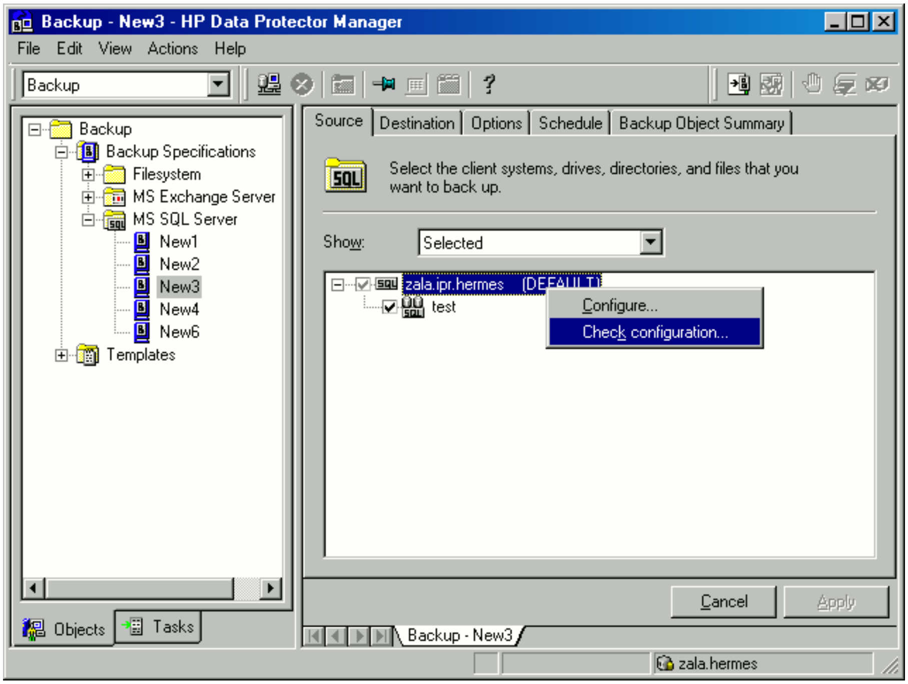
Changing and checking configuration

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" on page 32.

5. Right-click SQL Server and select **Check Configuration**. See Figure 6 on page 38.



Select the client systems, drives, directories, and files that you want to back up.

Show: Selected

Figure 6 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:instance_name]
```

If the optional parameter `-instance:`*`instance_name`* 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:instance_name]
```

If `-instance:`*`instance_name`* is not specified, Data Protector returns configuration for the default instance.

Backup

To run an online backup of an existing SQL Server backup specification:

- Schedule a backup using the Data Protector Scheduler.
- Start an interactive backup using the Data Protector GUI or CLI.

  For information on starting interactive backups using the CLI, see the `omnib` man page.

Limitations

- Backup preview is not supported.

Considerations

- A transaction log backup is not possible if the `Recovery model` option on SQL Server is *not* set to `Bulk-Logged` or `Full`. In this case, Data Protector performs a differential or full backup.

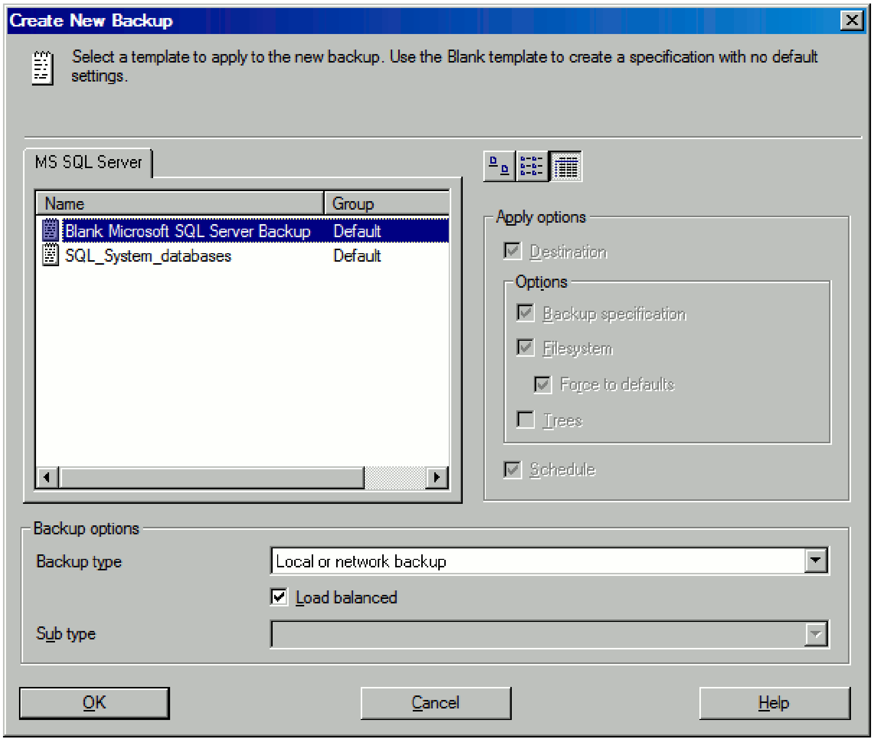
To configure a backup, create a Data Protector SQL Server backup specification.

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 **MS SQL Server**, and click **Add Backup**.

3. In the **Create New Backup** dialog box, select the **Blank Microsoft SQL Server Backup** template. See Figure 7 on page 40.



Create New Backup

Select a template to apply to the new backup. Use the Blank template to create a specification with no default settings.

MS SQL Server

Name	Group
Blank Microsoft SQL Server Backup	Default
SQL_System_databases	Default

Apply options

☑ Destination

Options

☑ Backup specification

☑ Filesystem

☑ Force to defaults

□ Trees

☑ Schedule

Backup options

Backup type: Local or network backup

☑ Load balanced

Sub type:

Figure 7 Selecting a blank template

Click **OK**.

4. In **Client**, select SQL Server. For cluster environments, select the virtual server of the SQL Server resource group.

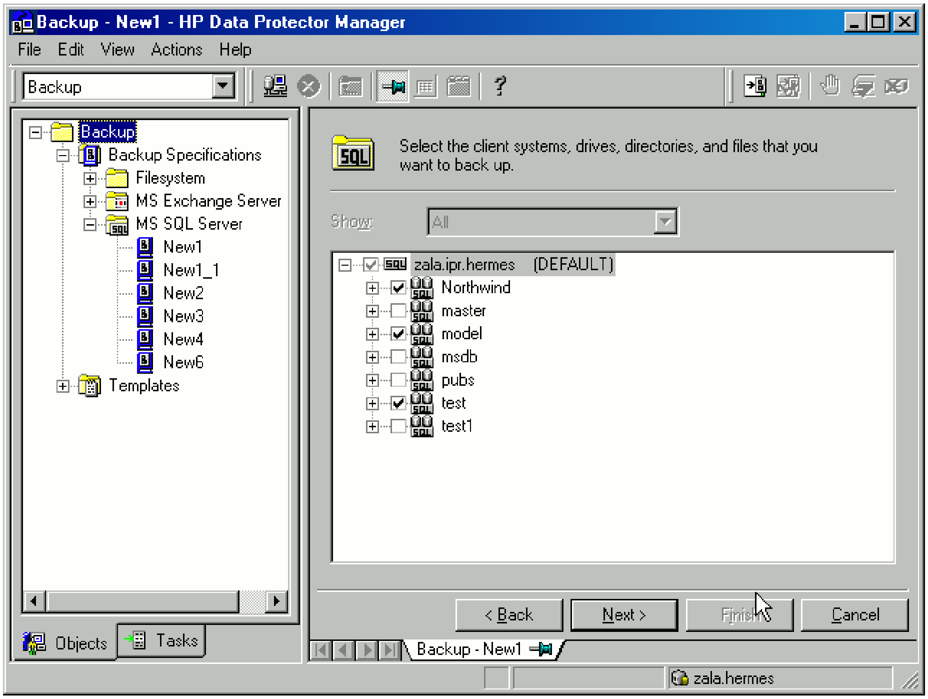
   In **Application database**, specify the name of the SQL Server instance.

   Windows Server 2008 only: If you intend to use the **Integrated authentication** option, specify the **User and group/domain** options. For information on the options, press **F1**.

   Click **Next**.

5. If the client is not configured, the **Configure MS SQL Server** dialog box appears. Configure it as described in “Configuring SQL Server instances” on page 32.

6. Depending on the version of Microsoft SQL Server for which you are configuring backup, perform the following:
   - With Microsoft SQL Server 2000 or 2005, select the databases, file groups, or data files you want to back up.
   - With Microsoft SQL Server versions prior to 2000, select the databases you want to back up.



Select the client systems, drives, directories, and files that you want to back up.

Show: All

- ☑ zala.ipr.hermes (DEFAULT)
  - ☑ Northwind
  - □ master
  - ☑ model
  - □ msdb
  - □ pubs
  - ☑ test
  - □ test1

Figure 8 Selecting backup objects

Click **Next**.

7. 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 online Help.

   Click **Next**.

8. Select backup options.

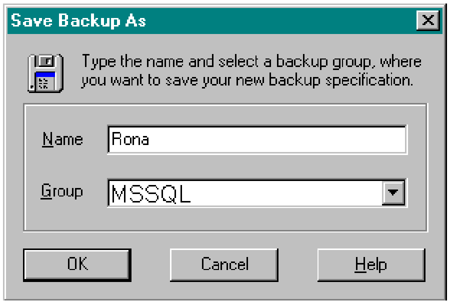
   For information on **Backup Specification Options** and **Common Application Options**, see the online Help.

   For information on **Application Specific Option**, see "SQL Server Specific Backup Options" on page 42.

   Click **Next**.

9. Optionally, schedule the backup. For information on scheduler, press **F1**.

10. Save the backup specification, specifying a name and backup specification group. You start the backup specification by clicking **Start Backup**.



Save Backup As

Type the name and select a backup group, where you want to save your new backup specification.

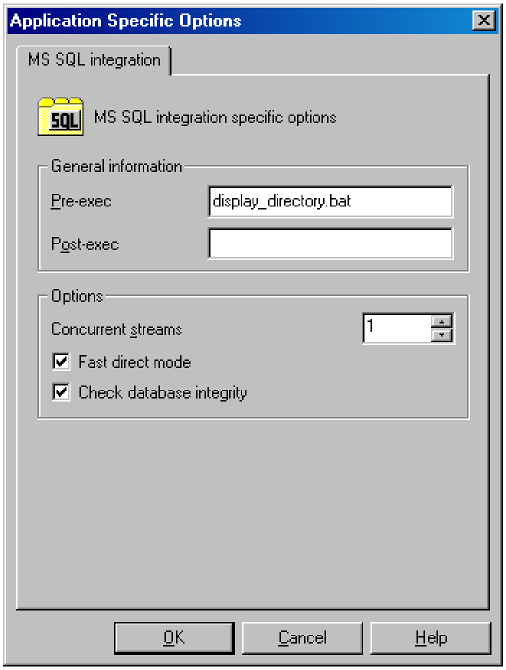
Name: Rona

Group: MSSQL

Figure 9 Saving a backup specification

SQL Server Specific Backup Options

SQL Server specific backup options are specified by clicking the **Advanced** tab in the **Application Specific Options** group box.



Application Specific Options
MS SQL integration
SQL
MS SQL integration specific options
General information
Options
OK
Cancel
Help

Pre-exec: display_directory.bat

Post-exec:

Concurrent streams: 1

☑ Fast direct mode

☑ Check database integrity

Figure 10 Application specific options

Table 5 SQL Server backup options

Concurrent streams	Sets the number of concurrent streams used for backup.
Fast direct mode	Used with locally connected devices to optimize performance. Must be combined with special device settings (see "Performance tuning" on page 58 for details).
Check database integrity	Performs data integrity validation before backup. If the check fails, the session completes with warnings.
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.

📝 NOTE:

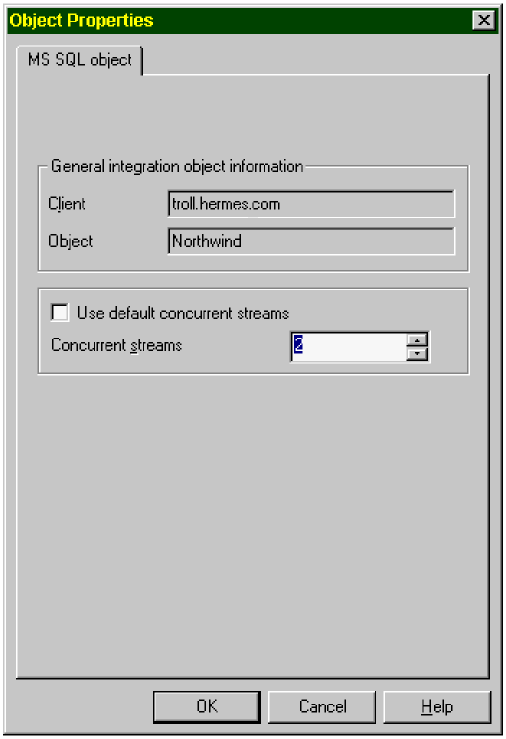
Do not use double quotes (" ") in object-specific pre-exec and post-exec commands.

Object specific options

If you selected one or more databases for backup (as opposed to a whole server backup), you can set backup options on a single database level by going to the **Backup Specification Summary** property page and double-clicking an object.

📝 NOTE:

If you selected a whole server backup, the same options as in the **Application Specific Options** windows are displayed.



Object Properties

MS SQL object

General integration object information

Client: troll.hermes.com

Object: Northwind

☐ Use default concurrent streams

Concurrent streams: 2

Figure 11 Object properties

Table 6 Object specific options

Use default concurrent streams	The number of concurrent streams is defined by Data Protector and all available devices are used.
Concurrent streams	Sets the number of concurrent streams (devices). VDI supports up to 32 virtual devices per database.

Scheduling backups

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

Scheduling example

To schedule a database backup 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 on page 46 and Step 2 on page 46 to schedule backups at 13:00 and 18:00.
4. Click **Apply** to save the changes.

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 start and select **Start Backup**.
3. Select **Backup type** and **Network load**. For information on these options, click **Help**. Click **OK**.

Restore

Data Protector offers different restore types depending on your needs. You can select point-in-time restore, full database restore, as well as restore your SQL Server data to a new location, to another SQL Server or another SQL Server instance. For detailed information, see "Restore options" on page 51.

Restore methods

You can restore SQL Server databases using:

- The Data Protector GUI. See "Restoring using the Data Protector GUI " on page 47.
- The Data Protector CLI. See "Restoring using the Data Protector CLI" on page 54.

Before you begin

- Before starting restore, verify that the database is not being in use.

Restoring using the Data Protector GUI

NOTE:

On SQL Server 2000 and higher, there is no need to create an empty database before restore, because the database and its files are generated automatically.

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 MS SQL Server 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:

   - With Microsoft SQL Server 2000 or 2005, select the backed up databases or data files you want to restore.

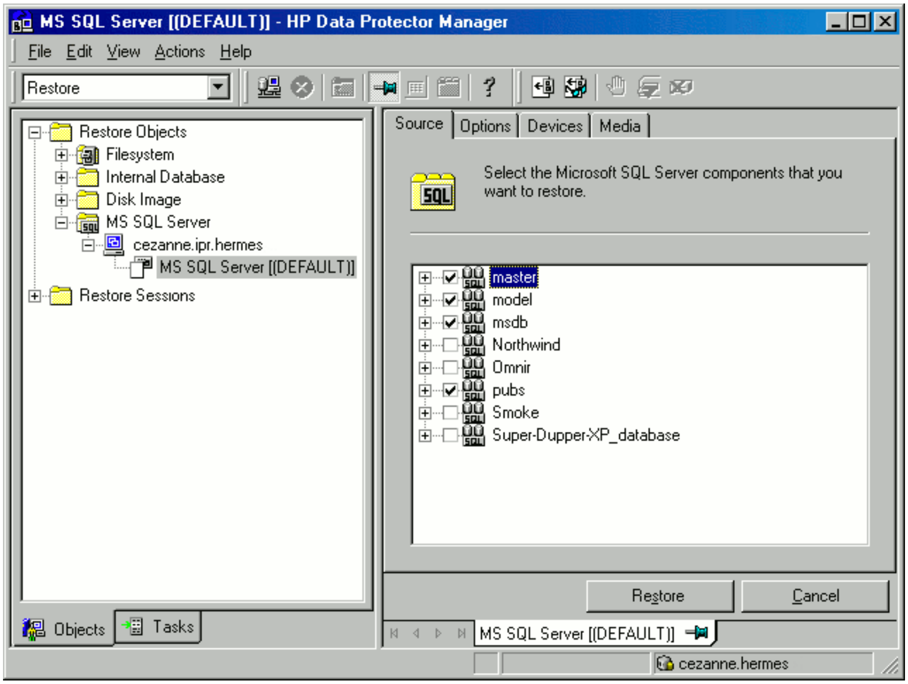
     To restore a file group, expand it and select all data files in it.

IMPORTANT:

Before a data file can be restored, the active transaction log of the database must be backed up. In case the log has been corrupted, particular data files cannot be restored, and you can only restore the entire database.

   - With Microsoft SQL Server versions prior to 2000, select the backed up databases you want to restore.

   See Figure 12 on page 48.

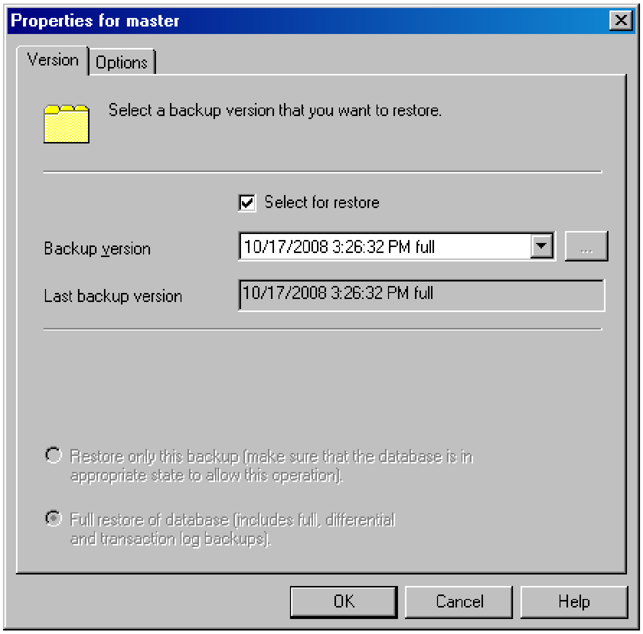


Select the Microsoft SQL Server components that you want to restore.

☑ master
☑ model
☑ msdb
□ Northwind
□ Omnir
☑ pubs
□ Smoke
□ Super-Dupper-XP_database

Figure 12 Restore objects

To select backup object specific options, right-click the object and select **Properties**.



Properties for master

Version | Options

Select a backup version that you want to restore.

☑ Select for restore

Backup version: 10/17/2008 3:26:32 PM full

Last backup version: 10/17/2008 3:26:32 PM full

○ Restore only this backup (make sure that the database is in appropriate state to allow this operation).

● Full restore of database (includes full, differential and transaction log backups).

Figure 13 Selecting object specific options

You can select the version (backup date) from which you want to restore and choose SQL Server specific restore options. Note that some options are not available for restore of data files. See "Restore options" on page 51 for details.

Click **OK**.

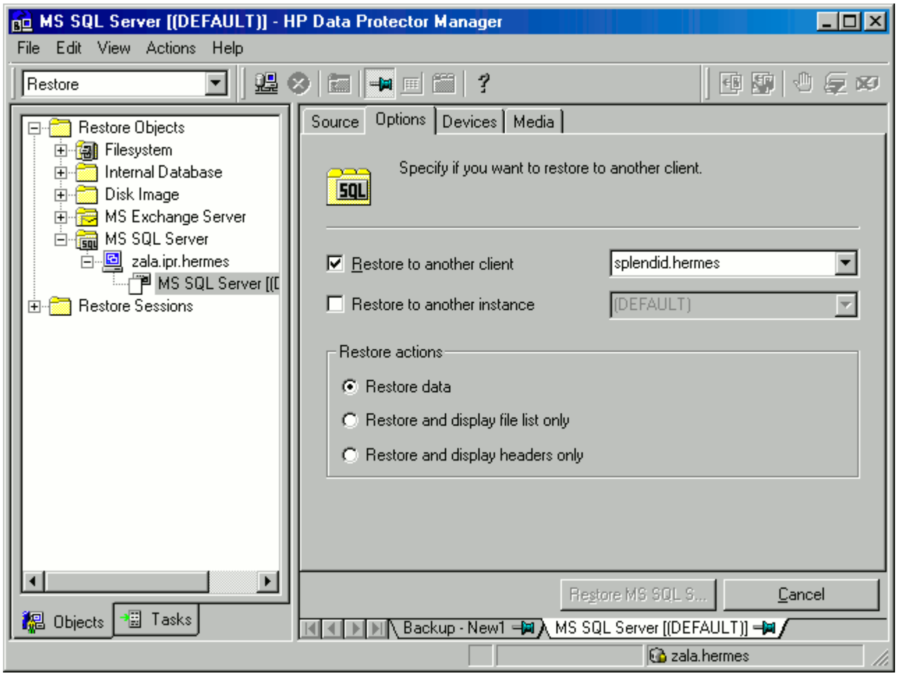
4. If you want to restore your data to another client or instance, specify new locations for the databases in the **Options** property page. See "Restore options" on page 51.

NOTE:

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.

Select one of the following **Restore actions**:

- **Restore data** (default). Select to restore the whole database.
- **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.



Specify if you want to restore to another client.

☑ Restore to another client: splendid.hermes

☐ Restore to another instance: (DEFAULT)

Restore actions

● Restore data

○ Restore and display file list only

○ Restore and display headers only

Figure 14 Restore options

5. In the **Devices** page, select devices to use for the restore.

   The **Automatic device selection** option is selected by default, but it is recommended to select the **Original device selection** option.

IMPORTANT:

If you decide to select the **Automatic device selection** option, ensure that the number of available devices is equal to or greater than the number of devices that were used for backup.

NOTE:

For restore, you can use a different device than you used for backup. For information on restoring using another device, see the online Help index: “selecting, devices for restore”.

6. Click **Restore MS SQL Server** and then **Next** to select **Report level** and **Network load**.

   Click **Finish** to start restore.

Restore options

Table 7 SQL Server 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. Only transaction logs written before the specified date and time are applied to the database.

Option	Description
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	Overwrites the existing database residing on the target SQL Server instance. If a database with the same name as the one you are restoring already exists and has a different internal structure, SQL Server does not let you rewrite the database unless you select this option. If you are restoring a data file from the PRIMARY group to an existing database, you *must* set this option for that data file.
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.

Option	Description
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 if you restore data to another server, instance, or make a database copy on the same server.

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 existing database**.

Restoring to another SQL Server instance or/and another 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 configuration procedure, see “Creating backup specifications” on page 39.

NOTE:

This restore type is supported on SQL Server 2000 and higher.

1. Select the databases you want to restore and their versions.

2. Select the following:
    - To restore to another SQL Server client, select **Restore to another client** and the target client from the drop-down list.
    - To restore to another SQL Server instance, select **Restore to another instance**. If there are no instances in the drop-down list, enter the instance name yourself.
    - Ensure that the specified SQL Server instance exists on the target client. Otherwise, restore fails.
3. Specify new database locations.
4. Start restore. See "Restore" on page 46.

Restoring using the Data Protector CLI

From the *Data_Protector_home*`\bin` directory, run:

```
omnir -mssql -barhost ClientName [-destination ClientName]
[-instance SourceInstanceName] [-destinstance
DestinationInstanceName] {—base DBName [—session SessionID]
[MSSQL_OPTIONS]... | —base DBName —datafile
GroupName/DataFileName —session SessionID
[DATAFILE_OPTIONS]...}
```

```
MSSQL_OPTIONS
```

```
-asbase NewDBName {-file LogicalFileName1 PhysicalFileName1
[-file LogicalFileName2 PhysicalFileName2]...}
```

```
-replace
```

```
-nochain
```

```
-recovery {rec | norec}
```

```
-standby File
```

```
DATAFILE_OPTIONS
```

```
-replace
```

```
-nochain
```

```
-recovery {rec | norec}
```

Provide the *Session_ID* of the backup session. For object copies, do not use the copy session ID, but the object backup ID (equals the object backup session ID).

For description of the CLI options, see the `omnir` man page or the *HP Data Protector command line interface reference*.

Examples

To restore the database `RONA` running on the SQL Server `ALMA` to the same destination, run:

```
omnir -msssql -barhost ALMA -base RONA
```

To restore the data file `DATAFILE_01` in the file group `FILEGROUP_02` of the database `RONA` running on the SQL Server `ALMA` to the same destination, run:

```
omnir -MSSQL -barhost ALMA -base RONA –datafile
FILEGROUP_02/DATAFILE_01 –session 2008/10/17-3
```

Disaster recovery

Disaster recovery is a complex process involving products from different vendors. Therefore, you need to check the instructions from the database/application vendor on how to prepare for disaster recovery.

As a first step, perform a general disaster recovery procedure described in the *HP Data Protector disaster recovery guide*. Next, restore SQL Server databases. See the below sections for instructions.

IMPORTANT:

If a disk failure occurred, recover the operating system prior to any other recovery tasks. Data Protector disaster recovery is used to bring the operating system back on the damaged system.

IMPORTANT:

When reinstalling SQL Server, ensure that you use original local settings. Before restoring to another client, ensure that local settings on the target system match the original.

Recovering the master database

The master database holds the vital information about SQL Server. If it gets corrupted or lost, all other databases become unavailable. Recover the master database first to make SQL Server operational:

1. Rebuild the master database.

   Create the basic master database:

   a. Shut down SQL Server if it is running.

   b. Start the Rebuild Master utility `SQL\bin\rebuildm.exe`.

   c. Select an appropriate character set and sort order to match the backed up data. You can check this in the latest backup session report.

   d. Rebuild the database.

   For more information, see the SQL Server documentation.

2. Set user rights or reconfigure the integration.

   Set user rights using SQL Server Enterprise Manager:

   a. From the server desktop, click **Start - Programs - Microsoft SQL Server 7/Microsoft SQL Server - Enterprise Manager**.

   b. Right-click the required server and select **Register Server**. Configure SQL Server to use trusted connections.

   c. Go to **Security - Logins** and select appropriate user rights.

   d. Return to the server, right-click its name, and select **Register Server**.

      Enter the account you selected in **Manage - Logins**.

      Perform any additional administration tasks required to run SQL Server.

   Reconfigure the SQL Server integration as described in "Creating backup specifications" on page 39.

3. Stop SQL Server services by going to **Start - Programs - Microsoft SQL Server 7**, starting SQL Service Manager and stopping the services.

4. Start SQL Server service in a single-user mode:

   a. In the **Control Panel**, go to **Administrative Tools**, **Services**.

   b. Select the MSSQL Server Service.

   c. Enter `–m` as a start-up parameter and start the services.

5. Restore the master database using the Data Protector Manager.
6. Restart SQL Server services in normal mode.

   After the master database is recovered, the SQL Server service is automatically shut down. Start SQL Server Service Manager and restart SQL services.

IMPORTANT:

To complete disaster recovery, restore *all* other databases as well (or reattach databases if they exist on disks to the newly-rebuilt master database). See "Recovering user databases" on page 57.

Recovering user databases

To restore user databases, proceed as described in "Restore" on page 46.

Note that restoring databases to a certain state often requires a multiphase restore. This means that multiple versions need to be restored to retrieve the data. The latest full backup, the latest differential backup and all transaction log backups after the last full or differential backup must be restored.

Example

Suppose you have the following backup sequence:

F D T T *D* *T* *T* *T* ***T*** T

and want to restore the version marked ***T***, then all the backup versions in *italic* will be restored.

TIP:

You can restore versions one by one to have more control over the restore process. Use the options **Restore only this backup** and **Recovery completion state** to do this.

For more information on disaster recovery, see the *HP Data Protector disaster recovery guide* and the SQL Server documentation.

Performance tuning

Performance tuning means customizing your environment to improve backup and restore performance. Follow these guidelines:

1. Ensure that SQL Server database files are on separate disks.
2. Calculate the number of devices to be used in parallel. Select a number of devices matching the bandwidth of the incoming data stream and identify the bottleneck. This can either be the network, if devices are connected to remote systems, or SQL Server, if the devices are connected locally.

   As the network bandwidths are most often ~10 MB/s (100 Mbit Ethernet), though the actual throughput is usually lower, you will not need more than one fast device (such as DLT 7000 for remote backups).

   There are two possibilities for locally connected devices:

   a. Devices are dedicated to local SQL Server backups and backup/restore performance is important. Use fast direct mode, which enables Data Protector to read data directly from the SQL Server shared memory and can therefore increase the backup speed to local devices.

   b. Devices are shared within the Data Protector cell and backup/restore performance is not very important. Disable fast direct mode.

   Determine the maximum backup speed by backing up to a few null file devices on a local server, and select the number of devices that fits best with the measured performance.

TIP:

Create separate backup specifications for local and remote devices. It is not recommended to use both in one backup specification.

3. Adjust block sizes for local backup devices.

   - Enable/disable **Fast direct mode**.

     Use this option only if the highest performance is required. Due to specific device settings, these device definitions should not be shared with conventional (filesystem) backups. Therefore, using this option in general is not recommended.

     Disable **Fast direct mode** (as well as special local device settings) if backup performance is not very critical and/or other data is backed up to devices connected to SQL Server.

> NOTE:
>
> Fast direct mode is ignored for remote devices.

   - Set the block size (if **Fast direct mode** is enabled).

     Adjusted block sizes are calculated as follows:

```
block size (kB) = 64*N + 4 (N=1,...,64)
block size (kB) = 68, 132, ..., 4100 kB
```

     All selected devices must have the same block size.

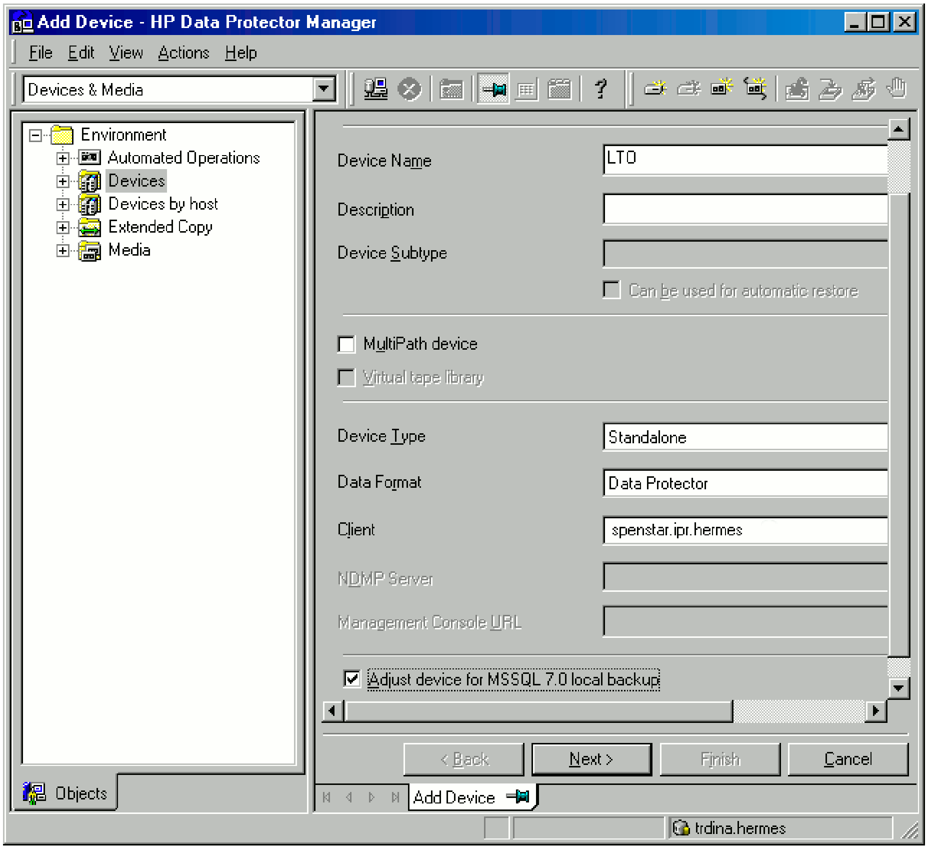
     You can gain some performance improvement by specifying a block size larger than 68 KB (recommended). You can also increase the block size step by step and compare the performance achieved for each step.

     You can adjust block size during the initial device definition for local devices by checking the attached check box and selecting the block size. See Figure 15 on page 60.

     You can modify block size later; however, you must first calculate it using the formula above and then insert the value as shown in Figure 16 on page 61.

   - Modify the registry.

     To use block size larger than 56 KB, some SCSI interface cards require you to adjust related values in the registry of the system where the device is connected. See the online Help index: “changing block size” for instructions.



Device Name: LTO

Description:

Device Subtype:

☐ Can be used for automatic restore

☐ MultiPath device

☐ Virtual tape library

Device Type: Standalone

Data Format: Data Protector

Client: spenstar.ipr.hermes

NDMP Server:

Management Console URL:

☑ Adjust device for MSSQL 7.0 local backup

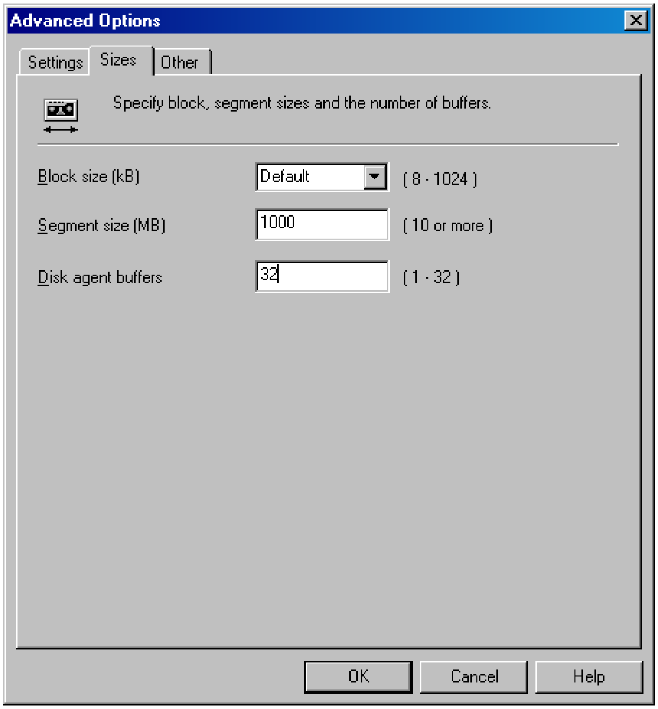
Figure 15 Adjusted local device

To modify block sizes of an existing device:

a. Switch to the **Devices & Media** context.

In the Scoping Pane, expand **Devices** and click the locally connected device you want to modify. In the Results Area, select **Settings**, and then click **Advanced**.

b. In the **Advanced Options** window, click **Sizes**.



Specify block, segment sizes and the number of buffers.

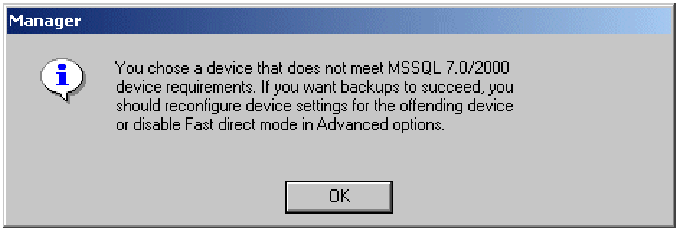
Block size (kB) Default (8 - 1024)

Segment size (MB) 1000 (10 or more)

Disk agent buffers 32 (1 - 32)

Figure 16 Advanced options

If **Fast direct mode** is activated and not all selected local devices in a backup specification are adjusted accordingly, you get the warning when saving the backup specification:



You chose a device that does not meet MSSQL 7.0/2000 device requirements. If you want backups to succeed, you should reconfigure device settings for the offending device or disable Fast direct mode in Advanced options.

Figure 17 Block sizes not adjusted

4. Scheduling.

   Backup schedule depends on the number of transactions on the server. Generally, you should not let transaction log files grow over a certain limit, which depends on a specific production database and the size of its transaction log files. These are some general rules on how to schedule backups:

   - Weekly full backup
   - Differential backup daily
   - Transaction log backups as needed

   Schedule full and differential backups when the server is not heavily loaded (nights and weekends). Do transaction log backups several times a day.

   The final decision on scheduling must be made according to the actual database configuration.

   For more information, see the SQL Server documentation and the online Help.

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 online 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" on page 64. 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*.

Before you begin

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

Checks and verifications

If your configuration, backup, or restore failed:

- Check that SQL Server services are running.
- Examine system errors reported in `*Data_Protector_home*\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 online 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 restore, if the following error occurred when executing an SQL statement:

```
Error message: "Microsoft SQL-DMO (ODBC SQLState: 01000)?15[152:5]
1646 [Microsoft][ODBC SQL Server Driver][SQL Server]The master database
has been successfully restored. Shutting down SQL Server.[Microsoft]
[ODBC SQL Server Driver] [SQL Server]SQL Server is terminating this
process."
```

note that this is the expected behavior when the master database is restored in a 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@computer1.com "MSSQL70"
  Time: 3/14/2000 8:19:22 PM
  Error has occurred while executing SQL statement.
  Error message: 'Microsoft SQL-DMO (ODBC SQLState: 42000) Error
  number: bc5
  [Microsoft][ODBC SQL Server Driver][SQL Server]Backup or restore
  operation terminating abnormally.'
  [Critical] From: OB2BAR@computer1.com "MSSQL70"
  Time: 3/14/00 8:19:24 PM
  Received ABORT request from SM => aborting
  ```

- SQL Server error log contains an entry similar to:

  ```
  2000-03-14 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:

```
2000/03/15 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 if concurrency is set to more than one and one of the devices fails or is not started at all

This can happen because of a medium error.

Action

Set the device concurrency to one or replace the invalid media.

Problem

Restore from an object copy fails

When you try to restore an SQL Server database from an object copy session, the restore fails.

An SQL Server database backed up using multiple streams (the **Concurrent streams** option set to more than 1) can only be restored if the backup objects created by the streams reside on separate media. During a Data Protector Microsoft SQL Server backup, each stream is always backed up to a separate medium. However, if you copy these backup objects on the same medium, using the object copy functionality, and start a restore from the object copy session, the restore fails.

Action

Before restarting the restore:

1. Increase the number of Disk Agent buffers for the device.
2. In the **Internal Database** context, find the objects belonging to the same backup (identified by the same backup ID).

3. Copy each object in a separate object copy session to a separate device, for example a file library. For each object, use a separate medium with the non-appendable media policy.
4. Set the highest media location priority for the newly created copies.

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

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” on page 30).

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

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 "Restoring using the Data Protector GUI " on page 47.
11. Click **OK** to close the Properties window.
12. In the Options, Devices, and Media property pages, specify the appropriate options. For details, see "Restoring using the Data Protector GUI " on page 47.
13. Click **Restore** and then **Next** to select the Report level and Network load.
14. Click **Finish** to start the restore session.

2 Integrating Microsoft SharePoint Portal Server and Data Protector

Introduction

This chapter explains how to configure and use the Data Protector Microsoft SharePoint Portal Server integration (SPS integration). It describes concepts and methods you need to understand to back up and restore the following SharePoint Portal Server objects (SPS objects):

- Content databases (team databases)
- Site databases (*portal_name*_SITE, *portal_name*_SERV, *portal_name*_PROF)
- Index servers
- Single sign-on database
- Document library

Data Protector integrates with Microsoft SharePoint Portal Server (SPS Server) to back up SPS objects online. During backup, the SPS Server and Microsoft SQL Server instances are online and actively used.

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

Table 8 Backup types

Full	Backs up all selected objects.
Trans (MS SQL Server objects only)	Backs up only transaction logs of the selected SQL Server databases. Other selected SPS objects are backed up completely.

Differential (MS SQL Server objects only)	Backs up only changes made to the selected SQL Server databases since the last full backup. Other selected SPS objects are backed up completely. Before you run a differential backup, ensure that a full backup exists. Otherwise, a restore from such a differential backup session fails.

You can restore SQL Server databases to the original location or:

- To another SQL Server system
- To another SQL Server instance
- Under different names

You can restore SPS index servers to the original location or:

- To another client
- To another directory

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

Integration concepts

Data Protector integrates with SPS Server through the Data Protector integration agents (SPS and SQL agents), which channel communication between the Data Protector Session Manager and the clients in the SPS farm.

Whether your SPS environment consists of a single server system or multiple server systems (small, medium, or large farm), the architecture of the integration is basically the same.

Figure 18 on page 71 shows the architecture of the Data Protector integration with a SPS medium server farm.

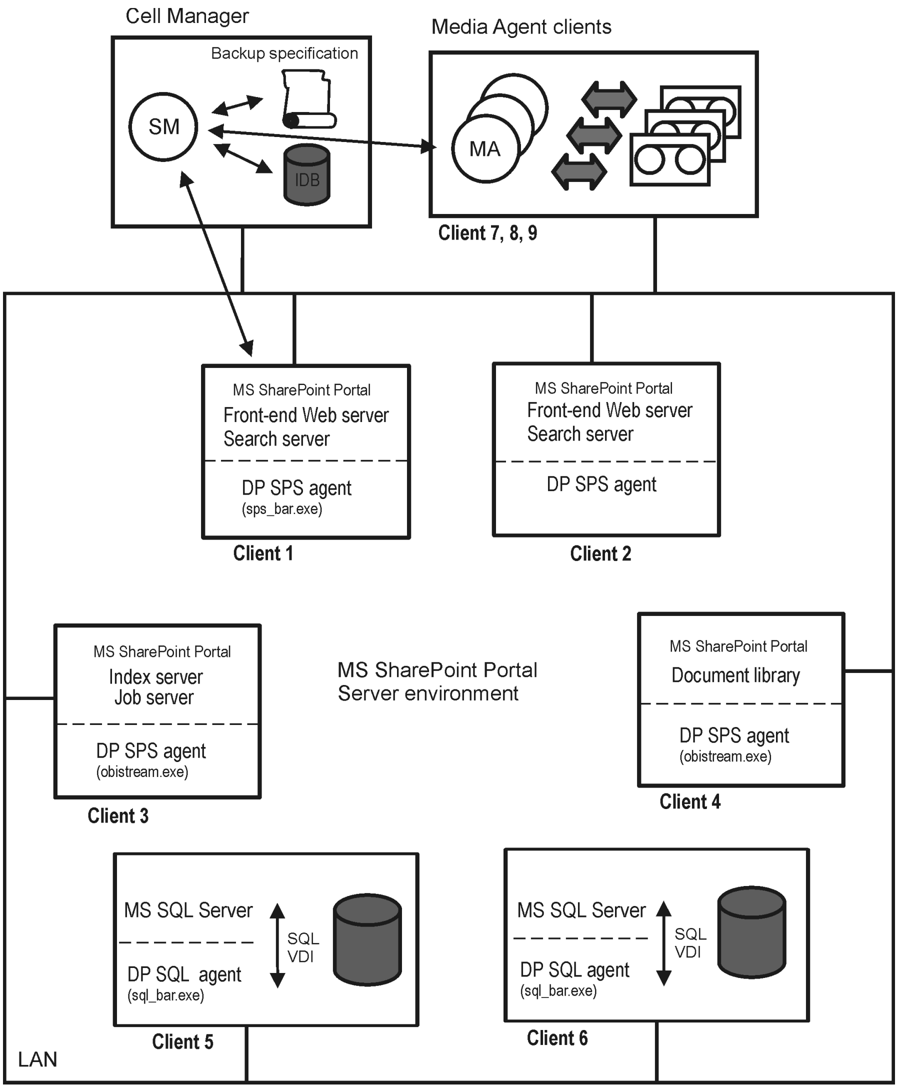


Figure 18 SPS integration architecture

Table 9 Legend

SM	Data Protector Session Manager: Backup Session Manager during backup and Restore Session Manager during restore
Backup Specification	A list of objects to be backed up, backup devices, and options to be used

IDB	The Data Protector Internal Database
DP SPS agent	A set of Data Protector executables that enable data transfer between SPS Server and Data Protector media
DP SQL agent	A set of Data Protector executables that enable data transfer between SQL Server and Data Protector media
SQL VDI	SQL Server virtual device interface, through which SQL Server and Data Protector exchange control and data
MA	Data Protector General Media Agent
LAN	Local Area Network

Table 10 briefly describes the SPS objects that you can back up and restore using the Data Protector SPS integration.

Table 10 SPS objects

SPS object	Description
Content database	Virtual server specific SQL Server database that stores Web site data.
Site databases	Portal specific SQL Server databases: • *portal_name*_PROF Contains user profiles and audiences. • *portal_name*_SERV Stores information for services, such as search and alerts, provided by the portal. • *portal_name*_SITE Contains site content information.
Index server	Data used by index management server, which builds and updates indexes, and crawls content.
Single sign-on database	SQL Server database that stores account credentials. The single sign-on functionality enables users to retrieve information from third-party applications without additional sign-on operations.

SPS object	Description
Document library	Folder that stores files. Each file is associated with user-defined information.

Backup and restore flow

The following procedure assumes that all SPS objects are selected for backup/restore.

1. Data Protector Session Manager starts `sps_bar.exe` on the front-end Web server client, providing a list of objects to be backed up/restored.
2. The `sps_bar.exe` agent browses the SharePoint Portal Server topology.
3. For each portal:
   a. The `sps_bar.exe` agent starts `sql_bar.exe` on the SQL Server clients on which the portal site and content databases reside.

      The `sql_bar.exe` agent establishes connection with the Session Manager and sends backup/restore requests to the SQL Server using the SQL Server VDI. The actual data transfer is then performed by the SQL Server. The databases are backed up/restored in parallel.

   b. If the portal provides index service, `sps_bar.exe` also starts `obistream.exe` on the client functioning as index server. `obistream.exe` establishes connection with the Session Manager to enable backup/restore data flow for the index server database.
4. The `sps_bar.exe` agent starts `obistream.exe` on the document library client. `obistream.exe` establishes connection with the Session Manager to enable backup/restore data flow for the document library database.
5. The `sps_bar.exe` agent starts `sql_bar.exe` on the SQL Server client on which the single sign-on database resides, which is then backed up/restored like all the other SQL Server databases.

Configuring the integration

You need to configure the SPS farm and SPS users.

Prerequisites

- Ensure that you have correctly installed and configured SPS Server.
  - For supported versions, platforms, devices, and other information, see the latest support matrices at http://www.hp.com/support/manuals.
  - For information on installing, configuring, and using SPS Server, see the Microsoft SharePoint Portal Server documentation.
- 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*.

  The following Data Protector components must be installed:
  - `MS SharePoint Portal Server Integration` - on SPS Server systems
  - `MS SQL Integration` - on SQL Server systems

Before you begin

- Configure devices and media for use with Data Protector.
- On every client in the SPS farm, restart the Data Protector `Inet` service under a Windows domain user account that has Windows administrative rights on the client. For information, see the online Help index: "changing Data Protector Inet account".
- To test whether the SPS farm and the Cell Manager communicate properly, configure and run a Data Protector filesystem backup and restore on every client system in the farm.

Configuring SPS users

For every client in the SPS farm, add the Windows domain user account under which the Data Protector `Inet` service is running to the Data Protector `admin` or `operator` user group. For details on adding users to Data Protector groups, see the online Help index: "adding users".

Configuring SPS farms

You need to provide Data Protector with the following configuration parameters for the SPS farm:

- SPS administrator
- Password

- Domain

Data Protector then creates the SPS configuration file on the Cell Manager and verifies the connection to the farm.

Before You Begin

- Ensure that the SPS Server and SQL Server instances are online.

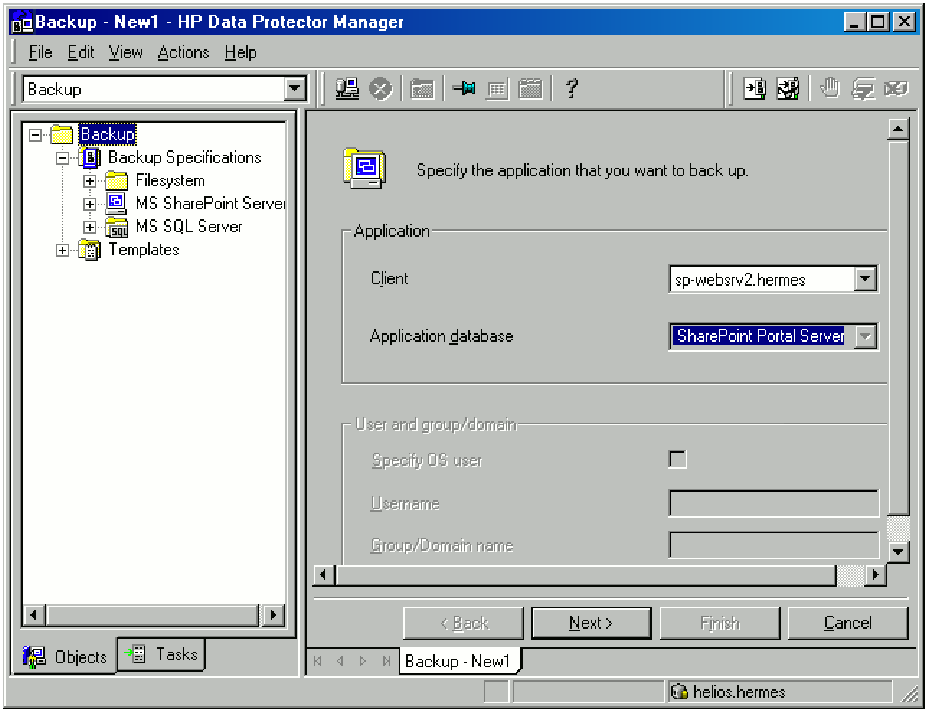
To configure the SPS Server, use the Data Protector Manager:

1. In the Context List, click **Backup**.
2. In the Scoping Pane, expand **Backup Specifications**, right-click **MS SharePoint Server**, and click **Add Backup**.
3. In the **Create New Backup dialog box**, click **OK**.

4. In **Client**, select the front-end Web server system of the SPS farm.

NOTE:

In a farm with multiple front-end Web server systems, select one of them.



Backup - New1 - HP Data Protector Manager

Specify the application that you want to back up.

Application

Client: sp-websrv2.hermes

Application database: SharePoint Portal Server

User and group/domain

Specify OS user □

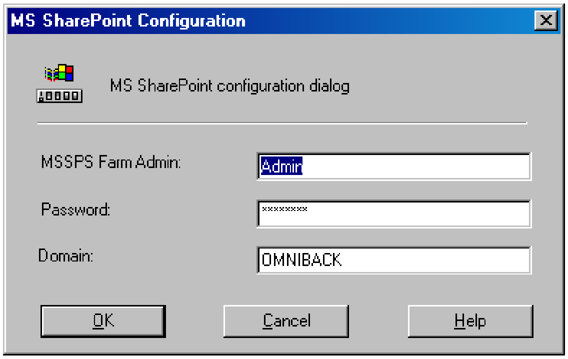
Username

Group/Domain name

Figure 19 Selecting a front-end Web server system

Click **Next**.

5. In the **MS SharePoint Configuration** dialog box, type the SPS administrator, its password, and domain.



MS SharePoint Configuration

MS SharePoint configuration dialog

MSSPS Farm Admin: Admin

Password: ********

Domain: OMNIBACK

Figure 20 Configuring an SPS farm

Click **OK**.

6. The SPS Server farm is configured. Exit the GUI or proceed with creating the backup specification at Step 6 on page 130.

Checking the configuration

You can verify the connection to the SPS farm after you have created at least one backup specification for the farm.

To verify the connection, use the Data Protector Manager:

1. In the Context List, select **Backup**.
2. In the Scoping Pane, expand **Backup Specifications** and then **MS SharePoint Server**. Click the backup specification to display the SPS farm to be checked.
3. Right-click the front-end Web server system of the SPS farm and click **Check configuration**.

Backup

You can back up the following SPS objects:

- Content databases (team databases)
- Site databases (`*portal_name*_SITE`, `*portal_name*_SERV`, `*portal_name*_PROF`)
- Index servers

- Single sign-on database
- Document library

The integration provides online backups of the following types:

Table 11 Backup types

Full	Backs up all selected objects.
Trans (MS SQL Server objects only)	Backs up only transaction logs of the selected SQL Server databases[1]. Other selected SPS objects are backed up completely.
Differential (MS SQL Server objects only)	Backs up only changes made to the selected SQL Server databases[1] since the last full backup. Other selected SPS objects are backed up completely. Before you run a differential backup, ensure that a full backup exists. Otherwise, a restore from such a differential backup session fails.

[1] SQL Server databases are content databases, site databases, and the single sign-on database.

For details on SQL Server transaction log backups and differential database backups, see the Microsoft SQL Server documentation.

NOTE:

If the encryption key is used for the single sign-on service, back up the encryption key as described in Microsoft SharePoint Portal Server documentation.

Before you begin

- Ensure that the SPS services run under the SPS administrator account.

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 **MS SharePoint Server**, and click **Add Backup**.
3. In the **Create New Backup** dialog box, click **OK**.

4. In **Client**, select the front-end Web server system of the SPS farm.

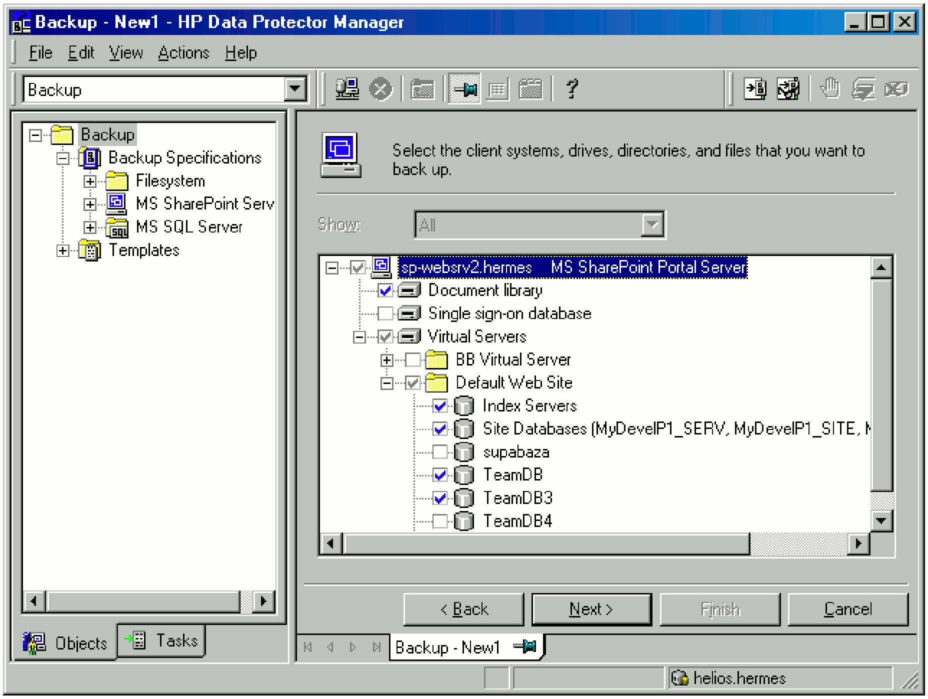
NOTE:

In a farm with multiple front-end Web server systems, select the one that was specified during the configuration.

Click **Next**.

5. If the SPS farm is not configured for use with Data Protector, the **MS SharePoint Configuration** dialog box is displayed. Configure it as described in "Configuring SPS farms" on page 74.

6. Select SPS objects to be backed up.



Select the client systems, drives, directories, and files that you want to back up.

- ☑ sp-websrv2.hermes MS SharePoint Portal Server
  - ☑ Document library
  - ☐ Single sign-on database
  - ☑ Virtual Servers
    - ☐ BB Virtual Server
    - ☑ Default Web Site
      - ☑ Index Servers
      - ☑ Site Databases (MyDevelP1_SERV, MyDevelP1_SITE, M
      - ☐ supabaza
      - ☑ TeamDB
      - ☑ TeamDB3
      - ☐ TeamDB4

Figure 21 Selecting SPS objects

Click **Next**.

7. 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 you will use.

   NOTE:

   Every site database, service database, profile database, content database, portal metadata, document library, and index server can be backed up in a separate stream.

   Click **Next**.

8. Set backup options. For information on application specific backup options, see Table 12 on page 81.

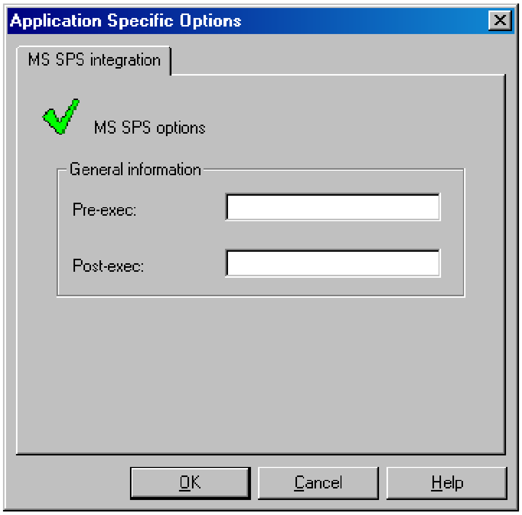


Figure 22 Application specific options

   Click **Next**.

9. Optionally, schedule the backup. See "Scheduling backup specifications" on page 81.

   Click **Next**.

10. 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” on page 82.

Table 12 SPS backup options

Options	Description
Pre-exec, **Post-exec**	Specify a command to be run by `sps_bar.exe` on the front-end Web server system before the backup (`pre-exec`) or after it (`post-exec`). Do not use double quotes. Type only the name of the command and ensure that the command resides in the *`Data_Protector_home`*`\bin` directory on the front-end Web server system.

Modifying backup specifications

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

Scheduling backup specifications

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

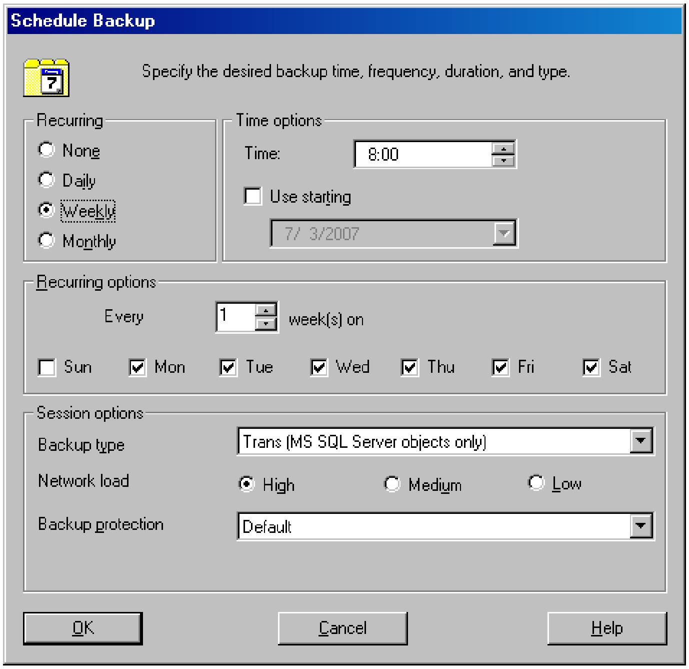
Scheduling example

To schedule transaction log backups of selected SPS objects 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 Figure 23 on page 82. Under **Session options**, select **Trans (for SQL objects only)** from the **Backup type** drop-down list.

   Click **OK**.

3. Repeat Step 1 on page 81 and Step 2 on page 81 to schedule backups at 13:00 and 18:00.
4. Click **Apply** to save the changes.



Schedule Backup

Specify the desired backup time, frequency, duration, and type.

Recurring

○ None
○ Daily
● Weekly
○ Monthly

Time options

Time: 8:00

□ Use starting

7/ 3/2007

Recurring options

Every 1 week(s) on

□ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat

Session options

Backup type: Trans (MS SQL Server objects only)

Network load: ● High ○ Medium ○ Low

Backup protection: Default

Figure 23 Scheduling a backup specification

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 SharePoint Server**. Right-click the backup specification you want to preview and click **Preview Backup**.
3. Specify the **Backup type** and **Network load**. Click **OK**.

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

Using the Data Protector CLI

From the directory *`Data_Protector_home`*`\bin`, run:

```
omnib -mssps_list backup_specification_name -test_bar
```

What happens during the preview?

The following is tested:

- Communication between the SPS Server and Data Protector
- 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.

To start a backup, use the Data Protector GUI or CLI.

Before you begin

- Ensure that the SPS Server and SQL Server instances are online.

Using the Data Protector GUI

1. In the Context List, click **Backup**.
2. In the Scoping Pane, expand **Backup Specifications**, and then **MS SharePoint Server**. Right-click the backup specification you want to start 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

From the directory *Data_Protector_home*\bin, run:

```
omnib -mssps_list backup_specification_name [-barmode
SPS_mode][List_options]
```

where *SPS_mode* is one of the following backup types:

```
full|trans|diff
```

For *List_options*, see the omnib command in the HP Data Protector command line interface reference.

Examples

To start a full backup using the backup specification MyWebPortals, run:

```
omnib -mssps_list MyWebPortals -barmode full
```

To start a differential backup using the same backup specification, run:

```
omnib -mssps_list MyWebPortals -barmode diff
```

Preparing for disaster recovery

To prepare for a disaster recovery, back up the following objects:

Table 13 What must be backed up

Objects	How to back up
IIS database (from all the front-end Web server clients)	Use Data Protector filesystem backup. For details, see online Help. IIS database of a particular client is located in the client CONFIGURATION.
Encryption key (if it is used for the single sign-on service)	See the Microsoft SharePoint Portal Server documentation.
Master database (of all the SQL Server instances)	Use the Data Protector SQL Server backup. For details, see Chapter 1 on page 27.
SPS objects	Use the Data Protector SPS backup.

Restore

You can restore SPS objects using the Data Protector GUI or CLI.

Before you begin

- Ensure that the SPS Server and the SQL Server instances are online and that the SPS services run under the SPS administrator account.
- If you plan to restore SQL Server databases to another location:
  - Ensure that the destination SQL Server system is part of the SharePoint Portal Server environment and has the `MS SQL Integration` component installed.
  - Ensure that the destination SQL Server instance exists, is configured for use with Data Protector, and is online.
- The following is applicable only if encryption key is used for the single sign-on service: before restoring the single sign-on database, ensure that you use the same encryption key as was used during backup.

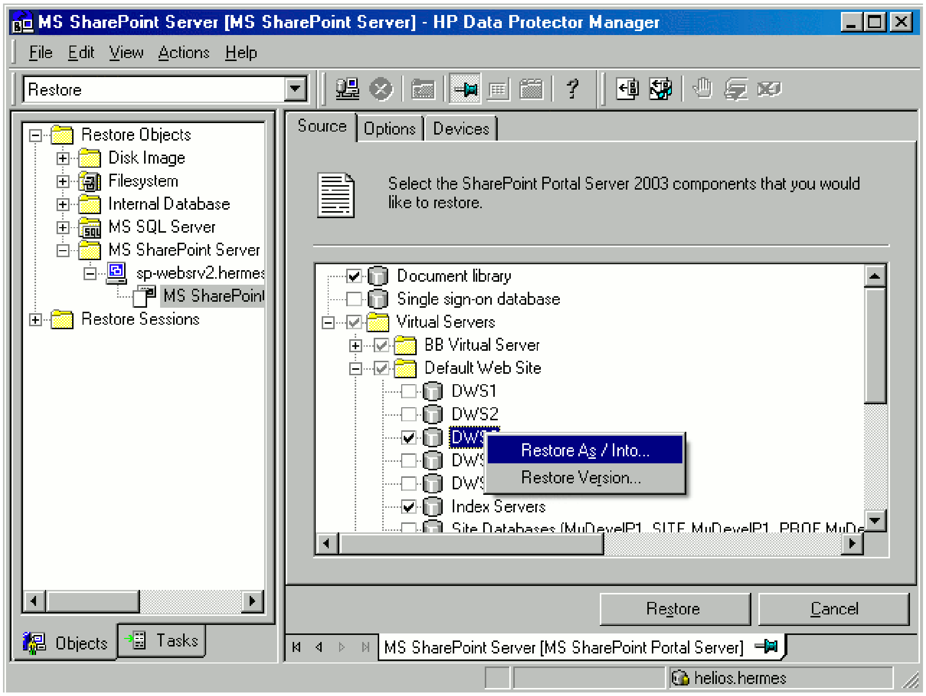
Considerations

- If you have two or more SPS farms within the same Data Protector cell, you cannot restore/migrate SPS objects from one farm to another.

Restoring using the Data Protector GUI

1. In the Context List, click **Restore**.
2. In the Scoping Pane, expand **MS SharePoint Server**, expand the front-end Web server system of the SPS farm to be restored, and then click **MS SharePoint Server [MS SharePoint Portal Server]**.

3. In the **Source** page, select SPS objects to be restored.



Select the SharePoint Portal Server 2003 components that you would like to restore.

Figure 24 Selecting SPS objects for restore

You can specify a backup version to restore from for each SPS object separately: right-click an object and click **Restore Version**.

For an SQL Server database, Data Protector automatically restores the full chain. For example, if you select:

Full backup	Data Protector restores the selected backup session.
Differential backup	Data Protector first restores the latest Full backup and then the selected Differential backup.
Trans backup	Data Protector first restores the latest Full backup, then the latest Differential backup (if one exists) and all the Trans backups from the latest Differential or Full backup up to the selected version.

You can specify the restore destinations for SQL Server databases and index servers: right-click a database/index server and click **Restore As/Into**.

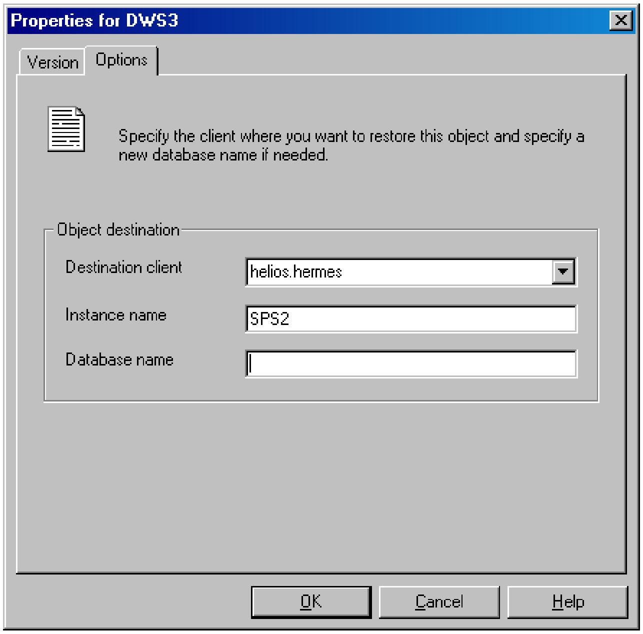
You can restore an SQL Server database to a different SQL Server system, SQL Server instance, or under a different name. See Figure 25 on page 87.

NOTE:

To restore to a not-named (default) SQL Server instance, type `(DEFAULT)` in the **Instance name** text box.

NOTE:

Site databases (*portal_name*`_PROF`, *portal_name*`_SERV`, *portal_name*`_SITE`) cannot be restored under a different name.



Specify the client where you want to restore this object and specify a new database name if needed.

Object destination

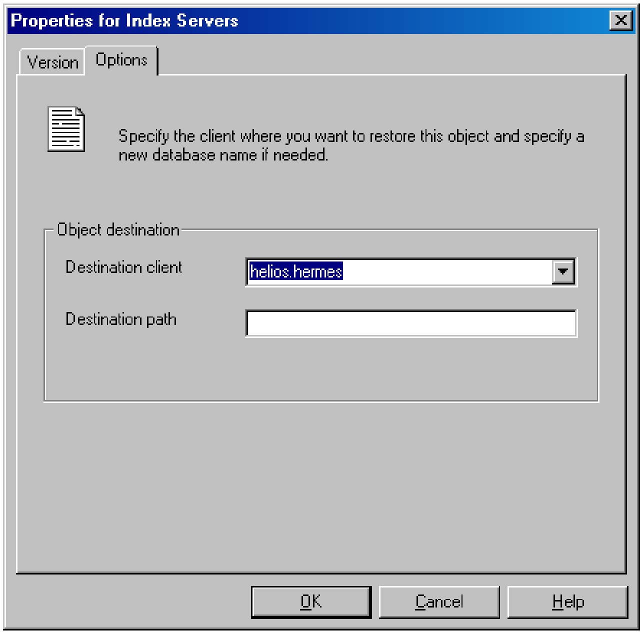
Destination client: helios.hermes

Instance name: SPS2

Database name:

Figure 25 Specifying the restore destination for an SQL Server database

You can restore an index server to a different client or directory. See Figure 26 on page 88.



Properties for Index Servers

Version | Options

Specify the client where you want to restore this object and specify a new database name if needed.

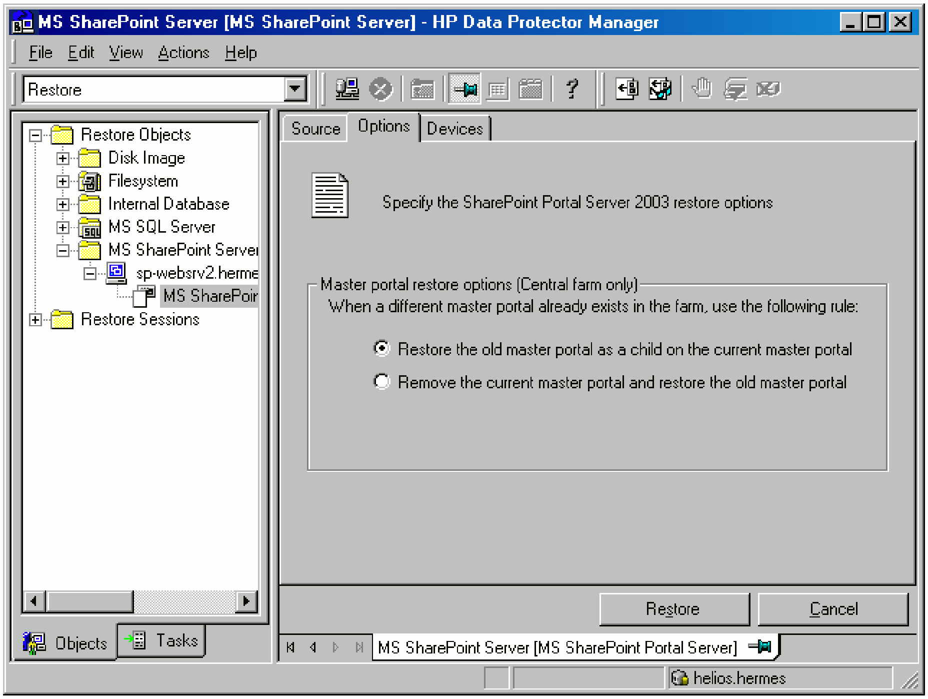
Object destination

Destination client: helios.hermes

Destination path:

Figure 26 Specifying the restore destination for an index server

4. In the **Options** page, select the SPS specific restore options. These options are applicable only to farms that are centralized (having the master portal and child portals). Otherwise, the options are ignored.



MS SharePoint Server [MS SharePoint Server] - HP Data Protector Manager

Specify the SharePoint Portal Server 2003 restore options

Master portal restore options (Central farm only)

When a different master portal already exists in the farm, use the following rule:

● Restore the old master portal as a child on the current master portal

○ Remove the current master portal and restore the old master portal

Figure 27 SPS restore options

5. In the **Devices** page, select devices to use for restore.

   The **Automatic device selection** option is selected by default, but it is recommended to select the **Original device selection** option.

IMPORTANT:

If you decide to select the **Automatic device selection** option, ensure that the number of available devices is equal to or greater than the number of devices that were used for backup.

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.

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

Table 14 SPS restore options

Option	Description
Restore the old master portal as a child on the current master portal	Applicable only if your SPS farm is centralized (having the master and child portals) and you are restoring the master portal. If this option is ON, the old master portal is restored as a child portal on the current master portal. Default: ON.
Remove the current master portal and restore the old master portal	Applicable only if your SPS Server farm is centralized (having the master and child portals) and you are restoring the master portal. If this option is ON, the current master portal becomes a child of the restored master portal. Default: OFF.

Restoring using the Data Protector CLI

From the directory *Data_Protector_home*\bin, run:

```
omnir -mssps -barhost front_end_server MSSPS_options
```

where *MSSPS_options* are:

```
[-portal virtual_server {[-teamdb db_name SQL_options] [-index
index_options] [-sitedbs sitedbs_options]}] [-ssodb
SQL_options] [-doclib -session sessionID] [-changemaster]
```

SQL_options are:

```
-session sessionID [-tohost client] [-instance instance] [-as
new_dbname]
```

index_options are:

```
-session sessionID [-tohost client] [-todir directory]
```

and *sitedbs_options* are:

```
-session sessionID [-tohost client] [-instance instance]
```

Parameter description

front_end_server — Front-end Web server system. In a farm with multiple front-end Web servers, specify the same front-end Web server system that was used for the backup.

virtual_server — SPS virtual server of the portal to be restored.

-teamdb — Specifies a portal's content database for restore.

-session — Specifies a backup session to restore from.

-tohost — Specifies a client system to restore to. By default, SPS objects are restored to the original clients.

-instance — Specifies an SQL Server instance to restore to. By default, SQL Server databases are restored to the original SQL Server instances.

-as — Specifies a new name for the database to be restored. By default, databases are restored with the original names.

-index — Specifies the portal's index server for restore.

-todir — Specifies a directory to which to restore the portal's index server. By default, index servers are restored to the original directories.

-sitedbs — Specifies the portal's site databases (*portal_name*_PROF, *portal_name*_SERV, *portal_name*_SITE) for restore.

-doclib — Specifies the document library for restore.

-ssodb — Specifies the single sign-on database for restore.

-changemaster — Applicable only if you are restoring the master portal. If this option is specified, the current master portal becomes a child of the restored master portal.

Example

To restore the content database `TeamDB1` (from the backup `2006/10/9-34`) and `Index Server` (from the backup `2006/2/7-31`) of the portal created on the SPS virtual server `Virtual1` that belongs to the farm with the `Front1.company.com` front-end Web server system, run:

Example

```
omnir -mssps -barhost Front1.company.com -portal Virtual1
-teamdb TeamDB1 -session 2006/10/9-34 -index -session
2006/2/7-31
```

To restore the content database `TeamDB1` of the portal created on the SPS virtual server `Virtual2` that belongs to the farm with the `Front1.company.com` front-end Web Server system, under the name `TeamDB1_backup`, from the backup `2006/10/9-34`, run:

```
omnir -mssps -barhost Front1.company.com -portal Virtual2
-teamdb TeamDB1 -session 2006/10/9-34 -as TeamDB1_backup
```

Restoring using another device

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

Using the Data Protector GUI

On how to specify another device for restore using the Data Protector GUI, see the online Help index: “restore, selecting devices for”.

Using the Data Protector CLI

If you are restoring using the Data Protector CLI, specify the new device on the Cell Manager in the file:

`Data_Protector_home``\Config\Server\cell\restoredev`

Disaster recovery

Disaster recovery is a very complex process, involving products from different vendors. Therefore, you need to check the instructions from the database/application vendor on how to prepare for disaster recovery.

To do a disaster recovery of a SharePoint Portal Server farm:

1. Reinstall the SharePoint Portal Server farm (including Windows Server 2003, IIS, SQL Server). For details, see the Microsoft SharePoint Portal Server documentation.
2. Reinstall the Data Protector integration components and import the SharePoint Portal Server clients in the Data Protector cell.
3. Recover the master databases of all the SQL Server instances. For details, see "Recovering the master database" on page 56.
4. Restore IIS databases to corresponding front-end Web server clients using the Data Protector filesystem restore.
5. Restore the encryption key (if it was used for the single sign-on service). For details, see the Microsoft SharePoint Portal Server documentation.
6. Restore other SPS objects (site databases, content databases, index servers, document library, single sign-on database) using the Data Protector SPS integration.

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.

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

Troubleshooting

This section lists general checks and verifications, plus problems you might encounter when using the SPS integration.

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

Before you begin

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

Checks and verifications

If your configuration, backup, or restore failed:

- On the client system, examine system errors reported in the `debug.log` located in *`Data_Protector_home`*`\log`.
- Check if you can do a filesystem backup and restore on the problematic client. For information, see online Help.
- For each client in the SPS farm, ensure that the Data Protector `Inet` service is running under a Windows domain user account that is in the Windows Administrators group.

Additionally, if your configuration or backup failed:

- Ensure that the SPS Server and SQL Server instances are online.

Additionally, if your backup failed:

- Check the configuration of the SPS farm as described in “Checking the configuration” on page 77.

Problems

Problem

Restore of a portal fails

If the Site databases (*`portal_name`*`_SITE`, *`portal_name`*`_SERV`, *`portal_name`*`_PROF`) of a portal are deleted or corrupted, SPS Server may lock the configuration database, which prevents you from restoring the portal (and the Site databases).

Action

1. Restart the services of the SPS Server and the SQL Server instance to unlock the configuration database.
2. Restart the restore.

Problem

Restore fails with “Object reference not set to an instance of an object”

When you start a restore of individual content databases (not the whole portal) to an unextended virtual server, an error similar to the following is displayed:

```
[Critical] From: OB2BAR_SPS_BAR@siska.hermes.com "MSSPS" Time:
10.1.2007 16:12:32 SPS_FarmRestore failed with error
System.NullReferenceException: Object reference not set to
an instance of an object.
```

Action

1. Extend the virtual server.
2. Restart the restore.

You do not need to extend the virtual server when restoring the whole portal.

Problem

Restore from a differential backup fails

When you start a restore from a differential backup, an error similar to the following is displayed:

```
[Critical] From: OB2BAR_Main@siska.hermes.com "MSSPS" Time:
21.12.2006 11:55:57
```

```
There are no objects in the Data Protector Internal Database
for object 'TESTNOOk1_SERV'.
```

You cannot restore from a differential backup if you do not have a full backup.

Action

Ensure that a full backup exists before you run a differential backup.

Problem

Backup of index servers fails

If the SPS services run under a user account different than the SPS administrator account and you start a backup of index servers, the following error is displayed:

```
Exception occurred during backup of search server! Access is
denied.
```

Action

1. Start the SPS services under the SPS administrator account.
2. Restart the backup.

Problem

Restore to another SQL Server instance fails

If you start a restore of SQL Server databases to an SQL Server instance that does not exist or is not online, an error similar to the following is displayed:

```
[Critical] From: OB2BAR_SPS_BAR@sp-websrv2.hermes.com "MSSPS"
Time: 1/4/2007 9:21:56 AM
```

```
RestorePortal failed with error
System.Data.SqlClient.SqlException: SQL Server does not exist
or access denied.
```

Action

1. Ensure that the SQL Server instance that you plan to restore to exists, configure it for use with Data Protector, and ensure that it is online.
2. Restart the restore.

NOTE:

The error message may also contain a part starting with:

```
Unhandled Exception: System.Data.SqlClient.SqlException:
```

This is a Microsoft issue and can be fixed by installing the hotfix KB 904422. After installing the hotfix, this part of the error is not displayed. For more information, see:

http://support.microsoft.com/?id=904422

3 Integrating Microsoft Exchange Server and Data Protector

Introduction

This chapter explains how to configure and use the Data Protector Microsoft Exchange Server integration. It describes the concepts and methods you need to understand to back up and restore Microsoft Exchange Server (**Exchange Server**) database objects.

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

Table 15 Exchange Server online backup types

Full database backup	Includes all data (database and all log files) regardless of the changes made after the last backup.
Incremental backup	Includes log files only. Refers to the previous full or incremental backup, whichever was performed last. After the backup, log files are deleted. Before you run an incremental backup, ensure that a full database backup exists. Otherwise, a restore from such an incremental backup session fails.

Using the Exchange Server integration, you can back up and restore the whole server or particular databases listed below:

- Microsoft Exchange Server (Microsoft Information Store)
- Microsoft Exchange Server (Microsoft Key Management Service)
- Microsoft Exchange Server (Microsoft Site Replication Service)
- Single mailboxes. See Chapter 4 on page 123.

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

Integration concepts

Data Protector integrates with Exchange Server through the Data Protector `ese_bar.exe` executable, installed on Exchange Server. It controls the activities between Exchange Server and Data Protector backup and restore processes.

You can perform interactive and scheduled full and incremental database backups. The last full backup combined with incremental prevents data loss if a disk failure occurs. Transaction logs are backed up to perform rollforward recovery.

Exchange Server databases are grouped into **storage groups**. Exchange Server 2000/2003 supports up to 4 storage groups and up to 5 databases per storage group. Exchange Server 2007 supports up to 50 storage groups and up to 50 databases, where each storage group is limited to a maximum of 5 databases. The databases within a storage group are backed up sequentially. Storage groups are backed up in parallel. The maximum number of devices used in a session equals the number of storage groups you want to back up.

Using the Data Protector User Interface, you define which objects and object versions to restore. Data Protector then passes the information about objects and backup versions to the backup API. General Media Agents are started and the data flows from the media to the target Exchange Server. See Figure 28.

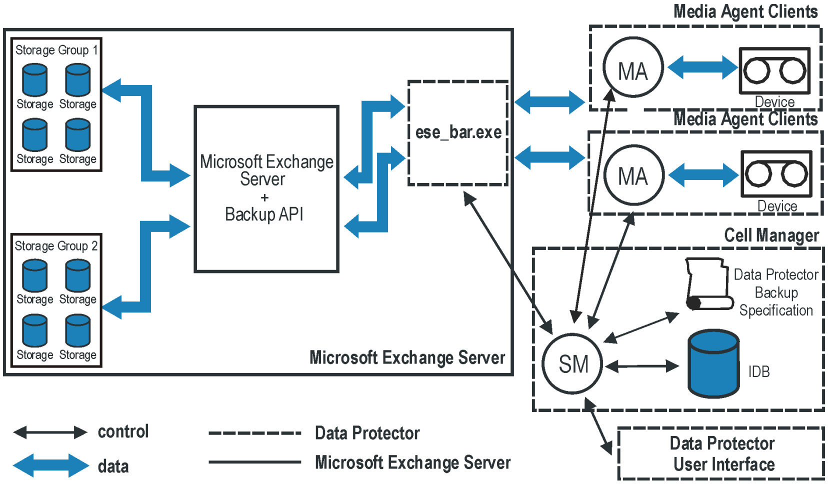


Figure 28 Data Protector Exchange Server integration architecture

Table 16 Legend

SM	Data Protector Session Manager: Backup Session Manager during backup and Restore Session Manager during restore.
Backup API	The Microsoft defined interface that enables data transfer between Data Protector and Exchange Server.
MA	Data Protector General Media Agent.
Storage Group	A collection of mailbox stores and public folder stores that share a set of transaction log files.

Configuring the integration

Prerequisites

- You need a license to use the Exchange Server integration. See the *HP Data Protector installation and licensing guide* for information.
- Ensure that you correctly installed and configured Exchange Server.
  - For supported versions, platforms, devices, and other information, see the latest support matrices at http://www.hp.com/support/manuals.

- For information on installing, configuring, and using Exchange Server, see the Exchange Server documentation.

- Ensure that you correctly installed Data Protector. For information on installing Data Protector in various architectures and installing the Data Protector Exchange Server integration, see the *HP Data Protector installation and licensing guide*.

  Every Exchange Server system to be used with Data Protector must have the `MS Exchange Integration` component installed.

Limitations

- Due to incompatibility between Microsoft Exchange Server 2007 and earlier Exchange Server versions, Exchange Server 2007 backup objects cannot be restored to Data Protector clients on which an earlier Exchange Server version is installed, and vice versa.

Before you begin

- Configure devices and media for use with Data Protector. See the online Help index: “configuring devices” and “creating media pools” for instructions.
- To test whether Exchange Server and Cell Manager communicate properly, configure and run a Data Protector filesystem backup and restore. See the online Help for instructions.
- Before performing incremental backups, disable **circular logging** for all storage groups.

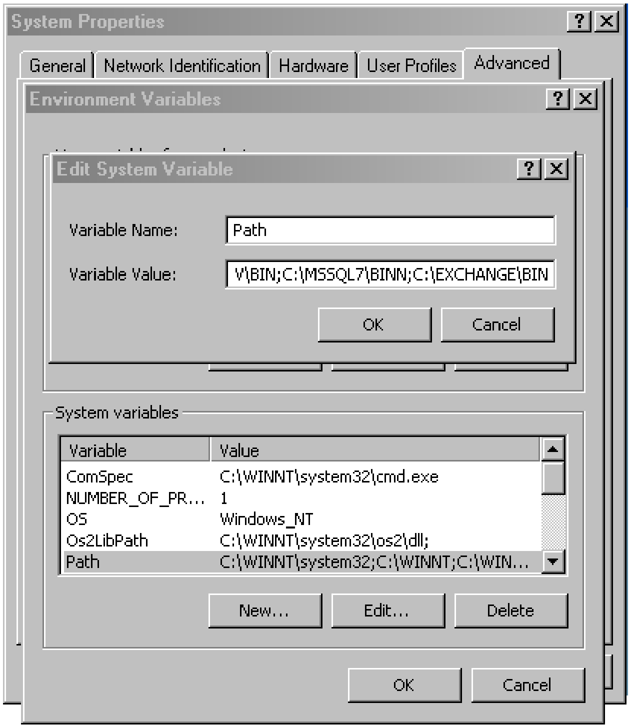
  If the application is cluster-aware, disable circular logging on all cluster nodes.

- Add the *`Exchange_home`*`\bin` directory to the Windows **Path** environment variable:

  1. In the Windows Explorer, right-click **My Computer** and click **Properties**.
  2. In the **Properties** dialog box, click **Advanced** and then **Environment Variables**.
  3. Select **Path** in the **System Variables** list and click **Edit**.
  4. Add *`Exchange_home`*`\bin` in the **Variable Value** text box and click **OK**.

  See Figure 29.

  If the integration is cluster-aware, perform this procedure on all cluster nodes.



Variable Name: Path

Variable Value: V\BIN;C:\MSSQL7\BINN;C:\EXCHANGE\BIN

System variables

Variable	Value
ComSpec	C:\WINNT\system32\cmd.exe
NUMBER_OF_PR...	1
OS	Windows_NT
Os2LibPath	C:\WINNT\system32\os2\dll;
Path	C:\WINNT\system32;C:\WINNT;C:\WIN...

Figure 29 Path system variable

Backup

To run an online backup of an existing Exchange Server backup specification:

- Schedule a backup using the Data Protector Scheduler.
- Start an interactive backup using the Data Protector GUI or CLI.

  For information on starting interactive backups using the CLI, see the `omnib` man page.

Limitations

- Backup preview is not supported.

Considerations

- You can perform incremental backups only if circular logging is disabled for the involved Exchange Server.

Circular logging is a Microsoft Exchange mode, where transaction logs are automatically overwritten when the data they contain is committed to the database.

If enabled, this option reduces disk storage space requirements, but does not allow you to perform incremental backups.

- Do not use double quotes (`"  "`) in object-specific pre and post-exec commands.

Configuring Exchange Server Backup

To configure a backup:

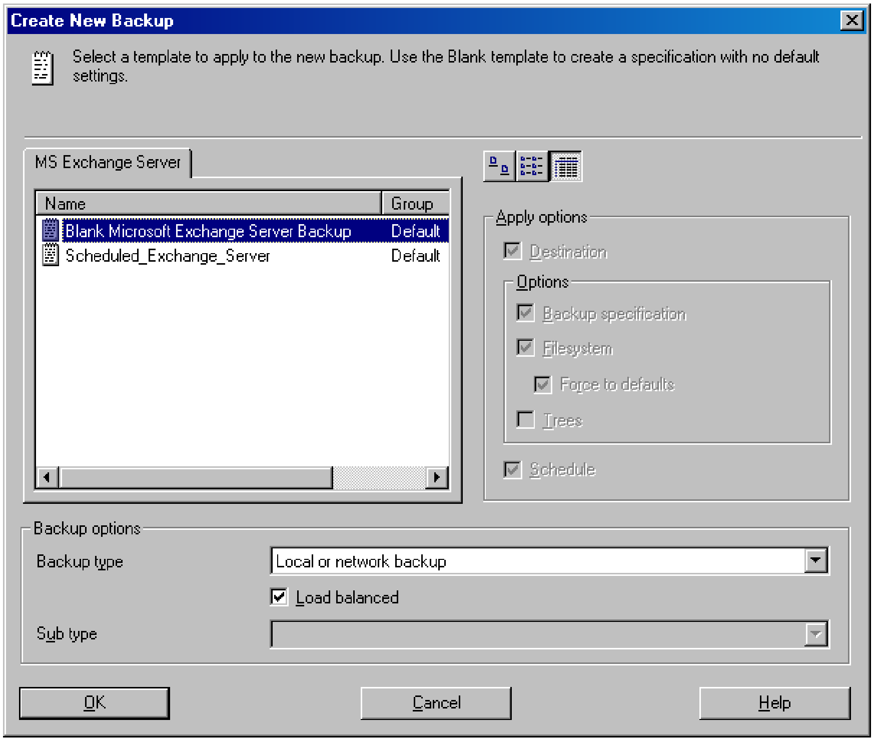
1. Configure devices and media for backup.
2. Create a Data Protector Exchange Server backup specification.

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 **MS Exchange Server**, and click **Add Backup**.

3. In the **Create New Backup** dialog box, select the **Blank Microsoft Exchange Server Backup** template, and click **OK**.



Create New Backup

Select a template to apply to the new backup. Use the Blank template to create a specification with no default settings.

MS Exchange Server

Name	Group
Blank Microsoft Exchange Server Backup	Default
Scheduled_Exchange_Server	Default

Apply options

☑ Destination

Options

☑ Backup specification

☑ Filesystem

☑ Force to defaults

☐ Trees

☑ Schedule

Backup options

Backup type: Local or network backup

☑ Load balanced

Sub type:

Figure 30 Selecting a blank template

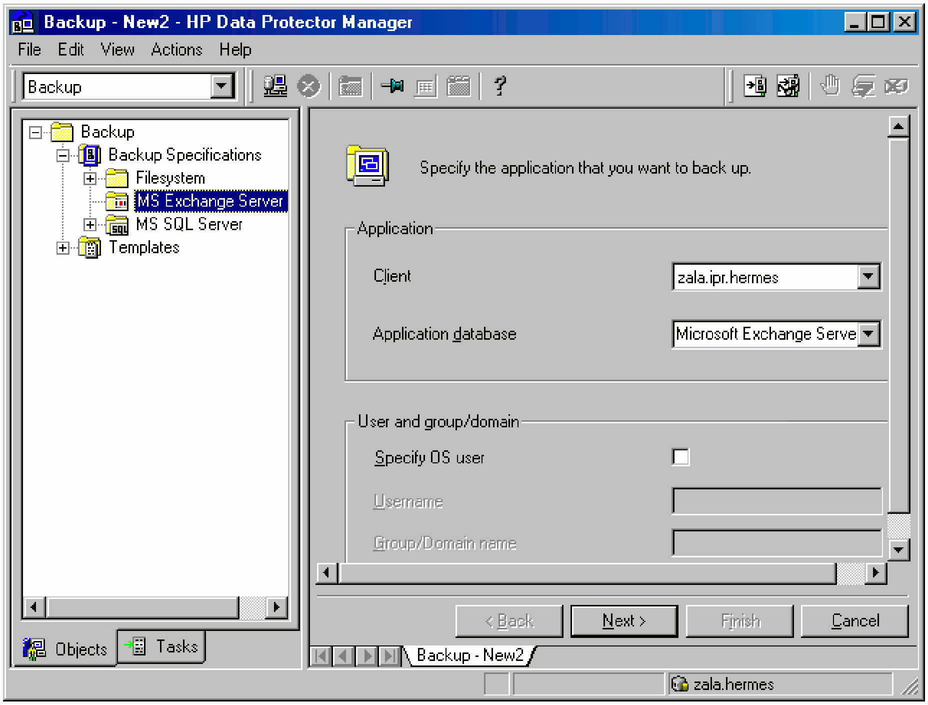
4. In **Client**, select Exchange Server. For cluster environments, select the virtual server of the Exchange Server resource group.

   In **Application database**, select one of the following:

   - **Microsoft Exchange Server (Microsoft Information Store)**
   - **Microsoft Exchange Server (Microsoft Key Management Service)** (if installed)
   - **Microsoft Exchange Server (Microsoft Site Replication Service)** (if installed)

   For information on the **User and group/domain** options, press **F1**.

   Click **Next**.



Specify the application that you want to back up.

Application

Client: zala.ipr.hermes

Application database: Microsoft Exchange Serve

User and group/domain

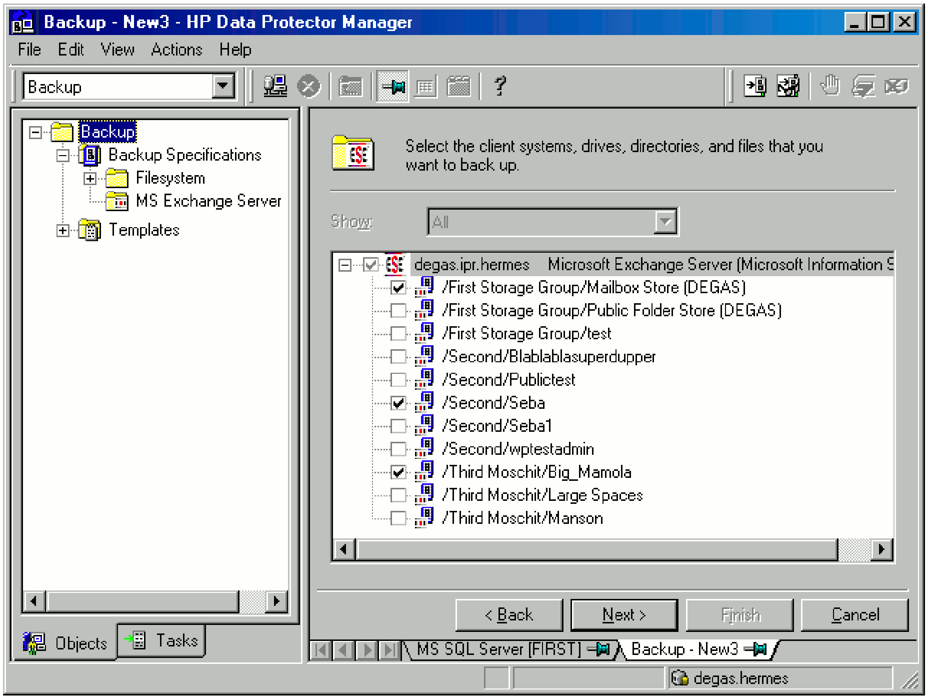
Specify OS user □

Username

Group/Domain name

Figure 31 Client name and application database

5. Select Exchange Server databases you want to back up.



Select the client systems, drives, directories, and files that you want to back up.

- ☑ degas.ipr.hermes Microsoft Exchange Server (Microsoft Information S
  - ☑ /First Storage Group/Mailbox Store (DEGAS)
  - □ /First Storage Group/Public Folder Store (DEGAS)
  - □ /First Storage Group/test
  - □ /Second/Blablablasuperdupper
  - □ /Second/Publictest
  - ☑ /Second/Seba
  - □ /Second/Seba1
  - □ /Second/wptestadmin
  - ☑ /Third Moschit/Big_Mamola
  - □ /Third Moschit/Large Spaces
  - □ /Third Moschit/Manson

Figure 32 Backup objects

Click **Next**.

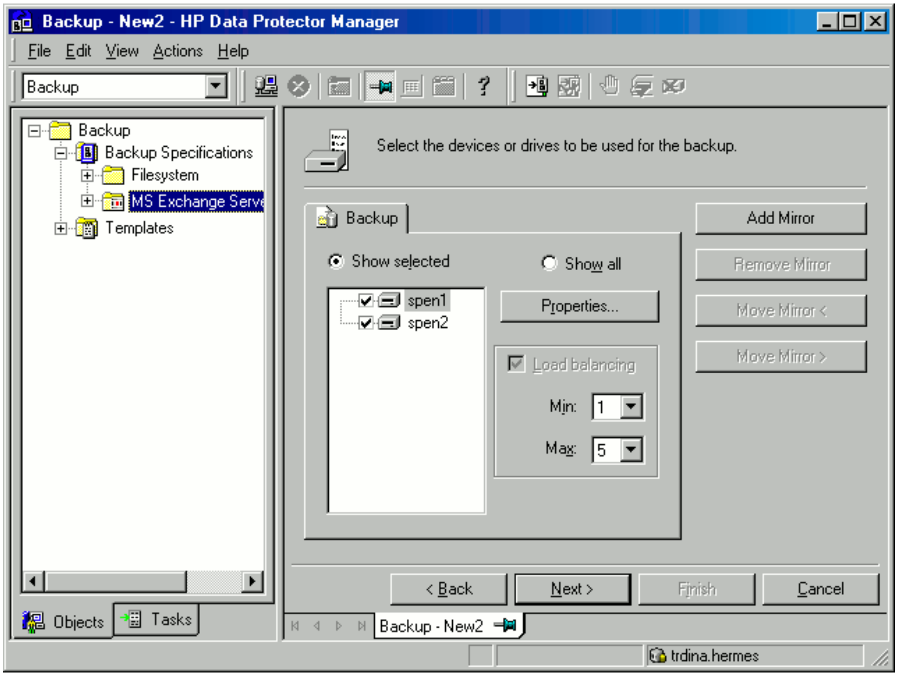
6. Select the device(s). Click **Properties** to set the device concurrency, media pool, and preallocation policy. For more information on options, click **Help**.

   To create additional backup copies (mirrors), click **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 information on object mirroring, see the online Help index: "object mirroring".

NOTE:

The recommended maximum device concurrency is two for devices connected directly to the server, and one for those connected remotely.



Select the devices or drives to be used for the backup.

● Show selected ○ Show all

☑ spen1
☑ spen2

☑ Load balancing

Min: 1

Max: 5

Figure 33 Backup devices

Click **Next** to proceed.

7. Select the backup options.

   For information on **Backup Specification Options** and **Common Application Options**, see the online Help.

   For information on **Application Specific Option**, see SQL Server Specific Backup Options or the online Help.

   Click **Next**.

8. Optionally, schedule the backup. For information on scheduler, press **F1**.

9. Save the backup specification.

   Once saved, the backup specification can be started by clicking **Start Backup**.

Exchange Server specific backup options

You access these options from the **Options** property page by clicking the **Advanced** button next to **Application Specific Options**.

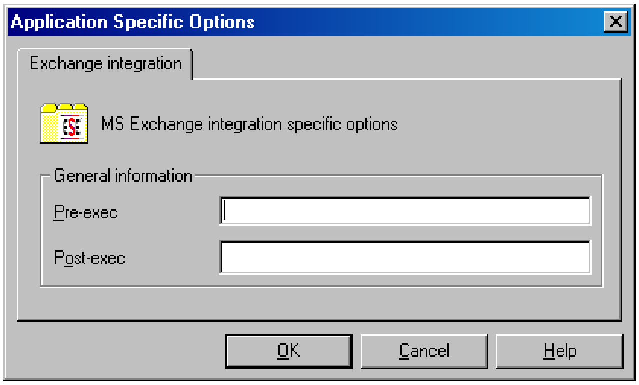

Application Specific Options
Exchange integration
MS Exchange integration specific options
General information
Pre-exec
Post-exec
OK
Cancel
Help

Figure 34 Application specific options

Table 17 Application specific options

Pre-exec	Specifies a command with arguments or a script started on Exchange client before backup. Only the filename must be provided in the backup specification.
Post-exec	Specifies a command with arguments or a script started on Exchange client after backup. Only the filename must be provided in the backup specification.

NOTE:

Pre- and post-exec scripts must reside in the `Data_Protector_home\bin` directory on the Exchange Server.

Scheduling backups

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

Scheduling example

To schedule a database backup 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.

Incremental backup backs up transaction log files that record changes to the database. Exchange Server automatically deletes `transaction log` files after they are backed up.

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 **Filesystem**. Right-click the backup specification you want to start and select **Start Backup**.

3. Select **Backup type** and **Network load**. For information on these options, click **Help**. Click **OK**.

   Click **OK**.

Restore

You can restore Exchange Server databases using the Data Protector GUI or CLI.

Considerations

- If the Recovery Storage Group (RSG) exists on the Exchange Server system when a restore session is started, the restore of databases is redirected to the RSG. To prevent the restore of databases in such circumstances, set the `omnirc` variable `OB2MSESE_CHECK_RSG` to `1`.

IMPORTANT:

The database (store) must be unmounted before a restore.

To unmount a database, use the Exchange Administration GUI:

1. In the **Exchange System Manager** window, right-click the backed up object (**Mailbox Store** or **Public Folder Store)**, and select **Dismount Store** from the pop-up menu.

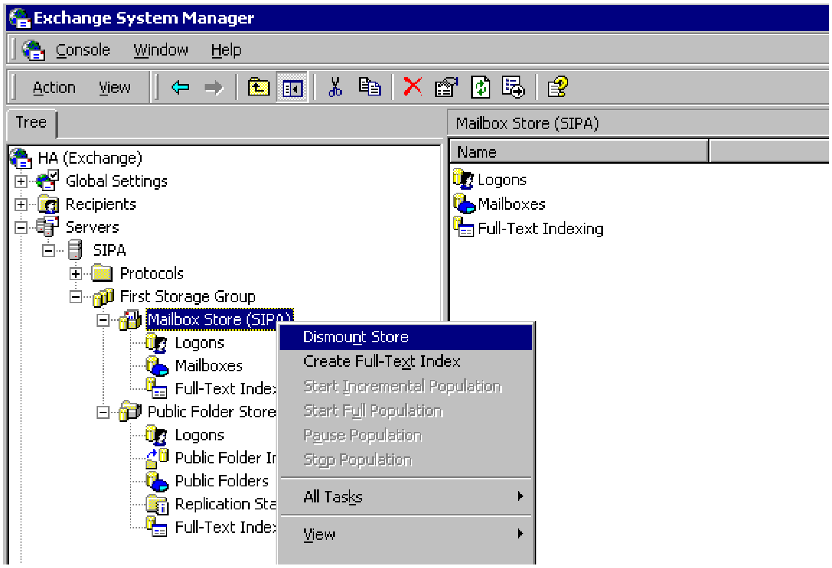


Figure 35 Unmounting a database

2. A warning appears. Click **Yes** to continue unmounting.

When unmounting completes, you may start restore.

After hard recovery, databases can be mounted automatically. See Table 18 for details.

NOTE:

Log files for storage groups are saved in the subdirectory of the specified log directory.

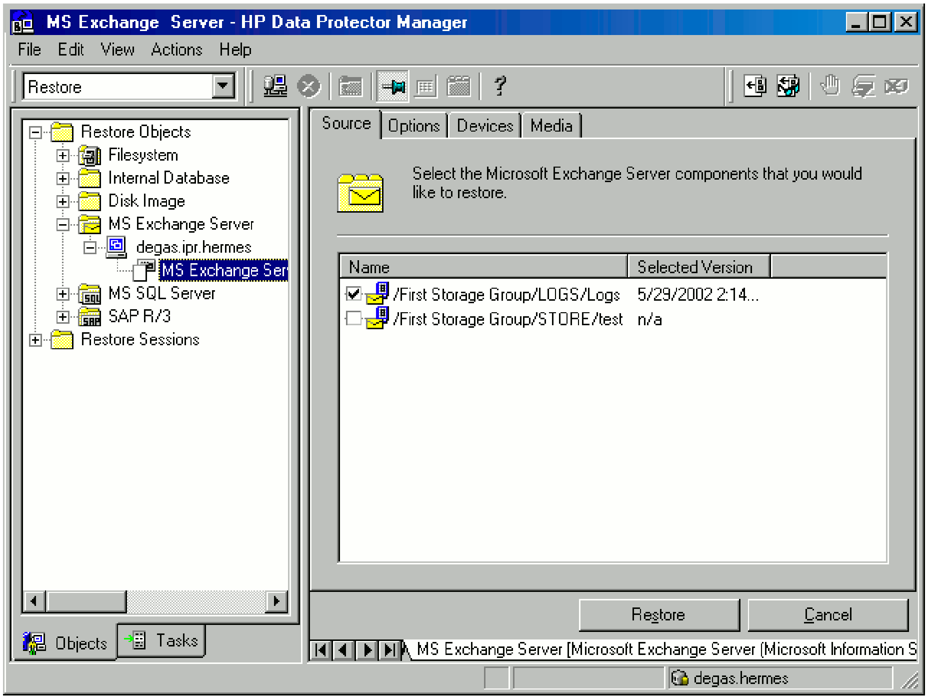
Restoring using the GUI

Proceed as follows using the Data Protector Manager:

1. In the Context List, click **Restore**.

2. In the Scoping Pane, expand **Restore Objects**, **MS Exchange Server**, and then select the client from which you want to restore. A list of backed up objects is displayed in the Results Area.

3. Select the restore objects.



Select the Microsoft Exchange Server components that you would like to restore.

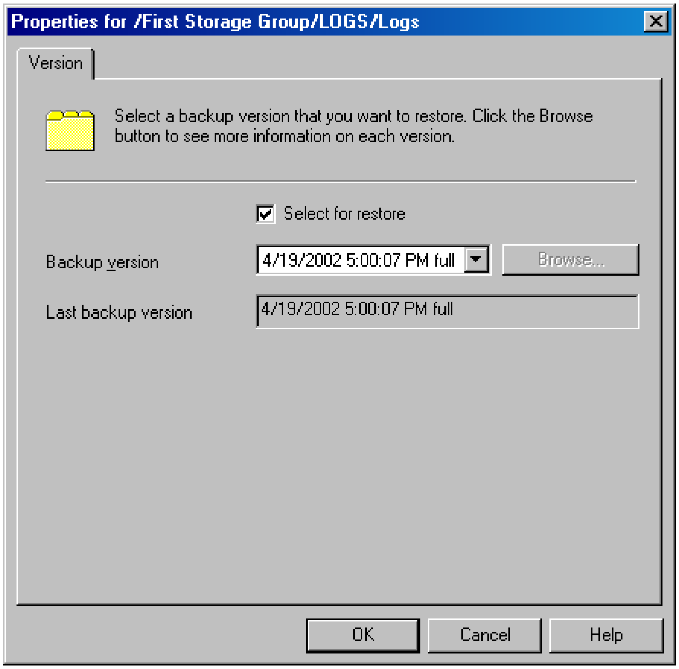
Name	Selected Version
☑ /First Storage Group/LOGS/Logs	5/29/2002 2:14...
□ /First Storage Group/STORE/test	n/a

Figure 36 Restore objects

To select a backup version, right-click the object and select **Properties**.

IMPORTANT:

When restoring several databases from the same storage group, ensure that their backup versions are the same. Otherwise, you need to restore them in separate sessions.



Properties for /First Storage Group/LOGS/Logs

Select a backup version that you want to restore. Click the Browse button to see more information on each version.

☑ Select for restore

Backup version: 4/19/2002 5:00:07 PM full

Last backup version: 4/19/2002 5:00:07 PM full

Figure 37 Selecting a backup version

NOTE:

Restoring databases to a certain state often requires a multiphase restore (multiple versions must be restored to retrieve data). During incremental backups, only transaction logs of storage groups are backed up (without information on physical location of the storage groups); therefore, you must restore last full backup first and then all transaction log backups made after the last full backup.

IMPORTANT:

When restoring from a full database backup, make sure you selected database files and transaction logs from the same version.

Example

Suppose you have the following backup sequence:

`F T T` *F T T* ***T*** `T`

and you want to restore the version marked T, then restore all versions in `italic`: first full and transaction log backup, second transaction log backup, and the last transaction log backup (**Last restore set (start recovery)** selected).

4. In the **Options** property page, select restore options. See Table 18 for details.

5. Click **Devices** and **Media** to select devices, verify device information, and set media priorities.

   Note that you can use a different device for restore than the one used for backup. See the online Help index: “selecting, devices for restore”.

IMPORTANT:

If the devices for restore are not those used for backup, select the same number of devices in the **Devices** property page as you used during backup.

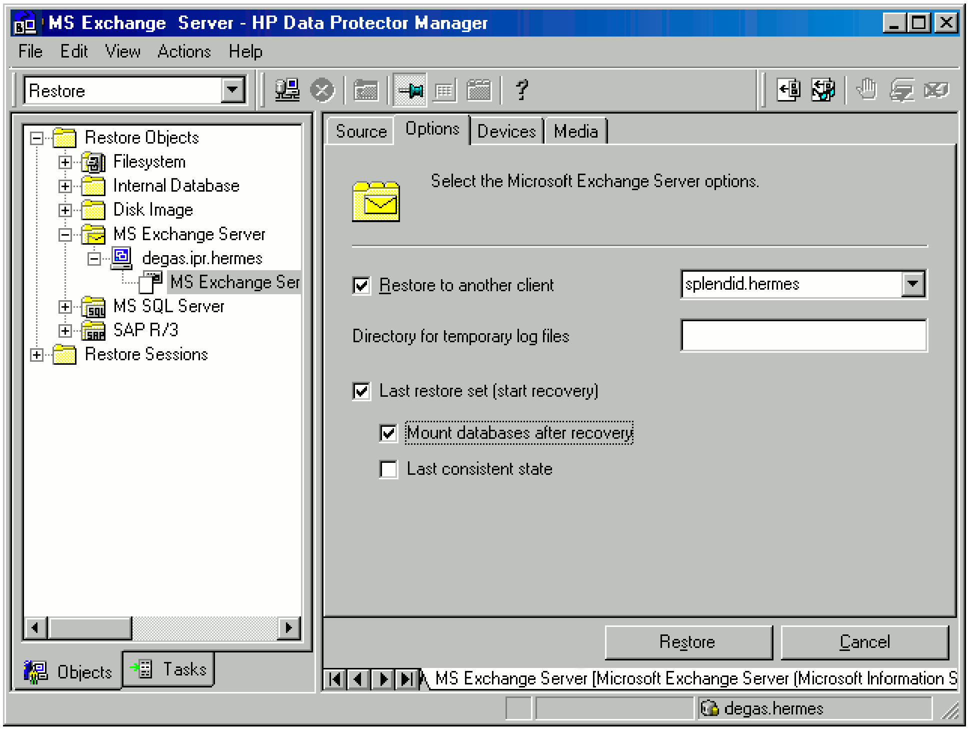
6. Click **Restore**. Review your selection and click **Finish** to start restore.

   If **Mount databases after recovery** is not specified, mount dismounted Information Stores after restore using the Exchange System Manager.

Table 18 Exchange Server restore options

Restore to another client	By default, the target client is the Exchange Server from which the application data was backed up. Nevertheless, you can restore databases to a different Exchange Server. The new target server must be a part of the Data Protector cell and have the `MS Exchange Integration` component installed.
Directory for temporary log files	Sets the temporary directory for log files restore. Using this directory, Exchange Server recovers the database - this is called **hard recovery**.
Last restore set (start recovery)	Performs a hard recovery after restore. Use to restore the last set of files. If you do not set this option, start the recovery manually by running `eseutil /cc /t` from the appropriate subdirectory of the directory for temporary log files.
Mount databases after recovery	Automatically mounts restored databases after hard recovery.

Last consistent state	Restores the database to its last consistent state. The latest log files, created after backup, are applied to the restored database during recovery.



Select the Microsoft Exchange Server options.

☑ Restore to another client: splendid.hermes

Directory for temporary log files:

☑ Last restore set (start recovery)

☑ Mount databases after recovery

☐ Last consistent state

Figure 38 Restore options

Restoring to another client

1. Install the same version of Exchange Server on a separate system, and install the same Exchange Server Service Pack version(s).

NOTE:

New system name can be different.

2. On the new Exchange Server, create *all* storage groups that existed on the backed up Exchange Server. For *every* storage group, use the *same* name, location, and parameters.

3. For *every* newly created storage group, create *all* stores (databases) that existed in this particular storage group on the backed up Exchange Server. When creating a store, use the *same* name, location, and parameters.
4. Install the Data Protector Exchange integration on this system.
5. Restore the last full backup of the Exchange Server database. Follow the normal restore procedure using the Data Protector GUI and set the following options in the **Options** property page:

   - `Restore to another client` and specify the target client name.
   - The directory for temporary log files on the target client, for example `c:\EsseRestore`.
   - `Last restore set (start recovery)` to restore the last set of files (if you have no incremental backups of the last full backup).

   See Table 18 for details.
6. Restore all subsequent incremental backups and specify the same directory for temporary log files on the target client as for the restore of the last full backup.

   When restoring the last incremental backup, select `Last restore set (start recovery)` to initiate automatic hard recovery of the Exchange Server database. If this option is not set, start recovery manually by running `eseutil /cc /t` from the temporary log files directory.

   If hard recovery is initiated after restore of the last set of files (`Last restore set (start recovery)` selected), temporary log files are deleted after recovery.

Restoring using the CLI

From the *`Data_Protector_home`*`\bin` directory, run:

```
omnir -msese

-barhost ClientName [-destination ClientName]

-appname full_application_name {-base DBName -session
SessionID}...

-logpath Path [-last [-mount] [-consistent]]
```

Provide the *`Session_ID`* of the backup session. For object copies, do not use the copy session ID, but the object backup ID (equals the object backup session ID).

For the description of options, see the `omnir` man page.

Example

To restore Information Store with the /First Storage Group/STORE/Public Folder Store store and /First Storage Group/LOGS/Logs logs to computer.company.com (where it was backed up), using the session ID 2003/07/07-13, plus restore log files to c:\temp, perform hard recovery after restore and mount the database after hard recovery, run:

```
omnir -msese -barhost computer.company.com -appname "Microsoft
Exchange Server (Microsoft Information Store)" -base "/First
Storage Group/LOGS/Logs" -session "2003/07/07-13" -base
"/First Storage Group/STORE/Public Folder Store" -session
"2003/07/07-13" -logpath c:\temp -last -mount
```

Troubleshooting

This section lists general checks and verifications, plus problems you might encounter when using the Data Protector Exchange Server integration. Start at Problems. 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*.

Before you begin

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

Checks and verifications

If your configuration, backup, or restore failed:

- Check that Exchange Server services (Microsoft Exchange System Attendant and Microsoft Exchange Information Store) are running.
- Using Exchange System Manager, check that all stores to be backed up are mounted and all stores to be restored are dismounted.

- Perform a backup of the Exchange Information Store using Windows Backup. If the backup fails, fix Exchange Server problems first, and then perform a backup using Data Protector.
- Ensure that the Cell Manager is correctly set on Exchange Server by checking the following registry entry:

  `HKEY_LOCAL_MACHINE\SOFTWARE\Hewlett-Packard\OpenView\OmniBack II\Site`

  Its name and value must be `CellServer` and `"`*`Cell Manager hostname`*`"`, respectively.
- Examine system errors reported in *`Data_Protector_home`*`\log\debug.log` on Exchange Server functioning as a Data Protector client.

  Additionally, examine the errors reported in the Windows Event log.
- Check if the following directories exist on the Data Protector Cell Manager:

  `Data_Protector_home``\config\server\barlists\msese`

  `Data_Protector_home``\config\server\barschedules\msese`
- Make a test filesystem backup and restore of the problematic client. For information, see the online Help.
- Create a backup specification to back up to a null or file device and run the backup. If the backup succeeds, the problem may be related to backup devices. See the *HP Data Protector troubleshooting guide* for instructions on troubleshooting devices.
- Try to restart the Microsoft Exchange Server and start the backup again.
- Check that the *`Exchange_home`*`\bin` directory is added to the Windows `Path` environment variable. For details, see "Configuring the integration" on page 99.
- When performing incremental backups, ensure that circular logging is disabled by starting Exchange System Manager and selecting **Properties** from the storage group you are backing up.
- If you cannot mount the storage after a successful restore, check that LOGS storage on the same storage group is also restored.
- Define a directory for temporary log files in the **Restore** context. Check if the specified directory exists. If it does not, create it or specify another existing directory.
- To restore to another system, make sure Exchange Server is installed on that system and has the same organization and site names as the restored server.

Problems

Problem

Restore session fails

During the restore session, the following error is displayed:

```
[Critical]
Target Instance, specified for restore, is not found or log files
do not match the backup set logs.
```

The problem occurs when there is a gap in the sequence of the restored and the current log files.

Action

At the command prompt, run `eseutil` from the directory with temporary log files of the corresponding storage group:

- If the storage group name consists only of the ASCII characters A-Z, a-z, 0-9, and space, run the following command from *`Storage_group_name`*:

  ```
  eseutil /cc /t
  ```

- If the storage group name consists of Unicode characters, proceed as follows:

  1. One of the subdirectories in the temporary log file directory contains an empty file whose filename equals the name of the storage group you are restoring. Identify the subdirectory where the file is located. The subdirectory name conforms to the following template:

     ```
     Storage Group Number
     ```

  2. Run:

     ```
     Drive_letter:
     ```

     ```
     cd "\Temporary_log_files_directory_path\Storage Group
     Number"
     ```

     ```
     eseutil /cc /t
     ```

Problem

Restore of a database fails

Restore of an Exchange Server 2007 database ends abnormally after reporting the following error:

```
[Critical] From: OB2BAR_main@Hostname "Microsoft Exchange Server
(Microsoft Information Store)"  Time: Date Time
[151:214] Recovery SG 'RSG_name' is configured on the Microsoft
Exchange Server.
```

The problem occurs in two cases:

- If you try to restore the database to its original location when the Recovery Storage Group (RSG) exists on the Exchange Server system.

  The RSG may have been created manually or using the VSS integration agent for restoring a store to the RSG. Under such circumstances, Exchange Server redirects the restore of the database to the RSG instead of restoring the database to the original storage group.
- If you try to restore the database to the RSG when the `omnirc` variable `OB2MSESE_CHECK_RSG` is set to `1`.

Action

To enable the restore of the database to the original storage group, perform one of the following:

- Using Exchange Management Console or Windows PowerShell, remove the RSG from the Exchange Server system.
- Add a registry key which will override redirection of restore to the RSG:
  1. Start Windows Registry Editor.
  2. In Registry Editor, expand the folder:

     `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeIS\ParametersSystem`
  3. Create a new `DWORD` value `Recovery SG Override` and set its value to `1`.

To enable the restore of the database to the RSG, set the `omnirc` variable `OB2MSESE_CHECK_RSG` to `0`.

Problem

Restore of a database to the Recovery Storage Group (RSG) fails

Restore of an Exchange Server 2007 database to the RSG ends abnormally after reporting the following error:

```
ESE subsystem or operating system reported error for Mailbox:
0xc7fe1f42: Database not found.
```

The problem occurs when the database being restored is not properly linked to the RSG.

Action

To enable the restore of the database to the RSG, using Exchange Management Console or Windows PowerShell appropriately link the database to the RSG.

Problem

Restore of a database to the Recovery Storage Group (RSG) fails

Restore of an Exchange Server 2007 database to the RSG ends abnormally after reporting the following error:

```
ESE subsystem or operating system reported error for ():
0x3f3: The configuration registry key could not be opened.
```

The problem occurs when the database, which has been successfully restored to the RSG, cannot be mounted.

Action

To enable the database that has been restored to the RSG to be mounted, perform one of the following:

- In the Exchange Management Console, go to the **Database Recovery Management** tool and perform the task **Set up the 'Database can be overwritten by restore' flag**.
- In the Windows PowerShell, run:

  ```
  Set-MailboxDatabase 'ExchangeServerName\RSGName\StoreName'
  -AllowFileRestore $true
  ```

4 Integrating Microsoft Exchange Single Mailbox and Data Protector

Introduction

This chapter explains how to configure and use the Data Protector Microsoft Exchange Single Mailbox integration (**Exchange Single Mailbox integration**). It describes concepts and methods you need to understand to back up and restore mailboxes and Public Folders from or to a Microsoft Exchange Server system.

You can back up the entire content of a mailbox or Public Folders, including e-mail messages, task assignments, calendar schedules, contacts, and so on (**Exchange items**). Or you can back up only individual Exchange items from different mailboxes and Public Folders.

Data Protector integrates with Microsoft Exchange Server (**Exchange Server**) to back up and restore Exchange items online, enabling the Exchange Server to be actively used during the session.

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

Table 19 Exchange Single Mailbox backup types

Full	Backs up all selected Exchange items.
Incr1	Backs up changes made to selected Exchange items since the last full backup.
Incr	Backs up changes made to selected Exchange items since the last backup of any type.

You can restore Exchange items:

- To the original location.

- To a new folder, created in the root of the mailbox or All Public Folders.
- To another mailbox.
- To another Exchange Server system.

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

Integration concepts

The main component of the Data Protector Exchange Single Mailbox integration is `mbx_bar.exe`, installed on the Exchange Server system, which channels communication between the Data Protector Session Manager, and, via the **MAPI interface**, the Exchange Server. Figure 39 on page 124 shows the architecture of the Data Protector Exchange Single Mailbox integration.

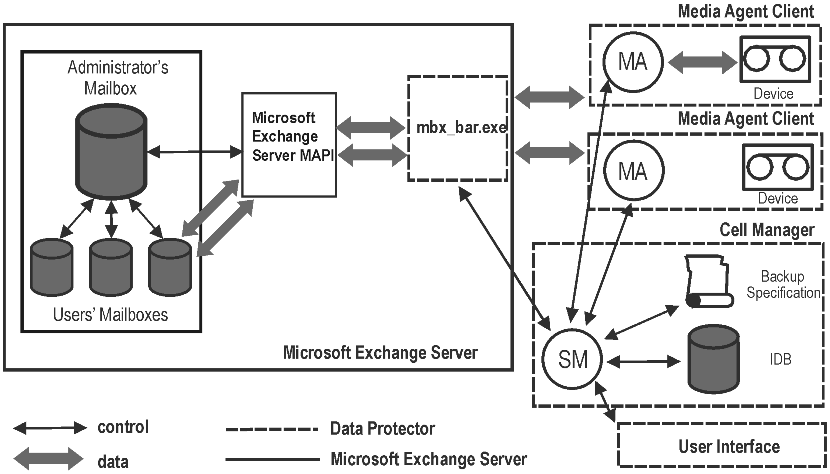


Figure 39 Exchange Single Mailbox integration architecture

Legend:

MAPI	The Messaging Application Programming Interface, enabling applications and messaging clients to interact with messaging and information systems.
SM	The Data Protector Session Manager, which controls the session.

mbx_bar.exe	The Data Protector component started by SM that logs in through the MAPI profile to the Exchange Server administrator's mailbox, establishing an MAPI session. Having access to all other mailboxes, `mbx_bar.exe` logs in to each mailbox selected for backup or restore and initiates data transfer between Exchange Server and Data Protector media.
MA	The Data Protector General Media Agent.
IDB	The Data Protector internal database.

While the Exchange Server is responsible for read/write operations to disk, Data Protector reads from and writes to devices, and manages media.

Configuring the integration

Configure every Exchange Server you intend to back up from or restore to and the corresponding Exchange Server users.

Prerequisites

- Ensure that you have correctly installed and configured Exchange Server.
  - For supported versions, platforms, devices, and other information, see the latest support matrices at http://www.hp.com/support/manuals.
  - For information on installing, configuring, and using Exchange Server, see the Exchange Server documentation.
- On Microsoft Exchange Server 2007 systems, ensure that the package Microsoft Exchange Server MAPI Client and Collaboration Data Objects is installed.

  The package can be obtained free of charge from the Microsoft web site http://www.microsoft.com/downloads/Search.aspx?displaylang=en.
- 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*.

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

Limitations

- The Data Protector Exchange Single Mailbox integration is supported only on Exchange Server systems. You cannot back up and restore Exchange items from or to other clients.

Before you begin

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

Cluster-aware clients

Configure the integration on all cluster nodes.

Configuring Exchange Server users

Add the Exchange Server administrator to the Data Protector `admin` or `operator` user group. For information, see the online Help index: “adding users” and “user groups”.

See the Exchange Server documentation for further information on different types of connections, roles and permissions of Exchange Server administrators, and security issues.

Configuring Exchange servers

Provide Data Protector with the name, password, and domain of the Exchange Server administrator. Data Protector then creates the Exchange Server configuration file on the Cell Manager and verifies the connection to the Exchange Server.

IMPORTANT:

Reconfigure the Exchange Server every time the Exchange Server administrator’s password changes.

Prerequisites

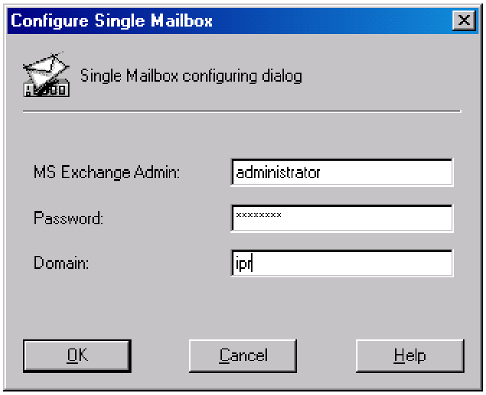
- Ensure that the Exchange Server is online.

Configure the Exchange Server using the Data Protector Manager.

1. In the Context List, click **Backup**.
2. In the Scoping Pane, expand **Backup Specifications**, right-click **MS Exchange Single Mailboxes**, and click **Add Backup**.
3. In the **Create New Backup** dialog box, click **OK**.
4. In **Client**, select the Exchange Server system. In a cluster environment, select the virtual server of the Exchange Server resource group.

   For information on the **User and group/domain** options, press **F1**.

   Click **Next**.
5. In the **Configure Single Mailbox** dialog box, provide the username, password, and domain of the Exchange Server administrator.

   Configure Single Mailbox

   Single Mailbox configuring dialog

   MS Exchange Admin: administrator

   Password: ********

   Domain: ipr

   Figure 40 Configuring the Exchange Server

   Click **OK**.
6. The Exchange Server is configured. Exit the GUI or proceed with creating the backup specification at Step 6 on page 130.

Checking the configuration

You can check the configuration of the Exchange Server after you have created at least one backup specification for the Exchange Server.

Check the Exchange Server configuration using the Data Protector Manager.

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

Backup

The integration provides online backups of the following types:

Table 20 Exchange Single Mailbox backup types

Full	Backs up all selected Exchange items.
Incr1	Backs up changes made to selected Exchange items since the last full backup.
Incr	Backs up changes made to selected Exchange items since the last backup of any type.

Limitations

- Backup sessions that back up the same mailbox cannot run simultaneously.
- The Data Protector Exchange Single Mailbox backup is slower and requires more media space than the Data Protector Exchange Server backup. In the latter case, a message that has been sent to several recipients is saved only once and linked to all recipients, whereas in the first case, the entire message is saved for each recipient separately.

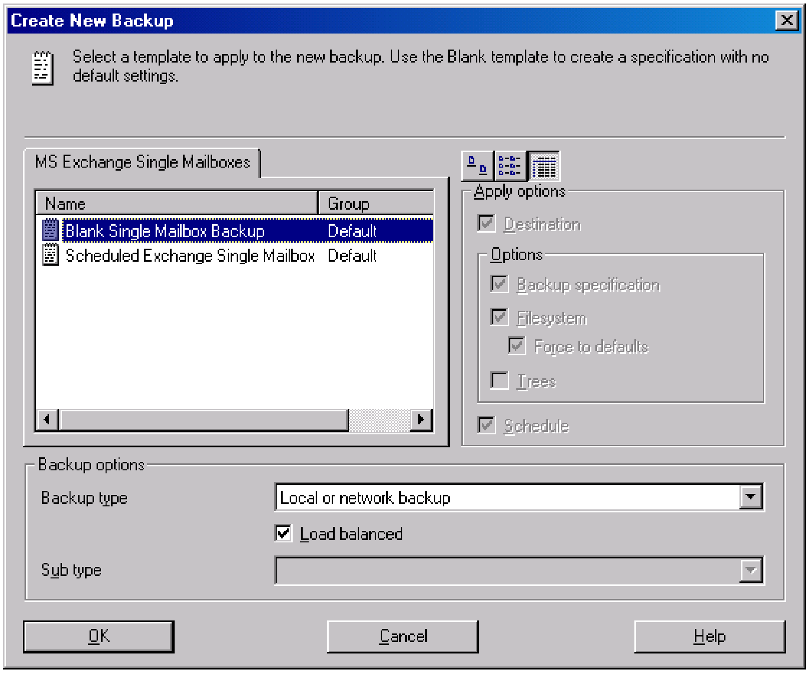
IMPORTANT:

Do not use Data Protector Exchange Single Mailbox backups as a replacement for Data Protector Exchange Server backups. The latter are still needed to successfully recover a system that has been struck by a disaster. For information, see “Backup” on page 101.

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 **MS Exchange Single Mailboxes**, and click **Add Backup**.
3. In the **Create New Backup** dialog box, select the template you want to use.



Create New Backup

Select a template to apply to the new backup. Use the Blank template to create a specification with no default settings.

MS Exchange Single Mailboxes

Name	Group
Blank Single Mailbox Backup	Default
Scheduled Exchange Single Mailbox	Default

Apply options

☑ Destination

Options

☑ Backup specification

☑ Filesystem

☑ Force to defaults

□ Trees

☑ Schedule

Backup options

Backup type: Local or network backup

☑ Load balanced

Sub type:

Figure 41 Selecting a template

4. In **Client**, select the Exchange Server system. In a cluster environment, select the virtual server.

   For information on the **User and group/domain** options, press **F1**.

   Click **Next**.

5. If the Exchange Server is not configured for use with Data Protector, the Configure Single Mailbox dialog box is displayed. Configure it as described in “Configuring Exchange servers” on page 126.

6. Select the Exchange items you want to back up.

Mailboxes are organized alphabetically. For example, mailboxes starting with the letter `S` are collected under the `S` folder.

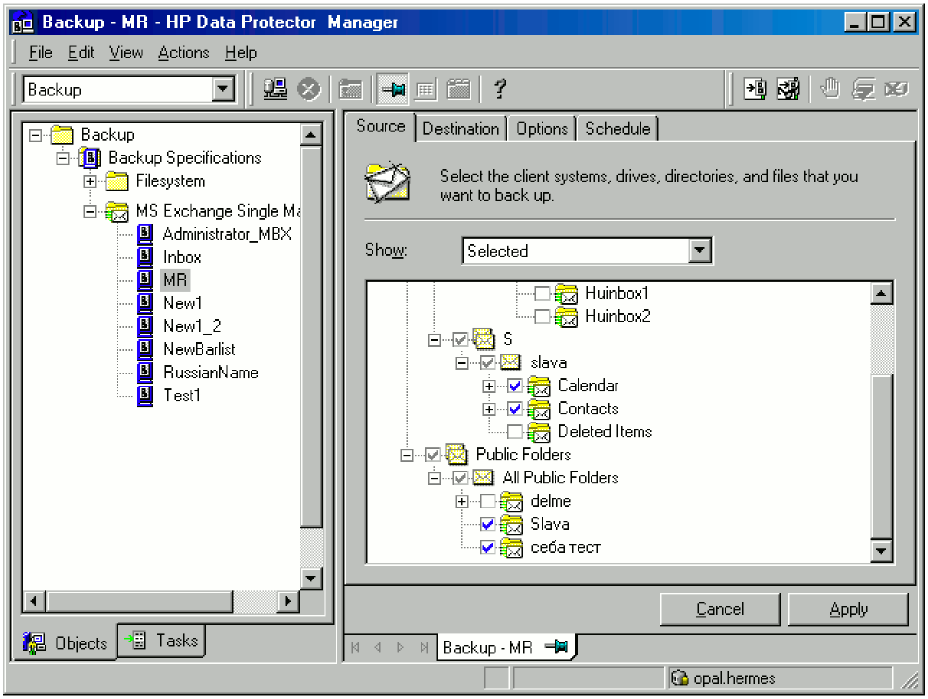
NOTE:

If some mailboxes have the same display name, Data Protector appends a user unique string at the end of each mailbox name.

To back up all mailboxes and Public Folders, select the Exchange Server system at the top. Or you can browse for and select individual mailboxes and Public Folders or individual Exchange items from different mailboxes and Public Folders.

NOTE:

Empty folders will not be backed up.



Select the client systems, drives, directories, and files that you want to back up.

Show: Selected

Figure 42 Selecting Exchange items for backup

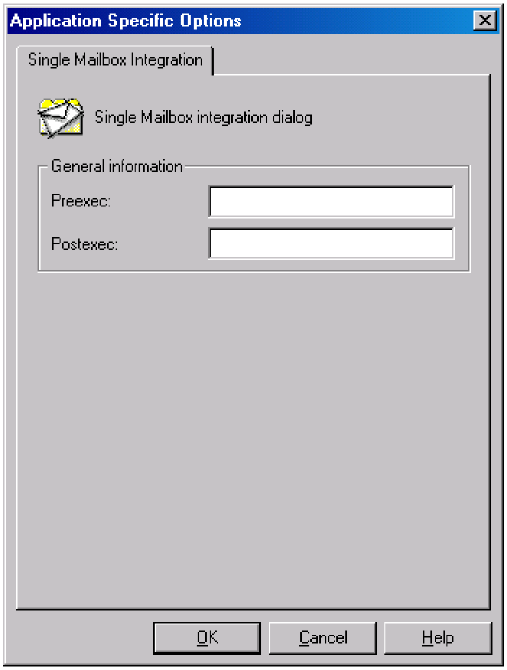
Click **Next**.

7. Select devices to use for the backup.

   To specify device options (for example, the device concurrency and the media pool to be used), right-click the device and click **Properties**.

   Click **Next**.

8. Set backup options. For information on application specific backup options (Figure 43 on page 131), see Figure 42 on page 130.



Application Specific Options

Single Mailbox Integration

Single Mailbox integration dialog

General information

Preexec:

Postexec:

Figure 43 Exchange Single Mailbox specific backup options

   Click **Next**.

9. Optionally, schedule the backup. See “Scheduling backup specifications” on page 81.

   Click **Next**.

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

TIP:

Preview backup session for your backup specification before using it. See "Previewing backup sessions" on page 82.

Table 21 Exchange Single Mailbox specific backup options

Option	Description
Pre-exec, **Post-exec**	Specify a command to be run by `mbx_bar.exe` on the Exchange Server system before the backup (`pre-exec`) or after it (`post-exec`). Do not use double quotes. Type only the name of the command and ensure that the command resides in the *`Data_Protector_home`*`\bin` directory on the Exchange Server system.

Modifying backup specifications

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

Scheduling backup specifications

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

Scheduling example

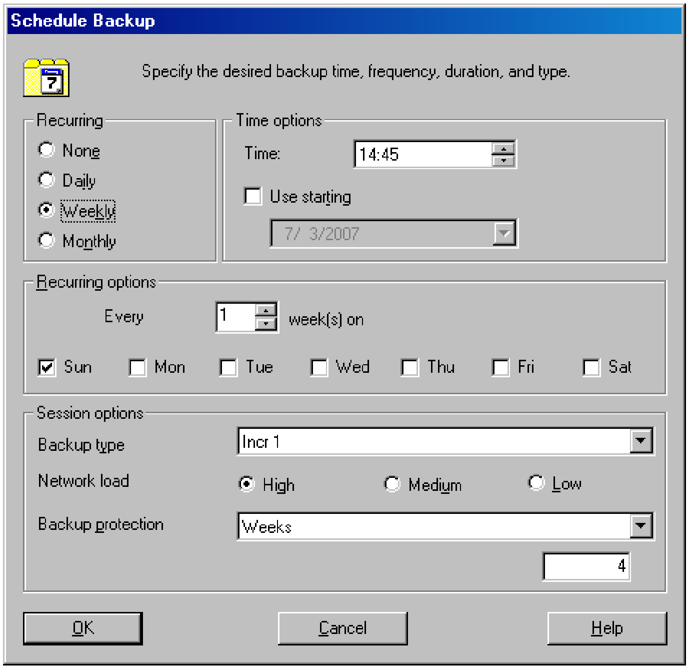
To perform Incr1 backups of selected Exchange items at 14:45, 18:00, and 20:00 on Sundays:

1. In the **Schedule** 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 **14:45**. Under **Recurring Options**, select **Sun**. Under **Session Options**, select the **Incr1** backup type. See Figure 44 on page 133.

   Click **OK**.

3. Repeat Step 1 on page 132 and Step 2 on page 132 to schedule backups at 18:00 and 20:00.

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



Schedule Backup

Specify the desired backup time, frequency, duration, and type.

Recurring

○ None
○ Daily
● Weekly
○ Monthly

Time options

Time: 14:45

□ Use starting

7/ 3/2007

Recurring options

Every 1 week(s) on

☑ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat

Session options

Backup type: Incr 1

Network load: ● High ○ Medium ○ Low

Backup protection: Weeks 4

Figure 44 Scheduling a backup specification

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 Single Mailbox**. 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

Run:

```
omnib -mbx_list backup_specification_name -test_bar
```

What happens during the preview?

The following are tested:

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

After that, the Exchange Server part of the preview starts, which checks if the selected Exchange items are in an appropriate state for backup.

Starting backup sessions

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

Use the Data Protector GUI 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 Single Mailboxes**. Right-click the backup specification you want to start 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

On the Exchange Server system, run:

```
omnib -mbx_list backup_specification_name [-barmode
mailbox_mode][list_options]
```

where *mailbox_mode* is one of the following:

```
{-full|-incr|-incr1}
```

For *list_options*, see the `omnib` man page.

Example

To start an incremental backup using the backup specification `FIRST` and to set data protection to 5 days, run:

```
omnib -mbx_list FIRST -barmode —incr -protect 5
```

Restore

Restore Exchange items using the Data Protector GUI or CLI.

Before you begin

- If you intend to restore Exchange items to another mailbox, ensure that the destination mailbox exists on the destination Exchange Server.
- If you intend to restore Exchange items to another Exchange Server system, ensure that the destination Exchange Server system has the `MS Exchange 2000/2003 Integration` component installed and that the Exchange Server is configured for use with Data Protector.
- If you intend to restore Exchange items from Data Protector A.05.50 backups, ensure that the `MBX_RESTORE_55 omnirc` variable is set to 1.

Restoring using the Data Protector GUI

1. In the Context List, click **Restore**.
2. In the Scoping Pane, expand **MS Exchange Single Mailboxes**, the client from which the data to be restored was backed up, and then click **MS Exchange Single Mailboxes**.

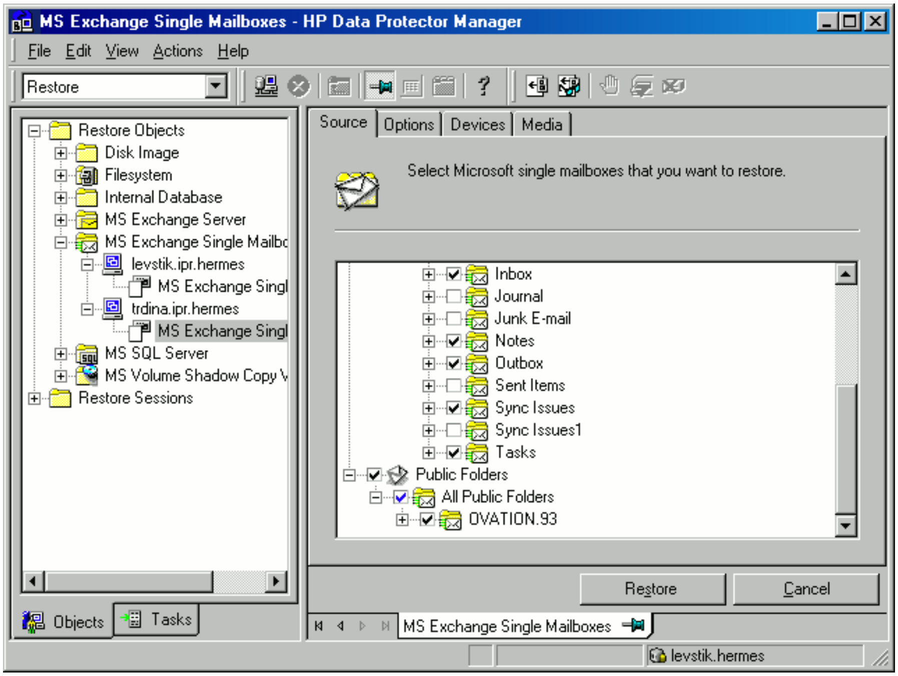
3. In the **Source** page, browse for and select Exchange items to restore.

   To restore all mailboxes and Public Folders, select **Mailboxes** and **Public Folders**. Or you can browse for and select individual mailboxes and Public Folders or individual Exchange items from different mailboxes and Public Folders.

   To restore the data from the root mailbox folder, select **Top of Information Store** under the appropriate user mailbox.

   Mailboxes are organized alphabetically. For example, mailboxes starting with the letter `S` are collected under the `S` folder.

   See Figure 45 on page 136.



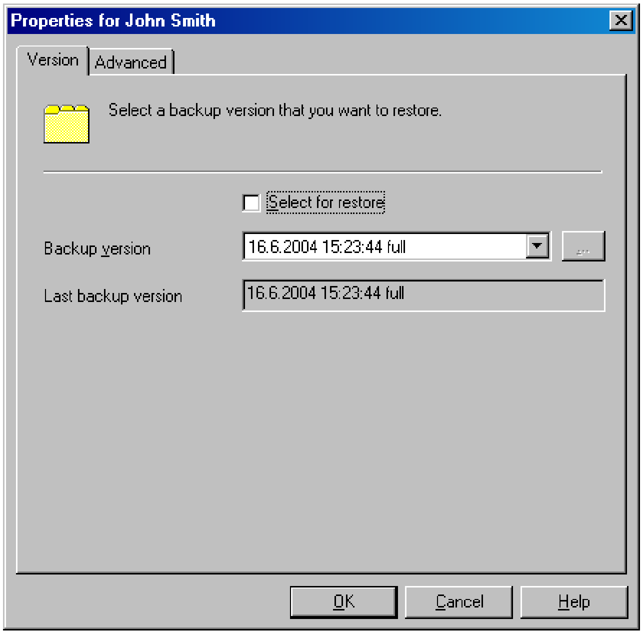
Select Microsoft single mailboxes that you want to restore.

- ☑ Inbox
- □ Journal
- □ Junk E-mail
- ☑ Notes
- ☑ Outbox
- □ Sent Items
- ☑ Sync Issues
- □ Sync Issues1
- ☑ Tasks
- ☑ Public Folders
  - ☑ All Public Folders
    - ☑ OVATION.93

Figure 45 Selecting Exchange items for restore

You can specify the backup version, the chain of backups to be used, and the restore destination for each mailbox or Public Folders separately.

By default, the last backup session is used for restore. To restore from another session, right-click the relevant mailbox or **Public Folders**, and click **Properties**. See Figure 46 on page 137.



Properties for John Smith

Select a backup version that you want to restore.

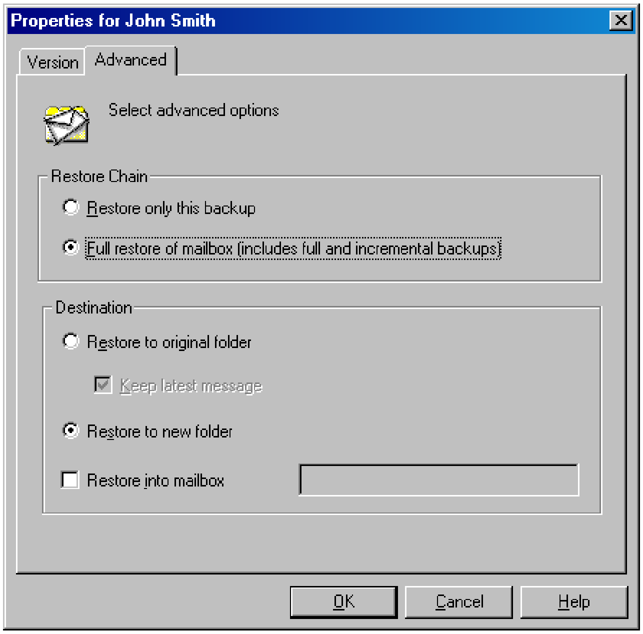
□ Select for restore

Backup version: 16.6.2004 15:23:44 full

Last backup version: 16.6.2004 15:23:44 full

Figure 46 Version properties

To specify the restore destination and the chain of backup sessions to be used, click the **Advanced** tab. See Figure 47 on page 138.



Properties for John Smith

Select advanced options

Restore Chain

○ Restore only this backup

● Full restore of mailbox (includes full and incremental backups)

Destination

○ Restore to original folder

☑ Keep latest message

● Restore to new folder

□ Restore into mailbox

Figure 47 Advanced properties

For details on these options, see Table 22 on page 140.

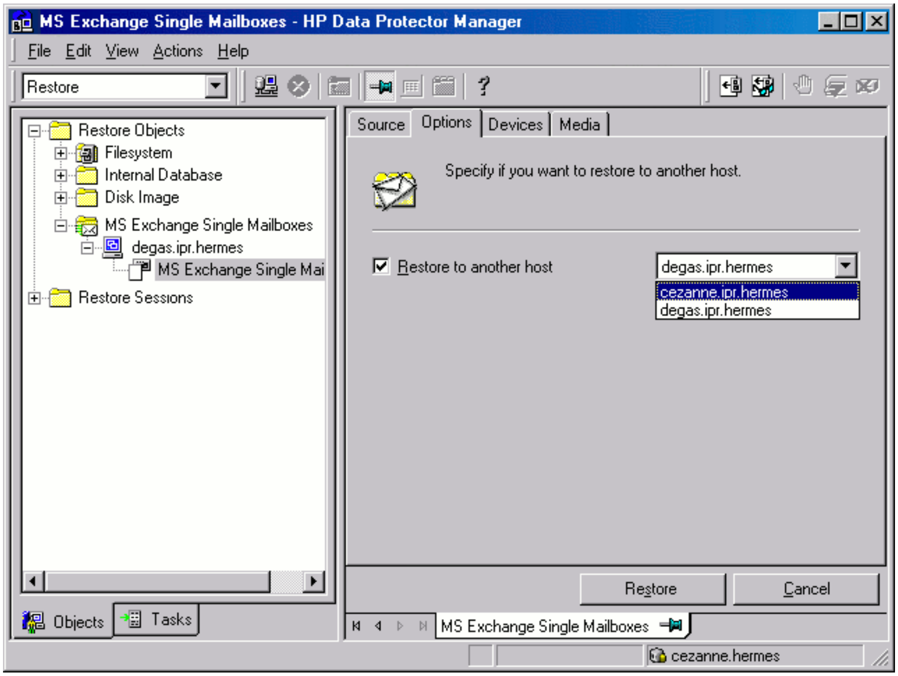
NOTE:

Which Exchange items are displayed in the Results Area depends on the selected backup session and the **Restore Chain** options.

For example, if **Restore only this backup** is selected, only the Exchange items backed up in the selected session are displayed, whereas if **Full restore of mailbox** is selected, all Exchange items backed up in the restore chain of backup sessions are displayed.

The **Full restore of mailbox** and **Restore to new folder** options are selected by default.

4. In the **Options** page, specify the destination Exchange Server system. By default, the original Exchange Server system is selected.



Specify if you want to restore to another host.

☑ Restore to another host: degas.ipr.hermes

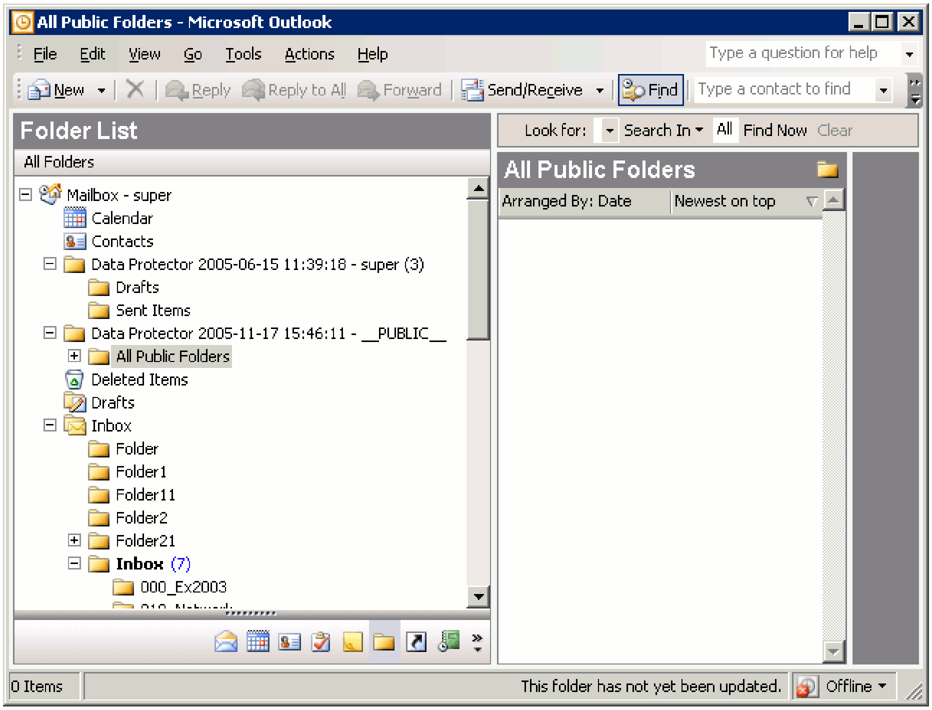
cezanne.ipr.hermes
degas.ipr.hermes

Figure 48 Selecting the destination Exchange Server system

5. In the **Devices** page, select devices to use for the restore.
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.

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



This folder has not yet been updated.

Figure 49 Restored mailbox and public folders content with the restore to new folder option selected.

To transfer restored data to `.pst` files:

1. On the client system, create a `.pst` file.
2. Connect to the Exchange Server system.
3. Move the restored data from the `Data Protector` *`backup date backup time`* folder or the `Data Protector` *`backup date backup time`* – `public folder` folder to the previously created `.pst` file.

Table 22 Exchange Single Mailbox restore options

Option	Description
Restore only this backup	Select this option to restore data only from the selected backup session.

Option	Description
Full restore of mailbox	Selected by default. Data is restored, not only from the selected backup session, but also from the latest full, the latest incremental1 (if it exists), and any incremental backups from the last incremental1 up to the selected backup version. Note that any Exchange item that was backed up in any of these sessions is displayed and can be selected for restore.
Restore to original folder	Data Protector restores Exchange items to the same location from which they were backed up. If `Keep latest message` is selected, existing messages in the destination mailbox or Public Folders are not restored even if they differ from their backed up versions. If `Keep latest message` is not selected, all messages are restored, replacing their current versions (if they exist). If different versions of the same message exist in the mailbox or Public Folders (for example, if you have a copy of the message), only one is replaced with the backed up version and all other versions remain intact. The messages in the mailbox that were not backed up in the specified backup session (or the restore chain of backup sessions) always remain intact. By default, this option is not selected.
Restore to new folder	Selected by default. Data Protector creates a new folder in the root of the mailbox (or in the root of `All Public Folders`) and restores Exchange items into it. See Figure 49 on page 140. When restoring a mailbox, the folder is named `Data Protector` *`backup_date backup_time`*. When restoring Public Folders it is named `Data Protector` *`backup_date backup_time`* `- public folder`. If you restore from the same backup several times, a number is appended to the folder name. For example, in the second restore session of a mailbox, the folder `Data Protector` *`backup_date backup_time`* `(1)` is created.
Restore into mailbox	By default, Exchange items from a mailbox are restored to the original mailbox. Select this option to specify a different destination mailbox. Note that you can restore Exchange items from different mailboxes to the same mailbox. For privacy protection, you cannot restore Exchange items from mailboxes to Public Folders.

Option	Description
Restore to another host	By default, Exchange items are restored to the original Exchange Server system. Select this option, to specify a different destination Exchange Server system.

Restoring using the Data Protector CLI

On the Exchange Server system, run:

```
omnir -mbx
-barhost ClientName
[-destination DestClientName]
-mailbox MailboxName -session SessionID [MAILBOX_OPTIONS]
-public -session SessionID [PUBLIC_FOLDERS_OPTIONS]
[GENERAL_OPTIONS]

MAILBOX_OPTIONS
-destmailbox DestMailboxName
-folder Folder
-exclude ExFolder
-originalfolder {-keep_msg | -overwrite_msg}
-chain

PUBLIC_FOLDERS_OPTIONS
-folder Folder
-exclude ExFolder
-originalfolder {-keep_msg | -overwrite_msg}
-chain
```

NOTE:

To restore multiple mailboxes, repeat the options `—mailbox` *`MailboxName`* `-session` *`SessionID`* `[`*`MAILBOX_OPTIONS`*`]`.

To restore or exclude from restore multiple folders, repeat the options `–folder` *`Folder`* and `-exclude` *`ExFolder`*.

Parameter description

`ClientName` Original Exchange Server system, from which Exchange items to be restored were backed up.

DestClientName

Destination Exchange Server system, to which the Exchange items will be restored (needed only if you are not restoring to the original Exchange Server system).

SessionID

Backup version ID. For object copies, use the object’s backup ID (which equals the object’s backup session ID). Do not use the object’s copy session ID.

MailboxName

Original mailbox, from which Exchange items to be restored were backed up. If the name contains a space, put the name in quotes. For example, `"John Smith"`.

DestMailboxName

Destination mailbox, to which the Exchange items from the mailbox will be restored (needed only if you are not restoring to the original mailbox).

Folder

Folder to be restored. Specify its pathname, starting from the root directory in the mailbox or Public Folders.

If the pathname contains a space, put the pathname in quotes. For example, `"Inbox\My folder"`.

ExFolder

Subfolder to be excluded from restore of the mailbox or Public Folders.

Option description

`-originalfolder`

This option is equivalent to the Data Protector GUI option `Restore to original folder`. If not specified, the same results occur as if the Data Protector GUI option `Restore to new folder` was selected.

`-chain`

This option is equivalent to the Data Protector GUI option `Full restore of mailbox`. If not specified, the same results occur as if the Data

Protector GUI option Restore only this backup was selected.

Limitations

- If any of the mailbox names or folder names specified in the omnir command contains a slash (/), backslash (\), or double quote (") character, the restore fails.

Restore examples

Example 1

To restore the mailbox FIRST, backed up in the session 2005/01/10-1 from the Exchange Server system infinity.ipr.hermes, to a new folder in the mailbox TEMP on the same Exchange Server system, run:

```
omnir -mbx -barhost infinity.ipr.hermes -mailbox FIRST
-session 2005/01/10-1 -destmailbox TEMP
```

Example 2

To restore the folder Inbox from the mailbox User 1, backed up in the session 2005/03/10-18 from the Exchange Server system exchange.hp.com, to the original folder without overwriting the messages in the original folder, run:

```
omnir -mbx -barhost exchange.hp.com -mailbox "User 1" -session
2005/03/10-18 -folder Inbox -originalfolder -keep_msg
```

Example 3

To restore the mailbox User 2, backed up in the session 2005/03/10-19 from the Exchange Server system exchange.hp.com, to a new folder in the original mailbox, without restoring the messages from the folder Deleted Items, run:

```
omnir -mbx -barhost exchange.hp.com -mailbox "User 2" -session
2005/03/10-19 -exclude "Deleted Items"
```

Example 4

To restore two public folders, Administration and Addresses, which are subfolders of All Public Folders, and the mailbox My Mailbox, backed up in the session 2005/06/10-19 from the Exchange Server system exchange.hp.com, to a new folder in Public Folders and to the original folders in the mailbox respectively, run:

```
omnir -mbx -barhost exchange.hp.com -public -session
2005/06/10-19 -folder "All Public Folders\Administration"
-folder "All Public Folders\Addresses" -mailbox "My Mailbox"
-originalfolder -keep_msg
```

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 online Help index: “viewing currently running sessions”.

Performance tuning

Performance tuning means customizing Exchange Server and Data Protector to achieve better backup and restore results.

Data Protector creates a separate backup object out of selected Exchange items from a single mailbox or Public Folders. This object is then backed up as a separate data stream. `mbx_bar.exe` spends a significant amount of time creating Data Protector backup objects and logging mailboxes on/off. Meanwhile, the Data Protector devices are in an idle state, waiting for the actual data transfer to start.

Backup performance can be enhanced by streaming two or more backup objects to the same device concurrently. While one stream is preparing the backup object and logging the mailbox on/off, data from the other backup object is being transferred to the tape, keeping the device busy.

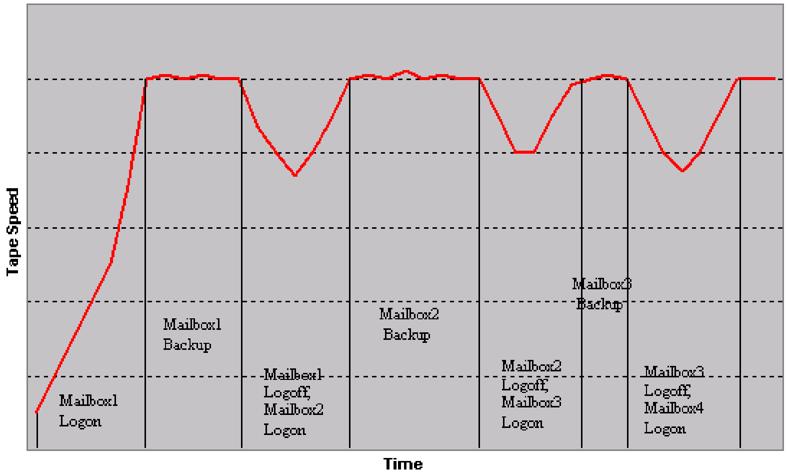


Figure 50 Example of backup with concurrency 1

Tests have shown that best performance is achieved when backing up mailboxes and Public Folders using two concurrent data streams, either by specifying one device with concurrency 2 or two devices with concurrency 1.

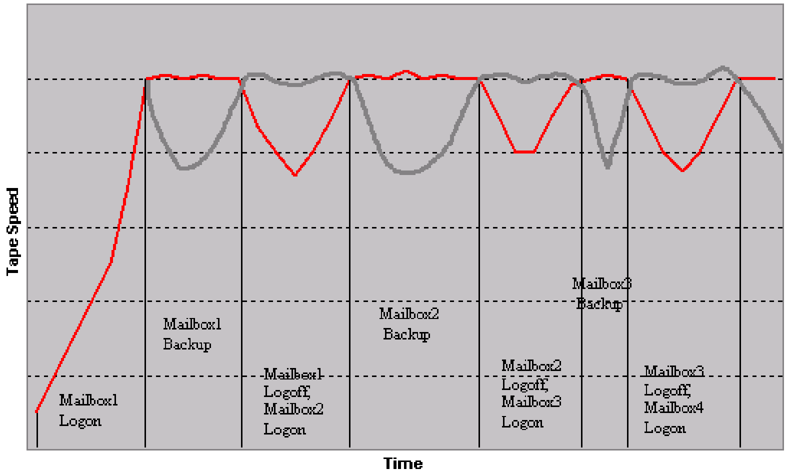


Figure 51 Example of backup with concurrency 2

NOTE:

Data Protector cannot create more than one backup object out of Exchange items from a single mailbox or Public Folders.

Troubleshooting

This section lists general checks and verifications plus problems you might encounter when using the Data Protector Exchange Single Mailbox integration. Start at "Problems" on page 148. 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*.

Before you begin

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

Checks and verifications

If your configuration, backup, or restore failed:

- Ensure that the following directories exist on the Data Protector Cell Manager:

  Data_Protector_home\config\server\barlists\Mailbox

  Data_Protector_home\config\server\barschedules\Mailbox
- Examine errors reported in

  Data_Protector_home\log\debug.log on the Exchange Server system.

Additionally, if your backup or restore failed:

- Ensure that the Cell Manager is correctly specified on the Exchange Server system: ensure that a value entry with the name CellServer and the value "*Cell Manager*" exists under the key:

  HKEY_LOCAL_MACHINE\SOFTWARE\Hewlett-Packard\OpenView\OmniBack II\Site
- Examine errors logged in the Windows Event log.

Additionally, if your backup failed:

- Preview the Data Protector Exchange Single Mailbox backup.

  If the Exchange Server part of the preview fails, ensure that the Exchange Server is online.

  If the Data Protector part of the preview fails:

  - Ensure that the Exchange Server is configured for use with Data Protector. See "Configuring Exchange servers" on page 126.
  - Create an Exchange Single Mailbox backup specification to back up to a null or file device.

    If the backup succeeds, the problem is probably related to devices. For information on troubleshooting devices, see online Help.

Problems

Problem

You do not have permissions to log in to the system

Data_Protector_home\log\debug.log on the Exchange Server contains one of the following messages:

```
Error = 596
Logon failure: the user has not been granted the requested logon type to
this computer.
```

or:

```
[MBX_ImpersonateUser] A required privilege is not held by the
client.
```

Action

Check if the Domain Controller system has domain-level policy settings defined. Go to:

`Start > Settings > Control Panel > Administrative Tools > Domain Security Policy > Local Policies > User Rights Assignment`

and check if the Act as part of the operating system and Log on as a service user rights are set to `Defined`.

If domain-level policy settings are defined:

1. On the Domain Controller system:
   - **a.** Go to:

     `Start` > `Settings` > `Control Panel` > `Administrative Tools` > `Domain Security Policy` > `Local Policies` > `User Rights Assignment`.

   - **b.** Set `Act as part of the operating system` and `Log on as a service` user rights for the Exchange Server administrator.
   - **c.** Run:

     ```
     secedit /refreshpolicy machine_policy /enforce
     ```

2. On the Exchange Server system:
   - **a.** Log off from the system and log in again under the same user account.
   - **b.** Go to:

     `Start` > `Settings` > `Control Panel` > `Administrative Tools` > `Local Security Policy` > `Local Policies` > `User Rights Assignment`.

   - **c.** Ensure that `Act as part of the operating system` and `Log on as a service` user rights are set for the Exchange Server administrator in both `Local Setting` and `Effective Setting` columns.
   - **d.** Restart the `Data Protector Inet` service.

If domain-level policy settings are not defined:

1. Log in to the Exchange Server system.
2. Go to:

   `Start` > `Settings` > `Control Panel` > `Administrative Tools` > `Local Security Policy` > `Local Policies` > `User Rights Assignment`.

3. Set `Act as part of the operating system` and `Log on as a service` user rights for the Exchange Server administrator.
4. Log off from the system and log in again under the same user account.
5. Restart the `Data Protector Inet` service.

Problem

Configuration of the Exchange Server fails

`*Data_Protector_home*\log\debug.log` on the Exchange Server system contains the following message:

```
An error has occurred while creating a profile administration
object.
```

Action

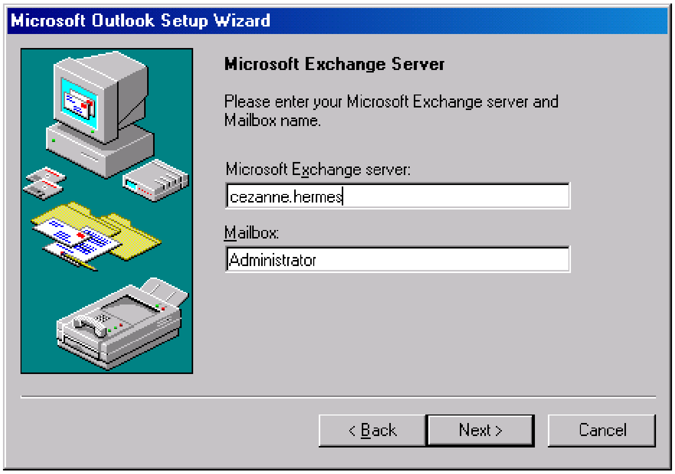
1. Log in to the Exchange Server system.
2. Delete the incorrect administrator's profile:

   ```
   mbx_bar.exe delete
   ```

3. Manually create a new profile:

   ```
   mbx_bar.exe create
   ```

4. In the **Choose Profile** page, click **New**.
5. Follow the setup wizard. Type `$$$Data Protector` for the profile name. Specify the Exchange Server system and the name of the Exchange Server administrator's mailbox. See Figure 52 on page 150.



Please enter your Microsoft Exchange server and Mailbox name.

Microsoft Exchange server: cezanne.hermes

Mailbox: Administrator

Figure 52 Specifying the Exchange Server administrator's mailbox

Problem

Restore to another client fails

Action

Ensure that Exchange Server and Data Protector **MS Exchange Single Mailbox integration** component are installed and configured on the destination system to which you restore.

Problem

Restore to another mailbox fails

Action

Ensure that the destination mailbox exists on the destination Exchange Server.

5 Integrating Microsoft Volume Shadow Copy Service with Data Protector

Introduction

A traditional backup process is based on the direct communication between the backup application and the application whose data is backed up. This backup method requires from the backup application an individual interface for each application it backs up.

The number of applications on the market is constantly increasing. The necessity of handling application specific features can cause difficulties in backup, restore, and storage activities. An effective solution to this problem is introducing a coordinator among the actors of the backup and restore process.

Volume Shadow Copy Service

Volume Shadow Copy Service (VSS) is a software service introduced by Microsoft on Windows operating systems.

During backup, the service collaborates with a backup application (for example, Data Protector), applications to be backed up (usually database applications), shadow copy providers, and the operating system kernel to create a consistent, point-in-time shadow copy set, which can be backed up to backup media or can be kept on a disk array for instant recovery or data mining.

During restore, the service collaborates with the backup application and database application to prepare for the restore operation and to perform the recovery of the restored data.

Data Protector supports the integration with VSS.

The Data Protector Volume Shadow Copy integration provides a unified communication interface that can coordinate backup and restore of an application regardless of their specific features. With this approach, a backup application does not need to handle each application to be backed up specifically. However, the production application as well as the backup application must conform to the VSS specification.

Figure 53 on page 155 and Figure 54 on page 155 show the differences between the traditional backup model and the model with the Data Protector Microsoft Volume Shadow Copy integration.

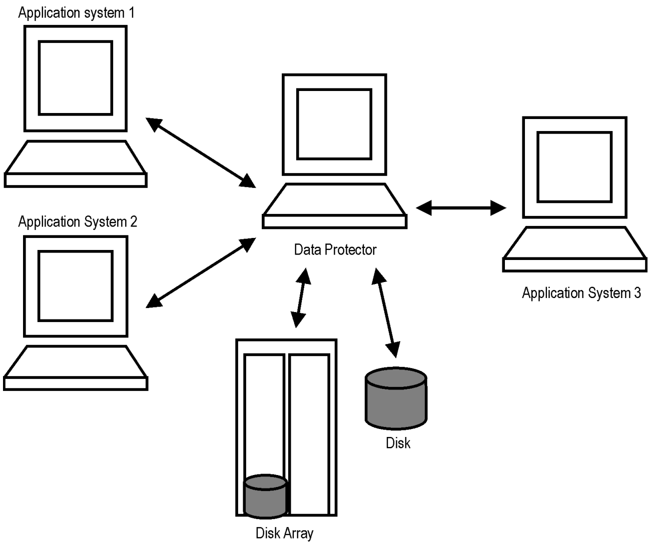


Figure 53 Actors of the traditional backup model

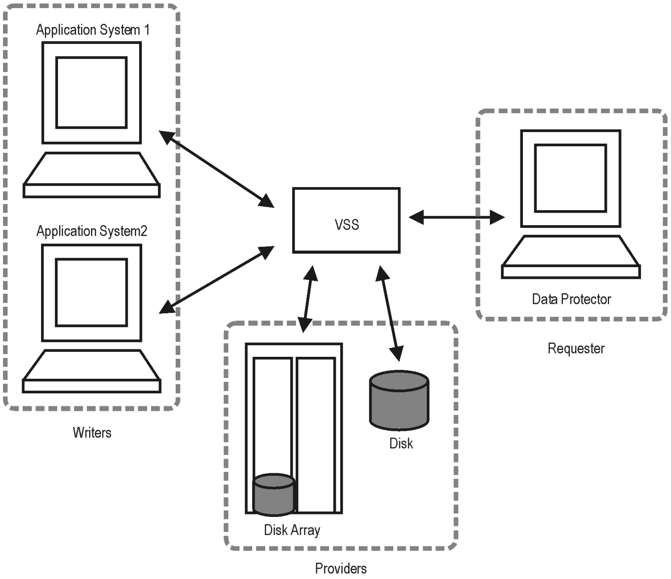


Figure 54 Actors of the Data Protector VSS integration backup model

Without using the Volume Shadow Copy Service, Data Protector has to communicate with each application to be backed up individually. The Data Protector VSS integration introduces a unified backup and restore interface and provides the coordination among the participants of the backup and restore process.

Integration concepts

The Data Protector integration with the Microsoft Volume Shadow Copy Service provides full support for certified VSS writers.

For a complete list of supported VSS writers and provider, see the latest support matrices at http://www.hp.com/support/manuals.

Benefits of using the integration

Advantages of using the Data Protector VSS integration are the following:

- Unified backup interface is provided for all applications that provide a writer.
- Data integrity is provided on application level, because it is provided by the writers. No interference is needed from the backup application.

VSSBAR agent

The central part of the integration is the **VSSBAR agent**, which links Data Protector with the Microsoft Volume Shadow Copy Service. Data Protector Microsoft Volume Shadow Copy integration uses the VSSBAR agent for automatic browsing of VSS-aware writers, coordinating backup and restore. VSSBAR agent is responsible for the following actions:

- detecting VSS writers
- examining and analyzing Writer Metadata Document (WMD)

  Writer Metadata Document (WMD) is metadata provided by each writer. Writers identify themselves by the metadata and instruct the backup application what to back up and how to restore the data. Thus, Data Protector follows the requirements provided by the writer when selecting the volumes to be backed up and the restore method.
- requesting shadow copy creation
- backing up writers' data to media
- coordinating restore session start
- restoring the Writer Metadata Document
- restoring writer's data from media

Backup

During the Data Protector VSS integration backup, Data Protector does not interact directly with each writer, but through the VSS interface. It uses the VSSBAR agent to coordinate the backup process. The consistency of data is a responsibility of the VSS writer and not dependent on Data Protector functionality. The backup process of the VSS writers consists of the following phases:

1. When you select writers and components you want to back up and start a VSS integration backup, Data Protector communicates with the Volume Shadow Copy Service (backup coordinator) to notify that the backup is about to start.
2. The coordinator identifies all writers that support the VSS feature and passes the list of available writers and their characteristics (Writer Metadata Document) back to Data Protector.
3. Data Protector examines Writer Metadata and identifies the volumes that contain the data to be backed up. Then the VSS informs available writers about selected components.
4. Data Protector prepares a list of volumes (shadow copy set) that must be put into consistent state, and passes the list back to the coordinator for preparing a shadow copy.
5. The VSSBAR agent notifies the writers about the shadow copy creation. The VSS mechanism ensures that there are no writes on the volume while the shadow copy is being created.

NOTE:

When the VSSBAR agent creates a shadow copy of the volume, this volume is marked in order to avoid attempts to simultaneously create another shadow copy of the same volume. In order to prevent any deadlocks arising from volume locking, only a single VSSBAR agent at a time is allowed to define a shadow copy set.

6. When the writers are fully prepared for the consistent shadow copy backup, the VSSBAR agent passes shadow copy creation requests to VSS.
7. After a shadow copy is created, the VSS service returns the related information to Data Protector.
8. Data Protector backs up the data from the shadow copy to media and then notifies the VSS service that the shadow copy can be released. VSS issues a command to the shadow copy provider to destroy the shadow copy that has been already backed up.

   Figure 55 on page 158 shows the relations between the actors of a local VSS backup.

9. The related information about the completed backup session is recorded in the VSSDB.

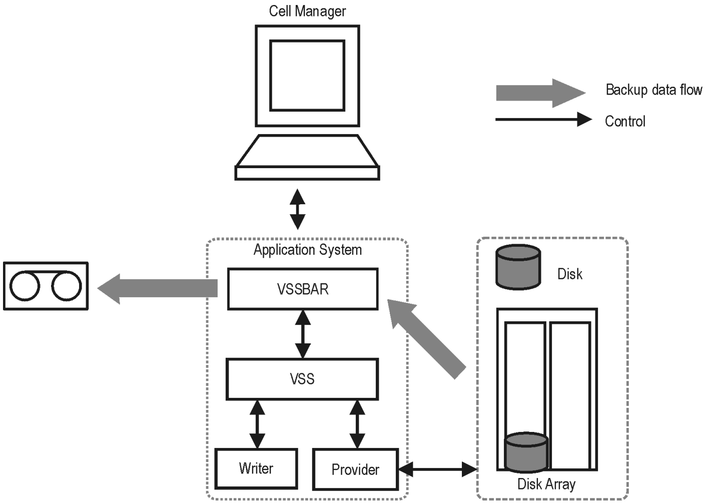


Figure 55 Local VSS backup

Data consistency

The **filesystem backup** does not guarantee application data consistency, only filesystem consistency. Application data consistency can be achieved only by using supported application writers, such as Microsoft Exchange Server writer.

Restore

Data Protector offers two restore modes:

- **component restore** using the VSS service
- **file restore** using the DMA instead of VSS.

By default, Data Protector restores writer components using the VSS service.

Instant recovery is also available within the Data Protector VSS integration. This functionality requires VDS hardware providers.

Restoring components

During the restore procedure, the Data Protector VSS integration coordinates communication between Data Protector and the writers. In general, the restore flow consists of the following phases: preparing for restore, restoring components, and notifying the application writers that a restore has been completed. The restore procedure of the VSS-aware writers consists of the following phases.

1. Data Protector first restores the metadata, which was collected during the backup. Then it examines the metadata to identify the backup components and determine the restore method. It also checks if restore to specific volumes is possible.
2. Data Protector connects to the coordinator (VSS service) to notify that the restore is about to start, which in turn communicates with the writer. Data Protector restores the data from the backup media to the locations specified in the backup metadata. During the restore, Data Protector follows the writers' instructions regarding any additional checking or processing specified in the WMD.
3. After the data are successfully restored from the backup media, Data Protector informs the coordinator that the restore is completed and the writers can now access the newly-restored data and start the internal processing, for example recovery.

Restoring files

For a successful restore of a VSS component, all files comprising this component must be restored. If a restore of a single file fails, the restore of the a whole component fails. Data Protector offers an additional restore mode for restoring single files that does not use the Microsoft Volume Shadow Copy Service, thus solving this problem. This mode can also be used for restoring to systems that do not support VSS or do not have a VSS writer installed.

When restoring files or a group of files, DMA is started and the files are restored using the standard Data Protector filesystem restore procedure.

IMPORTANT:

As the file restore mode does not utilize VSS services, additional tasks that are performed after a component restore – such as database recovery – are not performed and your application data may be left in an inconsistent state, requiring additional manual procedures before the application is recovered.

VSS database

The VSS database (VSSDB) is an extension to the Data Protector internal database (IDB) on the Cell Manager. It holds the VSS integration-specific information about the VSS backup sessions. The stored information can be used for the following purposes:

- Data mining (you can save backup components and writer metadata documents)
- Listing the backup sessions and viewing details about them
- Removing the backup sessions

You can query and manage the items of the VSSDB using the `omnidbvss` command. For information on the command syntax, description, and examples, see the *HP Data Protector command line interface reference*.

The following tasks can be performed using the `omnidbvss` command:

- Querying the VSSDB
- Deleting backup sessions

Querying the VSSDB

Using the `omnidbvss` command, you can list:

- All backup sessions, as well as their details.
- All backup sessions based on a specific backup specification, as well as their details.
- All backup sessions, which were created before a specified date, as well as their details.
- Details on a specific backup session, identified by the session ID.

Using the `omnidbvss` command, you can save the documents about the backup components and writer metadata to a specified directory.

See the `omnidbvss` man page for the command syntax and examples.

Deleting backup sessions

Using the `omnidbvss` command, you can delete:

- A specific backup session, identified by the session ID, from the the VSSDB.
- All backup sessions based on a specific backup specification or that were created before a specified date from the VSSDB.

See the `omnidbvss` man page for the command syntax and examples.

Microsoft Exchange Server 2007 writer concepts

This section gives details of additional features that Microsoft Exchange Server 2007 supports.

Backup

Microsoft Exchange Server 2007 offers two models of replication for data protection that are supported by Data Protector.

- local continuous replication (LCR)

  With LCR, you can create and maintain an exact copy (LCR copy) of databases in a storage group. LCR copies are used in the event of data corruption, since you can switch the Exchange server to use LCR copies in only a few seconds. If an LCR copy is used for backup and is located on a different disk from the original data, the load on a production database is minimal.

- cluster continuous replication (CCR)

  CCR has the same characteristics as LCR. The only difference is that in the CCR environment, databases and transaction logs are replicated to separate servers. Therefore, CCR copies can be used for disaster recovery. You can perform VSS backups on the passive Exchange Server node where the CCR copy is located and thus reduce the load on the active node.

The replicated storage groups are represented as a new Exchange Server writer instance, Exchange Replication Service. They are backed up in the same way as original or production storage groups.

If using LCR or CCR with Standby Continuous Replication (SCR) configured, backups can only be performed on the source side of the SCR. Microsoft does not support backups on the SCR target side. For further information on SCR and supported SCR configurations, refer to the Microsoft website.

Restore

With Microsoft Exchange Server 2007 writer, you can restore your data not only to the original location (from which the backup was performed) but also to a different location. You can restore:

- A whole storage group
- A single store

In both cases the respective LCR or CCR copies can also be restored.

You can restore data to:

- The original storage group
- A different storage group
- A non-Exchange location – With this restore method, after the restore is completed, the Recovery Storage Group (RSG) can be created automatically.
- A recovery server – This restore method restores data to different client and different storage group.

If you restore to a different storage group, you can access single mailboxes or individual e-mail messages at a different location without changing the original storage group content. Furthermore, if the whole server is destroyed, restoring to a different Exchange Server system (recovery server) will minimize the time window during which your mailboxes will be unavailable.

Microsoft Hyper-V VSS writer concepts

Microsoft Hyper-V writer is the successor to the Microsoft Virtual Server 2005 writer and is supported on Microsoft Windows Server 2008. It is a VSS writer with similar set of functionality as Virtual Server. With both, it is possible to perform backups and restores of virtual machines. With Hyper-V, it is possible to perform online backups using hardware providers.

For backup and restore specifics of Hyper-V writer, see "Microsoft Hyper-V VSS writer backup specifics" on page 181 and "Microsoft Hyper-V VSS writer restore specifics" on page 201.

Prerequisites

- Windows Server 2008 Service Pack 2 must be installed. For more information, see http://support.microsoft.com/kb/948465.

Microsoft SharePoint Services VSS writer concepts

The Microsoft SharePoint Services writer is a *reference* writer that integrates with the Windows VSS framework, allowing backup applications to backup up and restore Microsoft SharePoint data. This writer has dependencies on:

- Search writers:
  - OSearch VSS writer
  - SPSearch VSS writer
- SQL writers:

- MSDE writer for Microsoft SQL Server 2000
- Microsoft SQL 2005 writer for Microsoft SQL Server 2005

With the SharePoint Services writer you can back up and restore:

- the configuration database
- the central administration content database
- other content databases
- shared services provider databases
- search databases
- index files.

Backup types

The SharePoint Services writer supports the following Microsoft Office SharePoint Server 2007 backup type:

- Full (for databases and index files)

Limitations

- Multi-server SharePoint configurations (farms) are not supported.

Prerequisites

- The SharePoint Services writer and SQL writer are not started by default. Ensure that both writers are properly installed and registered. The SharePoint Services writer must be registered using the SharePoint command line administration tool:

```
stsadm -o  registerwsswriter
```

Prerequisites and limitations

This is a list of prerequisites and limitations for the Data Protector Microsoft Volume Shadow Copy Service integration. Additional limitations and recommendations that are not directly connected to the integration (such as operating system and GUI limitations) and disk array limitations are listed in the *HP Data Protector product announcements, software notes, and references*.

Prerequisites

- Before you begin, ensure that you have correctly installed and configured Data Protector, writers and shadow copy providers. Refer to the:
    - http://www.hp.com/support/manuals for an up-to-date list of supported versions, platforms, devices, disk arrays, limitations, and other information.
    - *HP Data Protector installation and licensing guide* on how to install Data Protector on various architectures and how to install the Data Protector Microsoft Volume Shadow Copy Service integration.
    - Writers and shadow copy providers documentation for instructions on how to install and configure writers and providers on your system.
- To enable successful shadow copy creation install the following Windows Server 2003 hotfixes: KB950903 and KB949002.

Limitations

For a list of general Data Protector limitations, see the *HP Data Protector product announcements, software notes, and references*.

- Maximum 512 shadow copies per volume are allowed. The number of shadow copies per volume is limited by system resources.
- To run a VSS integration backup, the writer's data must be on an NTFS filesystem. For hardware providers, this is not required.
- The VSS integration backup of writers which store their data on network shared volumes is not supported.
- The Data Protector Microsoft VSS integration does not provide any restore method for writers requesting a custom restore method. These writers are by default not presented by Data Protector.

  If a writer specifies a custom restore method, it is only possible to restore the writer's data as plain files using the Data Protector functionality. You can perform the custom restore manually. Refer to the writers documentation for additional information on the restore methods.
- Backup preview is only available for VSS filesystem backup sessions.

Configuring the integration

The Data Protector Microsoft Volume Shadow Copy integration by itself does not require any configuration steps neither on the Data Protector nor on the application side.

VSS writers are either a part of Windows operating system or delivered with applications. Data Protector automatically detects writers when the VSS backup specification is created and registers them.

You may check which writers and providers are installed and registered on your system using the following Windows operating system command:

- For a list of writers: `VSSadmin list writers`
- For a list of VSS providers: `VSSadmin list providers`

Microsoft Exchange Server writer specific configuration

A backup of the Microsoft Exchange database is considered successful only when consistency check of the replicated data files succeeds.

Prerequisites

- When configuring an Exchange Server 2007 LCR environment, ensure that the original database and the database copy of the Exchange Server have the same directory and file structure. Failing to do so will result in unsuccessful attempts to mount the database after restore of an LCR copy to the location where original database resides.

Writers specifics

This section describes specific information about VSS writers, that you need to take into account before backing up or restoring the writers.

VSS writers either come with the Windows operating system or with applications. For a complete list of supported VSS writers and providers, see the latest support matrices at http://www.hp.com/support/manuals.

The Data Protector Microsoft VSS integration does not provide any restore method for writers requesting a custom restore. If a writer specifies a custom restore method, it is only possible to restore the writer's data as plain files using the Data Protector functionality. You can perform the custom restore manually. Refer to the writers documentation for additional information on the restore methods.

NOTE:

Writers requiring custom restore methods are by default not shown by Data Protector. The `omnirc` variable `OB2VSS_SHOWALLWRITERS` must be set to `1` for all writers to be displayed.

Table 23 on page 166 provides a description of VSS writers.

Table 23 Writer description

Writer name	Description	Restore method
Certificate Authority Writer	This is a system writer, used to back up and restore Certificate Authority (CA) Service database. This service issues, revokes, and manages certificates employed in public key-based cryptography technologies.	Files are restored after a reboot.
Cluster Service Writer	This VSS writer using a custom API, is used to back up and restore Cluster Service on Microsoft Cluster Server (MSCS). The Cluster Service is a component on Windows servers used to control server cluster activities on cluster nodes. It is fundamental to the operation of the cluster.	Custom restore method
COM+ REGDB Writer	This VSS writer using a custom API, is used to back up and restore COM+ Database Service. This service provides automatic distribution of events to subscribing COM+ components.	Custom restore method
DHCP Jet Writer	This is a system writer, used to back up and restore DHCP Service database. DHCP Service provides dynamic IP address assignment and network configuration for Dynamic Host Configuration Protocol (DHCP) clients.	Files are restored after a reboot.
Event Log Writer	This is a system writer, used to back up and restore Event Logs. Event Logs are files where the Windows operating system saves information about events, such as starting and stopping services or the logging on and logging off of a user.	Files are restored after a reboot.

Writer name	**Description**	**Restore method**
FRS Writer	This VSS writer using a custom API, is used to back up and restore File Replication Service data. File Replication Service is a multithreaded replication engine that replicates system policies and logon scripts stored in System Volume (`SYSVOL`). FRS can also replicate data for Distributed File System (Dfs), copy and maintain shared files and folders on multiple servers simultaneously.	Custom restore method
IIS Metabase Writer	This is a system writer, used to back up and restore Microsoft Internet Information Server (IIS). IIS 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).	Files are restored after a reboot.
MSDE Writer	This is a writer used to back up and restore Microsoft SQL Server 2000/2005. SQL Server is a database management system that can respond to queries from client machines formatted in the SQL language.	Refer to "MSDE writer restore specifics" on page 191.
Microsoft SQL 2005 Writer	This is a writer used to back up and restore Microsoft SQL Server 2005. SQL Server is a database management system that can respond to queries from client machines formatted in the SQL language.	Standard VSS restore and instant recovery.
Microsoft Data Protection Manager 2006 Writer	This is a writer used to back up and restore Microsoft Data Protection Manager 2006. Microsoft Data Protection Manager is a server that creates and stores replicas of clients and uses them for recovering the data on clients	Refer to "Microsoft Data Protection Manager 2006 writer restore specifics" on page 198.
Microsoft Exchange Server Writer	This is a writer used to back up and restore Microsoft Exchange Server. Microsoft Exchange Server is a mail and groupware server.	Standard VSS restore and instant recovery.

Writer name	Description	Restore method
Microsoft Virtual Server 2005 Writer	This is a writer used to back up and restore Microsoft Virtual Server 2005. Microsoft Virtual Server 2005 is a virtualization platform for Microsoft Windows servers. Data Protector supports live backup of individual virtual machines and the Virtual Server configuration, ensuring data consistency of the backup and restore. Hardware providers are not supported if a Virtual Server Machine is in online mode; use a software provider or put the Virtual Server Machine in offline mode. For details about Virtual Server online and offline mode, see the Microsoft Virtual Server documentation. Cluster configurations are not supported, only individual nodes can be backed up.	Standard VSS restore and instant recovery.
Microsoft Hyper-V Writer	This is a writer used to back up and restore Microsoft Virtual Server 2008 Hyper-V configuration and individual or all virtual machines running on the server. Software and hardware providers are supported during online and offline backup. Cluster-aware backups are not supported.	Standard VSS restore and instant recovery.
SharePoint Services Writer	This is a reference writer used to back up and restore Microsoft Office SharePoint Server 2007 (MOSS). MOSS 2007 is an information portal used to connect and exchange expertise between people and teams. Only a single server configuration (farm) is supported. The OSearch VSS writer and SPSearch VSS writer are used by the reference writer to back up and restore the index files of user and help content. They must not be used for backup and restore.	Standard VSS restore. For writer specifics, see "Microsoft SharePoint Services VSS writer restore specifics" on page 202.

Writer name	Description	Restore method
NTDS Writer	This is a system writer used to back up and restore Microsoft Active Directory on Windows servers. Active Directory Service is a Windows server directory service that enables you to manage data structures distributed over a network. For example, Active Directory Service stores information about user accounts, passwords, phone numbers, profiles, and installed services. It provides methods for storing directory data and making this data available to network users and administrators.	To restore Active Directory, boot into Directory restore mode. Files will be restored if they can be overwritten.
Registry Writer	This VSS writer using a custom API, is used to back up and restore Windows Registry. Windows Registry is a database repository of information containing the Windows system configuration.	Custom restore method
Remote Storage Writer	This is a system writer used to back up and restore Remote Storage Service (RSS). RSS is used to automatically move infrequently accessed files from local to remote storage. Remote files are recalled automatically when the file is opened.	Files are restored after a reboot.
Removable Storage Manager Writer	This is a system writer used to back up and restore Removable Storage Manager Service. This service manages removable media, drives, and libraries.	Files are restored after a reboot.
System Writer	This is a system writer that backs up a specific set of Windows dynamic link libraries (DLL).	Files are restored after a reboot.
TermServLicencing Writer	This is a system writer that backs up Windows Terminal Services. These services provide a multi-session environment that allows client systems to access a virtual Windows desktop session and Windows-based programs running on the server.	Files are restored after a reboot.

Writer name	Description	Restore method
WINS Jet Writer	This is a system writer, used to back up and restore Windows Internet Name Service (WINS). WINS is a dynamic replicated database service that can register and resolve NetBIOS names to IP addresses used on a TCP/IP network.	Files are restored after a reboot.
WMI Writer	This is a system writer, used to back up and restore Windows Management Instrumentation (WMI). WMI is a unified management infrastructure in Windows for monitoring system resources.	Files are restored after a reboot.

Backing up writers data

Overview

To run backups and restores of the VSS writers and filesystems, you need to configure the Data Protector Microsoft Volume Shadow Copy Service integration backup specifications.

To configure the backup using the VSS integration, perform the following steps:

Configuration steps

1. Configure devices, media, and media pools needed for the backup. See the online Help for instructions.
2. Create a Data Protector VSS backup specification specifying the VSS components to back up, the media and devices to which you want your data to be backed up, as well as the Data Protector backup options that define the behavior of your backup or restore session.

Creating backup specifications using GUI

The procedure below shows how to back up Microsoft VSS objects using the Data Protector GUI. Some writers have specific limitations. For writers specific limitations, see:

- For Microsoft Exchange Server specifics, see "Microsoft Exchange Server writer backup specifics" on page 175.
- For Microsoft Data Protection Manager 2006 specifics, see "Microsoft Data Protection Manager 2006 writer specifics" on page 179.

To create a new backup specification for the VSS integration, proceed as follows:

1. In the **HP Data Protector Manager**, switch to the **Backup** context.
2. In the Scoping Pane, expand **Backup Specifications**.
3. Right-click **MS Volume Shadow Copy Writers** and click **Add Backup**.
4. In the **Create New Backup** dialog box, select **Local or network backup** for the backup type.
5. In Application system, specify the name of the client that has the VSSBAR agent installed.

   When backing up cluster-aware writers (such as SQL Server via the MSDE Writer, or Exchange Server in LCR or CCR environment), specify the virtual server name given in the particular writer resource group.

   Click **Next**.
6. In this page, the selection of your VSS client is displayed.

   On Windows Server 2008, you can specify the **User and group/domain** options. For information on these options, press **F1**.

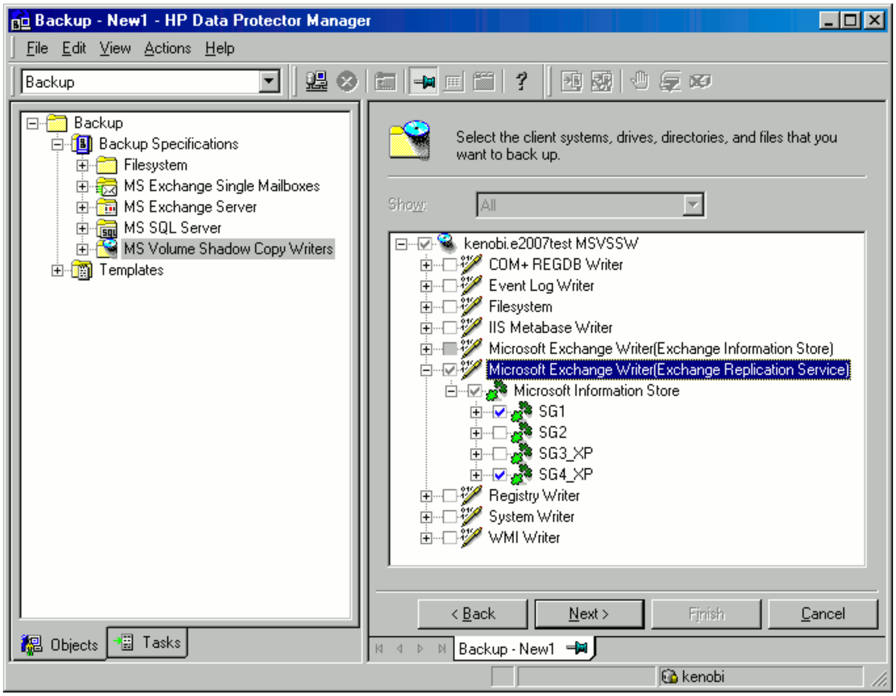
   Click **Next**.

7. Select the backup objects you want to back up.

   only a whole source volume to be backed up, regardless of the number of virtual machines residing on the volume.

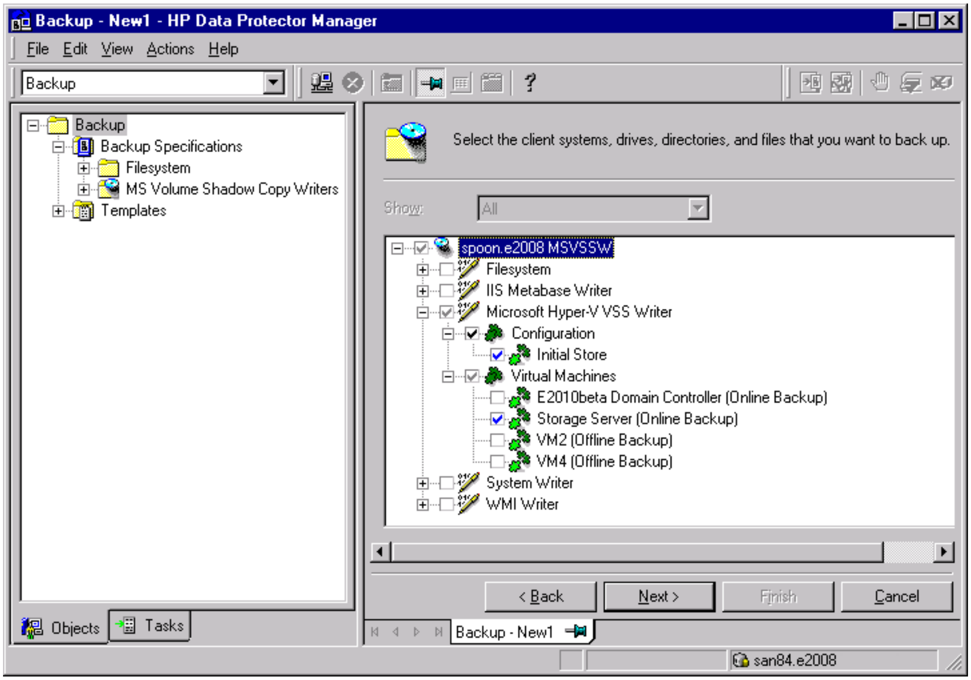
   You can specify a **full client backup** by selecting the top-level item (the name of the client), a single writer or a writer’s component backup by selecting a lower-level item.

   If full client is selected, Data Protector checks which writers exist on the client and backs up all of them at backup time.



Select the client systems, drives, directories, and files that you want to back up.

Figure 56 Selecting Microsoft Exchange Server 2007 CCR copy backup objects



Select the client systems, drives, directories, and files that you want to back up.

- ☑ spoon.e2008 MSVSSW
  - □ Filesystem
  - □ IIS Metabase Writer
  - ☑ Microsoft Hyper-V VSS Writer
    - ☑ Configuration
      - ☑ Initial Store
    - ☑ Virtual Machines
      - □ E2010beta Domain Controller (Online Backup)
      - ☑ Storage Server (Online Backup)
      - □ VM2 (Offline Backup)
      - □ VM4 (Offline Backup)
  - □ System Writer
  - □ WMI Writer

Figure 57 Selecting Microsoft Hyper–V VSS writer backup objects

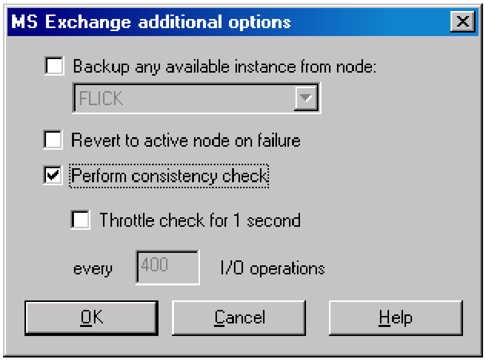
If a writer requires all of its components to be backed up, lower-level items are automatically selected. If you select such a writer for backup, all its components will be backed up.

If a writer has no components to be backed up, it is not displayed in the list of writers, and is not backed up when the full client is selected.

The **Filesystem** item displays all mounted disks. If another disk is mounted to a directory on a disk, the parent disk name is displayed twice. The first name represents the parent disk name (for example `c:`), while the second name represents the container for the mountpoint (for example `c:\mnt\1`). To select the mounted disk, select the container for the mountpoint.

Microsoft Exchange Writer: Optionally, to specify options for consistency check of Microsoft Exchange Server Writer, right-click **Microsoft Exchange Writer** and click **Additional options**.

Microsoft Exchange Server 2007 Writer in a CCR environment: Optionally, to specify clustering options, right-click **Microsoft Exchange Writer** and click **Additional options**.



MS Exchange additional options

□ Backup any available instance from node:

FLICK

□ Revert to active node on failure

☑ Perform consistency check

□ Throttle check for 1 second

every 400 I/O operations

Figure 58 Additional options for Microsoft Exchange Server 2007 in a CCR environment

8. Select the devices 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**. If you do not select a device, only backup to disk will be available.

   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 online Help.

9. Following the wizard, select the backup options and schedule your backup.

   TIP:

   If you are not sure about selecting the backup options, keep the default values.

   For details about the options common to all Data Protector backup specifications, see the online Help.

10. Once you have defined all backup options and the schedule, you need to name and save the newly-created backup specification. You have now completed the creation of a Microsoft Volume Shadow Copy Writers backup specification.

11. You can review the newly-created and saved backup specification in the **Backup** context, under the specified group of backup specifications.

12. You can run backup using one of the following methods:

    - Schedule the backup of an existing Microsoft Volume Shadow Copy Writers backup specification using the Data Protector Scheduler.
    - Start an interactive backup of an existing Microsoft Volume Shadow Copy Writers backup specification.

VSS specific backup options

Table 24 VSS specific backup options

Option	Description
Pre-exec	Specify a command that will be started by `vssbar.exe` on the application system before the backup. Do not use double quotes. Type only the name of the command, not the pathname. The command must reside in *`Data_Protector_home`*`\bin`.
Post-exec	Specify a command that will be started by `vssbar.exe` on the application system after the backup. Do not use double quotes. Type only the name of the command, not the pathname. The command must reside in *`Data_Protector_home`*`\bin`.

Microsoft Exchange Server writer backup specifics

The Microsoft Exchange Server Writer supports the following Microsoft Exchange backup types:

Backup types

The Microsoft Exchange Server Writer supports the following Microsoft Exchange backup types:

- *Full* - backs up databases, transaction logs, and checkpoint files. The transaction logs are truncated.
- *Incremental* - backs up the transaction logs to record changes since the last full or incremental backup. The transaction logs are truncated.
- *Differential* - similar as incremental backup, but the transaction logs are not truncated.
- *Copy* - a Full backup, but the logs are not truncated. This type of backup is not intended for use in recovering failed systems.

Limitations

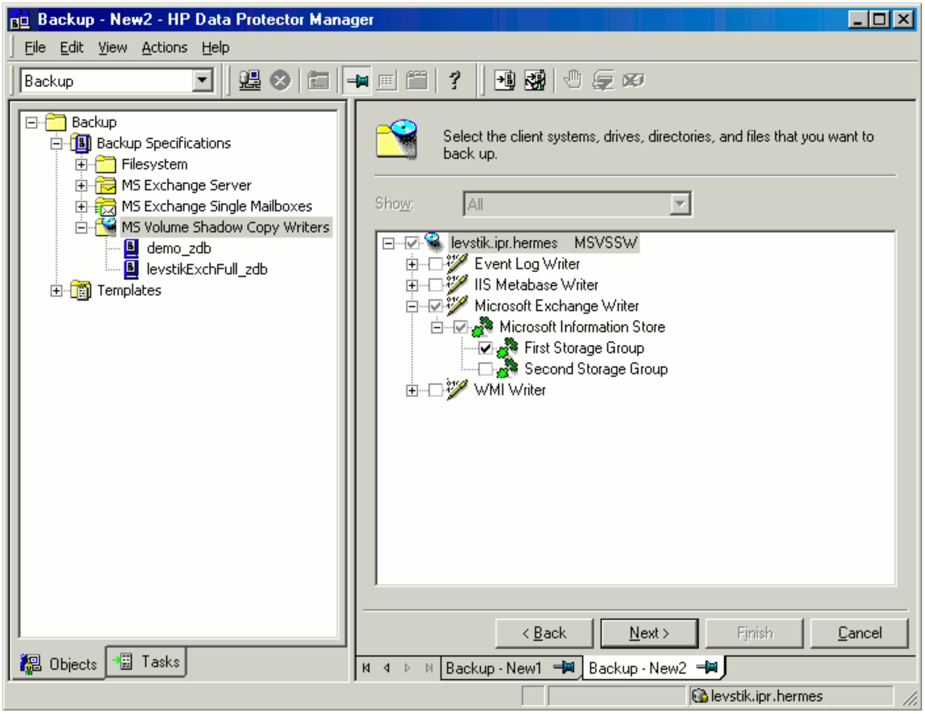
- A combination of VSS snapshot backups and non-VSS backups (for example, incremental stream backups) is not supported.
- You can back up only the whole server or full storage groups. Single stores cannot be backed up.
- Circular logging must be disabled.
- With Exchange Server 2003, only one VSS backup session can be running on the same application system at once. With Exchange Server 2007, only one VSS backup session backing up a specific storage group can be running on the same application system at once. Consequently, if you start such a backup session while another one is in progress, the latter waits until the first one finishes.

Rollforward recovery

Transaction logs must be backed up the rollforward operation.

Consistency check

A backup of the Microsoft Exchange Server database is considered as successful only if the consistency check of the replicated datafiles succeeds. The consistency check is enabled by default. To disable the consistency check, click on a created backup specification, right-click **Microsoft Exchange Writer** in the Source tab, and then click **Additional options**. In this page, you can also specify to throttle the consistency check for a second after the specified number of input/output operations.



Select the client systems, drives, directories, and files that you want to back up.

Show: All

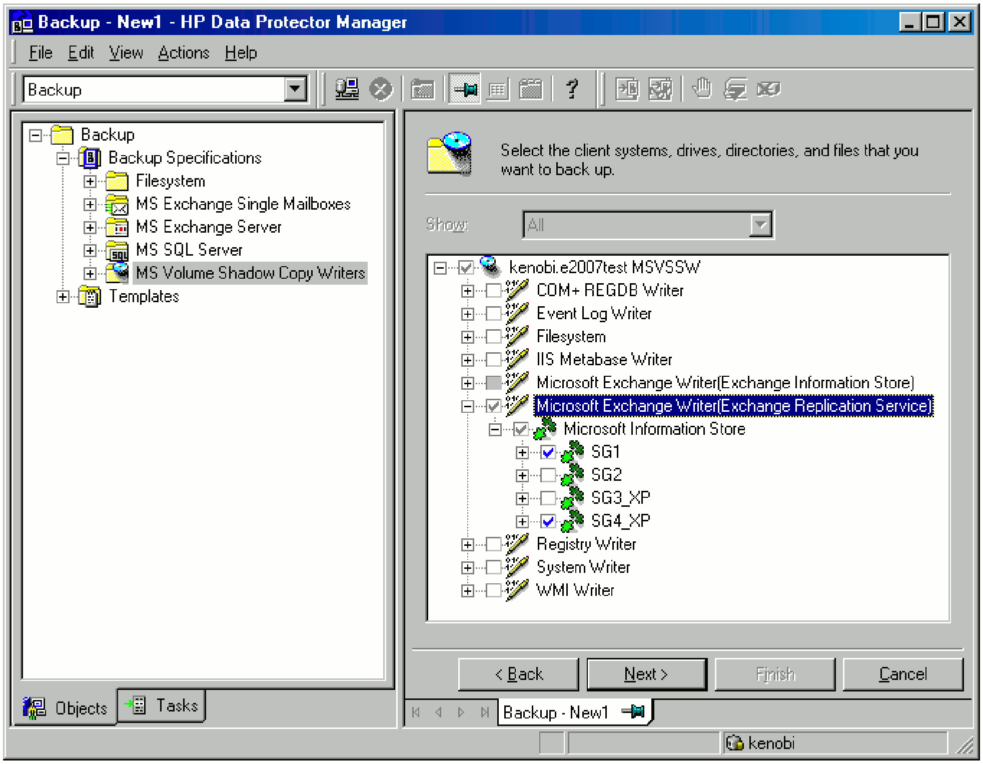
☑ levstik.ipr.hermes MSVSSW
- □ Event Log Writer
- □ IIS Metabase Writer
- ☑ Microsoft Exchange Writer
  - ☑ Microsoft Information Store
    - ☑ First Storage Group
    - □ Second Storage Group
- □ WMI Writer

Figure 59 Selecting Microsoft Exchange Server 2003 storage groups

Microsoft Exchange Server 2007 writer backup specifics

In LCR and CCR environments, the replicated storage groups are represented as a new instance of Exchange Server writer, **Exchange Replication Service**. The replicated storage groups are backed up in the same way as original (production) storage groups.

You can select any combination of storage groups for backup. However, you cannot select original and replicated storage group in the same backup specification. See Figure 60.



Select the client systems, drives, directories, and files that you want to back up.

- ☑ kenobi.e2007test MSVSSW
  - □ COM+ REGDB Writer
  - □ Event Log Writer
  - □ Filesystem
  - □ IIS Metabase Writer
  - ▨ Microsoft Exchange Writer(Exchange Information Store)
  - ☑ Microsoft Exchange Writer(Exchange Replication Service)
    - ☑ Microsoft Information Store
      - ☑ SG1
      - □ SG2
      - □ SG3_XP
      - ☑ SG4_XP
  - □ Registry Writer
  - □ System Writer
  - □ WMI Writer

Figure 60 Selecting a replicated Microsoft Exchange Server 2007 storage group

In a CCR environment, a cluster node from which you want a backup to be performed can be selected, regardless of which instance (Information Store or Replication Service) resides on this node. If you select the cluster node, Data Protector backs up any available instance on this node ignoring the selection of the instance in the GUI even if, for example, you select the replicated storage group (Exchange Replication Service) as backup object.

To specify the cluster node from which you want to perform a backup of any instance residing on this node, right-click an Exchange writer and select the node in the MS Exchange additional options dialog box under **Back up any available instance from node**. See Figure 58.

When backing up a Replication Service instance, backup may fail due to any of the following reasons:

- The selected node is not available.
- The status of the storage group to be backed up is not "Healthy".

- Data Protector is not running on the selected node.
- `Vssbar.exe` cannot not be started on the selected node.

To avoid the session failing, select the option **Revert to active node on failure** in the same dialog box. The backup will be restarted on the original server (active cluster node) and the original storage group will be backed up. This option is ignored during backup of an Information Store instance.

Prerequisites

- Before creating a backup specification and before running a backup, ensure that the Exchange Server 2007 copy status is “Healthy”. Otherwise, you cannot browse the objects to be backed up during creating backup specification, or the backup will fail. Note that the status “Initializing” is not acceptable.

Limitations

- In CCR environments, if a replicated storage group (Replication Service instance) is selected for backup, no other VSS writer (for example, filesystem writer or SQL Server writer) can be selected to be backed up in the same backup session. Because in this case, two writers would be located on different systems, but Data Protector limits VSS backup sessions to involve only one system.
- In LCR and CCR environments, each storage group can have only one store.
- CCR clusters can have only two nodes.

Considerations

- Transaction log files are truncated after each full or incremental Microsoft Exchange Server backup. The LCR and CCR clustering technologies, however, guarantee that logs that have not been replicated are not deleted. Thus, running backups in a mode that truncates logs may not actually free space. This may happen if replication of logs has not completed yet.

Microsoft Data Protection Manager 2006 writer specifics

Microsoft Data Protection Manager 2006 (DPM) is a server application that creates replicas of the clients, synchronizes them through LAN, and stores these replicas as snapshots.

The Data Protection Manager writer is used to back up:

- the Data Protection Manager database and the Data Protection Manager Report database
- the *latest version* of the DPM replicas.

IMPORTANT:

To ensure data consistency, schedule a DPM replica synchronization before starting a backup.

The DPM uses DPM snapshots for restore. These snapshots are *not* backed up. To be able to recreate DPM snapshots you must manually schedule a backup of the replica each time after the DPM creates a new replica.

Two backup types are supported:

- *Full* (for the DPM databases and replicas)
- *Incremental* (replicas only).

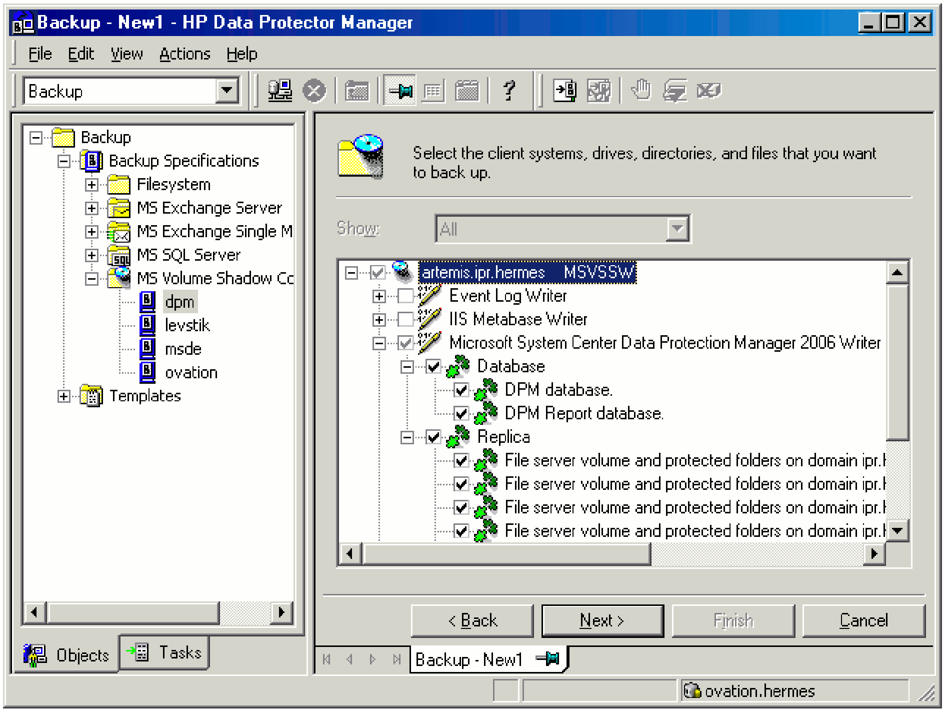
If you select unsupported backup types (*Copy* or *Differential*) when scheduling the backup, Data Protector will abort the backup and display an error message.

Prerequisite

The MSDE writer (used for backing up the DPM databases) must be installed.

Limitations

- Hardware providers are not supported with DPM.
- If you start a backup while an incremental synchronization of the DPM replica is still in progress, the backup gets corrupted, although Data Protector does not report any errors. In case of synchronization with consistency check, Data Protector automatically aborts the backup session.



Select the client systems, drives, directories, and files that you want to back up.

Show: All

Backup - New1 - HP Data Protector Manager
File Edit View Actions Help
Backup
Backup
Backup Specifications
Filesystem
MS Exchange Server
MS Exchange Single M
MS SQL Server
MS Volume Shadow Co
dpm
levstik
msde
ovation
Templates
artemis.ipr.hermes MSVSSW
Event Log Writer
IIS Metabase Writer
Microsoft System Center Data Protection Manager 2006 Writer
Database
DPM database.
DPM Report database.
Replica
File server volume and protected folders on domain ipr.h
File server volume and protected folders on domain ipr.h
File server volume and protected folders on domain ipr.h
File server volume and protected folders on domain ipr.h
< Back
Next >
Finish
Cancel
Objects
Tasks
Backup - New1
ovation.hermes

Figure 61 Selecting Microsoft Data Protection Manager database and replicas

Microsoft Hyper-V VSS writer backup specifics

With the Hyper-V VSS writer, it is possible to back up:

- The Hyper-V configuration
- Virtual machines

The following two types of backups are supported by the Data Protector VSS integration:

- *Online backup*

  Online backup of Hyper-V writer data is possible using a software provider or hardware provider.

  After restore of an online backup session, the virtual machine is always turned off, regardless of the state in which it was before the restore.

- *Offline backup*

  Offline backup is performed in the following cases:

  - The guest operating system – any other non-Microsoft guest operating system that is supported by Hyper-V – is not VSS enabled.
  - The guest operating system does not have Hyper-V VSS integration services installed.
  - The virtual machine to be backed up is turned off.

  Before offline backup, the virtual machine is automatically suspended (if not already) and resumed after the backup.

  After restore of an offline backup session, the virtual machine is suspended, regardless of the state it was in before the restore.

  The advantage of offline backup is that virtual machines are restored to the state they were in at backup time, including the state of applications running at the time of backup. This is possible because a virtual machine is in a suspended state during the backup.

Prerequisites

- For online backup:
  - The guest operating system must have the Hyper-V VSS integration services installed and should not use dynamics disks.
  - The snapshot file (`avhd` file) needs to be configured on the same volume as the virtual disk file (`vhd` file).
  - The virtual machine to be backed up must be online.
- For offline backup, if the prerequisites for online backup are met, a virtual machine to be backed up must be put in the offline or suspended state manually.

Limitations

- Cluster-aware backups are not supported.
- Only whole virtual machines can be backed up or restored.
- Backup of virtual machines configured to use physical disks is not supported.
- Hyper-V writer data backup is not supported using the XP VSS hardware provider.

Backup from a physical cluster node

When backing up from a cluster node consider the following:

- Offline backups trigger a failover.

  During offline backups the virtual machine to be backed up is suspended for a moment. The cluster server recognizes this as a failure and initiates the cluster failover. To avoid such a failover, perform one of the following:

    - Run only online backups.
    - Before running an offline backup, manually put the virtual machine into the "Saved" state using Failover Cluster Administrator.

- Whenever a failover happens, you need to use another backup specification.

  After a failover, the hostname where the virtual machine is running changes. Since this change is not reflected in the original backup specification, you need to create a new backup specification to specify the new hostname as the application system name.

Microsoft SharePoint Services VSS writer backup specifics

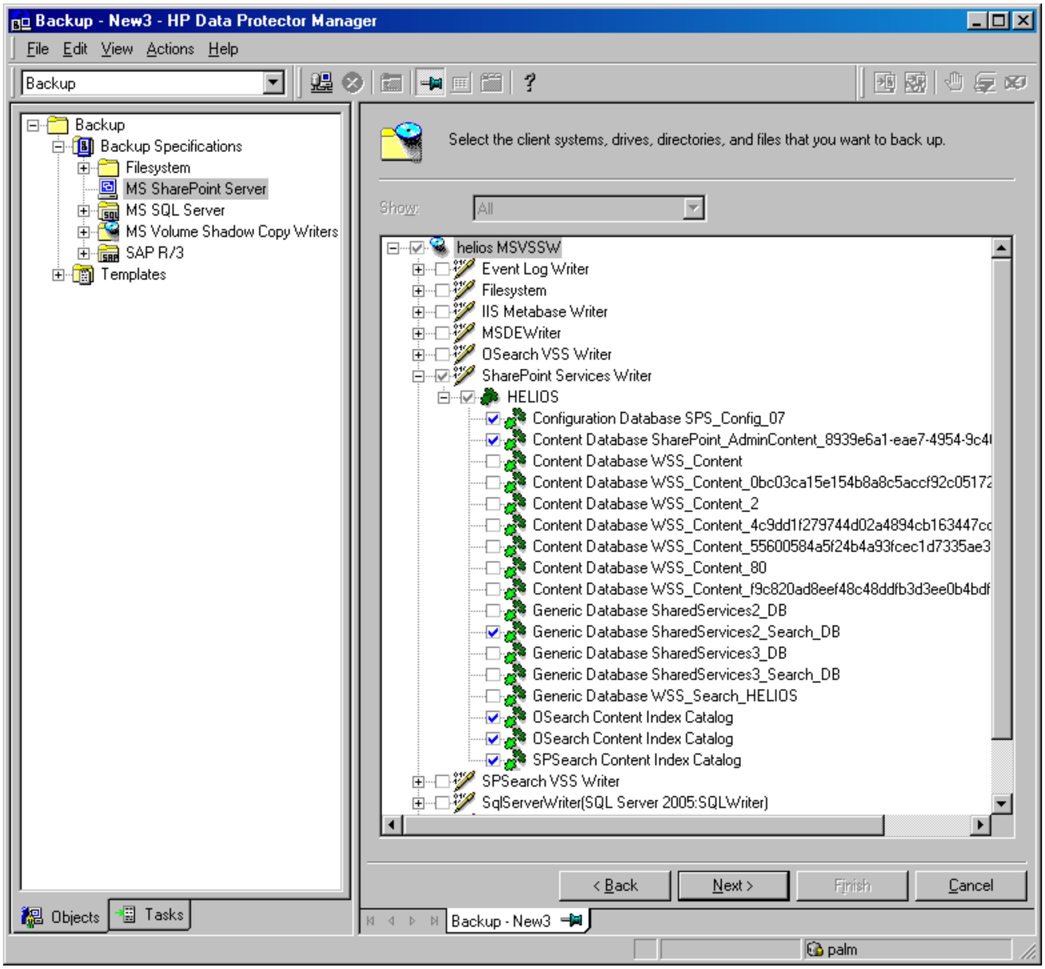
Limitations

- If you back up individual writer components, to ensure that data is synchronized, the following combinations of items must be backed up in the same session:
    - The configuration database and central administration content database
    - Search databases and corresponding index files

  This means that, for example, you should not back up just a search database. Instead, always *select also* the corresponding index file.

- Do not use the *standalone* (not part of the reference) OSearch and SPSearch writers for backing up the index files. If you use them, the search index will have to be reindexed.

See Figure 62 on page 184 for an example on how to select writer components.



Select the client systems, drives, directories, and files that you want to back up.

- ☑ helios MSVSSW
  - ☐ Event Log Writer
  - ☐ Filesystem
  - ☐ IIS Metabase Writer
  - ☐ MSDEWriter
  - ☐ OSearch VSS Writer
  - ☑ SharePoint Services Writer
    - ☑ HELIOS
      - ☑ Configuration Database SPS_Config_07
      - ☑ Content Database SharePoint_AdminContent_8939e6a1-eae7-4954-9c4
      - ☐ Content Database WSS_Content
      - ☐ Content Database WSS_Content_0bc03ca15e154b8a8c5accf92c0517
      - ☐ Content Database WSS_Content_2
      - ☐ Content Database WSS_Content_4c9dd1f279744d02a4894cb163447c
      - ☐ Content Database WSS_Content_55600584a5f24b4a93fcec1d7335ae3
      - ☐ Content Database WSS_Content_80
      - ☐ Content Database WSS_Content_f9c820ad8eef48c48ddfb3d3ee0b4bdf
      - ☐ Generic Database SharedServices2_DB
      - ☑ Generic Database SharedServices2_Search_DB
      - ☐ Generic Database SharedServices3_DB
      - ☐ Generic Database SharedServices3_Search_DB
      - ☐ Generic Database WSS_Search_HELIOS
      - ☑ OSearch Content Index Catalog
      - ☑ OSearch Content Index Catalog
      - ☑ SPSearch Content Index Catalog
  - ☐ SPSearch VSS Writer
  - ☐ SqlServerWriter(SQL Server 2005:SQLWriter)

Figure 62 Selecting Microsoft SharePoint Services writer and the corresponding search writers

Scheduling the backup

For more detailed information on scheduling, refer to the online Help index: “scheduled backups”.

To schedule a Microsoft Volume Shadow Copy Writers backup specification, perform the following steps in the Data Protector GUI:

1. In the **HP Data Protector Manager**, switch to the **Backup** context.

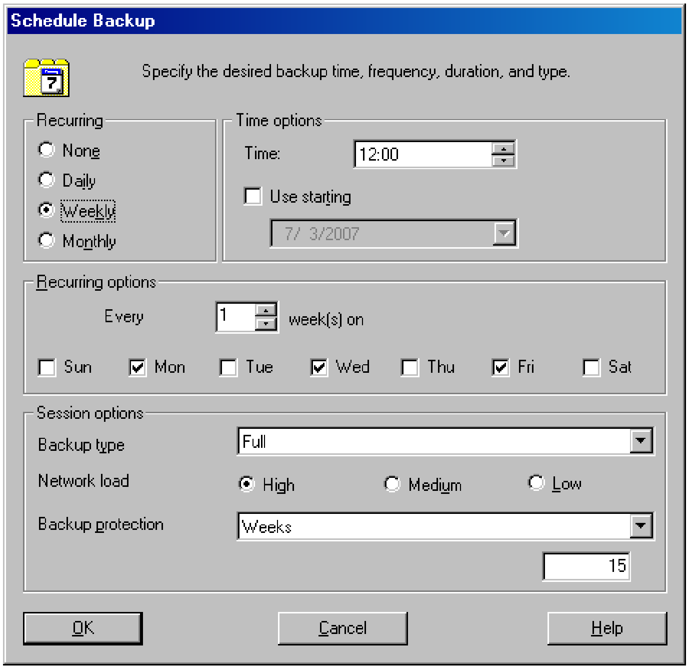
2. In the Scoping Pane, expand **Backup**, then **Backup Specifications**. Click **MS Volume Shadow Copy Writers**.

   A list of available backup specifications is displayed in the Results Area.

3. Double-click the backup specification you want to schedule and click the **Schedule** tab to open the **Schedule** property page.

4. In the **Schedule** property 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**.



Schedule Backup

Specify the desired backup time, frequency, duration, and type.

Recurring

○ None
○ Daily
● Weekly
○ Monthly

Time options

Time: 12:00

□ Use starting

7/ 3/2007

Recurring options

Every 1 week(s) on

□ Sun ☑ Mon □ Tue ☑ Wed □ Thu ☑ Fri □ Sat

Session options

Backup type: Full

Network load: ● High ○ Medium ○ Low

Backup protection: Weeks

15

Figure 63 Scheduling a backup

6. Click **OK** to return to the **Schedule** property page.

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

Running an interactive backup

An interactive backup can be started using the Data Protector GUI by following these steps:

1. In the **HP Data Protector Manager**, switch to the **Backup** context.

2. In the Scoping Pane, expand **Backup**; then expand the **Backup Specifications** and the **MS Volume Shadow Copy Writers** items.
3. Right-click the backup specification you want to run, and then select **Start Backup** from the pop-up menu.

   The **Start Backup** dialog box appears.

   Select the backup type and the network load (**High**, **Medium**, or **Low**).

   Refer to online Help for a description of network load.
4. Click **OK**. Upon successful completion of the backup session, a `Session Completed Successfully` message appears.

Restoring writers data

You can restore the Data Protector Microsoft Volume Shadow Copy Service integration backup objects using the Data Protector GUI.

NOTE:

Data Protector first restores the Writer Metadata collected during the backup time. This metadata contains the information about the backup components and the restore method. Data Protector performs restore according to the restore method specified by the writers.

Limitations for custom restore

- Data Protector Microsoft VSS integration does not automatically provide any restore method for writers requesting custom restore. If a writer specifies custom restore method, it is only possible to restore the writer's data as plain files using the Data Protector file restore functionality. You can use the `Restore Into` option to specify an alternate restore path for these plain files. You can then perform the custom restore from these plain files manually. For information on writer’s custom restore, refer to the writers documentation.

Restore procedure

The procedure below shows how to restore Microsoft VSS components using the Data Protector GUI. Some writers require custom restore procedures and/or have specific limitations. See also the appropriate sections:

- For Microsoft Exchange Server Writer specifics, see “Microsoft Exchange Server writer restore specifics” on page 193.
- For MSDE Writer specifics, see “MSDE writer restore specifics” on page 191.
- For Microsoft Data Protection Manager 2006 Writer specifics, see “Microsoft Data Protection Manager 2006 writer restore specifics” on page 198.

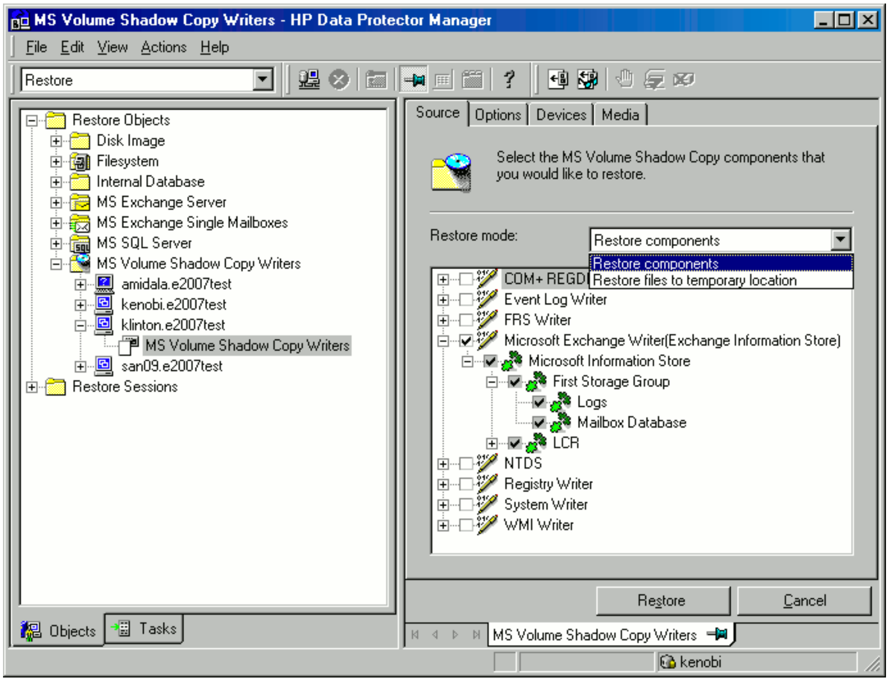
To restore Microsoft VSS objects using the Data Protector GUI, proceed as follows:

1. In the **HP Data Protector**, switch to the **Restore** context.
2. Expand **Restore Objects**, expand **MS Volume Shadow Copy Writers**, expand the client from which you want to restore the data, and then click **MS Volume Shadow Copy Writers**. In the Results Area, a list of writers, which were backed up on this client, is displayed.
3. Select the Restore mode:
   - **Restore components**

     With this option selected, whole components are restored using the Volume Shadow Copy Service. Individual files cannot be selected for restore.
   - **Restore files to temporary location**

     With this option, you can select individual files or a group of files that were backed up using the selected writer. The files are restored using the Data Mover Agent and not the Volume Shadow Copy service.

4. In the Results Area, select the writers or writers’ components (for component restore) or files or a group of files (for file restore mode).



Select the MS Volume Shadow Copy components that you would like to restore.

Restore mode: Restore components

Figure 64 Restore objects

You can select the top-level item (full writer restore) or only specific components. If you select a full writer restore, but some components of this writer were not backed up in the same session, the unavailable components are shaded and you cannot select them. To select the version (the date of a backup), right-click the object name and click **Properties**. The last available backup version is selected by default, however, you can select a different version from the drop-down list.

Exchange Server Writer: Optionally, to specify options for the consistency check of a Microsoft Exchange writer, right-click the writer and click **Additional options**.

You can perform *point-in-time* or *rollforward* restore of Microsoft Exchange Server writer. For more information, see Microsoft Exchange Server writer restore specifics.

Exchange Server 2007 Writer:

If you restore an LCR or CCR copy to the original location, the restore will be performed to the original database (Exchange Information Store) and not to the database copy (Exchange Replication Service).

a. Right-click a storage group, a store, or logs and click **Restore as**.

b. In the MS Exchange additional options dialog box, select the target location for the components you want to restore: target server, target storage group, and target stores. The following options are available:

- **Restore to a different store**

  This option is selected by default.

  Select this option to select the target stores for each store to be restored (original stores). First, select the target system from the Target server name drop-down list, and then choose the desired pairs of stores by selecting entries in the Original and Target drop-down lists. Note that only stores cannot be restored, so logs are automatically selected in the restore session to different location.

- **Restore to a non-Exchange location**

  Select this option to restore your data to a non-Exchange location. In this case, the restored data will not be managed by Exchange Server and a Recovery Storage Group (RSG) will not be created. You can manually create an RSG after the restore session completes. First, select the target system from the Target server name drop-down list, and then choose the desired stores using the Original drop-down list.

- **Restore to a non-Exchange location and create RSG**

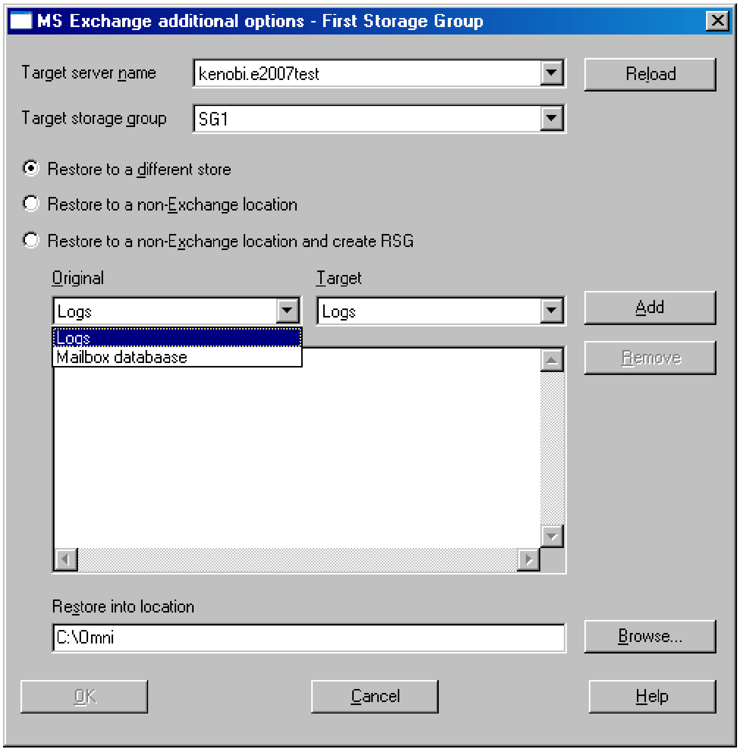
  Select this option to restore your data to a non-Exchange location. After restore, Data Protector will create a Recovery Storage Group called `DP RSG` on the target server. The selected stores and logs will be restored to this recovery group. First, select the target system from the Target server name drop-down list, and then choose the desired stores using the Original drop-down list.

By default, the storage group is restored in the `C:\Omni` directory. To select another location use the **Restore into location** option. Click **Browse** and select the desired location.

IMPORTANT:

The selected directory must be either empty or you can specify to create a new directory. If the directory is not empty, the restore session fails.

Note that you can only specify the restore location for the storage group and not for a specific store.



MS Exchange additional options - First Storage Group

Target server name: kenobi.e2007test

Target storage group: SG1

● Restore to a different store

○ Restore to a non-Exchange location

○ Restore to a non-Exchange location and create RSG

Original: Logs

Target: Logs

Logs
Mailbox databaase

Restore into location: C:\Omni

Figure 65 Restore to different location options (Exchange Server 2007 Writer)

5. In the **Options** property page, select the MS Volume Shadow Copy specific restore options. Refer to “Restore options” on page 191.
6. In the **Devices** and **Media** property pages, the devices and media for restore are automatically selected.

   Note that you can change the device used for the restore. Therefore, you have the possibility of using a different device for a restore than the one that was used for the backup. See the online Help index: “selecting devices for restore”.
7. Click **Restore**. Review your selection, and then click **Finish** to start a restore session.

   The restore session messages are displayed in the Results Area.
8. If you are restoring a VSS writer that requires a custom restore, continue manually, using the writers specific methods, if it is provided by a writer. Refer to the writers’ documentation.

Restore options

The following restore options are specific to the Data Protector MS Volume Shadow Copy integration.

NOTE:

Do not use these options for Microsoft Exchange Server 2007 writer since there are other Exchange Server 2007 specific options provided for restore to another location.

Restore to another client

By default, the components or files are restored to the client from which the application data was backed up. However, you may restore the data to another VSS client if you specify the **Restore to another client** option. The new target Microsoft VSS client must be a part of the Data Protector cell. For component restore, it must also run on the same platform and have the MS Volume Shadow Copy Integration software component installed. For file restore, the MS Volume Shadow Copy Integration software component is not required.

Restore into the following directory

By default, you restore the data to the same directory from which it was backed up (it can be on the original client or on some other client which you selected).

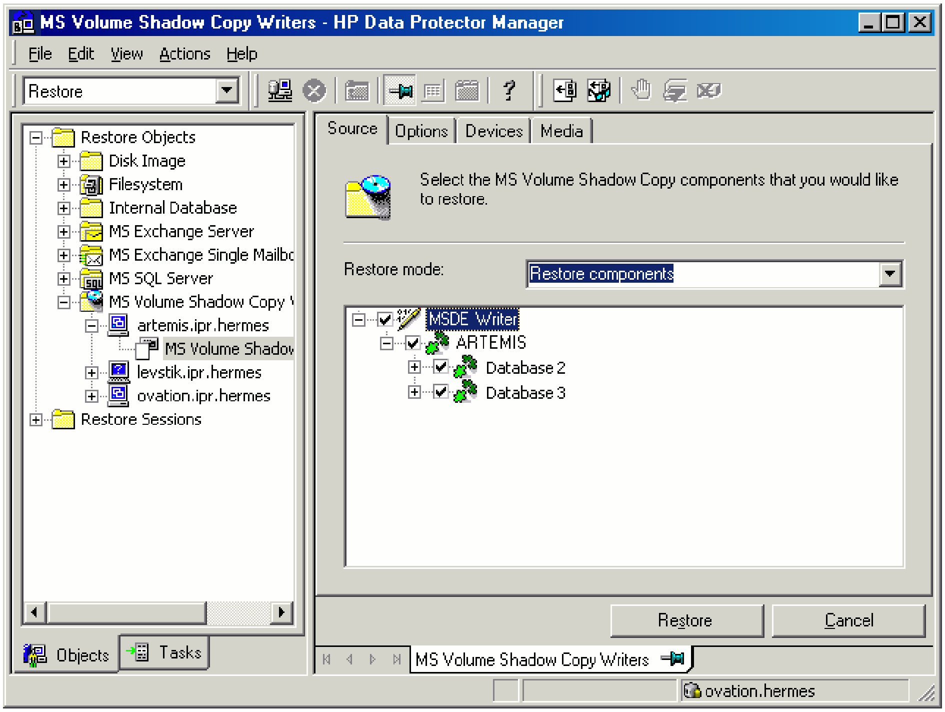
However, if you specify the **Restore into the following directory** option, your data will be restored to another directory. When defining the restore location, you can specify the path to the directory where you want to restore your data.

MSDE writer restore specifics

MSDE writer is used to back up and restore Microsoft SQL database.

IMPORTANT:

Before restoring the SQL system databases (`master`, `model`, `msdb` and `pub`), you have to stop the SQL service.



Select the MS Volume Shadow Copy components that you would like to restore.

Restore mode: Restore components

Figure 66 MSDE writer

When you expand the MSDE Writer item in the Results Area, all Microsoft SQL Server instances are displayed. Each instance contains all databases it includes. System databases (`master`, `model`, `msdb` and `pub`) are always listed there.

IMPORTANT:

If system databases are restored, the whole internal database structure will be changed.

NOTE:

Only point-in-time restore is possible. Rollforward restore is not supported.

User databases will be restored only if it is possible to overwrite the files. MSDE writer will take the user databases offline before the restore, while SQL service will have to be stopped manually in order to restore the system databases.

Microsoft Exchange Server writer restore specifics

Microsoft Exchange Server Writer is used to restore Microsoft Exchange Server database files.

When restoring from a Microsoft Exchange backup, the following two scenarios are possible:

- One or more databases are corrupted, but the log files are not damaged. In this case the database is restored and transaction logs are applied. See "Rollforward recovery from the loss of one or more databases" on page 193.
- The log files are corrupted or missing. In this case all databases and log files need to be restored. A rollforward recovery of the database is not possible. See "Point-in-time restore after loss of a log file" on page 194.

Microsoft Exchange Server 2003 limitations

- Shadow copies cannot be restored to alternate locations on the backup system.
- You cannot restore the shadow copy to the Recovery Storage Group.
- Rollforward recovery cannot be performed after a point-in-time restore.
- Restore to Microsoft Exchange Server 2007 from backup made with Microsoft Exchange Server 2003 is not supported.

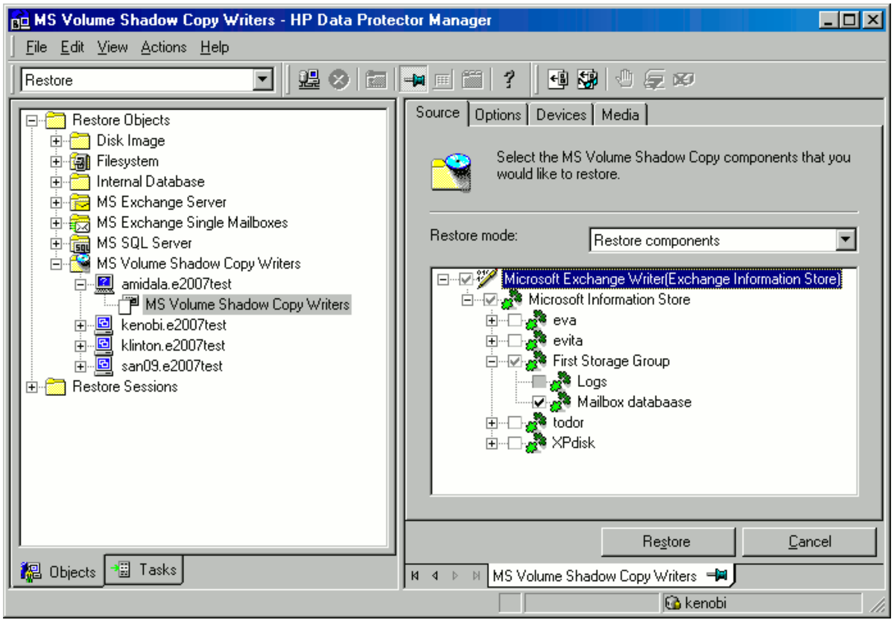
Rollforward recovery from the loss of one or more databases

For a rollforward recovery:

1. In case of Microsoft Exchange Server 2003 writer, dismount all stores from the storage group in which the target store resides using Microsoft Exchange System Manager.

2. In the Data Protector GUI, switch to the **Restore** context. Expand **Restore Objects** and **MS Volume Shadow Copy Writers** and select the client from which you want to restore the data.

   In the Results Area, expand Microsoft Exchange Writer and select the stores you want to recover. The **Logs** component is shaded and cannot be selected. You cannot select versions of individual stores, because a rollforward recovery is performed only to the current storage group state.



Select the MS Volume Shadow Copy components that you would like to restore.

Restore mode: Restore components

Figure 67 Selecting Microsoft Exchange Server 2007 stores for rollforward recovery

3. Proceed as with general VSS writer restore. See "Restore procedure" on page 186 for the general VSS writer restore procedure.

4. Mount all stores from the storage group in which they reside using Exchange System Manager. Selected stores are recovered.

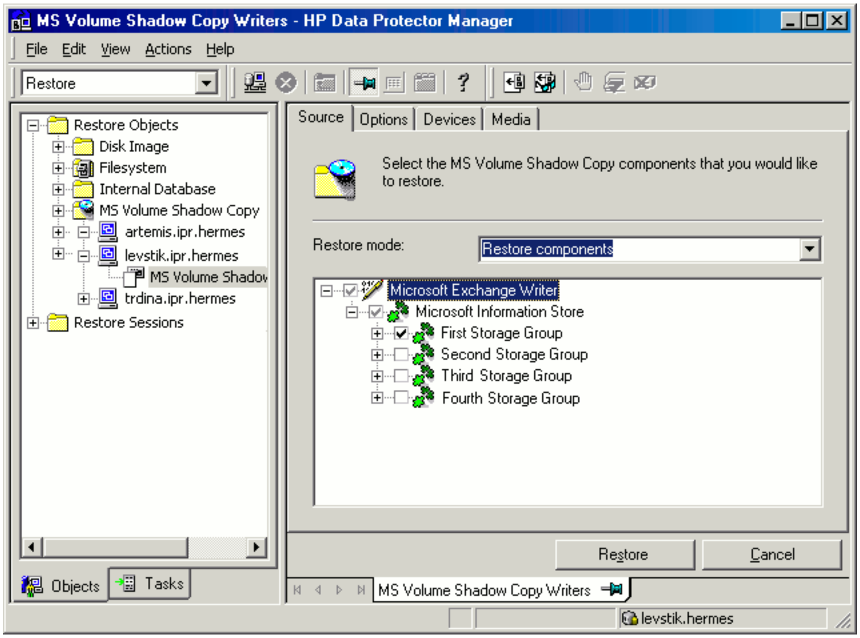
Point-in-time restore after loss of a log file

To perform a point-in-time restore:

1. In case of Microsoft Exchange Server 2003 writer, start Exchange System Manager and check if the storage group is already dismounted. If not, dismount the whole group.

2. Switch to the **Restore** context. Expand **Restore Objects** and **Microsoft Volume Shadow Copy Writers** and select the client from which you want to restore the data.

   In the Results Area, expand Microsoft Exchange Writer and select the whole storage group. Do not select individual stores.



Select the MS Volume Shadow Copy components that you would like to restore.

Restore mode: Restore components

- ☑ Microsoft Exchange Writer
  - ☑ Microsoft Information Store
    - ☑ First Storage Group
    - □ Second Storage Group
    - □ Third Storage Group
    - □ Fourth Storage Group

Figure 68 Selecting Microsoft Exchange Server 2003 stores for point-in-time restore

3. Proceed as with general VSS writer restore. See “Restore procedure” on page 186 for the general VSS writer restore procedure.

4. Mount the stores from the storage group in which the target stores reside using Exchange System Manager. All stores are mounted and put in the state as they were at the last selected full, incremental, or differential backup.

Microsoft Exchange Server 2007 writer restore specifics

Microsoft Exchange Server 2007 writer offers an additional restore option:

- Restore to a different location than the location from where the backup was made (original location). After that, a recovery storage group can be created by Data Protector.

The following restore scenarios are supported:

- Restore of a storage group or individual stores to the original location.
- Restore of LCR and CCR copies (storage groups or individual stores) to the location where the original database resides.
- Restore of a storage group or individual stores and LCR and CCR copies (storage groups or individual stores) to a different location:
  - *Restore to a different storage group*

    Data can be restored to a **different storage group**. Exchange Server can then replay the restored logs from the original storage group on the target storage group to bring the restored database up to date. If you perform restore to a different storage group, you can access single mailboxes or individual e-mail messages on the alternate location without compromising availability of the original storage group with a potentially unsuccessful restore operation.
  - *Restore to a non-Exchange location*

    Data can be restored to a **non-Exchange location**. On Data Protector session level, this option is already available if you use **Restore into the following directory** option. On a storage group level, however, a storage group can be restored to a target directory, and another one to a different storage group in the same session if the target client system is the same. Individual stores can also be restored to a non-Exchange location. During the restore, data is restored into target component destination path.

    In this scenario, the restored data is not managed by Exchange Server.
  - *Restore to a non-Exchange location with creation of Recovery Storage Group (RSG)*

    Data can be restored to a non-Exchange location and a **Recovery Storage Group** can be created for the databases afterwards. Exchange Server recognizes the Recovery Storage Group `DP RSG` created by Data Protector.
  - *Restore to Recovery Server*

    If the Exchange Server system is unusable, an entire storage group can be restored to another Exchange Server system (**Recovery Server**) and some other storage group. If the target system is identical to original (the same host name, storage group names, store names, and the same directory structure), restore can be started as normal restore to original location. In case of differences, restore to a different location must be used.

  To restore to a different location, right-click the storage group, or store, or logs to be restored and click **Restore as**. Select target locations for all the components you want to restore.

You can restore different storage groups to original and different location in the same restore session if the target restore client system is the same for all storage groups involved.

During restore to original location, all stores in the storage group are dismounted, even if only one store from the storage group will be restored. After restore, the stores are left dismounted.

Prerequisites

- For restore to a different location, `Inet` must run under a domain account which needs to be member of the following groups on the local system:
  - Administrators
  - Exchange Server Administrators
- While configuring restore to a different storage group in the Data Protector GUI, only mounted stores are displayed in the **Target** drop-down list. To enable all stores for target selection, mount the dismounted stores and click **Reload** in the **MS Exchange additional options**.

IMPORTANT:

During a restore to a non-Exchange location and creation of a Recovery Storage Group (RSG), Data Protector deletes an RSG that may already exists at the target location.

Limitations

Due to Microsoft Exchange Server limitations:

- Restore to an LCR or CCR storage group copy (Exchange Replication Service instance) is not supported. Restore of an LCR or CCR copy to original location will be performed to the location where original database resides (Exchange Information Store).
- All stores in an RSG must originate from the same storage group.
- You cannot mount public folders to an RSG.
- Because only one storage group in an RSG is supported, only one storage group can be restored with the option **Restore to a non-Exchange location and create RSG**.
- When restoring to a different location, you cannot restore a specific database store without the transaction logs. When a store is selected for restore, logs are automatically included in the restore.

- If an RSG for the storage group you are restoring already exists on some system other than the target system, the RSG is not automatically deleted and so the creation of an RSG on the target system fails. In this case, you should manually delete the RSG on the other system.

Microsoft Data Protection Manager 2006 writer restore specifics

When restoring the DPM writer, you can:

- Restore the DPM *server* first and then use the DPM to restore clients.

  In case of a disaster, when the entire DPM server is lost, perform a standard disaster recovery procedure first and continue with restoring the DPM server. See "Restore the DPM server first" on page 198

- Restore individual DPM *clients* directly, without using the DPM server (for example, if you cannot restore the DPM server or if you want to avoid the additional step of recreating the DPM snapshot). When restoring the DPM clients directly you can select between component restore and file restore modes. See "Restore the DPM clients directly" on page 201.

NOTE:

Although the Data Protection Manager databases could also be restored using the MSDE writer, this method is not recommended, because DPM is *not* shut down automatically as with the DPM writer. If you really need to use this writer, shut down the DPM server manually.

Limitations

- Restore to another server is not supported by the Data Protection Manager writer.
- Parallel restore to different clients is not supported.

Restore the DPM server first

1. Start the DPM administrator console and add disks to the storage pool so that you have enough free space to restore the replicas.

   Ensure that the DPM writer (service) is started.

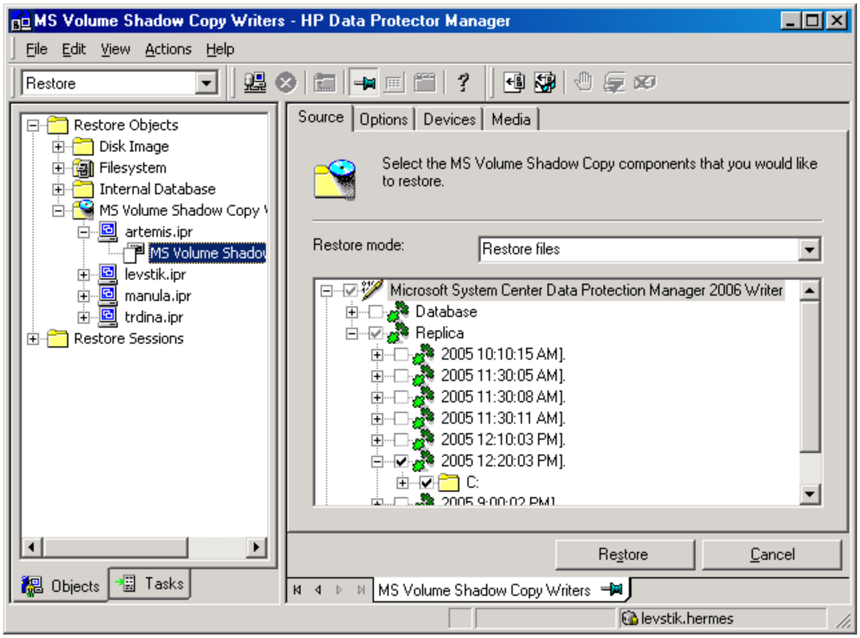
2. Switch to the Data Protector **Restore** context. Expand **Restore** and **Microsoft Volume Shadow Copy Writers** and select the client from which you want to restore the data.

3. In the Results Area, expand the DPM writer and select *only* the Data Protection Manager databases.

   Proceed as with general VSS writer restore. See "Restore procedure" on page 186 for the general VSS writer restore procedure.

4. Run the DPM command `DpmSync –Sync` to reallocate replicas.

5. Switch back to the Data Protector **Restore** context, and select and restore the necessary *replicas*.



- Restore Objects
  - Disk Image
  - Filesystem
  - Internal Database
  - MS Volume Shadow Copy \
    - artemis.ipr
      - MS Volume Shadov
    - levstik.ipr
    - manula.ipr
    - trdina.ipr
- Restore Sessions

Select the MS Volume Shadow Copy components that you would like to restore.

Restore mode: Restore files

- ☑ Microsoft System Center Data Protection Manager 2006 Writer
  - □ Database
  - ☑ Replica
    - □ 2005 10:10:15 AM]
    - □ 2005 11:30:05 AM]
    - □ 2005 11:30:08 AM]
    - □ 2005 11:30:11 AM]
    - □ 2005 12:10:03 PM]
    - ☑ 2005 12:20:03 PM]
      - ☑ C:
    - □ 2005 9:00:02 PM]

Figure 69 Restoring the Microsoft Data Protection Manager 2006 client

6. Use the DPM to restore individual clients.

IMPORTANT:

The DPM console does not automatically check for new or restored snapshots. Before you can start the restore of clients, you must use the Data Protection Manager to recreate a DPM snapshot.

a. In the DPM console, open the **Recovery** context. Under the **Browse** tab, select the server, right click on the restored replica, and select **Create shadow copy now**.

b. Select and restore the new snapshot to the client.

Restore the DPM clients directly

1. Switch to the **Restore** context. Expand **Restore** and **Microsoft Volume Shadow Copy Writers** and select the client from which you want to restore the data.
2. Select the restore modes:
   - **Restore Components**

     Use this mode *only* if the client to which you want to restore supports VSS, for example if you restore to Windows Server 2003 clients.

     You can restore only entire replicas.
   - **Restore Files**

     The client does not need to support VSS and you can restore individual folders or files.
3. When selecting the DPM writer for restore, select *only* the **Replica** components. Do not select the DPM database.
4. Click the **Options** tab, and under **Restore to another client** enter the name of the target client. Click **Next**.
5. Proceed as with general VSS writer restore. See "Restore procedure" on page 186 for the general VSS writer restore procedure.

Microsoft Hyper-V VSS writer restore specifics

Restore of Hyper-V writer data is possible to the original or to a different location. During a restore to a different location, the Hyper-V writer checks whether a virtual machine with the same identity already exists on the system. If it does, the Hyper-V writer removes the virtual machine from the system before restore and imports the restored virtual machine. If such a virtual machine does not exist on the system, it means that a restore session to this system is in progress or that the virtual machine was already removed. It is possible to perform restore of Hyper-V virtual machines to any Hyper-V system, which has a Hyper-V writer.

Restore from a physical cluster node

Backup sessions from a physical cluster node can be restored to any cluster node. To successfully restore such a session to a cluster node, perform the following steps:

1. Delete the cluster group of the virtual machine to be restored using Failover Cluster Management.

2. Perform standard restore of the virtual machine on the cluster node where the virtual machine disk is active. For the standard restore procedure, see "Restore procedure" on page 186.
3. Re-create the virtual machine cluster group using Failover Cluster Management.

Microsoft SharePoint Services VSS writer restore specifics

To ensure that data is synchronized the following items must be restored in the same session:

- Configuration database and central administration content database
- Search databases and corresponding index files

This means that, for example, you should not restore just a search database. Instead, always *select also* the corresponding index file.

See Figure 70 on page 203.

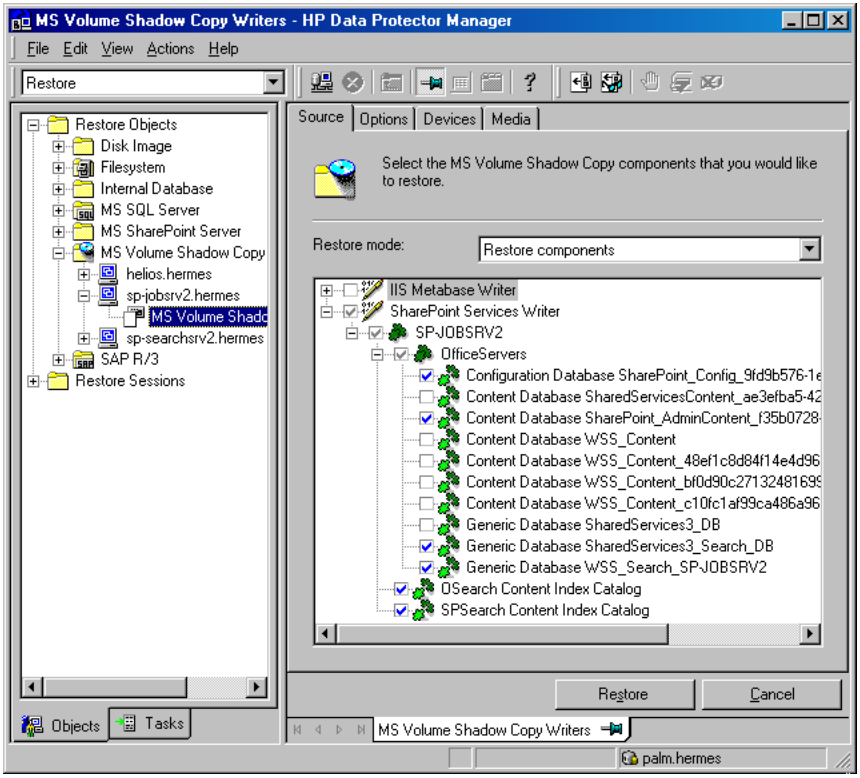
Because the configuration database and the central administration content database contain system-specific information, you can restore them only to an environment that you configure to be precisely the same, including all software updates, server names, and number of servers.

Prerequisites

- Before performing a restore, stop the following services:
  - Windows SharePoint Services Administration
  - Windows SharePoint Services Search
  - Windows SharePoint Services Timer
  - Office SharePoint Server Search
- If you restore the whole farm, you must shut down the Internet Information Server (IIS).

Limitations

- The VSS restore mode **Restore files to temporary location** is not supported.
- The VSS restore option **Restore to another client** is not supported.



Select the MS Volume Shadow Copy components that you would like to restore.

Restore mode: Restore components

- □ IIS Metabase Writer
- ☑ SharePoint Services Writer
  - ☑ SP-JOBSRV2
    - ☑ OfficeServers
      - ☑ Configuration Database SharePoint_Config_9fd9b576-1e
      - □ Content Database SharedServicesContent_ae3efba5-42
      - ☑ Content Database SharePoint_AdminContent_f35b0728-
      - □ Content Database WSS_Content
      - □ Content Database WSS_Content_48ef1c8d84f14e4d96
      - □ Content Database WSS_Content_bf0d90c27132481699
      - □ Content Database WSS_Content_c10fc1af99ca486a96
      - □ Generic Database SharedServices3_DB
      - ☑ Generic Database SharedServices3_Search_DB
      - ☑ Generic Database WSS_Search_SP-JOBSRV2
    - ☑ OSearch Content Index Catalog
    - ☑ SPSearch Content Index Catalog

Figure 70 Selecting Microsoft SharePoint Services writer and the corresponding search writers for restore

Monitoring a VSS backup and restore

The Data Protector GUI enables you to monitor current or view previous backup and restore sessions.

Monitoring is automatically activated when you start a restore or a backup interactively.

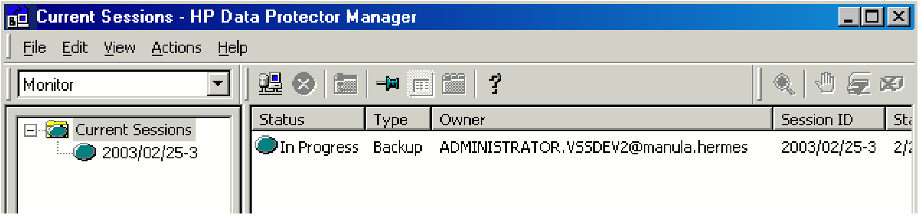
Monitoring current sessions

To monitor a currently running session using the Data Protector GUI, proceed as follows:

1. In the Context List, click **Monitor**.

   In the Results Area, all currently running sessions are listed. See Figure 71 on page 204.

2. Double-click the session you want to monitor.


Current Sessions - HP Data Protector Manager
File Edit View Actions Help
Monitor
Current Sessions
2003/02/25-3

Status	Type	Owner	Session ID	Sta
In Progress	Backup	ADMINISTRATOR.VSSDEV2@manula.hermes	2003/02/25-3	2/

Figure 71 Monitoring a current session

Clearing sessions

To remove all completed or aborted sessions from the Results Area of the **Monitor** context, proceed as follows:

1. In the Scoping Pane, click **Current Sessions**.
2. In the **Actions** menu, select **Clear Sessions**. Or click the **Clear Sessions** icon on the toolbar.

To remove a particular completed or aborted session from the current sessions list, right-click the session and select **Remove From List**.

NOTE:

All completed or aborted sessions are automatically removed from the Results Area of the **Monitor** context if you restart the Data Protector GUI.

For detailed information on a completed or aborted session, see “Viewing previous sessions” on page 204.

Viewing previous sessions

To view a previous session using the Data Protector GUI, proceed as follows:

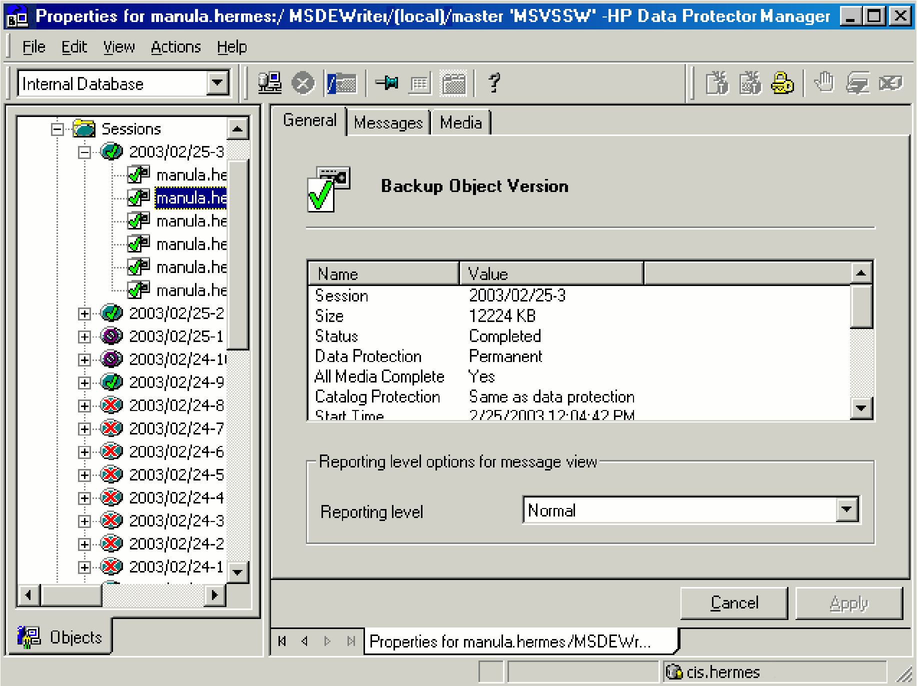
1. In the Context List, click **Internal Database**.

2. In the Scoping Pane, expand **Sessions** to display all the sessions stored in the IDB.

   The sessions are sorted by date. Each session is identified by a session ID consisting of a date in the YY/MM/DD format and a unique number.

3. Right-click the session and select **Properties** to view details on the session.

4. Click the **General**, **Messages** or **Media** tab to display general information on the session, session messages, or information on the media used for this session, respectively. See Figure 72 on page 205.



Name	Value
Session	2003/02/25-3
Size	12224 KB
Status	Completed
Data Protection	Permanent
All Media Complete	Yes
Catalog Protection	Same as data protection
Start Time	2/25/2003 12:04:42 PM

Reporting level options for message view

Reporting level: Normal

Figure 72 Viewing a previous session

Troubleshooting

This section lists problems you might encounter when using the Data Protector Microsoft Volume Shadow Copy integration.

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

Before you begin

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

Checks and verifications

- On the application and backup systems, examine system errors reported in:

  `Data_Protector_home\log\debug.log`

Backup problems

Problem

Microsoft Exchange Server 2003 writer backup failed

When you start a backup of a Microsoft Exchange Server 2003 Writer, the following error is displayed:

```
[MAJOR]: Writer ‘Microsoft Exchange Writer’ failed to prepare files
for backup.
```

The reason may be the failure of the previous backup and, due to a Microsoft Exchange Server 2003 issue, the Exchange Server Writer could not perform a proper cleanup.

Action

Restart the Information Store.

For more information, see the web page http://support.microsoft.com/kb/945424/en-us.

Problem

Microsoft Exchange Server 2003 aborts the backup if the shadow copy creation takes over 20 seconds

If an Exchange Server 2003 Writer is being backed up, the session can fail with VSSBAR reporting:

```
Snapshot could not be created.
```

In the application event log on the application system, the following event is recorded:

```
Event Type: Error
Event Source: ESE Event
Category: (16)
Event ID: 2004
Information Store (4916) Shadow copy 3 time-out (20000 ms).
```

Action

The following can help to solve the problem:

- Limit the number of users that are accessing the management system.
- Reduce the number of volumes in a snapshot set. Create a backup specification dedicated to each storage group instead of one specification for the whole server. See “Microsoft Exchange Server writer backup specifics” on page 175.

Problem

Backup of a Microsoft Exchange Server 2007 CCR database copy fails

During a backup session of a database copy in a Microsoft Exchange Server CCR environment, Data Protector reports a major error notifying that the backup session has failed.

This problem may occur in CCR environments, due to a Microsoft Exchange Server 2007 issue with incorrect display of database copy states in Exchange Management Console. In such a case, a database copy in a "Failed" state may be displayed as "Healthy".

Action

To make the Exchange Management Console show the real status of a database copy, perform either of the following actions:

- Update Microsoft Exchange Server 2007 with Service Pack 1.
- Perform re-seeding procedure as follows:
  1. On the passive node, suspend the replication by using `Suspend-StorageGroupCopy` cmdlet.
  2. Delete all log files from the `Logs` directory of the database copy.

3. Seed the database copy or re-synchronize the original database and its copy by using the `Update-StorageGroupCopy` cmdlet.
4. Resume the database copy by using the `Resume-StorageGroupCopy` cmdlet.
5. On the passive node, check the status of the Exchange Replication Service by using `vssadmin list writers` command. If the status is not `stable`, restart Microsoft Exchange Replication Service.

Problem

Exchange Replication Service writer instance in LCR environment is not displayed in the Data Protector GUI

In the Data Protector GUI, while creating a backup specification, the `Microsoft Exchange Writer(Exchange Replication Service)` object is not displayed on the pane for selection of backup objects.

This problem may occur in LCR environments, due to a Microsoft Exchange Server 2007 issue with incorrect display of database copy states in Exchange Management Console. In such a case, a database copy in a "Failed" state may be displayed as "Healthy".

Action

To make the Exchange Management Console show the real status of a database copy and to enable selection of the backup object, restart Microsoft Exchange Replication Service.

Restore problems

Problem

After the restore of system writers was aborted, the Windows operating system is corrupted when you restart it

If the restore of some system writers (for example, System Writer) is aborted for any reason (hardware or software failure, manually aborted, etc.), the Windows operating system may be corrupted after the restart (for example, the GUI or some system services cannot be started, etc.).

Action

Depending on the nature of the corruption, repair or re-install the operating system from the Windows installation CD-ROM.

Problem

Creation of an RSG fails when an RSG for the same storage group already exists

When you start a restore of the Microsoft Exchange Server 2007 writer with the option `Restore to a non-Exchange location and create RSG`, the following error is displayed:

```
[Major]
Application specific function 'PostRestoreEndExt' failed with error:
'The mailbox database that you specified is already associated with
a recovery mailbox database.
```

This error appears if an RSG for a storage group or mailbox database you restore is already created on some other system.

Action

Since only one RSG can exist for the same storage group and since Data Protector can only delete an RSG that exists on the target restore location, you need to manually delete the RSG on the other system and restart the restore.

Glossary

access rights

See user rights.

ACSLS

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

Active Directory

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

AES 256–bit encryption

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

AML

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

application agent

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

application system

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

archived redo log

(Oracle specific term) Also called offline redo log. If the Oracle database operates in the ARCHIVELOG mode, as each online redo log is filled, it is copied to an archived log destination. This copy is the archived redo log. The presence or absence of

an archived redo log is determined by the mode the database is using:

- ARCHIVELOG - The filled online redo log files are archived before they are reused. The database can be recovered if an instance or a disk fails. A “hot” backup can be performed only when the database is running in this mode.
- NOARCHIVELOG - The filled online redo log files are not archived.

See also online redo log.

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

ASR Set A collection of files stored on several diskettes, required for proper reconfiguration of the replacement disk (disk partitioning and logical volume configuration) and automatic recovery of the original system configuration and user data that was backed up during the full client backup. These files are stored as an ASR archive file on the Cell Manager in the directory `Data_Protector_program_data\Config\Server\dr\asr` (Windows Server 2008), `Data_Protector_home\Config\Server\dr\asr` (other Windows systesm), 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 *(Oracle specific term)* Automatic Storage Management is an Oracle 10g/11g integrated filesystem and volume manager that manages Oracle database files. It eliminates complexity associated with managing data and disk and provides striping and mirroring capabilities to optimize performance.

automigration

(VLS specific term) The functionality that allows data backups to be first made to the VLS' virtual tapes and then migrated to physical tapes (one virtual tape emulating one physical tape) without using an intermediate backup application.
See also Virtual Library System (VLS) and virtual tape.

BACKINT

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

backup API

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

backup chain

See restore chain.

backup device

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

backup generation

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

backup ID

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

backup object

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

- Client name: Hostname of the Data Protector client where the backup object resides.
- Mount point: For filesystem objects — the access point in a directory structure on the client where the backup object is

located (drive on Windows and mount point on UNIX). For integration objects — backup stream identification, indicating the backed up database/application items.

- Description: For filesystem objects — uniquely defines objects with identical client name and mount point. For integration objects — displays the integration type (for example, SAP or Lotus).
- Type: Backup object type. For filesystem objects — filesystem type (for example, WinFS). For integration objects — "Bar".

backup owner

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

backup session

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

backup set

A complete set of integration objects associated with a backup.

backup set

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

backup specification

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

backup system

(ZDB specific term) A system connected to target volumes of one or multiple application systems. The backup system is typically connected to a backup device to perform the backup of the data in a replica.

See also application system, target volume, and replica.

backup types

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

backup view

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

BC

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

BC

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

BC EVA

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

BC Process

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

BC VA

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

BCV

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

Boolean operators

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

boot volume/disk/ partition

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

BRARCHIVE

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

BRBACKUP

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

BRRESTORE

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

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

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

BSM

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

CA

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

CA+BC EVA

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

CAP

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

catalog protection

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

CDB

The Catalog Database is a part of the IDB that contains information about backup, restore, object copy, object consolidation, object verification, and media management sessions. Depending on the selected logging level, it also contains file names and file versions. This part of the database is always local to the cell.
See also MMDB.

CDF file

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

cell

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

Cell Manager

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

centralized licensing

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

Centralized Media Management Database (CMMDB)

See CMMDB.

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-aware application

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

cluster continuous replication

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

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

See also Exchange Replication Service and local continuous replication.

CMD Script for Informix Server

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

CMMDB

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

See also MoM.

COM+ 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-line interface (CLI)

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

Command View (CV) EVA

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

Command View VLS

(VLS specific term) A web browser-based GUI that is used to configure, manage, and monitor the VLS through a LAN.
See also Virtual Library System (VLS).

concurrency

See Disk Agent concurrency.

control file

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

copy set

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

CRS

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

CSM

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

data file

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

data protection

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

data stream

Sequence of data transferred over the communication channel.

Data_Protector_home

On Windows Vista and Windows Server 2008, the directory containing Data Protector program files. On other Windows operating systems, the directory containing Data Protector program files and data files. Its default path is `%ProgramFiles%\OmniBack`, but the path can be changed in the Data Protector Setup Wizard at installation time.
See also Data_Protector_program_data.

Data_Protector_program_data

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

database library

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

database parallelism

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

Data Replication (DR) group

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

database server

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

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

DC directory The Detail Catalog (DC) directory contains DC binary files, which store information about file versions. It represents the DCBF part of the IDB, which occupies approximately 80% of the IDB. The default DC directory is called the `dcbf` directory and is located on the Cell Manager in the directory `Data_Protector_program_data\db40` (Windows Server 2008), `Data_Protector_home\db40` (other Windows systems), or `/var/opt/omni/server/db40` (UNIX systems). You can create more DC directories and use a custom location. Up to 50 DC directories are supported per cell. The default maximum size of a DC directory is 16 GB.

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

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

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

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

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

device streaming A device is streaming if it can feed enough data to the medium to keep it moving forward continuously. Otherwise, the tape has to be stopped, the device waits for more data, reverses the tape a little and resumes to write to the tape, and so on. In other words, if the data rate written to the tape is less or equal the data rate which can be delivered to the device by the computer system, then the device is streaming. Streaming significantly improves the performance of the device and use of space.

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

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

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

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

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

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

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

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 (rawdisk) backup

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

disk quota

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

disk staging

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

distributed file media format

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

Distributed File System (DFS)

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

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

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

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

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

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

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

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

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

dynamic client
See client backup with disk discovery.

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

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

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 key 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 Event Log is accessible only to Data Protector users in the `Admin` group and to Data Protector users who are granted the `Reporting and notifications` user rights. You can view or delete all events in the Event Log.

Event Logs

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

Exchange Replication Service

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

exchanger

Also referred to as SCSI Exchanger.
See also library.

exporting media

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

Extensible Storage Engine (ESE)

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

failover

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

failover

(HP StorageWorks EVA specific term) An operation that reverses the roles of source and destination in CA+BC EVA configurations.
See also CA+BC EVA.

FC bridge

See Fibre Channel bridge.

Fibre Channel An ANSI standard for high-speed computer interconnection. Using either optical or copper cables, it allows the high speed bi-directional transmission of large data files and can be deployed between sites kilometers apart. Fibre Channel connects nodes using three physical topologies: point-to-point, loop, and switched.

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

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

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

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

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

file tree walk *(Windows specific term)* The process of traversing a filesystem to determine which objects have been created, modified, or deleted.

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

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

first-level mirror *(HP StorageWorks Disk Array XP specific term)* HP StorageWorks Disk Array XP allows up to three mirror copies of a primary

volume and each of these copies can have additional two copies. The three mirror copies are called first-level mirrors.
See also primary volume and MU number.

flash recovery area

(Oracle specific term) Flash recovery area is an Oracle 10g/11g managed directory, filesystem, or Automatic Storage Management disk group that serves as a centralized storage area for files related to backup and recovery (recovery files).
See also recovery files.

fnames.dat

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

formatting

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

free pool

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

full backup

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

full database backup

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

full mailbox backup

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

full ZDB

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

global options file

A file that allows you to customize Data Protector. It explains the global options, which cover various aspects of Data

Protector, typically time-outs and limits, and affect the entire Data Protector cell. The file is located on the Cell Manager in the directory `Data_Protector_program_data\Config\Server\Options` (Windows Server 2008), `Data_Protector_home\Config\Server\Options` (other Windows systems), or `/etc/opt/omni/server/options` (HP-UX or Solaris systems).

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

GUI
A graphical user interface provided by Data Protector for easy access to all configuration, administration, and operation tasks. Besides the original Data Protector GUI that runs on Windows, Data Protector also provides a Java-based graphical user interface with the same look and feel, which runs on numerous platforms.

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

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

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

Holidays file
A file that contains information about holidays. You can set different holidays by editing the Holidays file on the Cell Manager in the directory `Data_Protector_program_data\Config\Server\holidays` (Windows Server 2008), `Data_Protector_home\Config\Server\holidays` (other Windows systems), or `/etc/opt/omni/server/Holidays` (UNIX systems).

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

HP Operations Manager HP Operations Manager provides powerful capabilities for operations management of a large number of systems and applications in a network. Data Protector provides an integration into this management product. This integration is implemented as a SMART Plug-In for HP Operations Manager management servers on Windows, HP-UX, Solaris, and Linux. Earlier versions of HP Operations Manager were called IT/Operation, Operations Center, Vantage Point Operations, and OpenView Operations.

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

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

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

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

information or method invocation, and returns standardized responses.
See also HP StorageWorks EVA SMI-S Agent and Command View (CV) EVA.

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

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

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

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

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

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

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

See also backup types.

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

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

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

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

incremental ZDB A filesystem ZDB to tape or ZDB to disk+tape session in which only changes from the last protected full or incremental backup are streamed to tape.
See also full ZDB.

Inet A process that runs on each UNIX system or service that runs on each Windows system in the Data Protector cell. It is responsible for communication between systems in the cell and for starting other processes needed for backup and restore. The Inet service is started as soon as Data Protector is installed on a system. The Inet process is started by the inetd daemon.

Information Store *(Microsoft Exchange Server specific term)* The Microsoft Exchange Server service that is responsible for storage management. Information Store in Microsoft Exchange Server manages two kinds of stores: mailbox stores and public folder stores. A mailbox store consists of mailboxes that belong to individual users. A public folder store contains public folders and messages that are shared among several users.
See also Key Management Service and Site Replication Service.

Informix Server *(Informix Server specific term)* Refers to Informix Dynamic Server.

initializing *See* formatting.

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

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

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

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

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

ISQL

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

Java GUI Client

The Java GUI Client is a component of the Java GUI that contains only user interface related functionalities and requires connection to the Java GUI Server to function.

Java GUI Server

The Java GUI Server is a component of the Java GUI that is installed on the Data Protector Cell Manager system. The Java GUI Server receives requests from the Java GUI Client, processes them and then sends the responses back to the Java GUI Client. The communication is done through Hypertext Transfer Protocol (HTTP) on port 5556.

jukebox

See library.

jukebox device

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

keychain

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

Key Management Service

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

KMS

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

keystore

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

LBO

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

library

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

lights-out operation or unattended operation

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

LISTENER.ORA

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

load balancing

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

local and remote recovery

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

local continuous replication

(Microsoft Exchange Server specific term) Local continuous replication (LCR) is a single-server solution that creates and maintains an exact copy (LCR copy) of a storage group. An LCR copy is located on the same server as the original storage group. When an LCR copy is created, it is kept up to date through change propagation (log replay) technology. The replication feature in LCR guarantees that logs that have not been replicated are not deleted. The implication of this behavior is that running backups in a mode that deletes logs may not actually free space if replication is sufficiently far behind in its log copying.

An LCR copy is used for disaster recovery because you can switch to the LCR copy in a few seconds. If an LCR copy is used for backup and if it is located on a different disk than the original data, then the I/O load on a production database is minimal. A replicated storage group is represented as a new instance of Exchange writer called Exchange Replication Service and can be backed up (using VSS) as a normal storage group.
See also cluster continuous replication and Exchange Replication Service.

lock name You can configure the same physical device several times with different characteristics, by using different device names. The lock name is a user specified string that is used for locking all such device configurations to prevent collision if several such devices (device names) are used concurrently. Use an identical lock name for all device definitions which use the same physical device.

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

logging level The logging level determines the amount of details on files and directories written to the IDB during backup, object copying, or object consolidation. You can always restore your data, regardless of the logging level used during backup. Data Protector provides four logging levels: Log All, Log Directories, Log Files, and No Log. The different logging level settings influence the IDB growth, backup speed, and the convenience of browsing data for restore.

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

login ID

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

login information to the Oracle Target Database

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

- *`user_name`* is the name by which a user is known to Oracle Server and to other users. Every user name is associated with a password and both have to be entered to connect to an Oracle Target Database. This user must have Oracle SYSDBA or SYSOPER rights.
- *`password`* must be the same as the password specified in the Oracle password file (`orapwd`), which is used for authentication of users performing database administration.
- *`service`* is the name used to identify an SQL*Net server process for the target database.

login information to the Recovery Catalog Database

(Oracle specific term) The format of the login information to the Recovery (Oracle) Catalog Database is *`user_name/password@service`*, where the description of the user name, password, and service name is the same as in the Oracle SQL*Net V2 login information to the Oracle target database. In this case, *`service`* is the name of the service to the Recovery Catalog Database, not the Oracle target database. Note that the Oracle user specified here must be the owner of the Oracle Recovery Catalog.

Lotus C API

(Lotus Domino Server specific term) An interface for the exchange of backup and recovery information between Lotus Domino Server and a backup solution, like Data Protector.

LVM

A Logical Volume Manager is a subsystem for structuring and mapping physical disk space to logical volumes on UNIX systems. An LVM system consists of several volume groups, where each volume group has several volumes.

Magic Packet

See Wake ONLAN.

mailbox

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

mailbox store

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

Main Control Unit (MCU)

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

Manager-of-Managers (MoM)

See MoM.

make_net_recovery

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

make_tape_recovery

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

MAPI

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

MCU

See Main Control Unit (MCU).

Media Agent

A process that controls reading from and writing to a device, which reads from or writes to a medium (typically a tape). During a backup session, a Media Agent receives data from the Disk Agent and sends it to the device for writing it to the medium.

During a restore 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 sssion, the Disk Agent then writes the data to the disk. A Media Agent also manages the robotics control of a library.

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

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

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

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

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

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

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

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

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

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

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

merging

This defines one mode to resolve file conflicts during restore. If the file to be restored already exists at the destination, the one with the more recent modification date is kept. Files not present on the disk are always restored.
See also overwrite.

Microsoft Exchange Server

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

Microsoft Management Console (MMC)

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

Microsoft SQL Server

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

Microsoft Volume Shadow Copy Service (VSS)

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

mirror *(EMC Symmetrix and HP StorageWorks Disk Array XP specific term)*

See target volume.

mirror rotation *(HP StorageWorks Disk Array XP specific term)*

See replica set rotation.

MMD

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

MMDB

The Media Management Database (MMDB) is a part of the IDB that contains information about media, media pools, devices, libraries, library drives, and slots configured in the cell, as well as the Data Protector media used for backup. In an enterprise backup environment, this part of the database can be common to all cells.
See also CMMDB, CDB.

MoM

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

mount request

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

mount point

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

MSM

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

MU number

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

multi-drive server

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

obdrindex.dat

See IDB recovery file.

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

object
See backup object.

object consolidation
The process of merging a restore chain of a backup object, consisting of a full backup and at least one incremental backup, into a new, consolidated version of this object. The process is a part of the synthetic backup procedure. The result is a synthetic full backup of the specified backup object.

object consolidation session
A process that merges a restore chain of a backup object, consisting of a full backup and at least one incremental backup, into a new, consolidated version of this object.

object copy
A copy of a specific object version that is created during an object copy session or a backup session with object mirroring.

object copy session
A process that creates an additional copy of the backed up data on a different media set. During an object copy session, the selected backed up objects are copied from the source to the target media.

object copying
The process of copying selected object versions to a specific media set. You can select object versions from one or several backup sessions to be copied.

object ID
(Windows specific term) The object IDs (OIDs) enable access to NTFS 5 files no matter where in the system the files reside. Data Protector treats the OIDs as alternate streams of the files.

object mirror
A copy of a backup object created using object mirroring. Object mirrors are often referred to as object copies.

object mirroring
The process of writing the same data to several media sets during a backup session. Data Protector enables you to mirror all or some backup objects to one or more media sets.

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.

- For simple backup methods (non ZDB), the database is generally put into a quiescent state that allows use by the backup system, but not the application, for the whole backup period (several minutes or hours). For instance, for backup to tape, until streaming of data to the tape is finished.
- For ZDB methods, the database is also put into the quiescent state, but for the period of the data replication process only (several seconds). Normal database operation can then be resumed for the rest of the backup process.

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

offline recovery Offline recovery is performed if the Cell Manager is not accessible, for example, due to network problems. Only standalone and SCSI library devices can be used for offline recovery. Recovery of the Cell Manager is always offline.

offline redo log *See* archived redo log.

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

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

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

online backup

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

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

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

online redo log

(Oracle specific term) Redo logs that have not been archived, but are either available to the instance for recording database activity or are filled and waiting to be archived or reused.
See also archived redo log.

OpenSSH

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

Oracle Data Guard

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

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

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

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

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

ownership Backup ownership affects the ability of users to see and restore data. Each backup session and all the data backed up within it is assigned an owner. The owner can be the user that starts an interactive backup, the account under which the CRS process is running, or the user specified as the owner in the backup specification options.
If a user starts an existing backup specification without modifying it, the backup session is not considered as interactive.
If a modified backup specification is started by a user, the user is the owner unless the following is true:

- The user has the Switch Session Ownership user right.
- The backup session owner is explicitly defined in the backup specification, where the username, group or domain name, and the system name are specified.

If a backup is scheduled on a UNIX Cell Manager, the session owner is root:sys unless the above conditions are true.
If a backup is scheduled on a Windows Cell Manager, the session owner is the user specified during the installation, unless the above conditions are true.

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

`*Data_Protector_program_data*\Config\Server\dr\p1s` (Windows Server 2008), `*Data_Protector_home*\Config\Server\dr\p1s` (other 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 StorageWorks Disk Array XP specific term)* A mirrored pair of disks can have various status values depending on the action performed on it. The three most important status values are:

- COPY - The mirrored pair is currently re-synchronizing. Data is transferred from one disk to the other. The disks do not contain the same data.
- PAIR - The mirrored pair is completely synchronized and both disks (the primary volume and the mirrored volume) contain identical data.
- SUSPENDED - The link between the mirrored disks is suspended. That means that both disks are accessed and updated independently. However, the mirror relationship is still maintained and the pair can be re-synchronized without transferring the complete disk.

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

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

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 and as shell scripts on UNIX.
See also pre-exec.

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

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

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

primary volume (P-VOL)
(HP StorageWorks Disk Array XP specific term) Standard HP StorageWorks Disk Array XP LDEVs that act as a primary volume for the CA and BC configurations. The P-VOL is located in the MCU.
See also secondary volume (S-VOL) and Main Control Unit (MCU).

protection
See data protection and also catalog protection.

public folder store

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

public/private backed up data

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

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

RAID

Redundant Array of Inexpensive Disks.

RAID Manager Library

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

RAID Manager XP

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

rawdisk backup

See disk image backup.

RCU

See Remote Control Unit (RCU).

RDBMS

Relational Database Management System.

RDF1/RDF2

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

RDS

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

Recovery Catalog

(Oracle specific term) A set of Oracle tables and views that are used by Recovery Manager to store information about Oracle databases. This information is used by Recovery Manager to manage the backup, restore, and recovery of Oracle databases. The recovery catalog contains information about:

- The physical schema of the Oracle target database
- Data file and archived log backup sets
- Data file copies
- Archived Redo Logs
- Stored scripts

Recovery Catalog Database

(Oracle specific term) An Oracle database that contains a recovery catalog schema. You should not store the recovery catalog in your target database.

recovery files

(Oracle specific term) Recovery files are Oracle 10g/11g specific files that reside in the flash recovery area: the current control file, online redo logs, archived redo logs, flashback logs, control file autobackups, datafile copies, and backup pieces. *See also* flash recovery area.

RecoveryInfo

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

Recovery Manager (RMAN)

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

recycle

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

redo log

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

Remote Control Unit (RCU)

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

Removable Storage Management Database

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

reparse point

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

replica

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

replica set

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

replica set rotation

(ZDB specific term) The use of a replica set for regular backup production: Each time the same backup specification requiring the use of a replica set is run, a new replica is created and added to the set, until the maximum number for the set is

reached. After that, the oldest replica in the set is replaced, maintaining the maximum number of replicas in the set.
See also replica and replica set.

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

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

resync mode *(HP StorageWorks Disk Array XP VSS provider specific term)* One of two XP VSS hardware provider operation modes. When the XP provider is in the resync mode, the source volume (P-VOL) and its replica (S-VOL) are in the suspended mirror relationship after a backup. The maximum number of replicas (S-VOLs per a P-VOL) rotated is three provided that MU range is 0-2 or 0, 1, 2. Restore from a backup in such a configuration is possible only by re-synchronization of an S-VOL with its P-VOL.
See also VSS compliant mode, source volume, primary volume (P-VOL), replica, secondary volume (S-VOL), MU number, and replica set rotation.

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

RSM The Data Protector Restore Session Manager controls 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.

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

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

Scheduler

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

secondary volume (S-VOL)

(HP StorageWorks Disk Array XP specific term) secondary volumes, or S-VOLs, are XP LDEVs that act as a secondary CA or BC mirror of another LDEV (a P-VOL). In the case of CA, S-VOLs can be used as failover devices in a MetroCluster configuration. The S-VOLs are assigned separate SCSI addresses, different from the addresses used by the P-VOLs.
See also primary volume (P-VOL) and Main Control Unit (MCU)

session

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

session ID

An identifier of a backup, restore, object copy, object consolidation, 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.

SIBF

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

Site Replication Service

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

slot

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

SMB

See split mirror backup.

smart copy

(VLS specific term) A copy of the backed up data created from the virtual tape to the physical tape library. The smart copy process allows Data Protector to distinguish between the source and the target medium thus enabling media management.
See also Virtual Library System (VLS).

smart copy pool

(VLS specific term) A pool that defines which destination library slots are available as smart copy targets for a specified source virtual library.
See also Virtual Library System (VLS) and smart copy.

SMBF

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

snapshot

(HP StorageWorks VA and HP StorageWorks EVA specific term) A form of replica produced using snapshot creation techniques.

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

snapshot backup *(HP StorageWorks VA and HP StorageWorks EVA specific term)*

See ZDB to tape, ZDB to disk, and ZDB to disk+tape.

snapshot creation

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

source (R1) device

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

source volume

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

sparse file

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

split mirror

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

split mirror backup *(EMC Symmetrix specific term)*

See ZDB to tape.

split mirror backup *(HP StorageWorks Disk Array XP specific term)*

See ZDB to tape, ZDB to disk, and ZDB to disk+tape.

split mirror creation

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

split mirror restore

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

sqlhosts file

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

SRD file

(disaster recovery specific term) A text file in the Unicode (UTF-16) format, generated during CONFIGURATION backup of a Windows 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

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

sst.conf file

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

st.conf file

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

stackers

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

standalone file device

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

Storage Group

(Microsoft Exchange Server specific term) A collection of mailbox stores and public folder stores that share a set of transaction log files. Exchange Server manages each storage group with a separate server process.

StorageTek ACS library

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

storage volume

(ZDB specific term) A storage volume represents an object that may be presented to an operating system or some other entity (for example, a virtualization mechanism) upon which volume

management systems, file systems, or other objects may exist. The volume management systems, file systems are built on this storage. Typically, these can be created or exist within a storage system such as a disk array.

switchover

See failover.

Sybase Backup Server API

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

Sybase SQL Server

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

Symmetrix Agent (SYMA)

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

synthetic backup

A backup solution that produces a synthetic full backup, an equivalent to a conventional full backup in terms of data, without putting stress on the production servers or the network. A synthetic full backup is created from a previous full backup and any number of incremental backups.

synthetic full backup

The result of an object consolidation operation, where a restore chain of a backup objects is merged into a new, synthetic full version of this object. A synthetic full backup is equivalent to a conventional full backup in terms of restore speed.

System Backup to Tape

(Oracle specific term) An Oracle interface that handles the actions required to load, label, and unload correct backup devices when Oracle issues a backup or restore request.

system databases

(Sybase specific term) The four system databases on a newly installed Sybase SQL Server are the:

- master database (master)
- temporary database (tempdb)
- system procedure database (sybsystemprocs)
- model database (model).

System 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.

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

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

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

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

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

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

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

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

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

TLU Tape Library Unit.

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

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

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

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

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

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

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

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

transportable snapshot *(Microsoft VSS specific term)* A shadow copy that is created on the application system and can be presented to the backup system where a backup can be performed.
See also Microsoft Volume Shadow Copy Service (VSS).

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

UIProxy The Java GUI Server (`UIProxy` service) runs on the Data Protector Cell Manager. It is responsible for communication between the Java GUI Client and the Cell Manager, moreover, it performs business logic operations and sends only important information to the client. The service is started as soon as Data Protector is installed on the Cell Manager.

unattended operation *See* lights-out operation.

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

User Account Control (UAC) A security component in Windows Vista and Windows Server 2008 that limits application software to standard user privileges until an administrator authorizes an increase in privilege level.

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

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

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

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

vaulting media The process of storing media to a safe and remote place. The media are brought back to the data center when they are needed for restore or are ready for reuse in subsequent backups. The vaulting procedure depends on your company's backup strategy and policies for data protection/reliability.

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

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

Virtual Device Interface

(Microsoft SQL Server specific term) This is a SQL Server programming interface that allows fast backup and restore of large databases.

virtual disk

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

virtual full backup

An efficient type of synthetic backup where data is consolidated using pointers instead of being copied. It is performed if all the backups (the full backup, incremental backups, and the resulting virtual full backup) are written to a single file library that uses distributed file medium format.

Virtual Library System (VLS)

A disk-based data storage device hosting one or more virtual tape libraries (VTLs).

virtual server

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

virtual tape

(VLS specific term) An archival storage technology that backs up data to disk drives in the same way as if it were being stored on tape. Benefits of virtual tape systems include improved backup and recovery speed and lower operating costs.
See also Virtual Library System (VLS) and Virtual Tape Library.

Virtual Tape Library (VTL)

(VLS specific term) An emulated tape library that provides the functionality of traditional tape-based storage.
See also Virtual Library System (VLS).

VMware management client

(VMware integration specific term) The client that Data Protector uses to communicate with VMware Virtual Infrastructure. This can be a VirtualCenter Server system (VirtualCenter environment) or an ESX Server system (standalone ESX Server environment).

volser

(ADIC and STK specific term) A VOLume SERial number is a label on the medium to identify the physical tape used in very

large libraries. A volser is a naming convention specific to ADIC/GRAU and StorageTek devices.

volume group
A unit of data storage in an LVM system. A volume group can consist of one or more physical volumes. There can be more than one volume group on the system.

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

Volume Shadow Copy Service
See Microsoft Volume Shadow Copy Service.

VSS
See Microsoft Volume Shadow Copy Service.

VSS compliant mode
(HP StorageWorks Disk Array XP VSS provider specific term) One of two XP VSS hardware provider operation modes. When the XP provider is in the VSS compliant mode, the source volume (P-VOL) and its replica (S-VOL) are in simplex, unpaired state after a backup. Therefore the number of replicas (S-VOLs per a P-VOL) rotated is not limited. Restore from a backup in such a configuration is possible only by switching of the disks.
See also resync mode, source volume, primary volume (P-VOL), replica, secondary volume (S-VOL), and replica set rotation.

VxFS
Veritas Journal Filesystem.

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

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

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

wildcard character
A keyboard character that can be used to represent one or many characters. The asterisk (*), for example, typically represents

one or more characters, and the question mark (?) typically represents a single character. Wildcard characters are often used in operating systems as a means of specifying more than one file by name.

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

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

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

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

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

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

ZDB
See zero downtime backup (ZDB).

ZDB database
(ZDB specific term) A part of the IDB, storing ZDB related information such as source volumes, replicas and security

information. The ZDB database is used for ZDB, instant recovery, and split mirror restore.
See also zero downtime backup (ZDB).

ZDB to disk

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

ZDB to disk+tape

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

ZDB to tape

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

zero downtime backup (ZDB)

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

Index

A

advantages
  VSS integration, 156

architecture
  MS Exchange Server integration, 99
  MS Exchange Single Mailbox integration, 124
  MS SPS integration, 70
  MS SQL Server integration, 29
  VSS integration, 155, 158

audience, 15

B

backing up MS SPS
  previewing backups, 82
  starting backups, 83

backing up MS SQL Server
  backup specifications, creating, 39
  concepts, parallelism, 29

backing up MS Exchange Server
  backup options, 107

backing up MS SQL Server
  backup options, 42
  scheduling backups, 45

backing up Informix
  full backups, 27, 97
  incremental backups, 27, 97

backing up MS Exchange Server
  backup specifications, creating, 102

backing up MS Exchange Single Mailbox, 128
  backup options, 132
  backup types, 123
  backup specifications, creating, 128
  backup specifications, modifying, 132
  full backups, 123
  incremental backups, 123
  performance tuning, 145
  previewing backups, 133
  scheduling backups, 132
  scheduling backups, example, 132
  starting backups, 134
  starting backups, example, 135

backing up MS SPS, 77 - 84
  backup options, 81
  backup specifications, creating, 78
  backup types, 78
  backup flow, 73
  backup specification, modifying, 81
  differential backups, 78
  full backups, 78
  scheduling backups, 81
  scheduling backups, example, 81
  transaction logs backups, 78

backing up MS SQL Server, 39, 46

backing up VSS, 170 - 186
  architecture, 155, 158
  backup flow, 156
  backup specifications, creating, 170
  scheduling backups, 184
  starting backups, 185

backup
  problems, 206
  scheduling, 184
  troubleshooting, 206
backup options
  MS SPS integration, 81
backup specifications, scheduling
  MS SPS integration, 81
  VSS integration, 184
backup flow
  VSS integration, 156
  MS SPS integration, 73
backup objects, 172
backup options
  MS Exchange Server integration, 107
  MS SQL Server integration, 42
  MS Exchange Single Mailbox integration, 132
backup specifications, creating
  VSS integration, 170
backup specifications, creating
  MS Exchange Server integration, 102
  MS Exchange Single Mailbox integration, 128
  MS SPS integration, 78
  MS SQL Server integration, 39
backup specifications, modifying
  MS Exchange Single Mailbox integration, 132
  MS SPS integration, 81
backup specifications, scheduling
  MS Exchange Single Mailbox integration, 132
  MS SQL Server integration, 45
backup types
  MS Exchange Single Mailbox integration, 123
  MS SPS integration, 78

C
checking configuration
  MS Exchange Single Mailbox integration, 127
  MS SPS integration, 77
  MS SQL Server integration, 37
checks and verifications, 206
cluster continuous replication, 161
concepts
  MS Exchange Server integration, 99
  MS SPS integration, 70
  MS Exchange Server integration, 98
  MS Exchange Single Mailbox integration, 124
  MS SQL Server integration, 28, 30
  VSS integration, 156
  VSS, Microsoft Exchange Server 2007 writer, 161
  VSS, Microsoft Hyper–V writer, 162
  VSS, Microsoft SharePoint Services writer, 162
configuration files
  MS SQL Server integration, 31
configuring
  Microsoft Exchange Server writer, 165
  VSS integration, 164
configuring MS SQL Server
  checking configuration, 37
configuring MS Exchange Server, 99 - 101
configuring MS Exchange Single Mailbox, 125 - 128
  checking configuration, 127
configuring MS SPS, 73 - 77
  checking configuration, 77
configuring MS SQL Server, 30, 39
  configuration files, 31
configuring VSS, 164
conventions
  document, 23

creating backup specifications
  MS Exchange Server integration, 102
  MS Exchange Single Mailbox integration, 128
  MS SPS integration, 78
  MS SQL Server integration, 39
  VSS integration, 170

D

differential backups
  MS SPS integration, 78
disaster recovery
  MS SQL Server integration, 55
document
  conventions, 23
  related documentation, 15
documentation
  HP website, 15
  providing feedback, 26

E

examples, MS Exchange Server integration
  restoring using CLI, 117
examples, MS Exchange Single Mailbox integration
  restoring, 144
  scheduling backups, 132
  starting backups, 135
examples, MS SPS integration
  scheduling backups, 81
  starting interactive backups, 84
examples, MS SQL Server integration
  restoring using CLI, 55
Exchange Replication Service, 177

F

full backups
  Informix integration, 27, 97
  MS Exchange Single Mailbox integration, 123
  MS SPS integration, 78

H

help
  obtaining, 25
HP
  technical support, 25

I

incremental backups
  Informix integration, 27, 97
  MS Exchange Single Mailbox integration, 123
Informix backup
  incremental backups, 27, 97
Informix backup
  full backups, 27, 97
instant recovery
  problems, 208
  troubleshooting, 208
integrated authentication, MS SQL Server integration, 35
interactive backups
  MS Exchange Single Mailbox integration, 134
  MS SPS integration, 83
  VSS integration, 185
introduction
  MS SQL Server integration, 27
  MS Exchange Server integration, 97
  MS SPS integration, 69
  MS Exchange Single Mailbox integration, 123
  VSS integration, 153

L

limitations
  VSS integration, 164
local continuous replication, 161

M

Microsoft Exchange Server
  configuring writer, 165
  storage groups, 177
  writer backup specifics, 175
Microsoft Exchange Server 2007
  writer backup specifics, 177
modifying backup specifications
  MS Exchange Single Mailbox integration, 132
  MS SPS integration, 81
monitoring sessions
  MS Exchange Single Mailbox integration, 145
  MS SPS integration, 93
  MS SQL Server integration, 62
  VSS integration, 203
MS Exchange Server backup
  backup specifications, creating, 102
MS Exchange Single Mailbox backup
  backup options, 132
  backup types, 123
  incremental backups, 123
  starting backups, 134
MS SPS backup
  backup types, 78
  scheduling backups, 81
  transaction logs backups, 78
MS SPS configuration, 73 - 77
MS SPS integration
  concepts, 70
  introduction, 69
  monitoring sessions, 93
MS SPS troubleshooting, 93 - 96
MS Exchange Server integration
  restore, 109 - 117
MS Exchange Server backup
  backup options, 107
MS Exchange Server configuration, 99 - 101
MS Exchange Server integration
  architecture, 99
  concepts, 98
  configuration, 99 - 101
  introduction, 97
  troubleshooting, 117 - 121
MS Exchange Server restore, 109
  restore options, 114
  using CLI, 116
  using GUI, 110
MS Exchange Server troubleshooting, 117 - 121
MS Exchange Single Mailbox backup
  full backups, 123
MS Exchange Single Mailbox backup, 128
  backup specifications, creating, 128
  backup specifications, modifying, 132
  performance tuning, 145
  previewing backups, 133
  scheduling backups, 132
  scheduling backups, example, 132
  starting backups, example, 135
MS Exchange Single Mailbox configuration, 125 - 128
  checking configuration, 127
MS Exchange Single Mailbox integration
  architecture, 124
  backup, 128 - 135
  concepts, 124
  configuration, 125 - 128
  introduction, 123
  monitoring sessions, 145
  restore, 135 - 145
  troubleshooting, 147 - 151 - 151

MS Exchange Single Mailbox restore, 135 - 145
examples, 144
restore options, 142
using CLI, 142
using GUI, 135
MS Exchange Single Mailbox troubleshooting, 147
MS SPS restore
using CLI, 90
using GUI, 85
MS SPS backup, 77 - 84
backup specification, modifying, 81
backup flow, 73
backup options, 81
backup specifications, creating, 78
differential backups, 78
full backups, 78
previewing backups, 82
scheduling backups, example, 81
starting backups, 83
MS SPS configuration
checking configuration, 77
MS SPS integration
architecture, 70
backup, 77 - 84
configuration, 73 - 77
restore, 85 - 92
troubleshooting, 93 - 96
MS SPS restore, 85 - 92
restore flow, 73
restore options, 90
specifying restore destination, 87
using another device, 92
MS SQL Server backup, 39
MS SQL Server backup, 46
backup options, 42
backup specifications, creating, 39
concepts, parallelism, 29
scheduling backups, 45
MS SQL Server configuration, 30, 39
checking configuration, 37
configuration files, 31
MS SQL Server integration
architecture, 29
backup, 39, 46
concepts, 28, 30
configuration, 30, 39
disaster recovery, 55
introduction, 27
monitoring sessions, 62
performance tuning, 58
restore, 46, 57
troubleshooting, 63, 68
MS SQL Server restore, 46, 57
disaster recovery, 55
restore options, 51
using CLI, 54
MS SQL Server troubleshooting, 63, 68

O

offline backup, Hyper-V writer , 181
online backup, Hyper-V writer , 181
online backups
MS SPS integration, 69

P

performance tuning
MS Exchange Single Mailbox integration, 145
performance tuning
MS SQL Server integration, 58
prerequisites
VSS integration, 164
previewing backups
MS Exchange Single Mailbox integration, 133
previewing backups
MS SPS integration, 82
problems, 205 - 209
backup, 206
instant recovery, 208
restore, 208

R

related documentation, 15
restore, 186
  problems, 208
  troubleshooting, 208
restore flow
  VSS integration, 158
  MS SPS integration, 73
restore options
  MS Exchange Server integration, 114
  Informix integration, 53
  MS SQL Server integration, 51
  MS Exchange Single Mailbox integration, 142
  MS SPS integration, 90
  VSS integration, 191
restoring MS Exchange Server, 109 - 117
restoring MS SPS
  restore flow, 73
  restore options, 90
  using another device, 92
restoring VSS
  using GUI, 186
restoring MS SQL Server, 46, 57
  using CLI, 54
restoring Informix
  restore options, 53
restoring MS Exchange Server
  restore options, 114
  using CLI, 116
  using GUI, 110
restoring MS Exchange Single Mailbox, 135
  examples, 144
  restore options, 142
  using CLI, 142
  using GUI, 135
restoring MS SPS, 85 - 92
  specifying restore destination, 87
  using CLI, 90
  using GUI, 85
restoring MS SQL Server
  disaster recovery, 55
  restore options, 51
restoring VSS, 186
  restore options, 191
  restore flow, 158
running backups
  See starting backups

S

scheduling backups
  MS Exchange Single Mailbox integration, 132
scheduling backups
  MS SPS integration, 81
  MS SQL Server integration, 45
  VSS integration, 184
SQL Server authentication, MS SQL Server integration, 35
starting backups
  MS SPS integration, 83
  VSS integration, 185
starting backups
  MS Exchange Single Mailbox integration, 134
storage groups, 177
Subscriber's Choice, HP, 26

T

technical support
  HP, 25
technical support
  service locator website, 26
transaction logs backups
  MS SPS integration, 78
troubleshooting, 206
  backup, 206
  instant recovery, 208
troubleshooting MS SQL Server, 63, 68
troubleshooting MS Exchange Server, 117 - 121

troubleshooting MS Exchange Single Mailbox, 147 - 151
troubleshooting MS SPS, 93 - 96
troubleshooting VSS, 205 - 209

V

Volume Shadow Copy Service
  VSS integration, 153
Volume Shadow Copy Service
  VSS integration, 153
VSS
  Exchange Server 2007 writer concepts, 161
  Microsoft Hyper–V writer concepts, 162
  Microsoft SharePoint services writer concepts, 162
VSS backup
  backup specifications, creating, 170
  flow, 156
VSS integration
  backup, 170 - 186
  monitoring sessions, 203
  restore, 186
VSS restore
  restore options, 191
VSS troubleshooting, 205 - 209
VSS backup, 170 - 186
  architecture, 155, 158
  backup flow, 156
  backup specifications, 170
  scheduling, 184
  scheduling backups, 184
  starting backups, 185
VSS configuration, 164
VSS database, 159
VSS integration
  prerequisites, 164
  advantages, 156
  architecture, 155, 158
  concepts, 156
  configuration, 164
  configuring, 164
  introduction, 153
  limitations, 164
  troubleshooting, 205 - 209
VSS restore, 186
  restore flow, 158
  using GUI, 186

W

websites
  HP Subscriber's Choice for Business, 26
  HP , 26
  product manuals, 15
Windows authentication, MS SQL Server integration, 35
writer backup specifics
  Microsoft Exchange Server, 175
  Microsoft Exchange Server 2007, 177
writers specifics, VSS integration
  Microsoft Exchange Server, 175
writers specifics, VSS integration, 165 - 170
  Microsoft Exchange Server, 193
  Microsoft Exchange Server 2007, 195
  Microsoft Hyper-V writer, 181, 201
  MS Data Protection Manager 2006, 179, 198
  MS SharePoint Services, 183, 202
  MSDE, 191