

HP Data Protector

Software Version: 8.10

Granular Recovery Extension User Guide for Microsoft SharePoint Server

Document Release Date: November 2016

Software Release Date: November 2016



Legal Notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notice

© Copyright 2016 Hewlett-Packard Development Company, L.P.

Trademark Notices

Adobe® is a trademark of Adobe Systems Incorporated.

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

UNIX® is a registered trademark of The Open Group.

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates or to verify that you are using the most recent edition of a document, go to: <http://h20230.www2.hp.com/selfsolve/manuals>

This site requires that you register for an HP Passport and sign in. To register for an HP Passport ID, go to: <http://h20229.www2.hp.com/passport-registration.html>

Or click the **New users - please register** link on the HP Passport login page.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details.

Support

Visit the HP Software Support Online web site at: <http://www.hp.com/go/hpsoftwaresupport>

This web site provides contact information and details about the products, services, and support that HP Software offers.

HP Software online support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support web site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract. To register for an HP Passport ID, go to:

<http://h20229.www2.hp.com/passport-registration.html>

To find more information about access levels, go to:

http://h20230.www2.hp.com/new_access_levels.jsp

HP Software Solutions Now accesses the HPSW Solution and Integration Portal Web site. This site enables you to explore HP Product Solutions to meet your business needs, includes a full list of Integrations between HP Products, as well as a listing of ITIL Processes. The URL for this Web site is <http://h20230.www2.hp.com/sc/solutions/index.jsp>

Contents

Contents	3
Chapter 1: Introduction	7
Backup	7
Recovery	7
Chapter 2: Installation	9
Prerequisites	9
Procedure	10
Chapter 3: Configuration	13
Verifying the configuration of the Recovery Web Application	13
Procedure	13
Configuring HP Data Protector user rights	13
Procedure	13
Configuring Data Protector backup specifications	14
Verifying the configuration of Internet Information Services application pools	15
Chapter 4: Backup	17
Considerations	17
Chapter 5: Recovery	19
Launching the HP Data Protector Granular Recovery Extension GUI	19
Procedure	19
Importing content databases from backup	22
Prerequisites	22
Considerations	22
Procedure	23
Importing content databases from the filesystem	25
Prerequisites	25
Considerations	25
Procedure	25
Executing Perform content recovery tasks	27
Prerequisites	28

Procedure	28
Recovering site items	28
Prerequisites	29
Supported items	29
Considerations	30
Procedure	31
Removing content databases from the cache	37
Procedure	37
Monitoring granular recovery import jobs	38
Procedure	38
Changing HP Data Protector Granular Recovery Extension settings	39
Procedure	40
Chapter 6: Command line reference	41
Examples	41
Restoring a content database from Data Protector backup	41
Monitoring jobs progress	42
Verifying target location disk space size	43
Listing content databases	43
Removing restore jobs	43
Recovering a site item to the original site	44
Recovering a site item to another location	44
Removing content databases from the cache	44
Removing content databases from disk	45
Setting content database automatic removal	45
Exporting items from a content database	45
Listing exported items	46
Importing items from a content database	46
Displaying Microsoft SharePoint farm information	46
Displaying content database information	46
Displaying a list of sites	47
Browsing sites	47
Displaying Granular Recovery Extension version	47

Displaying Granular Recovery product key	47
Chapter 7: Troubleshooting	49
Installation reports a warning "No full read permissions"	49
Remote installation fails	50
An import job fails	50
An import job fails	51
Recovery session fails	53
Restore from backup data created with the Data Protector Microsoft SharePoint Server 2007/2010 integration (VDI based integration) fails	53
Granular Recovery Cache Management link is not accessible from My Sites	54
Granular Recovery Cache Management link is not accessible from My Sites	55
HP Data Protector Granular Recovery Extension is not available on a newly created Web Application	57
Import from backup or from filesystem fails	57
Changing default recovery settings fails	57
Slow response of the command line interface	58
Slow response of the graphical user interface	58
The Data Protector service is not running	59
The restoring - Mount Request Pending status	60
Subfolders are not recovered to original location	60
Granular Recovery Extension upgrade fails	60
Granular Recovery Extension component installation fails	61
Granular Recovery Extension removal fails	61
Installation ends unexpectedly on a farm with multiple servers on Central Administration	62
Glossary	63
Index	104
We appreciate your feedback!	107

Chapter 1: Introduction

This guide describes Data Protector Granular Recovery Extension for Microsoft Office SharePoint Server 2007, Microsoft SharePoint Server 2010, and Microsoft SharePoint Server 2013 (**Microsoft SharePoint Server**).

A part of the information provided in this document is also available in a custom Help collection that the HP Data Protector Granular Recovery Extension for Microsoft SharePoint Server adds to the basic Microsoft SharePoint Server Help. The collection contains Granular Recovery Extension-related topics. You can access them by clicking the Help icon in a Granular Recovery Extension context of the Central Administration site.

Backup

Back up Microsoft SharePoint Server data using one of the following backup solutions:

- HP Data Protector Microsoft SharePoint Server 2007/2010/2013 integration
- HP Data Protector Microsoft SharePoint Server VSS based solution
- HP Data Protector Microsoft SQL Server integration
- HP Data Protector Microsoft Volume Shadow Copy Service integration

Recovery

The benefits of the HP Data Protector Granular Recovery Extension are the following:

- **recovery granularity**

The smallest object that you can restore with the backup solution is a Microsoft SQL Server database (**content database**), which may contain data of multiple websites. In contrast, the smallest object that you can recover with HP Data Protector Granular Recovery Extension is an individual website item, for example: a Calendar item, a Calendar, a Tasks item, a Team Discussion item, a document, a shared document, a folder, a list, a library, an announcement, a form, a reporting template, an object's metadata, and a document workflow.

- **integration into Microsoft SharePoint Server Central Administration**

Granular Recovery Extension is fully integrated into the Microsoft SharePoint Server Central Administration. This empowers Site Collection Administrators to perform recovery of single items independently or with minimal interference of backup administrators.

- **recovery of multiple sites**

Accidental deletion of a site is no longer an issue, even if you cannot use the recycle bin to recover your site. Granular Recovery Extension can recover an entire site with multiple subsites.

- **ease to search**

The Granular Recovery Extension advanced and quick search helps you find the item you need to recover. This search system checks object's metadata, enabling you to filter your search by document type, author, date and so on. Objects are displayed in object tree browser.

- **recovery to different locations**

The Granular Recovery Extension enables recovery to different destinations, for example you can recover your objects to different sites, different farms, and to filesystem.

Chapter 2: Installation

This chapter describes how to install Data Protector Granular Recovery Extension for Microsoft SharePoint Server.

Prerequisites

- **Microsoft packages:**

Install the following Windows Management Framework Core package:

- Microsoft PowerShell 2.0 or higher

- **Microsoft SQL Server packages:**

Install the following packages for Microsoft SQL Server 2005 or Microsoft SQL Server 2008:

- Microsoft SQL Server Native Client
- Microsoft Core XML Services (MSXML) 6.0
- Microsoft SQL Server 2008 Management Objects Collection

Install the following packages for Microsoft SQL Server 2012:

- Microsoft SQL Server Native Client
- Microsoft Core XML Services (MSXML) 6.0 or higher
- Microsoft SQL Server 2012 Management Objects Collection

These packages must be installed on all the Microsoft SharePoint Server systems that have at least one of the following services enabled:

- Central Administration
- Windows SharePoint Services Web Application (Microsoft Office SharePoint Server 2007)
- Microsoft SharePoint Foundation Web application (Microsoft SharePoint Server 2010/2013)

You can download the packages from the website:

<http://www.microsoft.com/downloads/en/default.aspx>.

Search for **Feature Pack for Microsoft SQL Server 2008** or **Feature Pack for Microsoft SQL Server 2012**.

- **Data Protector components:**

Ensure you installed and configured your Data Protector backup solution as described in:

- *HP Data Protector Installation and Licensing Guide*
- applicable chapters of the *HP Data Protector Integration Guide for Microsoft Applications: SQL Server, SharePoint Server, and Exchange Server*
- *HP Data Protector Zero Downtime Backup Integration Guide*
- *HP Data Protector Integration Guide for Microsoft Volume Shadow Copy Service*

In addition, ensure that the Data Protector User Interface component is installed on all Microsoft SharePoint Server systems that have at least one of the following services enabled:

- Central Administration
- Windows SharePoint Services Web Application (Microsoft Office SharePoint Server 2007)
- Microsoft SharePoint Foundation Web application (Microsoft SharePoint Server 2010/2013)

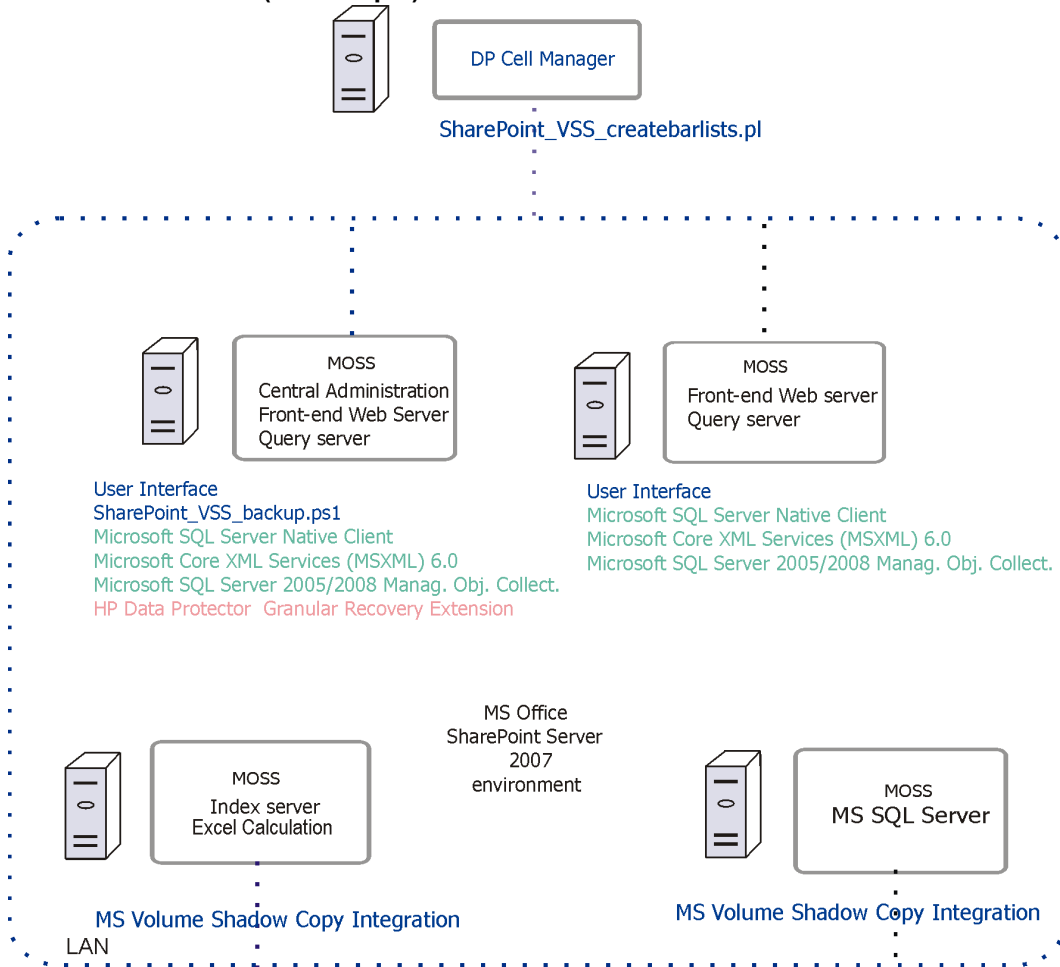
Procedure

For the installation procedure for Granular Recovery Extension for Microsoft SharePoint Server, see the Installing the Integration Clients chapter in *HP Data Protector Installation and Licensing Guide*.

Example

In the "Installing a medium farm that uses the HP Data Protector Microsoft SharePoint Server VSS based solution (an example)" on the next page, the HP Data Protector components are colored blue, the Microsoft SQL Server install packages are green, and the HP Data Protector Granular Recovery Extension component red.

Figure 1: Installing a medium farm that uses the HP Data Protector Microsoft SharePoint Server VSS based solution (an example)



Chapter 3: Configuration

This section describes the configuration steps that you need to follow. Not following these steps may lead to failure in recovering your objects.

Verifying the configuration of the Recovery Web Application

Procedure

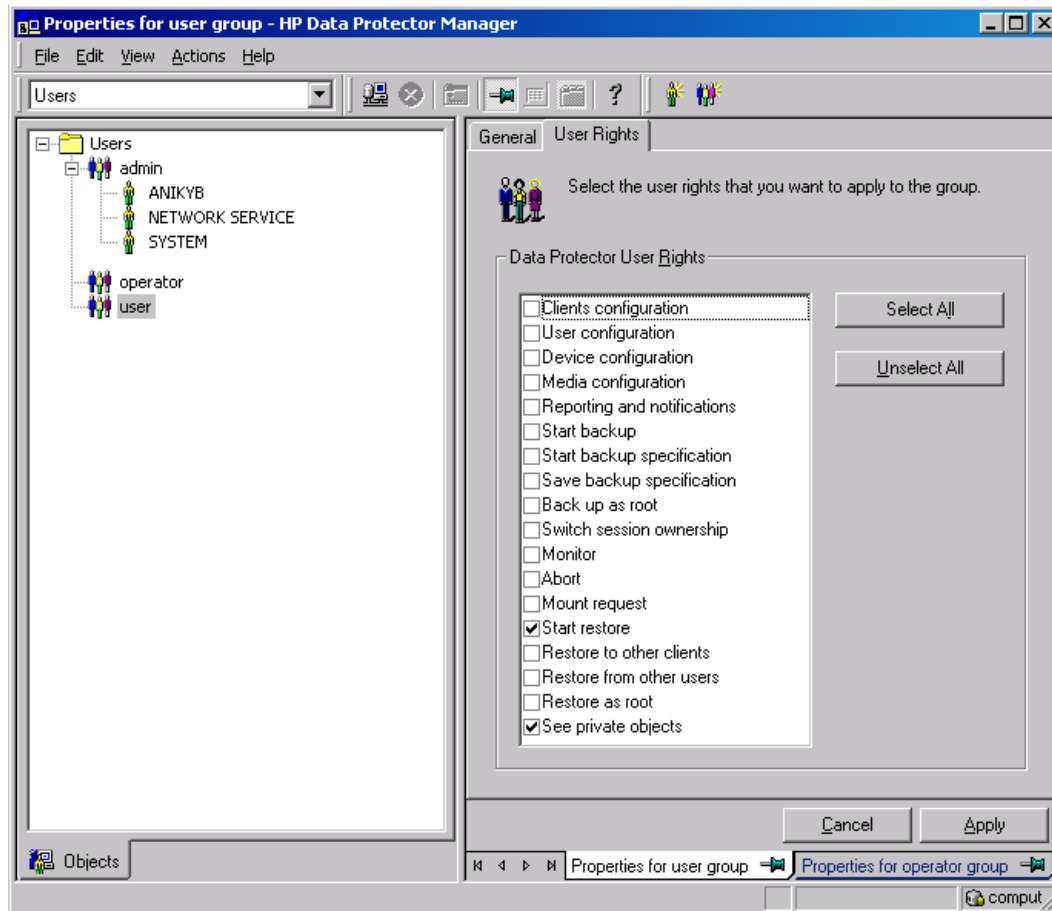
1. Open the Central Administration webpage and click the **Application Management** tab.
2. Under Application Security, click **Authentication providers** and click **Default**.
3. Ensure that the settings for the Recovery Web Application are the same as the default settings of the Central Administration Application.

Configuring HP Data Protector user rights

Procedure

1. Launch the Data Protector GUI (**Data Protector Manager**).
2. In the Context list, select **Users**.
3. Ensure the user account under which the Windows SharePoint Services Timer service is running is assigned the Data Protector `Start` `restore` and `See private objects` user rights.

Figure 2: Data Protector user rights



Note: The See private objects user right is useful in case you created your backup specification configured with access type private, and backup object owner. This is either the account under which the backup was executed or the account specified in the **Ownership** backup option. If this user account is different than the user account under which the Windows SharePoint Services Timer service is running, the private backup objects are not accessible in the Recovery Cache Management.

Configuring Data Protector backup specifications

- Ensure the option **track the replica for instant recovery** is not selected, when you create VSS transportable backup.
- To prevent Data Protector from backing up content databases that are in the Granular Recovery Cache Management (in other words, to prevent Data Protector from backing up the same content

databases twice), proceed with the following, depending on your configuration:

- If the same Microsoft SQL Server instance is used by both Microsoft SharePoint Server and HP Data Protector Granular Recovery Extension:

When you create backup specifications, select individual content databases, and not the client, Microsoft SQL Server instance, or Microsoft Volume Shadow Copy Writer.

The content databases restored by HP Data Protector Granular Recovery are named *OriginalName_DataProtectorSessionID*.

See " [Selecting content databases](#) " below.

Figure 3: Selecting content databases

The screenshot shows the HP Data Protector Granular Recovery Cache Management interface. The top navigation bar includes 'Site Actions', 'Granular Recovery Cache Management', 'Give Feedback', and 'User'. Below this is a toolbar with icons for 'Import from Backup', 'Import from Filesystem', 'Import Jobs Status', 'Remove Content Database', 'Start Recovery', and 'Help'. The main content area is divided into two sections: 'Content Databases' and 'Sites'.

Content Database	Backup Version	Content Database Size	Added	Expires On	Added By
WSS_Content	2010/09/16-2	49.0 MB	9/16/2010 3:42:13 PM	10/7/2010 3:42:13 PM	user

Original Site URL	Recovery Site URL
http://apno/	http://apno:38000/1
http://apno/sites/	http://apno:38000/sites/

Note: If you have a backup specification with individual content databases selected, each time a Farm Administrator adds a new content database, you need to include the newly-added content database in the backup specification.

- If a separate Microsoft SQL Server instance is used for granular recovery purposes, specify this system as the destination Microsoft SQL Server for the Import From Backup procedure.

Ensure that this system is excluded from the backup specification.

Verifying the configuration of Internet Information Services application pools

The same Microsoft SharePoint Server user account is used by both the **Recovery Web Application** and **SharePoint Central Administration v3/v4** application pools.

To be able to recover items to a filesystem, verify if the user specified in these application pools is granted enough permission. Ensure this user is granted full control of the filesystem.

To verify which user account is configured in the **Recovery Web Application** or **SharePoint Central Administration** (v3 for Microsoft Office SharePoint Server 2007 or v4 for Microsoft SharePoint Server 2010/2013) application pools:

1. Connect to the Microsoft SharePoint Server Central Administration system.
2. In the Start menu, click **Control Panel**, **Administrative Tools**, and **Internet Information Services (IIS) Manager**.
3. Depending on the operating system version, proceed as follows:

Windows Server 2008 or Windows Server 2012:

- a. Open the Application Pools page.
- b. Right-click an application pool and click **Advanced Settings**.
- c. Under Process Model, verify the Identity of the Microsoft SharePoint Server user account.

Windows Server 2003:

- a. Expand **Application Pools**.
- b. Right-click an application pool and click **Properties**.
- c. Click the **Identity** tab, select the **Configurable** option, and verify the selected Microsoft SharePoint Server user account.

Chapter 4: Backup

Back up Microsoft SharePoint Server data as described in your backup solution documentation.

For more information on the HP Data Protector backup solutions, see:

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

Note: Granular Recovery Extension for Microsoft SharePoint Server uses the same procedure for recovery of different objects. The recovery procedure does not depend on the backup type.

Considerations

- It is recommended to restore content databases bigger than 10 GB from VSS transportable backup.
- If you have configured VSS transportable backup using ZDB to disk+tape, Granular Recovery Extension for Microsoft SharePoint Server selects the content database version from disk for restore. This backup type does not require additional disk space and is adequate for bigger content databases, taking less time to complete the restore session.

Chapter 5: Recovery

Each site has its data stored in a Microsoft SQL Server database (**content database**). Therefore, to recover site items, follow this basic procedure:

1. **Import**

- a. **Restore**

Restore the content database from backup to a temporary location on a Microsoft SQL Server system.

- b. **Mount**

Present the restored content database (**recovery content database**) to the Microsoft SharePoint Server. This creates a temporary site (**recovery site**).

2. **Recover**

Transfer site items from the recovery site to the original site, or to another location of your choice.

3. **Dismount**

Dismount the recovery content database from the Microsoft SharePoint Server. Optionally, delete the database from the disk.

Launching the HP Data Protector Granular Recovery Extension GUI

Procedure

1. Log on to the Microsoft SharePoint Server Central Administration system under a Microsoft SharePoint Server **Farm Administrator** user account.
2. Connect to the Central Administration webpage.
3. A Microsoft Office SharePoint Server 2007 specific step: click the **Operations** tab.
4. Look for **HP Data Protector Granular Recovery Extension**:

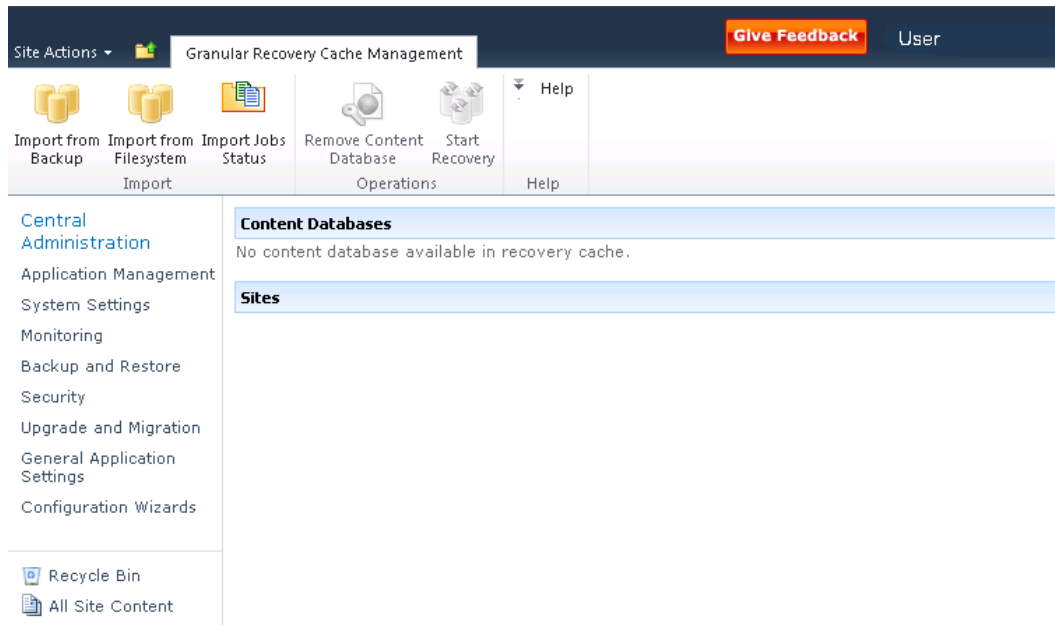
Figure 4: HP Data Protector Granular Recovery Extension links

[HP Data Protector Granular Recovery Extension](#)
[Granular Recovery Cache Management](#)
[Granular Recovery Import Job Status](#)
[Granular Recovery Settings](#)

5. Click **Granular Recovery Cache Management**. The Recovery Cache Management page is displayed.

The Granular Recovery Cache shows which recovery content databases are currently mounted to the Microsoft SharePoint Server. In the beginning, the Granular Recovery Cache is empty. See "[Recovery Cache Management \(empty\)](#)" below.

Figure 5: Recovery Cache Management (empty)



"[Recovery Cache Management with a content database mounted](#)" on the next page shows available functionality of the Recovery Cache Management when a content database is already mounted. For a high-level description of the functionality, see "[Granular Recovery Cache Management](#)" on the next page.

Figure 6: Recovery Cache Management with a content database mounted

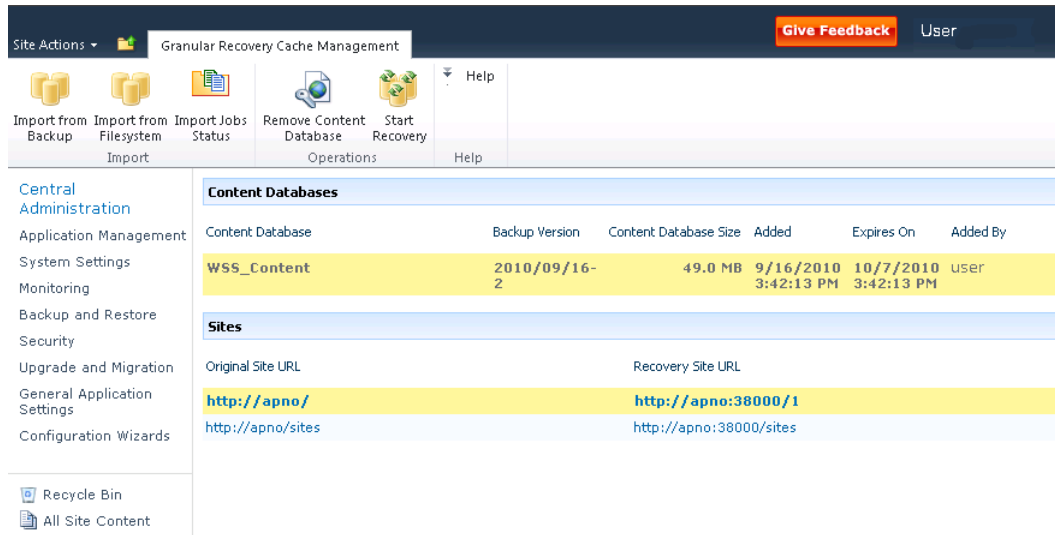


Table 1: Granular Recovery Cache Management

<p>■ Import From Backup</p> <p>After you have backed up your content database with an HP Data Protector backup solution, use Import From Backup to restore the database to a temporary location and to mount the database to the Microsoft SharePoint Server.</p> <p>For details, see "Importing content databases from backup" on the next page.</p>	<p>■ Import From Filesystem</p> <p>If you have restored the content database to the filesystem, use Import From Filesystem to mount the content database to the Microsoft SharePoint Server.</p> <p>For details, see "Importing content databases from the filesystem" on page 25.</p>
<p>■ Import Job Status</p> <p>This enables you to monitor import jobs (importing a content database from backup or from filesystem) status.</p> <p>For details, see "Monitoring granular recovery import jobs" on page 38.</p>	<p>■ Remove from Recovery Cache</p> <p>This dismounts a recovery content database from the Microsoft SharePoint Server (removes the content database from the Granular Recovery Cache) and removes the database files from the disk.</p> <p>For details, see "Removing content databases from the cache" on page 37.</p>

<p>■ Start Recovery</p> <p>Use this to browse and recover objects that are stored in a recovery content database.</p> <p>Note that this is also available for Site Collection Administrators from the original site:</p> <p>Microsoft SharePoint Server 2007/2010: Site Actions > Site Settings > Granular Recovery</p> <p>Microsoft SharePoint Server 2013: Settings icon > Site Settings > Granular Recovery</p> <p>For details, see "Executing Perform content recovery tasks" on page 27 and "Recovering site items" on page 28.</p>	<p>■ Original Site URL</p> <p>The link to the original site.</p> <p>■ Recovery Site URL</p> <p>The link to the recovery site.</p>
---	---

Importing content databases from backup

Prerequisites

On the destination Microsoft SQL Server system, you need enough disk space for the content database that you want to import.

Considerations

- If a site already exists in the Recovery Cache Management, and you perform an Import From Filesystem session for the same site, the URL changes as follows:
 - `http://computer.company.com:38000/OriginalNameSequenceNumber`
 - `http://computer.company.com:25884/SequenceNumber`
(root site)
- If the original site does not exist in the Recovery Cache Management, the site URL does not change.
- If a root site does not exist, the Recovery Cache Management uses an empty string during the restore session, and the URL of the root site changes to:
`http://computer.company.com:25884/SequenceNumber`

Procedure

1. In the Recovery Cache Management page, click **Import From Backup**. The Site Collection Selection page is displayed. Select the content database of the site you want to recover and click **Continue**.

Figure 7: Site Collection Selection page

← Back → Continue			
Site URL	Site Name	Content Database	Web Application Name
http://apno/		WSS_Content	SharePoint - 80
http://apno/	sites/user	WSS_Content	SharePoint - 80
http://apno:23902/		SharePoint_AdminContent_0a8c5c49-3c69-4838-aad0-760edd06b87e	
http://apno:23902/	sites/Help	SharePoint_AdminContent_0a8c5c49-3c69-4838-aad0-760edd06b87e	

2. In the Backup Version Selection page, select the content database version that you want to restore and click **Continue**.

Figure 8: Backup Version Selection page

← Back → Continue					
Name	Created Date	Size	Type	Method	Media
2010/04/13-2	4/13/2010 3:46:47 PM	31.5 MB	Full	MSVSS	TAPE

3. The Content Database Recovery page is displayed:

Figure 9: Content Database Recovery page

← Back ▶ Import content database	
Restore Settings	
SQL server:	<input type="text" value="APNO\SharePoint"/>
Restore path:	<input type="text" value="C:\Restore"/>

In the **SQL Server** drop-down list, select the destination Microsoft SQL Server instance. You can change the default restore location by specifying a new path. The default is C:\Restore.

Note: If your Microsoft SQL Server is configured in a cluster, ensure that the restore location resides on the Microsoft SQL Server cluster shared disk.

Click **Import content database**.

- Optionally, to monitor job status, click **Continue**. The Granular Recovery Import Job Status page is displayed:

Figure 10: Monitoring job status

Refresh
 Clear History
 Abort

Recovery Cache Management

Active

ID	Name	Started By	Started	Ended	Details
9528425a-7973-4110-9b84-d64ab0632416	gr-job-restore-recovery-database_WSS_Content_2010/04/13-2	user			None

History

No import of content databases to recovery cache performed.

- Click **Recovery Cache Management** to return to that page.

The content database is mounted to the Microsoft SharePoint Server.

Figure 11: Recovery Cache Management

Site Actions

Granular Recovery Cache Management

[Give Feedback](#)

User

Import from Backup

Import from Filesystem

Import Jobs Status

Remove Content Database

Start Recovery

Help

Import

Operations

Help

Central Administration

Application Management

System Settings

Monitoring

Backup and Restore

Security

Upgrade and Migration

General Application Settings

Configuration Wizards

Recycle Bin

All Site Content

Content Databases

Content Database	Backup Version	Content Database Size	Added	Expires On	Added By
WSS_Content	2010/09/16-2	49.0 MB	9/16/2010 3:42:13 PM	10/7/2010 3:42:13 PM	user

Sites

Original Site URL	Recovery Site URL
http://apno/	http://apno:38000/1
http://apno/sites	http://apno:38000/sites

Note: Once the content database is mounted to the Microsoft SharePoint Server, a **Perform content recovery** task is assigned to the Site Collection Administrator.

For details, see "[Executing Perform content recovery tasks](#)" on page 27.

Importing content databases from the filesystem

Prerequisites

- The content database must be restored to the filesystem.
- The user account under which the Windows SharePoint Services Timer (Microsoft Office SharePoint Server 2007), SharePoint 2010 Timer (Microsoft SharePoint Server 2010), or SharePoint Timer Service (Microsoft SharePoint Server 2013) service is running must be granted full control permission for the content database.

Considerations

- The Microsoft SQL Server Database Primary Data Files and all transaction log files cannot be imported from a network share.
- If a site already exists in the Recovery Cache Management, and you perform an Import From Filesystem session for the same site, the URL changes as follows:
 - `http://computer.company.com:38000/OriginalNameSequenceNumber`
 - `http://computer.company.com:25884/SequenceNumber`(root site)
- If the original site does not exist in the Recovery Cache Management, the site URL does not change.
- If a root site does not exist, the Recovery Cache Management uses an empty string during the restore session, the URL of the root site changes to:

`http://computer.company.com:25884/SequenceNumber`

Procedure

1. On the Recovery Cache Management page, click **Import From Filesystem**.
2. On the Enter content database data page, specify the location of the Microsoft SQL Server Database Primary Data File *AbsolutePath.mdf* and all transaction log files *AbsolutePath.ldf*. Click **Add**.

Click **Continue**.

Figure 12: Specifying content database files

Central Administration ▸ Enter content database data
Specify database files

← Back → Continue

Database File Location

Database file path: Add

Database Files

File path	
C:\Restore\2010-09-16-2\C\Program Files\Microsoft Office Servers\14.0\Data\MSSQL10.SHAREPOINT\MSSQL\DATA\WSS_Content.mdf	Remove
C:\Restore\2010-09-16-2\C\Program Files\Microsoft Office Servers\14.0\Data\MSSQL10.SHAREPOINT\MSSQL\DATA\WSS_Content_log.LDF	Remove

3. In the **SQL Server** drop-down list, select the destination Microsoft SQL Server instance.

Figure 13: Importing a content database from filesystem

Give Feedback User

Central Administration ▸ Import content database
Click **Import content database** to start import.

← Back → Import content database

Import Settings

SQL server:

Database name:

Version:

The content database name and version are filled in automatically. Optionally, you can edit the database name and version to better suit your needs.

Click **Import content database**.

4. Optionally, to monitor job status, click **Continue**.

The Granular Recovery Import Job Status page is displayed:

Figure 14: Monitoring job status

Refresh
 Clear History
 [Abort](#)
 Recovery Cache Management

Active

ID	Name	Started By	Started	Ended	Details
9528425a-7973-4110-9b84-d64ab0632416	gr-job-restore-recovery-database_WSS_Content_2010/04/13-2	user			None

History

No import of content databases to recovery cache performed.

- Click **Recovery Cache Management** to return to that page.

The content database is mounted to the Microsoft SharePoint Server.

Figure 15: Recovery Cache Management

Site Actions

Granular Recovery Cache Management
 [Give Feedback](#)
User

Import from Backup
 Import from Filesystem
 Import Jobs Status
 Remove Content Database
 Start Recovery
 Help

Import
 Operations
 Help

Central Administration

- Application Management
- System Settings
- Monitoring
- Backup and Restore
- Security
- Upgrade and Migration
- General Application Settings
- Configuration Wizards

Recycle Bin
 All Site Content

Content Databases

Content Database	Backup Version	Content Database Size	Added	Expires On	Added By
WSS_Content	2010/09/16-2	49.0 MB	9/16/2010 3:42:13 PM	10/7/2010 3:42:13 PM	user

Sites

Original Site URL	Recovery Site URL
http://apno/	http://apno:38000/1
http://apno/sites	http://apno:38000/sites

Note: Once the content database is mounted to the Microsoft SharePoint Server, a Perform content recovery task is assigned to the Site Collection Administrator.

For details, see "[Executing Perform content recovery tasks](#)" below.

Executing Perform content recovery tasks

Prerequisites

- The content database must be mounted to the Microsoft SharePoint Server, by "[Importing content databases from backup](#)" on page 22 or by "[Importing content databases from the filesystem](#)" on page 25.
- You must be a **Site Collection Administrator** of the site you want to recover. For more information on how to add a user to the Site Collection Administrator group, see the Microsoft SharePoint documentation.

Figure 16: Perform content recovery task

<div>Search</div>									
<input type="checkbox"/> Type	Title	Action	Associated Service	System Task	<input type="checkbox"/> Assigned To	Status	Order	Due Date	
	Perform content recovery 2010/09/17 -3 NEW	Perform granular recovery			User	Not Started	20	10/8/2010	

Figure 17: Perform content recovery link

Administrator Tasks - Perform content recovery 2010/04/13-2 □ ×

View

Manage Permissions Alert Me

Edit Item Delete Item

Manage

Actions

Predecessors	
Title	Perform content recovery 2010/04/13-2
Action	Perform granular recovery
Description	Perform granular recovery for site http://apno:23902
Order	20
Status	Not Started
Assigned To	User

Procedure

1. Click the link in the Perform content recovery task. The Browse and Select Objects page is displayed.
2. Proceed with the "[On the Browse and Select Objects page, select the site items that you want to recover.](#)" on page 32.

Recovering site items

Prerequisites

- On all the front-end Web Server systems, you need enough disk space for the site items that you plan to recover. The default location is C:\Recovery. To change the default path, see ["Changing HP Data Protector Granular Recovery Extension settings" on page 39](#).
- You must be a **Site Collection Administrator** of the site you want to recover. For more information on how to add a user to the Site Collection Administrator group, see the Microsoft SharePoint documentation.
- The recovery content database must be mounted to the Microsoft SharePoint Server.
- If the original site no longer exists, create a site collection without a template and with the same language as the original site. Use the **Overwrite Existing** recovery mode. You must be a **Farm Administrator** of the site you want to recover in the Recovery Cache Management. If you have a sub site in the recovered site, quick links, top navigation bar are relocated at the end of the lists.
- Ensure that the site URL length does not exceed 260 characters:

If you use the **Rename if Exists** recovery mode, the URL length should not exceed 255 characters.

Supported items

You can recover the following Microsoft SharePoint Server items with the HP Data Protector Granular Recovery Extension:

- Libraries:
 - Document library
 - Form library
 - Wiki page library
 - Report library
 - Asset library
 - Picture library
 - Translation Management Library
- Communication:
 - Announcements
 - Contacts

- Discussion board
- Tracking:
 - Links
 - Calendar
 - Tasks
 - Project tasks
 - Issue tracking
 - Survey
- Custom List
- User Information List
- Pages and Sites:
 - Page
 - Site
 - Publishing pages
 - Sites with a blog template: Posts, Comments, Categories
 - Sites with a meeting template: Meetings, Agenda, Attendees, Decision, Meeting Objective, Text Box, Things To Bring, Home Page Library

Considerations

- If the data to be recovered already exists at the destination, depending on the recovery mode, note the following:
 - **Rename if Exists** : Files and folders items are recovered with different names, *OriginalName_DPGRE_Timestamp*.

For example, suppose that on November 17, 2012 at 10:59:35 you start a recovery of the file `wizard.txt`. The file is recovered with the name `wizard_DPGRE_20121117-105935.txt`.

Other items (for example, form templates, documents and tasks items) are not recovered, and not renamed to the original location.

List items cannot be renamed as part of the recovery.
 - **Leave Existing** : Items are not recovered, the existing items remain the same in the target location.

- **Overwrite Existing** : Items are recovered with the original names, replacing the existing. For example, the existing Microsoft SharePoint Server items (Document Library) are overwritten with those from the backup data. Only lists and sites are not overwritten.
- If the data to be recovered does not exist at the destination, it is recovered with the original name.
- If the List items (Announcement, Contact, Link, Calendar, or Task) are recovered to other location, or to other farm twice, depending on the recovery mode:
 - **Overwrite Existing** : the List items are duplicated with the same names and different IDs. Delete the items with the same names.
 - **Rename if Exists** : the List items are renamed even though these kinds of items do not support renaming.
- If discussion items, with attachments and replies, or surveys with responses are recovered with the **Overwrite Existing** recovery mode, the items are overwritten but the attachments, replies, or responses are not recovered. To avoid data loss, delete the attachments, replies, or responses before starting your recovery session.
- Multiple recovery sessions can be performed in parallel, except if the same items are selected for recovery.
- Multiple farm administrators and site collection administrators can browse objects in parallel.
- To recover a document workflow status ensure you create a template and association at the destination site. Workflow status cannot be recovered to other farm.
 - Workflow history cannot be recovered.
- Unique user permissions of an item are not recovered. The recovered item inherits permissions of the destination container type where it is recovered to.

Procedure

1. On the Recovery Cache Management page, select the content database and the sites you want to recover. Note that a content database may contain data of multiple sites.

Tip: To recover items from multiple sites, hold **Ctrl** while selecting specific sites under Sites, and then click **Start Recovery**. You can also hold **Shift** while selecting a group of sites under Sites, and then click **Start Recovery**.

Figure 18: Selecting a content database and multiple sites for recovery

The screenshot shows the 'Granular Recovery Cache Management' interface. The top navigation bar includes 'Site Actions', 'Granular Recovery Cache Management', a 'Give Feedback' button, and a 'User' profile. Below this is a ribbon with tabs: 'Import from Backup', 'Import from Filesystem', 'Import Jobs Status', 'Remove Content Database', 'Start Recovery', and 'Help'. The left sidebar contains 'Central Administration' links: Application Management, System Settings, Monitoring, Backup and Restore, Security, Upgrade and Migration, General Application Settings, Configuration Wizards, Recycle Bin, and All Site Content. The main content area is divided into two sections: 'Content Databases' and 'Sites'.

Content Database	Backup Version	Content Database Size	Added	Expires On	Added By
WSS_Content	2010/09/16-2	49.0 MB	9/16/2010 3:42:13 PM	10/7/2010 3:42:13 PM	User

Original Site URL	Recovery Site URL
http://apno/	http://apno:38000/1
http://apno/sites/	http://apno:38000/sites/

Note: Alternatively, you can start a recovery session:

- By connecting to the original website.

Microsoft SharePoint Server 2007/2010: In the **Site Actions** menu, select **Site Settings**.

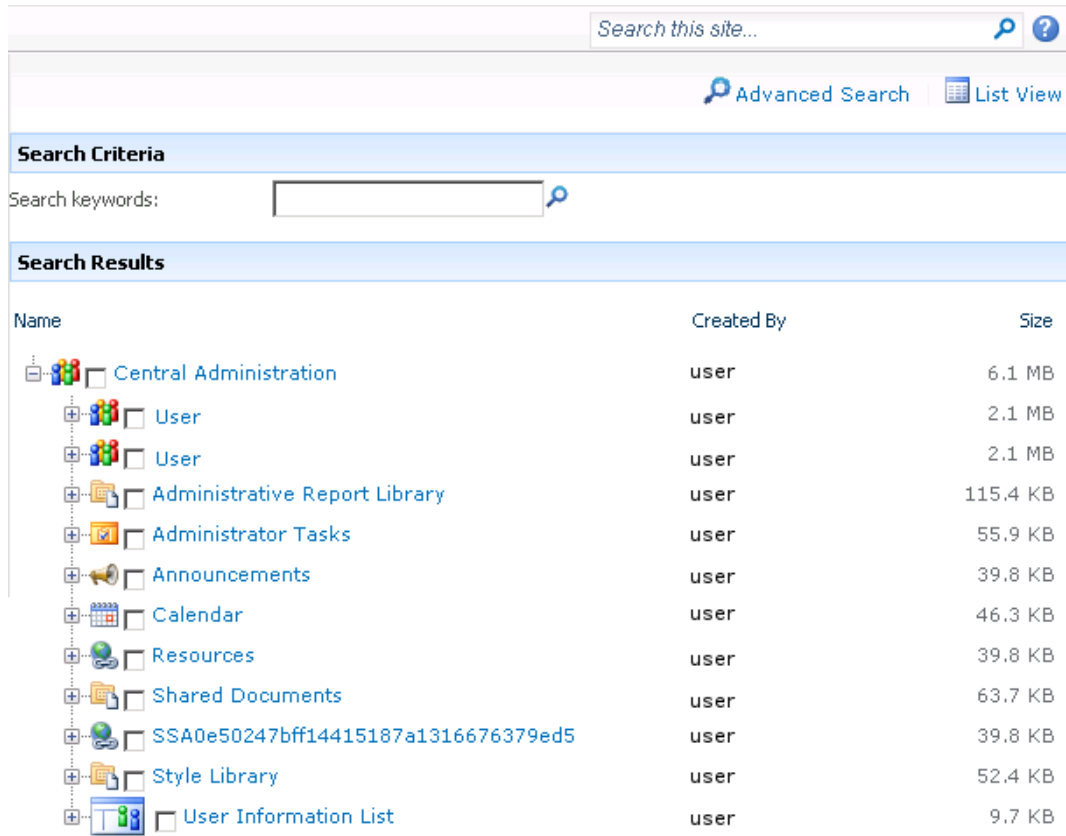
Microsoft SharePoint Server 2013: Click the **settings** icon and select **Site Settings**.

On the Site Settings page, look for HP Data Protector Granular Recovery Extension. Click **Granular Recovery**.

- By performing site tasks. For details, see "[Executing Perform content recovery tasks](#)" on [page 27](#).

2. On the Browse and Select Objects page, select the site items that you want to recover.

Figure 19: Selecting site items



Note: All items can be previewed by clicking on the item name.

Tip: To select multiple list view items, hold **Ctrl** while selecting specific items. Alternatively, you can hold **Shift** while selecting a group of items.

Figure 20: Advanced search

The screenshot shows the 'Advanced search' page in SharePoint Central Administration. The breadcrumb trail is 'Central Administration > Browse and Select Objects'. Below this is the instruction 'Select items for recovery.' and a search bar with the placeholder 'Search this site...'. A 'Continue' button is on the left, and 'Quick Search' and 'List View' links are on the right. The 'Search Criteria' section includes 'Find documents with...' with four input fields for 'All of these words:', 'The exact phrase:', 'Any of these words:', and 'None of these words:'. Below this is the 'Narrow the search...' section with a 'Result type' dropdown set to 'All Results'. The 'Add property restrictions...' section has a 'Where the Property...' dropdown set to '(Pick Property)', an 'Equals' dropdown, an empty text input, an 'And' dropdown, and an 'Add Property...' link. A 'Search' button is at the bottom.

Tip: You can filter the items using the **Advanced search**. For example, in **Result type**, select **Microsoft Office Word documents**. In **Add properties restriction**, select a property and click **Search**.

For details about the advanced and quick search, see the *Microsoft SharePoint Server Help*.

To select multiple list view items, hold **Ctrl** while selecting specific items. Alternatively, you can hold **Shift** while selecting a group of items.

Click **Continue**.

3. On the Recovery Objects page, the selected site items are displayed.

Note: The **Recovery mode** drop-down list offers the following options:

- **Rename if Exists** : Items such as files and folders are recovered with a new name *OriginalName_DPGRE_Timestamp*.
- **Leave Existing** : Items are not recovered, the existing items remain the same in the target location.
- **Overwrite Existing** : Recovered items replace the existing items.

Tip: When recovering recurring events, for example, weekly team meetings in Calendars, before selecting the **Overwrite Existing** recovery mode, ensure the deletion of all the recurring events.

Figure 21: Recovering site items

Central Administration ► Recovery Objects
Click **Start Recovery** to recover the selected items.

Search this site...

[Start Recovery](#) [Back](#)

Recovery Settings

Recovery Mode:

Temporary Path:

Items for Recovery

Status	Type	Name	Into	Created By	Size	Log
		Central Administration/Announcements	<input type="text" value="Original Location"/>	User	39.8 KB	
		Central Administration/Shared Documents	<input type="text" value="Original Location"/>	User	63.7 KB	

Status

The **Temporary Path** option specifies which location on your Microsoft SharePoint Server system to use for recovery.

Note: The **Into** drop-down list specifies the recovery destination:

- **Original Location** : The item is recovered to the original location in the original site. The option is not available for the recovery of sites or subsites with the **Rename If Exists**.
 - **Other Location** : The item is recovered to a different site or a different location in the original site. Use this location, if the original site no longer exists.
 - **Other Farm** : The item is recovered to a different destination farm.
 - **Filesystem** : The item is recovered to a directory in your filesystem. This option is available only for files and folders.
- If you select **Other Location**, the Recovery to other location dialog box is displayed.

Figure 22: Recovering site items to another location

Recovery to other location

Destination Site
Select destination site for recovery

Sites

☐ Apply to all items of the same type

In the Site drop-down list, select the destination site.

If you select the **Apply to all items of the same type** option, items of the same type (for example, calendar items) are recovered to the same location.

Click **OK**.

Tip: The sites listed in the Recovery to other location dialog box are those for which you have enough permission. For example, if you are a Site Collection Administrator, you need to be granted the read configuration database right.

- If you select **Other Farm**, the Recovery to other farm dialog box is displayed.

Figure 23: Recovering site items to another farm

Recovery to other farm

Connection Data
Enter connection data.

Site URL:

Domain:

Username:

Password:

☐ Apply to all items of the same type

Specify the destination farm and which Windows domain user account to use.

If you select the **Apply to all items of the same type** option, items of the same type (for example, calendar items) are recovered to the same farm.

Click **Connect**.

- If you select **Filesystem**, the Recovery to Filesystem dialog box is displayed.

Figure 24: Recovering site items to a network share

Recovery to Filesystem

Destination folder
Please enter destination folder.

☐ Apply to all items of the same type

In **Path**, specify the destination directory.

When specifying a network share as a destination, ensure that:

- Read, write, and change permissions are granted to the user that starts the recovery session.
- All necessary permissions are granted to the network share. Grant the same permissions specified for the user account configured in the **Web Recovery Application** and **SharePoint Central Administration v3/v4** application pools. For details, see ["Verifying the configuration of Internet Information Services application pools" on page 15](#).
- The share is accessible from the system where the Windows SharePoint Services Web Application (Microsoft Office SharePoint Server 2007) or Microsoft SharePoint Foundation Web Application (Microsoft SharePoint Server 2010/2013) is running, in which the recovery session was started.

When specifying a folder as a destination, ensure that:

- The folder is accessible from the system where the Windows SharePoint Services Web Application (Microsoft Office SharePoint Server 2007) or Microsoft SharePoint Foundation Web Application (Microsoft SharePoint Server 2010/2013) is running.
- Read, write, and change permissions are granted to the user that starts a recovery session.

If you select the **Apply to all files and folders** option, all files and folders are recovered to the same directory.

Click **OK**.

4. Click **Start Recovery**.

Once the recovery completes, you can find the recovered items at the specified destination.

Removing content databases from the cache

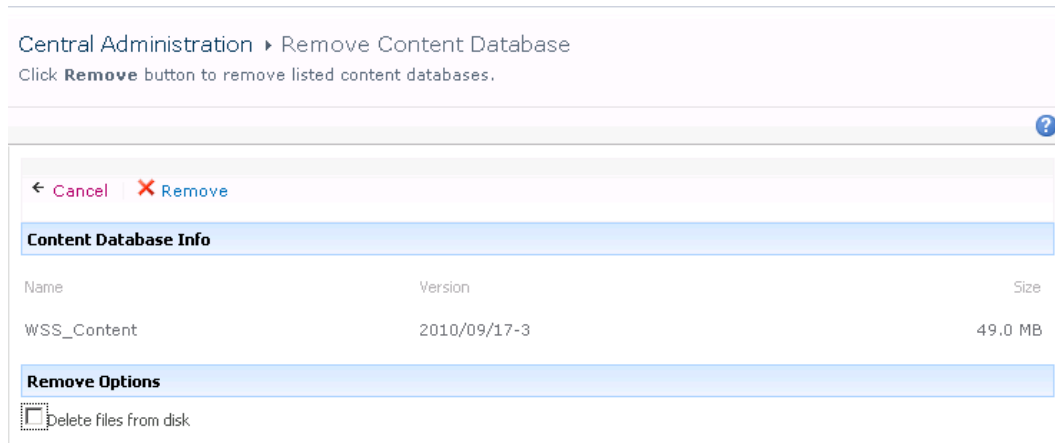
Procedure

Content databases are available for three weeks, after that they are removed from the cache automatically. To manually remove the content database from the Recovery Cache, proceed as follows:

1. On the Recovery Cache Management page, select which content database to remove, and click **Remove From Recovery Cache**. The Remove From Recovery Cache page is displayed.
2. To keep the content database files on the disk, clear the **Delete files from disk** option.

Click **Remove**.

Figure 25: Removing a content database



Monitoring granular recovery import jobs

Procedure

1. Connect to the Central Administration webpage.
2. A Microsoft Office SharePoint Server 2007 specific step: click the **Operations** tab.
3. Look for **HP Data Protector Granular Recovery Extension**, and click **Granular Recovery Job Status**. The Granular Recovery Import Jobs page is displayed.
4. Once you start a content database import session, HP Data Protector Granular Recovery Extension starts monitoring the import job progress.

Figure 26: Monitoring an import job progress

Central Administration ▶ Granular Recovery Import Job Status

Click **Refresh** to update jobs list.

Refresh

Clear History

Abort

Recovery Cache Management

Active

ID	Name	Started By	Started	Ended	Details
1021ebca-05b3-4637-9a90-27e9069e5111	gr-job-restore-recovery-database_WSS_Content_2010/04/13-2	user			None

History

Status	ID	Name	Started By	Started	Ended	Details
	93a17a01-0ec4-421b-8b7d-4778ecec0a14	gr-job-restore-recovery-database_WSS_Content_2010/09/16-2	user	9/16/2010 3:40:22 PM	9/16/2010 3:42:13 PM	Checking disk space Restoring Mounting Creating recovery cache remove job Starting recovery cache content source crawl Posting recovery tasks to site collection administrators

Optionally, after the recovery job is finished and you no longer need the job statuses, click **Clear History**.

To stop the operation in progress, click **Abort**.

Changing HP Data Protector Granular Recovery Extension settings

During a granular recovery session, a content database is first restored to a temporary location on the selected Microsoft SQL Server system (default: C:\Restore).

Before the site items are recovered, they are copied to a temporary location on a Microsoft SharePoint Server system (default: C:\Recovery).

Procedure

1. To change these default locations, connect to the Central Administration webpage.
2. A Microsoft Office SharePoint Server 2007 specific step: click the **Operations** tab.

Look for **HP Data Protector Granular Recovery Extension**, and click **Granular Recovery Settings**.

3. On the Granular Recovery Settings page, enter a new restore location or temporary recovery location and click **OK**.

Figure 27: Changing Granular Recovery settings

Product Version View Granular Recovery Extension version.	Version 6.11.28.1500
Default SQL Server for Import Select default SQL Server for import of content database.	SQL server <input type="text" value="APNO\SharePoint"/>
Restore Location Specify path on SQL server to which selected content database will be restored during import from backup.	Path <input type="text" value="C:\Restore"/> Example: c:\Restore
Temporary Location for Recovery Specify path for temporary files created during recovery.	Path <input type="text" value="C:\Recovery"/> Example: c:\Recovery

Chapter 6: Command line reference

Use the HP.SharePoint.GranularRecovery.CLI.exe command line tool that is located in:

Microsoft Office SharePoint Server 2007:

C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\12\BIN

Microsoft SharePoint Server 2010:

C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\14\BIN

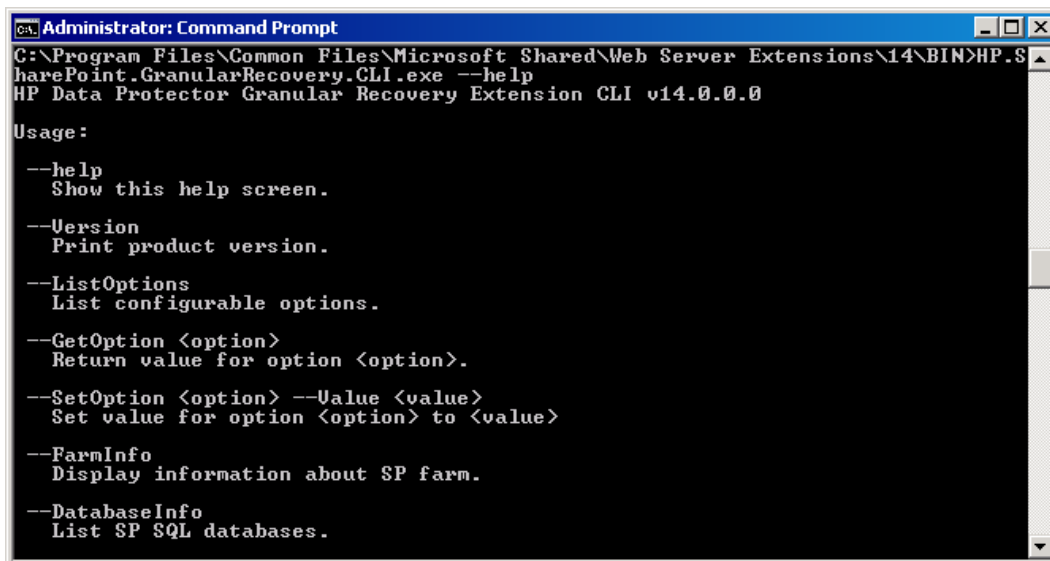
Microsoft SharePoint Server 2013:

C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\15\BIN

To display descriptions of options and their usage, run:

HP.SharePoint.GranularRecovery.CLI.exe --help.

Figure 28: Retrieving the command line help



```
Administrator: Command Prompt
C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\14\BIN>HP.SharePoint.GranularRecovery.CLI.exe --help
HP Data Protector Granular Recovery Extension CLI v14.0.0.0

Usage:
--help
    Show this help screen.
--Version
    Print product version.
--ListOptions
    List configurable options.
--GetOption <option>
    Return value for option <option>.
--SetOption <option> --Value <value>
    Set value for option <option> to <value>
--FarmInfo
    Display information about SP farm.
--DatabaseInfo
    List SP SQL databases.
```

Note: In the examples below, HP.SharePoint.GranularRecovery.CLI.exe is omitted for simplicity.

Examples

Restoring a content database from Data Protector backup

- To list all the backup versions of your content database named WSS_Content_054a5bfa-f23c-49b8-8f78-e0b3ce00b193, specify:

```
--ListBackupVersions --ContentDB=WSS_Content_054a5bfa-f23c-49b8-8f78-e0b3ce00b193
```

Monitoring jobs progress

- To list all the jobs that have been started of your content database, specify:

```
--ListJobs
```

- To start a restore job by importing the content database from the backup version "2010/04/20-4" to the default restore location C:\Restore, specify:

```
--StartImportJob
```

```
--ContentDB WSS_Content_054a5bfa-f23c-49b8-8f78-e0b3ce00b193
```

```
--BackupID "2010/04/20-4" --Server computer
```

```
--Instance OFFICESERVERS --TargetLocation C:\Restore
```

Note: To successfully import the content database when your Microsoft SQL Server is installed with the default instance, replace OFFICESERVERS with one of the following:

- the instance name
- DEFAULT
- MSSQLSERVER

You can also leave the instance name empty to ensure that Data Protector uses its correct name.

- Suppose you want to start a restore job by importing the content database from a filesystem to the Microsoft SharePoint Server to the default restore location C:\Restore.

If the Microsoft SQL Server Database Primary Data File is WSS_Content_054a5bfa-f23c-49b8-8f78-e0b3ce00b193.mdf and the SQL Server Transaction log file is WSS_Content054a5bfa-f23c-49b8-8f78-e0b3ce00b193_log.LDF, specify:

```
--StartImportJob
```

```
--ContentDB WSS_Content_054a5bfa-f23c-49b8-8f78-e0b3ce00b193
```

```
--BackupID "2010/04/20-4" --Server computer
```

```
--Instance OFFICESERVERS
```

```
--Files="C:\Restore\WSS_Content_054a5bfa-f23c-49b8-8f78-e0b3ce  
00b193.mdf";"C:\Restore\WSS_Content054a5bfa-f23c-49b8-8f78-e0b  
3ce00b193_log.LDF"  
--TargetLocation C:\Restore
```

Verifying target location disk space size

- To check the available disk space on the default restore location C:\Restore, specify:

```
--QueryServerInfo --Server computer --Instance OFFICESERVERS --TargetLocation  
C:\Restore
```

This also lists the location of all content database files in the tree structure.

Listing content databases

- To list all content databases in the Recovery Cache including the backup versions, specify:

```
--ListCache --All
```

- To list detailed information of the content databases, specify:

```
--ListCache --Verbose
```

Removing restore jobs

- To delete all the restore job statuses, specify:

```
--DeleteAllJobs Confirm
```

- To delete a specific restore job, specify:

```
--DeleteJob= JobID
```

- To abort all the inactive restore jobs, specify:

```
--DeleteJob= JobID
```

Recovering a site item to the original site

- Suppose you want to recover the site item `/Shared Documents/Document.txt` that was backed up from the site `http://computer.company.com:25884/sites/AnikyB`. Suppose the recovery site is `http://computer.company.com:38000/sites/AnikyB`. To recover the item to the original location, specify:

```
--Recover  
  
--Source http://computer.company.com:38000/sites/AnikyB  
  
--Destination http://computer.company.com:25884/sites/AnikyB  
  
--TempLocation="C:\Recovery"  
  
--Items "/Shared Documents/Document.txt"
```

The recovery session finishes and the following message is displayed:

```
recovery ended, object status:  
  object: [/Shared Documents/Document.txt]  
  destination: [/Shared Documents/Document_MOSSGR_24032010-024302.txt]  
  status: Finished  
  status details: [recovered to [http://computer.company.com:  
                  25884/sites/AnikyB//Shared Documents]]
```

Recovering a site item to another location

- To recover the site item `/Shared Documents/Document.txt` to My Documents, specify:

```
--Recover  
  
--Source http://computer.company.com:38000/sites/AnikyB  
  
--Destination http://computer.company.com:25884/sites/AnikyB  
  
--TempLocation="C:\Recovery"  
  
--Items "/Shared Documents/Document.txt:/My Documents"
```

Removing content databases from the cache

- To remove a database from the cache, specify:

```
--RemoveFromCache --ContentDB DatabaseName --BackupIDBackupID
```

- To remove all the content databases from the cache, specify:

```
--RemoveFromCache --All
```

Removing content databases from disk

- To delete a content database from the disk after you have removed it from the cache, specify:

```
--RemoveFromCache --ContentDB DatabaseName --DeleteFiles
```

Setting content database automatic removal

Content databases remain available for 21 days (default retention period), afterwards they are removed from the cache.

- To display the time (number of days) a content database remains available before it is removed from the cache, specify:

```
--GetOption RecoveryDatabaseAutoCleanupDays
```

- To set how long a content database remains available before it is automatically removed from the cache, specify:

```
--SetOption RecoveryDatabaseAutoCleanupDays --Value number_of_days
```

Exporting items from a content database

- To export an item from a content database, specify:

```
--Export --Source source --Location path
```

```
--Item item
```

- To export items from a content database, specify:

```
--Export --Source source --Location path
```

```
--Items item1 item2 item3
```

Note: Workflows cannot be exported.

Listing exported items

- To list the exported items, specify:

```
--ListExport --Location
```

Importing items from a content database

- To import an item from a content database, specify:

```
--Import --Destination destination --Location path
```

```
--Item item
```

- To import items from a content database, specify:

```
--Import --Destination destination --Location path
```

```
--Items item1item2item3
```

Note: Workflows cannot be imported.

Displaying Microsoft SharePoint farm information

- To display detailed information of the farm, such as name, display name, address, type name, role, version, status and all services running in this farm, specify:

```
--FarmInfo
```

Displaying content database information

- To display content database information such as: Office Servers, Shared Services, SharePoint configuration, Share Services Search, Recovery Web Application, Shared Services Content, SharePoint Admin Content, content database name, specify:

```
--DatabaseInfo
```

Displaying a list of sites

- To display the Web Application name, the site's URL, content database name and the all the sites in this content database, specify:

```
--ListSites
```

Browsing sites

- To browse a My Site structure and items such as: Forms, Lists, Template Gallery, Master Page Gallery, Personal Documents, Shared Documents, Shared Pictures, Site Template Gallery, User Information List, and Web Part Gallery, specify:

```
--BrowseSite --Site http://ivanka/personal/anikyb
```

Displaying Granular Recovery Extension version

- To display the Granular Recovery Extension version, specify:

```
--Version
```

Displaying Granular Recovery product key

- To display Granular Recovery product key, specify:

```
--getOption ProductKey
```

- To display Granular Recovery trial expiration date, specify:

```
--getOption TrialExpirationDate
```

- To set a new Granular Recovery product key, specify:

```
--setOption ProductKey --value ProductKey
```


Chapter 7: Troubleshooting

This chapter lists general checks and verifications, plus problems you might encounter when using the Data Protector Granular Recovery Extension for Microsoft SharePoint.

- For Microsoft SharePoint troubleshooting information, see the troubleshooting sections of the Microsoft SharePoint Server parts of the *HP Data Protector Integration Guide for Microsoft Applications: SQL Server, SharePoint Server, and Exchange Server*.
- For general Data Protector troubleshooting information, see the *HP Data Protector Troubleshooting Guide*.

The folder with debugs entries and logs is located in the folder:

Microsoft Office SharePoint Server 2007:

C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\12\LOGS\GranularRecovery

Microsoft SharePoint Server 2010:

C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\14\LOGS\GranularRecovery

Microsoft SharePoint Server 2013:

C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\15\LOGS\GranularRecovery

This folder contains the files `debugs.txt`, `debugs_cliproxy.txt`, `note.txt`, and `note_cliproxy.txt`. The folder location may vary depending on where you install the Microsoft SharePoint Server.

During installation, a setup debug log is created in the `Data_Protector_program_data\tmp\shp_gre_setup.txt` file.

Installation reports a warning "No full read permissions"

Problem

When installing the MS SharePoint Granular Recovery Extension component, Data Protector reports the following warning:

Windows SharePoint Services Search service has no full read permissions for all content databases.

Action

You can safely ignore the warning. However, to prevent it from appearing again, proceed as follows:

1. Open SQL Server Management Studio.
2. Under **Security**, expand **Logins**, right-click the user account under which the Windows SharePoint Services Search service is running, and click **Properties**.
3. In the Properties dialog box, click **User Mapping**. Select all content databases and assign the following two database roles to the user:
 - db_owner
 - WSS_Content_Application_Pools
4. Click **OK** to apply the changes.

Remote installation fails

Problem

When installing the MS SharePoint Granular Recovery Extension component remotely, the session fails with an error similar to the following:

```
[Critical] ClientName Post-installation script for the MS SharePoint Granular
Recovery Extension failed with the output: CreateProcessWithLogonW failed, trying
LogonUser/CreateProcessAsUser, GetLastError(): 1326 LogonUser failed, GetLastError():
1326
```

Action

Make sure that the user account under which Data Protector tries to connect to the Microsoft SharePoint Server system (for example, the Farm Administrator) has been assigned the **Allow log on locally** policy:

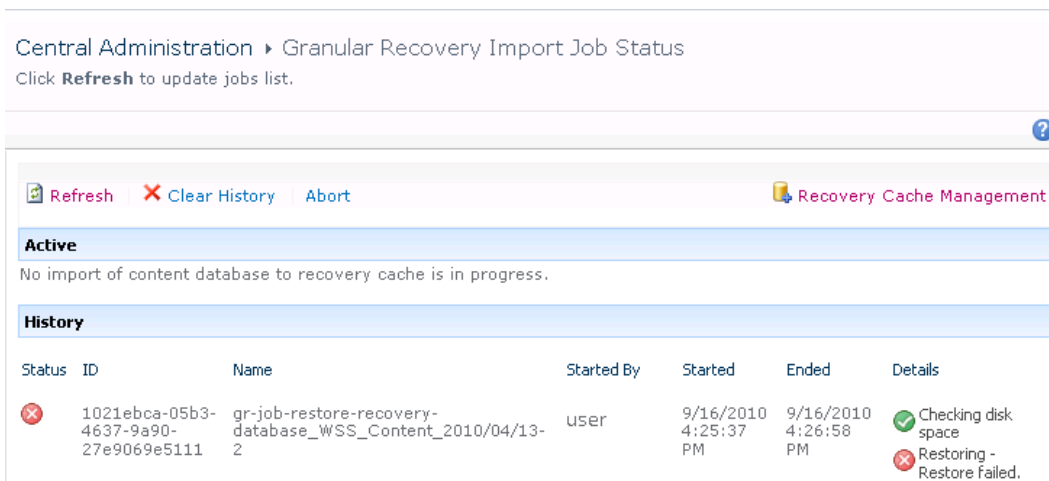
1. On the Microsoft SharePoint Server system, open **Administrative Tools** and then **Local Security Policy**.
2. Under Security Settings, expand **Local Policies** and then click **User Rights Assignment**.
3. Right-click the **Allow log on locally** policy, click **Properties**, and add the user.
4. Click **OK** to apply the changes.

An import job fails

Problem

After performing an Import From Backup, the Granular Recovery Import Job Status page reports a failed status in the Restoring phase.

Figure 29: Restore fails with not enough user rights



Action

Ensure the user account under which the Windows SharePoint Services Timer service is running is assigned the Data Protector Start restore, and the See private objects user rights. For example, if the Windows SharePoint Services Timer service is the one running under the Network Service account:

1. Launch the Data Protector GUI (**Data Protector Manager**).
2. In the Context list, select **Users**. Right-click the user group that has the Start restore and the See private objects user right enabled, and click **Add/Delete Users**.

The Network Service user account should be configured with the following properties:

- Name: Network Service
- Domain/Group: NT Authority
- Client system: Any

For details, see "[Configuring HP Data Protector user rights](#)" on page 13.

An import job fails

Problem

After performing an Import From Backup, the Granular Recovery Import Job Status page reports Not enough space available and the Details column reads Checking disk space.

Figure 30: Restore fails with not enough disk space

Refresh

Clear History

Recovery Cache Management

Active

ID	Name	Started By	Started	Ended	Details
<div> <div></div> <div>e06fc2ce-c9af-44b0-ba29-967d7a41ea7f</div> </div>	gr-job-restore-recovery-database_WSS_Content_2011/02/28-8	ESC\tic	2/28/2011 11:55:36 AM		<div> <div> <div>✓</div> <div>Checking disk space</div> </div> <div> <div>✓</div> <div>Checking disk space</div> </div> <div> <div>✓</div> <div>Checking disk space</div> </div> <div> <div>✓</div> <div>Checking disk space</div> </div> <div> <div>✓</div> <div>Checking disk space</div> </div> <div> <div>✓</div> <div>Checking disk space</div> </div> <div> <div>✓</div> <div>Checking disk space</div> </div> <div> <div>✓</div> <div>Checking disk space</div> </div> <div> <div>✓</div> <div>Checking disk space</div> </div> <div> <div>⌂</div> <div>Restoring</div> </div> </div> <div>0%</div>

Action

The root cause of the problem is that there is no Internet access and the HP Data Protector Granular Recovery Extension signature verification may take quite some time to complete. Perform the following:

- Ensure you have Internet access.
- Disable the signature verification:

To disable the HP Data Protector Granular Recovery Extension signature verification, proceed as follows:

- Locate the `cliproxy.exe` and the `HP.Sharepoint.GranularRecovery.CLI.exe` files in the Microsoft SharePoint Server BIN folder. By default, the BIN folder is located in the following directory:

Microsoft Office SharePoint Server 2007:

C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\12

Microsoft SharePoint Server 2010:

C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\14

Microsoft SharePoint Server 2013:

C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\15

- In the BIN folder, create the configuration files `cliproxy.exe.config` and `HP.Sharepoint.GranularRecovery.CLI.exe.config` with the following content:

```
<?xml version="1.0" encoding="utf-8" ?> <configuration>
  <runtime>
    <generatePublisherEvidence enabled="false"/>
  </runtime> </configuration>
```

Recovery session fails

Problem

If you start a recovery session by connecting to the original website, the following message is displayed:

No recovery available for this site http://computer:25884/sites/User! Please contact Granular Recovery Administrator for further info!

Action

The root cause of the problem is that the content database is not in the cache. Perform an import job.

Restore from backup data created with the Data Protector Microsoft SharePoint Server 2007/2010 integration (VDI based integration) fails

Problem

When HP Data Protector Granular Recovery Extension starts monitoring the import job progress, the restore fails. You probably performed the following steps:

1. You started a backup session with the Data Protector Microsoft SharePoint Server 2007/2010 integration.
2. On the Recovery Cache Management page of the extension, clicked **Import From Backup**, **Import the content database**, and then **Continue** to monitor the session.

On the Granular Recovery Import Job Status page, under the details column the status checking disk space was displayed, and then the import job progress is displayed the Restore failed status.

Action

The root cause of the problem is that a folder for the restore location is missing in the target location. Proceed as follows:

1. Manually create the folder, for example C:\Restore.
2. Restart the backup session.
3. Restart restore session.

On the Granular Recovery Import Job Status page, the Restoring status is successful.

Granular Recovery Cache Management link is not accessible from My Sites

Problem

After you create a new site collection or a new web application and then back up your new site collection, you cannot access the Granular Recovery Cache Management link from My Sites (**Site Actions > Site Settings > Granular Recovery** for Microsoft SharePoint Server 2007/2010 or **settings icon > Site Settings > Granular Recovery** for Microsoft SharePoint Server 2013). The following message is displayed:

GR resource files are missing in site's "App_GlobalResources" folder.

Action

1. Open **Central Administration** as follows:

Microsoft Office SharePoint Server 2007:

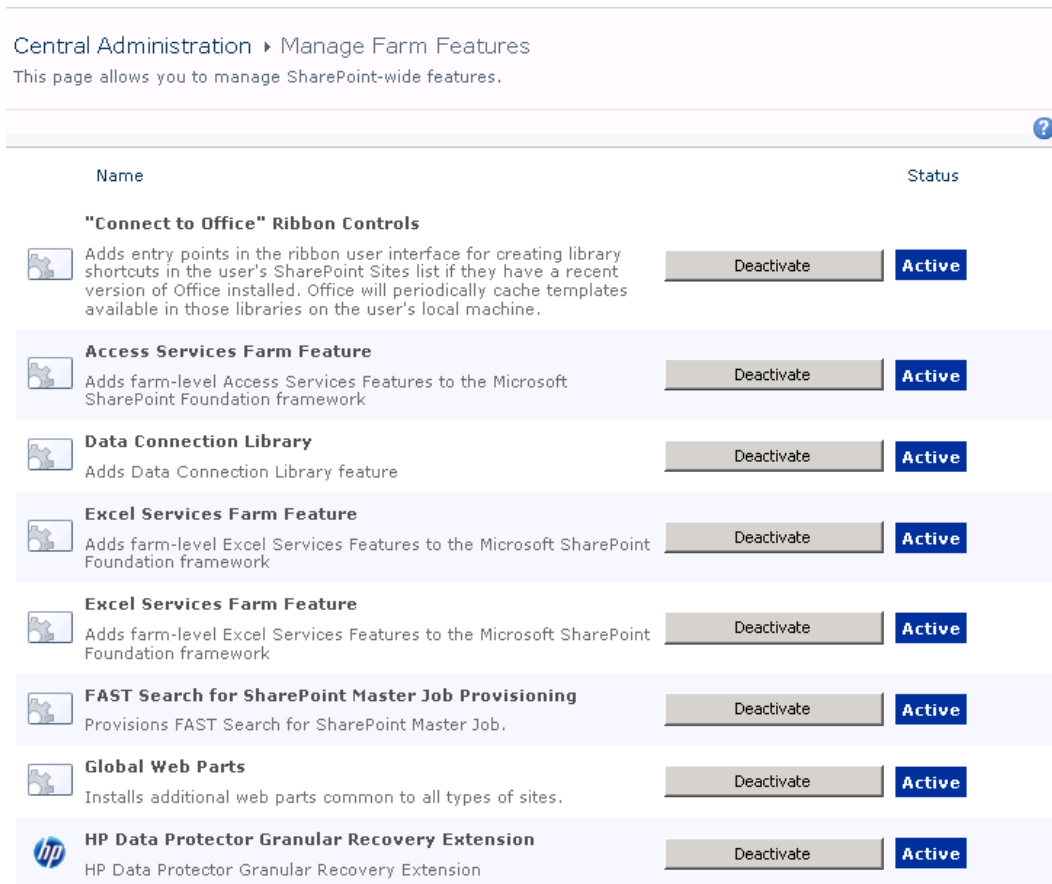
Click the Operations Tab and under Global Configuration, select **Manage Farm Features**.

Microsoft SharePoint Server 2010/2013:

Under System Settings, select **Manage Farm Features**.

2. By the HP Data Protector Granular Recovery Extension, click **Deactivate**. The Warning page is displayed, click the **Deactivate this feature** link. Return to Manage Farm Features. By the HP Data Protector Granular Recovery Extension, click **Activate**.

Figure 31: Manage Farm Features deactivating HP Data Protector Granular Recovery Extension



Granular Recovery Cache Management link is not accessible from My Sites

Problem

After you create a new site collection or a new web application and then back up your new site collection, you cannot access the Granular Recovery Cache Management link from My Sites (**Site Actions > Site Settings > Granular Recovery** for Microsoft SharePoint Server 2007/2010 or **settings icon > Site Settings > Granular Recovery** for Microsoft SharePoint Server 2013). The message "Access denied." is displayed. The following debug entry is displayed:

```
[6 - Fatal] FATAL debugs - Recovery.aspx: OnPreInit: - Exception: Thread was being aborted.
```

Action

Application pool users of every web application in the farm must be granted the Read permissions on the Recovery Web Application. To grant the Read permission to application pool user accounts:

1. Connect to the Microsoft SharePoint Server Central Administration system as follows:

Microsoft Office SharePoint Server 2007:

Click **Application Management**, under Application Security, and click **Policy for Web Application**.

Microsoft SharePoint Server 2010/2013:

Under Application Management, select **Manage web applications**, select **Recovery Web Application**, and click **User Policy**, the Policy for Web Application is displayed.

2. If a user does not exist in the Policy for Web Application, click **Add Users**. In the Add Users page, select **All Zones** and then click **Next**. Enter application pool users, select **Full Read - Has full read-only access** and then click **Finish**.
3. If a user exists in the Policy for Web Application, select the user and then click **Edit Permission of Selected Users**. In the Edit Users page, select **Full Read - Has full read-only access** and then click **Save**.

Figure 32: Granting Full Read permission

The screenshot shows the 'Edit Users' dialog box. It has a title bar with 'Edit Users' and window control buttons. The main content area is divided into three sections:

- Users:** A table with columns 'Zone', 'User Name', and 'Display Name'. The table contains one row: Zone (All zones), User Name (NT AUTHORITY\LOCAL SERVICE), and Display Name (NT AUTHORITY\L...).
- Permission Policy Levels:** A section with the text 'Choose the permissions you want these users to have.' and a list of permissions with checkboxes:
 - ☐ Full Control - Has full control.
 - ☒ Full Read - Has full read-only access.
 - ☐ Deny Write - Has no write access.
 - ☐ Deny All - Has no access.
- Choose System Settings:** A section with the text 'System accounts will not be recorded in the User Information lists unless the account is directly added to the permissions of the site. Any changes made by a system account will be recorded as made by the system instead of the actual user account.' and a checkbox:
 - ☐ Account operates as System

At the bottom of the dialog are two buttons: 'Save' and 'Cancel'.

HP Data Protector Granular Recovery Extension is not available on a newly created Web Application

Problem

After you added a new Web Application or a new Front-end Web Server to the farm where HP Data Protector Granular Recovery Extension is already installed, the Site Collection Administrator may have problems with accessing the Granular Recovery Extension user interface. HP Data Protector Granular Recovery Extension is not available on the newly created Web Applications.

Action

1. Open **Central Administration** as follows:

Microsoft Office SharePoint Server 2007:

Click the Operations Tab and under Global Configuration, select **Manage Farm Features**.

Microsoft SharePoint Server 2010/2013:

Under System Settings, select **Manage Farm Features**.

2. By the HP Data Protector Granular Recovery Extension, click **Deactivate**. The Warning page is displayed, click the **Deactivate this feature** link. Return to Manage Farm Features. By the HP Data Protector Granular Recovery Extension, click **Activate**.

Import from backup or from filesystem fails

Problem

Import from backup or from filesystem ends with an error `Checking disk space – Unknown error occurred`. This problem may occur if Microsoft SQL prerequisites are not met on one or more systems in the farm.

Action

Make sure that all prerequisites are installed. In case you had to install the missing packages, restart SharePoint Timer service and IIS on the updated clients.

Changing default recovery settings fails

Problem

When starting the recovery process, you cannot change the default recovery settings, for example, the recovery location. As the default recovery settings are configured in the pop-up windows, the problem can be caused by the enabled pop-up blocker in your browser.

Action

Disable any pop-up blocker software in your browser.

Slow response of the command line interface

Problem

You can notice slow response of the HP Data Protector Granular Recovery Extension command line interface. For example when you run the `HP.Sharepoint.GranularRecovery.CLI.exe --help` command, the command takes from 10 seconds to several minutes to display the usage. The root cause of the problem is the HP Data Protector Granular Recovery Extension signature verification which may take quite some time to complete.

Action

To import HP Data Protector Granular Recovery Extension signature certificate, proceed as follows:

To disable the HP Data Protector Granular Recovery Extension signature verification, proceed as follows:

1. Locate the `cliproxy.exe` and the `HP.Sharepoint.GranularRecovery.CLI.exe` files in the Microsoft SharePoint Server BIN folder. By default, the path of the BIN folder is:

Microsoft Office SharePoint Server 2007:

`C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\12\BIN`

Microsoft SharePoint Server 2010:

`C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\14\BIN`

Microsoft SharePoint Server 2013:

`C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\15\BIN`

2. In the BIN folder, create the configuration files `cliproxy.exe.config` and `HP.Sharepoint.GranularRecovery.CLI.exe.config` with the following content:

```
<?xml version="1.0" encoding="utf-8" ?> <configuration> <runtime>  
<generatePublisherEvidence enabled="false"/> </runtime> </configuration>
```

Slow response of the graphical user interface

Problem

You can notice slow response of the HP Data Protector Granular Recovery Extension GUI. For example when importing a content database from backup or from filesystem. The import job might fail, due to a

time-out. The root cause of the problem is the HP Data Protector Granular Recovery Extension signature verification which may take too long to complete.

Action

To disable the HP Data Protector Granular Recovery Extension signature verification, proceed as follows.

1. Locate the `cliproxy.exe` and the `HP.Sharepoint.GranularRecovery.CLI.exe` files in the Microsoft SharePoint Server BIN folder. By default, the path of the BIN folder is:

Microsoft Office SharePoint Server 2007:

`C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\12\BIN`

Microsoft SharePoint Server 2010:

`C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\14\BIN`

Microsoft SharePoint Server 2013:

`C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\15\BIN`

2. In the BIN folder, create the configuration files `cliproxy.exe.config` and `HP.Sharepoint.GranularRecovery.CLI.exe.config` with the following content:

```
<?xml version="1.0" encoding="utf-8" ?> <configuration>
  <runtime>
    <generatePublisherEvidence enabled="false"/>
  </runtime> </configuration>
```

The Data Protector service is not running

Problem

When performing an import from filesystem session, the following message is displayed: Required Data Protector service is not running!

Action

1. Open Control Panel, double-click **Administrative tools**, and double-click **Services**.

Find the Data Protector services, right-click the disabled service, and click **Start** to enable it.
2. In the Backup Version Selection page, click **Back** to finish your session.

The restoring - Mount Request Pending status

Problem

When performing an import from backup session, the status **Restoring - Mount Request Pending** is displayed on the Granular Recovery Import Job Status page.

Action

1. Launch the Data Protector GUI (Data Protector Manager).
2. In the Monitor context, check for any mount requests. Confirm the mount requests and restart the backup session.
3. Once the backup session is finished, perform an import from backup session again.

Subfolders are not recovered to original location

Problem

When recovering a folder with subfolders the parent folder is recovered but its subfolders are not.

Action

After you delete a folder, Microsoft SharePoint Server places this folder in the Site Collection Recycle bin. To recover your folder and its subfolders to original location using Granular Recovery Extension:

1. In the Site Collection Recycle bin, select the folder and click Delete Selection.
2. Perform a recovery session of your folder again.

Granular Recovery Extension upgrade fails

Problem

After upgrading from Microsoft Office SharePoint Server 2007 to Microsoft SharePoint Server 2010 and then upgrading from Granular Recovery Extension 1.00 to HP Data Protector Granular Recovery Extension, the upgrade fails with the following message:

A solution with the same name "moss_gr-1.1.5037.1353.wsp" or id "67f59f7b-5744-4f8f-98ea-94ea50a3db d3" already exists in the solution store. MOSS_GRE_2010.wsp: The Solution installation failed.

"MOSS_GRE_2010.wsp" does not exist in the solution store.Done.

Action

Before upgrading from Microsoft Office SharePoint Server 2007 to Microsoft SharePoint Server 2010, remove Granular Recovery Extension 1.00, upgrade to Microsoft SharePoint Server 2010 and then install the Granular Recovery Extension component.

Granular Recovery Extension component installation fails

Problem

Installing HP Data Protector with the HP Data Protector Granular Recovery Extension component enabled fails.

Action

To manually install the HP Data Protector Granular Recovery Extension without using standard HP Data Protector installation procedure:

1. Log on to the Microsoft SharePoint Server Central Administration system under a Microsoft SharePoint Server **Farm Administrator** user account.
2. In the Start menu, right-click **Command Prompt** and select **Run as Administrator**.
3. Change the current directory to the *Data_Protector_home\bin* directory where the files from the self-extracting archive were extracted during the product installation process.
4. Run `grm_install.bat` to install the HP Data Protector Granular Recovery Extension solution.

Granular Recovery Extension removal fails

Problem

After HP Data Protector deinstallation, the HP Data Protector Granular Recovery Extension is not removed from the system.

Action

To manually remove the HP Data Protector Granular Recovery Extension without using standard HP Data Protector removal procedure:

1. **Microsoft Office SharePoint Server 2007:**

Start Microsoft PowerShell v2.0 or higher using the SharePoint system account.

Microsoft SharePoint Server 2010/2013:

Start SharePoint 2010/2013 Management Shell using the SharePoint system account.

2. From the *Data_Protector_home\bin* directory, run:

`grm_check.ps1`

Installation ends unexpectedly on a farm with multiple servers on Central Administration

Problem

On a farm with multiple servers on Central Administration, the installation of the HP Data Protector Granular Recovery Extension ends unexpectedly.

Action

Ensure that the following service is enabled on Central Administration:

Microsoft Office SharePoint Server 2007:

Windows SharePoint Services Web Application

Microsoft SharePoint Server 2010/2013:

Microsoft SharePoint Foundation Web Application

Figure 33: Enabling Central Administration Services

The screenshot shows the 'Services on Server' page in the Central Administration console. The page title is 'Central Administration > Services on Server'. Below the title, it says 'Use this page to start or stop instances of services on servers in the farm'. The page has a navigation pane on the left with links to 'Central Administration', 'Application Management', 'System Settings', 'Monitoring', 'Backup and Restore', 'Security', 'Upgrade and Migration', 'General Application Settings', and 'Configuration Wizards'. The main content area has a table of services. The table has columns for 'Service', 'Status', and 'Action'. The 'Microsoft SharePoint Foundation Web Application' service is highlighted in blue. The status of this service is 'Started'.

Service	Status	Action
Access Database Service	Started	Stop
Application Registry Service	Started	Stop
Business Data Connectivity Service	Started	Stop
Central Administration	Started	Stop
Claims to Windows Token Service	Stopped	Start
Document Conversions Launcher Service	Stopped	Start
Document Conversions Load Balancer Service	Stopped	Start
Excel Calculation Services	Started	Stop
Lotus Notes Connector	Stopped	Start
Managed Metadata Web Service	Started	Stop
Microsoft SharePoint Foundation Incoming E-Mail	Started	Stop
Microsoft SharePoint Foundation Sandboxed Code Service	Stopped	Start
Microsoft SharePoint Foundation Subscription Settings Service	Stopped	Start
Microsoft SharePoint Foundation Web Application	Started	Stop
Microsoft SharePoint Foundation Workflow Timer Service	Started	Stop

Glossary

A

access rights

See user rights.

ACSLS (StorageTek specific term)

The Automated Cartridge System Library Server (ACSLS) software that manages the Automated Cartridge System (ACS).

Active Directory (Windows specific term)

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

AES 256-bit encryption

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

AML (ADIC/GRAU specific term)

Automated Mixed-Media library.

AMU (ADIC/GRAU specific term)

Archive Management Unit.

application agent

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

application system (ZDB specific term)

A system the application or database runs on. The application or database data is located on source volumes. See also backup system and source volume.

archive logging (Lotus Domino Server specific term)

Lotus Domino Server database mode where transaction log files are overwritten only after they have been backed up.

archived log files (Data Protector specific term)

Files that keep track of changes made to the Data Protector Internal Database (IDB). They are used for online or offline IDB restore and recovery where the IDB needs to be recreated either in its latest possible state, beyond the time of the most recent IDB backup session, or in a state between the times of two consecutive IDB backup sessions.

archived redo log (Oracle specific term)

Also called offline redo log. If the Oracle database operates in the ARCHIVELOG mode, as each online redo log is filled, it is copied to an archived log destination. This copy is the archived redo log. The presence or absence of an archived redo log is determined by the mode the database is using: ARCHIVELOG - The filled online redo log files are archived before they are reused. The database can be recovered if an instance or a disk fails. A "hot" backup can be performed only when the database is running in this mode. NOARCHIVELOG - The filled online redo log files are not archived. See also online redo log.

ASR set

A collection of files stored on several diskettes, required for proper reconfiguration of the replacement disk (disk partitioning and logical volume configuration) and automatic recovery of

the original system configuration and user data that was backed up during the full client backup. These files are stored as an ASR archive file on the Cell Manager in the directory <Data_Protector_program_data>\Config\Server\dr\asr (Windows systems) or /etc/opt/omni/server/dr/asr (UNIX systems), as well as on the backup medium. After a disaster occurs, the ASR archive file is extracted to diskettes which you need to perform ASR.

audit logs

Data files to which auditing information is stored.

audit report

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

auditing information

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

autochanger

See library.

autoloader

See library.

Automatic Storage Management (ASM) (Oracle specific term)

A filesystem and volume manager integrated into Oracle which manages Oracle database files. It eliminates complexity associated with data and disk management and optimizes performance by providing striping and mirroring capabilities.

auxiliary disk

A bootable disk that has a minimal operating system with networking and

Data Protector Disk Agent installed. It can be carried around and used to boot the target system in Phase 1 of Disk Delivery Disaster Recovery of UNIX clients.

B

BACKINT (SAP R/3 specific term)

A Data Protector interface program that lets the SAP R/3 backup programs communicate with the Data Protector software via calls to an open interface. For backup and restore, SAP R/3 programs issue commands through the Data Protector backint interface.

backup API (Oracle specific term)

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 reading and writing of data to media and also to allow creation, searching, and removing of backup files.

backup chain

See restore chain.

backup device

A device configured for use with Data Protector that 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 systems and mount point on UNIX systems), for integration objects - backup stream identification, indicating the backed up database/application items), description (for filesystem objects - uniquely defines objects with identical client name and mount point, for integration objects - displays the integration type), and type (for filesystem objects - filesystem type, 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. 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. All clients configured in one backup specification are backed up at the same time in one backup session using the same backup type (full or incremental).

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 of your 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 Continuances are processes that allow customers to access and manage instant copies of EMC Symmetrix standard devices.

BC Process (EMC Symmetrix specific term)

A protected storage environment solution, which uses specially configured EMC Symmetrix devices as mirrors or Business Continuation Volumes to protect data on EMC Symmetrix standard devices. See also BCV.

BCV (EMC Symmetrix specific term)

Business Continuation 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 Data Protector Help system are AND, OR, NOT, and NEAR. Used when searching, they enable you to define your query precisely by creating a relationship between search terms. If no operator is specified in a multi-word search, AND is used by default. For example, the query manual disaster recovery is equivalent to manual AND disaster AND recovery.

boot volume/disk/partition

A volume/disk/partition containing 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 BRARCHIVE and BRBACKUP.

BSM

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

C

CAP (StorageTek specific term)

The Cartridge Access Port built into the door panel of a library. The purpose is to enter or eject media.

Catalog Database (CDB)

A part of the Data Protector Internal Database (IDB) that contains information about backup, restore, object copy, object consolidation, object verification, and media management sessions. This part of the IDB is always local to the cell. It is stored in the embedded database. See also MMDB.

catalog protection

Defines how long information about backed up data (such as filenames and file attributes) is kept in the IDB. See also data protection.

CDB

See Catalog Database (CDB).

CDF file (UNIX systems specific term)

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

cell

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

Cell Manager

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

centralized licensing

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

Centralized Media Management Database (CMMDB)

See CMMDB.

Certificate Server

A Windows certificate server can be installed and configured to provide certificates for clients. It provides customizable services for issuing and managing certificates for the enterprise. These services issue, revoke, and manage certificates employed in public key-based cryptography technologies.

Change Journal (Windows specific term)

A Windows filesystem feature that logs a record of each change as it occurs to the files and directories on a local NTFS volume.

Change Log Provider

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' or type 'sbt_tape'. If the specified channel is of type 'sbt_tape' and Oracle is integrated with Data Protector, the server process will attempt to read backups from or write data files to Data Protector.

circular logging (Microsoft Exchange Server and Lotus Domino Server specific term)

Circular logging is a Microsoft Exchange Server database and Lotus Domino Server database mode, in which the transaction log file contents are periodically overwritten after the corresponding data is committed to the database. Circular logging reduces disk storage space requirements.

client backup

A backup of all volumes (filesystems) mounted on a Data Protector client. What is actually backed up depends on how you select objects in a backup specification. If you select the check box next to the client system name, a single backup object of the Client System type is created. As a result, at the time of the backup, Data Protector first detects all volumes that are mounted on the selected client and then backs them up. On Windows clients, CONFIGURATION is also backed up. If you individually select all volumes that are mounted on the client system, a separate backup object of the Filesystem type is created for each volume. As a result, at the time of the backup, only the selected volumes are backed up. Volumes that have been potentially mounted on the client after the

backup specification was created are not backed up.

client or client system

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

cluster continuous replication (Microsoft Exchange Server specific term)

Cluster continuous replication (CCR) is a high availability solution that uses cluster management and failover options to create and maintain an exact copy (CCR copy) of a storage group. A storage group is replicated to a separate server. CCR removes any single point of failure in your Exchange back-end servers. You can perform backups using VSS on your passive Exchange Server node where a CCR copy is located and thus reducing the load on the active node. A CCR copy is used for disaster recovery since you can switch to the CCR copy in a few seconds. A replicated storage group is represented as a new instance of Exchange writer called Exchange Replication Service and can be backed up (using VSS) like an ordinary storage group. See also Exchange Replication Service and local continuous replication.

cluster-aware application

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

CMD script for Informix Server (Informix Server specific term)

A Windows CMD script that is created in INFORMIXDIR when an Informix Server database is configured. The CMD script

is a set of system commands that export environment variables for Informix Server.

CMMDB

The Data Protector Centralized Media Management Database (CMMDB) is the result of merging MMDBs from several cells in the MoM environment. It allows you to share high-end devices and media across multiple cells in a MoM environment. One cell can control the robotics, serving the devices that are connected to systems in other cells. The CMMDB must reside on the 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 COM+ application attributes, class attributes, and computer-level attributes. This guaranties consistency among these attributes and provides common operation on top of these attributes.

command device (HP P9000 XP Disk Array Family specific term)

A dedicated volume in the disk array which acts as the interface between a management application and the disk array's storage system. It cannot be used for data storage and only accepts requests for operations that are then executed by the disk array.

command-line interface (CLI)

A set commands that you can use in shell scripts to perform Data Protector configuration, backup, restore, and management tasks.

concurrency

See Disk Agent concurrency.

container (HP P6000 EVA Disk Array Family specific term)

Space on a disk array, which is pre-allocated for later use as a standard snapshot, vsnap, or snapclone.

control file (Oracle and SAP R/3 specific term)

A data file that contains entries specifying the physical structure of the database. It provides database consistency information used for recovery.

copy set (HP P6000 EVA Disk Array Family specific term)

A pair that consists of the source volumes on a local P6000 EVA and their replica on a remote P6000 EVA. See also source volume, replica, and HP Continuous Access + Business Copy (CA+BC) P6000 EVA.

CRS

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

CSM

The Data Protector Copy and Consolidation Session Manager process controls the object copy and object consolidation sessions and runs on the Cell Manager system.

D**data file (Oracle and SAP R/3 specific term)**

A physical file created by Oracle that contains data structures such as tables and indexes. A data file can only belong to one Oracle database.

data protection

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

Data Protector user account

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

data replication (DR) group (HP P6000 EVA Disk Array Family specific term)

A logical grouping of HP P6000 EVA Disk Array Family virtual disks. It can contain up to eight copy sets provided they have common characteristics and share a common HP CA P6000 EVA log. See also copy set.

data stream

Sequence of data transferred over the communication channel.

Data_Protector_home

A reference to the directory containing Data Protector program files (on Windows Vista, Windows 7, Windows Server 2008, and Windows Server 2012) or the directory containing Data Protector program files and data files (on other Windows operating systems). Its default path is %ProgramFiles%\OmniBack, but the path can be changed in the Data Protector Setup Wizard at installation time. See also Data_Protector_program_data.

Data_Protector_program_data

A reference to the directory containing Data Protector data files on Windows Vista, Windows 7, Windows Server 2008, and Windows Server 2012. Its default path is %ProgramData%\OmniBack, but the path can be changed in the Data Protector Setup Wizard at installation time. See also Data_Protector_home.

database library

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

database parallelism

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

database server

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

Dbobject (Informix Server specific term)

An Informix Server physical database object. It can be a blob space, db space, or logical log file.

DC directory

A directory that contains DC binary files, one for each configured Data Protector backup medium. DC directories constitute the Detail Catalog Binary Files part of the Data Protector Internal Database. See also Detail Catalog Binary Files (DCBF) and Internal Database (IDB).

DCBF

See Detail Catalog Binary Files (DCBF).

delta backup

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

Detail Catalog Binary Files (DCBF)

A part of the Data Protector Internal Database that stores names, versions, and metadata of the backed up items. It consists of DC directories with DC binary files. See also DC directory and Internal Database (IDB).

device

See backup device.

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. -Get configuration, status, and performance statistics by device group. -Issue control operations that apply to all devices in the device group.

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 writing to the tape, and so on. If data is written to the tape slower than it is delivered to the device then the device is streaming. Streaming significantly improves the use of space and the performance of the device.

DHCP server

A system running the Dynamic Host Configuration Protocol (DHCP) providing dynamic IP address assignment and network configuration for DHCP clients.

differential backup

An incremental backup that backs up changes made since the last full backup. To perform this type of backup, specify the Incr1 backup type. See also incremental backup.

differential backup (Microsoft SQL Server specific term)

A database backup that records only the data changes made to the database after the last full database backup. See also backup types.

differential database backup

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

directory junction (Windows specific term)

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

disaster recovery

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

disaster recovery operating system

See DR OS.

Disk Agent

A component needed on a client to back it up and restore it. The Disk Agent controls reading from and writing to a disk. During a backup session, the Disk Agent reads data from a disk and sends it to the Media Agent, which then moves it to the device. During a restore session the Disk Agent receives data from the Media Agent and writes it to the disk. During an object verification session the Disk Agent receives data from the Media Agent and performs the verification process, but no data is written to disk.

Disk Agent concurrency

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

disk group (Veritas Volume Manager specific term)

The basic unit of data storage in VxVM system. A disk group can consist of one or more physical volumes. There can be more than one disk group on the system.

disk image (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.

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. It can also read the data from the medium and send it to the computer system.

drive index

A number that identifies the mechanical position of a drive inside a library device.

This number is used by the robotic control to access a drive.

drive-based encryption

The Data Protector drive-based encryption uses the encryption functionality of the drive. While performing the backup, the drive encrypts both the data and the metadata that is written to the medium.

E

EMC Symmetrix Agent

A Data Protector software module that prepares the EMC Symmetrix environment for backup and restore operations.

emergency boot file (Informix Server specific term)

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

encrypted control communication

Data Protector secure communication between the clients in the Data Protector cell is based on a Secure Socket Layer (SSL) that uses export grade SSLv3 algorithms to encrypt control communication. Control communication in a Data Protector cell is all communication between Data Protector processes, except the data transfer from Disk Agent (and Integrations) to Media Agent, and the other way round.

encryption key

A 256-bit randomly generated number used by the Data Protector encryption algorithm to encode information during backups for which AES 256-bit software encryption or drive-based encryption has been specified. The same key is used for subsequent decryption of the information. Encryption keys for a Data Protector cell are stored in a central keystore on the Cell Manager.

encryption KeyID-StoreID

Combined identifier used by the Data Protector Key Management Server to identify and administer encryption keys used by Data Protector. KeyID identifies the key within the keystore. StoreID identifies the keystore on the Cell Manager. If Data Protector has been upgraded from an earlier version with encryption functionality, there may be several StoreIDs 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

See library.

exporting media

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

**Extensible Storage Engine (ESE)
(Microsoft Exchange Server specific
term)**

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

F

failover

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

**failover (HP P6000 EVA Disk Array
Family specific term)**

An operation that reverses the roles of source and destination in HP Continuous Access + Business Copy (CA+BC) P6000 EVA configurations. See also HP Continuous Access + Business Copy (CA+BC) P6000 EVA.

FC bridge

See Fibre Channel bridge.

Fibre Channel

An ANSI standard for high-speed computer interconnection. Using either optical or copper cables, it allows the high speed bi-directional transmission of large data files and can be deployed between sites kilometers apart. Fibre Channel connects nodes using three physical topologies: point-to-point, loop, and switched.

Fibre Channel bridge

A Fibre Channel bridge or multiplexer provides the ability to migrate existing parallel SCSI devices, like RAID arrays, solid state disks (SSD), and tape libraries

to a Fibre Channel environment. On one side of the bridge or multiplexer there is a Fibre Channel interface while on the other side there are parallel SCSI ports. The bridge or multiplexer enables SCSI packets to be moved between the Fibre Channel and parallel SCSI devices.

file depot

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

file jukebox device

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

file library device

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

File Replication Service (FRS)

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

file tree walk

The process of traversing a filesystem to determine which objects have been created, modified, or deleted.

file version

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

filesystem

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

first-level mirror (HP P9000 XP Disk Array Family specific term)

A mirror of an internal disk (LDEV) of a disk array of the HP P9000 XP Disk Array Family which can be further mirrored itself, producing second-level mirrors. For Data Protector zero downtime backup and instant recovery purposes, only first-level mirrors can be used. See also primary volume and mirror unit (MU) number.

flash recovery area (Oracle specific term)

A directory, filesystem, or Automatic Storage Management (ASM) disk group managed by Oracle that serves as a centralized storage area for files related to backup, restore, and database recovery (recovery files). See also recovery files.

formatting

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

free pool

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

full backup

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

full database backup

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

full mailbox backup

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

full ZDB

A ZDB-to-tape or ZDB-to-disk+tape session in which all selected objects are streamed to tape, even if there are no changes from the previous backup. See also incremental ZDB.

G

global options

A set of options that define behavior of the entire Data Protector cell. The options are stored in a plain text file on the Cell Manager.

group (Microsoft Cluster Server specific term)

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

GUI

A graphical user interface provided by Data Protector for easy access to all configuration, administration, and operation tasks. It is available for Microsoft Windows operating systems.

H**hard recovery (Microsoft Exchange Server specific term)**

A Microsoft Exchange Server database recovery that is performed after a restore by the database engine, using transaction log files.

heartbeat

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

Hierarchical Storage Management (HSM)

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

Holidays file

A file that contains information about holidays. You can set different holidays by editing the Holidays file that resides on the Cell Manager at the following location: <Data_Protector_program_data>\Config\Server\holidays (Windows systems) and /etc/opt/omni/server/Holidays (UNIX systems).

hosting system

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

HP Business Copy (BC) P6000 EVA (HP P6000 EVA Disk Array Family specific term)

A local replication software solution that enables creation of point-in-time copies (replicas) of the source volumes using the snapshot and clone capabilities of the P6000 EVA firmware. See also replica, source volume, snapshot, and HP Continuous Access + Business Copy (CA+BC) P6000 EVA.

HP Business Copy (BC) P9000 XP (HP P9000 XP Disk Array Family specific term)

An HP P4000 SAN Solutions configuration that enables creation and maintenance of internal copies of LDEVs for various purposes, such as data duplication and backup. The copies (secondary volumes or S-VOLs) can be separated from the primary volumes (P-VOLs) and connected to a different system. For Data Protector zero downtime backup purposes, P-VOLs should be available to the application system, and one of the S-VOL sets should be available to the backup system. See also LDEV, HP Continuous Access (CA) P9000 XP, Main Control Unit (MCU), application system, and backup system.

HP Command View (CV) EVA (HP P6000 EVA Disk Array Family specific term)

The user interface that enables you to configure, manage, and monitor your P6000 EVA storage system. It is used to perform various storage management tasks, for example, creating virtual disk families, managing storage system hardware, and creating snapshots, snapclones, or mirrorclones of virtual disks. The HP Command View EVA software runs on the HP Storage Management Appliance, and is accessed

by a Web browser. See also HP P6000 / HP 3PAR SMI-S Agent and HP SMI-S P6000 EVA Array provider.

HP Continuous Access (CA) P9000 XP (HP P9000 XP Disk Array Family specific term)

An HP P9000 XP Disk Array Family configuration that enables creation and maintenance of remote copies of LDEVs for purposes such as data duplication, backup, and disaster recovery. HP CA P9000 XP operations involve main (primary) disk array units and remote (secondary) disk array units. The main disk array units are connected to the application system and contain primary volumes (P-VOLs), which store original data. The remote disk array units are connected to the backup system and contain secondary volumes (S-VOLs). See also HP BC P9000 XP (HP P9000 XP Disk Array Family specific term), Main Control Unit (MCU), and LDEV.

HP Continuous Access + Business Copy (CA+BC) P6000 EVA (HP P6000 EVA Disk Array Family specific term)

An HP P6000 EVA Disk Array Family configuration that enables creation and maintenance of copies (replicas) of the source volumes on a remote P6000 EVA, and later use of these copies as the source for local replication on this remote array. See also HP BC P6000 EVA, replica, and source volume.

HP P6000 / HP 3PAR SMI-S Agent

A Data Protector software module that executes all tasks required for the HP P6000 EVA Disk Array Family integration. With the P6000 / 3PAR SMI-S Agent, the control over the array is established through an appropriate SMI-S provider, which directs communication between incoming requests and the storage system's native interface. See

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

HP P9000 XP Agent

A Data Protector software component that executes all tasks needed by the Data Protector HP P9000 XP Disk Array Family integration. It communicates with the P9000 XP Array storage system via the RAID Manager Library.

HP SMI-S P6000 EVA Array provider

An interface used for controlling HP P6000 EVA Disk Array Family. SMI-S P6000 EVA Array provider runs as a separate service on the HP Storage Management Appliance system and acts as a gateway between incoming requests and HP Command View EVA. With the Data Protector HP P6000 EVA Disk Array Family integration, SMI-S P6000 EVA Array provider accepts standardized requests from the HP P6000 / HP 3PAR SMI-S Agent, communicates with HP Command View EVA for information or method invocation, and returns standardized responses. See also HP P6000 / HP 3PAR SMI-S Agent and HP Command View (CV) EVA.

ICDA (EMC Symmetrix specific term)

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

IDB

See Internal Database (IDB).

IDB recovery file

A file that maintains information about completed IDB backup sessions and the

backup media and backup devices used in them. If available, it significantly simplifies and speeds up offline recovery of the Internal Database in case of a Cell Manager disaster. Its filename is obdrindex.dat.

importing media

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

incremental (re-)establish (EMC Symmetrix specific term)

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

incremental backup

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

incremental backup (Microsoft Exchange Server specific term)

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

incremental mailbox backup

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

incremental restore (EMC Symmetrix specific term)

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

incremental ZDB

A filesystem ZDB-to-tape or ZDB-to-disk+tape session in which only changes from the last protected full or incremental backup are streamed to tape. See also full ZDB.

Incremental1 Mailbox Backup

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

Inet

A process that runs on each UNIX system or service that runs on each Windows system in the Data Protector cell. It is responsible for communication

between systems in the cell and for starting other processes needed for backup and restore. The Inet service is started as soon as Data Protector is installed on a system. The Inet process is started by the inetd daemon.

Information Store (Microsoft Exchange Server specific term)

The Microsoft Exchange Server service that is responsible for storage management. Information Store in Microsoft Exchange Server manages two kinds of stores: mailbox stores and public folder stores. A mailbox store consists of mailboxes that belong to individual users. A public folder store contains public folders and messages that are shared among several users. See also Key Management Service and Site Replication Service.

Informix Server (Informix Server specific term)

Refers to Informix Dynamic Server.

initializing

See formatting.

Installation Server

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

instant recovery (ZDB specific term)

A process in which a replica, produced by a ZDB-to-disk or a ZDB-to-disk+tape sessions, is used to restore the contents of the source volumes to their states at the time at which the replica was created, avoiding the need to perform a restore

from tape. Depending on the application/database concerned, this may be all that is required, or other steps, such as the application of transaction log files, may be required for full recovery. See also replica, zero downtime backup (ZDB), ZDB to disk, and ZDB to disk+tape.

integration object

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

Internal Database (IDB)

An entity in Data Protector that keeps information regarding which data was backed up, to which media it was backed up, how and when backup, restore, and other sessions were run, which devices, libraries, and disk arrays are configured, and so on. It is implemented with an embedded database and a collection of proprietary data files which reside on the Cell Manager. See also DC directory and Detail Catalog Binary Files (DCBF).

Internet Information Server (IIS) (Windows specific term)

Microsoft Internet Information Server is a network file and application server that supports multiple protocols. Primarily, IIS transmits information in Hypertext Markup Language (HTML) pages by using the Hypertext Transport Protocol (HTTP).

ISQL (Sybase specific term)

A Sybase utility used to perform system administration tasks on Sybase SQL Server.

J

jukebox

See library.

jukebox device

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

K

Key Management Service (Microsoft Exchange Server specific term)

The Microsoft Exchange Server service that provides encryption functionality for enhanced security. See also Information Store and Site Replication Service.

keychain

A tool that eliminates the supply of a passphrase manually when decrypting the private key. It needs to be installed and configured on the Installation Server if you perform remote installation using secure shell.

keystore

All encryption keys are centrally stored in the keystore on the Cell Manager and administered by the Key Management Server (KMS).

KMS

Key Management Server (KMS) is a centralized service that runs on the Cell Manager and provides key management for the Data Protector encryption functionality. The service is started as soon as Data Protector is installed on the Cell Manager.

L

LBO (Symmetric specific term)

A Backup Object (LBO) is an object of data storage/retrieval in the EMC Symmetrix environment. It is stored/retrieved by EMC Symmetrix as

one entity and can only be restored as a whole.

LDEV (HP P9000 XP Disk Array Family specific term)

A logical partition of a physical disk of a disk array of the HP P9000 XP Disk Array Family. An LDEV is the entity that can be replicated using the split-mirror or snapshot functionality of such disk array. See also HP Business Copy (BC) P9000 XP, HP Continuous Access (CA) P9000 XP, and replica.

library

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

lights-out operation or unattended operation

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

LISTENER.ORA (Oracle specific term)

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

load balancing

By default, Data Protector automatically balances the usage of devices selected for backup, so that they are used evenly. Load balancing optimizes the device usage by balancing the number of objects written to each device. Since load balancing is done automatically during

backup time, you do not need to manage how the data is actually backed up. You just specify the devices to be used. If you do not want to use load balancing, you can select which device will be used for each object in the backup specification. Data Protector will access the devices in the specified order.

local and remote recovery

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

local continuous replication (Microsoft Exchange Server specific term)

Local continuous replication (LCR) is a single-server solution that creates and maintains an exact copy (LCR copy) of a storage group. An LCR copy is located on the same server as the original storage group. When an LCR copy is created, it is kept up to date through change propagation (log replay) technology. The replication feature in LCR guarantees that logs that have not been replicated are not deleted. The implication of this behavior is that running backups in a mode that deletes logs may not actually free space if replication is sufficiently far behind in its log copying. An LCR copy is used for disaster recovery because you can switch to the LCR copy in a few seconds. If an LCR copy is used for backup and if it is located on a different disk than the original data, then the I/O load on a production database is minimal. A replicated storage group is represented as a new instance of Exchange writer called Exchange Replication Service and

can be backed up (using VSS) as a normal storage group. See also cluster continuous replication and Exchange Replication Service.

lock name

You can configure the same physical device several times with different characteristics, by using different device names. The lock name is a user specified string that is used for locking all such device configurations to prevent collision if several such devices (device names) are used concurrently. Use an identical lock name for all device definitions which use the same physical device.

log_full shell script (Informix Server UNIX systems specific term)

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

logging level

An option that determines the amount of details on files and directories written to the IDB during backup, object copying, or object consolidation. You can always restore your data, regardless of the logging level used during backup. Data Protector provides four logging levels: Log All, Log Directories, Log Files, and No Log. The different logging level settings mainly influence the IDB growth and the convenience of browsing data for restore.

logical-log files

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

login ID (Microsoft SQL Server specific term)

The name a user needs to log on to Microsoft SQL Server. A login ID is valid if Microsoft SQL Server has an entry for that user in the system table syslogin.

login information to the Oracle Target Database (Oracle and SAP R/3 specific term)

The format of the login information is <user_name>/<password>@<service>, where: <user_name> is the name by which a user is known to Oracle Server and to other users. Every user name is associated with a password and both have to be entered to connect to an Oracle Target Database. This user must have Oracle SYSDBA or SYSOPER rights. <password> must be the same as the password specified in the Oracle password file (orapwd), which is used for authentication of users performing database administration. <service> is the name used to identify an SQL*Net server process for the target database.

login information to the Recovery Catalog Database (Oracle specific term)

The format of the login information to the Recovery (Oracle) Catalog Database is <user_name>/<password>@<service>, where the description of the user name, password, and service name is the same as in the Oracle SQL*Net V2 login information to the Oracle target database.

In this case, <service> is the name of the service to the Recovery Catalog Database, not the Oracle target database. Note that the Oracle user specified here must be the owner of the Oracle Recovery Catalog.

Lotus C API (Lotus Domino Server specific term)

An interface for the exchange of backup and recovery information between Lotus Domino Server and a backup solution, like Data Protector.

LVM

A Logical Volume Manager is a subsystem for structuring and mapping physical disk space to logical volumes on UNIX systems. An LVM system consists of several volume groups, where each volume group has several volumes.

M

Magic Packet

See Wake ONLAN.

mailbox (Microsoft Exchange Server specific term)

The location to which e-mail is delivered, which is set up by the administrator for each user. If a set of personal folders is designated as the e-mail delivery location, e-mail is routed from the mailbox to this location.

mailbox store (Microsoft Exchange Server specific term)

A part of the Information Store that maintains information in user mailboxes. A mailbox store consists of a binary rich-text .edb file and a streaming native internet content .stm file.

Main Control Unit (MCU) (HP P9000 XP Disk Array Family specific term)

An HP P9000 XP Disk Array Family unit that contains primary volumes (P-VOLs) for the HP CA P9000 XP Array or HP CA+BC P9000 XP Array configuration and acts as a master device. See also HP Business Copy (BC) P9000 XP, HP Continuous Access (CA) P9000 XP, and LDEV.

maintenance mode

An operating mode you can initiate on the Cell Manager to prevent changes in the Internal Database. It enables you to perform various maintenance tasks, such as upgrading and patching the installation.

make_net_recovery

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

make_tape_recovery

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

Manager-of-Managers

See MoM.

MAPI (Microsoft Exchange specific term)

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

MCU

See Main Control Unit (MCU).

Media Agent

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

media allocation policy

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

media condition

The quality of a medium as derived from the media condition factors. Heavy usage and age result in an increased number of

read and write errors with tape media.
Media need to be replaced when they are marked as POOR.

media condition factors

The user-assigned age threshold and overwrite threshold used to assert the condition of a medium.

media label

A user-defined identifier used to describe a medium.

media location

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

media management session

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

media pool

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

media set

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

media type

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

media usage policy

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

medium ID

A unique identifier assigned to a medium by Data Protector.

merging

This defines one mode to resolve file conflicts during restore. If the file to be restored already exists at the destination, the one with the more recent modification date is kept. Files not present on the disk are always restored. See also overwrite.

Microsoft Exchange Server

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

**Microsoft Management Console (MMC)
(Windows specific term)**

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

Microsoft SQL Server

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

**Microsoft Volume Shadow Copy
Service (VSS)**

A software service that provides a unified communication interface to coordinate backup and restore of a VSS-aware application regardless of its specific features. This service collaborates with the backup application, writers, shadow

copy providers, and the operating system kernel to implement the management of volume shadow copies and shadow copy sets. See also shadow copy, shadow copy provider, replica, and writer.

mirror (EMC Symmetrix and HP P9000 XP Disk Array Family specific term)

See target volume.

mirror rotation (HP P9000 XP Disk Array Family specific term)

See replica set rotation.

mirror unit (MU) number (HP P9000 XP Disk Array Family specific term)

A non-negative integer number that determines a secondary volume (S-VOL) of an internal disk (LDEV) located on a disk array of the HP P9000 XP Disk Array Family. See also first-level mirror.

mirrorclone (HP P6000 EVA Disk Array Family specific term)

A dynamic replica of a storage volume, which is kept updated with changes made to the original storage volume via a local replication link. Replication between the original storage volume and its mirrorclone can be suspended. For each storage volume, a single mirrorclone can be created on the disk array.

MMD

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

MMDB

The Media Management Database (MMDB) is a part of the IDB that contains information about media, media pools, devices, libraries, library drives, and slots

configured in the cell, as well as the Data Protector media used for backup. In an enterprise backup environment, this part of the database can be common to all cells. See also CMMDB and Catalog Database (CDB).

MoM

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

mount point

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

mount request

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

MSM

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

multisnapping (HP P6000 EVA Disk Array Family specific term)

Simultaneous creation of target volumes so that the backup data is consistent not only on each individual target volume, but also across all the volumes that constitute a snapshot. See also snapshot.

O

OBDR capable device

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

obdrindex.dat

See IDB recovery file.

object

See backup object.

object consolidation

The process of merging a restore chain of a backup object, consisting of a full backup and at least one incremental backup, into a new, consolidated version of this object. The process is a part of the synthetic backup procedure. The result is a synthetic full backup of the specified backup object.

object consolidation session

A process that merges a restore chain of a backup object, consisting of a full backup and at least one incremental backup, into a new, consolidated version of this object.

object copy

A copy of a specific object version that is created during an object copy session or a backup session with object mirroring.

object copy session

A process that creates an additional copy of the backed up data on a different media set. During an object copy session, the selected backed up objects are copied from the source to the target media.

object copying

The process of copying selected object versions to a specific media set. You can

select object versions from one or several backup sessions to be copied.

object ID (Windows specific term)

The object IDs (OIDs) enable access to NTFS 5 files no matter where in the system the files reside. Data Protector treats the OIDs as alternate streams of the files.

object mirror

A copy of a backup object created using object mirroring. Object mirrors are often referred to as object copies.

object mirroring

The process of writing the same data to several media sets during a backup session. Data Protector enables you to mirror all or some backup objects to one or more media sets.

object verification

The process of verifying the data integrity of backup objects, from the Data Protector point of view, and the ability of Data Protector to deliver them to the required destination. The process can be used to provide a level of confidence in the ability to restore object versions created by backup, object copy, or object consolidation sessions.

object verification session

A process that verifies the data integrity of specified backup objects or object versions and the ability of selected Data Protector network components to deliver them to a specified host. Object verification sessions can be run interactively, or as specified in automated post-backup, or scheduled specifications.

offline backup

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

application. For simple backup methods (non ZDB), the database is generally put into a quiescent state that allows use by the backup system, but not the application, for the whole backup period (~minutes/hours). For instance, for backup to tape, until streaming of data to the tape is finished. For ZDB methods, the database is also put into the quiescent state, but for the period of the data replication process only (~seconds). Normal database operation can then be resumed for the rest of the backup process. See also zero downtime backup (ZDB) and online backup.

offline recovery

Offline recovery is performed if the Cell Manager is not accessible, for example, due to network problems. Only standalone and SCSI library devices can be used for offline recovery. Cell Manager can only be recovered offline.

offline redo log

See archived redo log.

ON-Bar (Informix Server specific term)

A backup and restore system for Informix Server. ON-Bar enables you to create a copy of your Informix Server data and later restore the data. The ON-Bar backup and restore system involves the following components: the onbar command, Data Protector as the backup solution, the XBSA interface, and 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 located in

the directory <INFORMIXDIR>\etc (on Windows systems) or <INFORMIXDIR>/etc/ (on UNIX systems).

online backup

A backup performed while a database application remains available for use. The database is placed into a special backup mode of operation for the time period that the backup application requires access to the original data objects. During this period, the database is fully operational, but there may be a small performance impact and log files may grow very quickly. For simple backup methods (non ZDB), backup mode is required for the whole backup period (~minutes/hours). For instance, for backup to tape, until streaming of data to tape is finished. For ZDB methods, backup mode is required for the short period of the data replication process only (~seconds). Normal database operation can then be resumed for the rest of the backup process. In some cases, transaction logs may also have to be backed up to allow a consistent database to be restored. See also zero downtime backup (ZDB) and offline backup.

online recovery

A type of the Internal Database recovery that you can use when the Cell Manager is accessible. In this case, the Cell Manager runs sessions, the sessions are logged into the IDB, and you can monitor the session progress using the GUI.

online redo log (Oracle specific term)

Redo logs that have not been archived, but are either available to the instance for recording database activity or are filled and waiting to be archived or reused. See also archived redo log.

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

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

P

P1S file

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

directory <Data_Protector_program_data>\Config\Server\dr\p1s (Windows systems) or /etc/opt/omni/dr/p1s (UNIX systems) with the filename recovery.p1s.

package (HP ServiceGuard and Veritas Cluster Specific Term)

A collection of resources (for example volume groups, application services, IP names, and addresses) that are needed to run a specific cluster-aware application.

pair status (HP P9000 XP Disk Array Family specific term)

The status of a disk pair (secondary volume and its corresponding primary volume) of a disk array of the HP P9000 XP Disk Array Family. Depending on the circumstances, the paired disks can be in various states. The following states are particularly important for the operation of the Data Protector HP P9000 XP Agent: PAIR - The secondary volume is prepared for zero downtime backup. If it is a mirror, it is completely synchronized, and if it is a volume to be used for snapshot storage, it is empty. SUSPENDED - The link between the disks is suspended. However, the pair relationship is still maintained, and the secondary disk can be prepared for zero downtime backup again at a later time. COPY - The disk pair is currently busy and making a transition into the PAIR state. If the secondary volume is a mirror, it is re-synchronizing with the primary volume, and if it is a volume to be used for snapshot storage, its contents are getting cleared.

parallel restore

Restoring backed up data to multiple disks at the same time (that is, in parallel) by running multiple Disk Agents, that receive data from one Media Agent. For the parallel restore to work, select data that is located on different disks or logical

volumes and during backup, the data from the different objects must have been sent to the same device using a concurrency of 2 or more. During a parallel restore, the data for multiple objects selected for restore is read from media at the same time, thereby improving performance.

parallelism

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

phase 0 of disaster recovery

Preparation for disaster recovery - the prerequisite condition for a successful disaster recovery.

phase 1 of disaster recovery

Installation and configuration of DR OS, establishing previous storage structure.

phase 2 of disaster recovery

Restoration of operating system (with all the configuration information that defines the environment) and Data Protector.

phase 3 of disaster recovery

Restoration of user and application data.

physical device

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

post-exec

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

pre- and post-exec commands

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

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 systems and as shell scripts on UNIX systems. See also post-exec.

primary volume (P-VOL) (HP P9000 XP Disk Array Family specific term)

An internal disk (LDEV) of a disk array of the HP P9000 XP Disk Array Family for which a secondary volume (S-VOL), either its mirror or a volume to be used for its snapshot storage, exists. In the HP CA P9000 XP and HP CA+BC P9000 XP configurations, primary volumes are located in the Main Control Unit (MCU). See also secondary volume (S-VOL) and Main Control Unit (MCU).

protection

See data protection and catalog protection.

public folder store (Microsoft Exchange Server specific term)

The part of the Information Store that maintains information in public folders. A

public folder store consists of a binary rich-text .edb file and a streaming native internet content .stm file.

public/private backed up data

When configuring a backup, you can select whether the backed up data will be: public, that is visible (and accessible for restore) to all Data Protector users private, that is, visible (and accessible for restore) only to the owner of the backup and administrators

R

RAID

Redundant Array of Independent Disks.

RAID Manager Library (HP P9000 XP Disk Array Family specific term)

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

RAID Manager P9000 XP (HP P9000 XP Disk Array Family specific term)

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

rawdisk backup

See disk image backup.

RCU

See Remote Control Unit (RCU).

RDBMS

Relational Database Management System.

RDF1/RDF2 (EMC Symmetrix specific term)

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

Recovery Catalog (Oracle specific term)

A set of Oracle tables and views that are used by Recovery Manager to store information about Oracle databases. This information is used by Recovery Manager to manage the backup, restore, and recovery of Oracle databases. The recovery catalog contains information about the physical schema of the Oracle target database, data file and archived log backup sets, data file copies, archived redo logs, and stored scripts.

Recovery Catalog Database (Oracle specific term)

An Oracle database that contains a recovery catalog schema. You should not store the recovery catalog in your target database.

recovery files (Oracle specific term)

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

Recovery Manager (RMAN) (Oracle specific term)

An Oracle command-line interface that directs an Oracle Server process to back up, restore, or recover the database it is connected to. RMAN uses either the

recovery catalog or the control file to store information about backups. This information can be used later in restore sessions.

RecoveryInfo

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

recycle or unprotect

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

redo log (Oracle specific term)

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

Remote Control Unit (RCU) (HP P9000 XP Disk Array Family specific term)

An HP P9000 XP Disk Array Family unit that acts as a slave device to the Main Control Unit (MCU) in the HP CA P9000 XP or HP CA+BC P9000 XP configuration. In bidirectional configurations, the RCU can also act as an MCU.

Removable Storage Management Database (Windows specific term)

A Windows service used for managing removable media (such as tapes and disks) and storage devices (libraries). Removable Storage allows applications

to access and share the same media resources.

reparse point (Windows specific term)

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

replica (ZDB specific term)

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

replica set (ZDB specific term)

A group of replicas, all created using the same backup specification. See also replica and replica set rotation.

replica set rotation (ZDB specific term)

The use of a replica set for regular backup production: Each time the same backup

specification requiring the use of a replica set is run, a new replica is created and added to the set, until the maximum number for the set is reached. After that, the oldest replica in the set is replaced, maintaining the maximum number of replicas in the set. See also replica and replica set.

restore chain

Backup images that are needed to restore a backed up object to the state it was in at the selected point in time. In general, a restore chain of an object consists of its full backup image and one or more related incremental backup images.

restore session

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

resync mode (HP P9000 XP Disk Array Family VSS provider specific term)

One of two P9000 XP Array VSS hardware provider operation modes. When the P9000 XP Array provider is in the resync mode, the source volume (P-VOL) and its replica (S-VOL) are in the suspended mirror relationship after a backup. The maximum number of replicas (S-VOLs per a P-VOL) rotated is three provided that MU range is 0-2 or 0, 1, 2. Restore from a backup in such a configuration is possible only by re-synchronization of an S-VOL with its P-VOL. See also VSS compliant mode, source volume, primary volume (P-VOL), replica, secondary volume (S-VOL), MU number, and replica set rotation.

RMAN (Oracle specific term)

See Recovery Manager.

RSM

The Data Protector Restore Session Manager controls restore and object

verification sessions. This process always runs on the Cell Manager system.

RSM (Windows specific term)

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

S

scanning

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

Scheduler

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

secondary volume (S-VOL) (HP P9000 XP Disk Array Family specific term)

An internal disk (LDEV) of a disk array of the HP P9000 XP Disk Array Family which is paired with another LDEV: a primary volume (P-VOL). It can act as a mirror of the P-VOL or as a volume to be used for the P-VOL's snapshot storage. An S-VOL is assigned a SCSI address different from the one used for the P-VOL. In an HP CA P9000 XP configuration, the S-VOLs acting as mirrors can be used as failover devices in a MetroCluster configuration. See also primary volume (P-VOL) and Main Control Unit (MCU).

session

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

session ID

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

session key

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

shadow copy (Microsoft VSS specific term)

A volume that represents a duplicate of the original volume at a certain point in time. The data is then backed up from the shadow copy and not from the original volume. The original volume continues to change as the backup process continues, but the shadow copy of the volume remains constant. See also Microsoft Volume Shadow Copy Service and replica.

shadow copy provider (Microsoft VSS specific term)

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

shadow copy set (Microsoft VSS specific term)

A collection of shadow copies created at the same point in time. See also shadow copy and replica set.

shared disks

A Windows disk on another system that has been made available to other users on the network. Systems with shared disks can be backed up without a Data Protector Disk Agent installed.

Site Replication Service (Microsoft Exchange Server specific term)

The Microsoft Exchange Server service that permits compatibility with Microsoft Exchange Server 5.5 by emulating the Exchange Server 5.5 directory service. See also Information Store and Key Management Service.

slot

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

SMB

See split mirror backup.

SMBF

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

SMI-S Agent (SMISA)

See HP P6000 / HP 3PAR SMI-S Agent.

snapshot (HP P4000 SAN Solutions, HP P6000 EVA Disk Array Family, HP P9000 XP Disk Array Family, and HP 3PAR StoreServ Storage specific term)

A type of target volumes created using a specific replication technology.

Depending on the disk array model and the chosen replication technique, a range of snapshot types with different characteristics is available. Basically, each snapshot may be either a virtual copy, still reliant upon the contents of the source volume, or an independent duplicate (clone) of the source volume. See also replica and snapshot creation.

snapshot backup

See ZDB to tape, ZDB to disk, and ZDB to disk+tape.

snapshot creation (HP P4000 SAN Solutions, HP P6000 EVA Disk Array Family, HP P9000 XP Disk Array Family, and HP 3PAR StoreServ Storage specific term)

A replica creation process in which copies of the selected source volumes are created using storage virtualization technology. Such a replica is considered to be created at a particular point in time, and is immediately available for use. However, with certain snapshot types, a background data copying process continues to run on the disk array after the moment of the replica creation. See also snapshot.

source (R1) device (EMC Symmetrix specific term)

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

source volume (ZDB specific term)

A storage volume containing data to be replicated.

sparse file

A file that contains data with portions of empty blocks. Examples are: -A matrix in which some or much of the data contains zeros -files from image applications -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 P9000 XP Disk Array Family specific term)

A type of target volumes created using a specific replication technology. A split-mirror replica provides independent duplicates (clones) of the source volumes. See also replica and split mirror creation.

split mirror backup (EMC Symmetrix specific term)

See ZDB to tape.

split mirror backup (HP P9000 XP Disk Array Family specific term)

See ZDB to tape, ZDB to disk, and ZDB to disk+tape.

split mirror creation (EMC Symmetrix and HP P9000 XP Disk Array Family specific term)

A replica creation technique, in which a pre-configured set of target volumes (a mirror) is kept synchronized with a set of source volumes until the time at which a replica of the contents of the source volumes is required. Then, the synchronization is stopped (the mirror is split) and a split mirror replica of the source volumes at the time of the split remains in the target volumes. See also split mirror.

split mirror restore (EMC Symmetrix and HP P9000 XP Disk Array Family specific term)

A process in which data backed up in a ZDB-to-tape or a ZDB-to-disk+tape session is first copied from the backup media to a replica, and from the replica to the source volumes afterwards. Individual backup objects or complete sessions can be restored using this method. See also ZDB to tape, ZDB to disk+tape, and replica.

sqlhosts file or registry (Informix Server specific term)

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

SRD file

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 (SSEA)

See HP P9000 XP Agent.

sst.conf file

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

st.conf file

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

stackers

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

standalone file device

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

Storage Group (Microsoft Exchange Server specific term)

A collection of mailbox stores and public folder stores that share a set of transaction log files. Exchange Server manages each storage group with a separate server process.

storage volume (ZDB specific term)

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.

Typically, these can be created or exist within a storage system such as a disk array.

StorageTek ACS library (StorageTek specific term)

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

switchover

See failover.

Sybase Backup Server API (Sybase specific term)

An industry-standard interface developed for the exchange of backup and recovery information between a Sybase SQL Server and a backup solution like Data Protector.

Sybase SQL Server (Sybase specific term)

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

SYMA

See EMC Symmetrix Agent.

synthetic backup

A backup solution that produces a synthetic full backup, an equivalent to a conventional full backup in terms of data, without putting stress on the production servers or the network. A synthetic full backup is created from a previous full backup and any number of incremental backups.

synthetic full backup

The result of an object consolidation operation, where a restore chain of a backup objects is merged into a new, synthetic full version of this object. A synthetic full backup is equivalent to a conventional full backup in terms of restore speed.

System Backup to Tape (SBT) (Oracle specific term)

An Oracle interface that handles the actions required to load, label, and unload correct backup devices when Oracle issues a backup or restore request.

system databases (Sybase specific term)

The four system databases on a newly installed Sybase SQL Server are the: - master database (master) -temporary database (tempdb) -system procedure database (sybsystemprocs) -model database (model).

System Recovery Data file

See SRD file.

System State (Windows specific term)

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

system volume/disk/partition

A volume/disk/partition containing operating system files. Microsoft

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

SysVol (Windows specific term)

A shared directory that stores the server copy of the domain's public files, which are replicated among all domain controllers in the domain.

T

tablespace

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

tapeless backup (ZDB specific term)

See ZDB to disk.

target (R2) device (EMC Symmetrix specific term)

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

target database (Oracle specific term)

In RMAN, the target database is the database that you are backing up or restoring.

target system (disaster recovery specific term)

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

target volume (ZDB specific term)

A storage volume to which data is replicated.

Terminal Services (Windows specific term)

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

thread (Microsoft SQL Server specific term)

An executable entity that belongs to only one process. It comprises a program counter, a user-mode stack, a kernel-mode stack, and a set of register values. Several threads can run at a time within one process.

TimeFinder (EMC Symmetrix specific term)

A business continuation process that creates an instant copy of single or multiple EMC 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

See Tape Library Unit.

TNSNAMES.ORA (Oracle and SAP R/3 specific term)

A network configuration file that contains connect descriptors mapped to service names. The file may be maintained centrally or locally, for use by all or individual clients.

transaction

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

transaction backup

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

transaction backup (Sybase and SQL specific term)

A backup of the transaction log providing a record of changes made since the last full or transaction backup.

transaction log backup

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

transaction log files

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

transaction log table (Sybase specific term)

A system table in which all changes to the database are automatically recorded.

transportable snapshot (Microsoft VSS specific term)

A shadow copy that is created on the application system and can be presented to the backup system which performs the backup. See also Microsoft Volume Shadow Copy Service (VSS).

U

unattended operation

See lights-out operation.

user account (Data Protector user account)

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

User Account Control (UAC)

A security component in Windows Vista 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.

user_restrictions file

A file that restricts specific user actions, which are available to Data Protector user groups according to the user rights assigned to them, to be performed only on specific systems of the Data Protector cell. Such restrictions apply only to Data Protector user groups other than admin and operator.

V

vaulting media

The process of storing media to a safe and remote place. The media are brought back to the data center when they are needed for restore or are ready for reuse in subsequent backups. The vaulting procedure depends on your company's backup strategy and policies for data protection/reliability.

verify

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

Virtual Controller Software (VCS) (HP P6000 EVA Disk Array Family specific term)

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

Virtual Device Interface (Microsoft SQL Server specific term)

This is a Microsoft SQL Server programming interface that allows fast backup and restore of large databases.

virtual disk (HP P6000 EVA Disk Array Family specific term)

A unit of storage allocated from a storage pool of a disk array of the HP P6000 EVA Disk Array Family. A virtual disk is the entity that can be replicated using the snapshot functionality of such disk array. See also source volume and target volume.

virtual full backup

An efficient type of synthetic backup where data is consolidated using pointers instead of being copied. It is performed if all the backups (the full backup, incremental backups, and the resulting virtual full backup) are written to a single file library that uses distributed file medium format.

Virtual Library System (VLS)

A disk-based data storage device hosting one or more virtual tape libraries (VTLs).

virtual server

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

virtual tape

An archival storage technology that backs up data to disk drives in the same way as if it were being stored on tape. Benefits of virtual tape systems include improved backup and recovery speed and lower operating costs. See also Virtual Library System (VLS) and virtual tape library (VTL).

virtual tape library (VTL)

Data storage virtualization software that is able to emulate tape devices and libraries thus providing the functionality of traditional tape-based storage. See also Virtual Library System (VLS).

volser

A VOLUME SERIAL number is a label on the medium to identify the physical tape used in very large libraries. A volser is a naming convention specific to ADIC/GRAU and StorageTek devices.

volume group

A unit of data storage in an LVM system. A volume group can consist of one or more physical volumes. There can be more than one volume group on the system.

volume mountpoint (Windows specific term)

An empty directory on a volume that can be used to mount another volume. The volume mount point acts as a gateway to

the target volume. Provided that the volume is mounted, users and applications can refer to the data on the mounted volume by the full (merged) filesystem path as if both volumes are one integral part.

Volume Shadow Copy Service

See Microsoft Volume Shadow Copy Service (VSS).

VSS

See Microsoft Volume Shadow Copy Service (VSS).

VSS compliant mode (HP P9000 XP Disk Array Family VSS provider specific term)

One of two P9000 XP Array VSS hardware provider operation modes. When the P9000 XP Array provider is in the VSS compliant mode, the source volume (P-VOL) and its replica (S-VOL) are in simplex, unpaired state after a backup. Therefore the number of replicas (S-VOLs per a P-VOL) rotated is not limited. Restore from a backup in such a configuration is possible only by switching 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.

W

Wake ONLAN

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

Web reporting

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

wildcard character

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

Windows configuration backup

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

Windows Registry

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

WINS server

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

writer (Microsoft VSS specific term)

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

X

XBSA Interface (Informix Server specific term)

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

Z

ZDB

See zero downtime backup.

ZDB 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 with specific disk array families, split mirror restore. See also zero downtime backup (ZDB), ZDB to disk, ZDB to tape, instant recovery, replica, and replica set rotation.

ZDB to tape (ZDB specific term)

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

zero downtime backup (ZDB)

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

Index

A

advanced search 33

B

backup 17

backup solutions 7

more information 10

backup specifications

configuring 14

backup, importing content databases
from 22

browsing sites 47

C

cache

management 21

removing content databases 37, 44

changing settings 39

CLI 41

command line reference 41

configuring 13

backup specifications 14

user rights 13

content databases 7

displaying information 46

exporting items 45

importing 22, 25

importing from backup 25

importing from filesystem 25

importing items 46

listing 43

removing from cache 37, 44

removing from disk 45

restoring 41

content recovery tasks 27

D

delay

command line 58

Granular Recovery Extension 58

disk space, verifying 43

displaying 47

E

exported items, listing 46

exporting from content database 45

F

farm information 46

filesystem, importing content databases
from 25

G

granular recovery

cache management 21

cache management, service is not
running error message 59

cache management, link not
accessible 54-55

monitoring import jobs 38

Granular Recovery Extension

changing settings 39

installing 9, 61

removing 61

starting 19

granularity 7

GUI, launching 19

I

- IIS application pools, verifying configuration 15
- import jobs, monitoring 38
- importing
 - content databases 22, 25
 - content databases from backup 22
 - content databases from filesystem 25
 - from backup 22
 - from filesystem 25
 - items from content database 46
- installation 9, 61
 - fails 49-50
- installing
 - Granular Recovery Extension 9, 61
- Internet Information Services 15

J

- jobs, monitoring 42

L

- launching the GUI 19
- listing exported items 46

M

- Microsoft SharePoint farm information 46
- monitoring jobs 42
- mount fails 50-51

O

- Office SharePoint farm information 46

P

- performing content recovery tasks 27
- prerequisites
 - before installing 9

- for recovering site items 29

R

- recover granularity capability 7
- recovering site items 28
 - to a folder 37
 - to a network share 36-37
 - to another farm 36
 - to another location 35, 44
 - to original site 44
- recovery 19
 - fails 53
- Recovery Web Application
 - settings 13
 - verifying configuration 13

- removal 61

- removing
 - content databases, from cache 37, 44
 - content databases, from disk 45
 - Granular Recovery Extension 61
 - restore jobs 43
- restore
 - fails 50-51, 53
 - jobs, removing 43

S

- setting
 - content databases, from disk 45
- settings, changing 39
- site items
 - advanced search 33
 - recovering 28
 - recovering to a folder 37

recovering to a network share 36-37

recovering to another farm 36

recovering to another location 35, 44

recovering to original site 44

sites

browsing 47

listing 47

starting

Granular Recovery Extension 19

T

tasks, content recovery 27

troubleshooting 49

U

user rights 13

V

verifying configuration

IIS application pools 15

Recovery Web Application 13

verifying target disk space 43

version 47

We appreciate your feedback!

If you have comments about this document, you can [contact the documentation team](#) by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on Granular Recovery Extension User Guide for Microsoft SharePoint Server (Data Protector 8.10)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to AutonomyTPFeedback@hpe.com.

