HP Data Protector

Software Version: 8.10

Granular Recovery Extension User Guide for VMware vSphere

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

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**

About this PDF Version of Online Help

This document is a PDF version of the online help. This PDF file is provided so you can easily print multiple topics from the help information or read the online help in PDF format. Because this content was originally created to be viewed as online help in a web browser, some topics may not be formatted properly. Some interactive topics may not be present in this PDF version. Those topics can be successfully printed from within the online help.

Contents

Chapter 1: Introduction

This guide describes Data Protector Granular Recovery Extension (GRE) for VMware vSphere.

> **Note:** The Data Protector GRE for VMware vSphere uses OpenSSL 1.0.2j.

Backup

The HP Data Protector Granular Recovery Extension for VMware vSphere relies on the Data Protector Virtual Environment integration to back up VMware vSphere virtual machine disks.

Restore and recovery

The HP Data Protector Granular Recovery Extension for VMware vSphere restores VMware vSphere virtual machine disks to a temporary restore location (a mount proxy system) and then recovers individual VMware virtual machine files instead of the whole virtual machine disks.

The benefits of this extension are the following:

- **Recovery granularity**

  The smallest item that can be restored is a disk, but from that restore, operators can recover individual files. This ability to recover items at file level helps minimize the use of disk space when dealing with large disks (100 GB or more). You can restore a set of virtual disks, mount them, and then only recover what you need.

- **Space-saving approach**

  Recovering items at file level is useful, especially when recovering large sized disks, avoiding extensive disk space usage. Only restoring a set of files of virtual disks, mounting these virtual machine disks and then recovering what is essential on the target system. You specify just the necessary data, specific files or folders to the recovery session, this avoids excessive use of disk space.

- **Integration into VMware vCenter Server**

  The extension is fully integrated into VMware vCenter Server, and has the same look and feel. This allows operators to request a restore and then recover individual items from virtual disks. Operators with Data Protector `start restore` right can also restore data by using Data Protector.

- **Operator-directed restore and recovery**

  Operators (VMware vCenter users) can be allowed to restore virtual disks and recover their own files. This enables operators to:

- request restore (the restore is handled by Granular Recovery Extension Administrators).
- recover single items independently or with minimal interference of Data Protector backup administrators (no need to be Data Protector backup administrators themselves or have Data Protector administrator rights).

  For detailed description of user roles and tasks, see "Granular Recovery Extension users" on page 16.

  For detailed configuration steps, see "Configuring Granular Recovery Extension Administrators using HP Data Protector" on page 23.

- **No Data Protector related expertise, low learning curve**

  Operators without any Data Protector knowledge, or expertise can request restores. After the Granular Recovery Extension administrator handles and performs the restore, operators can start recovery sessions. This way, operators can perform restore and recovery without ever starting Data Protector or planning any backups, or dealing with devices, managing disk spaces and so on.

- **Clear overview of restore and recovery objects**

  The HP Data Protector Granular Recovery Extension for VMware vSphere enables selection of objects at the file level, exactly the data needed. This increases the clarity, optimizing the overview of what is being restored or recovered.

- **Quickness and ease of use**

  The extension is quicker and easier to use than using the whole virtual machine restore and recovery solution. For example, it avoids additional configuration steps: start two virtual machines, copy the whole disk, configure network shares, IP names and addresses, and so on.

- **Monitoring restore progress**

  The HP Data Protector Granular Recovery Extension for VMware vSphere provides monitoring functionality. Operators without Data Protector backup administrators rights can monitor multiple restore requests, and recovery requests. Operators with Data Protector backup administrators rights handles these requests, have privileges to monitor multiple restore sessions, reject restore requests.

- **Recovery to different locations**

  Granular Recovery Extension Administrators can specify different locations for the restore and recovery of virtual disks.

  - Items can be first restored to different temporary locations:
    - different specified mount proxy systems, and different locations on a mount proxy system.

      If there is a shortage of disk space on a mount proxy system, they can add new virtual machine.

    - After the restore, the desired items can then be recovered to the following target locations:

        - virtual machines in online mode (with the same operating systems as the original backup).

          The virtual machine disks must be online for the recovery to be successful.

- **Security**

  The security of the virtual machines is based on the current VMware vCenter Server permissions. VMware virtual machine users can only access disks to which they are granted access in the VMware vCenter Server system. Access to secured data is granted to a limited number of users, so only certain users (the Granular Recovery Extension administrators) can access the extension in the VMware vCenter Administration component.

  In addition, access is restricted to requested virtual machines. This means that operators can mount and browse only disks on virtual machines to which they are granted access rights.

- **Users identification**

  When starting the extension, user rights are checked, identifying whether they are the Granular Recovery Extension administrators or operators. In addition, virtual machine operating systems credentials, a user name and a password must be specified before a recovery session can begin.

- **Specific access points**

  To access the Data Protector plug-in from VMware vSphere Web Client:

    - Open VMware vSphere Web Client and enter the user name and password. For administrative tasks, specify the credentials of the Data Protector user with the `Start restore` permission.

    - Click **Login**.

    - Under Inventories, expand the virtual machine node and select the desired virtual machine.

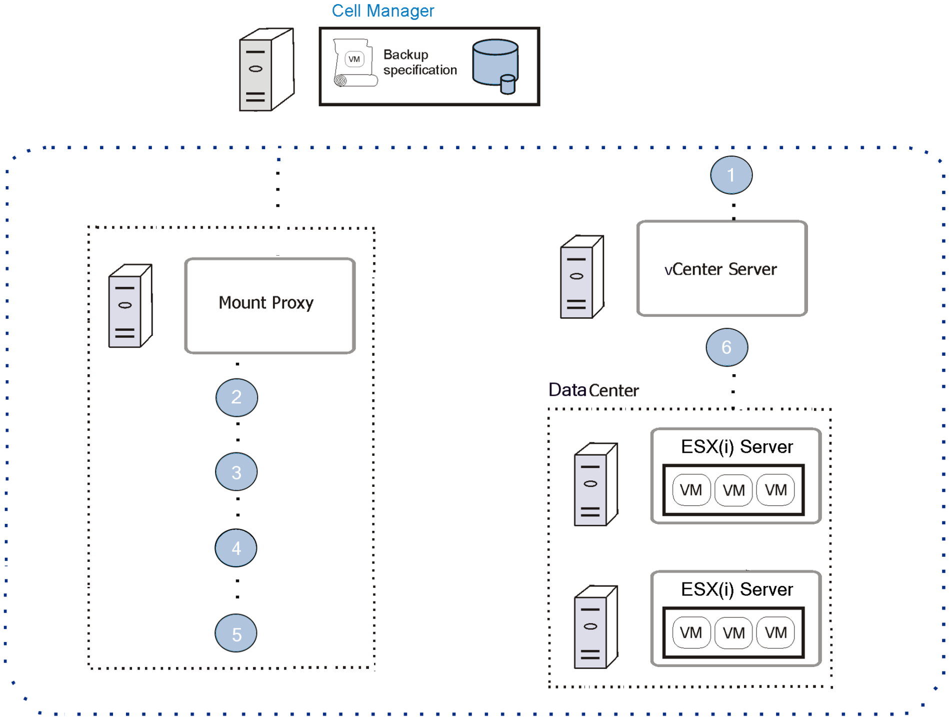
    - Click **Manage > HP Data Protector**.

      The HP Data Protector Granular Recovery Extension GUI opens in the operator or administrator mode.

Restore and recovery flow

The procedure for recovering virtual machine files is as follows:

Figure 1: Restore and recovery flow



1. **Request restore**

   A Granular Recovery Extension Operator (VMware vCenter user) requests a Granular Recovery Extension Administrator to perform a restore. The `VMware Granular Recovery Extension Agent` starts the restore session in conjunction with the `Virtual Environment Protection Agent` to restore the virtual machine files to the mount proxy system.

   For details on how to assign the Data Protector `Start restore` user right, see "Configuring Granular Recovery Extension Administrators using HP Data Protector" on page 23.

2. **Handle requests**

   In the Handle Requests page, the Administrator triggers restores of virtual machine files and folders that are submitted by Granular Recovery Extension Operators.

   When the Granular Recovery Extension Administrator clicks **Start restore**, the virtual machine files are copied to a restore location on the mount proxy system.

3. **Mount virtual machine disks**

   The Granular Recovery Extension Operator selects one of the available partitions and clicks **Browse**. The selected virtual machine disks are mounted and the virtual machine files can be browsed for a recovery.

   The mounted virtual machine disks are dismounted in the next step.

4. **Recover**

The Granular Recovery Extension Operator selects files and starts the recovery session. At this stage, the recover granularity is visible. Individual files are recovered to the vCenter Server environment. These files can then be recovered to the same location on the system or to a different location. Depending on the recovery options chosen, the files can be renamed, overwritten, or skipped. The location can be a different virtual machine, a different virtual machine disk, or a network share.

5. **Remove restored data files of virtual machine disks**

   The restored disks are deleted automatically after the retention period expires. If no more disk space is available on the mount proxy system, the administrator must remove virtual machine disks manually.

6. **Recover virtual machine disks**

   The default retention period for the restored files of virtual machine disks on the mount proxy system is 30 days. After that, the files are no longer available for recovery. After the retention period, the restored files are automatically deleted from the temporary restore location on the mount proxy system. It is an administrative task to change the default value according to the requirements of Granular Recovery Extension Operators.

   Note: Change retention period options in the **Settings** page. Changes only affect new requests.

Chapter 2: Installation

This chapter describes how to install the Data Protector Granular Recovery Extension for VMware vSphere.

Prerequisites

Data Protector:

- Install and configure Data Protector as described in the *HP Data Protector Installation and Licensing Guide*.

Data Protector Virtual Environment integration:

- Install and configure the Data Protector Virtual Environment integration as described in the *HP Data Protector Integration Guide for Virtualization Environments*, chapter *Data Protector Virtual Environment integration*.
- Install VMware tools 4.0 or later on each virtual machine on which you plan to perform restore sessions.

  For details on installing VMware tools, see the vSphere Client Help index: “upgrade VMware Tools”. You can download the VMware Tools installation package from the webpage http://www.vmware.com/download.

Mount proxy system:

- **Windows systems:**

  (Optional) Make sure to install the following utility if you want to use VIX API for file recovery:

  - VMware VIX API 1.13.0
- **Linux systems:**

  Make sure to install the following operating system components and utilities:

  - FUSE 2.7.3 or later
  - cifs-utils package (used for mounting Windows virtual machine disks on a Linux mount proxy system)
  - ntfs-3g package (used for mounting Windows virtual machine disks on a Linux mount proxy system)
  - VMware VIX API 1.12.2 (Optional; used for file recovery)
  - kpartx (required for disks with LVM partitions)

Note: Ensure that the ESX server hostname is resolved from the MountProxy. If you cannot access

> the ESX server from the MountProxy, add the ESX hostname and IP address in the host file.

vCenter Server:

- With vCenter Server 5.1, open the vCenter Tomcat web server configuration file and set the `autoDeploy` parameter to `true`. The file is located at:

  ```
  C:\Program Files\VMware\Infrastructure\tomcat\conf\server.xml
  ```

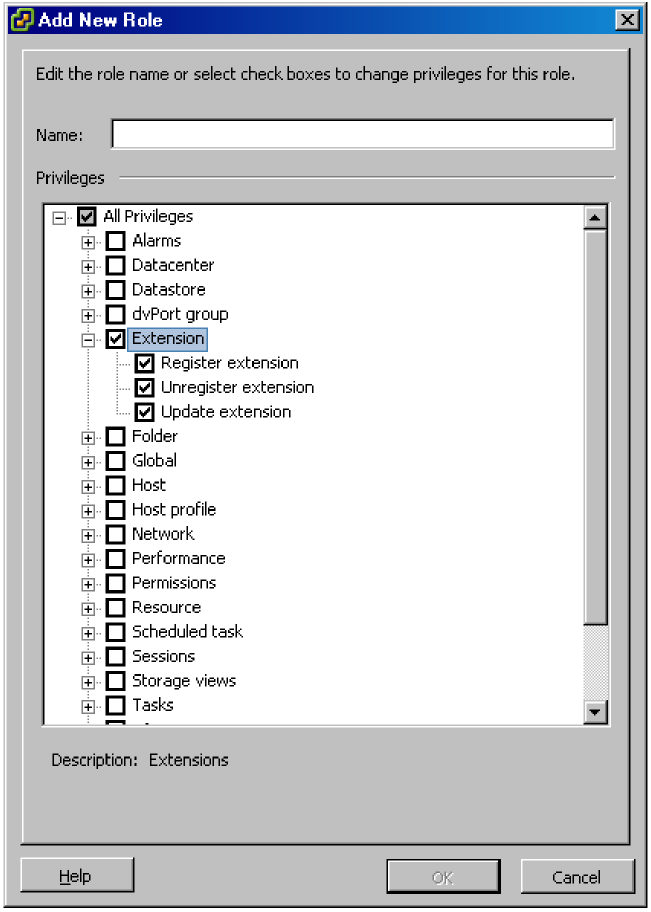
- Data Protector client

  To install the `VMware Granular Extension Web Plug-In` component to the vCenter Server, a Data Protector client has to be already installed on the vCenter Server.

  For details, see "Importing VMware vCenter Server" on page 18.

- To be able to install the `VMware Granular Extension Web Plug-In` component as a non-administrator user of the vCenter Server, make sure you have the vCenter Extension privilege set, with the Register extension, Unregister extension, and Update extension roles assigned.

Figure 2: Granting the Extension privileges to a vCenter Server user



Edit the role name or select check boxes to change privileges for this role.

Name:

Privileges

- ☑ All Privileges
  - ☐ Alarms
  - ☐ Datacenter
  - ☐ Datastore
  - ☐ dvPort group
  - ☑ Extension
    - ☑ Register extension
    - ☑ Unregister extension
    - ☑ Update extension
  - ☐ Folder
  - ☐ Global
  - ☐ Host
  - ☐ Host profile
  - ☐ Network
  - ☐ Performance
  - ☐ Permissions
  - ☐ Resource
  - ☐ Scheduled task
  - ☐ Sessions
  - ☐ Storage views
  - ☐ Tasks

Description: Extensions

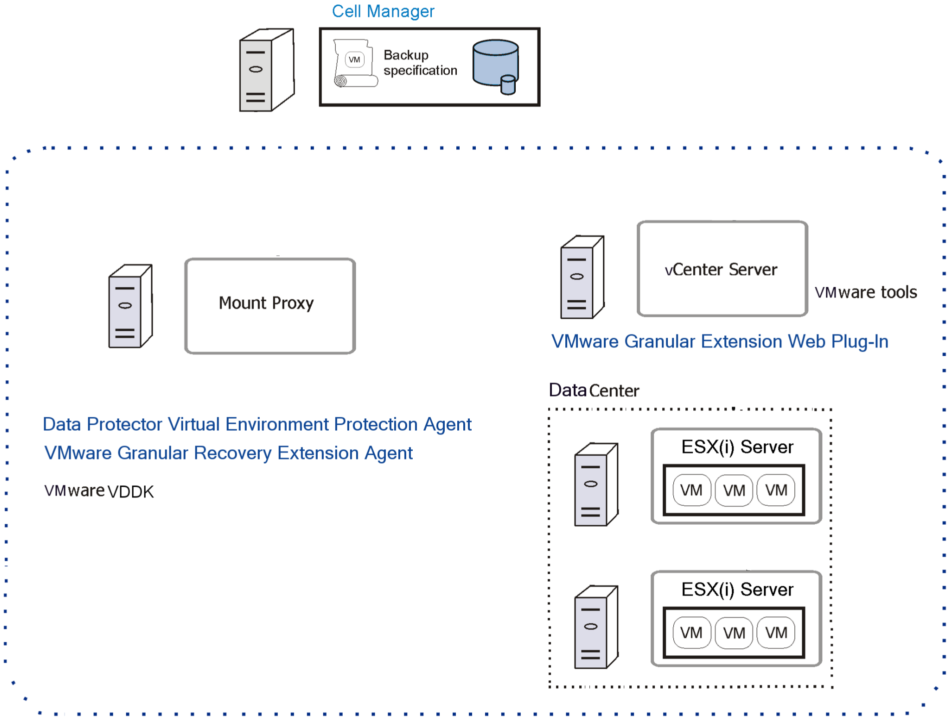
Considerations

- Remote installation of the HP Data Protector Granular Recovery Extension for VMware vSphere is recommended. If you cannot install the extension remotely, see "Local installation workaround" on page 73.
- Restart your system before installing the VMware GRE agent, if you have added or removed any of the HP Data Protector components or VMware VDDKs.
- Ensure that there are enough Linux loop devices on the mount proxy system. You need enough loop devices as the number of disks mounted to make the complete logical volume group available.

Granular Recovery Extension environment

In " Installing HP Data Protector Granular Recovery Extension " below, the HP Data Protector components appear in blue, and the VMware components appear in black.

Figure 3: Installing HP Data Protector Granular Recovery Extension



The HP Data Protector Granular Recovery Extension restores data using the Data Protector Virtual Environment integration; this extension is a recovery solution only. To use the extension, install and configure the following systems:

- Data Protector cell and client, imported with the `Virtual Environment Integration agent` enabled on it

- VMware vCenter Server system
- Mount proxy system

> **Note:** To ensure the proper functionality of the extension, do not install and configure both, a VMware vCenter Server system and a mount proxy system on the same client system.

For detailed Data Protector concepts, see the *HP Data Protector Concepts Guide*.

VMware vCenter Server system

The Data Protector Granular Recovery Extension (GRE) for VMware vSphere is integrated into the VMware vCenter Server. You access virtual machines using the vCenter vSphere Client. The HP Data Protector Granular Recovery Extension tab is added to the VMware vCenter Server interface.

> **Note:** The enhanced GUI for GRE supports the VMware vSphere Web Client from version 5.5.

Required Data Protector components

To use Data Protector Granular Recovery Extension for VMware vSphere, the following Data Protector components must be installed on the vCenter Server:

- A Data Protector client with any Data Protector component installed
- VMware Granular Extension Web Plug-In

For installation instructions, see the *HP Data Protector Installation and Licensing Guide*. If remote installation fails, see the "Local installation workaround" on page 73.

Mount proxy system

The HP Data Protector Granular Recovery Extension for VMware vSphere requires a mount proxy system as a temporary restore location between the original location and the target location on the VMware vCenter Server system. Any supported system, also a virtual machine, can be used as a mount proxy system. However, it is recommended to configure a dedicated system as the mount proxy system.

After a restore, files of virtual machine disks are located in a folder marked with the request ID. The folder contains a collection of virtual machine files, for example, vdmk, tmp files and so on. The virtual machine disks are not mounted yet. The mount session starts when you, as a VMware vCenter user, start browsing the files using the extension integrated in the vCenter environment.

The default retention period of a restored collection of virtual machine files is 30 days. You can change the setting as a Granular Recovery Extension administrator.

Only the selected files are recovered to the specified virtual machine disk target location in the VMware vCenter environment.

Your mount proxy system needs a sufficient disk space for the restored data. As a Granular Recovery Extension administrator, you can adjust the disk space on demand by attaching additional disks or by adding another mount proxy system.

For detailed description of data flow, see the "Restore and recovery flow" section in "Introduction" chapter.

For detailed list of tasks and description of user roles, see "Granular Recovery Extension users" below.

Required Data Protector components

To use the Data Protector Granular Recovery Extension for VMware vSphere, the following Data Protector components must be installed on the mount proxy system:

- `Virtual Environment Integration`
- `VMware Granular Recovery Extension Agent`

For installation instructions, see the *HP Data Protector Installation and Licensing Guide*. If remote installation fails, see "Local installation workaround" on page 73.

Granular Recovery Extension users

There is a distinction between two user roles:

- **Administrators**

  The administrators are VMware vCenter Server users that have the Data Protector `start restore` user right assigned. These users can perform additional administrative tasks, for detailed procedures, see the following sections of "Restore and recovery - VMware vSphere Web Client" on page 46:

  - Accessing the Data Protector plug-in from VMware vSphere Web Client
  - Configuring mount proxy systems
  - Handling restore requests
  - Triggering restore sessions
  - Rejecting restore requests
  - Monitoring restore requests
  - Recovering files from virtual machines
  - Removing virtual machine disks
  - About Granular Recovery Extension

- **Operators**

The operators are VMware vCenter Server users. These users can perform operational tasks, for detailed procedures, see the following sections of "Restore and recovery - VMware vSphere Web Client" on page 46:

- Accessing the Data Protector plug-in from VMware vSphere Web Client
- Requesting restores
- Monitoring restore requests
- Recovering files from virtual machines
- About Granular Recovery Extension

For details on configuring the Data Protector `start restore` user right, see "Configuring Granular Recovery Extension Administrators using HP Data Protector" on page 23.

Chapter 3: Configuration

This chapter describes the configuration steps that you need to follow.

Meeting Data Protector configuration requirements for Granular Recovery Extension

VMware vCenter Server system

Importing VMware vCenter Server

Prerequisite

You need to have the Data Protector client installed on the VMware vCenter Server.

Procedure

1. Install the Data Protector client with `Disk` or `Media Agent` component on the vCenter Server.
2. Import the Data Protector client as VMware vCenter.

   For more information, see the *HP Data Protector Installation and Licensing Guide*.

Configuring a Granular Recovery Extension VMware user group

Configuring a Granular Recovery Extension for VMware vSphere user group

Prerequisite

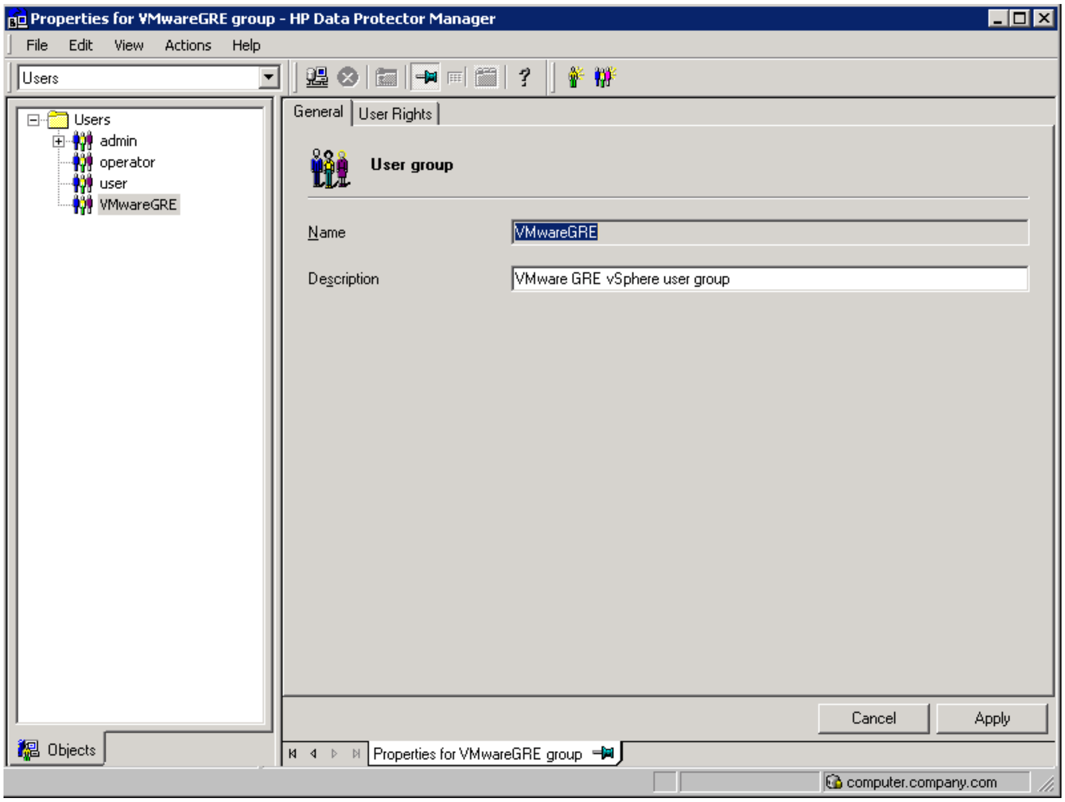
You need to have the Data Protector `User configuration` user right assigned.

Procedure

To create a Data Protector group for the Granular Recovery Extension VMware using the HP Data Protector GUI (Data Protector Manager):

1. In the Context List, click **Users**.
2. In the Scoping Pane, right-click **Users**.

Figure 4: GRE VMware vSphere user group


Properties for VMwareGRE group - HP Data Protector Manager
File Edit View Actions Help
Users
Users
admin
operator
user
VMwareGRE
Objects
General
User Rights
User group
Cancel
Apply
Properties for VMwareGRE group
computer.company.com

Name: VMwareGRE

Description: VMware GRE vSphere user group

3. Click **Add User Group** to open the wizard.

4. Under General, type the **Name**: `GRE VMware` and **Description** of the new group: `Granular Recovery Extension for VMware administrators`.

5. Click **Next**

6. Set the `start restore` user right for the group.

7. Click **Finish** to exit the wizard.

   The new GRE VMware user group is added to Data Protector.

   To add users, see "Adding users to the GRE VMware group" below.

Adding users to the GRE VMware group

Prerequisite

You need to have the `User configuration` user right to be able to add users.

Procedure

To add users to the GRE VMware group:

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

2. In the Scoping Pane, expand **Users**.

3. Right-click the user group to which you want to add a user.

4. Click **Add/Delete Users** to open the wizard.

5. In the Add/Delete Users dialog, enter the specific user properties.

   When entering **Name** and **Group/Domain**, make sure you enter information about an existing user on your network.

   To make sure that GRE VMware Administrators have an access to the administrative entry point of the extension, specify the following information:

   Type : Windows

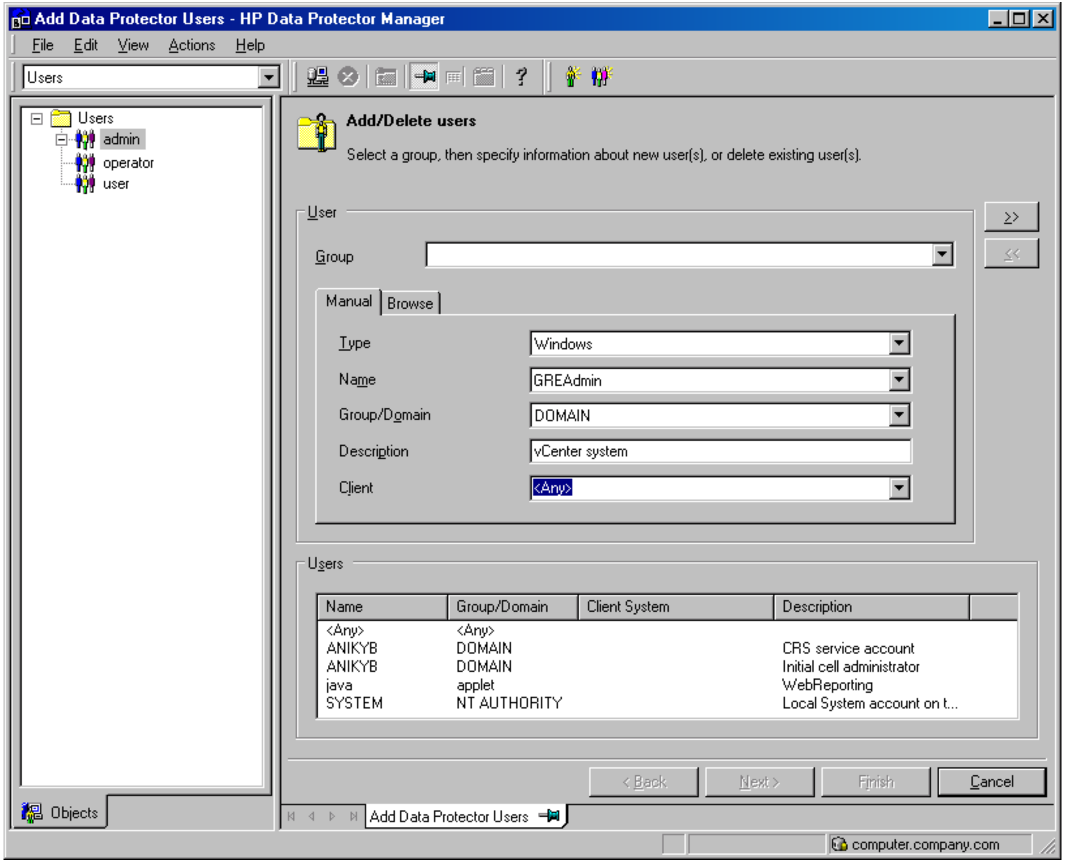
   Name : *`username`*

   Group/Domain : `GRE VMware user group, VCENTER`

   Client : *`VCenterSystemName`*

   The GRE VMware Administrators must be added to the vSphere permission tab. Set the user's role to Administrator. For detailed procedure, see "Configuring vCenter Server" on page 25.

Figure 5: Adding user domain information



Add/Delete users

Select a group, then specify information about new user(s), or delete existing user(s).

User

Group:

Type: Windows

Name: GREAdmin

Group/Domain: DOMAIN

Description: vCenter system

Client: <Any>

Users

Name	Group/Domain	Client System	Description
<Any>	<Any>		
ANIKYB	DOMAIN		CRS service account
ANIKYB	DOMAIN		Initial cell administrator
java	applet		WebReporting
SYSTEM	NT AUTHORITY		Local System account on t...

6. Click the arrow button **>>** to add the user to the user list.

7. Click **Finish** to exit the wizard.

The user is added to the Granular Recovery Extension for VMware administrators group and has the `start restore` user right assigned.

Tip: You can also delete a user by selecting the user in the user list and clicking **<<**.

For a detailed description of user roles and tasks, see "Granular Recovery Extension users" on page 16.

For details on how to configure Data Protector to meet the extension's user rights requirements, see "Configuring Granular Recovery Extension Administrators using HP Data Protector" on page 23.

Note: Granular Recovery Extension administrators should be added to the GRE VMware group, but you do not need to add Granular Recovery Extension operators. The Granular Recovery Extension operators can perform their tasks without using Data Protector.

Adding an Inet user account to the Data Protector Admin group

To ensure the proper functioning of the `VMware Granular Recovery Extension Agent`, and the `VMware Granular Extension Web Plug-In` extension components, you need to add an Inet user account to the Data Protector `Admin` user group on the following systems:

1. In the Context List, click **Users**.
2. In the Scoping Pane, expand **Users**.
3. Right-click the **admin** user group to which you want to add a user.
4. Click **Add/Delete Users** to open the wizard.
5. In the Add/Delete Users dialog, enter the following user properties:

   Mount proxy system:

   Type : `Windows` or `Linux`

   Name : `SYSTEM` or `root`

   Group/Domain : `NT AUTHORITY` or `root`

   > **Note:** Make sure that you specify an existing user account on your network.

   Client : *`MountProxySystemName`*

   vCenter Server system:

   Type : `Windows` or `Linux`

   Name : the account under which the VMware vCenter Server runs (by default, SYSTEM or root).

   Group/Domain : the account group/domain under which the VMware vCenter Server runs (by default, NT AUTHORITY or root).

   Client : *`VCenterSystemName`*.
6. Click the arrow button **>>** to add the user to the user list.
7. Click **Finish** to exit the wizard.

   The user accounts are added to the Data Protector `admin` user group with the user rights assigned to the group.

> **Note:** The Data Protector Inet uses `SYSTEM, NT AUTHORITY` which is used in the Data Protector

Local system account (in Windows operating system).

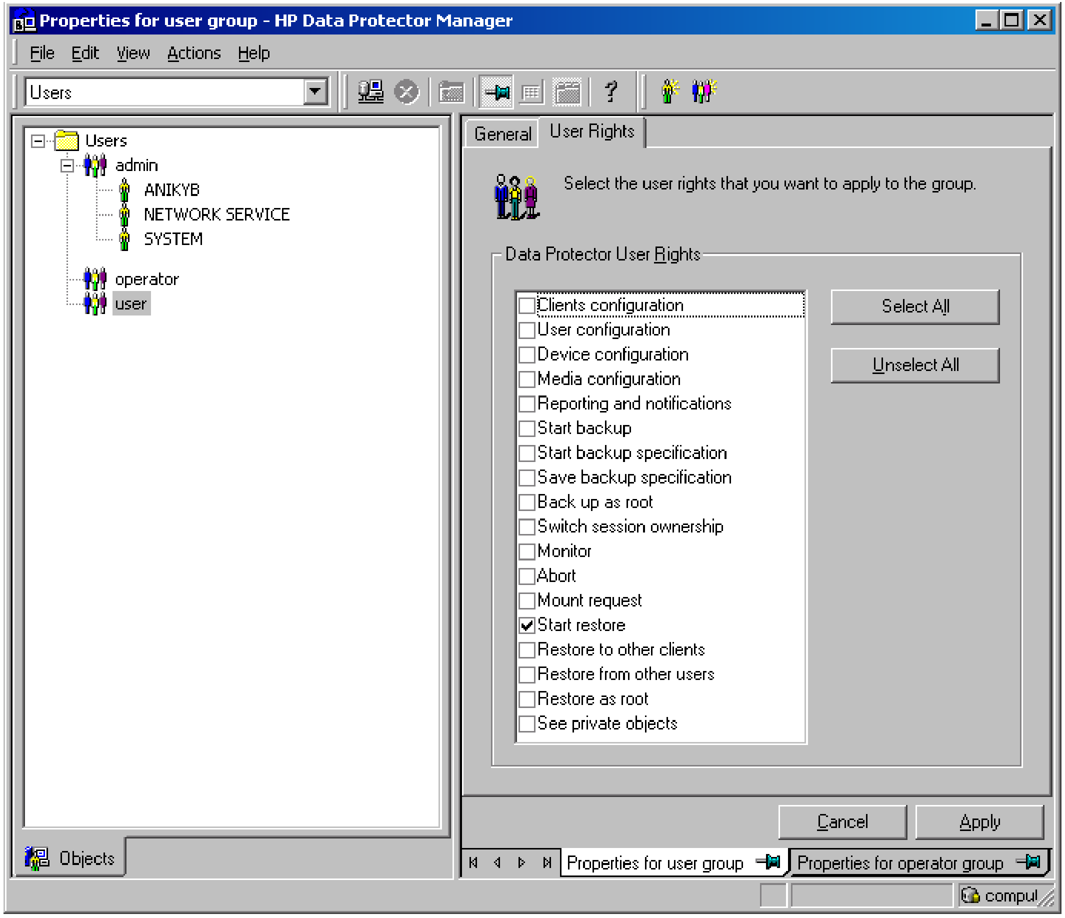
Configuring Granular Recovery Extension Administrators using HP Data Protector

Procedure

To enable the Granular Recovery Extension administrators a free access to the extension and their tasks, proceed as follows using the HP Data Protector GUI (**Data Protector Manager**):

1. In the Context list, select **Users**.
2. Right-click the GRE VMware user group.
3. Click **Properties** and then click the **User Rights** tab.
4. Make sure the Data Protector user account is assigned the Data Protector `Start restore` user right.

Figure 6: Data Protector user rights



Select the user rights that you want to apply to the group.

Data Protector User Rights

- ☐ Clients configuration
- ☐ User configuration
- ☐ Device configuration
- ☐ Media configuration
- ☐ Reporting and notifications
- ☐ Start backup
- ☐ Start backup specification
- ☐ Save backup specification
- ☐ Back up as root
- ☐ Switch session ownership
- ☐ Monitor
- ☐ Abort
- ☐ Mount request
- ☑ Start restore
- ☐ Restore to other clients
- ☐ Restore from other users
- ☐ Restore as root
- ☐ See private objects

> **Note:** In the Granular Recovery Extension for VMware vSphere environment, the administrators are Data Protector users assigned the Data Protector `Start restore` user right.
>
> For a detailed description of user roles and tasks, see "Granular Recovery Extension users" on page 16.
>
> The specified user rights are assigned to the user group and to all users belonging to the group.
>
> It is recommended to create a specific VMware GRE vSphere user group to which the extension's administrators belong.

For details, see "Configuring a Granular Recovery Extension VMware user group" on page 18.

Configuring your systems for VMware vSphere purposes

Configuring Windows Firewall exceptions

Setting VMware Granular Recovery Extension Agent under Firewall exceptions

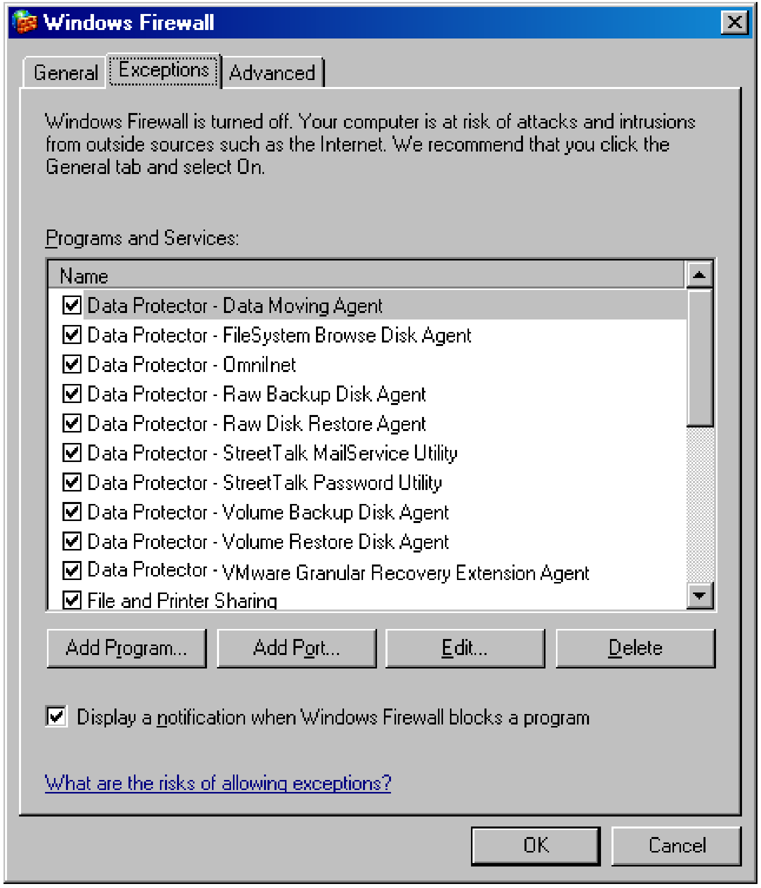
Procedure

To ensure communication between the mount proxy system component and the extension on the vCenter Server:

1. Check your Windows Firewall Exceptions list.

2. Make sure the `VMware Granular Recovery Extension Agent` (`vmwaregre-agent.exe`) is in the list of Windows Firewall exceptions, on both the mount proxy system and the vCenter Server systems:

Figure 7: Windows Firewall Exceptions tab



Windows Firewall is turned off. Your computer is at risk of attacks and intrusions from outside sources such as the Internet. We recommend that you click the General tab and select On.

Programs and Services:

Name
☑ Data Protector - Data Moving Agent
☑ Data Protector - FileSystem Browse Disk Agent
☑ Data Protector - OmniInet
☑ Data Protector - Raw Backup Disk Agent
☑ Data Protector - Raw Disk Restore Agent
☑ Data Protector - StreetTalk MailService Utility
☑ Data Protector - StreetTalk Password Utility
☑ Data Protector - Volume Backup Disk Agent
☑ Data Protector - Volume Restore Disk Agent
☑ Data Protector - VMware Granular Recovery Extension Agent
☑ File and Printer Sharing

☑ Display a notification when Windows Firewall blocks a program

What are the risks of allowing exceptions?

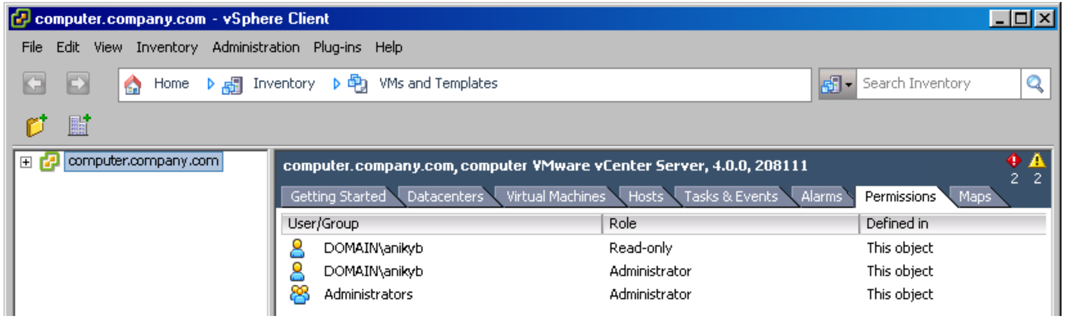
Note: Only inbound firewall rules are automatically created during the installation of the Granular Recovery Extension for VMware vSphere. You need to manually create any outbound firewall rule. This is required for communication between the extension's components and the vCenter Server. For the required port ranges, see the *HP Data Protector Help* index: “firewall support”.

Configuring vCenter Server

Procedure

Under Permissions tab, set the Administrator permission role to the user account on your vCenter Server. Read-only does not provide all the necessary permissions. For reference, see " vCenter Server role options" on the next page.

Figure 8: vCenter Server role options



User/Group	Role	Defined in
DOMAIN\anikyb	Read-only	This object
DOMAIN\anikyb	Administrator	This object
Administrators	Administrator	This object

Configuring Encrypted Control Communication

If you have enabled encrypted control communication (ECC) in the Data Protector cell, ensure that one of the following conditions are met:

- ECC is enabled on both the mount proxy and the vCenter Server system.
- ECC is disabled on both the mount proxy and the vCenter Server system.

The following configurations are not supported:

- ECC is enabled on the mount proxy and disabled on the vCenter Server system.
- ECC is disabled on the mount proxy and enabled on the vCenter Server system.

Chapter 4: Backup

The HP Data Protector Granular Recovery Extension for VMware vSphere relies on the Data Protector Virtual Environment integration for VMware vSphere to back up VMware vSphere virtual machine disks. Back up your VMware vSphere data using the Data Protector backup solution. For details, see the *HP Data Protector Integration Guide for Virtualization Environments*, the chapter about the Data Protector Virtual Environment integration.

The extension supports full, incremental and differential backups. For details on Data Protector backup types, see the *HP Data Protector Help* index: “backup types”. A backup of virtual machines with user snapshots and quiescence is also supported.

Note: The Granular Recovery Extension for VMware vSphere uses the same procedure for recovery of all VMware vSphere data. The procedure does not depend on the backup type.

It is recommended to set up a dedicated mount proxy system. The extension will need to allocate extendable disk space (disk space that can be made larger) for the temporary restore location of virtual machine disks.

Chapter 5: Restore and recovery

Considerations

- The Granular Recovery Extension for VMware vSphere does not support a cross-platform recovery. A recovery of Windows virtual machine files from a Windows virtual machine to a Linux virtual machine and the other way around is not supported. However, you can perform a restore of Windows virtual machine disks to different mount proxy system platforms. A restore of Linux virtual machine disks to Windows mount proxy systems is not supported.
- Consider a VMware vSphere Web Client with two or more vCenters and each vCenter being a member of different Data Protector cell configuration. If each Data Protector cell contains the same user in user lists but with a different set of permissions, the user acquires privileges from the Data Protector cell on which the VMware GRE agent for selected vCenter starts to run first.
- You cannot recover a virtual machine from an incremental and differential backup, if the virtual machine name in the vSphere Center has been changed after full backup.
- If two operators connect remotely using the VMware vSphere Client with the same user account and browse one partition of a virtual machine disk simultaneously, once the first partition is mounted the second partition is dismounted. Parallel mounting of partitions is not supported.
- The extension displays the whole restore chain. When browsing through files, the objects displayed contain the whole restore chain: a full backup of the object and any number of related incremental backups.
- You may experience slow performance when browsing too many files and sub files in a folder.

Note: To fine-tune the display of the Granular Recovery Extension interface, use Windows Internet Explorer 8 or a later version.

For a list of supported environments, see the latest support matrices at http://support.openview.hp.com/selfsolve/manuals.

Limitations

Data Protector Granular Recovery Extension (GRE) for VMware vSphere has certain limitations.

You cannot:

- Recover empty folders.
- Perform VIX related recovery for files or folders with non-ASCII characters in their names.
- Perform the recovery of files from Windows 2012 Resilient File System (ReFS) file system as ReFS is mounted as read-only by VixMntApi, though VMware GRE requires the mounted file system to be

writeable.

- Recover files with longer path names. Those files are accessible on the mount proxy after the partition is mounted.

> **Note:** You must ensure that the file path in the mount point and the selected disk does not exceed 260 characters for the disk mounted on a mount proxy.

- List the skipped and failed files in recovery details, if the target machine does not have sufficient disk space.
- Only one mount proxy host per operating system platform is supported.

Restoration and preservation of Ownerships, ACLs, File attributes, and Alternate data streams

The tables below list the file properties, and the preservation conditions.

Windows VM/Windows mount proxy

File properties	Files	Directories
Ownership	Yes	No
ACLs	Yes	No
File attributes	Yes. Some file attributes are not preserved due to operating system limitations, such as hidden file attribute, compressed file attribute, and encrypted file.	No
Alternate data streams	Yes	No

Linux VM/Linux mount proxy

File properties	Files	Directories

Ownership	Yes. Files that do not have `root:root` ownership are preserved. Files with `root:root` ownership are not preserved, because the ownership becomes `nobody:nobody`. The ownership settings depend on the NFS settings `/etc/exports` that is set in the target Linux system.	No. Ownership becomes `root:root`.
ACLs	No	No
File attributes `e:Extent format` is set as a default value.	No	No
Permissions	Yes	No

Note: If VIX is used, none of the file properties are preserved.

If the Ownership, ACLs, File attributes, and Alternate data streams are not preserved by the GRE operation, the restored objects have the VM operating system credentials (mentioned in the GRE page) as their properties.

The following limitations apply, if a virtual machine **is** on the network:

- A Linux target virtual machine and a Linux mount proxy system:
  - POSIX ACLs are not preserved during recovery.
  - To preserve ownership and permission bits UID/GUID on a target virtual machine and a mount proxy system, both must be mapped. A network share server should be properly configured to support it.
  - The LVM logical volumes configured on a non-partitioned disk are not supported by the VDDK VIX mount API.

    Note: You need to partition the disk before adding a volume group. The partitions reported in `fdisk –l` can only be considered.

Restore and recovery - VMware vSphere Desktop Client

Operator tasks

Opening the GUI of the HP Data Protector Granular Recovery Extension for VMware vSphere

Procedure

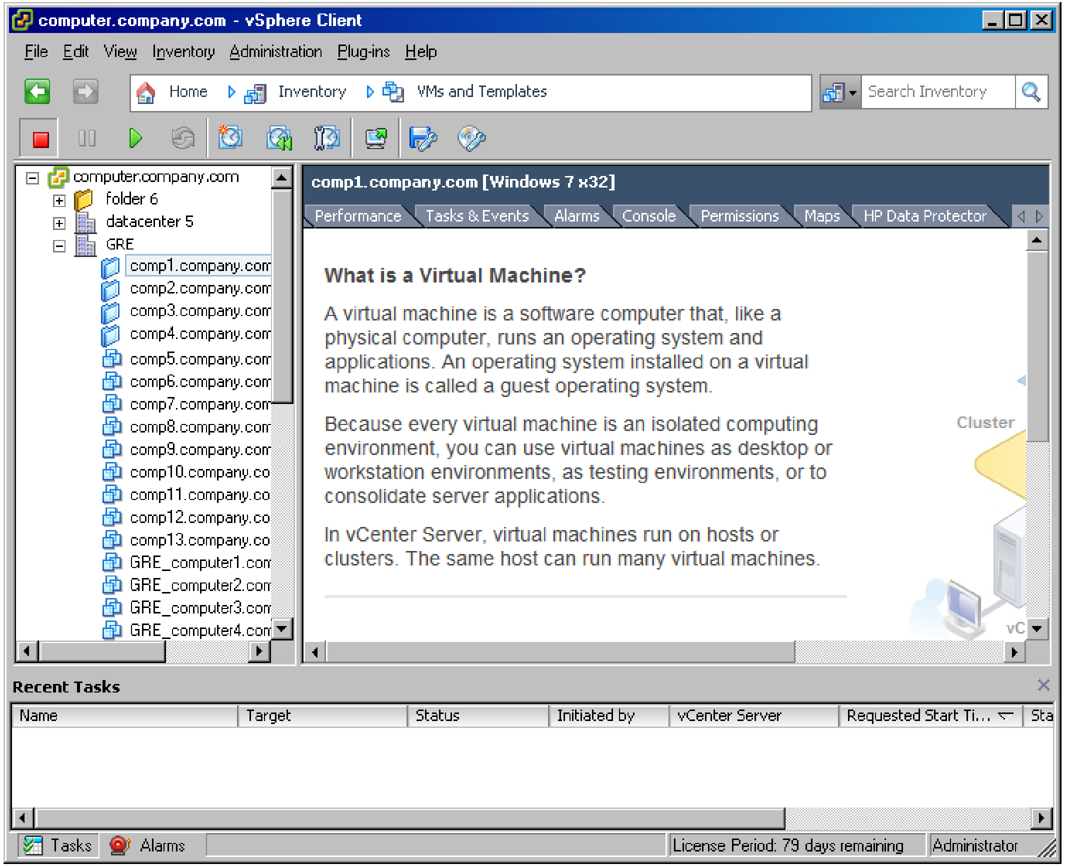
To open the GUI of the HP Data Protector Granular Recovery Extension for VMware vSphere:

1. Using the VMware vSphere Client, connect to the vCenter Server system and enter the user name and password.

2. In the VMware vSphere Client navigation bar, under the Inventory tab click **VMs and templates** and then expand the virtual machine browse tree. Select the desired virtual machine

3. Click the **HP Data Protector** tab.

Figure 9: Accessing the extension



What is a Virtual Machine?

A virtual machine is a software computer that, like a physical computer, runs an operating system and applications. An operating system installed on a virtual machine is called a guest operating system.

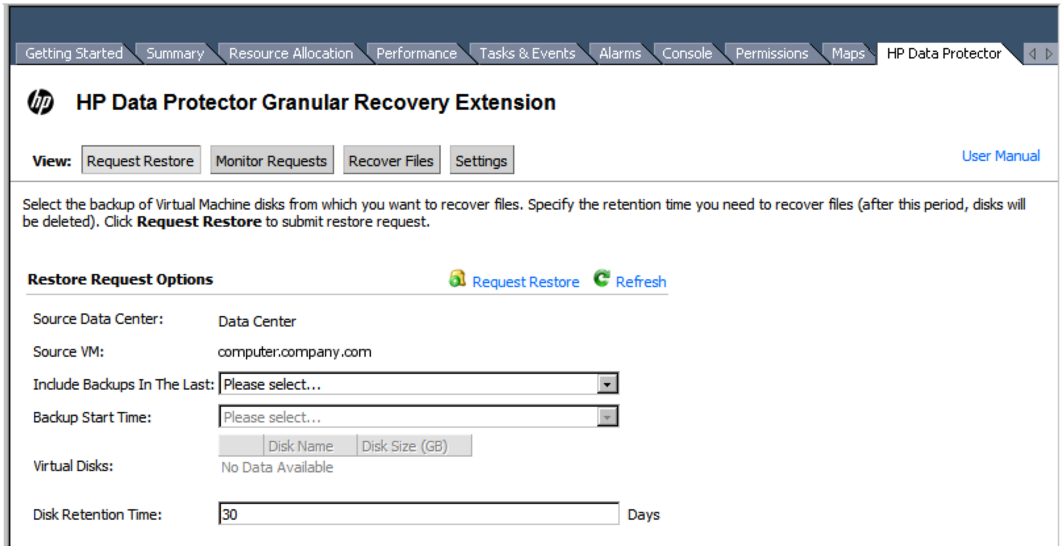
Because every virtual machine is an isolated computing environment, you can use virtual machines as desktop or workstation environments, as testing environments, or to consolidate server applications.

In vCenter Server, virtual machines run on hosts or clusters. The same host can run many virtual machines.

> **Important:** If you receive the security alert notification after clicking the HP Data Protector tab, you do not have the vSphere certificate installed on your system. Click **Yes** to open the extension. For details on how to obtain a valid vSphere certificate, see the VMware end-user documentation or Help index: "About vCenter Server Certificates" or "Replacing vCenter Server Certificates".

The HP Data Protector Granular Recovery Extension GUI is opened in the operator mode.

Figure 10: The Granular Recovery Extension GUI opened in the operator mode



Select the backup of Virtual Machine disks from which you want to recover files. Specify the retention time you need to recover files (after this period, disks will be deleted). Click **Request Restore** to submit restore request.

Restore Request Options

Source Data Center:	Data Center
Source VM:	computer.company.com
Include Backups In The Last:	Please select...
Backup Start Time:	Please select...
Virtual Disks:	No Data Available
Disk Retention Time:	30 Days

Requesting restores

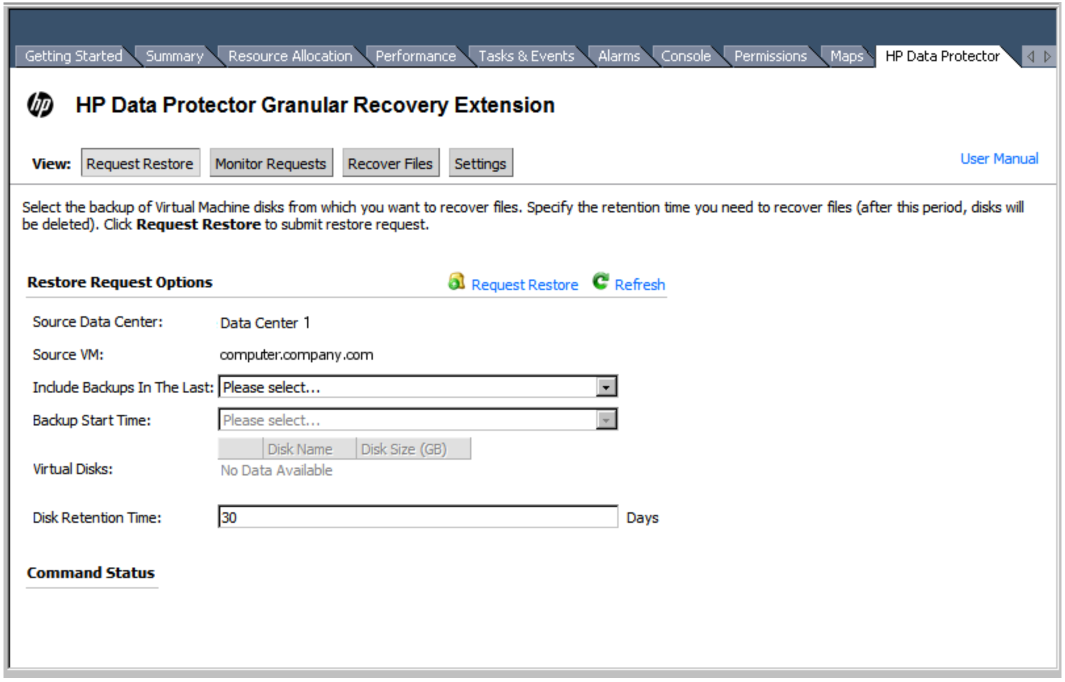
Procedure

To request restores:

1. In the HP Data Protector Granular Recovery Extension page, click **Request Restore**.

   The Restore Request Options page is displayed.

Figure 11: Restore request page



HP Data Protector Granular Recovery Extension

Select the backup of Virtual Machine disks from which you want to recover files. Specify the retention time you need to recover files (after this period, disks will be deleted). Click **Request Restore** to submit restore request.

Restore Request Options

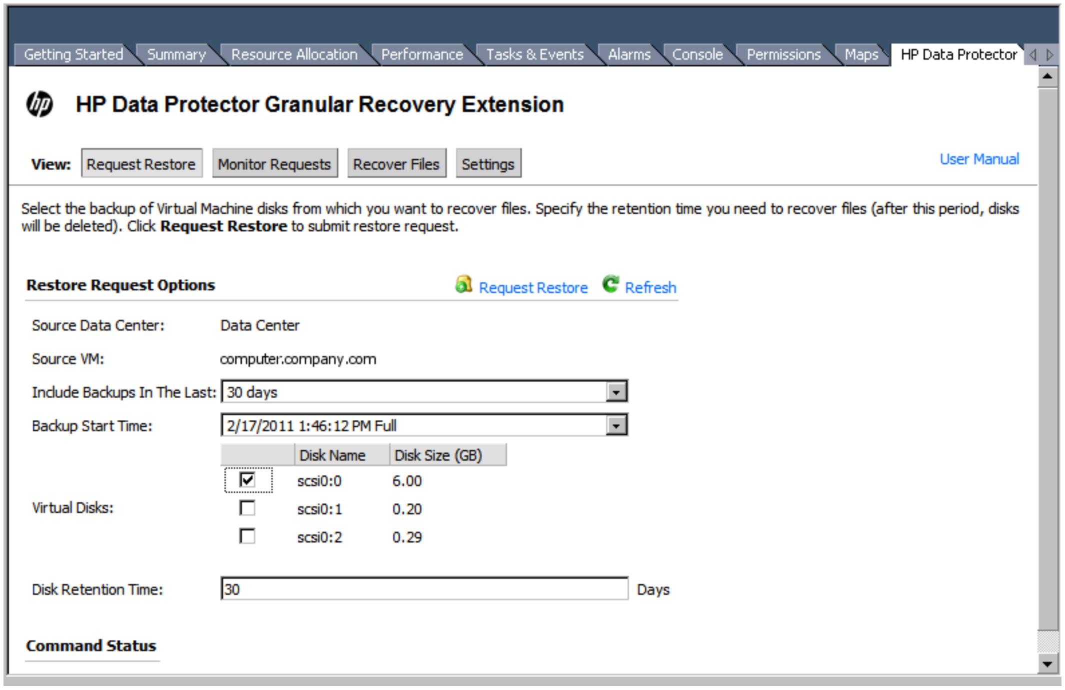
Source Data Center:	Data Center 1
Source VM:	computer.company.com
Include Backups In The Last:	Please select...
Backup Start Time:	Please select...
Virtual Disks:	Disk Name, Disk Size (GB) No Data Available
Disk Retention Time:	30 Days

Command Status

2. In the **Include Backups in The Last** drop-down list, select the backup period. In the **Backup Start Time** drop-down list, select the start date, time, and backup type of the backup.

3. Select the virtual machine disk to be restored.

Figure 12: Selecting virtual machine disks



HP Data Protector Granular Recovery Extension

Select the backup of Virtual Machine disks from which you want to recover files. Specify the retention time you need to recover files (after this period, disks will be deleted). Click **Request Restore** to submit restore request.

Restore Request Options

Source Data Center:	Data Center
Source VM:	computer.company.com
Include Backups In The Last:	30 days
Backup Start Time:	2/17/2011 1:46:12 PM Full
Disk Retention Time:	30 Days

Virtual Disks:

	Disk Name	Disk Size (GB)
☑	scsi0:0	6.00
□	scsi0:1	0.20
□	scsi0:2	0.29

Command Status

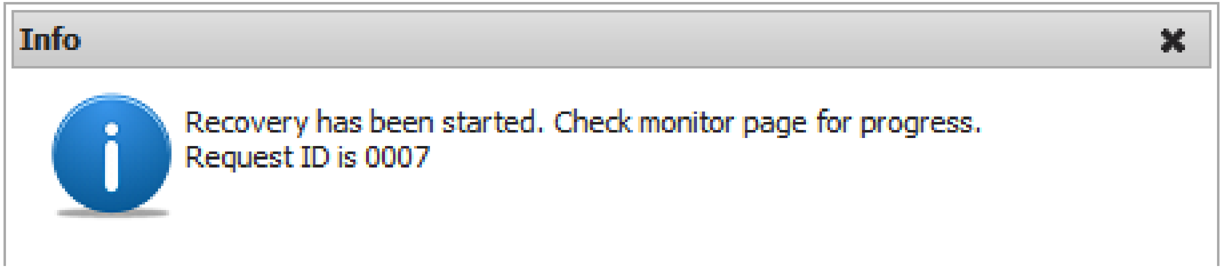
4. Specify the retention period. This period starts at the moment of the restore. After the retention period

the virtual machine disks are no longer available. Click **Request Restore**.

> **Note:** The default retention period of the restored data is 30 days.

5. Click **Monitor Requests** to display the request status. For future reference, note your request ID to easily identify your request.

Figure 13: Request ID



Recovery has been started. Check monitor page for progress.
Request ID is 0007

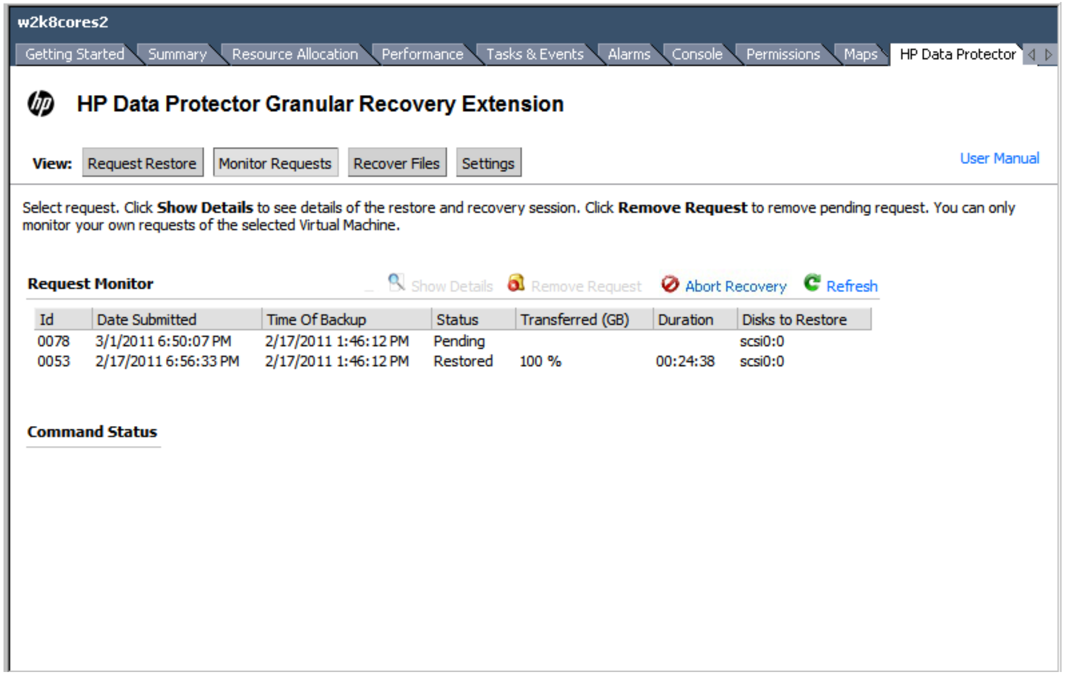
Monitoring restore requests

Procedure

To monitor restore requests:

1. In the HP Data Protector Granular Recovery Extension page, click **Monitor Requests**.

Figure 14: Viewing restore requests



Select request. Click **Show Details** to see details of the restore and recovery session. Click **Remove Request** to remove pending request. You can only monitor your own requests of the selected Virtual Machine.

Id	Date Submitted	Time Of Backup	Status	Transferred (GB)	Duration	Disks to Restore
0078	3/1/2011 6:50:07 PM	2/17/2011 1:46:12 PM	Pending			scsi0:0
0053	2/17/2011 6:56:33 PM	2/17/2011 1:46:12 PM	Restored	100 %	00:24:38	scsi0:0

2. Select your request identified by its ID number.

3. You can:

   - Click **Show Details** to display information about your request.
   - Click **Remove Request** to delete the pending requests that are no longer needed.
   - Click **Abort Recovery** to stop recovering files of virtual machine disks.

     The **Abort Recovery** option does not revert the already recovered files, but it stops recovering the rest of the files.

     Under the Command Status, the request status message is displayed.

     > **Note:** If you try to abort a recovery of a large file and the recovery does not finish in 5 seconds, the `Abort recovery of files is started for request id=xxxx` status message is displayed. When the recovery of the large file completes, the rest of the files stop recovering.

   - Click **Refresh** to update the status of your request.

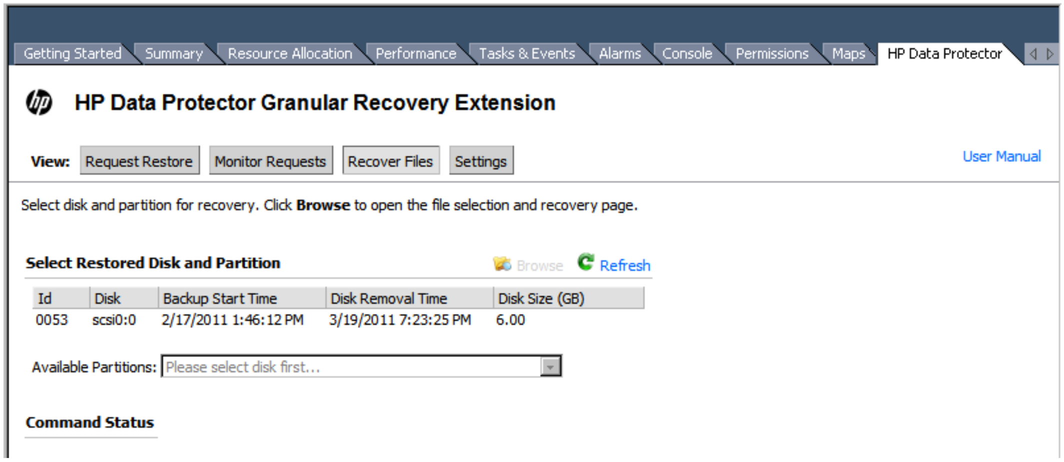
Recovering virtual machines

Procedure

To recover files of virtual machine disks:

1. In the HP Data Protector Granular Recovery Extension page, click **Recover files**.

Figure 15: Recover files



Select disk and partition for recovery. Click **Browse** to open the file selection and recovery page.

Select Restored Disk and Partition

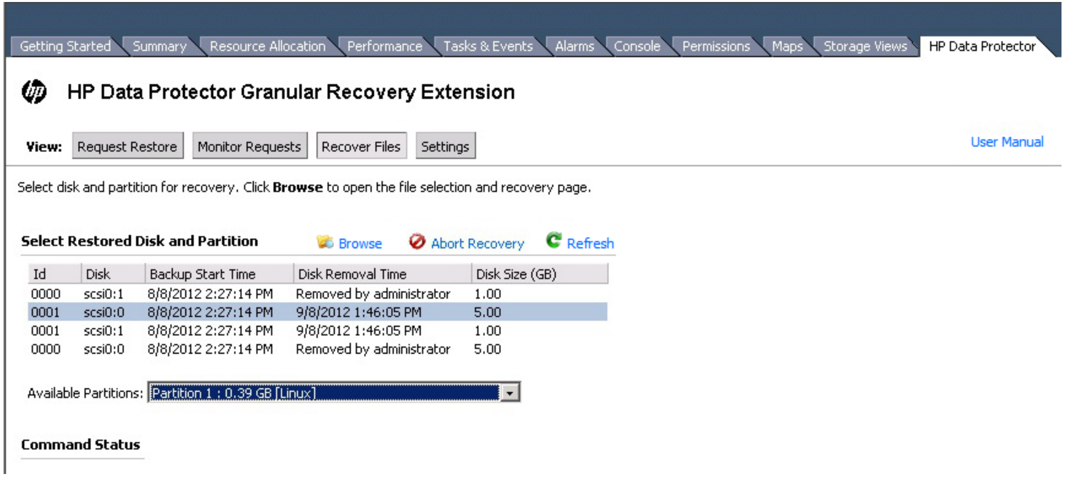
Id	Disk	Backup Start Time	Disk Removal Time	Disk Size (GB)
0053	scsi0:0	2/17/2011 1:46:12 PM	3/19/2011 7:23:25 PM	6.00

Available Partitions: Please select disk first...

Command Status

2. Select the virtual machine disk which contains the files that you want to recover. In the **Available Partitions** drop-down list, select the desired partition. For LVM partitions, select also a volume from the **Logical volumes** drop-down list. Click **Browse**. The Select Files to Recover page is displayed. Under the Virtual Machine OS Credentials, select the virtual machine, and specify its user name and password.

Figure 16: Selecting virtual disks



Select disk and partition for recovery. Click **Browse** to open the file selection and recovery page.

Select Restored Disk and Partition

Id	Disk	Backup Start Time	Disk Removal Time	Disk Size (GB)
0000	scsi0:1	8/8/2012 2:27:14 PM	Removed by administrator	1.00
0001	scsi0:0	8/8/2012 2:27:14 PM	9/8/2012 1:46:05 PM	5.00
0001	scsi0:1	8/8/2012 2:27:14 PM	9/8/2012 1:46:05 PM	1.00
0000	scsi0:0	8/8/2012 2:27:14 PM	Removed by administrator	5.00

Available Partitions: Partition 1 : 0.39 GB [Linux]

Command Status

Under the Recovery Options, enter the path to a target recovery location:

- For locations on Windows systems, use the format *`DriveLetter`*`:\`*`Folder`*`\`*`Subfolder`*.
- For locations on Linux systems, use the format */Directory/Subdirectory*.

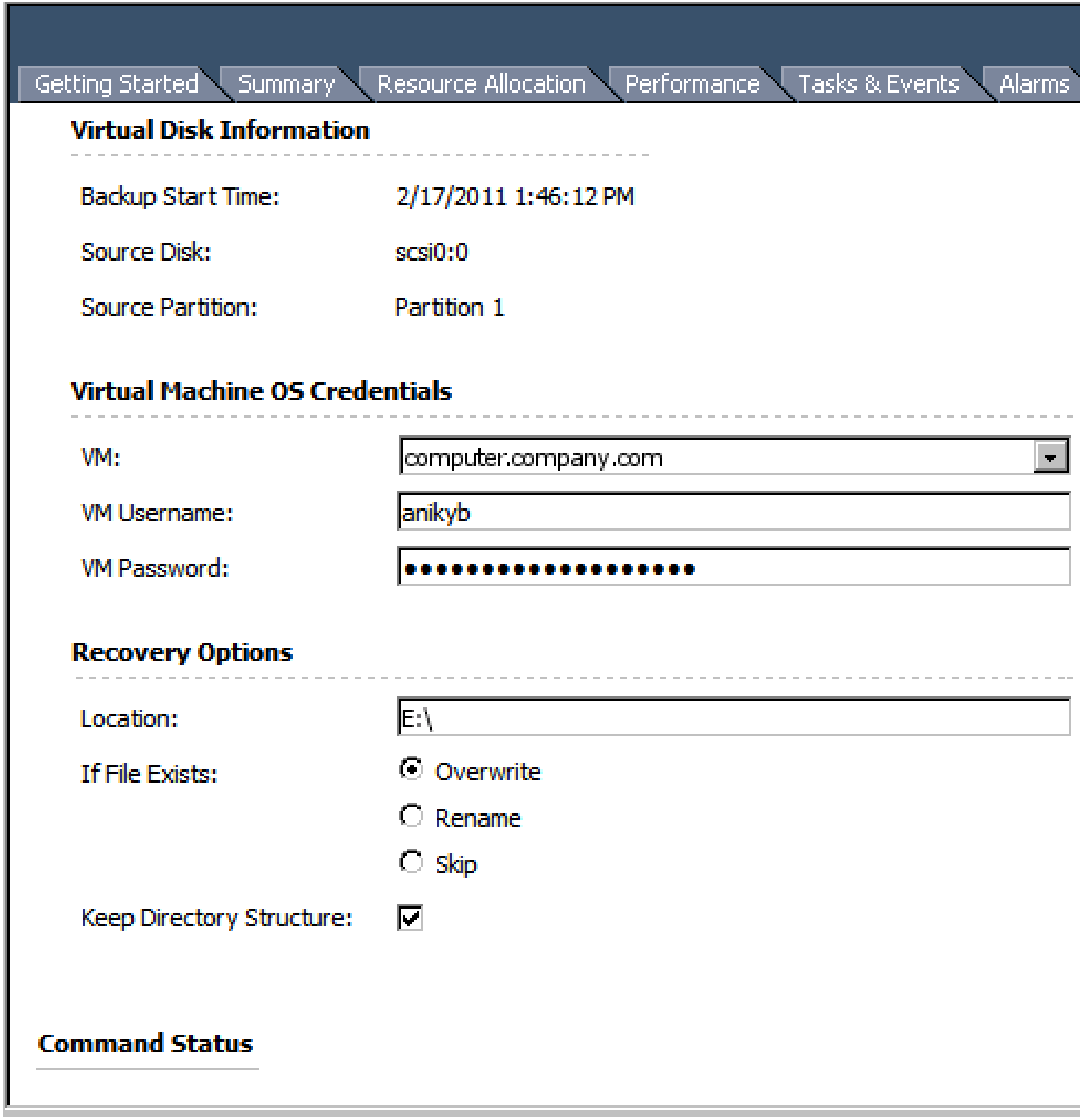
  Note that for shared directories, you need to enter the paths without the hostname. For example, for an NFS share `hostname:/shared_dir/subdir`, you need to enter `/shared_dir/subdir`.

  Any missing directories in the path will be created automatically. For example, if you specify `/shared_dir/subdir1/subdir2`, `subdir1/subdir2` will be automatically created inside `/shared_dir`.

If the file already exists on the target system, select the recovery option to be used:

- **Overwrite** : deletes the original files and folders and saves the latest files and folders.
- **Rename** : keeps the original files and folders, and saves the recovered files and folders with the name string *`pathname.timestamp`*.
- **Skip** : keeps the original files and folders unaffected.

Figure 17: Setting recovery options



Virtual Disk Information

Backup Start Time: 2/17/2011 1:46:12 PM

Source Disk: scsi0:0

Source Partition: Partition 1

Virtual Machine OS Credentials

VM: computer.company.com

VM Username: anikyb

VM Password: ●●●●●●●●●●●●●●●●●●●

Recovery Options

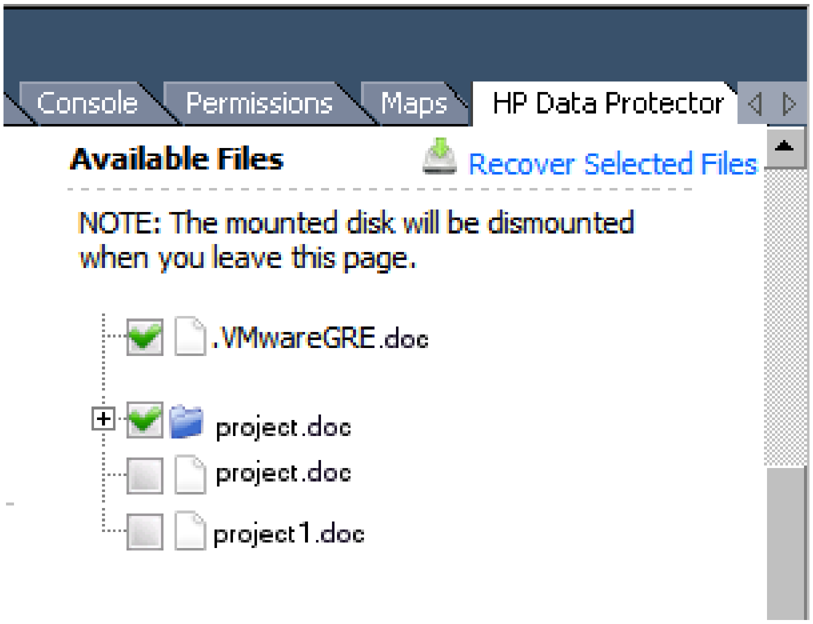
Location: E:\

If File Exists: ● Overwrite ○ Rename ○ Skip

Keep Directory Structure: ☑

Command Status

Figure 18: Granular recovery, selecting files for recovery



NOTE: The mounted disk will be dismounted when you leave this page.

3. Select **Keep Directory Structure** to maintain the original directory file structure of the source virtual machine disk on the target system.

4. Under **Available Files**, select files and folders to be recovered and click **Recover Selected Files**.

> **Note:** The files and folders displayed in this page depend on the backup type that you selected in the Request Restore procedure. For instance, if you selected an incremental backup, the whole restore chain is displayed. For details, see the *HP Data Protector Help* index: backup types or restore chain.

Administrator tasks

Opening the GUI of the HP Data Protector Granular Recovery Extension for VMware vSphere

Procedure

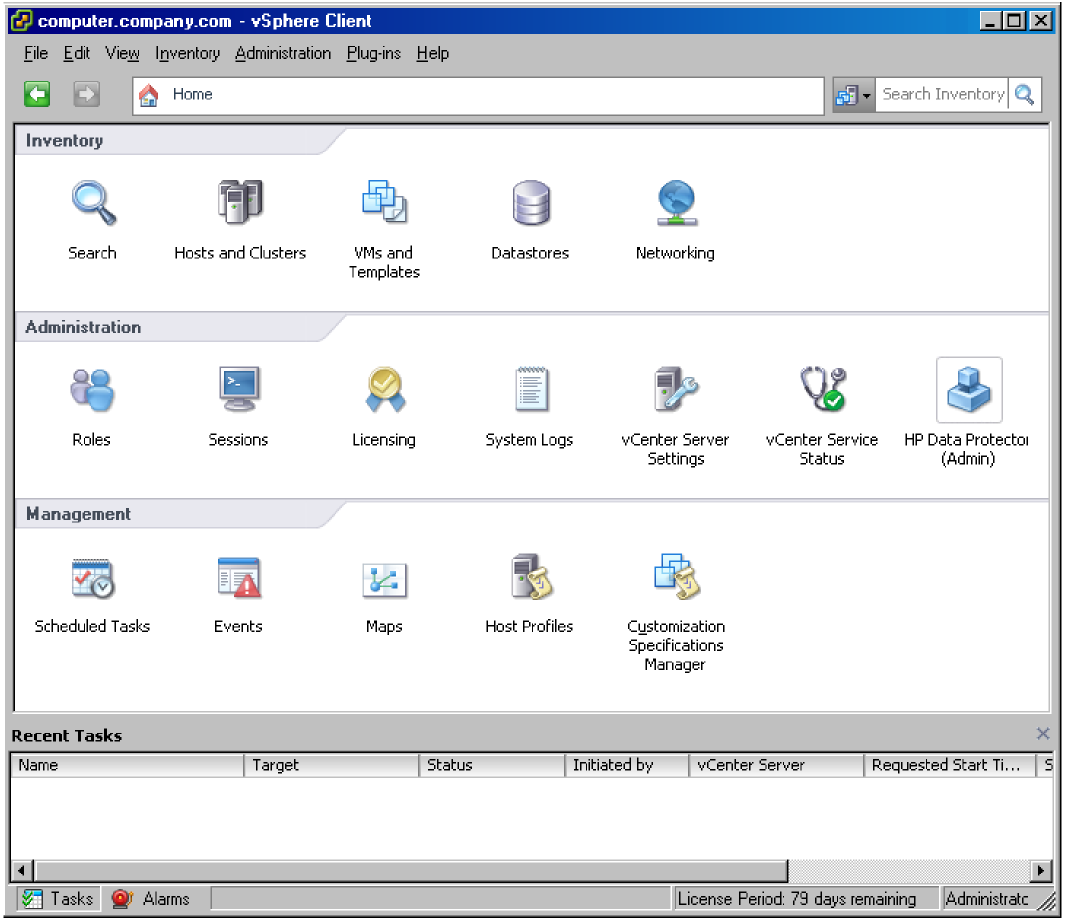
To open the GUI of the HP Data Protector Granular Recovery Extension for VMware vSphere:

1. Using the VMware vSphere Client, connect to the vCenter Server system and enter the user name and password. Specify the user credentials of the Data Protector user to which the `Start restore` right is assigned.

2. In the VMware vSphere Client navigation bar, click **Home**.

3. Under the Administration tab, click **HP Data Protector (Admin)**.

Figure 19: Locating the HP Data Protector (Admin) link



Important: If you receive the security alert notification after clicking the HP Data Protector tab, you do not have the vSphere certificate installed on your system. Click **Yes** to open the extension. For details on how to obtain a valid vSphere certificate, see the VMware end-user documentation or Help index: "About vCenter Server Certificates", or "Replacing vCenter Server Certificates".

The **HP Data Protector Granular Recovery Extension** GUI is opened in the administrator mode, in the Handle Requests page. For details, see "Handling restore requests" on page 41.

Note: Alternatively, you can open the HP Data Protector Granular Recovery Extension GUI in the administrator mode by selecting **View**, **Administration**, and **HP Data Protector (Admin)**.

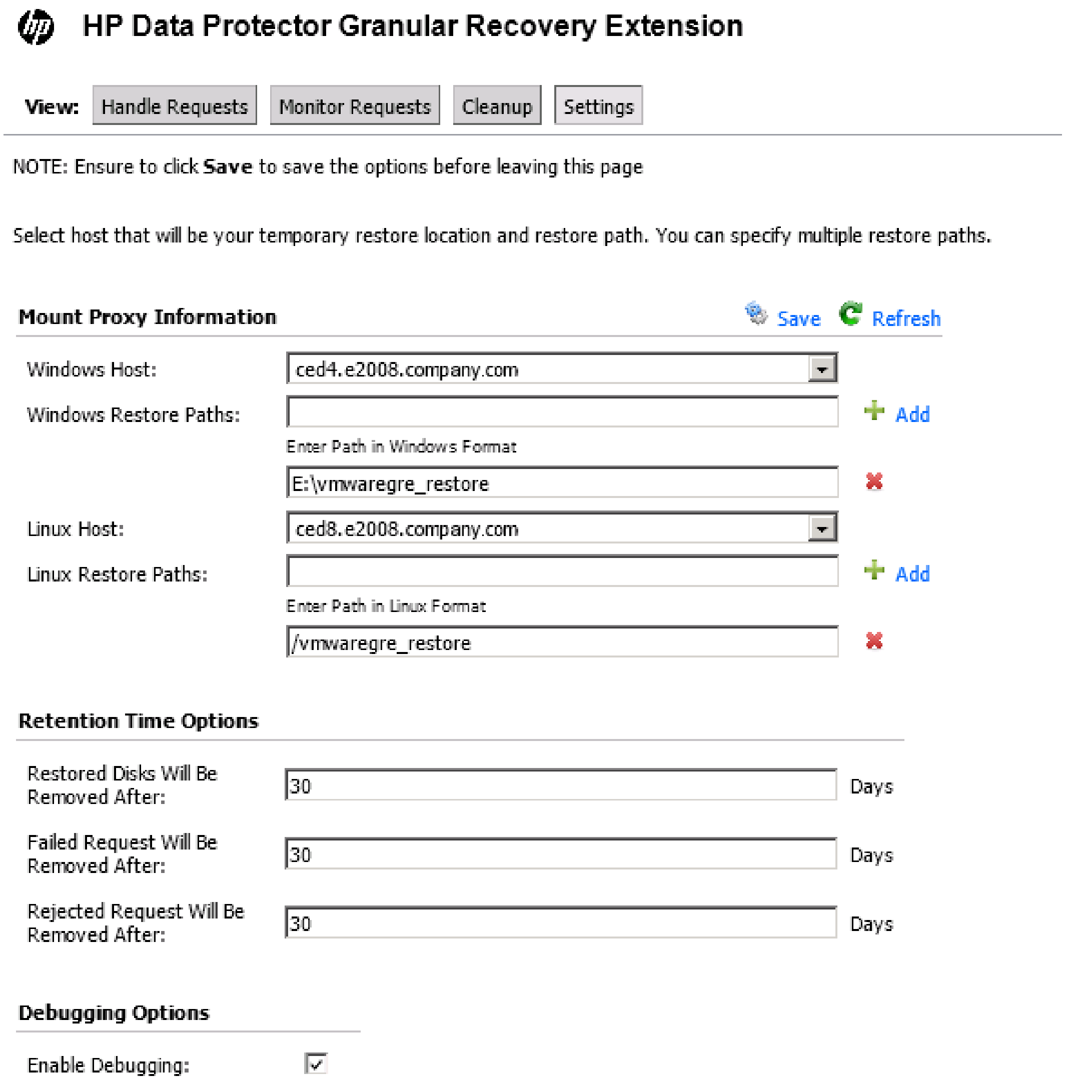
Configuring mount proxy systems

Procedure

To specify a mount proxy system used as a target location for restoring virtual machine disks:

1. In the HP Data Protector Granular Recovery Extension for VMware vSphere GUI, click **Settings**.

Figure 20: Administrative settings



HP Data Protector Granular Recovery Extension

NOTE: Ensure to click **Save** to save the options before leaving this page

Select host that will be your temporary restore location and restore path. You can specify multiple restore paths.

Mount Proxy Information

Windows Host: ced4.e2008.company.com

Windows Restore Paths:

Enter Path in Windows Format

E:\vmwaregre_restore

Linux Host: ced8.e2008.company.com

Linux Restore Paths:

Enter Path in Linux Format

/vmwaregre_restore

Retention Time Options

Restored Disks Will Be Removed After: 30 Days

Failed Request Will Be Removed After: 30 Days

Rejected Request Will Be Removed After: 30 Days

Debugging Options

Enable Debugging: ☑

2. Depending on your environment configuration and guest operating systems of the virtual machines you are going to recover, proceed as follows:

   - In the Windows Host drop-down list, select an available Windows mount proxy system.
   - In the Linux Host drop-down list, select an available Linux mount proxy system.
   - Make both of the above selections.

   For each mount proxy system, specify a restore directory which you want to restore your virtual machine disks to:

a. Enter the path to a location on the mount proxy system in the Windows Restore Paths text box, Linux Restore Paths text box, or both, in the format *DriveLetter*:\Folder\Subfolder (Windows mount proxy system) or /*Directory*/*Subdirectory* (Linux mount proxy system).

b. Click **Add** to add the specified path to the applicable list of restore paths.

c. Optionally, add more restore paths to the list by repeating substeps a and b. You can delete a specified restore path by clicking the red cross icon next to the corresponding text box.

d. Click **Save**.

> **Note:** To disable an already configured mount proxy system, select **Select Host ...** from an applicable Host drop-down list.

Handling restore requests

Procedure

After receiving a restore request from an operator, you can perform the following:

- "Triggering restore sessions" below.
- "Rejecting restore requests" on page 43.

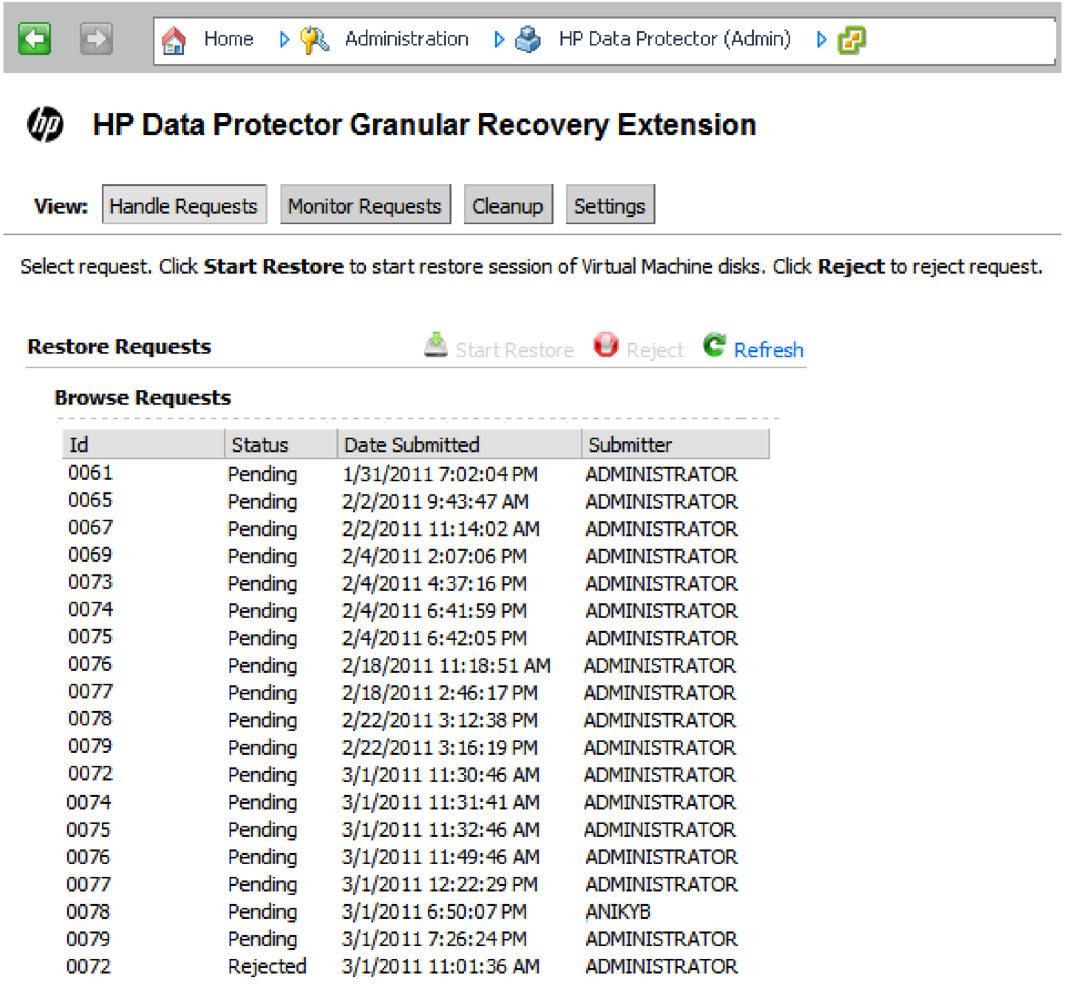
Triggering restore sessions

Procedure

To trigger the restore sessions:

1. In the HP Data Protector Granular Recovery Extension for VMware vSphere GUI, click **Handle Requests**.

Figure 21: Managing restore requests



Select request. Click **Start Restore** to start restore session of Virtual Machine disks. Click **Reject** to reject request.

Id	Status	Date Submitted	Submitter
0061	Pending	1/31/2011 7:02:04 PM	ADMINISTRATOR
0065	Pending	2/2/2011 9:43:47 AM	ADMINISTRATOR
0067	Pending	2/2/2011 11:14:02 AM	ADMINISTRATOR
0069	Pending	2/4/2011 2:07:06 PM	ADMINISTRATOR
0073	Pending	2/4/2011 4:37:16 PM	ADMINISTRATOR
0074	Pending	2/4/2011 6:41:59 PM	ADMINISTRATOR
0075	Pending	2/4/2011 6:42:05 PM	ADMINISTRATOR
0076	Pending	2/18/2011 11:18:51 AM	ADMINISTRATOR
0077	Pending	2/18/2011 2:46:17 PM	ADMINISTRATOR
0078	Pending	2/22/2011 3:12:38 PM	ADMINISTRATOR
0079	Pending	2/22/2011 3:16:19 PM	ADMINISTRATOR
0072	Pending	3/1/2011 11:30:46 AM	ADMINISTRATOR
0074	Pending	3/1/2011 11:31:41 AM	ADMINISTRATOR
0075	Pending	3/1/2011 11:32:46 AM	ADMINISTRATOR
0076	Pending	3/1/2011 11:49:46 AM	ADMINISTRATOR
0077	Pending	3/1/2011 12:22:29 PM	ADMINISTRATOR
0078	Pending	3/1/2011 6:50:07 PM	ANIKYB
0079	Pending	3/1/2011 7:26:24 PM	ADMINISTRATOR
0072	Rejected	3/1/2011 11:01:36 AM	ADMINISTRATOR

2. In the Browse Requests list, click the pending restore request you want to handle. The restore request details are displayed on the right.

3. You have configured a Windows and a Linux mount proxy system. When restoring Windows virtual machine disks, you can select a mount proxy system from the Mount Proxy drop-down list. When restoring Linux virtual machine disks, a Linux mount proxy system is selected by default and displayed as a label.

   If you have configured only one mount proxy system, it is automatically selected and displayed as a label. To be able to restore Linux virtual machine disks, the configured mount proxy system must be a Linux type.

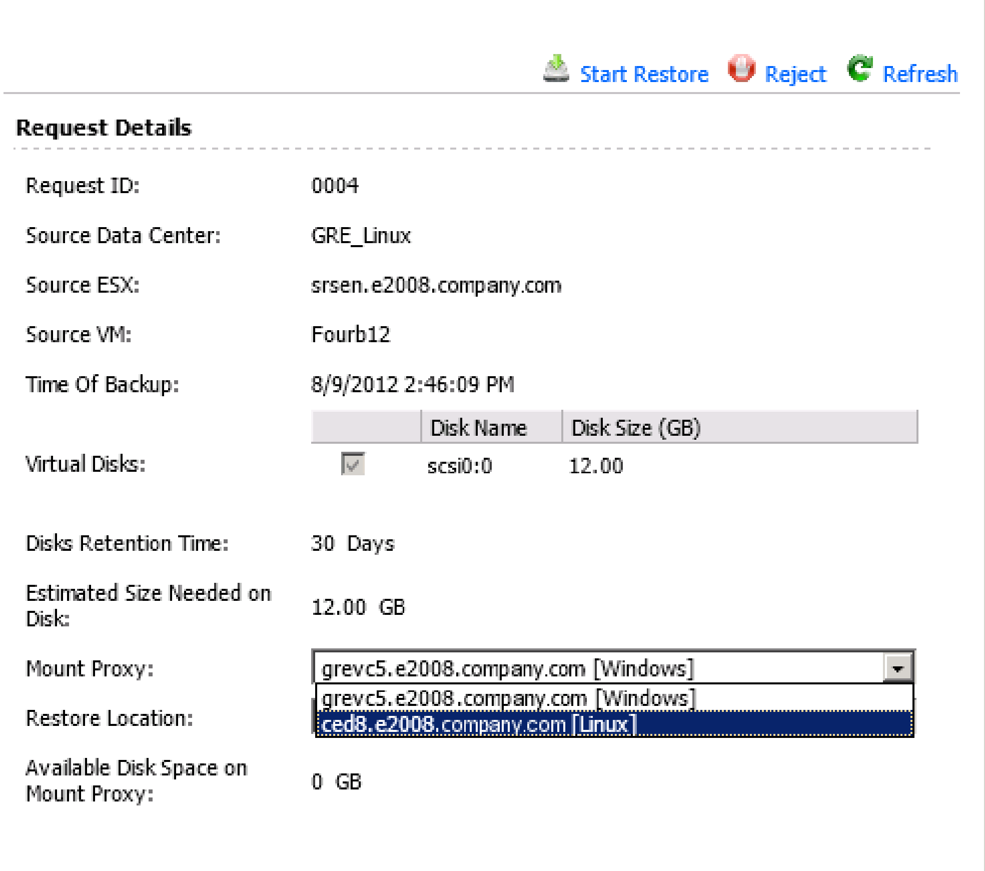
   > **Note:** You can use a Windows or a Linux mount proxy system to restore a Windows virtual machine disks, but you can only use a Linux mount proxy system to restore Linux virtual machine disks.

In the **Restore location** drop-down list, select one of the already specified restore paths (for Windows or for Linux virtual machines). The available disk space on the target restore location and the cumulative size of the disks selected for restore are displayed.

> **Note:** To change the mount proxy system, or specify an additional restore path, see "Configuring mount proxy systems" on page 39.

4. After specifying the restore options for the selected restore request, click **Start Restore**.

Figure 22: Starting operators restore requests



Request Details

Request ID:	0004
Source Data Center:	GRE_Linux
Source ESX:	srsen.e2008.company.com
Source VM:	Fourb12
Time Of Backup:	8/9/2012 2:46:09 PM

Virtual Disks:

	Disk Name	Disk Size (GB)
☑	scsi0:0	12.00

Disks Retention Time:	30 Days
Estimated Size Needed on Disk:	12.00 GB
Mount Proxy:	grevc5.e2008.company.com [Windows]
Restore Location:	grevc5.e2008.company.com [Windows] ced8.e2008.company.com [Linux]
Available Disk Space on Mount Proxy:	0 GB

Rejecting restore requests

Procedure

To reject an operator restore request:

1. In the HP Data Protector Granular Recovery Extension for VMware vSphere GUI, click **Handle Requests**.

2. In the Browse Requests list, click the pending restore request you want to reject.

3. Click **Reject**.

Monitoring restore requests

Procedure

To monitor requests:

1. In the HP Data Protector Granular Recovery Extension for VMware vSphere GUI, click **Monitor Requests**.

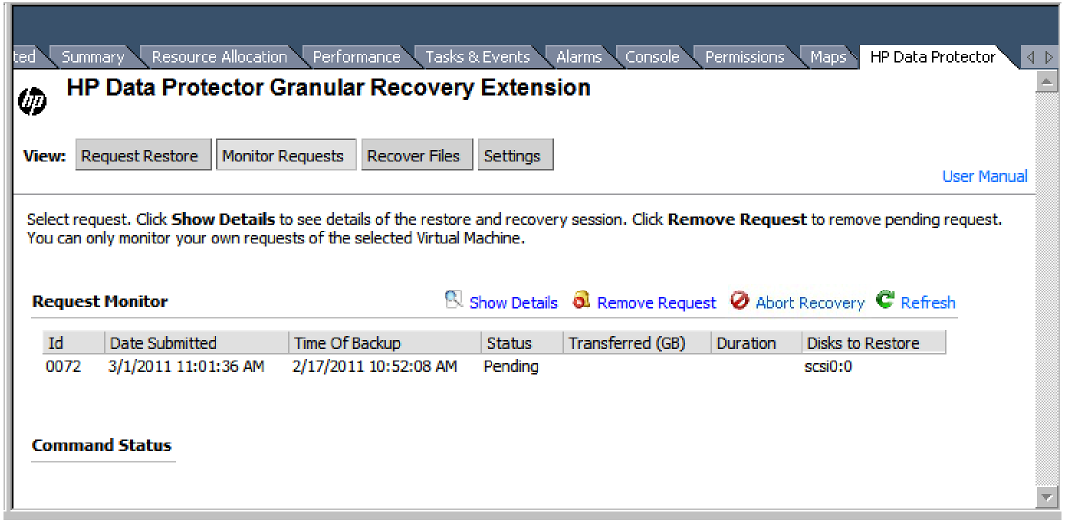
   The Request Monitor list displays all pending and triggered restore requests. A restore request can have the following status: Restoring (In Progress), Restored, Recovering, or Failed.

2. To see a detailed restore session report for a specific restore session, select this session from the list and then click **Show Details**.

3. To change the owner of a request, select a session and click **Change Owner**. Type a new owner into the text box and click **Change**. Use the *`Domain\Username`* form for domain users.

4. To end the running restore session (the session with the In Progress status), select the session you want to end and then click **Stop Restore**.

Figure 23: Monitoring operator restore requests — changing owner



HP Data Protector Granular Recovery Extension

Select request. Click **Show Details** to see details of the restore and recovery session. Click **Remove Request** to remove pending request.
You can only monitor your own requests of the selected Virtual Machine.

Request Monitor

Id	Date Submitted	Time Of Backup	Status	Transferred (GB)	Duration	Disks to Restore
0072	3/1/2011 11:01:36 AM	2/17/2011 10:52:08 AM	Pending			scsi0:0

Command Status

Removing virtual machine disks

Procedure

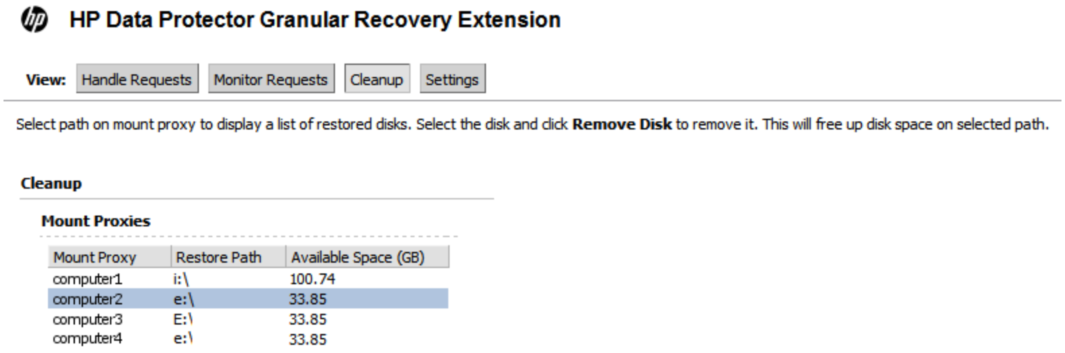
When the specified retention period expires, the virtual machine disks are deleted automatically.

In certain cases, you have to remove the virtual machine disks manually. Otherwise, the manual removal is not recommended.

To delete virtual machine disks manually:

1. In the HP Data Protector Granular Recovery Extension for VMware vSphere GUI, click **Cleanup**.

Figure 24: Removing disks



HP Data Protector Granular Recovery Extension

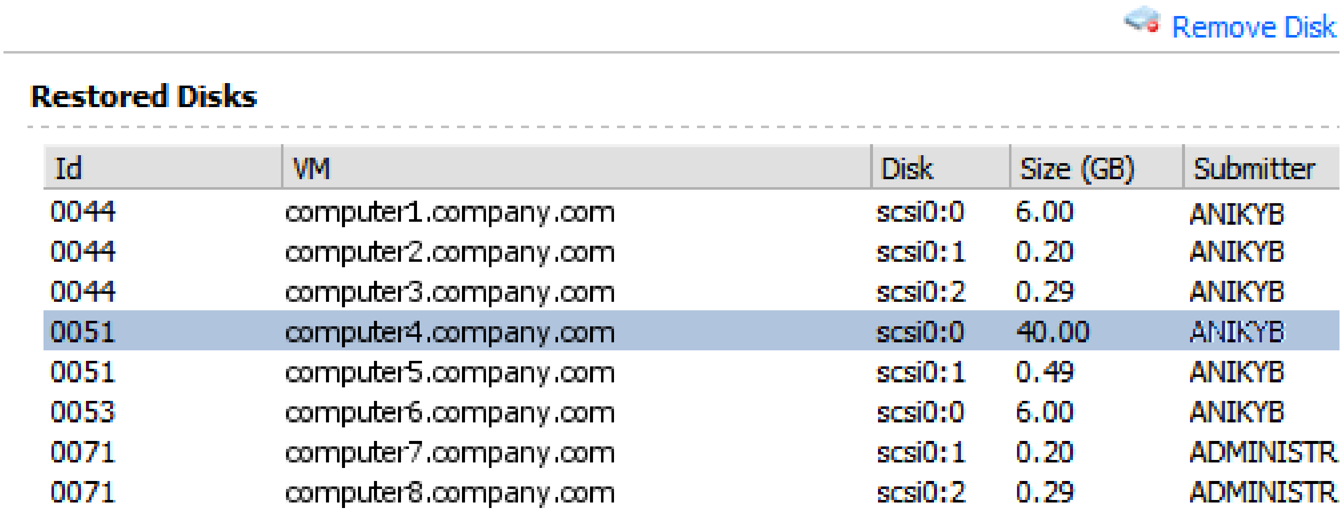
Select path on mount proxy to display a list of restored disks. Select the disk and click **Remove Disk** to remove it. This will free up disk space on selected path.

Cleanup

Mount Proxies

Mount Proxy	Restore Path	Available Space (GB)
computer1	i:\	100.74
computer2	e:\	33.85
computer3	E:\	33.85
computer4	e:\	33.85

Figure 25: Clean up



Restored Disks

Id	VM	Disk	Size (GB)	Submitter
0044	computer1.company.com	scsi0:0	6.00	ANIKYB
0044	computer2.company.com	scsi0:1	0.20	ANIKYB
0044	computer3.company.com	scsi0:2	0.29	ANIKYB
0051	computer4.company.com	scsi0:0	40.00	ANIKYB
0051	computer5.company.com	scsi0:1	0.49	ANIKYB
0053	computer6.company.com	scsi0:0	6.00	ANIKYB
0071	computer7.company.com	scsi0:1	0.20	ADMINISTR
0071	computer8.company.com	scsi0:2	0.29	ADMINISTR

The Cleanup list displays the restored virtual machine disks.

2. To remove the restored virtual machine disk from the mount proxy system, in the Cleanup list select the desired disk and then click **Remove Disk**.

Restore and recovery - VMware vSphere Web Client

Operator tasks

Accessing the Data Protector plug-in from VMware vSphere Web Client

Procedure

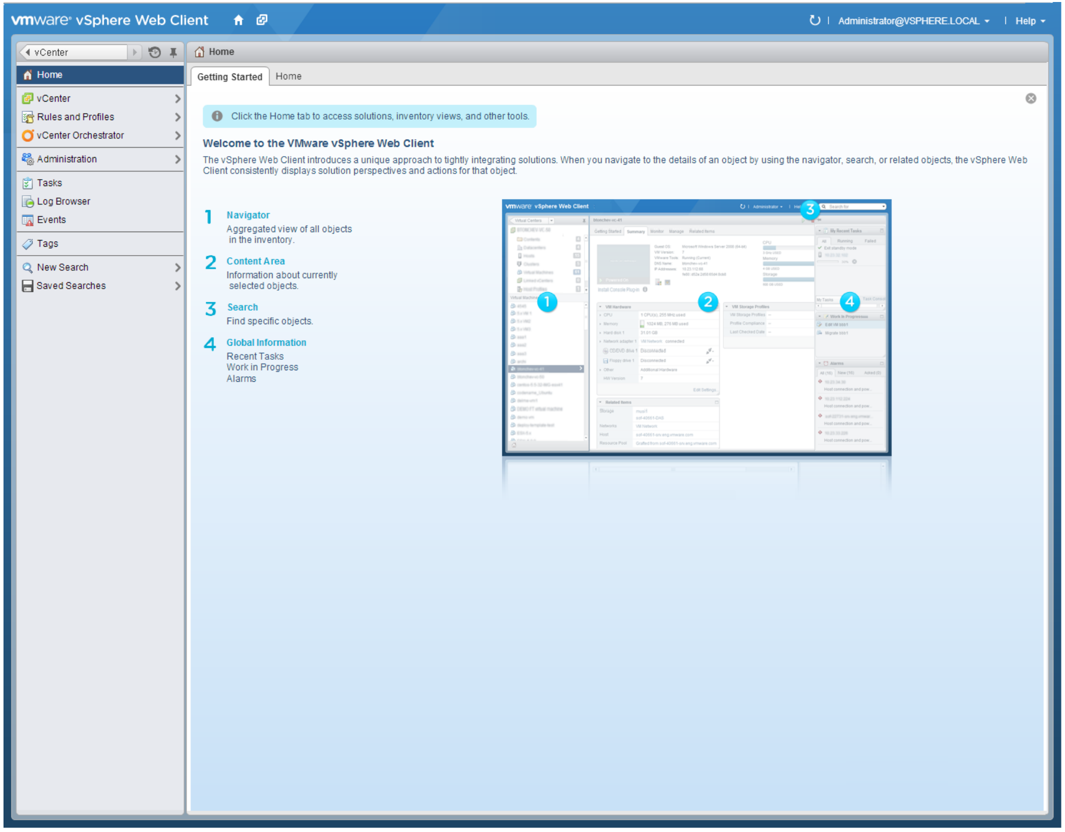
To access the Data Protector plug-in from VMware vSphere Web Client:

1. Open VMware vSphere Web Client and enter the user name and password.

2. Click **Login**.

   The VMware vSphere Web Client main page is displayed. It comprises the following key components: object navigator, main workspace, tasks, and alarms panel.

Figure 26: VMware vSphere Web Client main page



Click the Home tab to access solutions, inventory views, and other tools.

Welcome to the VMware vSphere Web Client

The vSphere Web Client introduces a unique approach to tightly integrating solutions. When you navigate to the details of an object by using the navigator, search, or related objects, the vSphere Web Client consistently displays solution perspectives and actions for that object.

1 Navigator
Aggregated view of all objects in the inventory.

2 Content Area
Information about currently selected objects.

3 Search
Find specific objects.

4 Global Information
Recent Tasks
Work in Progress
Alarms

3. Under Inventories, expand the virtual machine node and select the desired virtual machine.

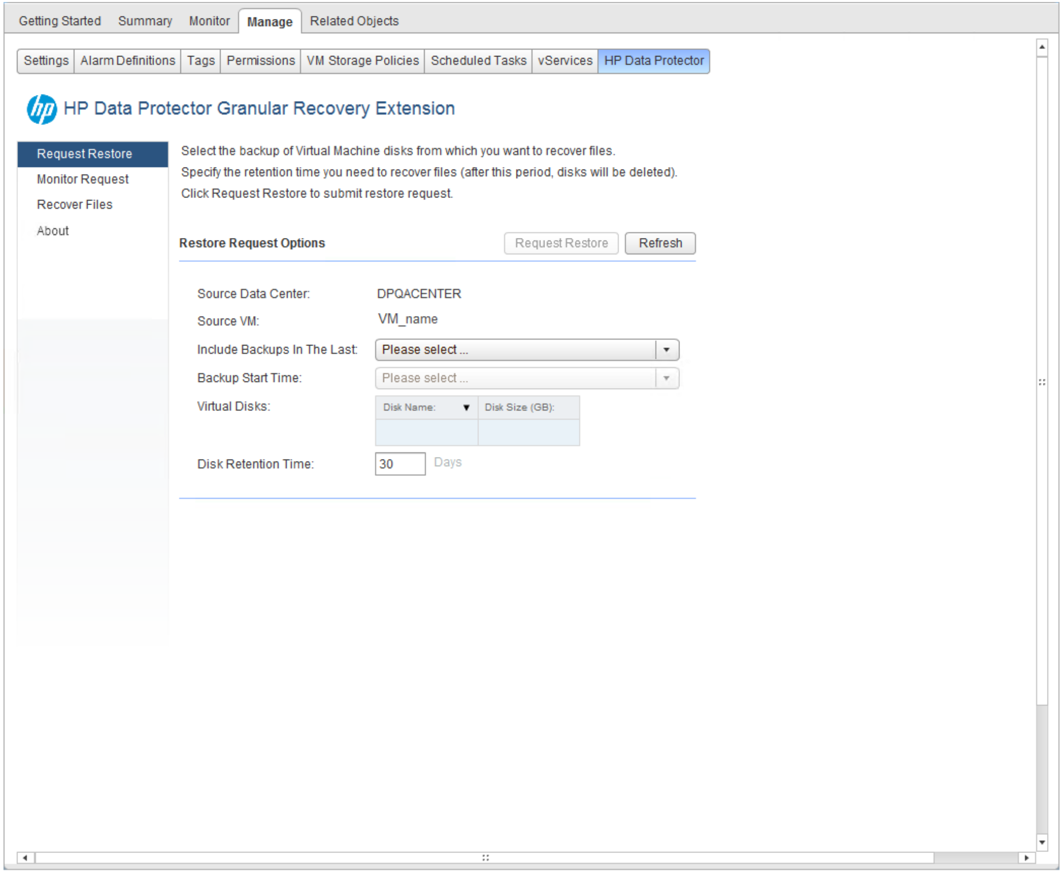
4. Click **Manage > HP Data Protector**.

> **Important:** If you receive the security alert notification after accessing the VMware vSphere Web Client application, you do not have the vSphere certificate installed on your system. Click **Yes** to open the extension. For details on how to obtain a valid vSphere certificate, see the VMware end-user documentation or Help index: "About vCenter Server Certificates" or "Replacing vCenter Server Certificates".

> **Note:** A pop-up error message is displayed when you log in to the HP Data Protector Granular Recovery Extension GUI for the first time to notify that you do not have all the Admin rights.

The HP Data Protector Granular Recovery Extension GUI opens in the operator mode. The left pane displays various tabs and the right pane displays the main workspace area.

Figure 27: HP Data Protector Granular Recovery Extension GUI (Operator mode)



Select the backup of Virtual Machine disks from which you want to recover files.
Specify the retention time you need to recover files (after this period, disks will be deleted).
Click Request Restore to submit restore request.

Restore Request Options

Source Data Center: DPQACENTER
Source VM: VM_name
Include Backups In The Last: Please select ...
Backup Start Time: Please select ...
Virtual Disks:

Disk Name:	Disk Size (GB):

Disk Retention Time: 30 Days

Requesting restores

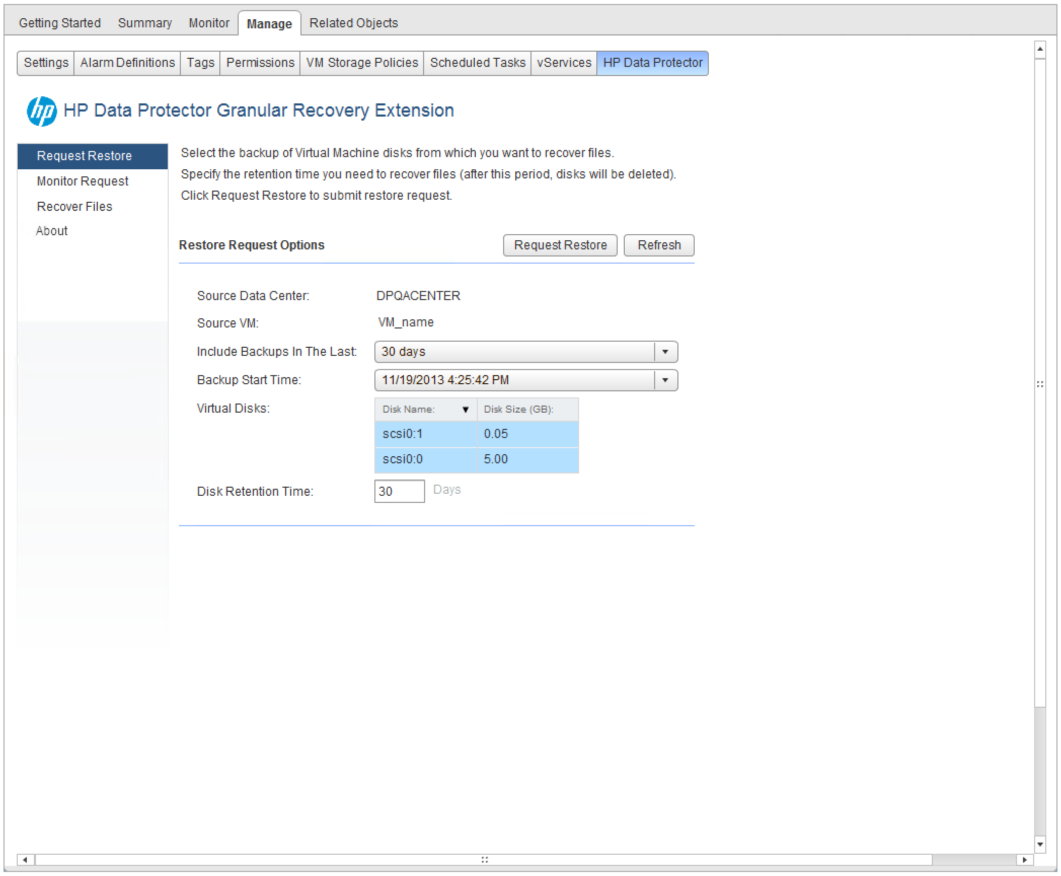
Procedure

To request restores:

1. In the HP Data Protector Granular Recovery Extension page, click the **Request Restore** tab.

   The Restore Request Options page is displayed.

   Figure 28: Request restore of virtual disks



HP Data Protector Granular Recovery Extension

Select the backup of Virtual Machine disks from which you want to recover files.
Specify the retention time you need to recover files (after this period, disks will be deleted).
Click Request Restore to submit restore request.

Restore Request Options

Source Data Center: DPQACENTER
Source VM: VM_name
Include Backups In The Last: 30 days
Backup Start Time: 11/19/2013 4:25:42 PM
Virtual Disks:

Disk Name:	Disk Size (GB):
scsi0:1	0.05
scsi0:0	5.00

Disk Retention Time: 30 Days

2. In the Request Restore Options page, proceed as follows:

   - In the Include Backups in The Last drop-down list, select the backup period.
   - In the Backup Start Time drop-down list, select the start date, time, and backup type.
   - From the Virtual Disks list, select single or multiple virtual disks for restore.
   - In the Disk Retention Time text box, enter the retention period. This period starts from the restore operation. After the retention period, the virtual disks are not available.

   Note: The default retention period of the restored data is 30 days.

3. Click **Request Restore**.

4. Click the **Monitor Request** tab to display the request status. For future reference, note your request ID to identify your request.

Monitoring restore requests

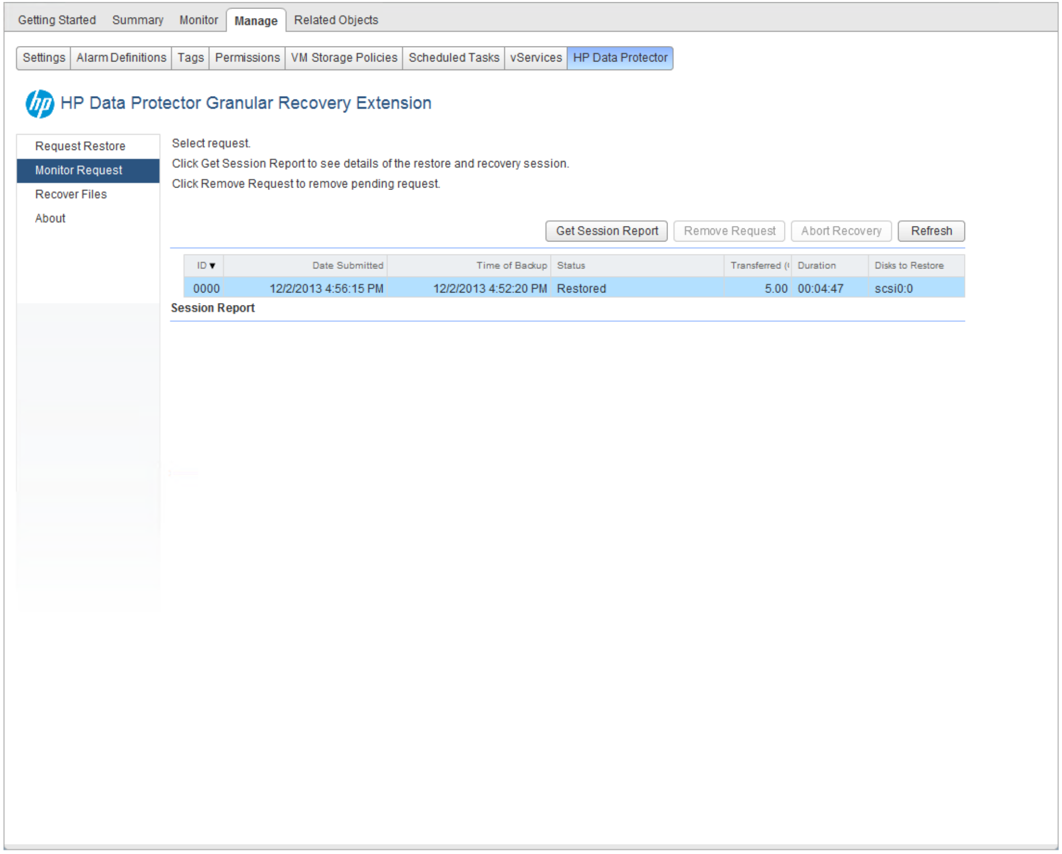
Procedure

To monitor restore requests:

1. In the HP Data Protector Granular Recovery Extension page, click the **Monitor Request** tab.

   The Monitor requests page is displayed.

   Figure 29: Monitor requests

   Select request.
   Click Get Session Report to see details of the restore and recovery session.
   Click Remove Request to remove pending request.

ID ▾	Date Submitted	Time of Backup	Status	Transferred ((	Duration	Disks to Restore
0000	12/2/2013 4:56:15 PM	12/2/2013 4:52:20 PM	Restored	5.00	00:04:47	scsi0:0

   Session Report

2. Select your request identified by its ID number.

3. You can:

   - Click **Get Session Report** to display the following session information under Session Report.

State	Session Information
Restored	Restoring session information
Recovering	Recovery session information

   - Click **Remove Request** to delete the unwanted pending requests.

- Click **Abort Recovery** to stop recovering the files of virtual machine disks.

  The Abort Recovery option is not applicable to already recovered files, but it stops recovering the rest of the files.

  Under Session Report, the request status message is displayed.

  > **Note:** If you abort recovery of a large file and recovery does not finish in 5 seconds, the following status message is displayed: `Abort recovery of files is started for request id=xxxx`. When the recovery of the large file completes, the rest of the files stop recovering.

- Click **Refresh** to update the status of your request.

Recovering files from virtual machines

Procedure

To recover files from virtual machine disks:

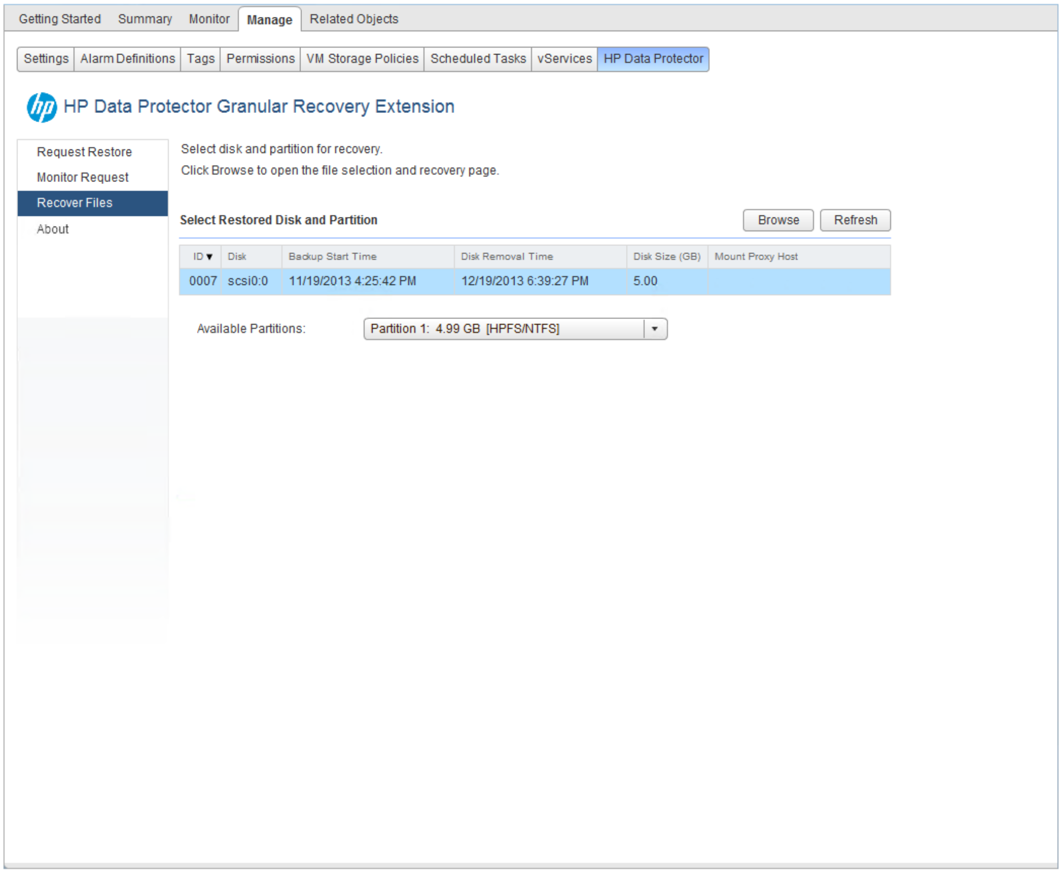
1. In the HP Data Protector Granular Recovery Extension page, click the **Recover Files** tab

   The Select Restored Disk and Partition page is displayed.

2. To select the virtual machine disk containing the files to recover, proceed as follows:

   a. In the **Available Partitions** drop-down list, select the desired partition and its type (Windows or Linux).

Figure 30: Recovering files (select the Windows partition for browse)



Select disk and partition for recovery.
Click Browse to open the file selection and recovery page.

Select Restored Disk and Partition

ID ▾	Disk	Backup Start Time	Disk Removal Time	Disk Size (GB)	Mount Proxy Host
0007	scsi0:0	11/19/2013 4:25:42 PM	12/19/2013 6:39:27 PM	5.00	

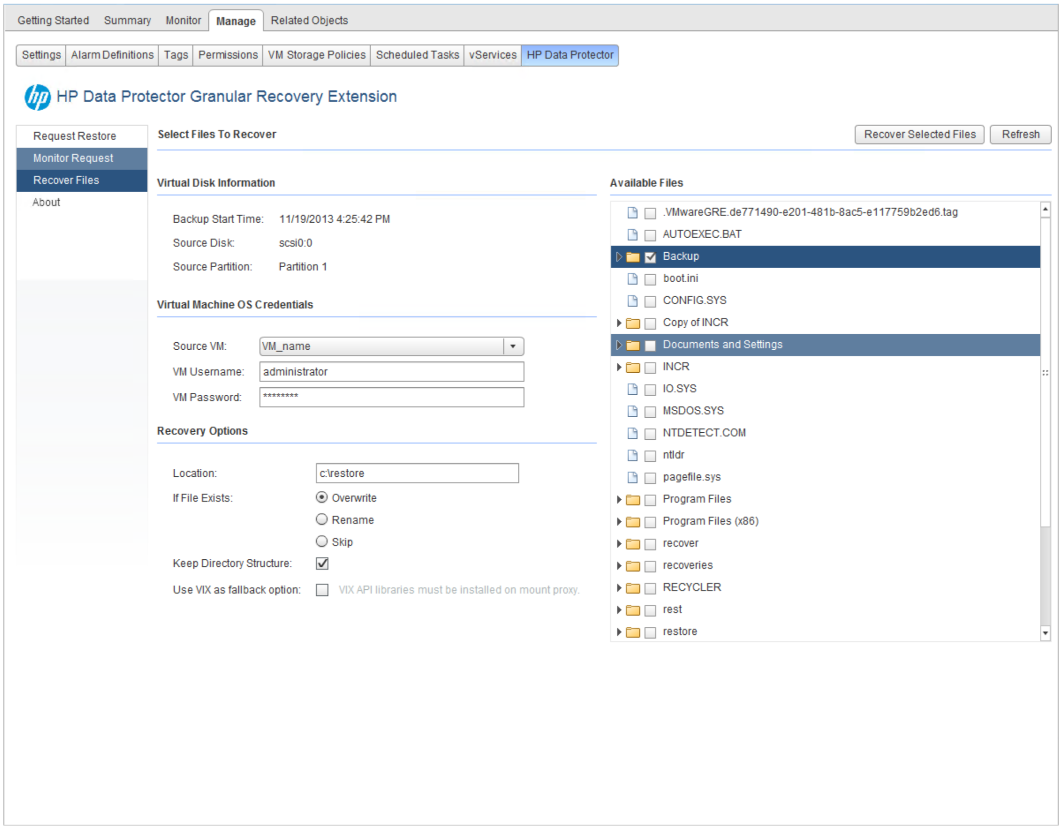
Available Partitions: Partition 1: 4.99 GB [HPFS/NTFS]

A new **Available Partitions** drop-down list is displayed that contains the logical volumes.

b. Select a logical volume and click **Browse**.

The Select Files To Recover page is displayed.

Figure 31: Recover files from the selected disk



Select Files To Recover

Virtual Disk Information

Backup Start Time: 11/19/2013 4:25:42 PM
Source Disk: scsi0:0
Source Partition: Partition 1

Virtual Machine OS Credentials

Source VM: VM_name
VM Username: administrator
VM Password: ********

Recovery Options

Location: c:\restore
If File Exists: ● Overwrite ○ Rename ○ Skip
Keep Directory Structure: ☑
Use VIX as fallback option: □ VIX API libraries must be installed on mount proxy.

Available Files

- □ .VMwareGRE.de771490-e201-481b-8ac5-e117759b2ed6.tag
- □ AUTOEXEC.BAT
- ☑ Backup
- □ boot.ini
- □ CONFIG.SYS
- □ Copy of INCR
- □ Documents and Settings
- □ INCR
- □ IO.SYS
- □ MSDOS.SYS
- □ NTDETECT.COM
- □ ntldr
- □ pagefile.sys
- □ Program Files
- □ Program Files (x86)
- □ recover
- □ recoveries
- □ RECYCLER
- □ rest
- □ restore

3. Under Virtual Machine OS Credentials, select the virtual machine from the **Source VM** drop-down list, and enter its credentials in the VM Username and VM Password text boxes.

4. In the Location text box, enter the target recovery location path.

   - For locations on Windows systems, use the format `DriveLetter:\Folder\Subfolder`.
   - For locations on Linux systems, use the format `/Directory/Subdirectory`.

   > **Note:** For shared directories, enter the path without the hostname. For example, in case of an NFS share hostname: `/shared_dir/subdir`, use `/shared_dir/subdir`. Also, ensure that the Samba and NFS shares are set up correctly. The NFS share must also be exported as pseudo root shares.

   Any missing directories in the path are created automatically. For example, if you specify `/shared_dir/subdir1/subdir2`, the `subdir1/subdir2` subdirectories are automatically created inside `/shared_dir`.

5. If the file already exists on the target system, select one of the following recovery options:

- **Overwrite**: deletes the original files and folders, and saves the latest files and folders.
- **Rename**: keeps the original files and folders, and saves the recovered files and folders with the name string pathname.timestamp.
- **Skip**: keeps the original files and folders.

6. Select **Keep Directory Structure** to maintain the original directory structure of the source virtual machine disk on the target system.
7. Select **Use VIX as fallback option** when network share is not available.
8. Under Available Files, select the files and folders to be recovered.
9. Click **Recover Selected Files**.

About Granular Recovery Extension

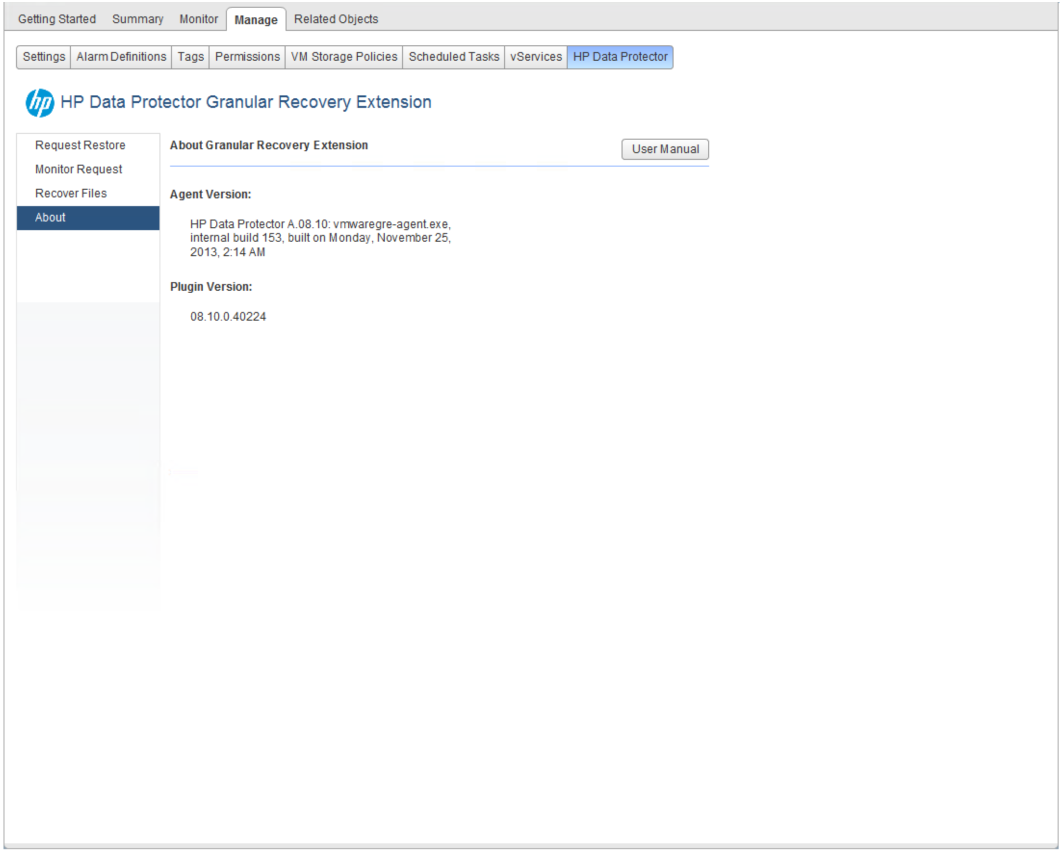
Procedure

To know about the VMware Granular Recovery Extension agent and Plugin version:

1. In the HP Data Protector Granular Recovery Extension for VMware vSphere GUI, click the **About** tab.

   The About Granular Recovery Extension page is displayed.

Figure 32: About Granular Recovery Extension GUI (Operator mode)



About Granular Recovery Extension

Agent Version:

HP Data Protector A.08.10: vmwaregre-agent.exe, internal build 153, built on Monday, November 25, 2013, 2:14 AM

Plugin Version:

08.10.0.40224

2. Click **User Manual** to download a copy of the *HP Data Protector 8.10 Granular Recovery Extension User Guide for VMware vSphere*.

> **Note:** You can download the GRE guide if the Data Protector documentation component is installed on the vCenter Server.

Administrator tasks

Accessing the Data Protector plug-in from VMware vSphere Web Client

To access the Data Protector plug-in from VMware vSphere Web Client:

1. Open VMware vSphere Web Client, and connect to the vCenter server. Specify the credentials of the Data Protector user with the `Start restore` permission.

2. Click **Login**.

   The VMware vSphere Web Client home page is displayed. The **Home** tab is selected by default.

3. Under Inventories, expand the virtual machine node and select the desired virtual machine.

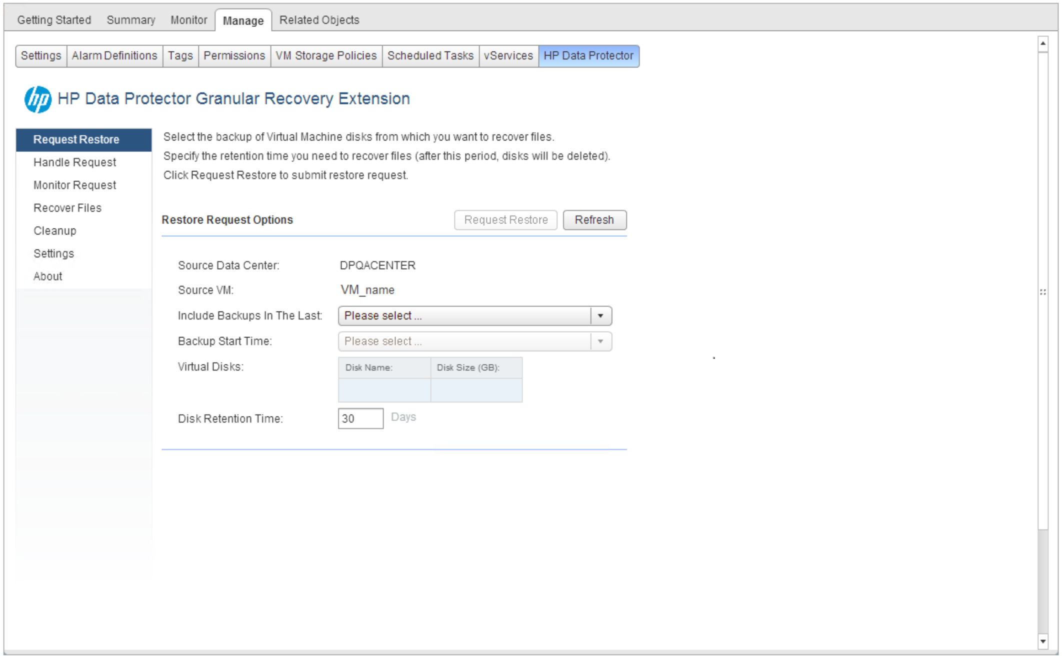
4. Click **Manage > HP Data Protector**.

   > **Important:** If you receive the security alert notification after accessing the VMware vSphere Web Client application, you do not have the vSphere certificate installed on your system. Click **Yes** to open the extension. For details on how to obtain a valid vSphere certificate, see the VMware end-user documentation or Help index: "About vCenter Server Certificates", or "Replacing vCenter Server Certificates".

   The HP Data Protector Granular Recovery Extension GUI opens in the administrator mode. The left pane displays various tabs and the right pane displays the main workspace area.

   > **Note:** As an Administrator, you need to configure mount proxies in the **Settings** tab when you access the HP Data Protector Granular Recovery Extension for the first time. Otherwise, the following error message is displayed:
   >
   > ```
   > The configuration check failed.
   > ```

Figure 33: HP Data Protector Granular Recovery Extension GUI (Administrator mode)



Select the backup of Virtual Machine disks from which you want to recover files.
Specify the retention time you need to recover files (after this period, disks will be deleted).
Click Request Restore to submit restore request.

Source Data Center: DPQACENTER
Source VM: VM_name
Include Backups In The Last: Please select ...
Backup Start Time: Please select ...
Virtual Disks:

Disk Name:	Disk Size (GB):

Disk Retention Time: 30 Days

Configuring mount proxy systems

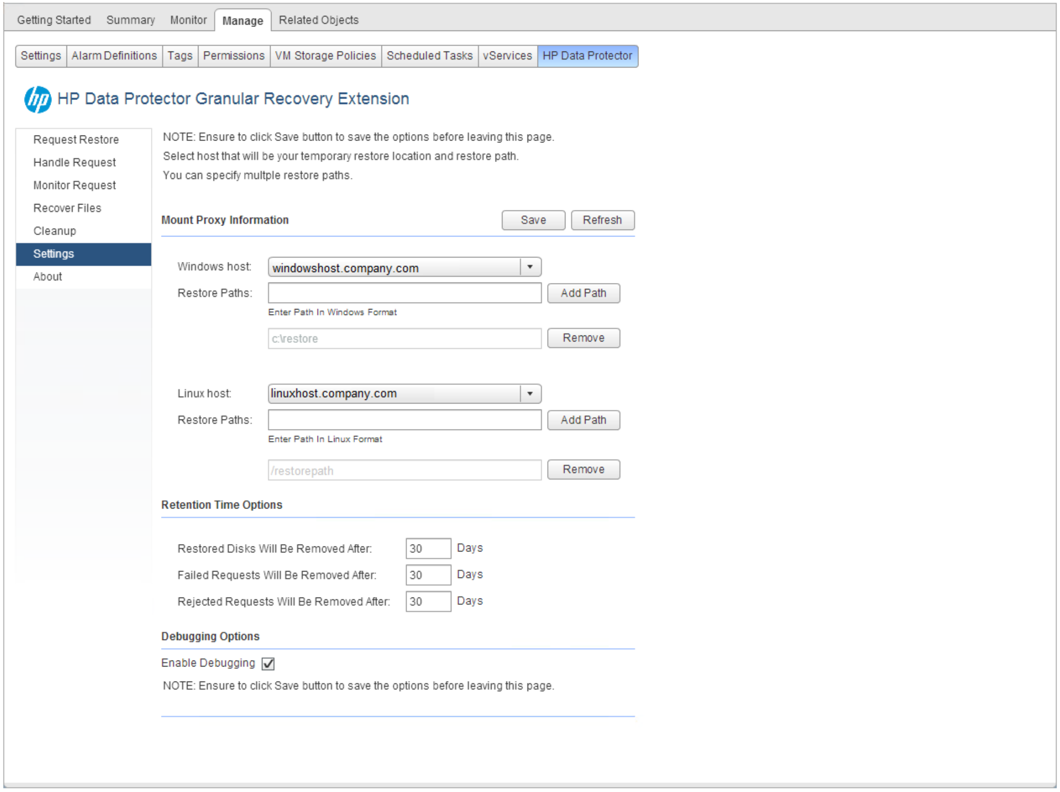
Procedure

To specify a mount proxy system used as a target location for restoring virtual machine disks:

1. In the HP Data Protector Granular Recovery Extension for VMware vSphere GUI, click the **Settings** tab.

   The Mount Proxy Information page is displayed.

   Figure 34: Administrative settings



NOTE: Ensure to click Save button to save the options before leaving this page.
Select host that will be your temporary restore location and restore path.
You can specify multple restore paths.

Mount Proxy Information

Windows host: windowshost.company.com
Restore Paths:
Enter Path In Windows Format
c:\restore

Linux host: linuxhost.company.com
Restore Paths:
Enter Path In Linux Format
/restorepath

Retention Time Options

Restored Disks Will Be Removed After: 30 Days
Failed Requests Will Be Removed After: 30 Days
Rejected Requests Will Be Removed After: 30 Days

Debugging Options

Enable Debugging ☑
NOTE: Ensure to click Save button to save the options before leaving this page.

2. From the **Windows** or **Linux Host** drop-down list, select the available Windows or Linux mount proxy system.

   > **Note:** Select the following:
   >
   > - A Windows or Linux mount proxy system (for Windows Host)
   > - A Linux mount proxy system (for Linux Host)

3. In the Windows and/or Linux **Restore Paths** text box, enter the path to a location on the mount proxy system. Use the following format:

   - *DriveLetter*:\Folder\Subfolder (Windows mount proxy system)
   - /*Directory*/*Subdirectory* (Linux mount proxy system)

4. Click **Add Path** to add the specified path to the applicable list of restore paths.

5. Proceed as follows:

   a. Optionally, add more restore paths to the list by repeating steps 3 and 4.

   b. Click **Remove** to delete the desired restore path(s).

   > **Note:** To disable an already configured mount proxy system, select **Disable mount proxy host** from the required host drop-down list.

6. Under **Retention Time Options**, enter the retention period for the following text boxes:

   - Restored Disks Will Be Removed After
   - Failed Requests Will Be Removed After
   - Rejected Requests Will Be Removed After

   > **Note:** The default retention period of the restored data is 30 days. During this time period, only one mount proxy of each type can be active.

7. Under Debugging Options, select **Enable Debugging** to receive bug files.

8. Click **Save**.

   > **Note:** Click **Refresh** to get the previously saved changes.

Handling restore requests

Procedure

After receiving a restore request from an operator, you have the following options:

- " Triggering restore sessions " below
- " Rejecting restore requests " on page 59

Triggering restore sessions

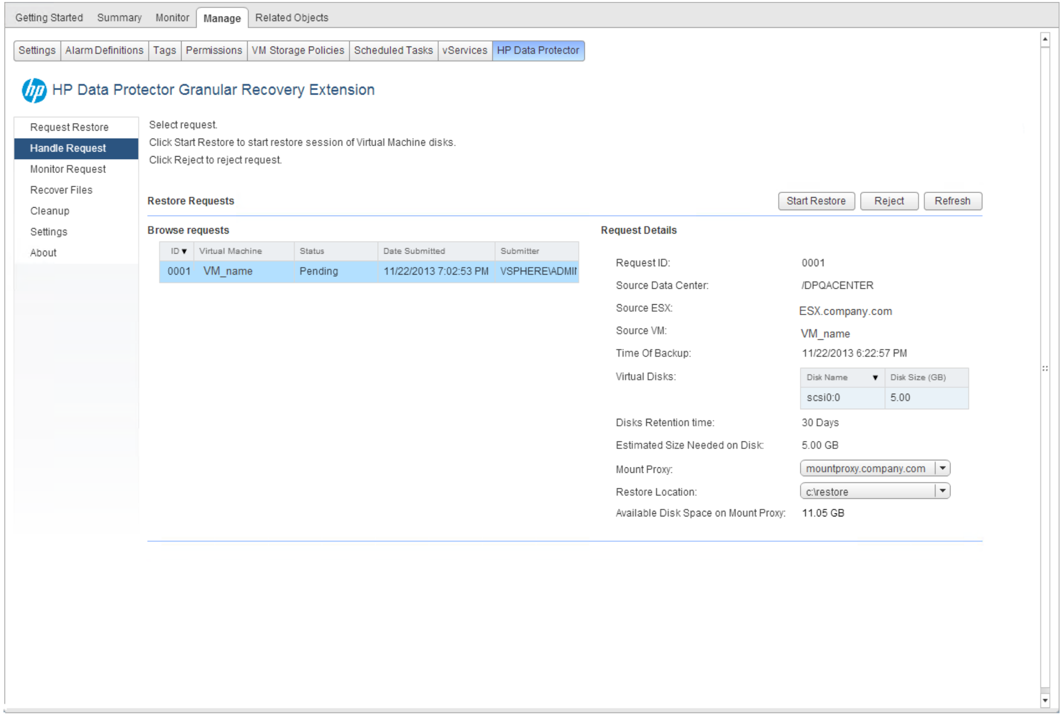
Procedure

To trigger the restore sessions:

1. In the HP Data Protector Granular Recovery Extension for VMware vSphere GUI, click the **Handle Request** tab.

The Restore Requests page is displayed.

Figure 35: Managing restore requests



Select request.
Click Start Restore to start restore session of Virtual Machine disks.
Click Reject to reject request.

Restore Requests

Browse requests

ID ▾	Virtual Machine	Status	Date Submitted	Submitter
0001	VM_name	Pending	11/22/2013 7:02:53 PM	VSPHERE\ADMII

Request Details

Request ID: 0001
Source Data Center: /DPQACENTER
Source ESX: ESX.company.com
Source VM: VM_name
Time Of Backup: 11/22/2013 6:22:57 PM
Virtual Disks:

Disk Name ▾	Disk Size (GB)
scsi0:0	5.00

Disks Retention time: 30 Days
Estimated Size Needed on Disk: 5.00 GB
Mount Proxy: mountproxy.company.com
Restore Location: c:\restore
Available Disk Space on Mount Proxy: 11.05 GB

2. Under Browse requests, select the required restore request ID number. The restore request details are displayed on the right.

> **Note:** To configure a Windows and Linux mount proxy system, see " Configuring mount proxy systems " on page 55.

3. From the **Mount Proxy** drop-down list, select one of the following when restoring Windows or Linux virtual machine disks:

   - A Windows or Linux mount proxy system (for Windows virtual machine disks)
   - A Linux mount proxy system (for Linux virtual machine disks)

> **Note:** If you have configured only one mount proxy system, it is automatically selected and displayed in the drop-down list. To restore Linux virtual machine disks, the configured mount proxy system must be of the Linux type.

4. From the **Restore Location** drop-down list, select one of the already specified restore paths (for Windows or Linux virtual machines). The available disk space on the target restore location and the cumulative size of the disks selected for restore are displayed.

> **Note:** To change the mount proxy system or to specify an additional restore path, see " Configuring mount proxy systems " on page 55.

5. After specifying the restore options for the selected restore request, click **Start Restore**.

Rejecting restore requests

Procedure

To reject a restore request:

1. In the HP Data Protector Granular Recovery Extension for VMware vSphere GUI, click the **Handle Request** tab.

   The Restore Requests page is displayed.

2. Under Browse requests, select the restore request ID number you want to reject.

3. Click **Reject**.

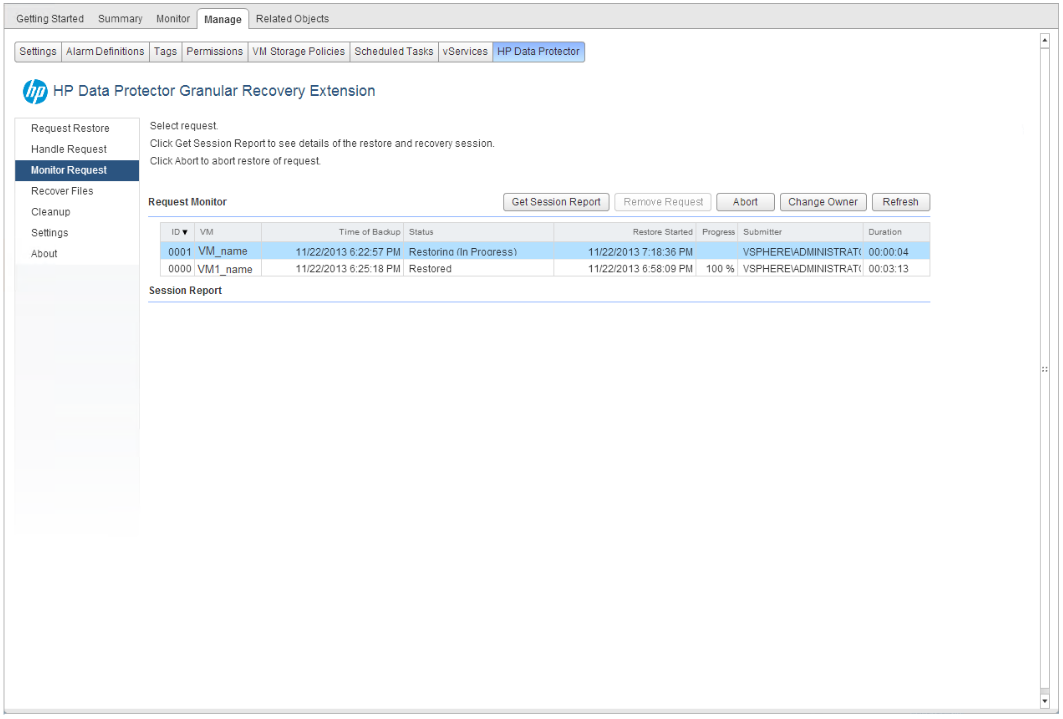
Monitoring restore requests

Procedure

To monitor restore requests:

1. In the HP Data Protector Granular Recovery Extension for VMware vSphere GUI, click the **Monitor Request** tab.

Figure 36: Monitor requests (Admin) page



HP Data Protector Granular Recovery Extension

Select request.
Click Get Session Report to see details of the restore and recovery session.
Click Abort to abort restore of request.

Request Monitor

ID ▾	VM	Time of Backup	Status	Restore Started	Progress	Submitter	Duration
0001	VM_name	11/22/2013 6:22:57 PM	Restoring (In Progress)	11/22/2013 7:18:36 PM		VSPHERE\ADMINISTRAT(	00:00:04
0000	VM1_name	11/22/2013 6:25:18 PM	Restored	11/22/2013 6:58:09 PM	100 %	VSPHERE\ADMINISTRAT(	00:03:13

Session Report

The Request Monitor list displays all the pending and triggered restore requests. A restore request can have the following status: In Progress, Restored, Pending, or Failed.

2. Select your request identified by its ID number.

3. You can:

   - Click **Get Session Report** to display the following session information under Session Report.

State	Session Information
Restored	Restoring session information
Recovering	Recovery session information

   - Click **Remove Request** to delete the unwanted pending requests.

   - Click **Abort** that serves two functions depending on the state of request. For more details, see the below mentioned table.

State of request	Request status message
Recovering	Recovery of files are aborted.
Restoring	Restore of virtual machines are aborted.

   - Click **Change Owner** to change the owner of the recovery process. Enter a new owner in the

Change Owner text box and click **Change**.

- Click **Refresh** to update the status of your request.

Recovering files from virtual machines

Procedure

To recover files from virtual machine disks:

1. In the HP Data Protector Granular Recovery Extension page, click the **Recover Files** tab

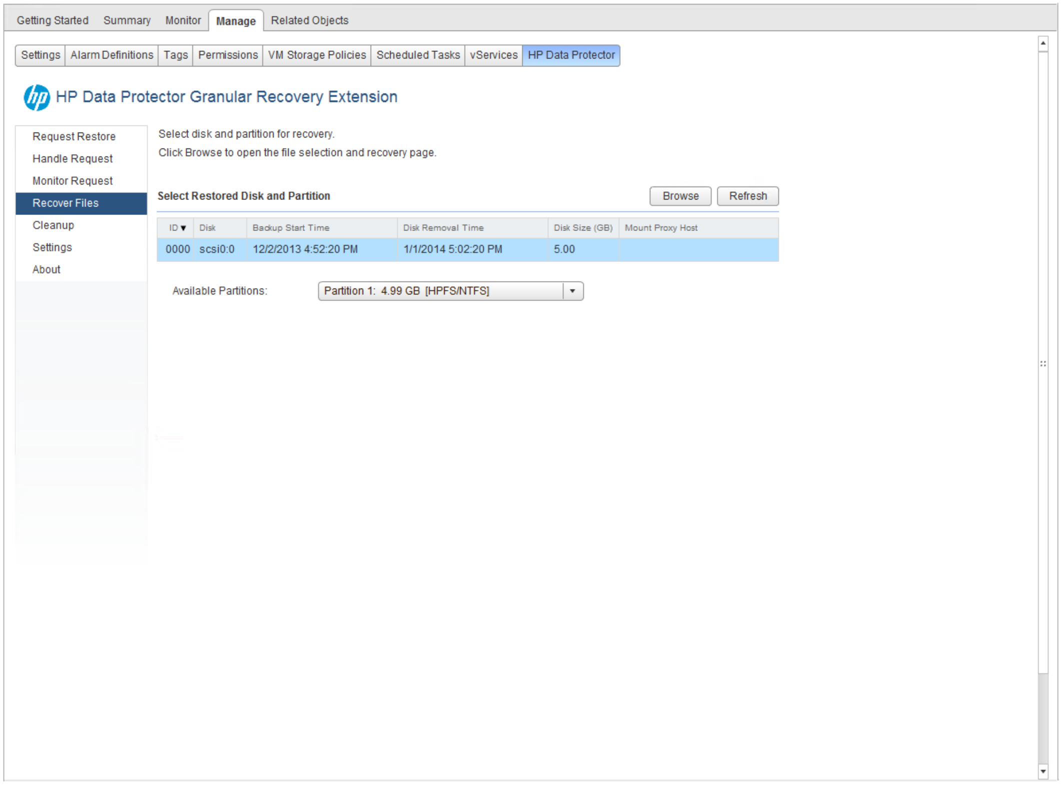
   The Select Restored Disk and Partition page is displayed.

   > **Note:** If you abort recovery of a large file and recovery does not finish in 5 seconds, the following status message is displayed: `Abort recovery of files is started for request id=xxxx`. When the recovery of the large file completes, the rest of the files stop recovering.

2. To select the virtual machine disk containing the files to recover, proceed as follows:

   a. In the **Available Partitions** drop-down list, select the desired partition and its type (Windows or Linux).

Figure 37: Recovering files (select the Windows partition for browse)



Select disk and partition for recovery.
Click Browse to open the file selection and recovery page.

Select Restored Disk and Partition

ID ▾	Disk	Backup Start Time	Disk Removal Time	Disk Size (GB)	Mount Proxy Host
0000	scsi0:0	12/2/2013 4:52:20 PM	1/1/2014 5:02:20 PM	5.00	

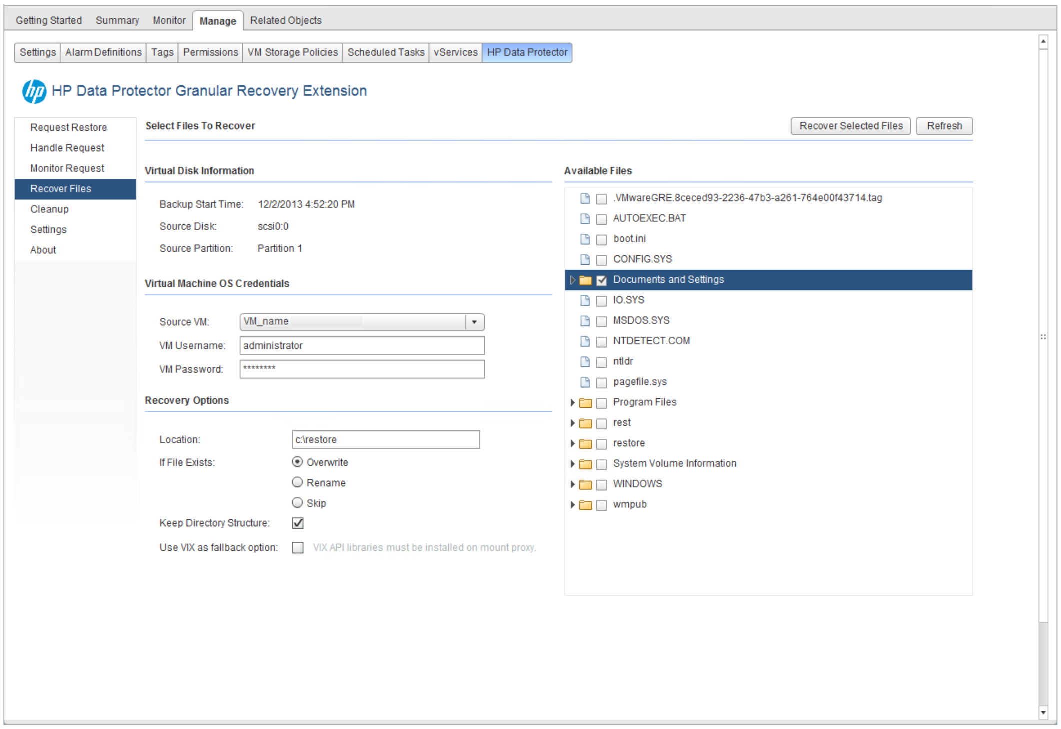
Available Partitions: Partition 1: 4.99 GB [HPFS/NTFS]

A new **Available Partitions** drop-down list is displayed that contains the logical volumes.

b. Select a logical volume and click **Browse**.

   The Select Files To Recover page is displayed.

Figure 38: Recover files from the selected disk



Select Files To Recover

Virtual Disk Information

Backup Start Time: 12/2/2013 4:52:20 PM
Source Disk: scsi0:0
Source Partition: Partition 1

Virtual Machine OS Credentials

Source VM: VM_name
VM Username: administrator
VM Password: ********

Recovery Options

Location: c:\restore
If File Exists: ● Overwrite ○ Rename ○ Skip
Keep Directory Structure: ☑
Use VIX as fallback option: □ VIX API libraries must be installed on mount proxy.

Available Files

- □ .VMwareGRE.8ceced93-2236-47b3-a261-764e00f43714.tag
- □ AUTOEXEC.BAT
- □ boot.ini
- □ CONFIG.SYS
- ☑ Documents and Settings
- □ IO.SYS
- □ MSDOS.SYS
- □ NTDETECT.COM
- □ ntldr
- □ pagefile.sys
- □ Program Files
- □ rest
- □ restore
- □ System Volume Information
- □ WINDOWS
- □ wmpub

3. Under Virtual Machine OS Credentials, select the virtual machine from the **Source VM** drop-down list, and enter its credentials in the VM Username and VM Password text boxes.

4. In the Location text box, enter the target recovery location path.

   - For locations on Windows systems, use the format `DriveLetter:\Folder\Subfolder`.

   - For locations on Linux systems, use the format `/Directory/Subdirectory`.

   Note: For shared directories, enter the path without the hostname. For example, in case of an NFS share hostname: `/shared_dir/subdir`, use `/shared_dir/subdir`. Also, ensure that the Samba and NFS shares are set up correctly. The NFS share must also be exported as pseudo root shares.

   Any missing directories in the path are created automatically. For example, if you specify `/shared_dir/subdir1/subdir2`, the `subdir1/subdir2` subdirectories are automatically created inside `/shared_dir`.

5. If the file already exists on the target system, select one of the following recovery options:

- **Overwrite**: deletes the original files and folders, and saves the latest files and folders.
- **Rename**: keeps the original files and folders, and saves the recovered files and folders with the name string pathname.timestamp.
- **Skip**: keeps the original files and folders.

6. Select **Keep Directory Structure** to maintain the original directory structure of the source virtual machine disk on the target system.
7. Select **Use VIX as fallback option** when network share is not available.
8. Under Available Files, select the files and folders to be recovered.
9. Click **Recover Selected Files**.

Removing virtual machine disks

Procedure

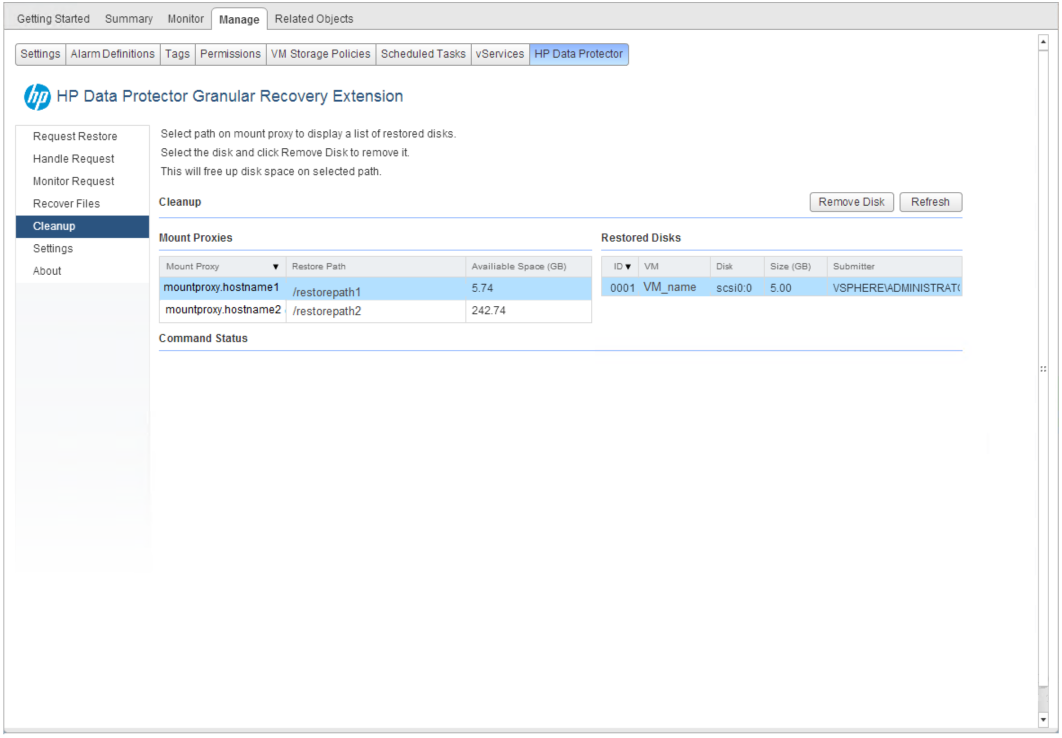
When the specified retention period expires, the virtual machine disks are deleted automatically. You can remove the virtual machine disks manually, if you want to remove the disks before the retention period. Otherwise, the manual removal is not recommended.

To delete virtual machine disks manually:

1. In the HP Data Protector Granular Recovery Extension for VMware vSphere GUI, click the **Cleanup** tab.

   The Cleanup page is displayed.

Figure 39: Removing disks



Select path on mount proxy to display a list of restored disks.
Select the disk and click Remove Disk to remove it.
This will free up disk space on selected path.

Cleanup

Mount Proxies

Mount Proxy ▼	Restore Path	Availiable Space (GB)
mountproxy.hostname1	/restorepath1	5.74
mountproxy.hostname2	/restorepath2	242.74

Restored Disks

ID ▼	VM	Disk	Size (GB)	Submitter
0001	VM_name	scsi0:0	5.00	VSPHERE\ADMINISTRAT(

Command Status

2. Under Mount Proxies, select the mount proxy and the restore path from where you want to remove the disks.

   The table in the Restored Disks area displays the restored virtual machine disks in the selected path.

3. Under Restored Disks, select the desired disk and click **Remove Disk** to remove the restored virtual machine disk from the mount proxy system.

   A confirmation message is displayed in the Command Status area.

About Granular Recovery Extension

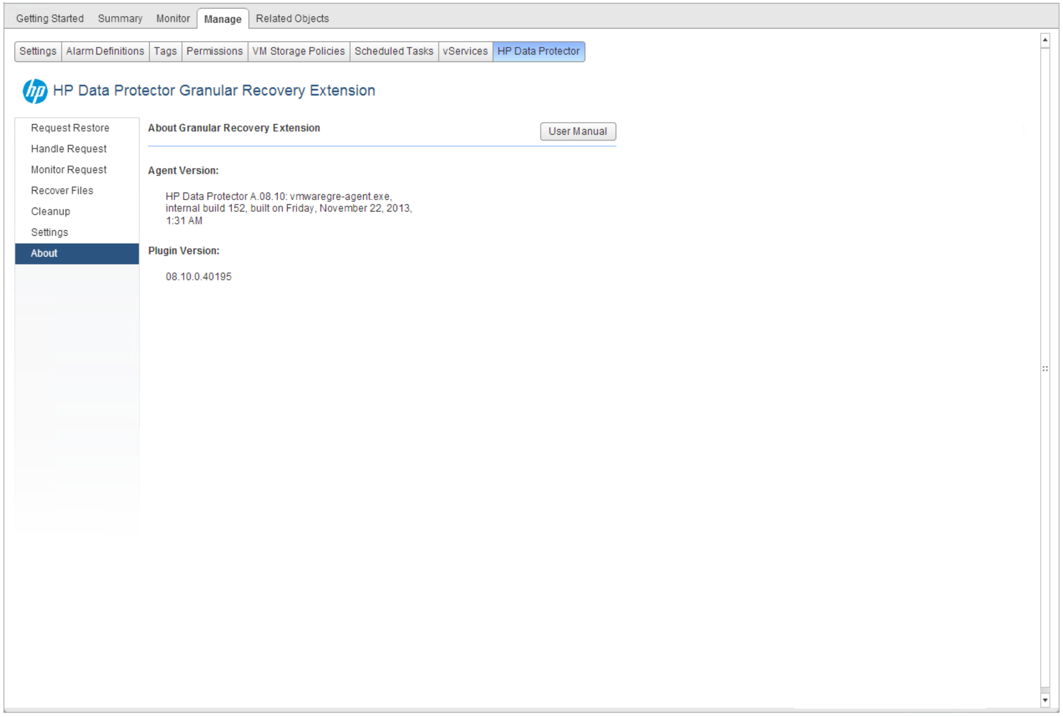
Procedure

To know about the VMware Granular Recovery Extension agent and Plugin version:

1. In the HP Data Protector Granular Recovery Extension for VMware vSphere GUI, click the **About** tab.

   The About Granular Recovery Extension page is displayed.

Figure 40: About Granular Recovery Extension GUI (Administrator mode)



About Granular Recovery Extension

Agent Version:

HP Data Protector A.08.10: vmwaregre-agent.exe,
internal build 152, built on Friday, November 22, 2013,
1:31 AM

Plugin Version:

08.10.0.40195

2. Click **User Manual** to download a copy of the *HP Data Protector 8.10 Granular Recovery Extension User Guide for VMware vSphere*.

> **Note:** You can download the GRE guide if the Data Protector documentation component is installed on the vCenter Server.

Chapter 6: Troubleshooting

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

- For Virtualization Environments troubleshooting information, see the troubleshooting section of the VMware part about the Data Protector Virtual Environment integration, in the HP Data Protector Integration Guide for Virtualization Environments.

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

Before you begin

- To enable debugging, see "Enabling debugging option" below.

- Ensure that the latest official Data Protector patches are installed. See the *HP Data Protector Help* index: “patches” on how to verify this.

- For general Data Protector limitations, as well as recognized issues and workarounds, see the *HP Data Protector Product Announcements, Software Notes, and References*.

- For an up-to-date list of supported versions, platforms, and other information, see http://support.openview.hp.com/selfsolve/manuals.

Debugging

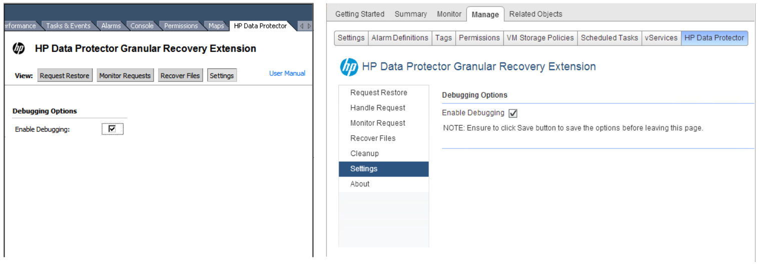
Enabling debugging option

1. If you encounter an issue when using this extension, the information in the log files can help you determine the problem. To enable the debugging option, locate the Settings page by clicking the **Settings** button. The Settings page is displayed.

2. Locate the Debugging option, select **Enable Debugging**. When you close the vSphere client interface this option is cleared, and the debugging option for this extension disabled.

   For detailed descriptions of the Data Protector log files, see the HP Data Protector Troubleshooting Guide, index: “Contents of log files”.

Figure 41: Debugging option enabled in Desktop and Web Client



HP Data Protector Granular Recovery Extension

Debugging Options

Enable Debugging: ☑

HP Data Protector Granular Recovery Extension

Debugging Options

Enable Debugging ☑

NOTE: Ensure to click Save button to save the options before leaving this page.

Log files are located in the default Data Protector log files directory and the default temporary files directory.

For a list of known issues and workarounds, see "Known issues and workarounds" below.

Known issues and workarounds

Mounting virtual machine disks

Problem

When performing recovery of files, the following message is displayed after selecting a partition:

```
[EXCEPTION] boost: filesystem: status: The volume does not contain a recognized file
system. Please make sure that all required file system drivers are loaded and that
the volume is not corrupted: "\\?\M:\" ProxyGetAllNodesForPath.
```

After mounting the virtual disks manually, the following is displayed in the command line interface:

```
The volume does not contain a recognized file system. Please make sure that all
required file system drivers are loaded and that the volume is not corrupted
```

Your configuration is not supported. The extension and the VMware VDDK do not support GPT disk layout and dynamic disks. This is a known VMware-mount limitation. The issue may occur when a partition does not contain any file system, or it contains a different unsupported file system.

Action

- For Windows virtual machine disks, use one of the supported file systems, for example NTFS or FAT system formats.
- For Linux virtual machine disks, use NTFS or FAT system formats, or one of the supported Linux file systems.

For a list of supported file systems, see the latest support matrices at http://support.openview.hp.com/selfsolve/manuals.

Inability to browse a virtual machine disk

Problem

When browsing a virtual machine disk, an external error is reported

When you try to browse a virtual machine disk in the vSphere Client, the following error message is displayed in a pop-up window:

```
External utility reported error
```

The error details read:

```
/opt/omni/lib/vddk/vmware-mount -K VirtualDiskRestorePath/Hostname.vmdk:
```

```
umount VirtualDiskMountPoint: device is busy. (In some cases useful info about
processes that use the device is found by lsof(8) or fuser (1) ) Failed to unmount
all partitions on disk 'VirtualDiskRestorePath/Hostname.vmdk': umount command failed
```

This problem occurs after the `vmware-mount` utility fails to delete the lock for the mounted disk after dismounting it. The Data Protector VMware Granular Recovery Extension Agent is therefore unable to mount the disk again.

Action

Delete the *`Hostname`*`.vmdk.lck` directory from the *`VirtualDiskRestorePath`* folder.

Issues after removing the extension

Problem

You removed the `VMware Granular Recovery Extension Agent` component and the post-install script. When you remove the component, the removal tries to delete the driver. If the removal command is not successful, the driver stays in the stopped state. Even after repeating the installation procedure the driver stays in a stopped state.

When you try again to install the `VMware Granular Recovery Extension Agent` component, the HP Data Protector Manager displays the following message in the monitor session:

```
Status: SERVICE_NAME: vstor2-mntapi10-shared
```

```
[Critical] computer.company.com Post-installation script for the VMware Granular
Recovery Extension Agent failed with the output
```

```
Data_Protector_home\bin
```

```
perl -I "..\lib\perl" vmwgre_ag.pl -install
```

In the command line interface this message is displayed:

```
Installation of driver failed: System error 2 has occurred.
```

Action

Check the driver status by running the command:

```
sc query vstor2-mntapi10-shared
```

Check if the service state is `RUNNING`. If not, remove the service and run the command:

```
sc delete vstor2-mntapi10-shared
```

Check if the service is removed and start a remote installation of the `VMware Granular Recovery Extension Agent` component.

Note: If the vdkm driver is already installed on the system and running, then this driver is used; it is not removed or reinstalled. The upgrade procedure is successful.

VMware VirtualCenter Management Webservices service is not running

Problem

The debug log file contains the following message:

```
File not found - C:\Program Files (x86)
\VMware\Infrastructure\tomcat\webapps\VMWareGRE\register.xml
```

```
There is a problem with VMware VirtualCenter Management Webservices service. Check
that the target system has VMware VirtualCenter Management Webservices running.
```

Action

Check if the `C:\Program Files (x86)\VMware\Infrastructure\tomcat\webapps\VMWareGRE` folder exists. If it exists, remove it. The VMware VirtualCenter Management Webservices service should create a new folder automatically. Run the script: *`Data_Protector_home`*`\bin\vmwgre_wp.cmd`

If folder does not exist, VMware VirtualCenter Management Webservices is probably not started. Start it, check that the folder is created and run the script: *`Data_Protector_home`*`\bin\vmwgre_wp.cmd`.

RSA certificates with keys that are less than 1024 bits long are blocked

Problem

After installation of the Microsoft Security Advisory update (KB2661254), connection to the vCenter Server VMware GRE plugin may fail.

Action

This happens because the VMware vCenter Server by default uses RSA certificates which are 512 bits and the update in Microsoft Security Advisory kb2661254, blocks the use of RSA certificates which are less than 1024 bits long.

For more details, on the resolution see
http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2037082

and Microsoft Security Advisory update: **kb2661254** = http://support.microsoft.com/kb/2661254

Remote installation of VMware Granular Recovery Extension Web Plug-In ends unexpectedly

Problem

The remote installation of VMware Granular Recovery Extension Web Plug-In ends unexpectedly. In the `debug.log` file on the target system the following message is displayed:

```
Log on to Virtual Center  computer.company.com  could not be performed. Web service
error: No connection could be made because the target machine actively refused it.
```

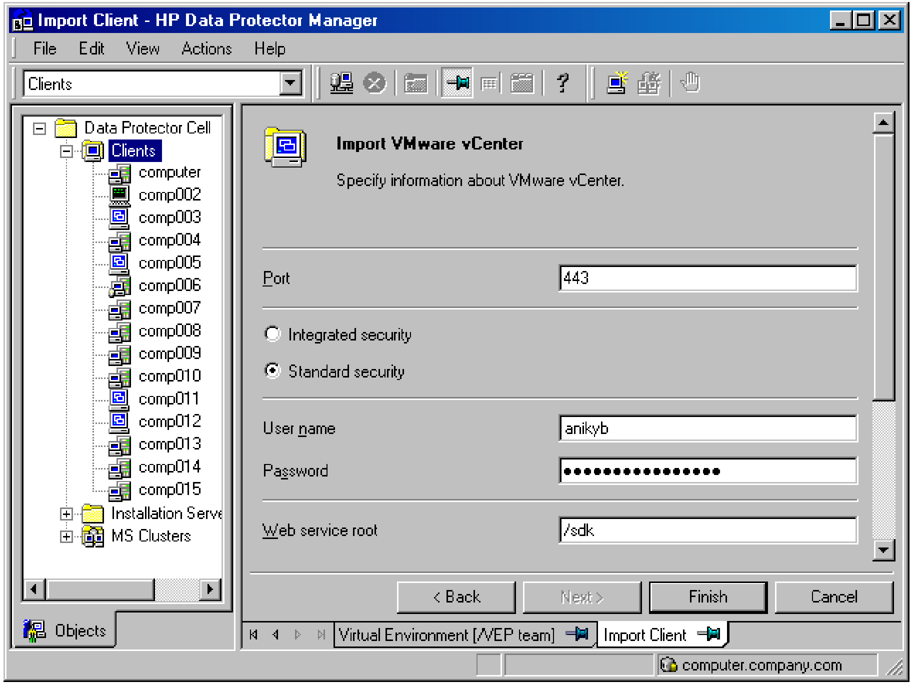
Or:

```
Log on to Virtual Center computer.company.com could not be performed. Details: Web
service error: Cannot complete login due to an incorrect user name or password.
```

Action

Ensure the user credential information and the correct port number are specified on the following HP Data Protector client import settings page:

Figure 42: User credentials during the import client procedure



Import VMware vCenter

Specify information about VMware vCenter.

Port: 443

○ Integrated security
● Standard security

User name: anikyb
Password: ••••••••••••••••

Web service root: /sdk

VMware Granular Recovery Extension Web Plug-In installation fails

Problem

The post-installation script for the `VMware Granular Recovery Extension Web Plug-In` fails with the following error message:

```
C:\Program Files\OmniBack\bin>perl -I "..\lib\perl" vmwgre_wp.pl -install
```

```
There was a problem during VMware Granular Recovery Extension Web Plug-In
installation. Check if the target system has VMware vCenter Server installed and
configured.
```

Action

1. Navigate to the installation `log` file under `C:\Program Files\OmniBack\tmp` to determine the failure of the post-installation script.

   > **Note:** The created installation log file is of the form: `OB2DBG_...__VMWGRE_WP_...txt`.

   The possible causes are:

   - The Data Protector client is not installed on vCenter host and imported as VMware vCenter to Data Protector Cell.
   - The username and password specified when importing the vCenter host to the Data Protector cell are not valid.
   - Due to some leftovers from the previous installation.
   - The `Auto deploy` is not enabled on the vCenter Tomcat web server.

2. Fix the possible causes and push the component again.

Mounting of LVM logical volumes fail when deploying VMware GRE on Linux

Problem

When you try to browse an LVM logical volume, it fails with the following error message:

```
There are no partitions on selected disk.
```

Action

To allow the VDDK VIX mount to work, proceed as follows:

1. `fdisk /dev/<device_name>`
2. Create a new partition by pressing `n` and configure the settings for this partition.
3. After creating a partition, press `t` and set the partition type to `8e`.
4. Press `w` to write the partition table.
5. Create a physical volume on the newly created partition: `pvcreate /dev/<partition_name>`.
6. Create a volume group on the physical volume: `vgcreate <VGNAME> /dev/<partition_name>`.

7. Create a logical volume in the volume group: `lvcreate -l <Total PE> -n <LVNAME> /dev/<VGNAME>`.

   > **Note:** `<Total PE>` refers to the size of the volume group. You can get that using `vgdisplay -v <VGNAME>`.

8. Create a file system over the newly created logical volume: `mkfs -t ext3 /dev/<VGNAME>/<LVNAME>`.

9. Mount the logical volume to any location of your choice.

   > **Note:** You can view that there is one LVM partition in the disk if you run the `fdisk -l over /dev/<partition_name>` command. Hence, the VDDK VIX mount locates the partitions on the selected disk and mounts them.

VMware Granular Recovery Extension tab is missing

Problem

You connected with vSphere Client to vCenter. When you select a virtual machine in the VMs and Templates view, there is no HP Data Protector tab, the extension is missing. The root cause is the firewall is probably preventing communication.

Action

On the vCenter server, configure the Windows Firewall. Select the Exceptions tab and **Add port** of the VMware vCenter Server-Web Services HTTPS (default 8443) to the exceptions list, and restart the vSphere Client interface.

VMware Granular Recovery Extension tab is missing with vCenter Server plug-in disabled

Problem

You connected with vSphere Client to vCenter. When you select a virtual machine in the VMs and Templates view, there is no HP Data Protector tab, and the extension is missing. The root cause is an installation that ended abnormally.

Action

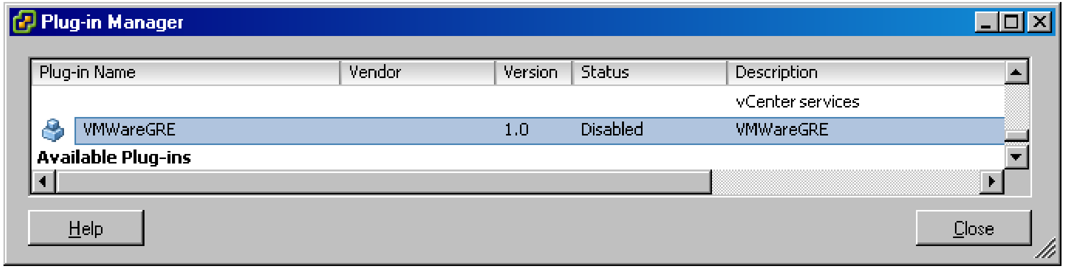
1. On the vCenter server, remove the extension from the system.

2. Remotely install the extension again. For details, see "VMware vCenter Server system" on page 18.

3. Connect with the vSphere Client interface to a vCenter Server system, and click **Plug-ins**. The Plug-in Manager window is displayed.

4. Under the Plug-in Name column, locate VMwareGRE, right click it, and click **Enable**.

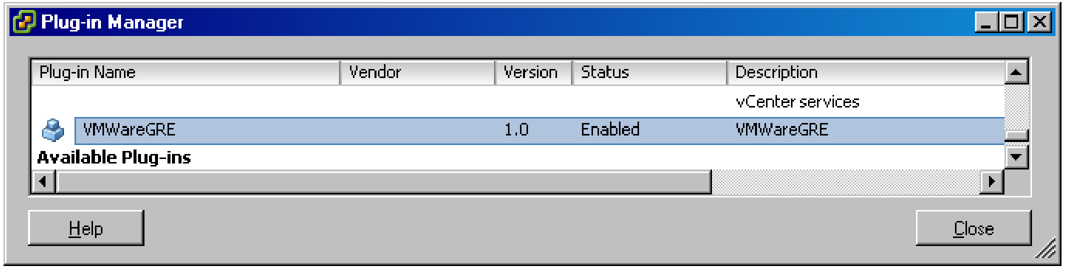
Figure 43: Extension disabled



Plug-in Name	Vendor	Version	Status	Description
				vCenter services
VMWareGRE		1.0	Disabled	VMWareGRE

Available Plug-ins

Figure 44: Extension enabled



Plug-in Name	Vendor	Version	Status	Description
				vCenter services
VMWareGRE		1.0	Enabled	VMWareGRE

Available Plug-ins

HP Data Protector cannot add any Granular Recovery Extension component

Problem

HP Data Protector cannot add components. The probable root cause is that HP Data Protector was installed on your system in the following order:

1. Data Protector cell and client, was imported with the `Virtual Environment Integration agent` enabled on it.

2. The HP Data Protector client was imported.

Action

1. Re-import the HP Data Protector client.

2. Import the `Virtual Environment Integration agent` and select VMware as the client type.

Local installation workaround

Problem

You cannot install the extension remotely on your system.

Action

Install the extension on your local system.

For details of the importing procedure, see "Importing VMware vCenter Server" on page 18.

Local installation workaround

1. To install this extension on a Data Protector cell system, follow these steps:

   Install the `VMware Granular Extension Web Plug-In` component or the `VMware Granular Recovery Extension Agent` component by changing the directory to:

   Insert the Windows installation DVD-ROM by changing the directory to:

   32–bit Windows systems:

   `\Windows_other\i386`

   64–bit Windows systems:

   `\Windows_other\x8664`

2. Run the `VMware Granular Extension Web Plug-In` component installation:

   The \ denotes continuation of the command line.

   ```
   csetup.exe /quiet ADDLOCAL=core,vmwaregre_webplugin \

    INSTALLATIONTYPE="Client" \

   CELLNAME="CellManagerSystemName" \

   CELLCLIENTNAME="VirtualCenterSystemName" \

   INSTALLDIR="InstallationPath"\

   INETPORT=InetPort OPTDNSCHECK=1 OPT_MSG=1 \

   PUSHADDUPG=1
   ```

   Run the `VMware Granular Recovery Extension Agent` component installation:

   ```
   csetup.exe /quiet ADDLOCAL=core,vmwaregre_agent \

   INSTALLATIONTYPE="Client" \

   CELLNAME="CellManagerSystemName" \

   CELLCLIENTNAME="TargetSystemName" \

   INSTALLDIR="InstallationPath" \

   INETPORT=InetPort OPTDNSCHECK=1 OPT_MSG=1 \

   PUSHADDUPG=1
   ```

Monitor displays request removed by administrator

Problem

A message, similar to the following is displayed when monitoring your request:

```
0030 scsi0:1 2/17/2011 10:35:07 AM Removed by administrator 3.00
```

Your administrator has removed this disk.

Action

- To recover your files, ensure that you request a new restore for this removed disk.

  For details on the procedure, see "Restore and recovery" on page 28.

Overwritten files issues

Problem

A message, similar to the following is displayed when recovering items with the **Overwrite** option selected:

The \ denotes continuation of the command line.

```
[Failed] c:\vix_27-2\incremental-21-2\incremental\ \

 Username \CheckVix\vixlibs\arp.ico

Source:\incremental-21-2\incremental\Username\CheckVix\ \

vixlibs\arp.ico

You do not have access rights to this file.

[Failed] c:\overwrite_incr-21-2\incr24-2\incremental-21-2\ \

incremental\Username\CheckVix\vixlibs\vix.h

Source:\incr24-2\incremental-21-2\incremental\Username\ \

CheckVix\vixlibs\vix.h

[5] Access is denied.
```

The item already exists on the target system. This item cannot be overwritten due to the file security option. If the source location contains NTFS file system and the target virtual machine disk are on the network, the Granular Recovery Extension for VMware recovers all security information associated with the items. This information cannot be overwritten.

Action

If the item already exists in the target location, perform one of the following instead:

- Recover these items to another location.
- Select the **Skip** recovery option.
- Select the **Rename** recovery option.
- Change the file permissions on the target location manually before starting recovery.

Missing VIX API libraries

Problem

File recovery fails due to missing VIX API libraries with the following error message:

```
Could not start recovery.
```

```
Cannot find support libraries; Vix appears to have not been installed.
```

Action

1. Install VMware tools on the target VM.
2. Install VMware VIX API on the mount proxy system:
   - Windows: VMware VIX API 1.13.0
   - Linux: VMware VIX API 1.12.2

Insufficient permission in the Host Operating System

Problem

The following error message is displayed when performing the recovery of files:

```
Insufficient permission in host operating system.
```

Action

The user entered when importing the vCenter to the DP cell must have the following permission assigned on the vCenter:

```
Virtual machine -> Interaction-> Guest operating system management by VIX API
```

Authentication failure or insufficient permission in the Guest Operating System

Problem

The following error message is displayed when performing the recovery of files:

```
Authentication failure or insufficient permissions in guest operating system.
```

Action

The user entered when specifying the options for the recovery of files in the Web Plug-In GUI must be able to log in to the target VM. The user can perform only the operations to which access rights has been provided on the target machine.

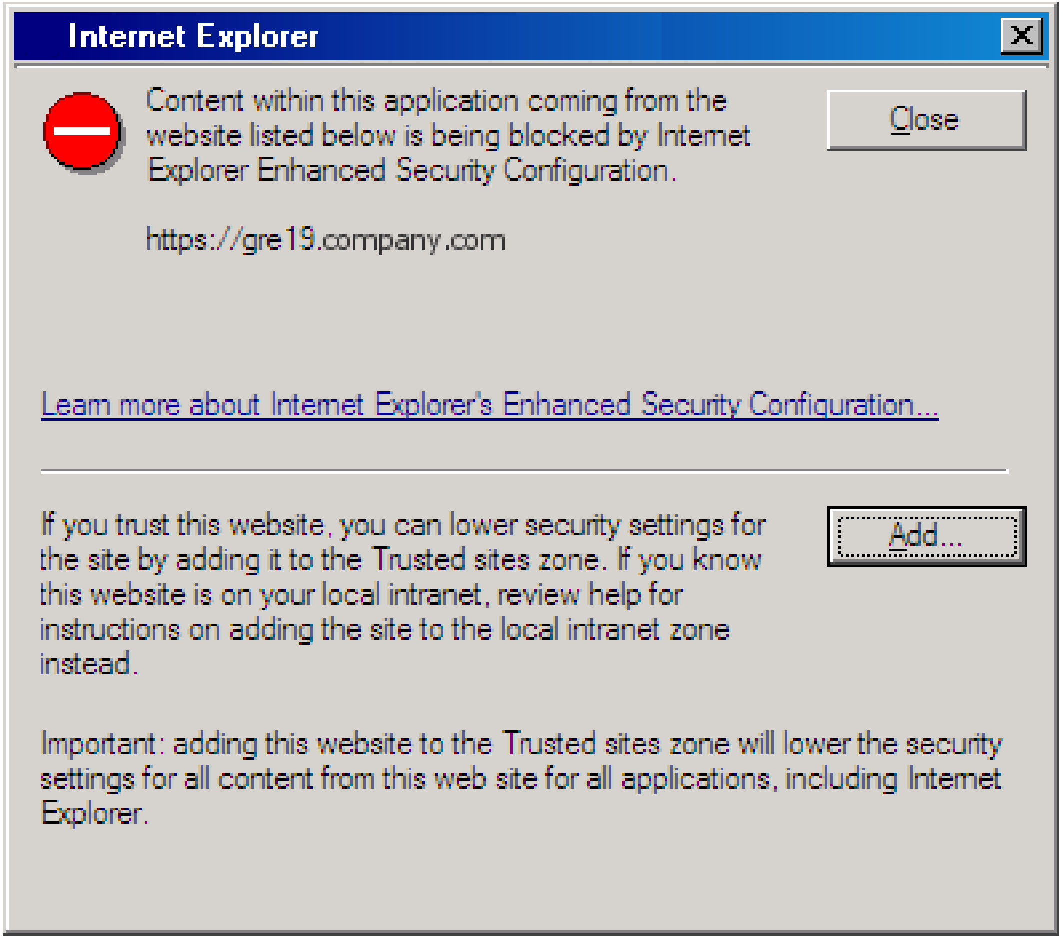
For example, if you want to write to a folder, you need to have permissions to recover files to that folder.

Opening the extension with script errors

Problem

After you install the extension and attempt to open the extension interface for the first time, the following Internet Explorer pop-up windows are displayed:

Figure 45: Blocked website message displayed by Internet Explorer



Internet Explorer

Content within this application coming from the website listed below is being blocked by Internet Explorer Enhanced Security Configuration.

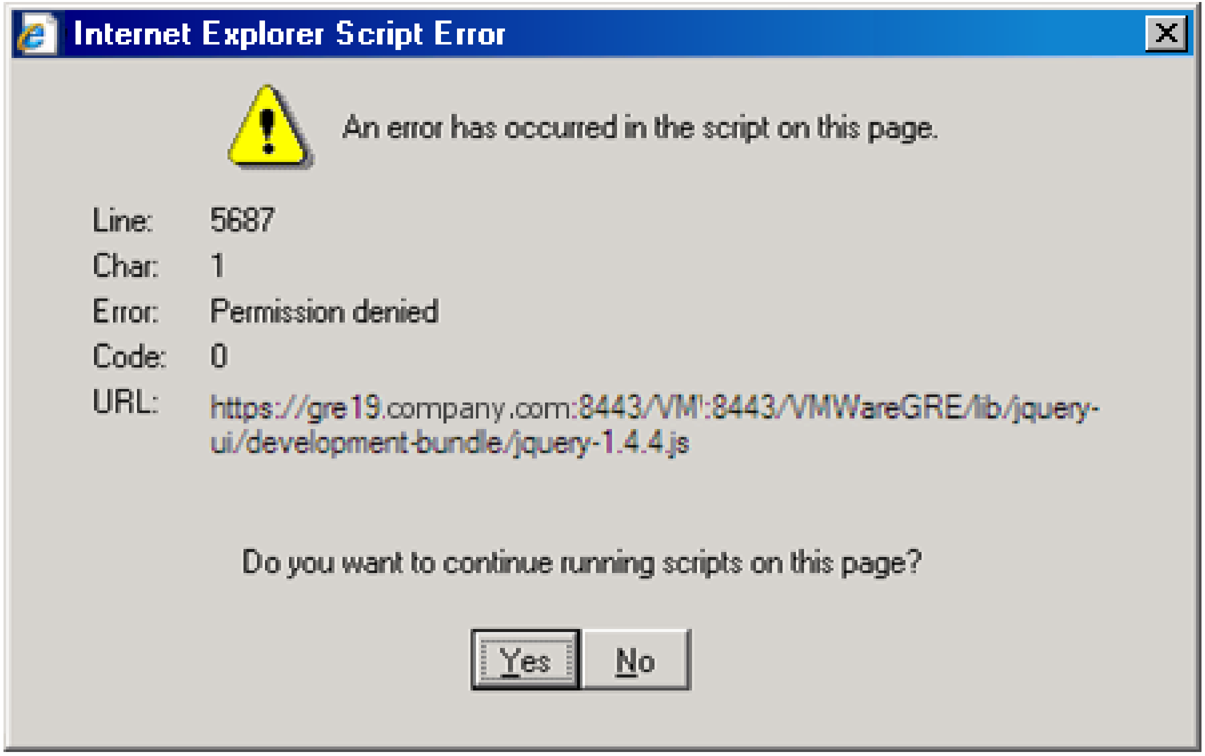
https://gre19.company.com

Learn more about Internet Explorer's Enhanced Security Configuration...

If you trust this website, you can lower security settings for the site by adding it to the Trusted sites zone. If you know this website is on your local intranet, review help for instructions on adding the site to the local intranet zone instead.

Important: adding this website to the Trusted sites zone will lower the security settings for all content from this web site for all applications, including Internet Explorer.

Figure 46: Script error message displayed by Internet Explorer



Internet Explorer Script Error

An error has occurred in the script on this page.

Line: 5687
Char: 1
Error: Permission denied
Code: 0
URL: https://gre19.company.com:8443/VM':8443/VMWareGRE/lib/jquery-ui/development-bundle/jquery-1.4.4.js

Do you want to continue running scripts on this page?

Additional pop-up windows may appear, containing similar error messages:

```
An error has occurred in the script on this page. Offset.setoffset is null or not an
object. Code 0
```

```
Object does not support this property or method.
```

Action

To resolve the problem, lower the security settings and add the web service entry point URI to the list of trusted sites:

1. When the pop-up window displayed on " Blocked website message displayed by Internet Explorer " on the previous page appears, click **Add**. The Internet Explorer Script Error is displayed.

   See " Script error message displayed by Internet Explorer" above.

2. When the pop-up window displayed on " Script error message displayed by Internet Explorer" above appears, click **Yes** to continue running these scripts. When this error message dialog box is displayed again, click **Yes** to proceed.

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 Continuance Volumes to protect data on EMC Symmetrix standard devices. See also BCV.

BCV (EMC Symmetrix specific term)

Business Continuance Volumes, or BCV devices, are dedicated SLDs that are pre-configured in the ICDA on which the business continuation operation runs. BCV devices are assigned separate SCSI addresses, differing from the addresses used by the SLDs they mirror. The BCV devices are used as splitable mirrors of the primary EMC Symmetrix SLDs that need to be protected. See also BC and BC Process.

Boolean operators

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

boot volume/disk/partition

A volume/disk/partition 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 blobspace, dbspace, or logical log file.

DC directory

A directory that contains DC binary files, one for each configured Data Protector backup medium. DC directories constitute the Detail Catalog Binary Files part of the Data Protector Internal Database. See also Detail Catalog Binary Files (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 (Microsfot 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 mirrorcloens 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 confgiuration 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 aray 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 maintainance 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.

I

ICDA (EMC Symmetrix specific term)

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

IDB

See Internal Database (IDB).

IDB recovery file

A file that maintains information about completed IDB backup sessions and the backup media and backup devices used in them. If available, it significantly simplifies and speeds up offline recovery of the Internal Database in case of a Cell Manager disaster. Its filename is obdrindex.dat.

importing media

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

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

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

incremental backup

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

incremental backup (Microsoft Exchange Server specific term)

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

incremental mailbox backup

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

incremental restore (EMC Symmetrix specific term)

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

incremental ZDB

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

Incremental1 Mailbox Backup

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

Inet

A process that runs on each UNIX system or service that runs on each Windows system in the Data Protector cell. It is responsible for communication between systems in the cell and for starting other processes needed for backup and restore. The Inet service is started as soon as Data Protector is installed on a system. The Inet process is started by the inetd daemon.

Information Store (Microsoft Exchange Server specific term)

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

Informix Server (Informix Server specific term)

Refers to Informix Dynamic Server.

initializing

See formatting.

Installation Server

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

instant recovery (ZDB specific term)

A process in which a replica, produced by a ZDB-to-disk or a ZDB-to-disk+tape 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 optino 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 Protectorpoint 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 changes 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

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 VMware vSphere (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.