HP Data Protector

Software Version: 8.10

Integration Guide for Virtualization

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**

Contents

Part 1: VMware

Data Protector offers different ways to back up VMware virtual machines online. Choose the appropriate backup and restore solution depending on your VMware solution and the desired functionality.

VMware vSphere

To back up virtual machines from a VMware vSphere environment, you can use the following solutions:

- ***Data Protector Virtual Environment integration***

  This integration enables you to back up and restore the following VMware logical objects:

  - Datacenters
  - Virtual machines
  - Virtual machine disks
  - Virtual machine templates

  The integration uses the VMware vStorage API to communicate with VMware vSphere.

  See Data Protector Virtual Environment integration on page 13.

VMware vCloud Director

To back up virtual machines from a VMware vCloud Director environment, you can use the following solution:

- ***Data Protector Virtual Environment integration***

  This integration enables you to back up and restore the following VMware logical objects:

  - Virtual applications
  - Virtual machines

  The integration uses the VMware vStorage API to communicate with VMware vCloud Director.

  See Data Protector Virtual Environment integration on page 13.

Note: You can also back up VMware virtual machines using common Data Protector filesystem backup functionality, which operates on the file level. The smallest object that you can back up or restore this way is a file. To ensure data consistency, you must shut the virtual machines down before starting a backup session.

Table 1: Data Protector backup solutions for VMware

Feature		Filesystem backup [1]	Virtual Environment integration
Online backup			✓
Crash-consistent backup		✓	✓
Application-consistent backup			✓
Granularity		File	VM disk
Backup types	Full	✓	✓
	Incremental	✓	✓
	Differential	✓	✓
Are zero downtime backup and instant recovery supported?		✓	
Is VCB software required?			
Is changed block tracking supported?			✓
Where does the Data Protector component need to be installed?		• ESX Server system [2]	• Backup host [3]
Extra licenses needed		• Zero Downtime Backup (optional) • Instant Recovery (optional)	• On-line Extension

[1] Filesystem backup refers to backing up virtual machines as files from an ESX Server. It serves as a comparison to other integrations in the table.
[2] Filesystem backup refers to backing up virtual machines as files from an ESX Server. It serves as a comparison to other integrations in the table.
[3] The integration agent can be installed on a dedicated system, from which Data Protector remotely contacts vCenter Server or ESX Server system, increasing the range of support for VMware products compared with the Data Protector VMware (Legacy) integration.

Chapter 1: Data Protector Virtual Environment integration

Introduction

This chapter explains how to configure and use the Data Protector Virtual Environment integration for VMware vSphere and VMware vCloud Director. Data Protector integrates with VMware vSphere and VMware vCloud Director, including ESX Server, ESXi Server systems, and vCenter Server systems, to back up and restore the following **VMware objects**:

VMware vSphere:

- Virtual machines
- Virtual machine disks
- Virtual machine templates

VMware vCloud Director:

- Virtual applications
- Virtual machines

Note: The Data Protector Virtual Environment integration for VMware uses OpenSSL 1.0.2j.

Backup

The following backup methods are available:

- vStorage Image
- vCD vStorage Image

These are snapshot-based methods that can be used to back up virtual machines while powered off (**offline backup**) or actively used (**online backup**).

For details on the backup methods, see vStorage Image backup method on page 21.

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

- Full
- Incremental
- Differential

For details on the backup types see, Backup types on page 24.

Restore

Virtual machines can be restored:

- **To a datacenter** (integration with VMware vSphere)

  This datacenter can be a standalone ESX(i) Server system or any of the datacenters created and managed by a vCenter Server system.

- **To an organization** (integration with VMware vCloud Director)

  This organization can be any of the organizations created and managed by a VMware vCloud Director.

- **To a directory**

  This can be a directory on any client with the Data Protector `Virtual Environment` component installed. After such a restore, you need to manually move the restored virtual machine images to an ESX Server or ESXi Server system, using the VMware Converter.

This chapter provides information specific to the Data Protector Virtual Environment integration for VMware vSphere and VMware vCloud Director. For other limitations and recommendations, see the *HP Data Protector Product Announcements, Software Notes, and References*. For general Data Protector procedures and options, see the *HP Data Protector Help*.

Integration concepts

Supported environments

Data Protector supports environments where ESX Server and/or ESXi Server systems are managed through a vCloud Director (**vCloud Director environments**), through a vCenter Server (**vCenter environments**) as well as environments with standalone ESX and ESXi Server systems (**standalone ESX(i) Server environments**). Mixed environments, in which some of the ESX Server and/or ESXi Server systems are managed through a vCenter Server system and some are standalone, are also supported. You can even have multiple vCenter Server systems in your environment, each managing its own set of ESX Server and/or ESXi Server systems.

vCloud Director environment

VMware vCloud Director is software for managing resources from several vCenter Server systems. It enables you to create and manage virtual datacenters, each of which can be used by a different organization. Data Protector supports backup and restore of virtual machines from such virtual datacenters.

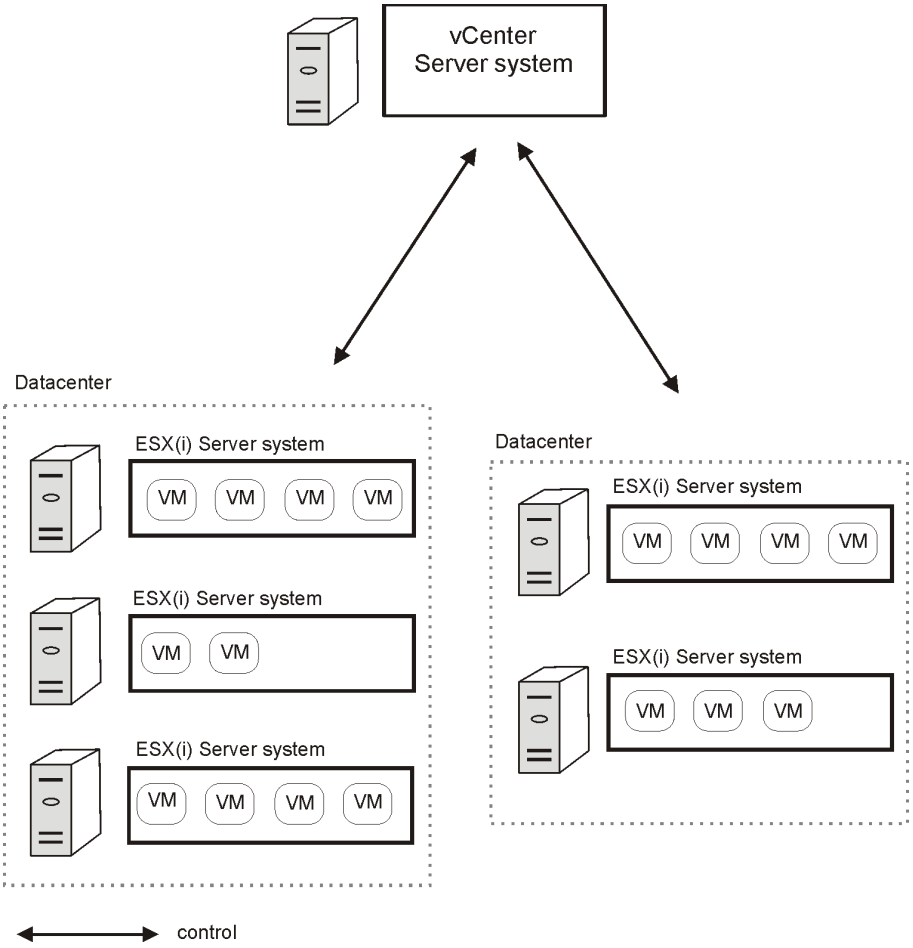
Note: To be able to back up virtual machines from virtual datacenters using the vCD vStorage Image backup method, make sure that you import all vCenter Server systems used by VMware vCloud Director in the Data Protector Cell as **VMware vCenter** clients.

vCenter environment

In a vCenter environment, Data Protector communicates with the VMware vSphere through the vCenter Server system. All backup and restore requests are sent there.

In one session, you can back up virtual machines from one or multiple datacenters.

Figure 1: vCenter environment



ESX Server or ESXi Server system	VMware platform capable of hosting multiple virtual machines.
VM	Virtual machine. Virtualized x86 or x64 PC environment, in which a guest operating system and associated application software can run.
Datacenter	An organizational unit that consists of one or more ESX Server and/or ESXi Server systems and the related storage for virtual machines (datastores). Datastores can reside on local disks/RAID, iSCSI or SAN storage.

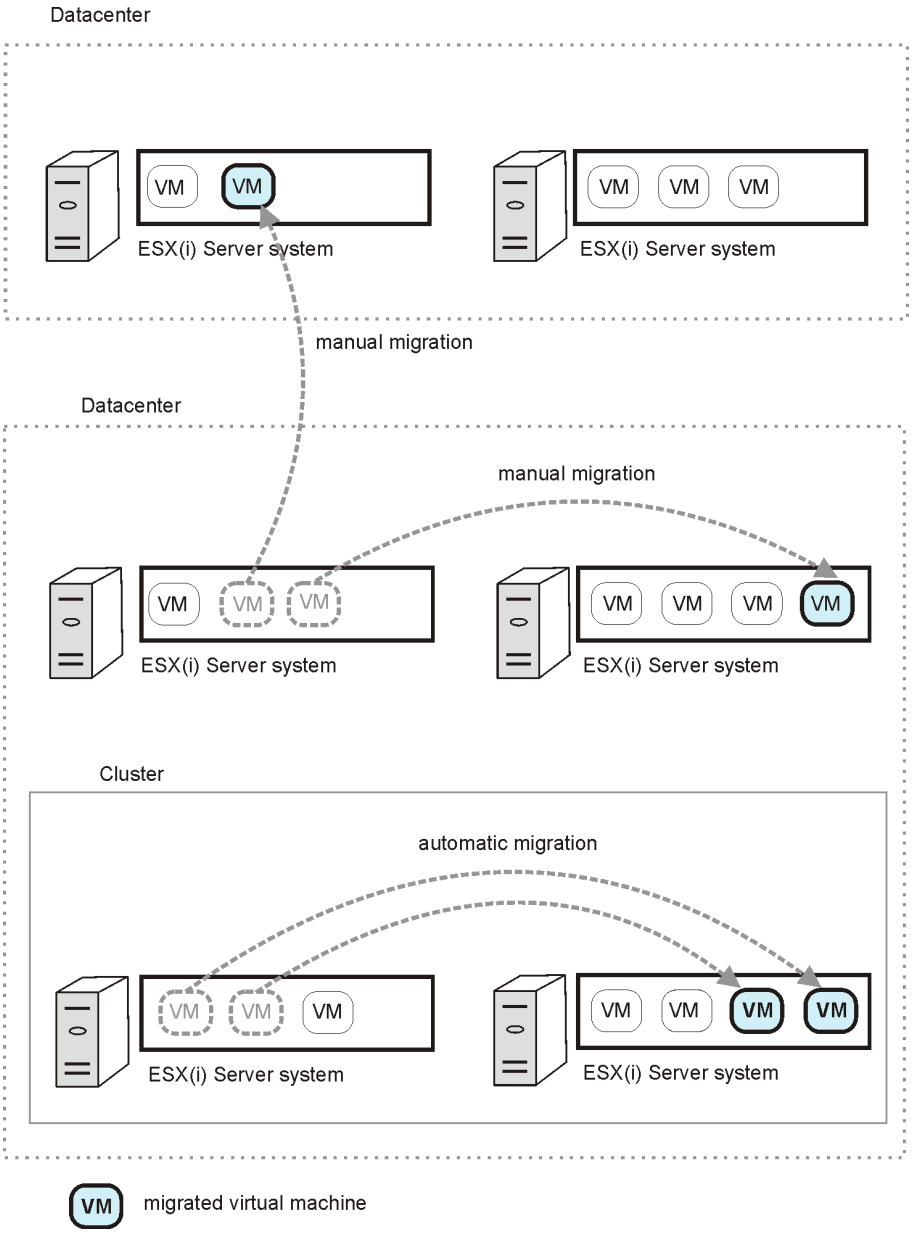
Migration of virtual machines

In a vCenter environment, Data Protector supports migration (using VMotion and Storage VMotion) of virtual machines between ESX(i) Server systems in the same datacenter and, for supported versions of VMware vSphere, in different datacenters.

Virtual machines migrate from one ESX(i) Server system to another for various reasons:

- If ESX(i) Server systems are configured in a **VMware high availability cluster**, virtual machines automatically migrate when the original ESX(i) Server system fails.
- If ESX(i) Server systems are configured in a **VMware load balancing cluster**, virtual machines automatically migrate to ESX(i) Server systems with less workload.
- You can start a migration of a virtual machine manually, using the VMware vSphere client.

Figure 2: Migration of virtual machines



Whatever the reason for the migration, you do not need to create a new backup specification afterwards. Data Protector will automatically find the migrated virtual machines and back them up.

vCenter Server system in a cluster

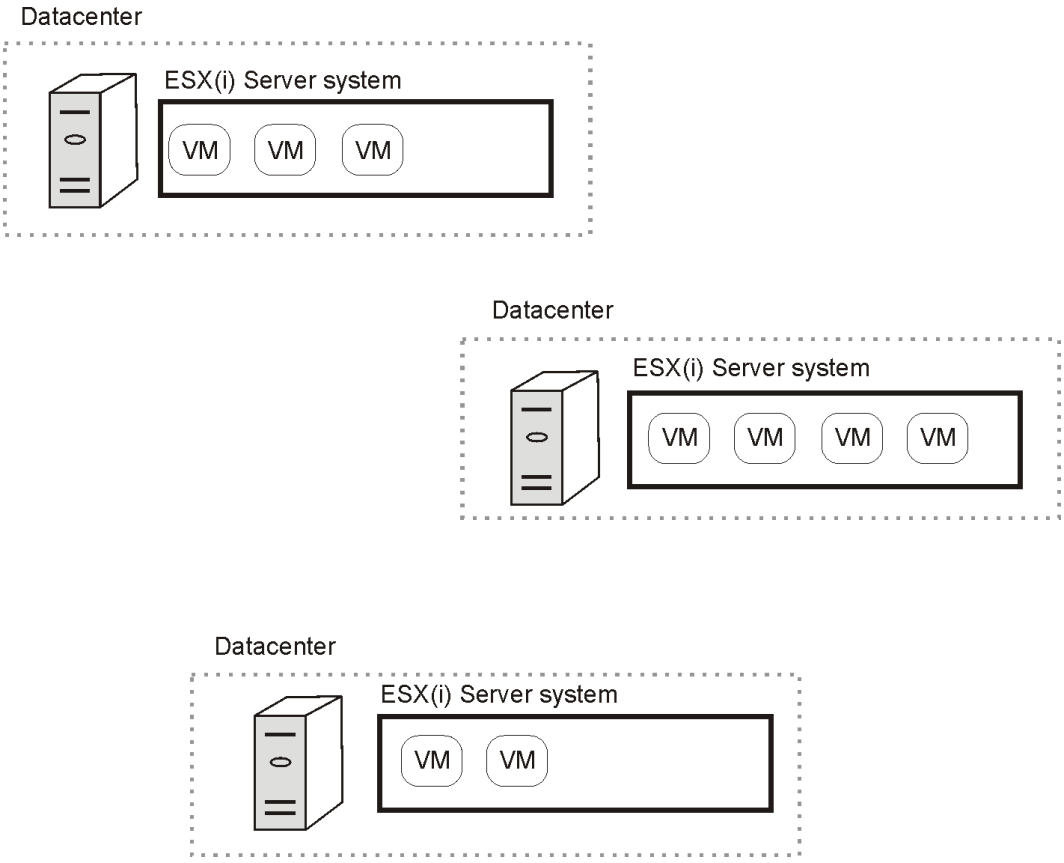
Data Protector also supports environments with a vCenter Server system in a Microsoft Cluster Service cluster. After a failover in such a cluster, you do not need to change the backup specification. However, if the failover occurs during a backup or restore session, the session fails and has to be restarted.

Standalone ESX/ESXi Server environment

In a standalone ESX(i) Server environment, Data Protector communicates with VMware vSphere through the ESX(i) Server system. All backup and restore requests are sent there.

In a single session, you can back up virtual machines from only one ESX(i) Server system.

Figure 3: Standalone ESX/ESXi Server environment



Data Protector components

Data Protector Cell Manager

The Data Protector Cell Manager can be installed on a virtual machine, vCenter Server system, or a separate system outside the virtualization environment.

Data Protector Virtual Environment Integration component

The Data Protector `Virtual Environment Integration` component (**VEAgent**) must be installed on at least one Data Protector client in the cell. This client will be called the **backup host** and can be:

- A virtual machine
- The vCenter Server system
- The Data Protector Cell Manager
- A dedicated physical backup host

The component includes the following major parts:

- `vepa_bar.exe`, activated during backup and restore operations on virtual environments.
- `vepa_util.exe`, activated during browsing and query operations on virtual environments.
- `vepalib_vmware.dll`, a dynamic link library for VMware vSphere specific backup, restore, query, and browsing tasks.
- `vepalib_vcd.dll`, a dynamic link library for VMware vCloud Director specific backup, restore, query, and browsing tasks.
- `vepalib_hyperv.dll`, a dynamic link library for Microsoft Hyper-V specific backup, restore, query, and browsing tasks.[1]

Note: VEPA stands for Virtual Environment Protection Agent.

Data Protector Disk Agent component

The Data Protector `Disk Agent` component must be installed on the backup host to use the browse directory button (this button is used when you restore to a directory on a backup host).

Data Protector Media Agents

The Data Protector `Media Agent` component must be installed on clients that will transfer data to backup devices.

Note: The `Virtual Environment Integration` component does not enable the backup host to write to backup devices. You still need a client with the `Media Agent` component installed. However, note that the `Cell Manager`, `Media Agent`, and `Virtual Environment Integration` components can all be installed together on the same system (physical or virtual).

[1]The Data Protector Virtual Environment integration can also be used to back up virtual machines from Microsoft Hyper-V virtualization environments. For details, see the Microsoft Hyper-V part.

Backup concepts

What is backed up?

Using the Data Protector Virtual Environment integration, you can back up the following VMware objects:

VMware vSphere:

- Virtual machines
- Virtual machine disks
- Virtual machine templates

VMware vCloud Director:

- Virtual applications
- Virtual machines

Data Protector identifies datacenters and virtual machines by their VMware vSphere inventory path. A standalone ESX Server system has only one datacenter `/ha-datacenter` and two folders: `/host` and `/vm`. Virtual machines are stored in the folder `/host`.

Example:

Datacenter: `/ha-datacenter`

Virtual machine: `/vm/myvm1`

In a vCenter environment, you can organize virtual machines and datacenters within folders that you create yourself. If you subsequently move a virtual machine, you do not need to create a new backup specification because Data Protector will find a virtual machine using its UUID.

Example:

Virtual machine: `/vm/myfolder1/myfolder2/.../myvm2`

Datacenter: `/myfolder/mydatacenter`

In a vCloud Director environment, you can organize virtual machines within vApps, vDatacenters, and organizations that you create yourself.

Example:

Virtual machine: `/ORG22/vDCOrg22/vAppORG22/vm1Org22`

Organization: `/vCD1/Mngmt/ORG22`

Virtual machines

When you back up a virtual machine, you actually back up virtual machine files of the following types:

- `.vmx`
- `.vmdk`
- `.vmsn`

Memory file

You can also specify that when a virtual machine is online during the backup, its memory is saved to a file and backed up together with other virtual machine files.

Note: The Backup memory file option can only be set at backup specification level (which means it applies to all virtual machines selected in the backup specification).

Virtual machine disks

Data Protector supports backup of individual virtual machine disks when using a VStorage Image backup method. In this case, all virtual machine files are backed up, except for virtual machine disks that are not specified. You can run full, incremental, and differential backups.

Note: After you add a new disk to a virtual machine, make sure you run a full backup session for the updated virtual machine.

Virtual machine templates

You can also back up virtual machine templates when using a VStorage Image backup method. When you create a backup specification, expand the **vm** folder and select the desired virtual machine templates.

vStorage Image backup method

The vStorage Image backup method provided by the Data Protector Virtual Environment integration is based on the VMware vStorage technology. For this method, a single central **backup host** is used to back up all virtual machines hosted by ESX(i) Server systems in a Data Protector cell. This backup host can be a dedicated physical host, a virtual machine, or the Cell Manager. The important thing is that it has the Data Protector `Virtual Environment Integration` component (**VEAgent**) installed.

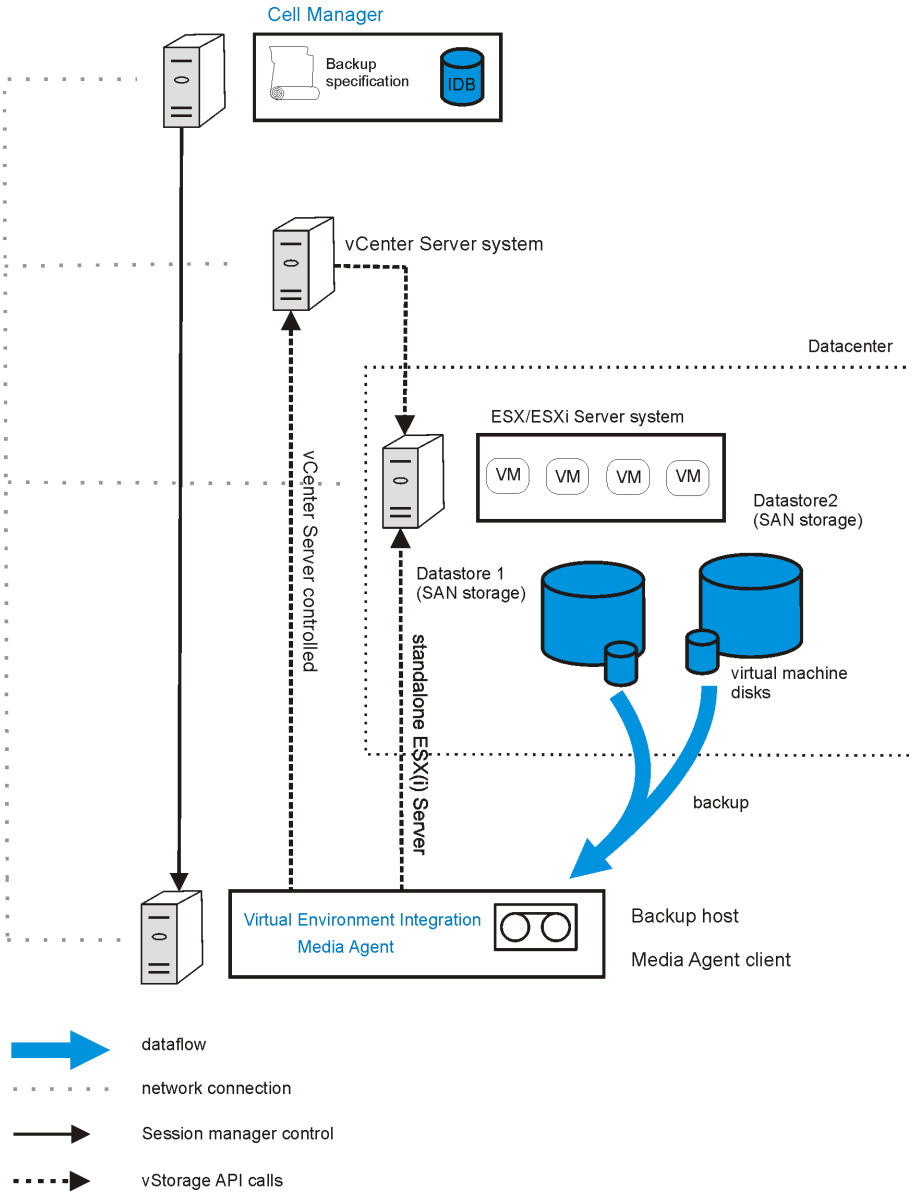
During a vStorage Image backup, VEAgent first establishes connections between the backup host and the virtualization host (an ESX(i) Server system). This connection can either be through a vCenter Server system (in the case of a vCenter environment), or direct (in the case of a standalone

ESX(i) Server environment). It then requests a snapshot of the virtual machine that is to be backed up, via the vStorage API for Data Protection (VADP). This snapshot is used during the period of the backup in order to keep the virtual machine in a consistent state.

VEAgent then opens the virtual machine disks across LAN or SAN, initializes the Media Agent client and controls the transfer to it of the virtual machine and all its associated data.

Note: You can use the `OB2_VEAGENT_OPEN_DISK_TIMEOUT` omnirc option to specify the time interval between opening two different disks. By default, a new disk is opened every 2 seconds.

Figure 4: vStorage Image method



In vStorage Image method on the previous page, the backup host is also a Media Agent client (it has the `Media Agent` component installed and a device connected to it).

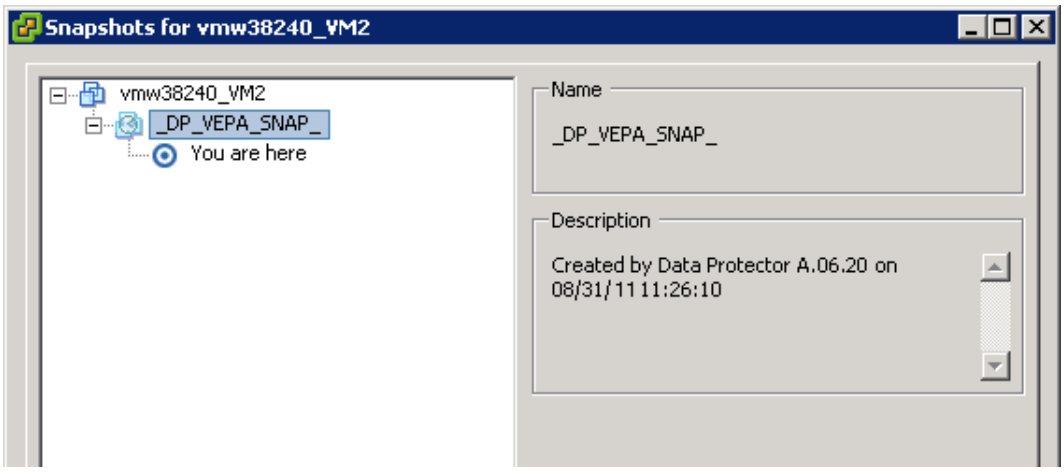
Snapshot management

The vStorage Image backup method relies on being able to create virtual machine snapshots. A virtual machine snapshot is an operation that puts the virtual machine into a consistent state. All subsequent changes made to the virtual machine disks are recorded to separate files. Note that snapshot operation is not supported by all virtual machine disks. For example, snapshots of independent disks are not supported; consequently, this type of virtual disks cannot be backed up using the Data Protector Virtual Environment integration. For details, see the VMware documentation.

During a vStorage Image backup, Data Protector creates a snapshot and copies data from the consistent state to Data Protector media. Then Data Protector deletes the snapshot. Note that snapshots created by Data Protector (**DP snapshots**) are distinguished from other snapshots by the label `_DP_VEPA_SNAP_` containing the product name, a description, and a timestamp.

Note: It does not matter if a user-created snapshot exists in a virtual machine snapshot tree at the time of backup; the user-created snapshot is backed up together with other virtual machine files. However, if Data Protector detects a user-created snapshot at the time of restore, which is only possible if the virtual machine to be restored still exists, the virtual machine is not restored. To restore such a virtual machine, you first need to manually remove all existing user-created snapshots. Also note that although the user-created snapshots of the virtual machine were backed up, when the virtual machine is restored, only the latest state is restored; the snapshots are not.

Figure 5: Virtual machine snapshot tree



Existing virtual machine snapshots reduce the overall performance of a virtual machine. For this reason, Data Protector automatically removes DP snapshots once they are no longer needed.

Important: Do not use the label `_DP_VEPA_SNAP_` for snapshots that you create for other purposes, otherwise they will be deleted by Data Protector.

The number of Data Protector snapshots that remain in the snapshot tree after a backup depends on three factors:

- Whether changed block tracking has been specified
- The Data Protector snapshot handling mode selected
- The backup type specified

The snapshots that remain in a snapshot tree play a great role for incremental and differential virtual machine backups. For details, see Backup types below.

Since the snapshot handling mode can affect virtual machine performance, it is specified per virtual machine.

vCD vStorage Image backup method

The vCD vStorage Image backup method provided by the Data Protector Virtual Environment integration is a variant of the vStorage Image backup method. It is used exclusively to back up virtual machines running on VMware ESX(i) Server systems from several vCenter Servers systems managed by VMware vCloud Director. Conceptually, both backup methods are identical.

For details on the vCD vStorage Image backup method concepts, see vStorage Image backup method on page 21.

Backup types

The type of backup to be performed is specified at backup specification level, either in the Scheduler page, or in the Start Backup dialog box for an interactive backup. However, the type of backup that can actually be performed depends on the snapshot handling mode specified and on whether changed block tracking is used or not.

Using the vStorage Image or vCD vStorage Image backup methods, you can perform the following backup types:

Table 2: Backup types

Full	Backs up the complete virtual machine (disk), including the virtual machine memory file (if specified).
Incremental	Backs up the changes made to a virtual machine (disk) since the last full, incremental, or differential backup.
Differential	Backs up the changes made to a virtual machine (disk) since the last full backup.

For incremental and differential backup sessions, you must also specify how Data Protector should identify changes:

- At file level
- At disk block level

To identify changes at file level (changed block tracking is not enabled), Data Protector uses the VMware snapshot functionality. For details, see Snapshot handling mode below.

To identify changes at disk block level, Data Protector uses the VMware changed block tracking functionality. For details, see Changed block tracking on page 31.

The possible combinations of snapshot handling mode and changed block tracking for VMware backups are summarized in Snapshot management below.

Table 3: Snapshot management

Changed block tracking	VM snapshot handling mode	Number of snapshots remaining after backup
Disabled	Disabled	0
	Single	1
	Mixed	up to 2
Enabled	Disabled	0
	Single	0
	Mixed	0

Note: When changed block tracking functionality is enabled, the number of snapshots remaining after backup is always 0.

Snapshot handling mode

The snapshot handling mode enables you to control the number of Data Protector snapshots left in a virtual machine's snapshot tree after a backup. You can set it per virtual machine, or specify a common setting which can be overridden for individual virtual machines. The types of backup that can be performed depend on this setting. The selected snapshot handling mode must therefore be suitable for the type of backup chain anticipated. The following snapshot handling modes are available:

- **Disabled** : Supports only full backups. The snapshot made at the beginning of a backup session is used only to create a consistent state. After the data transfer completes, the snapshot is removed. For details, see Snapshot mode: disabled on the next page.
- **Single** : Supports full, differential, and incremental backups in the following backup chains:

Full, differential, differential, differential ...

Full, incremental, incremental, incremental ...

You cannot mix incremental and differential backups within the same backup chain. The snapshot that is made at the beginning of a backup session is used to create a consistent state. After the backup completes, one DP snapshot remains in the snapshot tree. It is needed to track changes made since the last full or incremental backup. For details, see Snapshot mode: single on page 28.

- **Mixed** : Supports full, differential, and incremental backups in all possible backup chain forms. For example:

  Full, incremental, incremental, differential, incremental, differential ...

  The snapshot that is made at the beginning of a backup session is used to create a consistent state. After the backup completes, up to two DP snapshots remain in the snapshot tree. One is needed to track changes made since the last full backup and the other to track changes made since the last backup (incremental or differential). For details, see Snapshot mode: mixed on page 29.

When performing snapshot operations on a backed up virtual machine, you must be careful not to break your backup chains.

Important: A VMware object's snapshot which was not created with Data Protector cannot be used to set up a Data Protector backup chain (restore chain) for that object.

A backup chain gets broken if you perform any of the following operations:

- Delete a snapshot
- Revert to a snapshot
- Create a snapshot without involving Data Protector
- Change snapshot handling mode
- Add a new virtual machine disk or rename an existing one
- Restore the virtual machine
- Enable changed block tracking

After completing any of the above operations, you must first run a full backup to start a new backup chain. If you run a session for an incremental backup or a differential backup instead, Data Protector switches the effective backup type in the session to full.

Snapshot mode: disabled

A full backup in **Disabled** mode progresses as shown in the following figure.

Figure 6: Full backup (disabled mode)

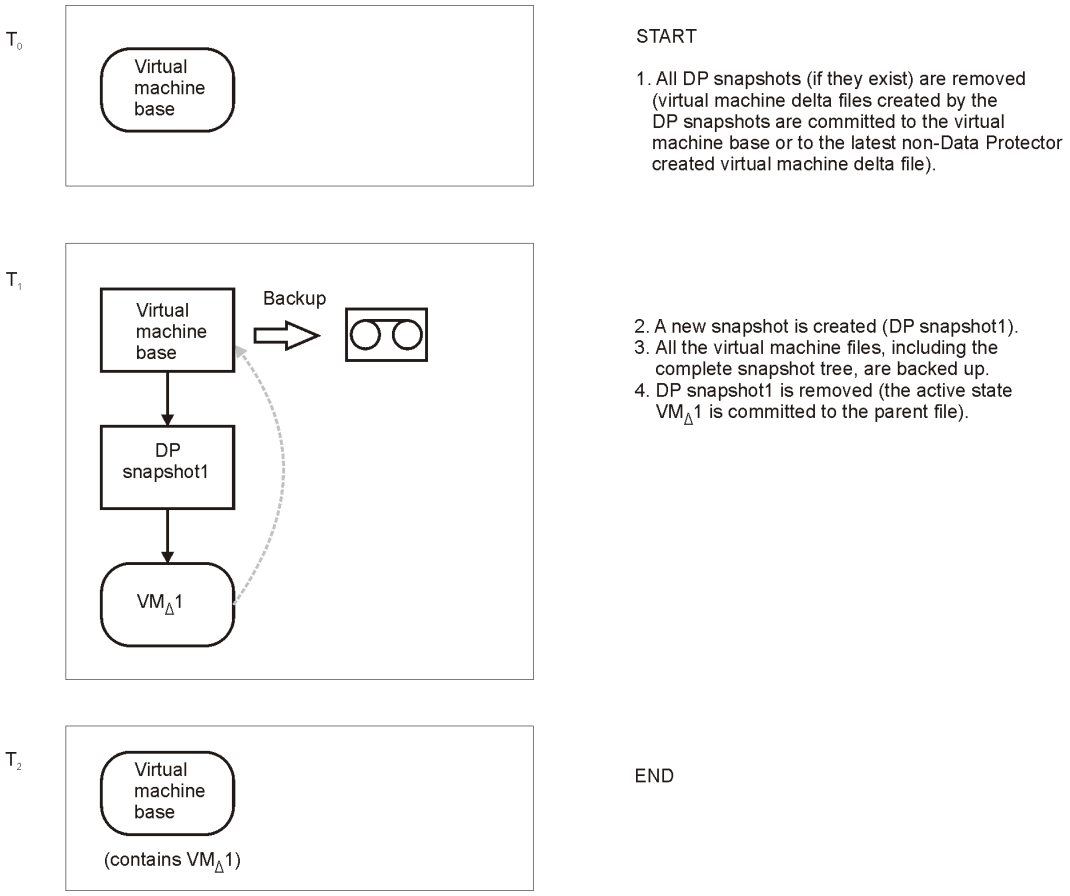


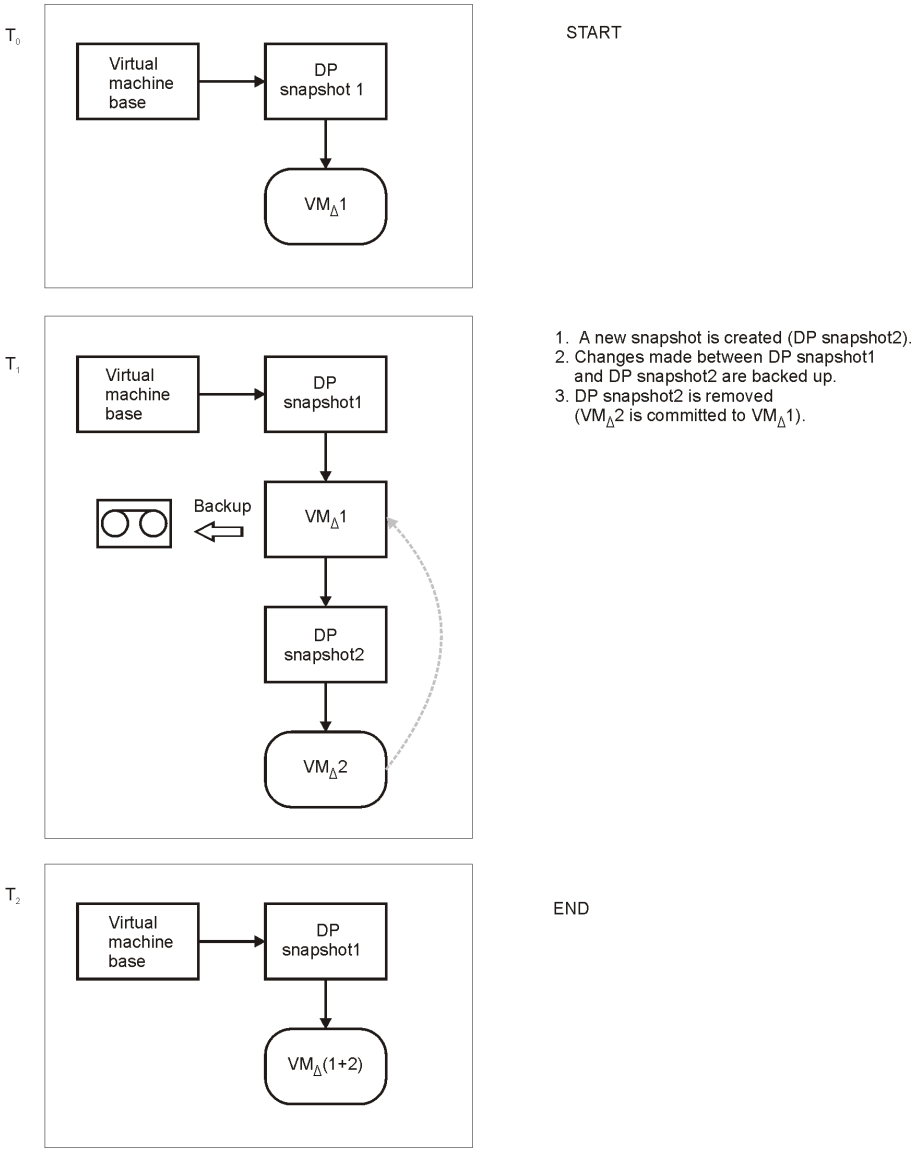
Table 4: Legend

Tn	Boxes denoted by Ti show how the virtual machine snapshot tree changes in time.
Virtual machine base	The rectangle denoted by Virtual machine base represents the virtual machine base or the last non-Data Protector created virtual machine delta file on the active branch.
VMΔ	A rectangle denoted by VMΔ represents a virtual machine delta file created by a Data Protector snapshot.
DP snapshot	A rectangle denoted by DP snapshot represents a process (snapshot operation triggered by Data Protector). This process closes the current active state to become a read-only file. At the same time, it creates a new delta file, which becomes the active state. The active state is denoted by round corners. The snapshot created by Data Protector is named _DP_VEPA_SNAP_.

Snapshot mode: single

A full backup in the **Single** mode progresses in the same way as a full backup in the **Disabled** mode, with the exception that the DP snapshot is not removed at the end (you end up with one DP snapshot). A subsequent differential backup is shown in the following figure.

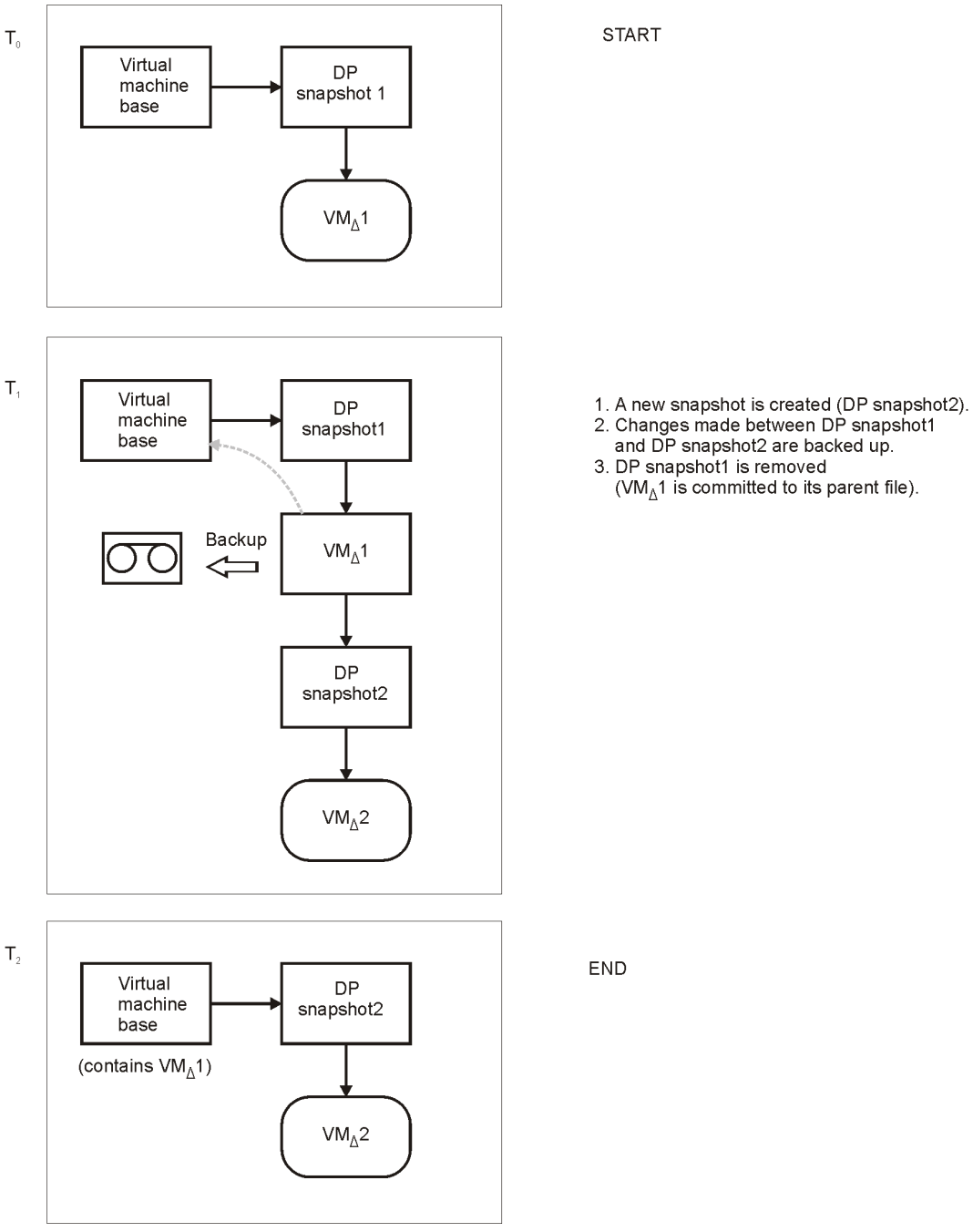
Figure 7: Differential backup (single mode)



DP snapshot1 remains in the snapshot tree to track changes made since the last full backup.

A backup chain consisting of a full backup that is followed by incremental sessions progresses in the same way, with the exception that, at the end of an incremental session, DP snapshot1 is removed instead of DP Snapshot2 (see Incremental backup (single mode) on the next page).

Figure 8: Incremental backup (single mode)



DP snapshot2 remains in the snapshot tree to track changes made since the last incremental backup.

Snapshot mode: mixed

A full backup in **Mixed** mode progresses in the same way as a full backup in **Single** mode (you end up with one DP snapshot). A subsequent differential or incremental backup progresses in the same

way as a differential or incremental backup in **Single** mode, with the exception that no DP snapshot is removed at the end (you end up with two DP snapshots).

The progress of a subsequent incremental backup is shown below.

Figure 9: Incremental backup (single mode)

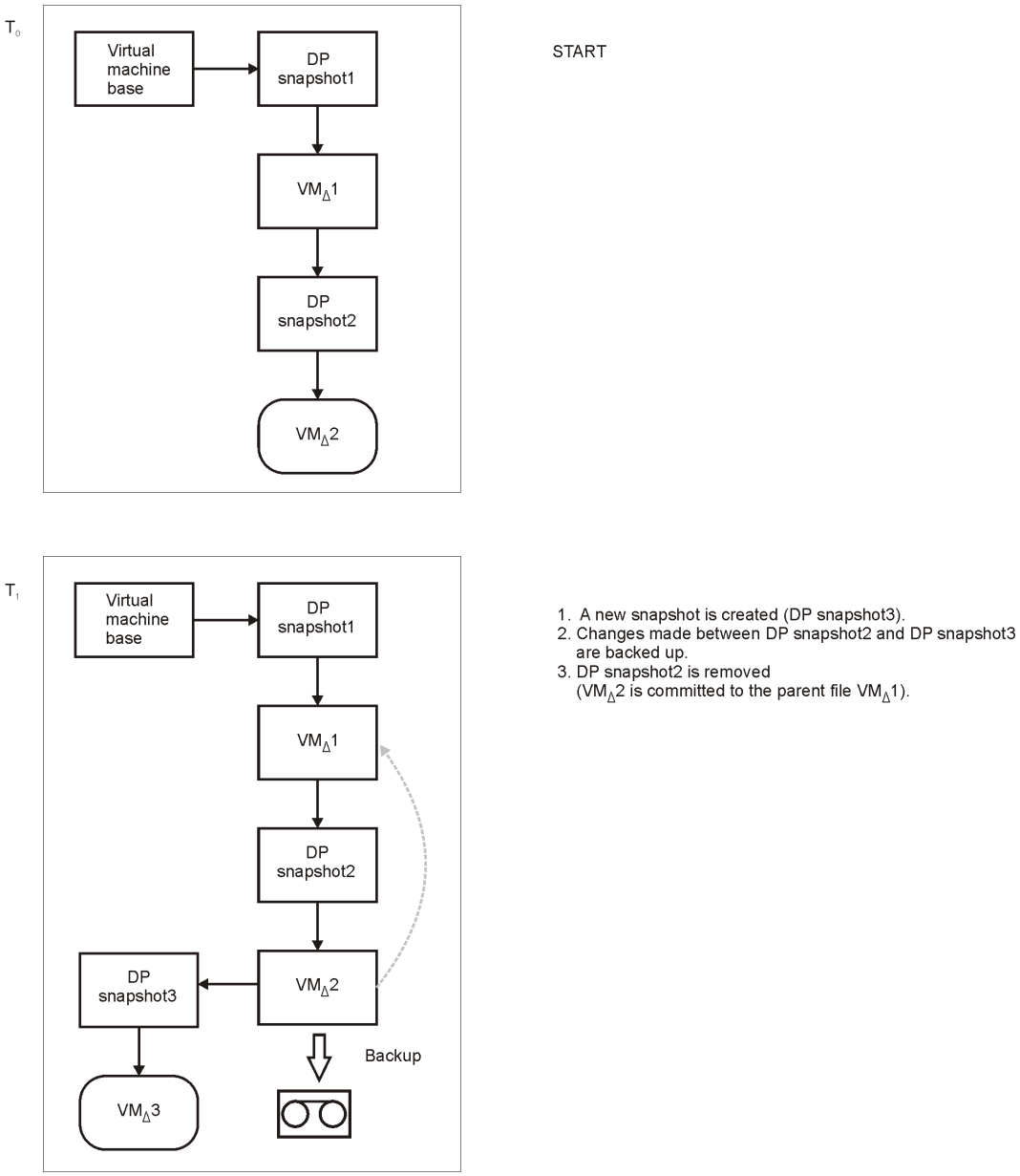
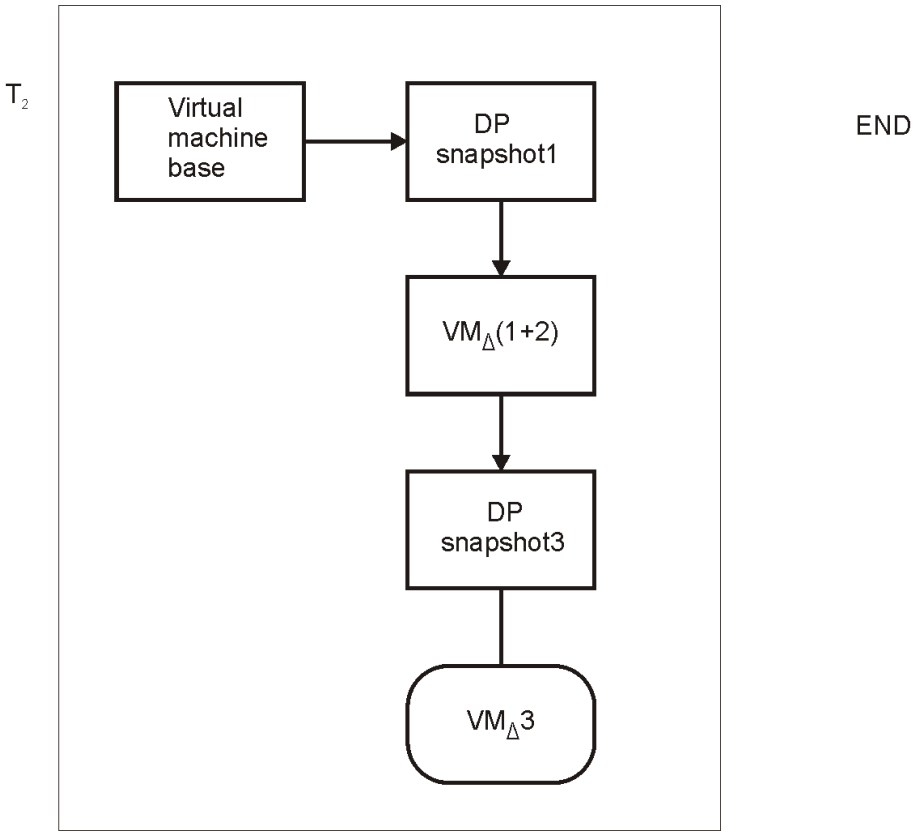


Figure 10: Incremental backup (mixed mode)



DP snapshot1 and DP snapshot3 remain in the snapshot tree to track changes made since the last full and the last backup respectively.

A subsequent differential backup progresses in the same way as an incremental backup session described in Incremental backup (mixed mode) above, with the following exceptions:

- DP snapshot2 is removed before DP snapshot3 is created.
- Instead of changes made between DP snapshot2 and DP snapshot3, changes made between DP snapshot1 and DP snapshot3 are backed up.

Changed block tracking

Changed block tracking (CBT) is a feature of later versions of VMware that can be used to improve the efficiency and speed of your backups.

For CBT, change IDs are used. A change ID is an identifier for the state of a virtual disk at a specific point in time. It is saved by the virtual disk logic whenever a snapshot is taken of the disk.

The main advantage of using changed block tracking is most noticeable on incremental or differential backups, because:

- It is not necessary to keep virtual machine snapshots on the system until the next backup, greatly reducing the system overhead.
- The changes to be backed up are calculated more easily, by obtaining change information from the kernel, rather than calculating it from snapshots.

During full backups, only active blocks on the disk are backed up, and unallocated blocks are ignored. This makes the backups space-efficient and faster.

When changed block tracking is enabled, a virtual machine's performance is slightly impacted, but this is small relative to what you gain. If it is enabled within VMware vSphere, Data Protector will use it. You can also enable it using the Data Protector GUI, if required.

When changed block tracking is used, Data Protector snapshots are still used to put a virtual machine in a consistent state. However, when the backup completes, they are deleted. Only changed block tracking log files change IDs are kept.

- Not all types of virtual disk support changed block tracking. In case of an unsupported disk, a virtual machine backup fails.
- When changed block tracking is first enabled, the next backup for a virtual machine will always be a full backup to provide a reference point for the tracking. In other words, a new backup chain is started.
- A CBT backup chain (Full, Differential, Incr,...) gets broken when you perform a restore session. When the restore session completes, run a full backup again to start a new backup chain, otherwise subsequent incremental and differential backup sessions will fail.

Backup flow

1. Data Protector triggers a snapshot.
2. A change ID is recorded for the current backup.

   If this is the first snapshot taken after changed block tracking was enabled, all active blocks are identified and change ID 0 is recorded.

   In case of a full backup, this change ID becomes the start reference point for a new backup chain.
3. This step depends on the backup type selected:
   - *Full*: The blocks changed since change ID 0 are identified.
   - *Incremental*: The blocks changed since the change ID for the previous backup (full, incremental, or differential) are identified.

- *Differential*: The blocks changed since the change ID for the previous full backup are identified.

4. The identified blocks are backed up.
5. The snapshot is deleted.

Table 5: Example of a backup chain with changed block tracking

Snapshot	Change ID	Blocks identified	Blocks backed up
1st after CBT enabled	ID 0	All active blocks	—
Full backup	ID *n*	Changed since ID 0	All active blocks from ID 0 + changed blocks since ID 0
Incremental backup	ID *n+m*	Changed since ID n	Changed block since ID *n*
Incremental backup	ID *n+p*	Changed since ID n+m	Changed blocks since ID *n+m*
Differential backup	ID *n+q*	Changed since ID n	Changed blocks since ID *n*
Full backup	ID *r*	Changed since ID 0	All active blocks from ID 0 + Changed blocks since ID 0

Quiescence

On Windows guest operating systems, it is possible to use the VSS framework to freeze, or quiesce, the states of the applications running within a virtual machine before a snapshot is created. If quiescence is selected for a Windows guest operating system, the snapshot process quiesces all system writers and registered application writers before taking the snapshot of the virtual machine.

During a backup with quiescence enabled, a `.zip` file is created that contains all the BCD and writer manifests located on the datastores concerned. Data Protector backs up this file. During a restore, the file is restored to the same location and then post-restore VSS steps like roll-forward can be performed manually.

Note: Specifying Quiescence can slow down the speed of backup sessions considerably.

Disk space requirements

A virtual machine backup requires sufficient disk space on the datastore(s) where the virtual machine disks reside.

Free space required option

You can use the Data Protector **Free space required %** option to make sure that a virtual machine is backed up only if there is enough free space.

The required free space is calculated based on the size of virtual machine disks just before the snapshot is created. Data Protector checks all datastores where the virtual machine disks reside. If one of the datastores does not meet the specified percentage of free space, no snapshot is created and the backup of the virtual machine fails with an error.

When backing up more than one virtual machine, the check is applied to each virtual machine separately. The virtual machines which pass the check are backed up and the ones which do not pass it are not.

If you specify 0%, the check is omitted.

Examples

The following examples illustrate how the **Free space required %** option works:

1. Backup of a single virtual machine "test1" with the disk "disk1" residing on the datastore "datastore1":

   If you specify 30% in the **Free space required %** option and the datastore has a size of 100 GB, the backup succeeds if there is at least 30 GB of free space on the datastore.

2. Backup of a single virtual machine "test1" with two disks, "disk1" and "disk2" residing on two datastores, "datastore1" and "datastore2":

   If you specify that 30% of free space is required, the backup succeeds if there is at least 30 GB of free space on each datastore.

3. Backup of two virtual machines, the virtual machine "test1" with the disk "disk1" on the datastore "datastore1" and the virtual machine "test2" with the disk "disk2" on the datastore "datastore2":

   If you require 30% of free space, the backup of both virtual machines succeeds if there is at least 30 GB of free space available on each datastore. If for example, the datastore "datastore1" has less than 30% of free space and the datastore "datastore2" has at least 30% of free space, the backup of the virtual machine "test1" fails and the backup of the virtual machine "test2" succeeds. If both datastores have less than 30% of free space, the backup of both virtual machines fails.

Table 6: Disk space requirements

Backup methods	Required disk space on datastores	Explanation
vStorage Image and vCD vStorage Image	The sum of the sizes of all the virtual machine disks, plus: • The size of any quiescence zip files, if quiescence is specified. • The size of the virtual machine memory file, if specified. • The size of the virtual machine snapshots if they are present (this applies to Single and Mixed snapshot handling modes with CBT disabled).	When a virtual machine snapshot is taken, changes made to the virtual machine disks are recorded to separate files (one delta file is created for each virtual machine disk). A delta file can grow up to the original virtual disk size.

Backup disk buffer

You can specify a disk buffer for your backup using the omnirc option `OB2_VEAGENT_BACKUP_DISK_BUFFER_SIZE`.

The SAN and the HotAdd backups support disk buffer sizes from 1 MB to 256 MB. By default, their disk buffer size is 8 MB. However, network backups, such as NBD and NBD (SSL), are always performed using the default disk buffer size of 1 MB.

- If there is not enough memory available for the specified disk buffer size, a fallback to 1 MB disk buffer size will happen to keep the backup running, and a warning message will be displayed.
- Using bigger disk buffer sizes improves the backup performance, but it also increases the memory consumption. At the certain level the backup performance does not improve anymore due to the limits of your backup host.

Backup parallelism

By default, virtual machines are backed up in parallel. In rare cases this may lead to problems. For example, backup sessions may end unexpectedly. In such cases, you may set the Data Protector `OB2_VEAGENT_THREADED_BACKUP` omnirc option on the backup host to `0` to disable parallel backups.

Note that virtual machine disks are backed up sequentially in both cases.

For details on how to use Data Protector omnirc options, see the *HP Data Protector Help* index: “omnirc options”.

Backup considerations

- **Concurrent backup sessions**

  Backup sessions that use the same devices cannot run in parallel.

  You cannot back up virtual machines and an ESX(i) Server systems or a datacenter where the virtual machines reside in parallel.

- **Transportation modes**

  You can use various transportation modes for backup. For details, see Advanced virtual machine settings on page 55.

  The SAN transportation mode automatically switches to NBD, if an incremental or differential session is selected, without CBT. It is recommended to use CBT for making incremental/differential backups because it is faster and uses less space on the backup device. In addition, incrementals / differentials without CBT uses the HTTPS method of downloads and uploads, hence requiring more time.

- **Thick and thin disks**

  Data Protector cannot detect whether virtual machine disks are thick or thin. In both cases, complete disks are backed up (that is, the complete space allocated at a disk’s creation time is backed up, even if the space is still empty). To create space-efficient backups, enable changed block tracking. Note that not all datastores support changed block tracking.

- **Migration and vCD vStorage Image backup**

  Migration of virtual machines or vApps through the VMware vCloud Director during the vCD vStorage Image backup is not supported.

Restore concepts

You can restore VMware objects backed up with either of vStorage Image backup methods in different ways.

Restore of VMware objects backed up with vStorage Image method

Virtual machines, virtual machine disks, and virtual machines templates backed up with the **vStorage Image** method can be restored:

- To a datacenter
- To a directory on a backup host

Restore to a datacenter

By default, virtual machines are restored to the original datacenter and the original datastore, but you can select a different datacenter if you want.

By default, Data Protector deletes a virtual machine (if it exists) before it is restored, even if it resides in a different datacenter from the datacenter you restore to.

Note: If you select an ESX(i) Server client in the Restore client option (destination client) in the restore wizard, the migrated virtual machine will not be deleted, as the ESX(i) Server client is not able to detect virtual machines that are located on different ESX(i) Server clients (only a vCenter client can do that). Consequently, you end up with two virtual machines having the same UUID.

Alternatively, you can choose to restore virtual machines only if they do not exist, leaving existing virtual machines intact.

For the restore, you can also specify the following:

- Whether the memory state of the virtual machine should be restored (if a memory file was included in the backup)
- Whether the restored virtual machines should be registered in the datacenter
- Whether the restored virtual machine snapshots should be consolidated when the restore completes
- Whether the restored virtual machines should be powered on

The restore options provided are, by default, set to restore virtual machines to the original datacenter.

Restore of individual virtual machine disks

To be able to restore individual virtual machine disks to a datacenter, the original virtual machine must still exist. Otherwise, the restore fails.

Here is the progress of a restore session:

1. The virtual machine is powered off.
2. If the disks to be restored still exist, they are removed.
3. The disks are restored from the backup.

Note: After restore, virtual disks that are part of a dynamic disk set or virtual disks from different points in time may require additional user action (for example, mounting, resignaturing, or recovery) in the guest operating system and/or applications running inside.

Restore to a directory

When restoring to a directory (restore outside a datacenter) all the files of virtual machines are restored to a directory of your choice (for example, `C:\tmp`) on a backup host.

In the directory you specified, subdirectories are created with names corresponding to those of the datastores where the virtual machines (their virtual disks) resided at the time of backup. The files related to the virtual disks are restored to the respective subdirectories.

After such a restore, the virtual machines are not functional. You need to manually move the restored virtual machine images to an ESX(i) Server system, using the VMware Converter as described in Recovering virtual machines after restore to a directory on page 96.

Restore of VMware objects backed up with vCD vStorage Image method

VMware vCloud Director vApps and VMs backed up with the **vCD vStorage Image** method can be restored:

- To an organization
- To a directory on a backup host

Restore to an organization

By default, VMs are restored to the original organization, and consequently to the original vDatacenter, vApp, and vCenter, but you can select a different organization, vDatacenter, vApp, and vCenter if you want.

For the restore, you can also specify the following:

- Whether the memory state of the virtual machine should be restored (if a memory file was included in the backup)
- Whether the restored virtual machine snapshots should be consolidated when the restore completes
- Whether the restored virtual machines should be powered on

The restore options provided are, by default, set to restore virtual machines to the original destination.

Restore to a directory

When restoring to a directory (restore outside a datacenter or an organization) all the files of virtual machines are restored to a directory of your choice (for example, `C:\tmp`) on a backup host.

After such a restore, the virtual machines are not functional. You need to manually move them to an organization as described in Recovering virtual machines after restore to an organization on page 103.

Restore chain

When you restore a virtual machine from a backup created in an incremental or differential session, Data Protector automatically restores the complete backup chain, starting with the last full backup, which is then followed by the last differential and all subsequent incremental backups (if they exist) up to the selected session.

Restore considerations

- **Concurrent sessions**

  Restore sessions that use the same devices cannot run concurrently.

- **Failed restore sessions**

  Sometimes, when a virtual machine restore fails, Data Protector creates extra files on the datastore which you need to clean up manually when the session completes. Otherwise, corrupt virtual machine backups may be created in subsequent sessions and restore from a such a backup also fails. For details, see Cleaning up a datastore after a failed restore on page 103.

  When restoring a virtual machine to a non-original datastore whose block size is not compatible with the virtual machine disks' sizes (that is, a `.vmdk` file size is not a multiple of the datastore block size), the restore fails.

- **Virtual machines in vApp**

  When you restore a virtual machine that resided in a vApp container at the time of backup, the virtual machine is not restored back to the vApp container, but to the ESX(i) Server root level. If the virtual machine in the vApp container still exists, it is deleted or the restore is skipped, depending on what you select in the Existing virtual machine handling option.

- **Partial restore from a vStorage Image backup**

  When performing a partial restore from a vStorage Image backup (for example, when restoring only some out of many backed up VM disks), the default option **Delete after restore** is ignored and the **Delete before restore** option is used instead.

  > **Note:** Partial restore of a virtual machine with **Restore As** or **Keep for forensics** options are not supported.

- **Transportation modes**

  The following recommendations for specific virtual machine transportation modes apply:

- SAN transportation mode: To use the SAN transportation mode for restore:
  - Select a physical backup host for a restore session.
  - Ensure that the storage volumes that are presented to both the backup host and ESX(i) Server systems are not read-only. For details on how to check storage volume properties, see Problem on page 106.
  - Ensure that the storage volume size is a multiple of the underlying VMFS block size. Otherwise, the Write operation to the remainder fails. For example, if the storage volume size is 16.3 MB and the block size 1 MB, writing to the remaining 0.3 MB fails. For details, see the VMware Knowledge Base at:

    http://kb.vmware.com/selfservice/microsites/searchEntry.do.

    Search for “Best practices when using SAN transport for backup and restore”.
- The SAN transportation mode automatically switches to NBD, if an incremental or differential session is selected, without CBT. It is recommended to use CBT for making incremental/differential backups because it is faster and uses less space on the backup device. In addition, incrementals / differentials without CBT uses the HTTPS method of downloads and uploads, hence requiring more time.

- Hotadd transportation mode: Hotadd transportation mode is available for restore, however VMware does not support multiple disks. Therefore, in a HotAdd environment use the omnirc option `OB2_VEAGENT_RESTORE_TRANSPORT_METHOD` to set the restore transport mode to NBD.

Performance

You can improve backup and restore performance by setting the device block size to the maximum value of 1024 kB.

Configuring the integration

Configure the integration as follows:

- Import VMware clients into the Data Protector Cell.
- Configure virtual machines you want to back up.

Recommendations

- HP recommends to not use the percent sign in names of virtual machines that will be backed up, restored and recovered with Data Protector. If a virtual machine name contains `%`, the name is displayed incorrectly in the Data Protector GUI and in the Data Protector session messages.

Prerequisites

- Make sure that you have a correctly installed and configured VMware vSphere or VMware vCloud Director environment.

  For supported versions, platforms, devices, and other information, see the latest support matrices at http://support.openview.hp.com/selfsolve/manuals.

- Ensure you have **Disable Methods** and **Enable Methods** Global privileges granted to the user account that is used to connect to the vCenter Server.

- Make sure you have the necessary VMware vSphere privileges granted to the user account that is used to connect to the vCenter Server. For details, see If you select Standard security, you need to manually specify which login credentials Data Protector should use to connect to the VMware client: on page 43.

- You have to be either a member of the VMware vCloud Director `System Administrator` user group or have granted the system administration user rights to perform backup and restore operations for VMware vCloud Director client.

- Make sure that you have correctly installed Data Protector. For information on installing Data Protector in various architectures, see the *HP Data Protector Installation and Licensing Guide*.

  Make sure that you have at least one client with the `Virtual Environment Integration` component installed (**backup host**) in your environment. No special configuration is required for the backup host after installation.

  Important: The client you intend to use as the backup host should not have the VMware Consolidated Backup (VCB) software installed.

  If you intend to restore virtual machine files to a directory on a backup host, also install the `Disk Agent` component on the backup host. Otherwise, you will not be able to use the **Browse** button to specify the target directory (however, you will still be able to type the directory by yourself).

Before you begin

- Configure devices and media for use with Data Protector.

Importing and configuring VMware clients

With the Data Protector Virtual Environment integration, it is not necessary to install any Data Protector components on the VMware clients (vCenter Server systems, ESX(i) Server systems, vCloud Director). To make them Data Protector clients, the VMware clients must be properly imported into the Data Protector cell and configured.

Important: A client cannot be imported and configured as VMware vCenter client, VMware vCloud Director client, and Hyper-V client at the same time.

Procedure

To import a client into a Data Protector cell:

1. In the Context List, click **Clients**.
2. In the Scoping Pane, expand **Data Protector Cell**, right-click **Clients**, and select **Import Client**.
3. In the Import client page, enter the client name in the **Name** option, select the appropriate client type (**VMware ESX(i)**, **VMware vCenter**, or **VMware vCloud Director**) from the **Type** drop-down list and click **Next**.

Figure 11: Importing a VMware vCenter Server client (Name and Type)

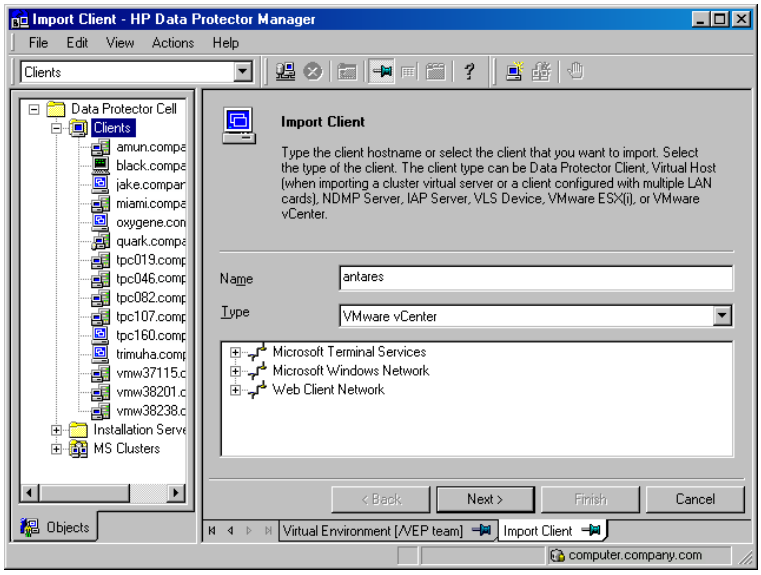
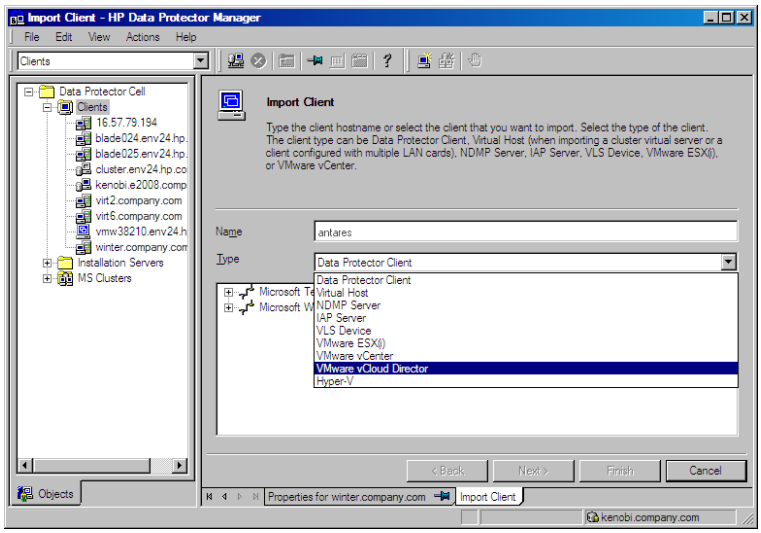


Figure 12: Importing a VMware vCloud Director client (Name and Type)



4. If you select **Standard security**, you need to manually specify which login credentials Data Protector should use to connect to the VMware client:

   Port : Specify the port that VMware vSphere is using. By default, VMware uses the port 443.

   Username and **Password**: Specify an operating system user account that has the following VMware vSphere privileges:

Datastore -> Allocate space
Datastore -> Browse datastore
Datastore -> Low level file operations
Datastore -> Remove file
Datastore -> Rename datastore
Folder -> Delete folder
Folder -> Rename folder
Global -> Disable methods
Global -> Enable methods
Global -> Licenses
Host -> Configuration -> Maintenance
Host -> Inventory -> Add standalone host
Network -> Assign network
Resource -> Assign virtual machine to resource pool
Resource -> Remove resource pool
Resource -> Rename resource pool
Sessions -> Validate session
vApp -> Delete
vApp -> Rename
vApp -> Add virtual machine
Virtual machine -> State -> Revert to snapshot
Virtual machine -> Configuration *
Virtual machine -> Interaction -> Answer question

Virtual machine -> Interaction -> Power Off
Virtual machine -> Interaction -> Power On
Virtual machine -> Inventory -> Create new
Virtual machine -> Inventory -> Register
Virtual machine -> Inventory -> Remove
Virtual machine -> Inventory -> Unregister
Virtual machine -> Provisioning *
Virtual machine -> State -> Create snapshot
Virtual machine -> State -> Remove snapshot

- **Web service** : Optionally, change the web service entry point URI. Default: `/sdk`

If you select **Integrated security**, which is only available for VMware vCenter Server systems, provided that both the application client and the backup host are Windows systems, Data Protector connects to the VMware vCenter Server system with the user account under which the `Data Protector Inet` service on the backup host is running. Ensure that this user account has appropriate VMware vSphere rights to connect to the VMware vCenter Server system and the `Data Protector Inet` service on the backup host is configured for user impersonation.

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

For the **Port** and **Web service root** options, Data Protector uses the values that are currently specified for the standard security. Integrated security is based on Security Support Provider Interface (SSPI).

Organization : The organization in the VMware vCloud Director that you connect to. This option cannot be modified. By default, the `System` organization, which is only accessible to VMware vCloud Director system administrators, is used.

Click **Finish**.

Figure 13: Importing a VMware vCenter Server client (login credentials)

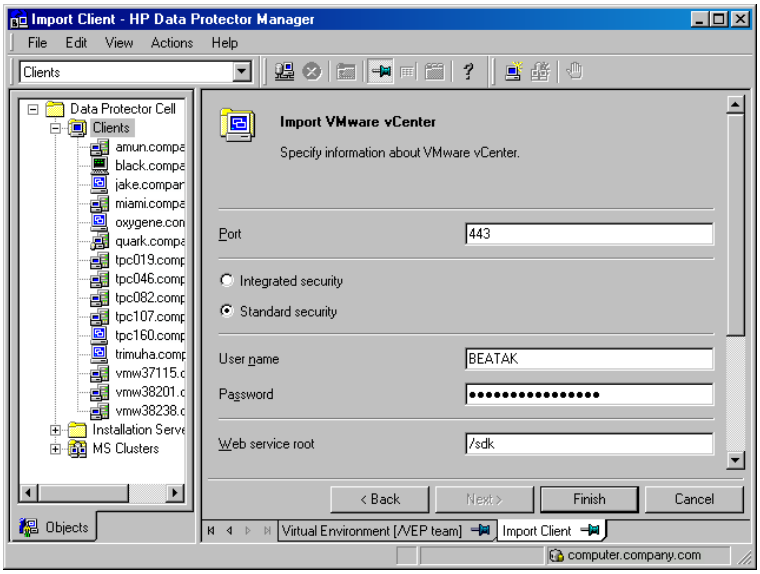
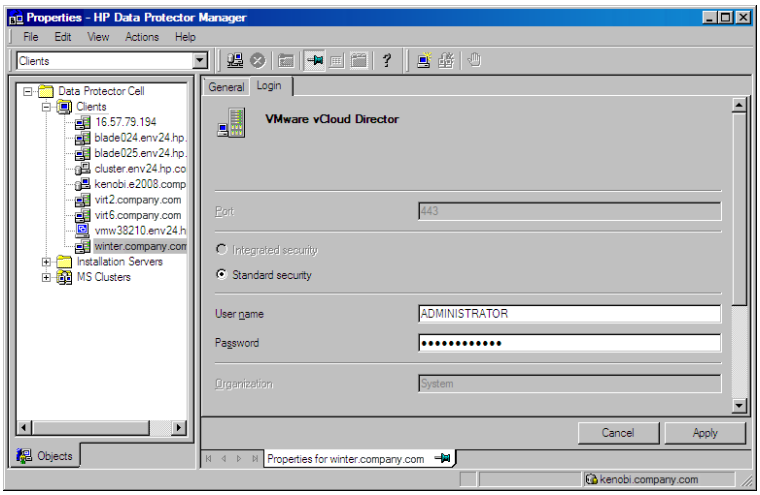


Figure 14: Importing a VMware vCloud Director client (login credentials)



Note: For details on how to change or check the parameters later, see Changing the configuration of VMware clients below and Checking the configuration of VMware clients on page 49.

Changing the configuration of VMware clients

When you update the credentials for connecting to a VMware client (vCenter Server, ESX(i) Server, or vCloud Director client), you actually update the `cell_info` file which resides on the Data Protector Cell Manager. Therefore, you can only change the login credentials if you have the Data Protector `Clients configuration` user right. For details on the Data Protector user rights, see the *HP Data Protector Help* index: ”user groups”.

To update the credentials, use the Data Protector GUI or CLI.

Using the Data Protector GUI

You can update the credentials in two different places: in the Clients or in the Backup context.

Clients context

1. In the Context List, click **Clients**.
2. In the Scoping Pane, expand Clients, and then select the client for which you want to change the login credentials.
3. In the Results Area, click the **Login** tab.
4. Update the credentials and click **Apply**.

Backup context

It is assumed that a backup specification for the VMware client for which you want to change the login credentials already exists.

1. In the Context List, click **Backup**.
2. Open a backup specification for the VMware client for which you want to change the login credentials.
3. In the Source page, right-click the client at the top, and select **Configure**.
4. In the Configure Virtual Environment dialog box, update the values and click **OK**.

Figure 15: Changing the configuration of a VMware vCenter Server or VMware ESX(i) Server client

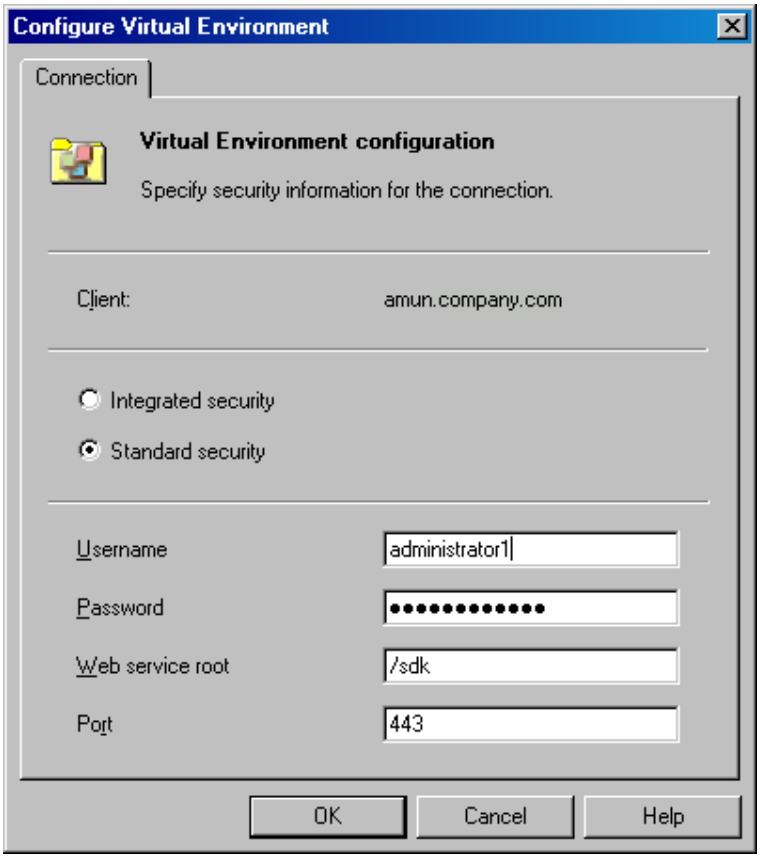
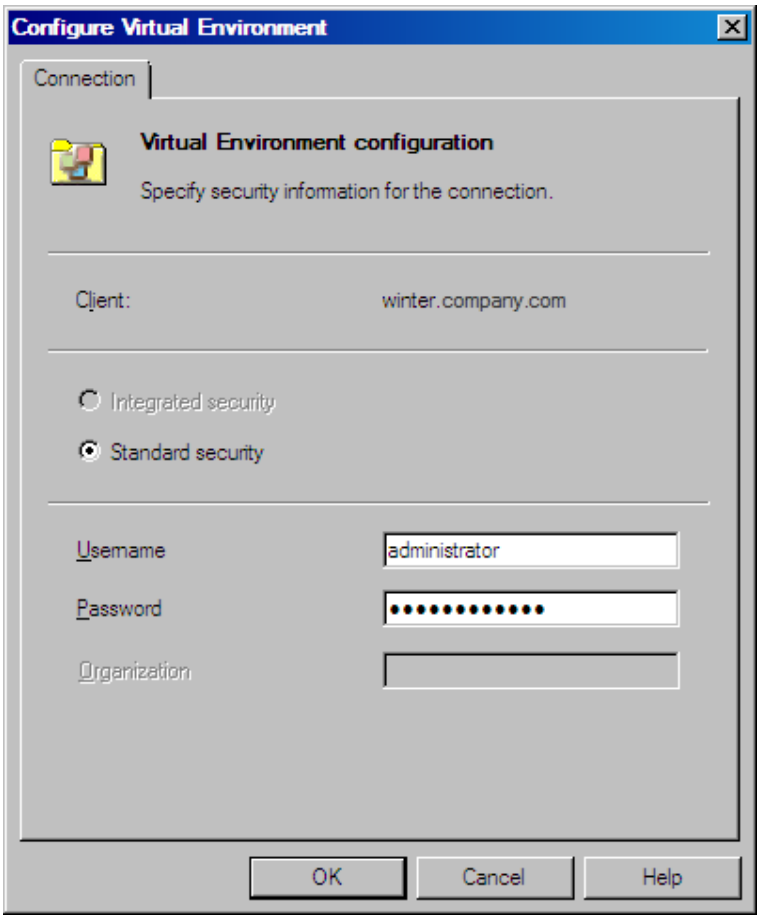


Figure 16: Changing the configuration of a VMware vCloud Director client



Using the Data Protector CLI

1. Log in to the backup host, open the command prompt and change to the directory in which the `vepa_util.exe` command is located.
2. Execute:

   For **Integrated security**:

   ```
   vepa_util.exe
   command
   --config
   --virtual-environment vmware
   --host VMwareClient
   --security-model 1
   ```

   For **Standard security**:

   VMware vCenter Server or VMware ESX(i) Server client

```
vepa_util.exe
command
--config
--virtual-environment vmware
--host VMwareClient
--security-model 0
--username Username
{--password Password | --encoded-password Password}
[--webroot WebServiceRoot]
              [--port WebServicePort]
```

VMware vCloud Director client

```
vepa_util.exe
command
--config
--virtual-environment vCD
--host vCDClient
--security-model 0
--username Username
{--password Password | --encoded-password Password}
```

The message `*RETVAL*0` indicates successful configuration.

For descriptions of the options, see the `vepa_util.exe` man page or the *HP Data Protector Command Line Interface Reference*.

Checking the configuration of VMware clients

During the configuration check, Data Protector tries to connect to a VMware client using the login credentials from the `cell_info` file on the Data Protector Cell Manager.

To verify the connection, use the Data Protector GUI or CLI.

Using the Data Protector GUI

You can verify the connection to a VMware client after you have created at least one backup specification for this client.

1. In the Context List, click **Backup**.
2. In the Scoping Pane, expand **Backup Specifications** and then **Virtual Environment**. Click the backup specification for the VMware client to be checked.
3. In the Source page, right-click the VMware client and select **Check configuration**.

Using the Data Protector CLI

1. Log in to the backup host, open the command prompt and change to the directory in which the `vepa_util.exe` command is located.
2. Execute:

   VMware vCenter Server or VMware ESX(i) Server client

   ```
   vepa_util.exe
   command
   --check-config
   --virtual-environment vmware
   --host VMwareClient
   ```

   VMware vCloud Director client

   ```
   vepa_util.exe
   command
   --check-config
   --virtual-environment vCD
   --host vCDClient
   ```

   The message `*RETVAL*0` indicates successful configuration.

   For option description, see the `vepa_util.exe` man page or the *HP Data Protector Command Line Interface Reference*.

Configuring virtual machines

To configure a virtual machine means to specify how the virtual machine should be backed up.

You can specify the following:

- Whether a virtual machine's disks should be defragmented and shrunk before they are backed up.
- (Windows virtual machines only) Whether a quiescence snapshot should be taken to make applications running inside a virtual machine consistent for backup.
- Which transportation mode should be used during backups.
- Which VMware functionality should be used to detect changes for incremental and differential virtual machine backups: the VMware snapshot functionality or the changed block tracking functionality (**CBT**).

For each datacenter, you can specify:

- Common settings that apply to all virtual machines in the datacenter.
- Virtual machine-specific settings that override the common settings. If there are no virtual machine-specific settings, the common settings are used for that particular virtual machine.

All these settings are saved in a datacenter-specific file *VMwareClient%DatacenterPath* on the Cell Manager. The file is used for all backup sessions that use any of the backup specifications for this datacenter.

Similarly, backup sessions using any of the backup specifications for `All datacenters`, use the settings from the file *VMwareClient%AllDatacenters*.

The files *VMwareClient%DatacenterPath* and *VMwareClient%AllDatacenters* are created or updated when you create or update a backup specification for a specific datacenter or all datacenters respectively.

To configure virtual machines, use the Data Protector GUI or CLI.

Using the Data Protector GUI

You can configure virtual machines when you create or modify a backup specification. In the Source page of a backup specification, right-click the client system at the top or any of the virtual machines listed below, and select **Configure Virtual Machines**.

Figure 17: Configure virtual machines (settings for VMware vCenter Server client)

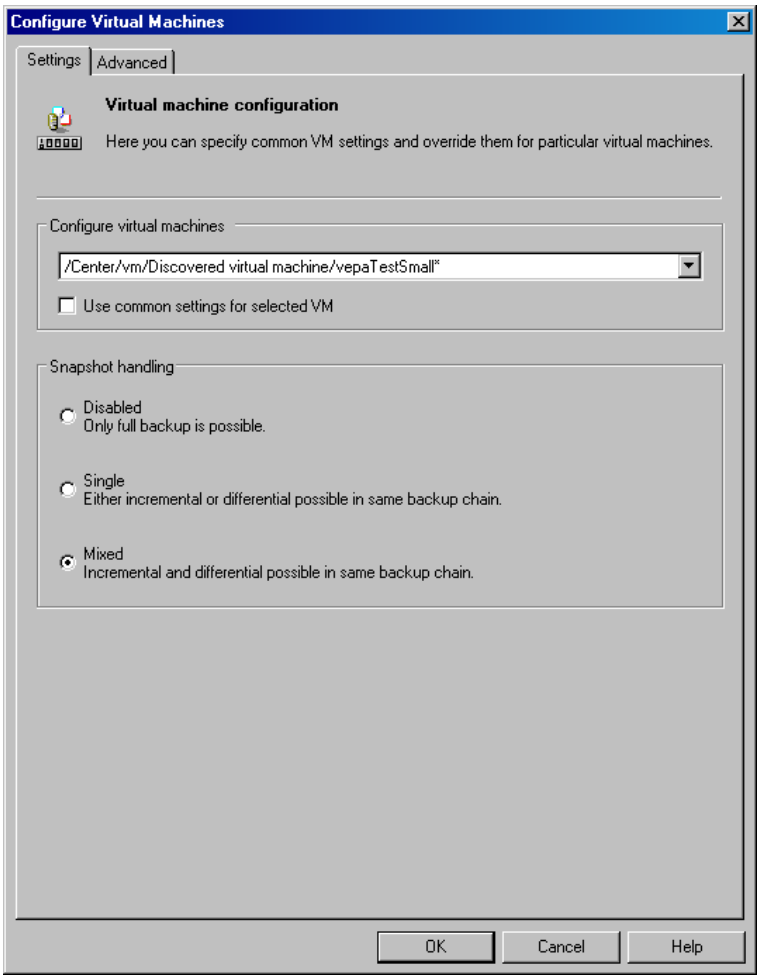
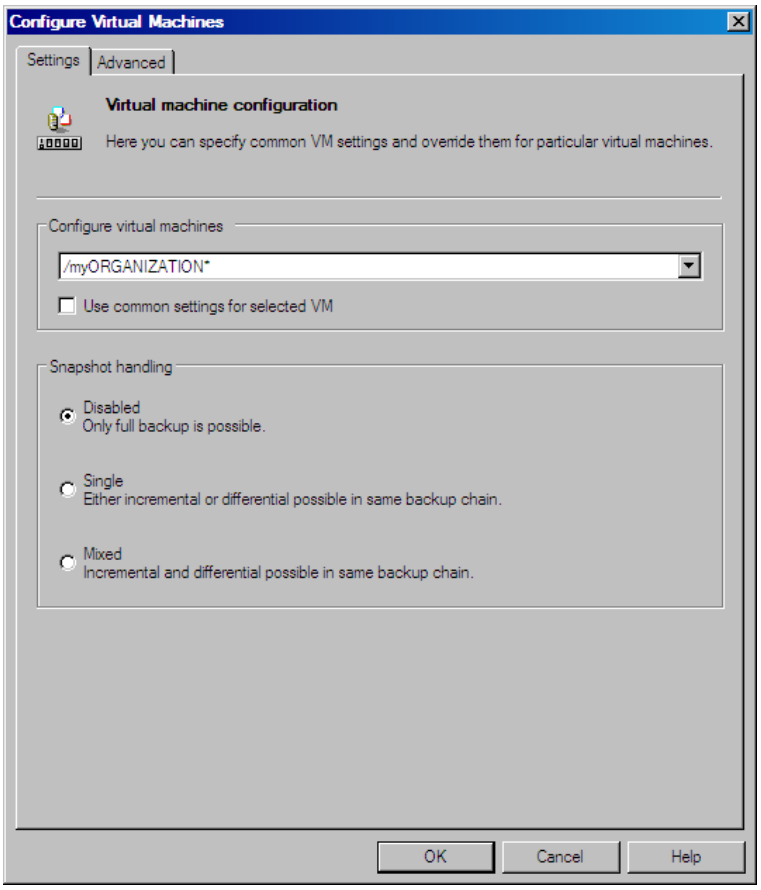


Figure 18: Configure virtual machines (settings for VMware vCloud Director client)



In the Configure Virtual Machines dialog box **Settings** page, specify the following settings:

Table 7: Virtual machine settings

Configure virtual machine	Select whether you want to specify common virtual machine settings (**Common VM Settings**) or settings for a specific virtual machine. Virtual machine specific settings override the common virtual machine settings.	
	Use common settings for selected VM	Available only if a virtual machine is selected. Select this option if you want the common settings to apply to the selected virtual machine. Default: selected
	Use default settings	Available only if **Common VM Settings** is selected. Select this option to set default values for the common virtual machine settings. Default: selected

Snapshot handling	**Disabled** (default)	This mode supports only full backups. The virtual machine snapshot that is created during backup is removed at the end of the session. For details, see Snapshot mode: disabled on page 26.
	Single	This mode supports full, incremental, and differential backups. However, you cannot mix incremental and differential backups within the same backup chain. Data Protector keeps one DP snapshot for backup purposes. For details, see Snapshot mode: single on page 28.
	Mixed	This mode supports full, incremental, and differential backups, in all combinations. Data Protector keeps up to two DP snapshots for backup purposes. For details, see Snapshot mode: mixed on page 29.

In the Configure Virtual Machines dialog box **Advanced** page, specify the following settings:

Figure 19: Configure virtual machines (Advanced)

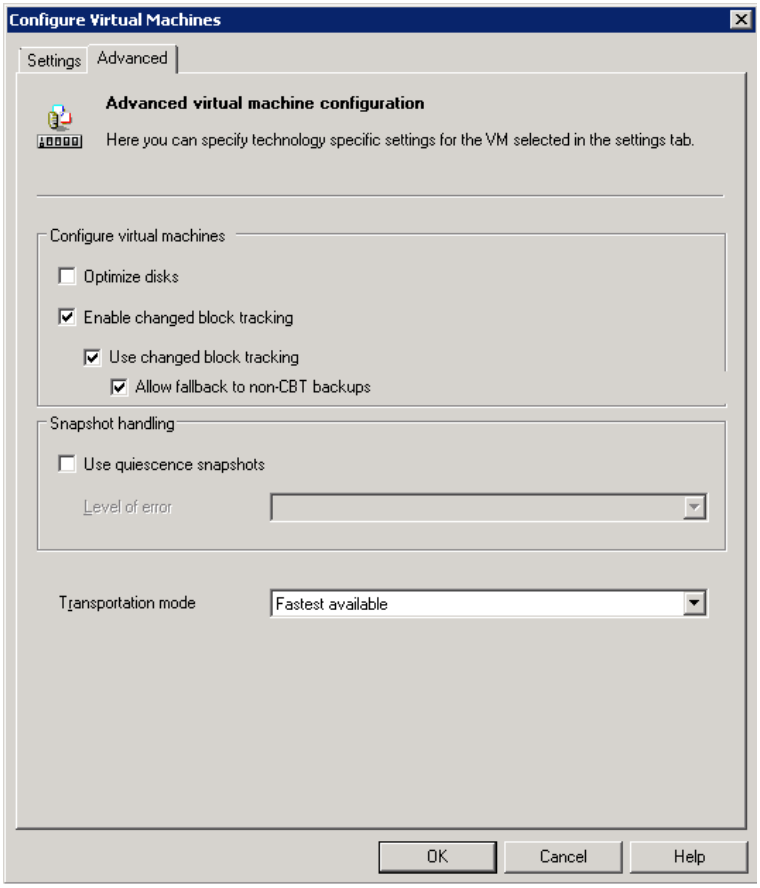


Table 8: Advanced virtual machine settings

Configure virtual machine	Specify advanced backup options to be used for the virtual machine backup. The options specified in this page apply to the virtual machines that are currently selected in the Settings page.	
	Optimize disks	This option is applicable only for thin virtual machine disks. Select this option to defragment and shrink virtual machine disks (`.vmdk` files) before they are backed up. Shrinking a virtual machine disk reclaims unused space and so reduces the amount of space the disk occupies on the ESX(i) Server system drive. Consequently, this reduces the size of backup data. However, note that such a backup needs more time to complete. Note that defragmentation results in disk block changes (even if there are no changes made to a virtual machine). Consider this if you are using changed block tracking for incremental and differential backups. Default: not selected.
	Enable changed block tracking	Select this option to enable the VMware changed block tracking functionality for the selected virtual machines. If the functionality has already been enabled using the VMware vSphere client, you cannot disable it by clearing this option. Default: not selected.
	Use changed block tracking	Available only if **Enable changed block tracking** is selected. Select this option to use the VMware changed block tracking functionality for incremental and differential backup sessions. For details, see Changed block tracking. Not all datastores support changed block tracking. If this option is selected and the datastore does not support this functionality, incremental and differential backup sessions will fail. Default: not selected.

	Allow fallback to non-CBT backups	Available only if **Use changed block tracking** is selected. Select this option to continue backup in a non-CBT mode for successful backup of Data Protector. If a user snapshot is present and the **Allow fallback to non-CBT backups** option is not enabled, Data Protector will fail continuously as the user snapshot cannot be consolidated or deleted. Default: not selected.
Snapshot handling	**Use quiescence snapshots**	Applicable for Windows virtual machines. Select this option to use Microsoft Volume Shadow Copy Service (VSS) functionality to quiesce all applications with VSS writers before performing the backup. This produces application-consistent backups. Do not select this option if one or more virtual machines selected in the backup specification have the **Backup memory file** specified. Default: not selected. For details, see Quiescence.
	Level of error	Available only if **Use quiescence snapshots** is selected. Specify the level of error to be reported if a quiescence snapshot fails.

Transportation mode		Select the transportation mode to be used when backing up a virtual machine. • **NBD** : Use this mode when your ESX(i) Server systems do not have access to a SAN, but use local storage devices or NAS to store virtual machine disks. This is an unencrypted transportation mode over a local area network that uses the Network Block Device (NBD) driver protocol. This transportation mode is usually slower than Fibre Channel. • **NBD (SSL)** : Same as NBD except that the communication over the network is encrypted using the Secure Socket Layer (SSL) cryptographic protocol. • **Hotadd** : Use this mode if your backup host (a client with the Data Protector `Virtual Environment Integration` component installed) is a virtual machine. Such a configuration enables you to back up other virtual machines residing on datastores visible to the ESX(i) Server that hosts the backup host. • **SAN** : Use this mode when your ESX(i) Server systems store their virtual machine disks on Fibre Channel SAN or iSCSI SAN. This is an unencrypted transportation mode over Fibre Channel or iSCSI. For details, see the VMware documentation. This transportation mode requires that the storage volumes on which the virtual machines are located are presented to the client with the `Virtual Environment Integration` component installed (**backup host**). **Caution:** Do not reformat these storage volumes. Otherwise, you will delete all your virtual machines. For details on these VMware transportation modes, see the VMware documentation. If you are not concerned which mode is used, select **Fastest available**. Default: **Fastest available**

Using the Data Protector CLI

1. Log in to the backup host, open the command prompt and change to the directory in which the `vepa_util.exe` command is located.
2. Execute:

```
vepa_util.exe
               command
               --configvm
               --virtual-environment { vmware | vCD }
               --host AppHostName
               --instance DatacenterPath
               --vm VMpathVM_OPTIONS VM_OPTIONS
               --snapshots { 0 | 1 | 2}
               --transportation–mode {san | nbd | nbdssl | hotadd | fastest}
               --enableCt { 0 | 1 }
               --useCt { 0 | 1 }
               --requiresCBT { 1 | 0 }
               --quiescence { 0 | 1 }
               --quiescenceErrLvl { 0 | 1 }
               --optimize–disks { 0 | 1 }
               --uuid UUID_of_VM
```

   The values `{ 0 | 1 | 2}` represent the **Disabled**, **Single**, and **Mixed** snapshot handling modes respectively. For details, see the `vepa_util.exe` man page or the *HP Data Protector Command Line Interface Reference*.

   To change the virtual machine specific settings back to the common virtual machine settings, execute:

```
vepa_util.exe
               command
               --configvm
               --virtual-environment { vmware | vCD }
               --host AppHostName
               --instance DatacenterPath
               --vm VMpath
               --uuid UUID_of_VM
               --default
```

   The message `*RETVAL*0` indicates successful configuration.

Example

To configure the virtual machine with the virtual machine path `/MyDatacenter/MyVM` and with the UUID `42375365-ebe1-e9da-7068-7beb727cab19` that resides in the datacenter `/MyDatacenter` and which is registered in the vCenter Server system `vc.company.com`, with the following settings:

- The snapshot handling mode is mixed.
- Before virtual machine disks are backed up, they are optimized.
- Quiescence snapshots are used.
- If a quiescence snapshot fails, the level of error is a warning.
- CBT is enabled and used.
- Fallback to non-CBT backups is enabled.
- The transportation mode is fastest available.

execute:

```
vepa_util.exe
               command
               --configvm
               --virtual-environment vmware
               --host vc.company.com
               --instance /MyDatacenter
               --vm /MyDatacenter/MyVM
               --snapshots 2
               --enableCt 1
               --useCt 1
               --requiresCBT 0
               --quiescence 1
               --quiescenceErrLvl 0
               --transportation-mode fastest
               --optimize—disks 1
               --uuid 42375365-ebe1-e9da-7068-7beb727cab19
```

Customizing the Data Protector behavior with omnirc options

The omnirc options are useful for troubleshooting or overriding other settings affecting the behavior of the Data Protector client. The options that apply to the Virtual Environment integration have the prefix `OB2_VEAGENT`.

For details on how to use Data Protector omnirc options, see the *HP Data Protector Help* index: “omnirc options”.

Backup

This section contains procedures that are needed to back up virtual machines. For details on backup concepts, see Backup concepts on page 20.

Backup limitations

- Before performing backups,ensure that you use only the supported characters in the names of any VMware vCenter, VMware ESX(i), or VMware vCloud Director objects (for example, virtual machines, datastores, datacenters, vApps, and so on), as special characters are not supported.

  The following list includes the `supported` characters:

  - Letters a-z without any special characters
  - Numbers 0-9
  - Single Quotes (')
  - Spaces
  - Underscores (_)
  - Hyphens (–)

  A **partial list** of special characters that are **not supported** is as follows:

  - % (percentage)
  - + (plus)
  - = (equals)
  - @ (at)
  - < (less than)
  - > (greater than)
  - : (colon)
  - " (double quote)
  - / (forward slash)
  - \ (backslash)
  - | (vertical bar or pipe)
  - ? (question mark)
  - * (asterisk)

Special characters are not supported due to a known VMware issue described at the following URLs:

http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd;=displayKC&externalId;=2017661

http://www.vmware.com/support/developer/vddk/VDDK-1.2.1-RelnoteOPs.html

- After you upgrade to Data Protector 8.11, you cannot restart the failed backup object versions from earlier Data Protector versions.
- For datastores not located on VMFS volume, the full backups take full size of the disk and not only the changed blocks. For more details, see the following URL:

  http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1020128

- Do not enable the vCenter option **disable-datastore-web**. This may result in unsuccessful backups of vmdk and vmx files. For more information, see vSphere Hardening Guides.

Creating backup specifications

Create a backup specification using the Data Protector Manager.

1. In the Context List, click **Backup**.
2. In the Scoping Pane, expand **Backup Specifications**, right-click **Virtual Environment**, and select **Add Backup**.
3. In the Create New Backup dialog box, click **OK**.
4. Specify the application to be backed up:
   - In the **Client** drop-down list, select a VMware client.

     Note: The drop-down list contains all clients that have been imported into the Data Protector cell as VMware vCenter, VMware ESX(i), or VMware vCloud Director clients. They have a corresponding label appended at the end of their names, such as ***(VMware vCenter)***, ***(VMware ESX(i))***, *or* ***(VMware vCloud Director)***.

     If the selected VMware client is not configured correctly, a warning is displayed. Click **OK** to open the Configure Virtual Environment dialog box and provide the connection parameters as described in Importing and configuring VMware clients on page 41.

   - In the **Backup host** drop-down list, select a system to be used to control the backup. The list contains all clients that have the Data Protector `Virtual Environment Integration`

component installed.

- In **Datacenter/Organization**, select a datacenter or a VMware vCloud Director organization to back up from.

  Note: If you have selected a standalone ESX(i) Server system in the **Client** option, there is only one datacenter available – **/ha-datacenter**.

  If you have selected a vCenter Server system in the **Client** option, you can select **All Datacenters** to back up virtual machines from different datacenters.

  If you have selected a vCloud Director in the **Client** option, you can select **All Organizations** to back up virtual machines from different organizations.

- In **Backup method**, the backup method is displayed:
  - **vStorage Image** for VMware vCenter and VMware ESX(i) clients
  - **vCD vStorage Image** for VMware vCloud Director clients
- In **Free space required [%]**, specify the percentage of disk space that should be free on a datastore before a virtual machine is backed up. The free space is calculated based on the size of the datastore where the virtual machine disks reside.

  The check is performed separately for each virtual machine. For details, see Free space required option on page 34.

Figure 20: Selecting a VMware vCenter Server client, backup host, and datacenter

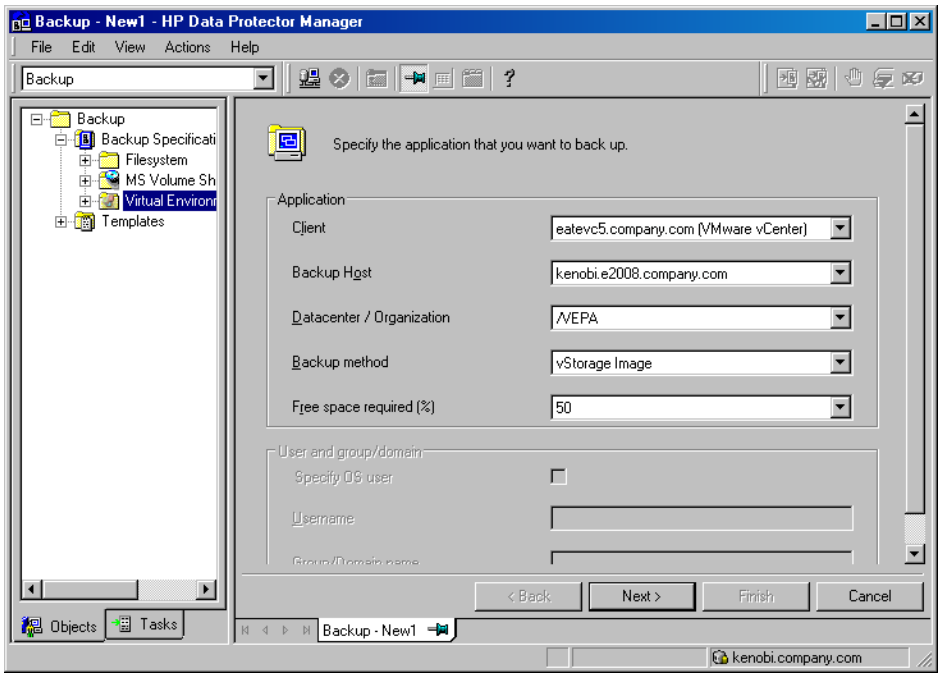
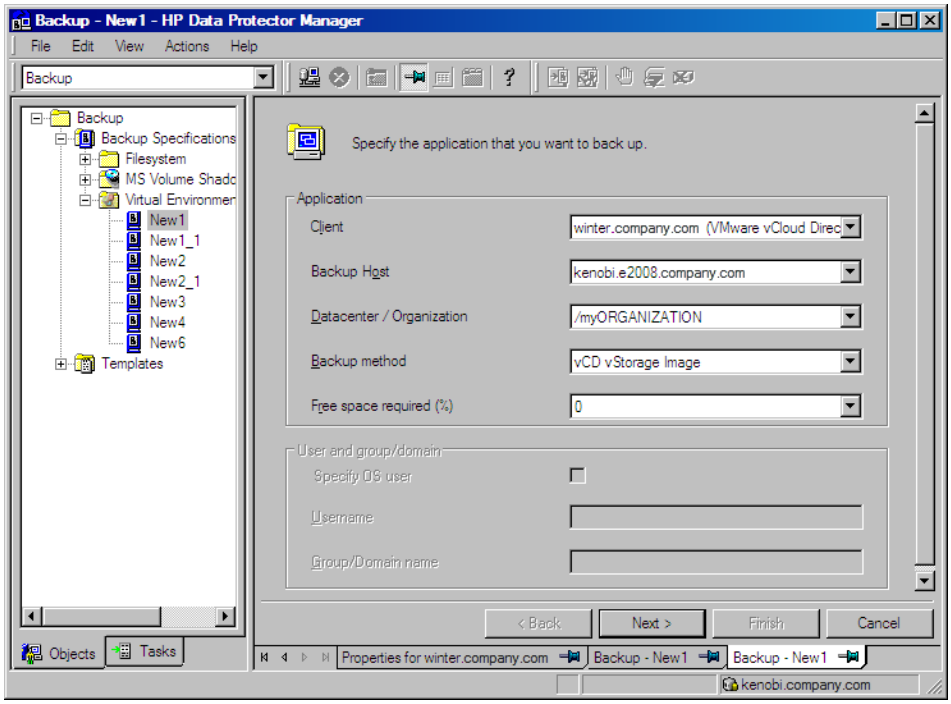


Figure 21: Selecting a VMware vCloud Director client, backup host, and organization



Click **Next**.

Note: The settings specified in this page of the wizard cannot be changed once the backup specification is saved. To change the settings, you will have to create a new backup specification.

5. Select the objects that you want to back up. In the **Show** drop-down list, simplify your selection by choosing the **Hosts and Clusters** or **VMs and Templates** view. By default, **Hosts and Clusters** is displayed.

   Note: If you switch the view after you have already selected one or more objects for backup, a warning dialog is displayed. Its confirmation clears the already selected objects, clicking **No** does no change to the view.

   You can make your selections at different levels:

   - For VMware vCenter and VMware ESX(i) clients:
     - ESX/ESXi Servers systems
     - Pools
     - vApps
     - VM folders
     - Individual VMs
     - VM disks
     - VM templates
   - For VMware vCloud Director clients:
     - Organizations
     - vDatacenters
     - vApps
     - Individual VMs

   If you select any level above individual VMs (for example, a vApp or a VMware vCloud Director organization), all VMs and VM disks contained in the selected item will be included in the backup specification. If VMs are added within the item after the backup specification is saved, they will also be backed up.

Figure 22: Selecting VMware objects (vCenter Server client)

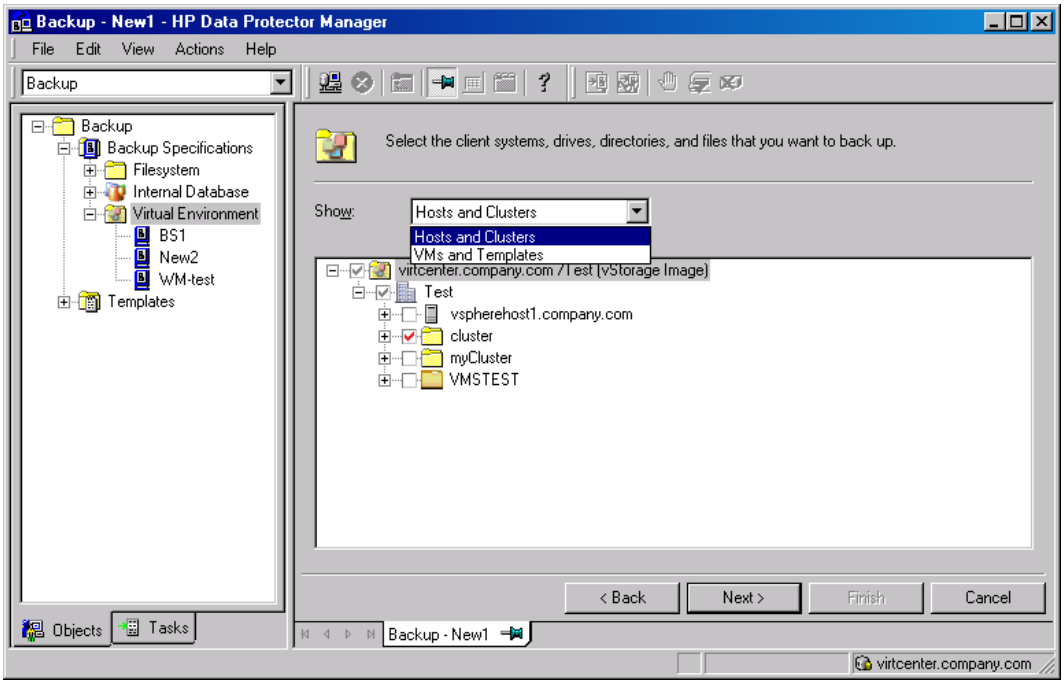


Figure 23: Switching view while selecting VMware objects (vCenter Server client) – warning

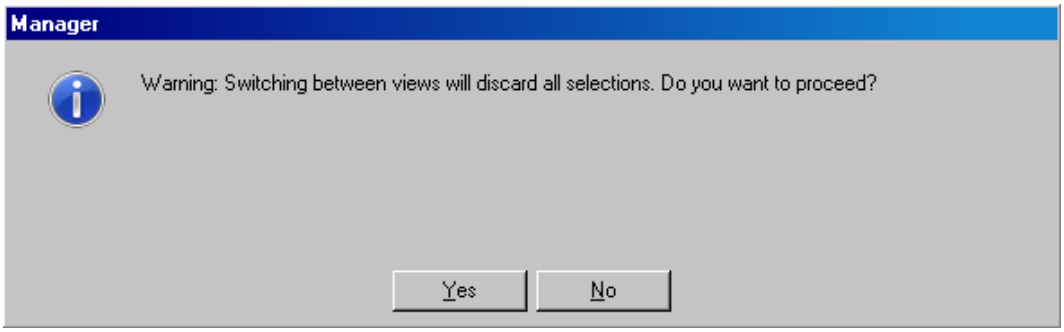
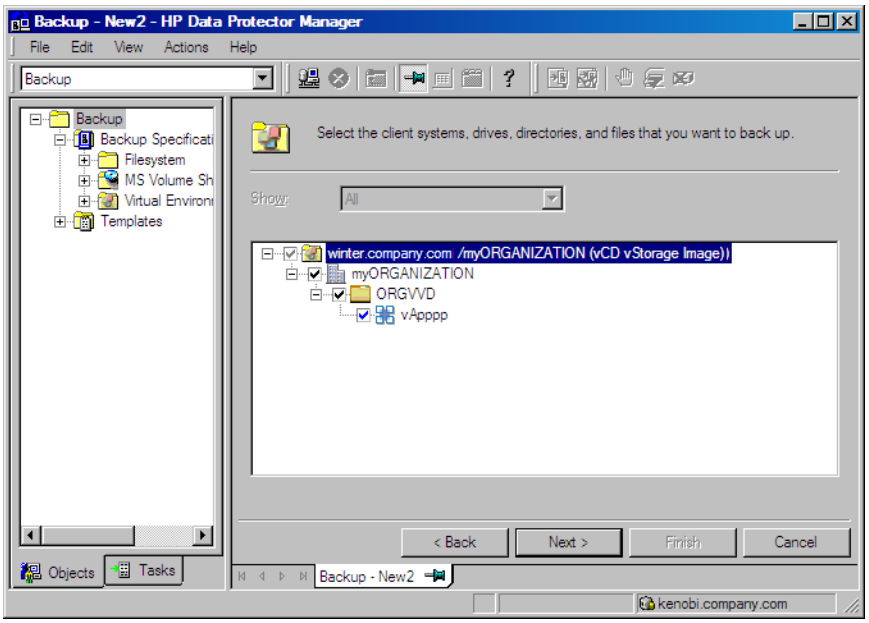


Figure 24: Selecting VMware objects (vCloud Director client)



Important: In the object tree of a particular VMware client, a virtual machine may be displayed as selected in two different ways:

- The *blue* check mark indicates that the virtual machine is selected for backup in its entirety, including its configuration and all its virtual disks.

  If such a virtual machine is backed up, it can be restored even if the original virtual machine does not exist anymore.

- The *gray* or *black* check mark indicates that some or all virtual disks belonging to the virtual machine are selected. The virtual machine itself and its configuration is omitted from the backup.

  If such a virtual machine is backed up, its disks can only be restored if the original virtual machine is still configured at the time of restore.

If your virtual machines are not configured yet, right-click the client system at the top or any of the virtual machines listed below, and select **Configure Virtual Machines**. For details, see Configuring virtual machines on page 50.

Click **Next**.

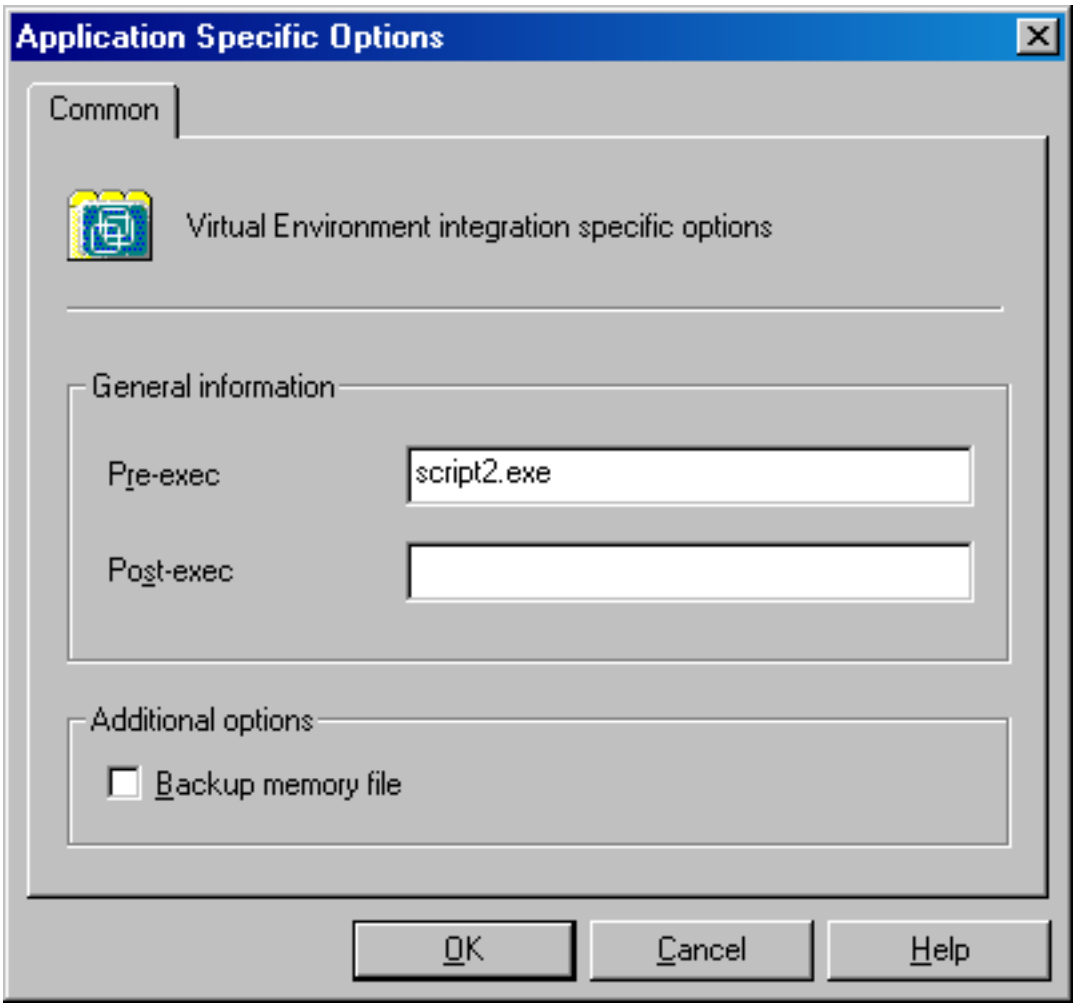
6. Select which devices to use for the backup.

   To specify device options, right-click the device and select **Properties**. Specify the number of parallel backup streams in the **Concurrency** tab and which media pool to use.

Click **Next**.

7. Set backup options.
8. For information on application-specific backup options, see VMware backup options on the next page.

Figure 25: Application-specific options



Click **Next**.

9. Optionally, schedule the backup. See Scheduling backup sessions on page 72.

Click **Next**.

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

Tip: Preview your backup specification before using it for a real backup. See Previewing

backup sessions on page 73.

Table 9: VMware backup options

Option	Description
Pre-exec , **Post-exec**	Specifies which command line to run on the backup host before (`pre-exec`) or after (`post-exec`) the backup. Do not use double quotes. Type only the name of the command and ensure that the command resides in the default Data Protector administrative commands directory on the backup host. *Windows systems*: `Data_Protector_home\bin` *Linux systems*: `/opt/omni/bin`
Backup memory file	If this option is selected, the memory of a running virtual machine is saved into a file and backed up. Do not select this option if one or more virtual machines selected in the backup specification have the **Use quiescence snapshots** selected.

Modifying backup specifications

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

In the Source page, you can modify the backup objects by using the **Show** drop-down list. In the drop-down list, the **Hosts and Clusters** view or the **VMs and Templates** view are available. The view that you have used during the creation of your backup specification has the string `(Original)` appended. If you switch the view, a warning dialog is displayed and its confirmation clears the already selected objects.

Note: When modifying a backup specification created with one of the previous versions of Data Protector, you can switch between **Selected**, **All**, **Hosts and Clusters**, and **VMs and Templates** views. The view **All** is available for the legacy backup specifications only and provides a legacy browsing mechanism. Selecting **Hosts and Clusters** or **VMs and Templates** and clicking **Yes** in the warning dialog clears the previous backup object selection and upgrades your browsing mechanism. After saving the backup specification only the **Hosts and Clusters** and **VMs and Templates** views are available.

Figure 26: Modifying a backup specification (VMware vCenter Server client)

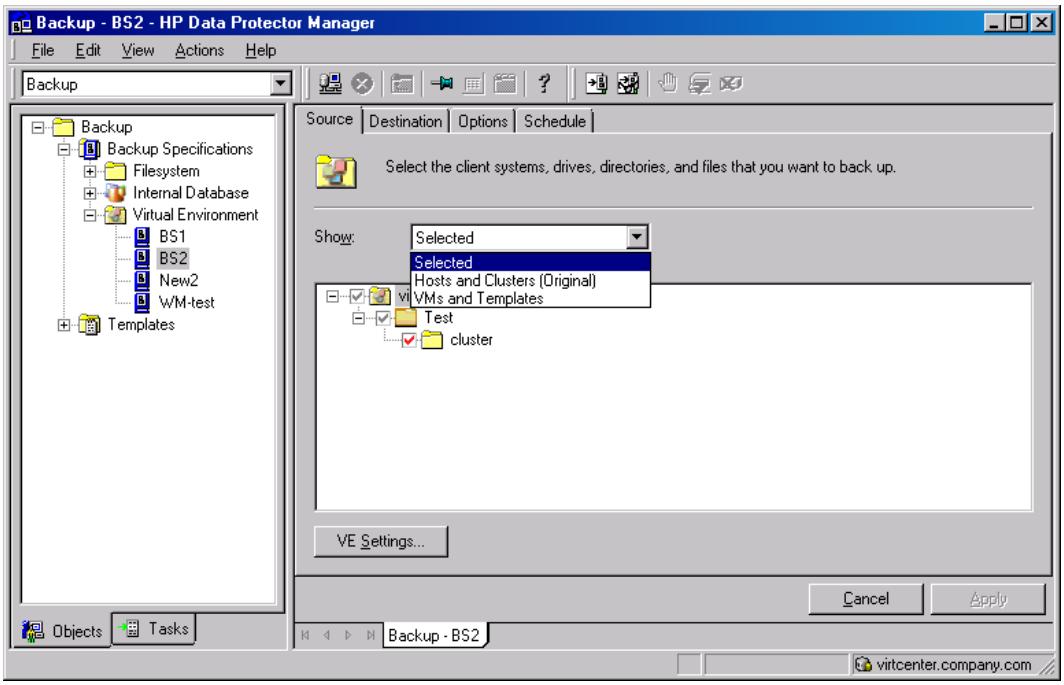


Figure 27: Switching view while modifying a backup specification (VMware vCenter Server client) – warning

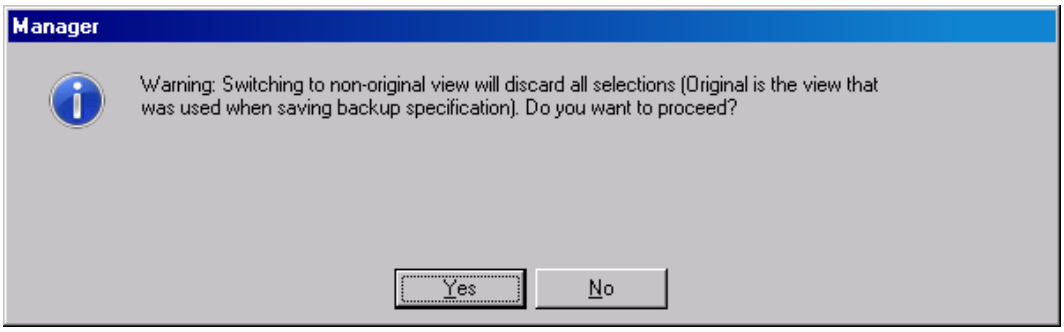
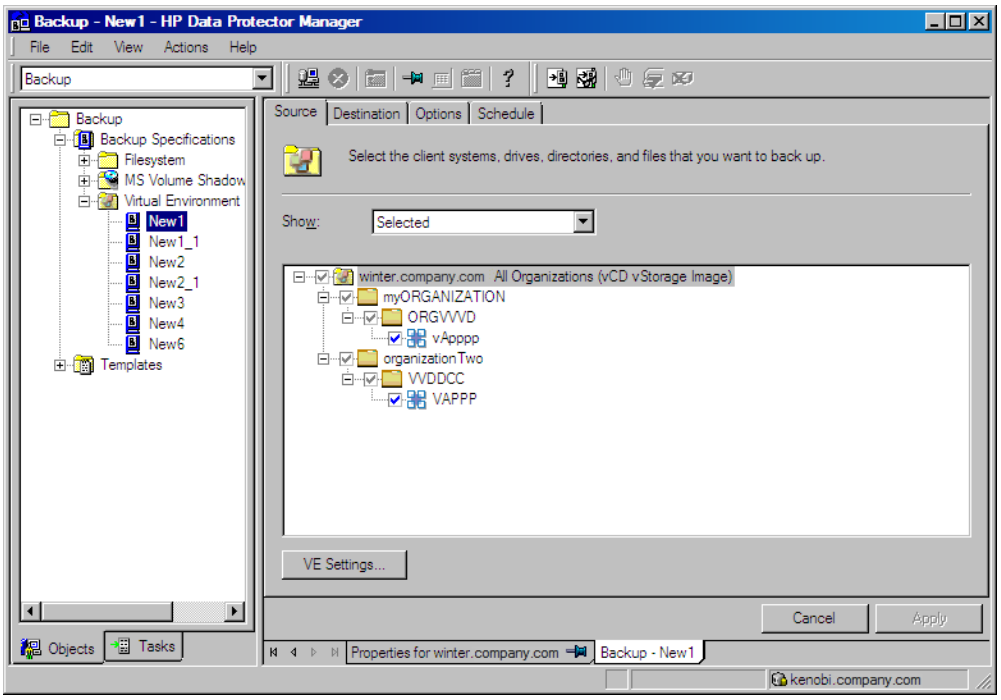


Figure 28: Modifying a backup specification (VMware vCloud Director client)



To display the virtual environment settings, in the Results Area, click **VE Settings**. Not all settings can be modified.

Figure 29: Virtual environment settings (VMware vCenter Server client)

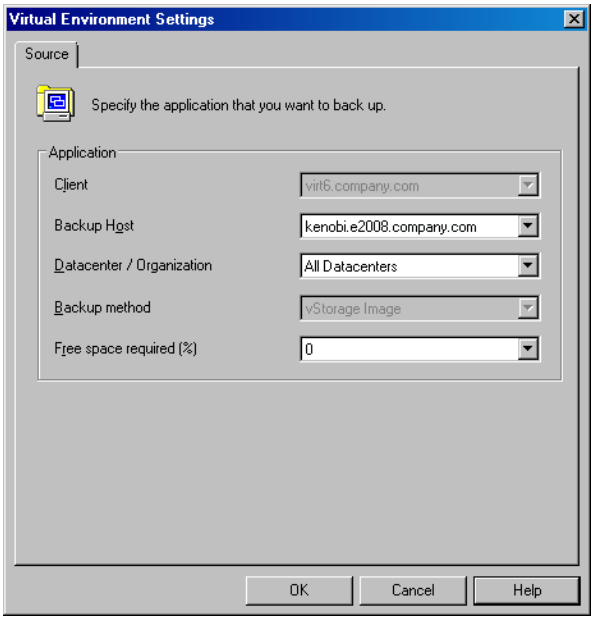
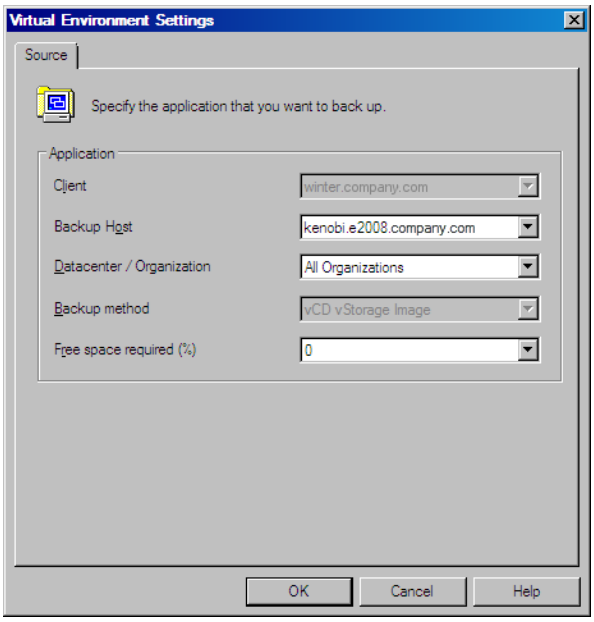


Figure 30: Virtual environment settings (VMware vCloud Director client)



Scheduling backup sessions

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

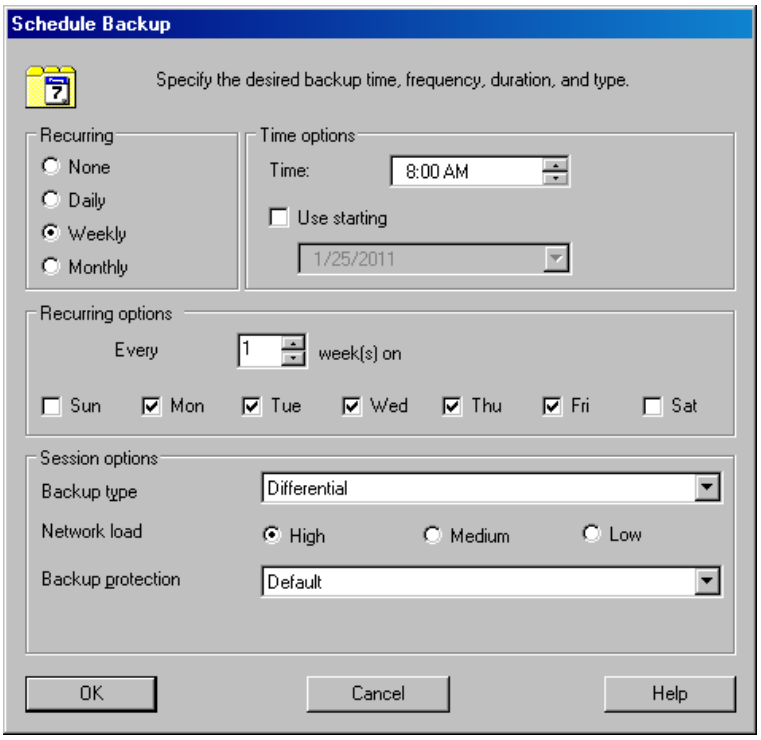
Scheduling example

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

1. In the Schedule property page of the backup specification, select the starting date in the calendar and click **Add** to open the **Schedule Backup** dialog box.
2. Under Recurring, select **Weekly**. Under Time options, select **8:00**. Under Recurring options, select **Mon**, **Tue**, **Wed**, **Thu**, and **Fri**. See Scheduling a backup session on the next page. Under Session options, select **Differential** from the **Backup type** drop-down list.

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

Figure 31: Scheduling a backup session



Previewing backup sessions

Preview the backup session to test it. You can use the Data Protector GUI or CLI.

Using the Data Protector GUI

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

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

Using the Data Protector CLI

1. Log in to any client with the Data Protector `User Interface` component installed.
2. Open the command prompt and change to the directory in which the `omnib` command is located.

3. Execute:

   ```
   omnib -veagent_list BackupSpecificationName -test_bar
   ```

What happens during the preview?

The following are tested:

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

Starting backup sessions

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

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

Using the Data Protector GUI

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

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

Using the Data Protector CLI

1. Log in to any client with the Data Protector `User Interface` component installed.
2. Open the command prompt and change to the directory in which the `omnib` command is located.
3. Execute:

   ```
   omnib -veagent_list BackupSpecificationName [-barmode VirtualEnvironmentMode]
   [ListOptions]
   ```

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

full|diff|incr

The default is full.

For *ListOptions*, see the omnib man page or the *HP Data Protector Command Line Interface Reference*.

Examples

To start a full backup using the backup specification MyVirtualMachines, execute:

```
omnib -veagent_list MyVirtualMachines -barmode full
```

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

```
omnib -veagent_list MyVirtualMachines -barmode diff
```

Preparing for disaster recovery

To do a disaster recovery, you need backups of the following VMware objects:

Table 10: What must be backed up

VMware object	How to back it up
ESX/ESXi Server console	***ESX Server systems:*** 1. Ensure that the Data Protector `Disk Agent` component is installed on all the ESX Server systems. 2. In the Backup context of the Data Protector GUI, right-click **Filesystem** and select **Add backup** to create a backup specification of the filesystem type. In the Source page of the backup specification, select ESX Server consoles of all ESX Server systems. For details on what to back up, see the topic "ESX Server Configuration Backup and Restore procedure" at http://kb.vmware.com/selfservice/microsites/microsite.do. 3. Start a backup using the newly created backup specification. ***ESXi Server systems:*** With ESXi Server systems, it is not possible to install a Data Protector `Disk Agent`, so you will need to use VMware utilities to back up the configuration. A tool, `esxcfg-cfgbackup` is available from VMware. For information, see the VMware website.
vCenter configuration database *(applicable only for VirtualCenter environments)*	The vCenter configuration database can be an Oracle database or Microsoft SQL Server database. To back up the database, use the corresponding Data Protector integration. For example, if it is an Oracle database, follow these steps: 1. Ensure that the Data Protector `Oracle Integration` component is installed on the vCenter Server system. 2. In the Backup context of the Data Protector GUI, right-click **Oracle Server** and select **Add backup** to create a backup specification of the Oracle type. In **Application database**, type the name of the vCenter configuration database. Continue with the backup specification creation as described in the *HP Data Protector Integration Guide for Oracle and SAP*. 3. Start a backup using the newly created backup specification.
VMware virtual machines	Back up the virtual machines as described in this chapter.

Restore

This section contains procedures that are needed to restore virtual machines. For details on restore concepts, see Restore concepts on page 36.

Restore limitations

- When restoring a VM to a datacenter with a datastore shared among several inventory objects (hosts or clusters) or several cluster nodes, and the restore option for its subsequent registration is selected, the restored VM may not register at the original inventory location:
  - If several inventory objects share the datastore, the VM is registered with the first available host or cluster.
  - If several cluster nodes share the datastore, the VM is registered with the first available cluster node.

  If the VM must be registered at its original inventory location, migrate it appropriately after the restore session completes.
- Before performing a restore,ensure that you use only the supported characters in the names of any VMware vCenter, VMware ESX(i), or VMware vCloud Director objects (for example, virtual machines, datastores, datacenters, vApps, and so on), as special characters are not supported. For more details on the supported characters, see Backup Limitations.
- Before a restore of a virtual machine backed up with the vCD vStorage Image backup method is started, the vApp where the selected VM resides enters maintenance mode for consistency reasons. As a consequence all VMs in this vApp are shut down.
- Restoring virtual machines to a specific datastore is not supported using the vCD Storage Image backup method.
- vDatacenters that are disabled do not allow adding or removing of vApps. Consequently restore to a disabled vDatacenter is not supported.
- In a vSphere environment, do not use the left parenthesis (the (character) in names of vSphere distributed port groups. Data Protector is unable to connect a restored virtual machine to a non-original vSphere network that uses distributed switches and is assigned such a distributed port group. In this case, after the restore, you need to manually connect the restored virtual machine to the desired network using vSphere Client.
- Recovering virtual machines after a restore to a directory is not supported for incremental or differential backups. The VMware Converter that is used for moving the restored VM images to an ESX Server or ESXi Server system recognizes only the full backup type.
- Recovering virtual machines from a backup chain (for example, full, incremental, incremental, incremental...) is supported only for a restore to a datacenter.

- All the media related to a session should be exported or imported together.If a media from the full backup object is missing then the Incremental/Differential backup will not detect a missing media and continue to run in the selected mode. A restore from such a session will not be successful.
- A virtual machine can be seen as different objects in the Internal Database (IDB) and in the restore context based on how the backup specification was created.
- It is not possible to restore a suspended Virtual Machine.
- Restoring virtual machine disks from backups created with earlier versions of Data Protector reads all disks including ones that are not selected for restore.
- Movement from one disk to another on a tape is not possible. Consider a virtual machine with five disks (scsi0:0, scsi0:1, scsi0:2, scsi0:3, and scsi0:4). You select disks scsi0:1 and scsi0:3 for restore and scsi0:2 is being read but it is not restored as it is not selected for restore. So, if you do not select consecutive disks for restore, all the disks from the first to the last are read but only the selected ones are restored.

Finding information for restore

You can find information about backup objects in the Data Protector IDB, such as which backup type and media were used, and which messages were displayed during the backup. To retrieve this information, use the Data Protector GUI or CLI.

Using the Data Protector GUI

In the Internal Database context, expand **Objects** or **Sessions**.

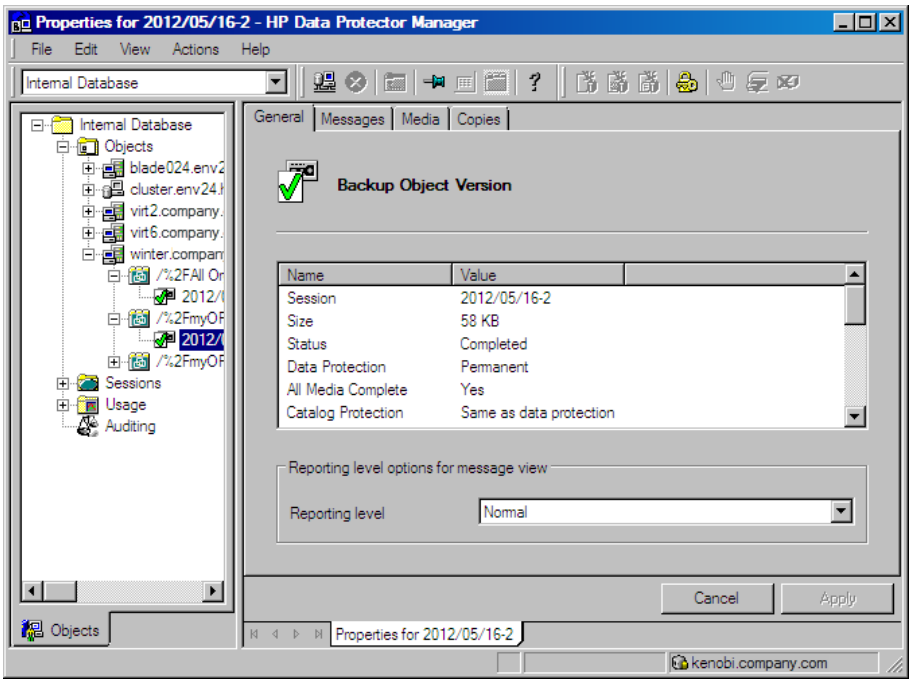
If you expand **Objects**, backup objects are sorted according to the virtual machine for which they were created. For example:

- Backup objects for the virtual machine `/vm/mach1` are listed under `/4/vCenterName%2FvmInstanceUUID`.
- Backup objects for the virtual machine `/vm1Org22` from vApp `vAppORG22`, from vDatacenter `vDCOrg22`, from the VMware vCloud Director organization `ORG22` are listed under `/%2FORG22/8/%2FORG22%2FvDCOrg22%2vAppORG22%2Fvm1Org22`.

If you expand **Sessions**, backup objects are sorted according to the session in which they were created. For example, backup objects created in the session `2012/07/10-82` are listed under `2012/07/10-82`.

To view details on a backup object, right-click the backup object and select **Properties**.

Figure 32: Backup object information



Tip: To view the messages displayed during the session, click the **Messages** tab.

Using the Data Protector CLI

1. Log in to any client with the Data Protector `User Interface` component installed.
2. Open the command prompt and change to the directory in which the `omnidb` command is located.
3. Get a list of VMware backup objects created in a backup session with the session ID *SessionID*:

   ```
   omnidb -session SessionID
   ```

4. Get details on a backup object with the backup object name *BackupObjectName*:

   ```
   omnidb -veagent BackupObjectName -session SessionID -catalog
   ```

   Here is one example of a backup object name:

   ```
   gabriel.company.com::/%2FElDatacentro/0/%2Fvm%2Fharbour
   ```

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

Restoring using the Data Protector GUI

1. In the Context List, click **Restore**.
2. In the Scoping Pane, expand **Virtual Environment**, expand the relevant client and click the datacenter or the VMware vCloud Director organization from which you backed up.
3. In the Source page, Data Protector displays VMware objects.

   By using the **From** and **To** options, you can narrow the scope of displayed virtual machines to those backed up within the specified time interval.

   In the VM Filter text box, enter filter text for the VM and press **Enter**, or click **Apply Filter**.

   The filter hides the VMs, vApps, and resource pools that do not match the filter pattern allowing you to find the desired object easily.

   Note: Filters are case-sensitive and apply to VMware Virtual Machine objects, VMware Virtual Application (vApp) objects, and resource pools. If a matching sub-node is found (such as, another VM, vApp, or resource pool), they are displayed. If you leave the VM Filter text box empty, all the VMs, vApps, and resource pools are displayed. However, if you enter filter text, only the matching sub-nodes (if any) are displayed. If you modify the filter values using the `From`, or `To` drop-down lists, filtering is re-applied. Filter does not apply to already selected VMs, vApps, or resource pools. This means that you can filter machines using one filter, select objects, and again change the filter. In the new filter, the previously marked objects remain visible.

   The following are the types of filter usage:

   - **Simple substring usage** - If you enter part of a VM, vApp, or resource pool name, all VMs, vApps, or resource pools in the object tree that have the entered string in their name remain visible. All other objects are filtered out.
   - **Wildcards and question mark usage** - The following are the filtering options:
     - `<filter string>*` - Filters VM, vApp, or resource pool names that start with the `<filter string>` and end with any set of characters.
     - `*<filter string>*` - Filters VM, vApp, or resource pool names that start and end with any set of characters, and have the `<filter string>` in between.
     - `*<filter string>` - Filters VM, vApp, or resource pool names that start with any set of characters and end with the `<filter string>`.
     - `<filter string>*01` - Filters VM, vApp, or resource pool names that start with the `<filter string>`, end with a "01", and have any set of characters in place of the wildcards (*). For example, `Production_VM01`.

- `<filter string>*0?` - Filters VM, vApp, or resource pool names that start with the `<filter string>`, end with a "0" and have a character, number, or letter in place of the question mark (?). For example, `Production_VM01` and `Production_VM0A`, but not `Production_VM11`.

Select the objects that you want to restore.

Note: Data Protector restores the full restore chain for each selected VMware object, beginning with the last full backup session (even if that full backup is outside the specified time interval) and ending with the last backup session performed during the specified time interval.

Figure 33: Selecting VMware objects for restore (vCenter Server client)

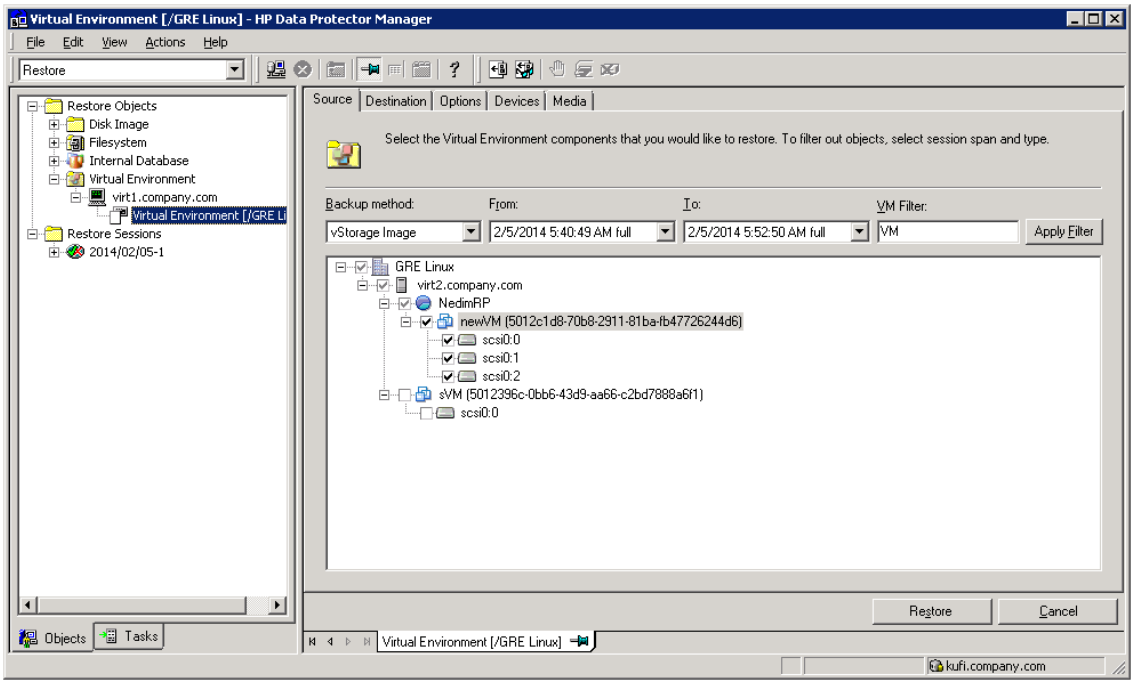
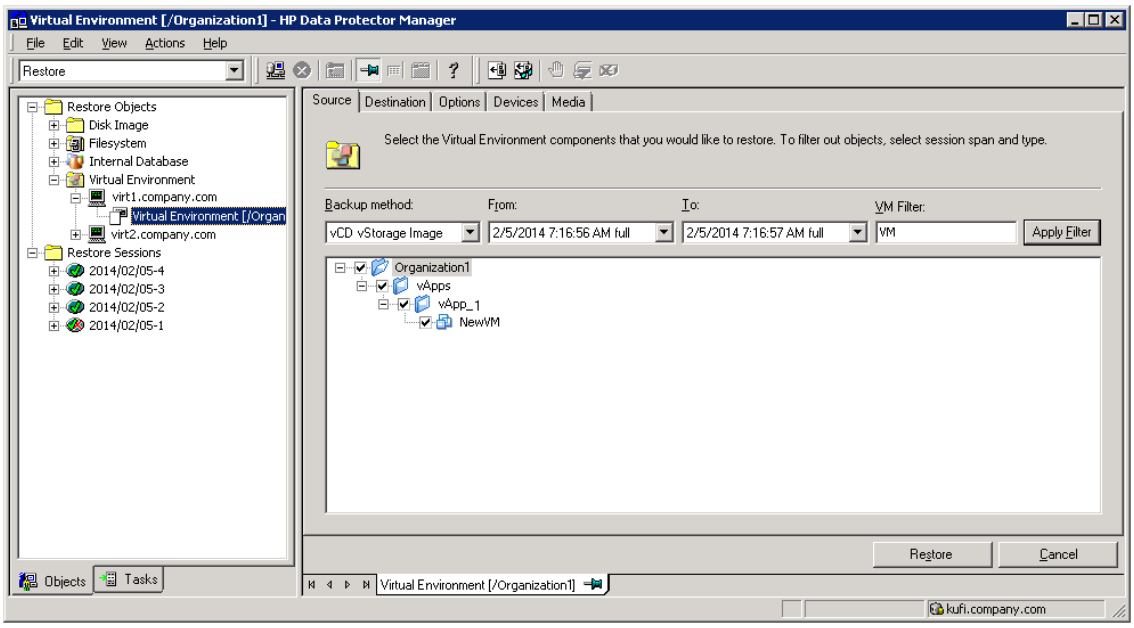
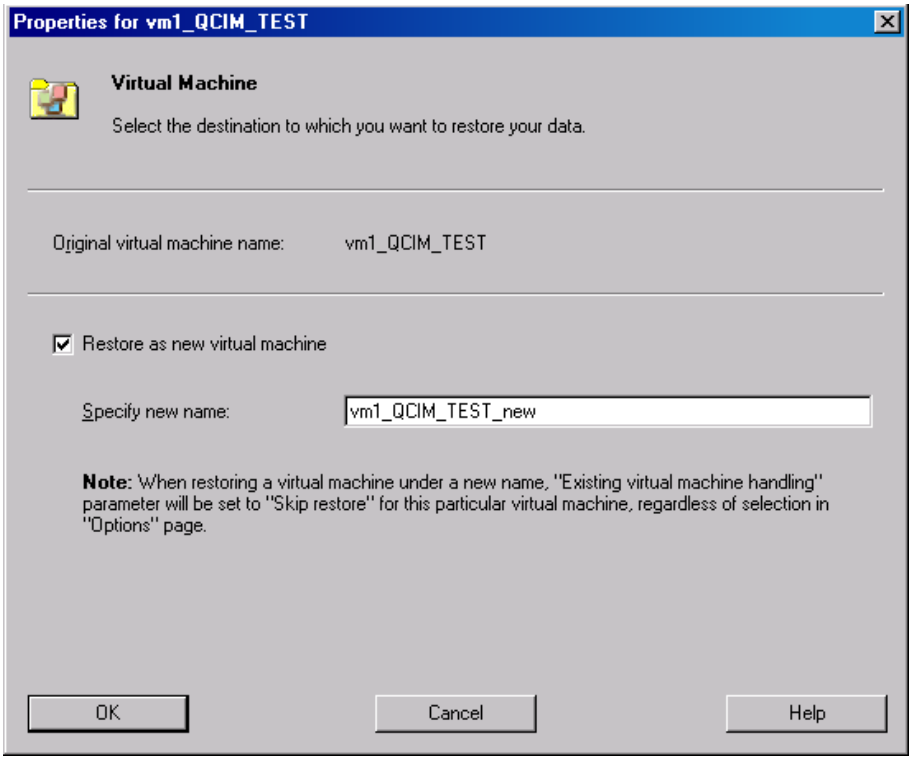


Figure 34: Selecting VMware objects for restore (vCloud Director client)



Optionally, by right-clicking the selected virtual machine and then clicking **Restore As / Into**, you can restore it as a new virtual machine. A new dialog box opens to specify the name of the virtual machine.

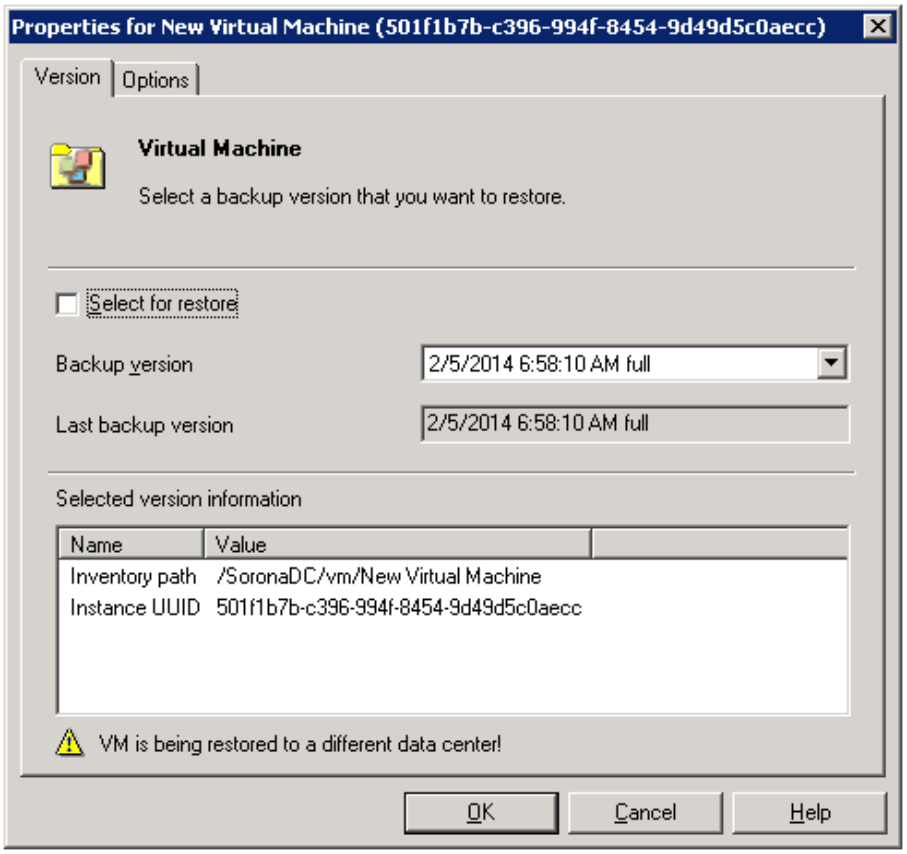
Figure 35: Restoring as a new virtual machine



However, by right-clicking the selected virtual machine and clicking **Restore Version**, you can select a backup version that you want to restore. A new dialog box opens to specify the backup version which will be appended to the virtual machine name.

Note: A warning message `VM is being restored to a different data center` is displayed in the dialog box when the backup version is selected from a different datacenter.

Figure 36: Restoring selected backup version



4. In the Destination page, specify the restore destination. For details, see Restore destination (VMware vCenter Server and VMware ESX(i) Server clients) on page 87 or Restore destination (VMware vCloud Director client) on page 89.

Figure 37: Restore destination (VMware vCenter Server client)

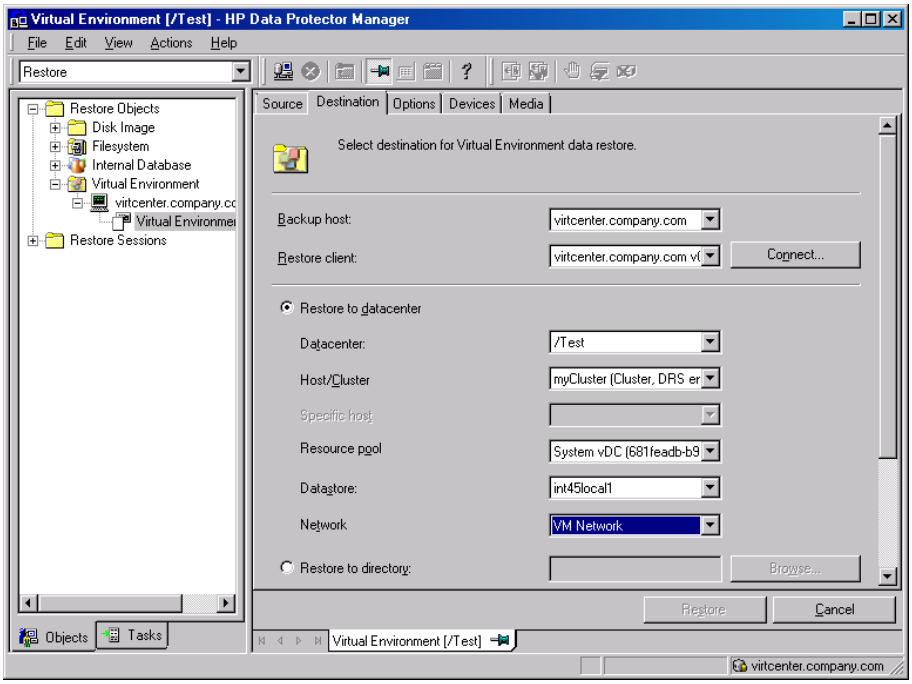
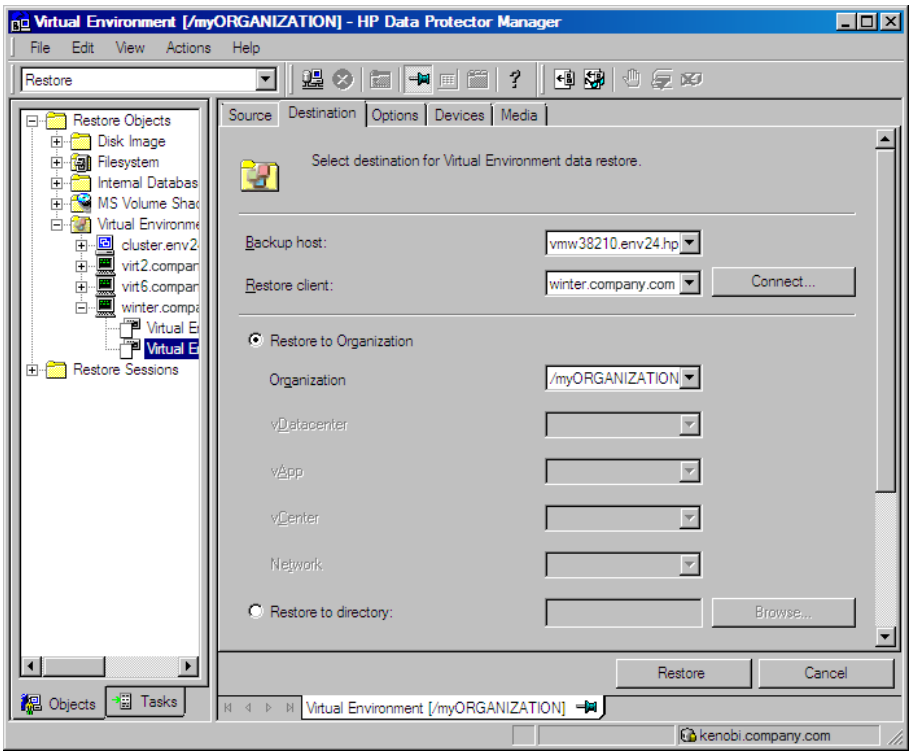


Figure 38: Restore destination (VMware vCloud Director client)



5. In the Options page, specify the VMware restore options. For details, see Restore options on

page 90.

Figure 39: Restore options (VMware vCenter Server and VMware ESX(i) Server clients)

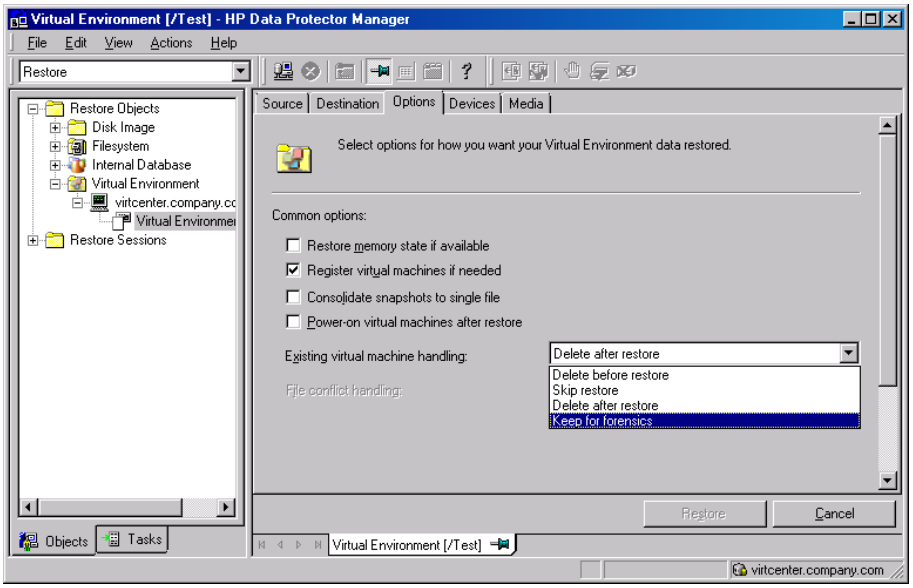
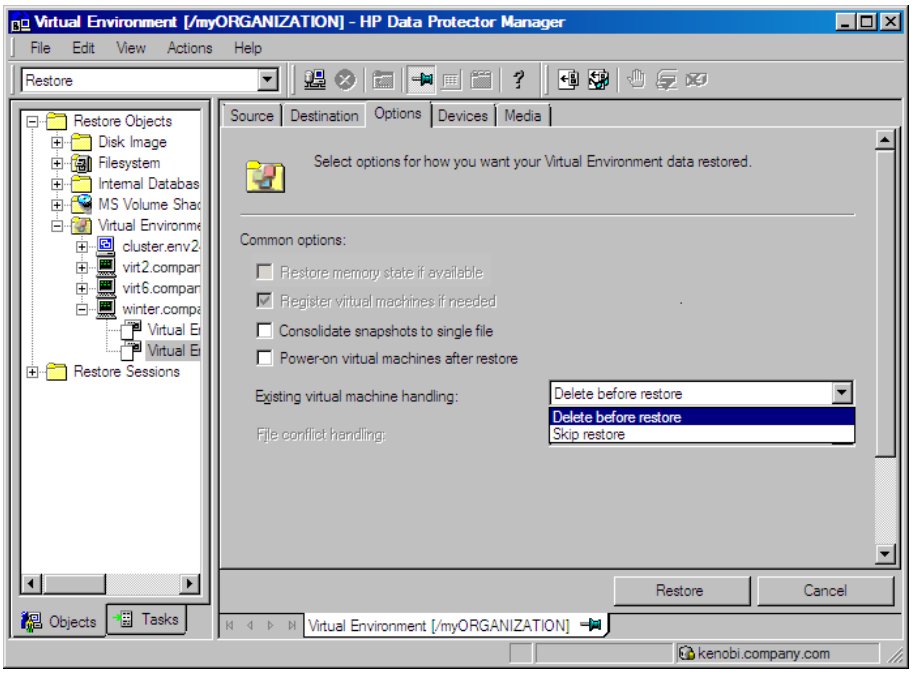


Figure 40: Restore options (VMware vCloud Director client)



6. In the Devices page, select devices to use for restore.
7. Click **Restore**.

8. In the Start Restore Session dialog box, click **Next**.
9. Specify **Report level** and **Network load**.

   Note: Select **Display statistical information** to view the restore profile messages in the session output.

10. Click **Finish** to start the restore.

    The statistics of the restore session, along with the message `Session completed successfully` is displayed at the end of the session output.

    Note: If the restore fails, see Cleaning up a datastore after a failed restore on page 103.

    Note: It is not possible to restore the memory state of the Virtual Machine during the restore of a vCD vStorage Image backup, as the Virtual Machine needs to be running to restore the memory and it is also not possible to import a running Virtual machine to the vCD.

    However, it is possible to restore the session to the vCenters (vStorage Image restore) by selecting the options **Power-on virtual machines after restore** and **Restore memory state if available**.

    After the restore operation is completed, the required operations can be performed in the restored virtual machine through the Vcenter. Shut down the restored virtual machine and import it into the vCD.

    vStorage Restore: To restore the memory state of the Virtual Machine you need to power on the virtual machine and that cannot be done unless you select the **Power-on virtual machines after restore** option. If this option is not selected then the **Restore memory state** option is ignored.

Table 11: Restore destination (VMware vCenter Server and VMware ESX(i) Server clients)

GUI/CLI option	Description
Backup host / `-barhost`	Specifies the client with the Virtual Environment Integration installed to control the restore session. By default, the same client as used for the backup is selected.

GUI/CLI option	Description
Restore client / `-apphost`	Specifies the client that the selected virtual machine objects should be registered and restored to. By default, the client from which the virtual machines were backed up is selected. To change the client configuration, click the **Connect** button.
Restore to datacenter / `-instance -newinstance`	Select this option to restore a virtual machine to a datacenter. By default, virtual machines are restored to the original datacenter.
Host/Cluster / `-host/cluster`	Select the ESX(i) Server system or the cluster to which virtual machines should be restored. By default, virtual machines are restored to the original ESX(i) Server system or cluster.
Specific host / `-specificHost`	Select the specific ESX(i) Server system in the cluster to which virtual machines should be restored. By default, virtual machines are restored to the original ESX(i) Server system.
Resource pool / `-resourcePool`	Select the resource pool on the ESX(i) Server system or the cluster to which virtual machines should be restored. By default, virtual machines are restored to the original resource pool.
Datastore / `-store`	Specifies the datastore to which the virtual machines should be restored. You can choose among all datastores that are accessible from the selected restore target host. If you leave this option empty, the virtual machines are restored to the original datastore.
Restore to directory / `-directory`	Select this option to restore virtual-machine files to a directory (outside of the datacenter) on the backup host. You can use the **Browse** button to find the target directory. After such a restore, the virtual machines are not functional. You need to manually move the restored virtual machine images to an ESX Server or ESXi Server system, using the VMware Converter as described in Recovering virtual machines after restore to a directory on page 96.

Table 12: Restore destination (VMware vCloud Director client)

GUI/CLI option	Description
Backup host / `-barhost`	Specifies the VMware vCloud Director client with the Virtual Environment Integration installed to control the restore session. By default, the same client as used for the backup is selected.
Restore client / `-apphost`	Specifies the client that the selected virtual machine objects should be registered and restored to. By default, the client from which the virtual machines were backed up is selected. To change the client configuration, click the **Connect** button.
Restore to organization / `–neworganization`	Select this option to restore virtual machines to an organization. By default, virtual machines are restored to the original organization, but you can specify a different destination organization.

vDatacenter /
`-virtual_datacenter_path`
`-virtual_datacenter_uuid`
	Specifies the vDatacenter to which the virtual machines should be restored. By default, the virtual machines are restored to the original vDatacenter.

vApp /
`-vapp_path`
`-vapp_uuid`
	Specifies the vApp to which the virtual machines should be restored. By default, the virtual machines are restored to the original vApp.
	Note that the virtual machines are restored as a new vApp if the original vApp is no longer available or all virtual machines of the selected vApp are restored.

vCenter /
`-vcenter_path`
`-vcenter_uuid`
	Specifies the vCenter to which the virtual machines should be restored. By default, the virtual machines are restored to the original vCenter.
	If this option is not selected, the virtual machines are restored to the vCenter used by the selected vDatacenter or vApp.

GUI/CLI option	Description

Network /
`-network_name`
`-network_uuid`
	Select a network to enable virtual machines communication.
	If an individual virtual machine is restored into an existing vApp, the vApp network is selected.
	If all virtual machines of the selected vApp are restored, the Organization network is selected.

Restore to directory / `-directory`	Select this option to restore virtual-machine files to a directory (outside of the organization) on the backup host. You can use the **Browse** button to find the target directory. After such a restore, the virtual machines are not functional. You need to manually move the restored virtual machine images to an ESX Server or ESXi Server system, using the VMware Converter as described in Recovering virtual machines after restore to a directory on page 96.

Table 13: Restore options

GUI/CLI option	Description
Restore memory state if available / `-memory`	Available if **Restore to datacenter** and **Power-on virtual machines after restore** is selected. Select this option to restore the memory file if it is included in the backup.
Register virtual machines if needed / `-register`	Available if **Restore to datacenter** is selected. Select this option to register restored virtual machines. If this option is not selected, you need to manually recover the restored virtual machines as described in Recovering virtual machines manually on page 96. Default: selected.
Consolidate snapshots to single file / `-consolidate`	Select this option to commit all snapshots (including non-Data Protector ones) to the virtual machine base once a virtual machine is restored. Available if **Restore to datacenter** is selected.

GUI/CLI option	Description
Power-on virtual machines after restore / `-poweron`	Select this option to power the virtual machines on once they are restored. Available if **Restore to datacenter** is selected.

GUI/CLI option		Description
Existing virtual machine handling	Specifies Data Protector's behavior when restoring existing virtual machines.	
	Delete before restore / `-deletebefore`	Select this option to delete an existing virtual machine before it is restored, and then restore it from new. The existing virtual machine is deleted even if it resides in a different datacenter from your target datacenter. This is the space-efficient option, but is less secure, since the old virtual machine is not available if the restore fails, so select it with caution.
	Skip restore / `-skip`	Select this option to skip the restore of an existing virtual machine. This allows you to restore missing virtual machines without affecting existing ones.
	Delete after restore / `-deleteafter`	Select this option to delete an existing virtual machine after it is restored. The existing virtual machine is deleted even if it resides in a different datacenter than your target datacenter. If the restore fails, the existing virtual machine is not deleted. Default: selected. This option is not available for VMware vCloud Director client. This option cannot be used if the virtual machine is in a suspended state.If the virtual machine is in a suspended state, do any of the following: • Restore to a different location. • Select the **Delete before restore** option. • Power On or Off the virtual machine.
	Keep for forensics / –keep_for_ forensics	Select this option to mark an existing virtual machine with a timestamp. The virtual machine which is kept for forensics is powered off after the restore and remains at the original location. It does not affect consecutive backups of the original virtual machine. This option is not available for VMware vCloud Director and Microsoft Hyper-V clients.

GUI/CLI option		Description
File conflict handling	Specifies Data Protector's behavior when restoring existing files.	
	Overwrite / `-overwrite`	Select this option to overwrite existing files with those from the backup. Default: selected.
	Keep latest / `-latest`	Select this option to leave an existing file intact if it is more recent than the one from the backup. Otherwise, the existing file is overwritten with the one from the backup.
	Skip / `-skip`	Select this option to preserve an existing file (the file is not restored from the backup).

Restoring using the Data Protector CLI

1. Log in to any client with the Data Protector `User Interface` component installed.
2. Open the command prompt and change to the directory in which the `omnir` command is located.
3. Execute:

   VMware vCenter Server or VMware ESX(i) Server client

```
omnir -veagent
       -virtual-environment vmware
       -barhost BackupHost
       -apphost OriginalVMwareClient
       -instance OriginalDatacenter
       -method vStorageImage
       [-session BackupID]
       VirtualMachine [VirtualMachine...]
       [VMwareClient | Directory]

       VirtualMachine
       -vm VMPath -instanceUUID [-new_name NewVirtualMachineName][-disk DiskName [-
disk Disk...]]

       VMwareClient
       [-newinstance TargetDatacenter]
       [-store TargetDatastore]
       [-network_name TargetNetwork]
       [-destination TargetVMwareClient]
       [-consolidate] [-memory] [-register][-poweron]
       [-deletebefore | -deleteafter | -skip | -keep_for_forensics]
```

```
       Directory
       -directory RestoreDirectory
       [–overwrite | -skip | –latest]
```

VMware vCloud Director client

```
omnir -veagent
       -virtual–environment vcd
       -barhost BackupHost
       -apphost OriginalVMwareClient
       –instance OriginalDatacenter
       –method vCDvStorageImage
       [-session BackupID]
       VirtualMachine [VirtualMachine...]
       [NewOrganization | Directory]

       VirtualMachine
       -vm VMPath [-disk DiskName [-disk Disk...]]

       NewOrganization
       [–neworganization TargetOrganization]
       [[-virtual_datacenter_path | -virtual_datacenter_uuid ]
       TargetVDC]
       [[-vapp_path | -vapp_uuid ] TargetVApp]
       [[-vcenter_path | -vcenter_uuid ] TargetVCenter]
       [[-network_name | -network_uuid ] TargetNetwork]
       [-consolidate] [-memory] [–register][–poweron]
       [–deletebefore | -skip]

       Directory
       -directory RestoreDirectory
       [–overwrite | -skip | –latest]
```

For a description of all the options, see the `omnir` man page or the *HP Data Protector Command Line Interface Reference*.

Note: You should not specify the instanceUUID parameter for restore while restoring the virtual machine backed up from earlier versions.

Important: A backup ID is a point in time. All objects (backup data) created in a backup session have the same backup ID, which is the same as the session ID of the backup session.

Mirrored objects and objects created in an object copy session have the same backup ID as objects created in the original backup session. Suppose the media set created in the original backup session no longer exists, but the media set created in an object copy session still

exists. To restore the objects, you have to specify the session ID of the original backup session (that is, the backup ID) and not the session ID of the object copy session.

The `omnir` syntax does not let you specify from which object copy to restore if several copies of the same object exist. This is only possible using the Data Protector GUI by setting the media allocation priority list.

Note: If the restore fails, see Cleaning up a datastore after a failed restore on page 103.

Example (Restoring virtual machines to a datacenter)

Suppose you want to restore the virtual machine `/vm/machineA` and the individual disks (`scsi0:0` and `scsi0:1`) of the virtual machine `/vm/machineB`. At the time of backup, the virtual machines were running on the ESX Server systems that belonged to the datacenter `/MyDatacenter` managed by the vCenter Server system `vcenter.company.com`. The virtual machines were backed up with the `vStorage Image` backup method.

To restore them to the original location, using the backup session `2011/01/11–1`, and to ensure that the newly restored virtual machines are put online when the session completes, execute:

```
omnir -veagent -virtual–environment vmware -barhost backuphost.company.com -
apphost vcenter.company.com –instance /MyDatacenter -method vStorageImage –
session 2011/1/11-1 –vm /vm/machineA –vm /vm/machineB -disk scsi0:0 –disk
scsi0:1 –memory –poweron
```

Example (Restoring virtual machines to a directory)

Suppose the virtual machines `/MyVirtualMachines/machineA` and `/MyVirtualMachines/machineB` were backed up in the session `2011/02/12-5` from the datacenter `/MyDatacenter` that is managed by the vCenter Server system `vcenter.company.com`, using the `vStorage Image` backup method. To restore the virtual machines outside of the datacenter, to the directory `C:\tmp` on the backup host `backuphost.company.com`, execute:

```
omnir -veagent -virtual–environment vmware -barhost backuphost.company.com -
apphost vcenter.company.com -instance /MyDatacenter -method vStorageImage -
session 2011/2/12-5 -vm /MyVirtualMachines/machineA -vm
/MyVirtualMachines/machineB -directory c:\tmp
```

Example (Restoring object names with instanceUUID in its name)

To support restore of object names with instanceUUID in its name, execute:

```
omnir.exe -veagent -virtual-environment vmware -barhost barHostName -apphost
appHostName -instance instanceName -method vStorageImage -session sessionID -vm
vmPath –instanceUUID vminstanceUUID -register -poweron -deletebefore
```

Recovering virtual machines manually

There are two different scenarios in which you need to recover virtual machines manually after they have been restored with Data Protector:

- If you have restored the virtual machines to a directory on a backup host (**Restore to directory**).

  For details, see Recovering virtual machines after restore to a directory below.

- If you have restored the virtual machines to a datacenter (**Restore to datacenter**) without selecting the restore option Register virtual machines if needed.

  For details, see Recovering virtual machines after restore to a datacenter on page 103.

Recovering virtual machines after restore to a directory

The steps for recovering virtual machines after restore to a directory depend on the format in which the virtual machine configuration file was backed up.

Recovering with the VM configuration file in the VMX format

Suppose the virtual machine `helios` was restored to the directory `C:\tmp\helios` on the backup host using the following backup session:

- Backup method: **vStorage Image**
- Backup type: Incremental
- CBT: Enabled and used

To move the virtual machine files manually to the ESX(i) Server system `dioxide.company.com` managed by the vCenter Server system `bmwvc2.company.com`, using the VMware Converter:

1. Display the contents of the directory `C:\tmp\helios`:

```
helios.vmdk
helios.vmx
helios.vmdk
scsi0-0.cbt
scsi0-0.meta
helios-flat.vmdk
helios.vmx-1
helios.vmdk-1
scsi0-0.cbt-1
scsi0-0.meta-1
helios.vmx-2
```

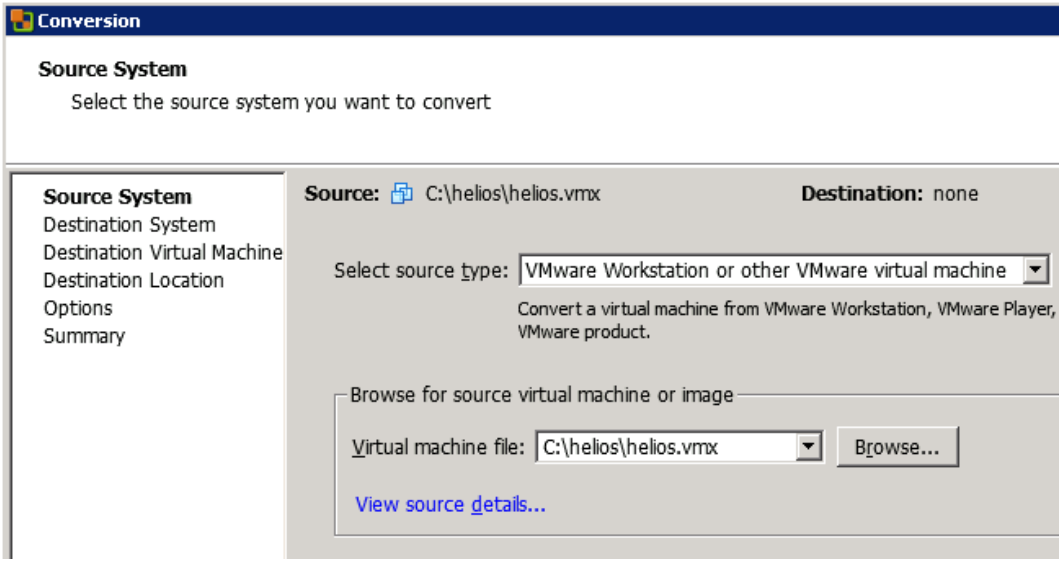
```
helios.vmdk-2
scsi0-0.cbt-2
scsi0-0.meta-2
```

Note that all files backed up in the last full, differential, and the selected incremental session are restored.

2. Share the folder `C:\tmp\helios` so that it can be accessed from the system with the VMware Converter installed.
3. Log in to the system with the VMware Converter installed and open the VMware Converter user interface.
4. Click **Convert Machine** to open the Conversion wizard.
5. In the Source System page, select **VMware Workstation or other VMware virtual machine** for the source type, browse to the `C:\tmp\helios` directory, and select the `helios.vmx` file.

   Click **Next**.

   Figure 41: Conversion (Source System)

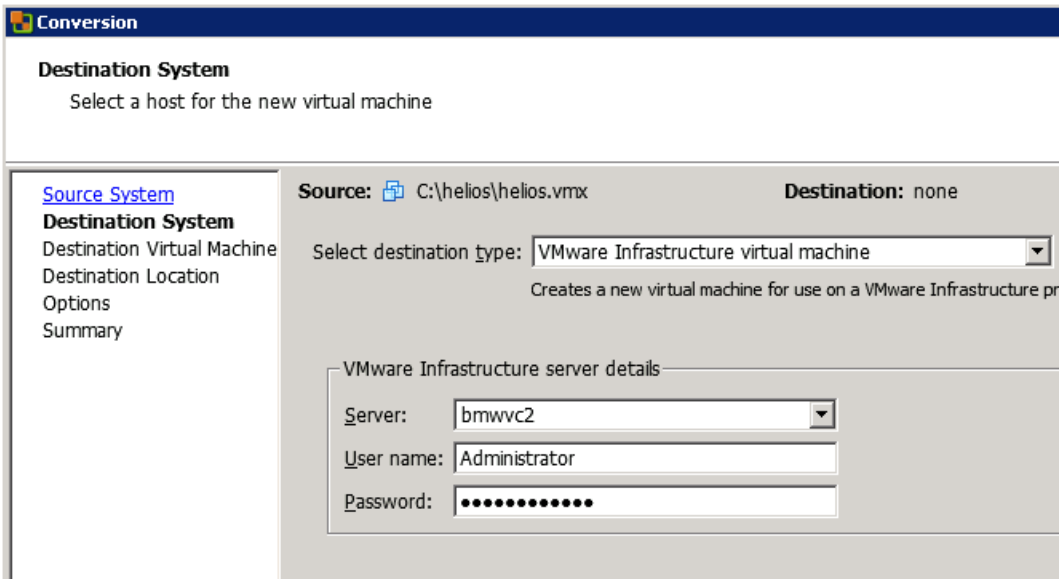


Note: In our example, the VMware Converter is installed on the backup host.

6. In the Destination System page, select **VMware Infrastructure virtual machine** for the destination type and provide the login credentials for the vCenter Server system.

   Click **Next**.

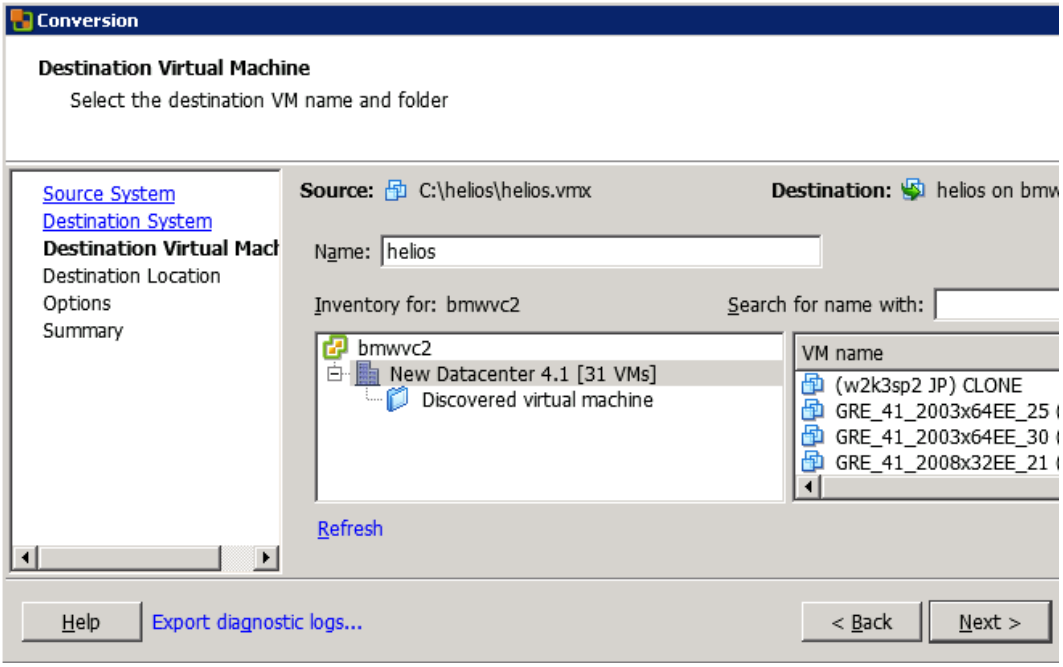
Figure 42: Conversion (Destination System)



7. In the Destination Virtual Machine page, specify the name under which the virtual machine should be recovered.

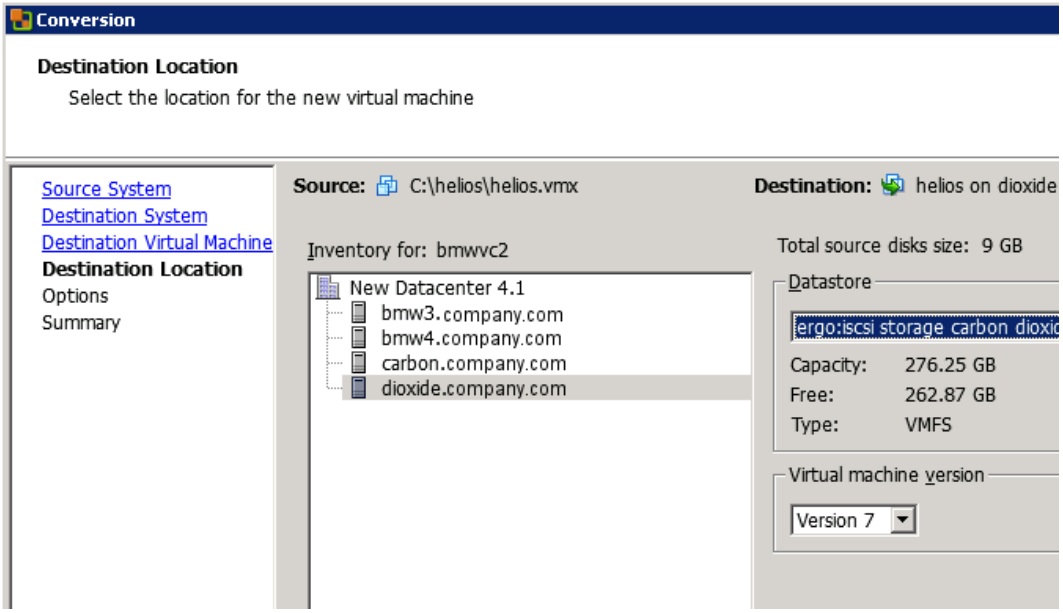
   Click **Next**.

Figure 43: Conversion (Destination Virtual Machine)



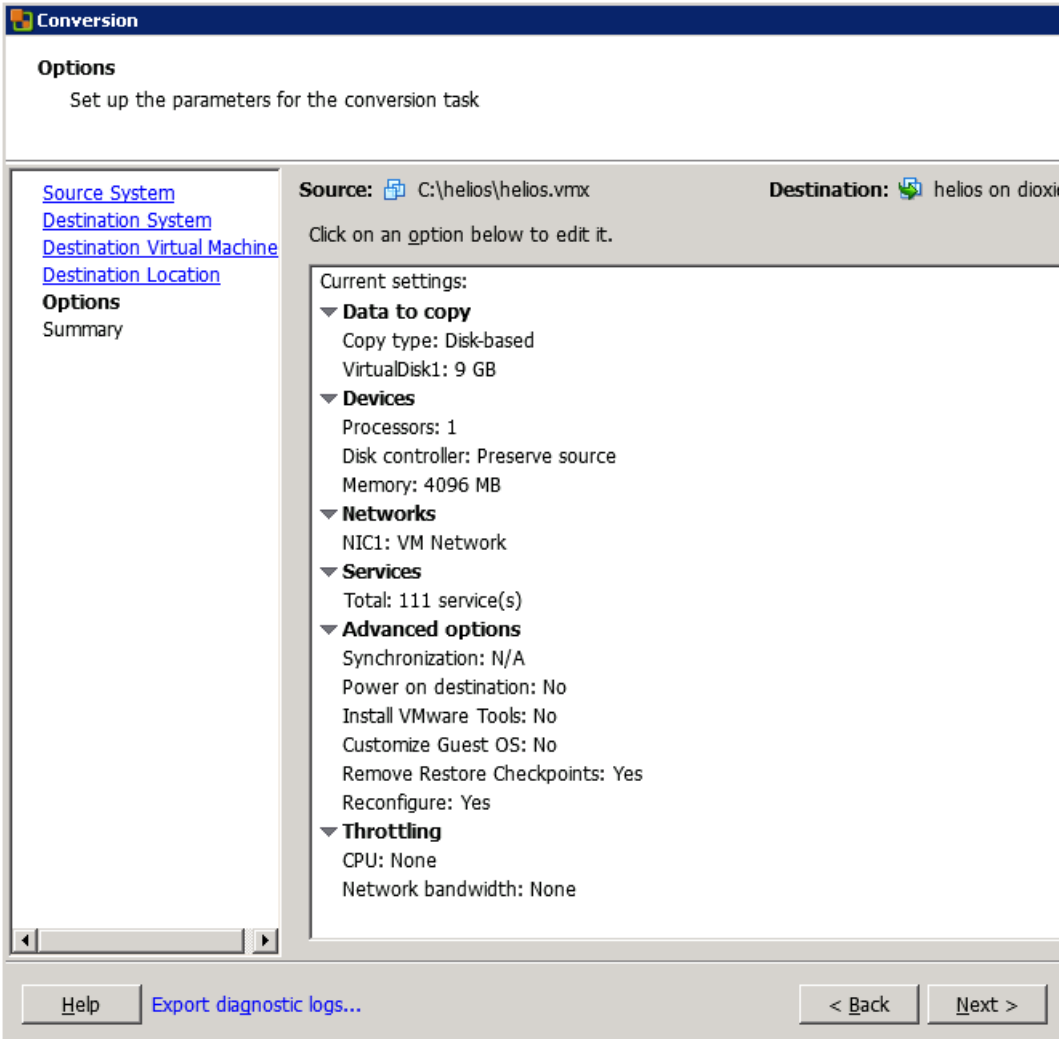
8. In the Destination Location page, select the destination ESX(i) Server system and datastore.

Figure 44: Conversion (Destination Location)



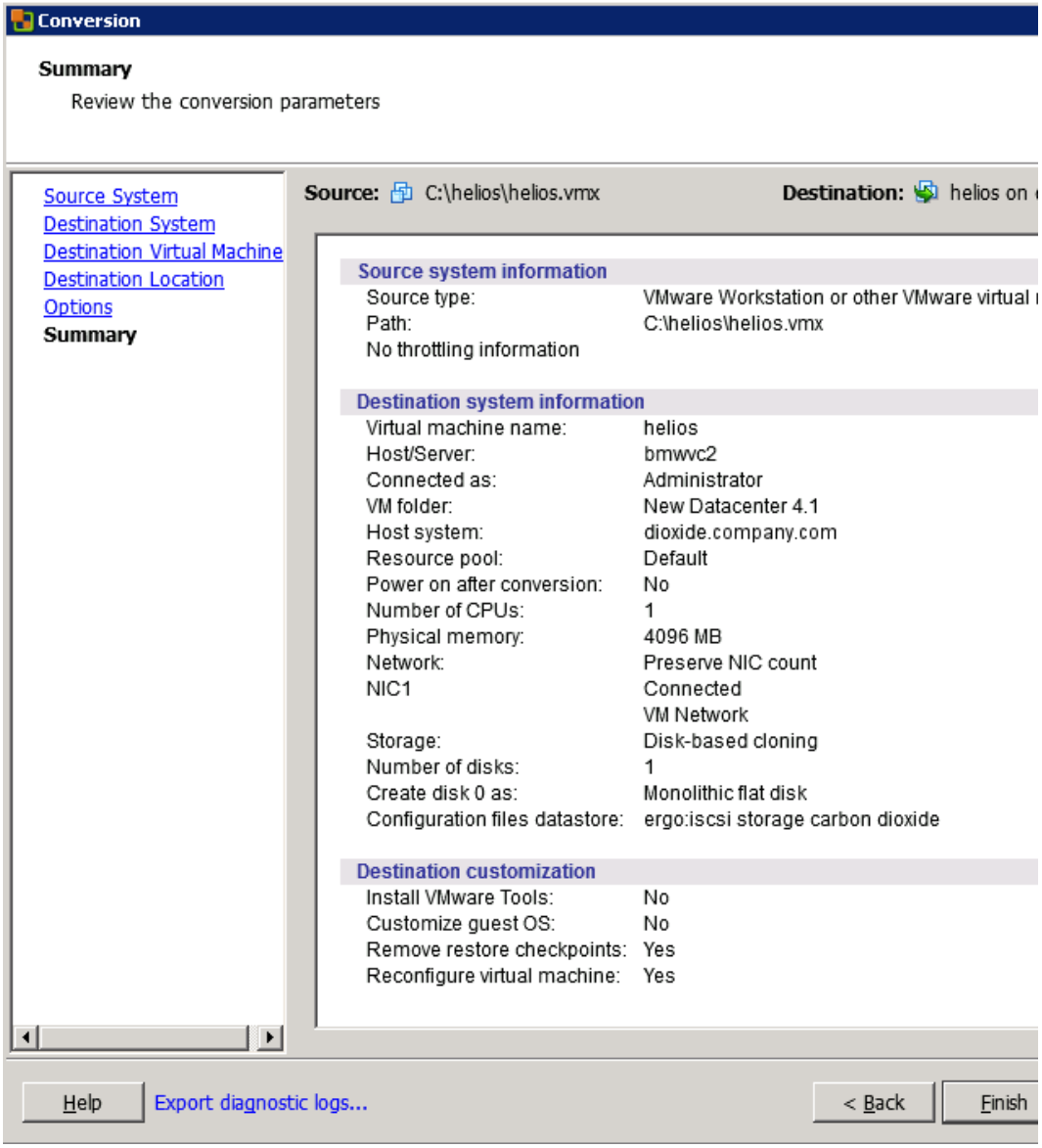
9. In the Options page, edit the options and click **Next**.

Figure 45: Conversion (Options)



10. In the Summary page, review your selection and click **Finish**.

Figure 46: Conversion (Summary)



11. Open the Datastore Browser and upload the files created in the incremental and differential backup sessions to the virtual machine directory:

```
helios.vmx-1
helios.vmdk-1
scsi0-0.cbt-1
scsi0-0.meta-1
helios.vmx-2
helios.vmdk-2
scsi0-0.cbt-2
scsi0-0.meta-2
```

12. Power the virtual machine on.

Recovering with the VM configuration file in the XML format

Follow the procedure:

1. Open vSphere Client and log in to an ESX(i) Server or vCenter Server system.

   If the virtual machine is still configured, remove all its hard disks:

   a. In the inventory object tree, right-click the virtual machine and select **Edit Settings**.

   b. In the Virtual Machine Properties window, in the **Hardware** tab, select each hard disk and click **Remove**.

   c. Click **OK** to confirm the removal.

   If the virtual machine is no longer present, configure a new virtual machine without hard disks, and use the name of the original virtual machine.

   In either case, remember the associated datastore name.

2. Upload the virtual machine files that were created during the backup session:

   a. In the inventory objects tree, select the ESX(i) Server system that hosts the virtual machine.

   b. Click the **Configuration** tab and select **Storage** under Hardware.

   c. Right-click the datastore name and select **Browse Datastore**.

   d. In the Datastore Browser window, in the folder tree, select the virtual machine folder, and click a corresponding icon on the window toolbar. Select **Upload File** or **Upload Folder** as appropriate.

   e. Select all applicable files and complete the upload.

3. Add hard disks to the virtual machine by reusing their backup copies:

   a. In the inventory object tree, right-click the virtual machine and select **Edit Settings**.

   b. In the Virtual Machine Properties window, click **Add**.

   c. In the Add Hardware window, select **Hard Disk** and click **Next**.

   d. Select **Use an existing virtual disk** and click **Next**.

   e. Click **Browse**.

f. In the Browse Datastores window, browse to the appropriate datastore and open the virtual machine folder. Select the virtual disk file and click **OK**.

g. Follow the Add Hardware wizard to complete the process.

h. Repeat the substeps from b to g for each additional hard disk for which a backup copy exists.

4. Power the virtual machine on.

Recovering virtual machines after restore to a datacenter

If you have restored a virtual machine to a datacenter without selecting the option Register virtual machines if needed:

1. Open the Datastore Browser and browse to the restored virtual machine directory.
2. Right-click the virtual machine `*.vmx` file and select **Add to Inventory**.
3. Follow the wizard and click **Finish**.

Recovering virtual machines after restore to an organization

For a detailed procedure on how to recover virtual machine to a vCloud Director organization, see VMware vCloud Director Administrator's Guide.

Restoring using another device

You can restore using a device other than that used for backup. For details, see the *HP Data Protector Help* index: “restore, selecting devices for”.

Cleaning up a datastore after a failed restore

Sometimes, when a virtual machine restore fails, Data Protector creates extra files on the virtual machine datastore. If these files are not deleted, corrupt virtual machine backups may be created in subsequent sessions and, consequently, restore from such a backup also fails.

Suppose the virtual machine `MyVirtualMachine` failed to be restored. To clean up the datastore after the restore:

1. Open the VMware vSphere client.
2. Right-click the virtual machine and select **Delete from disk**.
3. Open the **Datastore Browser**.

   The directory `MyVirtualMachine` should no longer be there.

Check if there are any extra directories:

`MyVirtualMachine_1`

`MyVirtualMachine_2`

and so on.

Right-click each such directory and select **Delete from disk**.

Disaster recovery

Disaster recovery is very complex, involving different products from different vendors. Check the instructions from the guest operating systems and VMware on how to prepare for it.

The following are the main steps needed to recover a virtual machine after a disaster:

1. Reinstall the VMware environment. The configuration should be the same as during the backup.
2. Install Data Protector in the newly configured environment.
3. Restore the service console of the ESX Server system on which the virtual machine was running to the newly configured ESX Server system from a Data Protector filesystem backup.

   For details on what to restore, see the topic “ESX Server Configuration Backup and Restore procedure” at http://kb.vmware.com/selfservice/microsites/microsite.do.

   For details on how to restore from a filesystem backup, see the *HP Data Protector Help*.
4. Restore the original vCenter database (if needed). For details, see the Data Protector integration that was used to back up the database.
5. Restore the virtual machine from a Data Protector Virtual Environment backup as described in this chapter.

Monitoring sessions

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

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

To monitor a session, see the *HP Data Protector Help* index: “viewing currently running sessions”.

Troubleshooting

This section lists general checks and verifications, plus problems you might encounter when using the Data Protector Virtual Environment integration.

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

Before you begin

- Ensure that the latest official Data Protector patches are installed. See the *HP Data Protector Help* index: “patches” on how to verify this.
- See the *HP Data Protector Product Announcements, Software Notes, and References* for general Data Protector limitations, as well as recognized issues and workarounds.
- See http://support.openview.hp.com/selfsolve/manuals for an up-to-date list of supported versions, platforms, and other information.

Checks and verifications

If your configuration, backup, or restore failed:

- Examine system errors reported in the `debug.log` on the backup host.
- Check if you can do a filesystem backup and restore on the problematic client. For information, see the *HP Data Protector Help*.

Additionally, if your backup failed:

- Check the configuration of the vCenter Server or standalone ESX(i) Server system as described in Checking the configuration of VMware clients on page 49.

Problems

Problem

An incremental or differential CBT backup session fails

When performing an incremental or differential backup session with the Use changed block tracking option enabled, the session fails with an error similar to the following:

```
[Critical] From: OB2BAR_VEPA_BAR@droid.company.com "/New Datacenter 4.1"
Time: 2/10/2011 11:14:52 AM
        Virtual Machine 'ddd': Could not gather changed blocks on disk scsi0:0
...
```

The reason may be that you performed a restore session and forgot to run a full backup session to start a new backup chain.

To make sure changed block tracking is working properly, certain requirements need to be met. For details, see

http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd;=displayKC&externalId;=1020128

Action

1. Run a full backup session.
2. Run an incremental or differential backup session.

Problem

After a restore or move to a different folder, backups are not performed correctly

After you have restored or moved a virtual machine to a different folder, the virtual machine is not backed up correctly. For example, instead of an incremental backup, a full backup is performed.

The reason for this is that the datacenter configuration file has been updated. As a result, it contains two virtual machine sections with the same UUID; this is from where the inconsistencies arise.

Action

Re-configure the virtual machine:

1. Open the backup specification.
2. In the Source page, right-click the VMware client and select **Configure Virtual Machines**.
3. Click **OK**.

Problem

A restore session is using LAN instead of SAN

If the backup host used to control a restore session is a virtual machine, Data Protector automatically switches to LAN transportation mode.

Action

To use SAN transportation mode for restore, configure a backup host on a physical system (that is, install the `Virtual Environment Integration` component on a physical system) and select this system as a backup host for the restore session.

For details on transportation modes, see the *VMware Virtual Disk Programming Guide*.

Problem

A restore session using SAN transportation mode fails

A restore session that is using SAN transportation mode fails with a message similar to the following:

```
[Critical] From: OB2BAR_VEAgent@dpi00019.company.com
"/BlrVirtual01_ESX401"  Time: 13-03-2011 12:22:57
Virtual Machine 'Win2k3_x64_dpi00002': Error restoring item
\a1f9f4e3-482d-4b7f-afcb-cb16babe1980\%2FBlrVirtual01_ESX401\vms
\%2FBlrVirtual01_ESX401%2Fhost%2FClus01%2FWin2k3_x64_dpi00002\
images\3\scsi2:15.
```

This may happen if a storage volume that is shared between the backup host and an ESX(i) Server system is read-only.

Action

1. Log in to the backup host and open the command prompt.
2. Execute `diskpart`.

   ```
   C:\Users\Administrator>diskpart

   Microsoft DiskPart version 6.1.7600
   Copyright (C) 1999-2008 Microsoft Corporation.
   On computer: TPC134
   ```

3. Set the SAN policy to `onlineAll`.

   ```
   DISKPART> san policy=onlineAll

   DiskPart successfully changed the SAN policy for the current
   operating system.
   ```

4. Select the disk (storage volume) that should be used for restore.

   ```
   DISKPART> list disk

     Disk ###  Status         Size     Free     Dyn  Gpt
     --------  -------------  -------  -------  ---  ---
     Disk 0    Online          136 GB  1024 KB
     Disk 1    Offline          14 GB    14 GB
     Disk 2    Offline          14 GB    14 GB
     Disk 3    Offline          14 GB    14 GB
     Disk 4    Offline          14 GB    14 GB
     Disk 5    Offline          50 GB    50 GB
     Disk 6    Offline          14 GB    14 GB
     Disk 7    Offline          14 GB    14 GB

   DISKPART> select disk 1
   ```

5. Bring the disk online.

```
DISKPART> online disk

DiskPart successfully onlined the selected disk.
```

6. Ensure the disk is not read-only.

   List the disk properties.

```
DISKPART> detail disk

HP OPEN-V SCSI Disk Device
Disk ID: 00000000
Type   : FIBRE
Status : Online
Path   : 0
Target : 0
LUN ID : 0
Location Path : UNAVAILABLE
Current Read-only State : Yes
Read-only  : Yes
Boot Disk  : No
Pagefile Disk  : No
Hibernation File Disk  : No
Crashdump Disk  : No
Clustered Disk  : No

There are no volumes.
```

   Clear the read-only attribute.

```
DISKPART> attribute disk clear readonly

Disk attributes cleared successfully.
```

   List the disk properties again.

```
DISKPART> detail disk

HP OPEN-V SCSI Disk Device
Disk ID: 00000000
Type   : FIBRE
Status : Online
Path   : 0
Target : 0
LUN ID : 0
Location Path : UNAVAILABLE
Current Read-only State : No
```

```
Read-only  : No
Boot Disk  : No
Pagefile Disk  : No
Hibernation File Disk  : No
Crashdump Disk  : No
Clustered Disk  : No

There are no volumes.
```

Exit the session.

```
DISKPART> exit
```

7. Restart the restore session.

Problem

Slow performance of vepa_util.exe browse command on newer Red Hat Enterprise Linux (RHEL) versions

When executing the `vepa_util.exe browse` command on a newer RHEL version its performance is significantly slower than on other operating systems.

Action

The root cause of the problem is that on newer versions of RHEL systems name service cache daemon is not enabled by default.

Start the name service cache daemon by invoking the following command: `/etc/init.d/nscd start`. To enable automatic daemon start-up during system start-up, execute: `chkconfig nscd on`.

Problem

A restore job fails when restoring virtual machines to ESX(i) hosts managed by vCenter Server 5.x

When restoring a virtual machine to an ESX(i) host, which is managed by a vCenter Server 5.x, the restore job fails and the virtual machine is not restored successfully. Starting with ESX(i) 5.0, VMware has blocked the ability to restore a virtual machine to an ESX(i) which is managed by vCenter.

Action

To resolve this issue, either restore virtual machines through the vCenter Server or restore them through ESX/ESX(i) after unmanaging the host from the vCenter Server.

For more details on how to unmanage an ESX/ESXi host from vCenter Server, see http://kb.vmware.com/kb/2038838

Problem

Restore of a virtual machine using an ESX(i) Server system ends with a corrupted VM guest operating system

In a vSphere environment, when you restore a virtual machine to a `/ha-datacenter` using an ESX (i) 5.0 Server system or later as a restore client, the restore session ends successfully, but the guest operating system on the virtual machine is corrupted.

Action

When selecting the objects for restore, in the **Destination** page, in the **Restore client** drop-down list, select a vCenter Server instead of an ESX(i) Server system.

Problem

Backing up many VMs from VMware vCloud Director at once fails

When backing up many virtual machines (for example, 30) from numerous vApps in the VMware vCloud Director at the same time, the backup session may fail due to a limitation on the number of simultaneously opened HTTP connections to the vCenter Server system.

Action

Reduce the limit of opened parallel connections by setting the omnirc option `OB2_VEAGENT_VCENTER_CONNECTION_LIMIT` to a lower number, for example, to `5`. By default, the option is set to 10.

Problem

Download of memory file bigger than 4GB fails.

If the **Backup memory file** option was set for a memory file of a very large size, then it takes a longer time to process or may also fail.

Action

This can be resolved by increasing the value of the timeout variable `VI_API_TIMEOUT` to a range between 600 and 1500.

Problem

Virtual machine restore: Could not find object on three disks in virtual environment.

While restoring a virtual machine, the object could not be found on the three disks in the virtual environment.

Action

To enable partial restore of a virtual machine that is no longer available on the data store, proceed as follows:

1. Create a temporary virtual machine with the same UUID as the original backup.
2. Restore partial data from backup to the temporary virtual machine.

Problem

Error while creating virtual machine snapshots and object backup fails

An error occurs when creating the snapshots of a virtual machine :

```
[Critical] From: VEPALIB_VMWARE@<HostName> "<AppName>"  Time: <Timestamp>
           Error mounting datastores
[Normal]   From: VEPALIB_VMWARE@BACKUPHOSTNAME  "/DATACENTERNAME"
           Virtual Machine ‘VMNAME’: Creating snapshot ...
[Major]    From: VEPALIB_VMWARE@BACKUPHOSTNAME "/DATACENTERNAME "
           Virtual Machine ‘VMNAME’: Error removing snapshot
[Critical] From: VEPALIB_VMWARE@BACKUPHOSTNAME "/CPD2"  Time: 19/03/2016 8:01:48
           Backup of object failed.
           Name: VMNAME
           Path: / DATACENTERNAME /DATASTORE/ VMNAME
           InstanceUUID: IUUIDOFVM
```

This issue occurs when the virtual machines are located in Site Recovery Manager (SRM).

Action

The create snapshot API is disabled for virtual machines in SRM and therefore, backup operation is not supported.

Part 2: Microsoft Hyper-V

Data Protector offers different ways to back up Microsoft Hyper-V data online. Choose the appropriate backup and restore solution depending on desired functionality.

You can select from among the following solutions:

- ***Data Protector Virtual Environment integration***

  This integration operates on the level of Microsoft Hyper-V virtual machines. The smallest object that you can back up and restore is a Microsoft Hyper-V virtual machine. In one session you can back up virtual machines from multiple Microsoft Hyper-V systems if they are configured in a cluster.

  The main advantage over the Data Protector Microsoft Volume Shadow Copy Service integration is that this integration supports virtual machine migration in a Microsoft Hyper-V cluster, and that it supports the incremental backup type in applicable Microsoft Hyper-V environments.

  For details, see Data Protector Virtual Environment integration on page 115.

- ***Data Protector Microsoft Volume Shadow Copy Service integration***

  This integration operates on the level of Microsoft Volume Shadow Copy Service writers. Since the Microsoft Hyper-V writer is only one of them, Microsoft Hyper-V data does not have the highest visibility. The smallest object that you can back up or restore is a Microsoft Hyper-V virtual machine. In one session, you can back up data from only one Microsoft Hyper-V system. The only supported backup type is full backup.

  For details, see the *HP Data Protector Integration Guide for Microsoft Volume Shadow Copy Service*.

Note: You can also back up Microsoft Hyper-V virtual machines using common Data Protector filesystem backup functionality, which operates on the file level. The smallest object that you can back up or restore this way is a file. To ensure data consistency, you must shut the virtual machines down before starting a backup session.

Table 14: Data Protector backup solutions for Microsoft Hyper-V

Feature	Disk Agent (filesystem backup)	Volume Shadow Copy Service integration	Virtual Environment integration
Online backup		✓	✓
Crash-consistent backup	✓	✓	✓

Feature		Disk Agent (filesystem backup)	Volume Shadow Copy Service integration	Virtual Environment integration
Application-consistent backup			✓	✓
Granularity		File	Virtual machine	Virtual machine
Backup types	Full	✓	✓	✓
	Incremental	✓		✓
	Differential	✓		
Is zero downtime backup (ZDB) supported?		✓	✓	✓
Is instant recovery supported?		✓	✓	
Is virtual machine migration within a Microsoft Hyper-V cluster supported?				✓
Extra licenses needed		• Zero Downtime Backup (optional) • Instant Recovery (optional)	• On-line Extension • Zero Downtime Backup (optional) • Instant Recovery (optional)	• On-line Extension • Zero Downtime Backup (optional)

Chapter 2: Data Protector Virtual Environment integration

Introduction

This chapter explains how to configure and use the Data Protector Virtual Environment integration for Microsoft Hyper-V. It describes concepts and methods you need to understand to back up and restore Microsoft Hyper-V virtual machines.

The integration supports both standalone Microsoft Hyper-V system environments (**standalone environments**) as well as environments in which Microsoft Hyper-V systems are configured in a cluster (**clustered environments**).

The Data Protector Virtual Environment integration for Microsoft Hyper-V is based on the Data Protector Volume Shadow Copy Service integration (**VSS integration**). For details on the VSS concepts, see the *HP Data Protector Integration Guide for Microsoft Volume Shadow Copy Service*.

Backup

During backup, virtual machines can be either powered off (**offline backup**) or actively used (**online backup**).

The following backup method is available:

- Hyper-V Image

For details, see Hyper-V Image backup method on page 124.

As Microsoft Hyper-V and VSS are involved, you should specify the following backup types for each backup session:

- **Microsoft Hyper-V backup type**

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

  - Full
  - Incremental

- **VSS backup type**

  The supported VSS backup types are:

  - Local backup
  - Transportable backup

For details on the backup types, see Backup types on page 125.

Restore

You can restore Microsoft Hyper-V virtual machines:

- **To the default (original) location**

  Using this option, you can restore virtual machines to the original location on the original or a different Microsoft Hyper-V system.

- **To a different location**

  Using this option, you can restore virtual machines to a different location on the original or a different Microsoft Hyper-V system.

- **To a directory**

  Using this option, you can restore virtual machine files to a directory on any client with the Data Protector `Virtual Environment Integration` and `MS Volume Shadow Copy Integration` components installed. After such a restore you need to import virtual machines to a Microsoft Hyper-V system for virtual machines to become functional again.

The Data Protector Virtual Environment integration does not support instant recovery.

This chapter provides information specific to the Data Protector Virtual Environment integration for Microsoft Hyper-V. For limitations, see the *HP Data Protector Product Announcements, Software Notes, and References*. For general Data Protector procedures and options, see the *HP Data Protector Help*.

Integration concepts

Supported environments

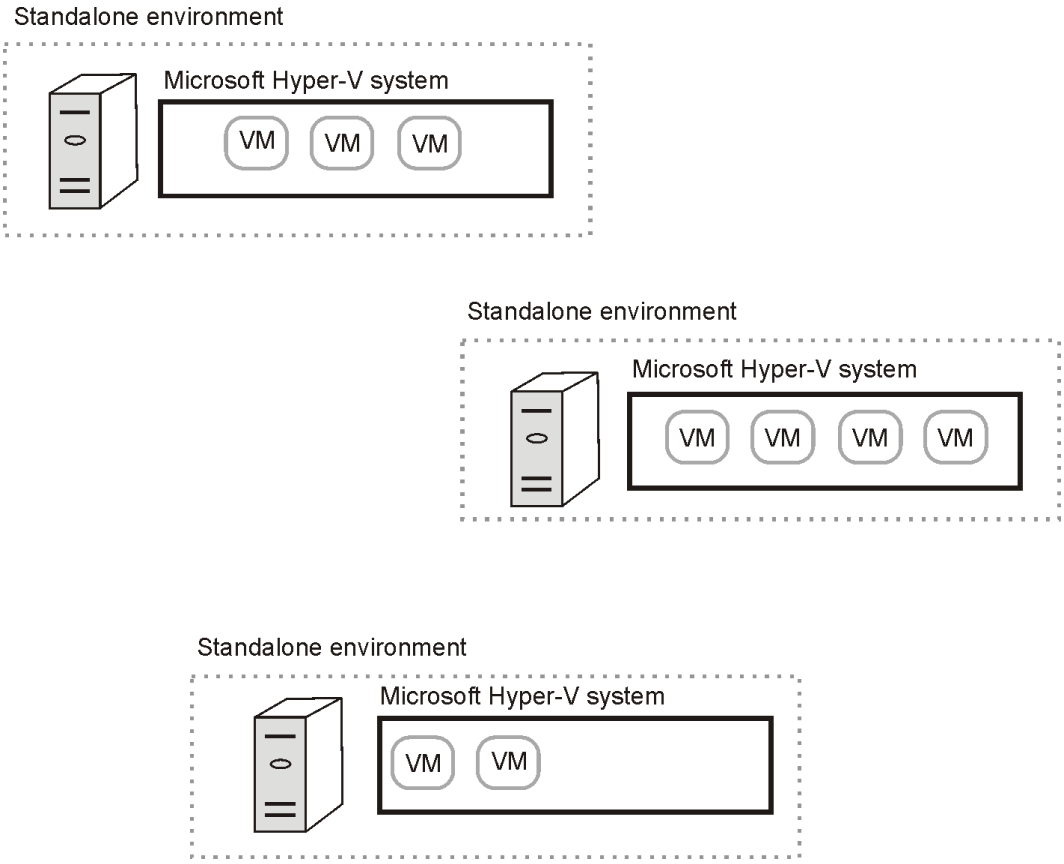
Data Protector supports both standalone and clustered Microsoft Hyper-V environments.

Standalone environments

In a standalone Microsoft Hyper-V environment, the Cell Manager communicates a backup request to the backup host, which then sends the request to the corresponding standalone Microsoft Hyper-V system. A **backup host** is a system in the Data Protector cell that has the Data Protector `Virtual Environment Integration` and `MS Volume Shadow Copy Integration` components installed and controls the process of backing up Microsoft Hyper-V virtual machines.

In a single session, virtual machines that reside on the same Microsoft Hyper-V system can be selected for backup. Where the data is actually backed up from depends on configuration of the Microsoft Hyper-V virtual machine replication and options selected in your Data Protector backup specification.

Figure 47: Hyper-V standalone environments



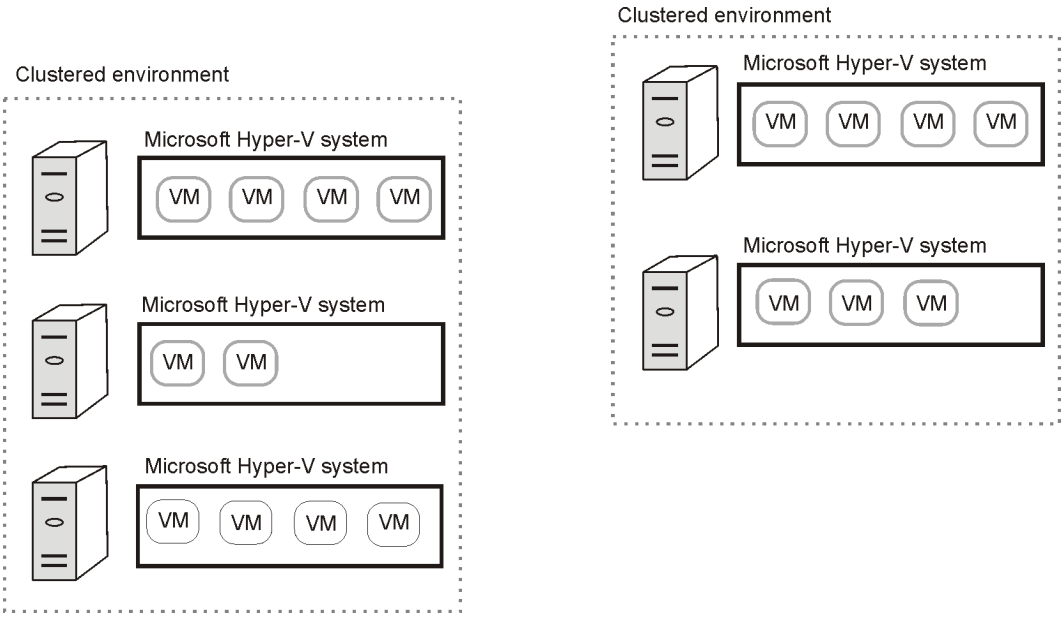
For standalone Microsoft Hyper-V systems, it is only possible to migrate a virtual machine by manually exporting it from one Microsoft Hyper-V system and then importing it into another.

Clustered environments

In a clustered Microsoft Hyper-V environment, the Cell Manager communicates a backup request to the backup host, which then sends the request to the Microsoft Hyper-V system on which the virtual machine to be backed up resides.

In a single session, virtual machines that reside in the same Microsoft Hyper-V cluster can be selected for backup. Where the data is actually backed up from depends on configuration of the Microsoft Hyper-V virtual machine replication and options selected in your Data Protector backup specification.

Figure 48: Hyper-V clustered environments



Example

The following figures illustrate an environment consisting of non-cluster and cluster VMs. The figures show how the VMs are presented in Windows Server Manager and in the Data Protector backup specification.

Figure 49: Windows Server Manager — Cluster VMs

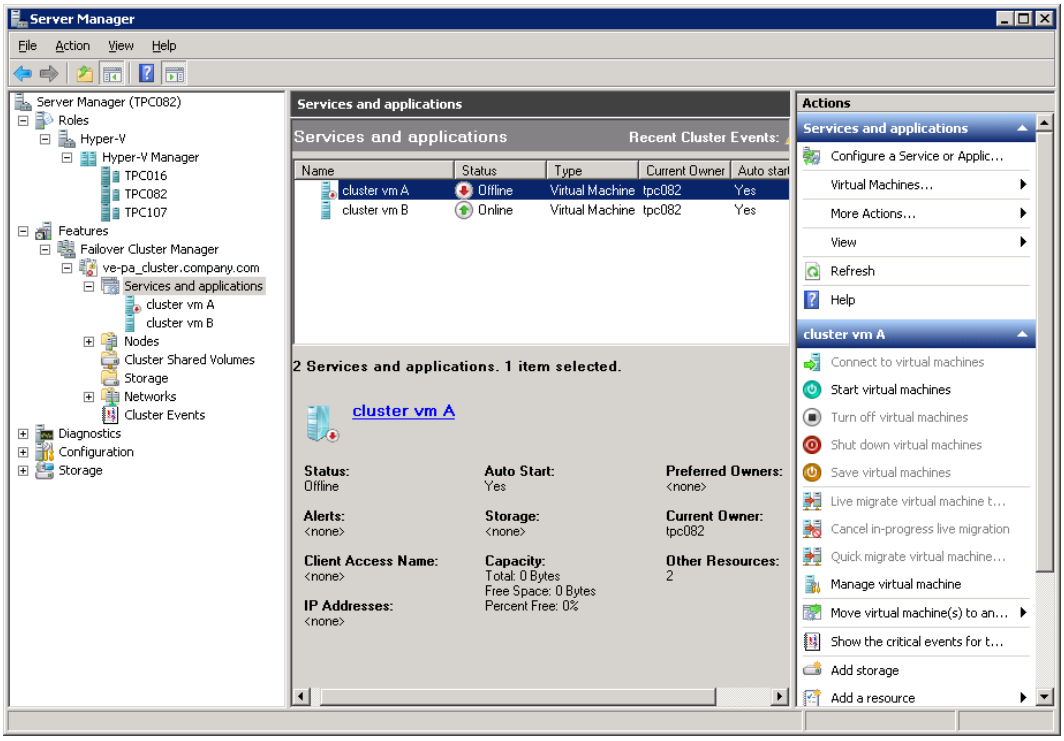


Figure 50: Windows Server Manager — VMs running on TPC082

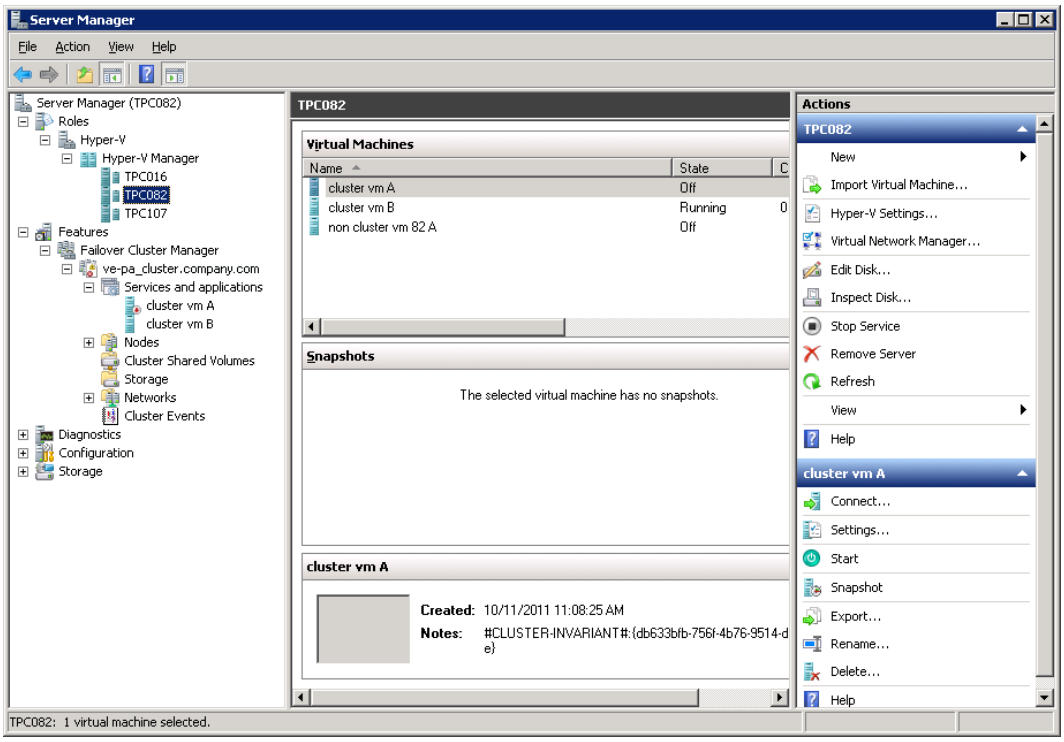
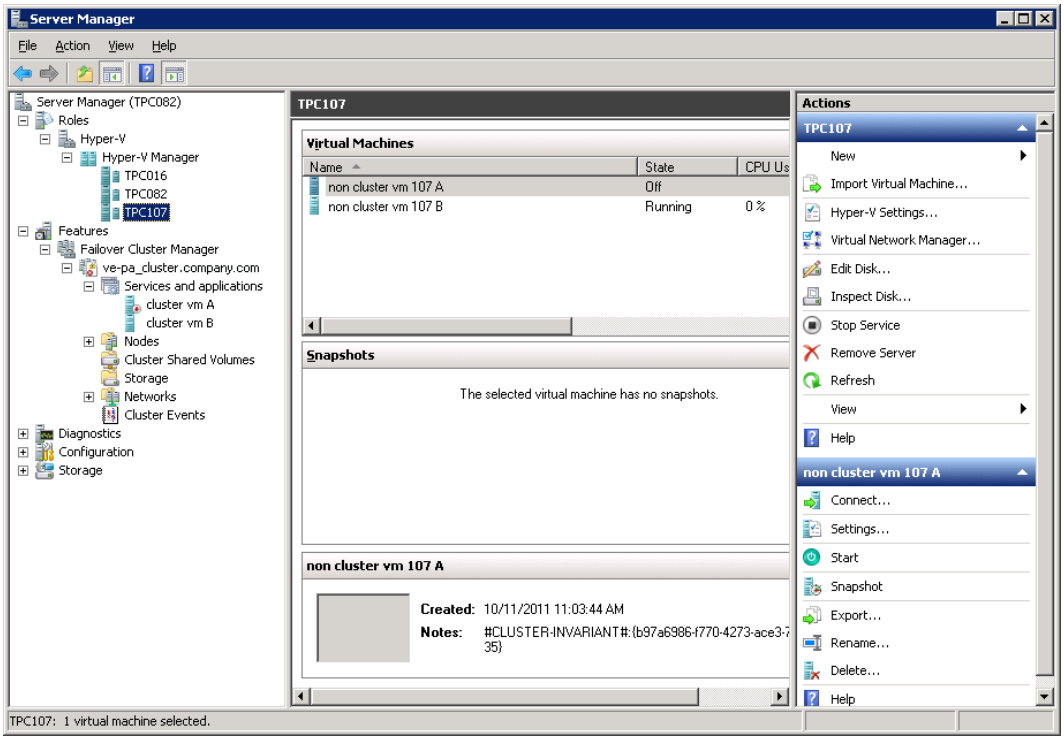
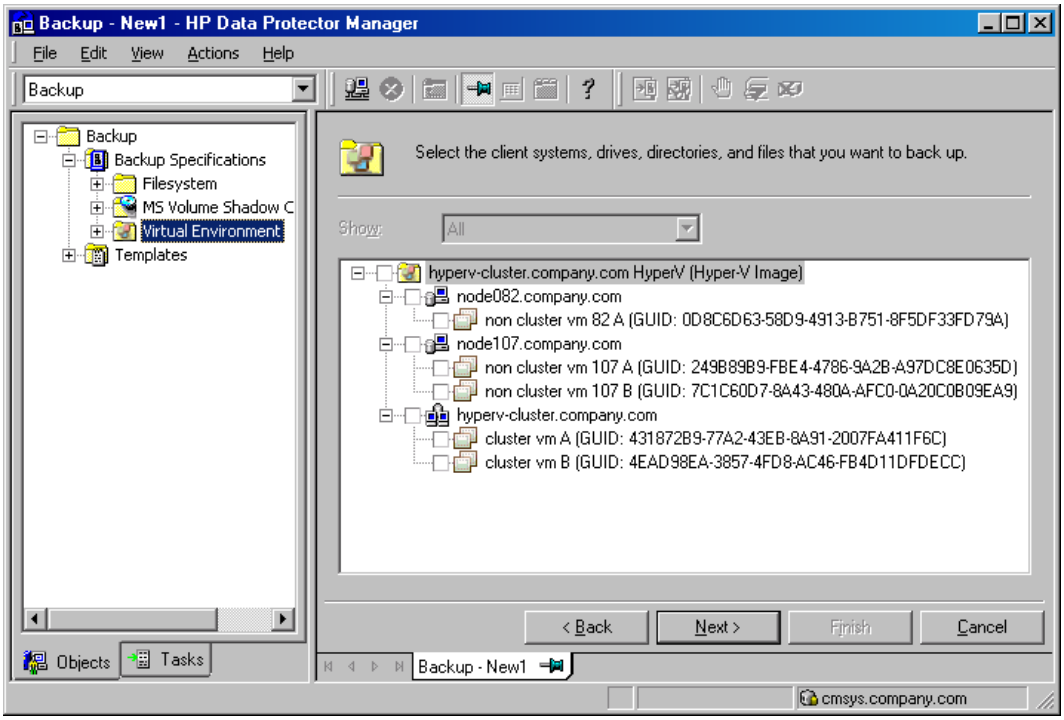


Figure 51: Windows Server Manager — VMs running on TPC107



In the Data Protector backup specification, both non-cluster VMs and cluster VMs are displayed for all nodes of the cluster; non-cluster VMs are listed under their physical nodes and cluster VMs under their virtual system. See Data Protector backup specification below.

Figure 52: Data Protector backup specification

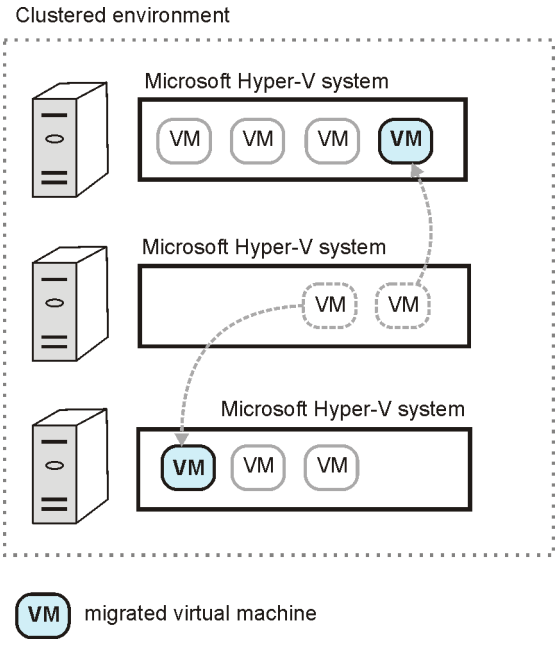


Migration of virtual machines

The Data Protector Virtual Environment integration supports migration of virtual machines between Microsoft Hyper-V systems within a clustered environment. After a virtual machine migration in such a cluster, you do not need to change the backup specification; Data Protector will find out where the virtual machine to be backed up has migrated, using the Microsoft Hyper-V WMI services, and back it up.

If the failover occurs during a backup or restore session, the session fails and has to be restarted. Similarly, if a virtual machine is in a live migration process when Data Protector attempts to back it up, the session fails.

Figure 53: Migration of virtual machines



Cluster Shared Volumes

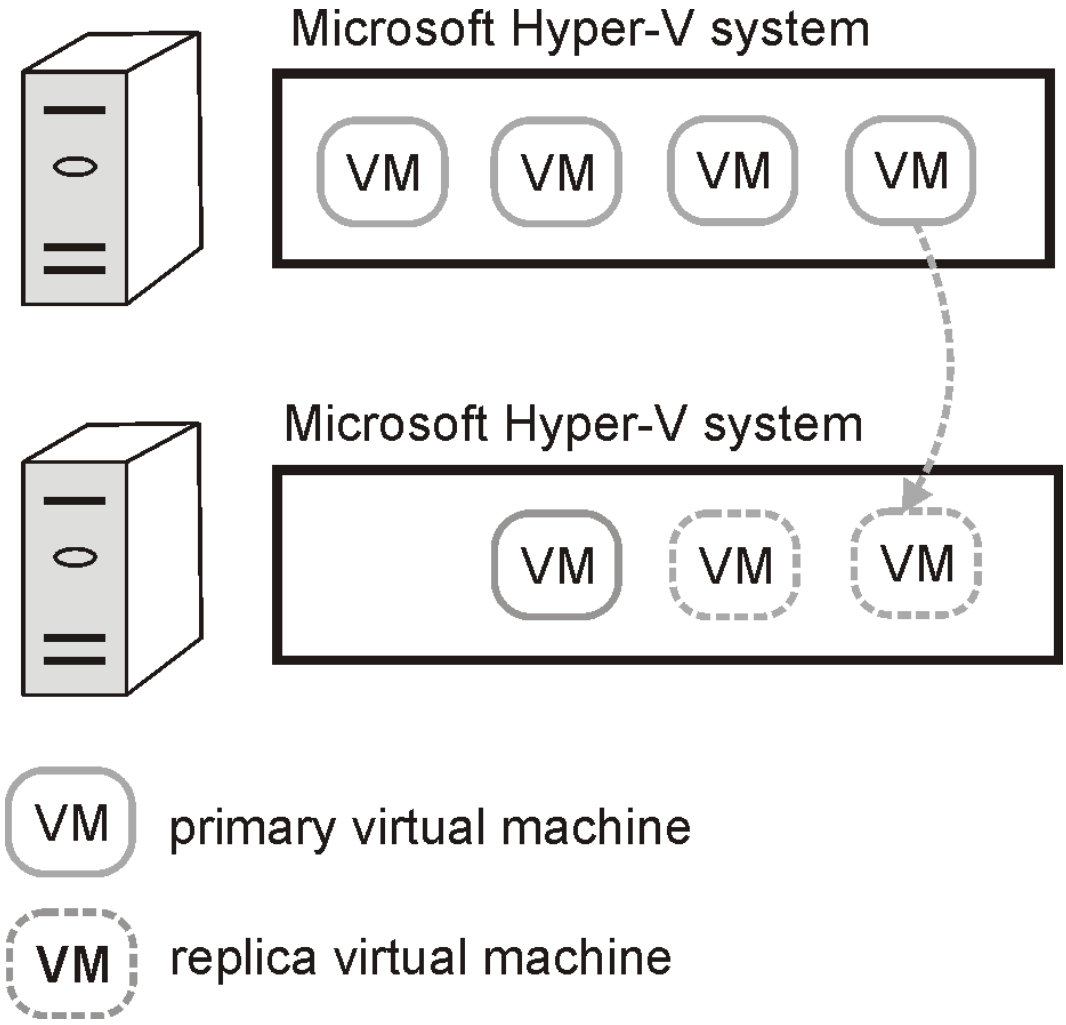
Data Protector supports Microsoft Hyper-V environments that use the Cluster Shared Volumes (CSV) feature of failover clustering. In clusters using CSV, multiple virtual machines can be configured to use the same LUN (disk) while still being able to move from one Microsoft Hyper-V system to another independently of each other.

Hyper-V Replica

In a replication configuration, a virtual machine (the **primary VM**) is replicated to another Hyper-V server (replica server). If the primary VM gets corrupted, the replication can fail over and the virtual machine replica (**replica VM**) becomes the primary VM.

The replica VM is a snapshot of the primary VM at a given time and can be kept for backup purposes or backed up instead of the primary VM to reduce the load on the host system. The primary VM and replica VM cannot use a common shared volume even if the primary VM resides in a cluster.

Figure 54: Virtual machine replication



Virtual machines on Windows file shares

Data Protector supports VMs on a Windows Server 2012 Hyper-V system, which store their data on a Windows Server 2012 file share (SMB 3.0).

Data Protector installation components

Data Protector Cell Manager

The Data Protector Cell Manager can be installed on a Microsoft Hyper-V virtual machine or a separate system outside the virtualization environment.

Data Protector Virtual Environment Integration component

The Data Protector `Virtual Environment Integration` component should be installed on at least one client in a Data Protector Cell. This client becomes a backup host.

The `Virtual Environment Integration` component includes the following major parts:

- `vepa_bar.exe`, used during backup and restore operations on virtual environments.
- `vepa_util.exe`, used during browsing and query operations on virtual environments.
- `vepalib_hyperv`, a dynamic link library providing Hyper-V specific functionality for backup, restore, query and browsing tasks.

Data Protector Disk Agent component

The Data Protector `Disk Agent` component must be installed on the backup host if you want to use the Browse button. This button is used to select a restore directory on a backup host.

Data Protector MS Volume Shadow Copy Integration component

The Data Protector `MS Volume Shadow Copy Integration` component must be installed on all Microsoft Hyper-V systems that you plan to back up virtual machines from or restore them to. If Microsoft Hyper-V systems are configured in a cluster, it must be installed on all cluster nodes. For VSS transportable backups, the component must also be installed on the backup system. In addition, the component must also be installed on the backup host.

Note: The terms backup system and backup host do not refer to the same entity. A backup host is a system that has the Data Protector `Virtual Environment Integration` component installed, and therefore controls a backup session, while a backup system is only used in VSS transportable backup sessions; it imports shadow copies from the disk array, provides access to them, and so enables data transfer to backup media.

Data Protector Media Agent component

The Data Protector `General Media Agent` component must be installed on the Data Protector client to which your backup device is connected. This can be any of the Microsoft Hyper-V systems, or a separate system outside the Microsoft Hyper-V virtualization environment.

Backup concepts

The Data Protector Virtual Environment integration for Hyper-V is based on the Data Protector Microsoft Volume Shadow Copy Service Integration. By providing its Virtual Environment integration, Data Protector allows you to back up and restore virtual machines without knowing the principles of the Microsoft VSS framework.

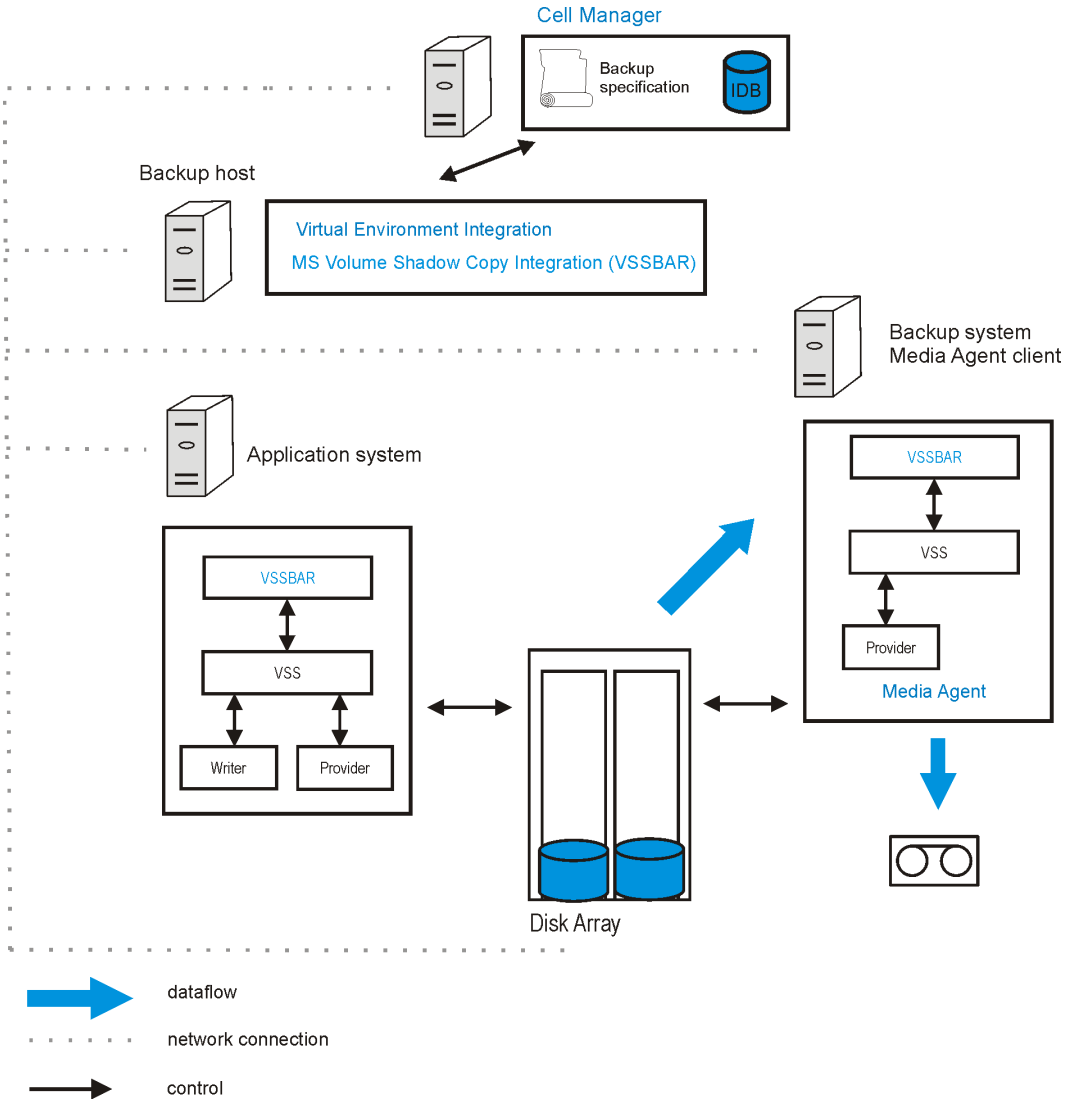
Hyper-V Image backup method

The Hyper-V Image backup method enables you to select Microsoft Hyper-V virtual machines as Data Protector backup objects. A Hyper-V Image backup session progresses as follows:

1. The Cell Manager establishes a connection with a backup host to send a backup request, and starts the virtual environment integration agent (`vepa_bar.exe`) on the backup host.
2. Using a custom dynamic link library (`dpvssapi.dll`, which is part of the `MS Volume Shadow Copy Integration` component installed on the backup host), `vepa_bar.exe` starts `vss_bar.exe` on the application system.
3. The `vss_bar.exe` agent on the application system, in turn, sends a request to the volume shadow copy service for a volume shadow copy creation. In case of a VSS transportable backup, `vss_bar.exe` also starts `vss_bar.exe` on the backup system.
4. When the volume shadow copy has been created, `vss_bar.exe` passes the volume shadow copy data to the Media Agent client, which transfers the data to backup media.
5. `vss_bar.exe` informs `vepa_bar.exe` that the backup has completed.

Note: You can use the omnirc option `OB2VEPA_HYPERV_TIMEOUT` to specify how long the `vepa_bar.exe` should wait for `vss_bar.exe` to send the “backup completed” message. By default, there is no time limit (the option is set to `INFINITE`).

Figure 55: Hyper-V Image backup method (VSS transportable backup)



In Hyper-V Image backup method (VSS transportable backup) above, the backup system is also a Media Agent client. It therefore has the `General Media Agent` component installed and a device connected to it.

For more information, see the *HP Data Protector Integration Guide for Microsoft Volume Shadow Copy Service*, chapter *Integration concepts*.

Backup types

As both Microsoft Hyper-V and VSS are involved, you must specify the following backup types for each backup session:

- Microsoft Hyper-V backup type
- VSS backup type

The type of backup to be performed is specified at a backup specification level.

Microsoft Hyper-V backup types

You can select from the following Microsoft Hyper-V backup types:

- Full (**Full**)

  A virtual machine is backed up in its entirety, including its complete virtual disks.

- Incremental (**Incr**)

  A virtual machine snapshot is first created by Microsoft Hyper-V and then backed up by Data Protector. Only changes made since the last backup of a virtual machine are included in the Data Protector backup image.

  Under specific circumstances, the incremental backup session falls back and Data Protector performs a full backup instead. Replicated virtual machines cannot be backed up incrementally. For more information, see Backup considerations on page 128.

VSS backup types

You can select from the following VSS backup types:

- Local backup (**Local or network backup**)

  This type is used for a single-host VSS configuration. The backup is done on the same Microsoft Hyper-V system on which the VSS shadow copy is created. This can be a Data Protector zero downtime backup (using a VSS hardware provider) or standard Data Protector backup (using the software provider).

  Note: In a Microsoft Hyper-V cluster environment, a local backup using the VSS hardware provider is not supported. This is a Microsoft product limitation.

- Transportable backup (**VSS transportable backup**)

  This type is used for a dual-host VSS configuration. It creates VSS shadow copies on the application system (Microsoft Hyper-V system) and presents them to the backup system, from where the backup to backup media can be performed. A VSS hardware provider is required for this type of backup.

  Note: In a Microsoft Hyper-V cluster environment, the backup host cannot be a virtual machine running on one of the Microsoft Hyper-V systems. This is a Microsoft product limitation.

For details, see the *HP Data Protector Integration Guide for Microsoft Volume Shadow Copy Service*.

Quiescence

For Windows virtual machines whose guest operating system is up and running at the time of backup, Data Protector uses the VSS framework to freeze, or quiesce, the states of the applications running within a virtual machine before it is backed up. This ensures data consistency for the programs concerned (an application-consistent backup is created).

Note: For quiescence to function properly, ensure that the Microsoft Hyper-V integration services are installed on all Microsoft Windows VMs.

If the guest operating system is not a Windows operating system or if the Microsoft Hyper-V integration services are not installed, quiescence is not possible. Such virtual machines are suspended at the time of backup.

Quiescence backup flow

1. The Microsoft Hyper-V writer triggers the integration services within the virtual machine.
2. The integration services trigger the VSS framework within the virtual machine to create a volume shadow copy (an *inner volume shadow copy* is created).
3. The VSS framework within the Microsoft Hyper-V system creates a volume shadow copy of the disk on which the virtual machine files are located (an *outer volume shadow copy* is created). In a ZDB use case, a replica storage volume is created.
4. The Microsoft Hyper-V writer performs auto-recovery to make the inner and outer volume shadow copies consistent before proceeding with the backup, as there is a time gap between the inner and outer volume shadow copy creation and some data stored on the virtual machine may change in the meantime.

Restore chain protection

In Microsoft Hyper-V environments, to prevent data loss during restore, the Data Protector Virtual Environment integration protects the restore chain during incremental backup sessions. For example, whenever a backup snapshot of a virtual machine is created or removed outside Data Protector, or a backup session is removed from the Data Protector Internal Database, the integration detects such a change at the beginning of a subsequent incremental backup session. As a result, Data Protector automatically switches the backup type in the affected session to full. Depending on your Microsoft Hyper-V environment, the fallback extent is an entire Microsoft Hyper-V system or cluster, meaning that the backup type is switched for all virtual machines participating in the session.

You can disable restore chain protection by setting the omnirc option `OB2_VEAGENT_DISABLE_RESTORE_CHAIN_PROTECTION` to the value `1`. See also Customizing the Data Protector behavior with omnirc options on page 142.

Backup considerations

- Using the Data Protector Virtual Environment integration, you cannot back up Microsoft Hyper-V system configuration data.
- Due to the architectural foundation of the Data Protector Virtual Environment integration, consider the Microsoft Hyper-V writer specifics described in the *HP Data Protector Integration Guide for Microsoft Volume Shadow Copy Service*.

Virtual machine storage

- Due to a Microsoft Hyper-V VSS writer limitation, the following cannot be backed up:
  - Data residing on physical disks that are attached directly to virtual machines.
  - Data residing on storage that is accessed directly by virtual machines using iSCSI initiators.

  For details, search for the terms “Hyper-V, Planning for Backup” in the Microsoft TechNet Library.
- **Windows Server 2012 systems:** On this operating system, the following cannot be backed up:
  - Data residing on storage that is directly accessed by a virtual fibre channel HBA

Concurrent sessions

- Backup sessions that use the same devices cannot run concurrently. If multiple sessions are started concurrently, one session waits for the other to complete.

Cluster Shared Volumes (CSV)

- Backup sessions that try to back up virtual machines from the same CSV cannot run in parallel. If two sessions are started, the second one fails.

  Windows Server 2012 systems: Virtual machines that are not on a CSV must be backed up in separate sessions, otherwise the session fails. If any part of the virtual machine, such as configuration or snapshot files are outside the CSV, the session will fail.

Virtual machines on SMB file shares

Data Protector supports backup of VMs that are located on Windows filesystem shares (SMB 3.0). The following prerequisites must be met:

- The Windows role `File Server VSS Agent Service` must be installed and enabled on the Windows file server.

To check if the service is enabled, open a PowerShell window and execute:

```
Get-WindowsOptionalFeature -Online -FeatureName FileServerVSSAgent
```

To enable the service, execute:

```
Enable-WindowsOptionalFeature -Online -FeatureName FileServerVSSAgent
```

Alternatively, open the Server Manager and use the Add Roles and Features wizard to check the status of the role and, if necessary, enable the File Server VSS Agent Service.

- Add constrained delegation for all Hyper-V nodes that are using the SMB file share:

  In Active Directory Users and Computers, select the domain and select **Computers** to list all systems. Right-click the selected Hyper-V node and select **Properties**. In the Properties dialog, select **Delegation** and add the `cifs` service to the list of trusted services.

- The SMB file share must be prepared and configured to host Hyper-V VMs:

  - The VM must be configured and running on an SMB 3.0 file share. Earlier versions of SMB file shares are not supported.

  - Make sure that computer accounts of all Hyper-V hosts, the SYSTEM account, and all Hyper-V administrators managing the virtual machines have Full Control access to the share. Additionally, make sure that all computer accounts of Hyper-V cluster virtual names have Full Control access to the share.

    To avoid manually adding permissions for each additional Hyper-V host or Hyper-V administrator, you can add the Hyper-V hosts and the Hyper-V administrators to a domain security group and grant Full Control permissions to this group instead to single user accounts. You need to create such a domain security group and add all computer accounts and user accounts to this group before you configure the share. When you add permissions to the share, you now only need to add Full Control permission for this security group instead of all single accounts.

  - When you create an SMB file share in a cluster environment, you need to perform the following additional steps:

    - Create a File Server cluster role. Depending on the file server type you select, create the share either within your CSVs in the path `C:\ClusterStorage` (for the `Scale-out File Server for application data` file server type) or on a cluster disk (for the `File Server for general use` file server type).

    - If dynamic DNS registrations do not work in your environment, manually register the IP addresses of all cluster nodes for the Distributed Server Name with your DNS Server using the Server Manager.

- When you back up online VMs, single VMs which contain data on an SMB file share and the

virtual disks on a local volume, are not backed up. For example, if your backup specification contains two VMs, and VM1 has data on an SMB file share and the virtual disk on a local volume, while VM2 is located completely on an SMB file share, only VM2 is backed up.

If multiple VMs that reside on a mixed location (each of them is only at one location) are backed up, then the backup of the entire host is aborted. Create separate backup specifications to back up such a configuration. For example, if your backup specification contains three VMs, and VM1 has data on a local volume, VM2 on a CSV, and VM3 on an SMB file share and all VMs reside on the same system, then the entire system is not backed up.

If the backup specification contains both, VMs with data on several locations and VMs with data only at one location, the VMs that have data on another location are skipped first. If the remaining VMs are on the same location, the host is backed up. If not, the backup is aborted.

You can deactivate the check for mixed location by setting the omnirc variable `OB2_VEAGENT_ENABLE_SMB_MIX_LOCATIONS` to `1`. However, note that although all the VMs are backed up, the complete backup on a given Hyper-V host will fail if there is one online backup performed.

- VMs on SMB file shares using Distributed File System Namespaces (DFSN) or Distributed File System Replication (DFSR) are not supported.
- If a system is both, a Hyper-V server and a File Server, the VM cannot have data on an SMB file share on the same system.

Incremental backup

- Each Microsoft Hyper-V virtual machine needs to be prepared for incremental backup in advance, before the first incremental backup session is run for it. You can prepare a virtual machine (enable its incremental backup) in two ways:
  - By running a full backup session for it, where the Enable incremental backup of VM(s) option in the related backup specification is selected
  - By running a full backup session for it, after you have executed the `vepa_util.exe command --enable-incremental` command for it; for details, see the *HP Data Protector Command Line Interface Reference* or the `vepa_util.exe` man page
- An incremental backup session falls back and Data Protector performs a full backup instead under any of the following conditions:
  - A virtual machine is not prepared for incremental backup
  - Replication to another Microsoft Hyper-V system is configured for a virtual machine selected for backup
  - The reference to a previously created backup image of a virtual machine no longer exists in the Data Protector Internal Database
  - The most recent backup snapshot of a virtual machine was not created by Data Protector

- Your backup specification is configured for virtual machine replicas
- Operating system on your Microsoft Hyper-V system or cluster does not support incremental snapshots of virtual machines; for information if your Microsoft Windows operating systems supports this feature, see the operating system documentation

Note: Depending on your Microsoft Hyper-V environment, the fallback extent is an entire Microsoft Hyper-V system or cluster. If the fallback occurs, the backup type used in the current session changes for all participating virtual machines.

Virtual machine replicas

- **Consistency of virtual machine backup images**

  Replica VMs are periodic snapshots of a virtual machine. If you restore a replica VM, the restored VM is only in a crash-consistent state.

  Additionally, you can configure the VM replication process to create recovery points and store them. However, these recovery snapshots are also only crash-consistent. To create application-consistent snapshots, enable the replication of incremental VSS copies.

  When backing up a replica VM, Data Protector backs up the current snapshot and all stored recovery points. To make sure that each Data Protector backup contains an application-consistent recovery point, select a shorter or equal interval for the incremental VSS replication than for the Data Protector backup. For example, select the VSS incremental replication to be performed every hour and four recovery points must be retained. Schedule the Data Protector backup on every fourth hour.

- **Backing up during the initial VM replication**

  Do not back up VMs during the initial VM replication. When backing up the primary VM, the backup session may fail. When backing up the replica VM, the session will also fail. However, if you select the replica VM and use the option **Back up selected VM(s)**, the session will finish without errors but back up only data which was replicated until that time.

- **Backup duration and replication intervals**

  During the backup session, the virtual machine configuration is locked and as a result, the VM replication fails. The Hyper-V service attempts to synchronize the replica for a specified time. If it does not succeed, the Hyper-V service stops attempts to automatically resynchronize. You must re-enable replication after the backup session finishes.

  Make sure that the backup session finishes in the specified time or change the time interval in which Hyper-V is allowed to automatically resynchronize the replicated VMs. See After a backup session, the VM replication state is “Error” and health is “Critical” on page 165.

- **VM replication state and health**

- If the replication connection does not function, a backup of the replica VM fails. To avoid this issue, select the option to use the primary replica if the connection does not work. See Application-specific backup options on page 147.
- After a VM failover, the replication state and health are `Error` and `FailedOverWaitingCompletion`, therefore the new replica VM is not used for backup.

  After the replication is reversed, the VM replication state and health is `Replicating` and `Normal` but the information provided by Hyper-V is updated only after the next successful VM replication and backup sessions can resume only afterwards.

Virtual machine migration

- ***Windows Server 2012 systems:*** During a migration, virtual machines are locked and cannot be backed up, and the other way round.

ZDB environments

- If your virtual machine files are located on a disk array and you intend to perform ZDB sessions in which the replica storage volumes are kept after the backup session completes, create backup specifications in such a way, that you select all virtual machines that reside on the same storage volume in the same backup specification. Otherwise, the replica storage volumes created in a ZDB session also contain the backups of the virtual machines that were not selected, but these backups are not application-consistent as these virtual machines were not quiesced before the replica storage volumes were created; such virtual machine backups are only crash-consistent. If you perform a ZDB-to-tape session, only the virtual machines that were selected are backed up to backup media.
- **HP P4000 SAN Solutions:** Due to a VSS hardware provider limitation, virtual machines whose files reside on an HP P4000 SAN Solutions disk array cannot be backed up while being online.

  There are two workarounds:

  - Use the software provider to back up the virtual machines while they are online (standard backup).
  - Back up the virtual machines when they are offline (zero downtime backup).

Object copy considerations

- To properly use the Data Protector object copy feature with Microsoft Hyper-V virtual machine snapshots, you need to copy all Data Protector backup objects created with the Hyper-V Image backup method in the same session. Ensure you select an entire backup session when selecting Data Protector Microsoft Hyper-V objects for interactive, post-backup, or scheduled copy sessions.

To indicate this guideline, the Data Protector GUI does not list Microsoft Hyper-V backup objects in the Copy > Object copy > Interactive > Objects scope of the Object Operations context.

Restore concepts

You can restore complete virtual machines from backups performed using the Data Protector **Hyper-V Image** method.

Restore of virtual machines

Virtual machines backed up with the **Hyper-V Image** method can be restored:

- To the default location
- To a different location
- To a directory

Restore to the default location

When restoring from a **Hyper-V Image** backup, by default, virtual machines are restored to their original Microsoft Hyper-V systems. If a virtual machine to be restored still exists on the original Microsoft Hyper-V system, it is deleted before the files from the backup are restored.

To keep, for example, for safety reasons, the existing virtual machine, you should export it from the system before performing the restore.

Note: If a virtual machine that was exported is re-imported, it is effectively a clone of the original. When you import the machine you are be asked if you want to use the old virtual machine GUID. If the original virtual machine, from which the exported machine was created, still exists, keeping the original GUID causes the import to fail. Also after importing, you may have network problems unless you change the IP address of the virtual machine.

For the restore, you can also specify:

- Whether virtual machines should be restored to a different Microsoft Hyper-V system
- Whether the restored virtual machines should be powered on

The options in the **Options** page are, by default, set to restore virtual machines with the same names, same GUIDs, to the same Microsoft Hyper-V system (or cluster), and to the same locations.

Restore in a cluster

When restoring VMs that are configured in a cluster, the cluster node where a restored VM will be running depends on the restore client selection and the state of the environment at the restore time.

It does not depend on the state of the environment at the backup time, that is, where the VM was running when it was backed up.

Note: If you use shared cluster disks (not CSV), you can restore a virtual machine only to the node on which the virtual machine is currently registered, as only this node can access the shared cluster disks.

Restore to a different location

To restore the virtual machine to a different location (on the same or another system), select **Restore to a target storage path**. The restore is performed using the Hyper-V writer, therefore the restored virtual machines are functional.

Restore to a directory

When restoring to a directory (restore outside a Microsoft Hyper-V system) all the virtual machine files can be restored to a directory of your choice (for example, `C:\tmp`) on the selected restore system.

After such a restore, the virtual machines are not functional. You need to import the files to a Microsoft Hyper-V system for the virtual machines to become functional.

Restore chain validation

When you select an incremental backup session to restore a virtual machine to the corresponding state, Data Protector automatically processes the restore chain, starting with the latest full backup image created before the selected session and then restoring all subsequent incremental backup images up to the selected session. To ensure integrity of the restored data, Data Protector checks the validity of the entire chain before starting the actual data restore. An invalid restore chain results in a failed session with no changes made to the virtual machine and its snapshots.

You can disable restore chain validation by setting the omnirc option `OB2_VEAGENT_DISABLE_RESTORE_CHAIN_PROTECTION` to the value `1`. See also Customizing the Data Protector behavior with omnirc options on page 142. Note that unprotected restore chains cannot be validated. Data Protector attempts to validate unprotected restore chains result in failed restore sessions.

Restore considerations

- Due to the architectural foundation of the Data Protector Virtual Environment integration, consider the Microsoft Hyper-V writer specifics described in the *HP Data Protector Integration Guide for Microsoft Volume Shadow Copy Service*.

Data Protector backup solutions

- Hyper-V backup objects that were created using the Data Protector Microsoft Volume Shadow Copy Service integration cannot be restored using the Data Protector Virtual Environment

integration.

Restore parallelism

- Restore sessions that use the same devices or restore to the same Microsoft Hyper-V system (or cluster) cannot run concurrently.
- Data Protector optimizes each restore session to the highest degree possible. When multiple virtual machines are selected for restore, data from their backup images is restored in parallel provided that the images were created in the same Data Protector backup session.

Restore to a backup host

- Data Protector clients that are not imported as Hyper-V clients cannot be selected for restore. Import the system you want to use as a backup host as a Data Protector Hyper-V client. If you use the system only for restore purposes, you can omit entering the user credentials during the import. After the import, you can select the client from the Restore client drop-down list.

  After the restore, you can remove the Hyper-V client and import it again as regular Data Protector client.

  Note that for a backup host, you can select any client that has the Data Protector `Virtual Environment Integration` and `MS Volume Shadow Copy Integration` components installed.

Restore to a different location

- If you restore a replica VM or a primary VM with a custom path configuration (Snapshot File Location and Smart Paging File Location are not set to the default virtual machine location) to a different location using the **Restore to a target storage path** option, the Smart Paging File Location and the Snapshot File Location paths are not updated. If you restore a replica VM that contains recovery points, only the Smart Paging File Location is not updated.

  After a restore, check the Smart Paging File Location and the Snapshot File Location paths and update them if necessary.

  Tip: To make sure that the Snapshot File Location is automatically updated after restore, HP recommends that you configure at least one recovery point for the replica VM.

Restore of virtual machine replicas

- When selecting a VM for restore, it is not possible to determine whether a primary or replica VM was backed up. The replication state after restore however depends on whether the backed up VM is a primary or replica VM:

- In case of a primary VM, the replication is disabled.
- In case of a replica VM, a failover is initiated, so that the replica VM becomes a primary VM.

- **Configuring the network adapter for the replicated virtual machine**

  Replica VMs are by default not connected to a network. When restored, it is without a network connection even if it is restored as a primary VM. You should manually map the virtual network switches to the NICs before starting the restored VM.

  If the replica VM is connected to a virtual network switch, the virtual switch names used on both the primary and replica side should be the same, otherwise the restored VM cannot be started. To avoid startup problems, connect the network adapter to an existing virtual network switch or remove the connection.

- **Cluster environments**
  - If a primary VM with data on a cluster shared volume (CSV) is replicated to a non-cluster system, the VM machine may not be highly available after restore.

    Data Protector by default restores the VMs to the original backup location. For the replica VM, this is a local volume, therefore the VM is restored to a local volume and the existing cluster resource group cannot be brought online, because it is not on a CSV. Data Protector deletes the cluster resource group and reattaches the VM to the cluster. If the restored VM data is residing on a local volume, the Storage resource is not included in the cluster resource group.
  - If the primary VM is replicated to a CSV on another Hyper-V cluster and the paths to the CSV are the same on the primary and replicated side, the VM is highly available after restore.
  - If the VMs are not located on a CSV and the storage location of the restored VM is changed, for example by restoring to a new storage location or restoring a replica VM to the primary cluster, Data Protector cannot recreate the cluster resource group and you must manually delete and recreate it.

Virtual machines on Windows shares

- During a restore to an SMB file share, the Data Protector VSS agent needs sufficient rights to modify the ACLs of the restored VM files. Therefore you need to run the Data Protector Inet service on the Hyper-V host under a domain user account with appropriate rights. See the Help index: ”Inet user impersonation”.

  Alternatively, add the computer account of the Hyper-V host to the Administrators group of the file server (SMB file share host).

- A virtual machine backed up from an SMB file share can be restored to a different Hyper-V host only if the Hyper-V machine account (*domain*\hyperv$) has Full Control permissions on the SMB file share and the restored files. You can achieve this by adding the target Hyper-V host in the same domain security group as used by the original Hyper-V host.

- You can restore a virtual machine backed up from an SMB file share or local volume to a different SMB file share. In both cases Data Protector adds the Hyper-V computer domain account (*domain*\hyperv$) to the ACLs of the restored VM files on the SMB file share with Full Control permissions.

Configuring the integration

To configure the integration:

- Enable automatic mounting of new volumes. See Enabling automatic mounting of new volumes on Microsoft Hyper-V systems on the next page.
- Import and configure Microsoft Hyper-V systems. See Importing and configuring Microsoft Hyper-V systems on page 139.
- **Microsoft Hyper-V cluster:** Resolve cluster nodes. See Configuring Microsoft Hyper-V clusters on the next page.

Prerequisites

- Ensure that you have a correctly installed and configured Microsoft Hyper-V virtualization environment.
- Ensure that you have correctly installed Data Protector.

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

  - Ensure that you have at least one client in your environment, with both the Data Protector `Virtual Environment Integration` and `MS Volume Shadow Copy Integration` components installed. Such a client is called the **backup host**. The backup host must have network access to all the Microsoft Hyper-V systems/clusters. No special configuration is required after installation.

    If you intend to restore virtual machine files to a directory on a backup host, also install the `Disk Agent` component on the backup host. Otherwise, you will not be able to use the **Browse** button to specify the target directory (however, you will still be able to type the directory yourself).

  - Ensure that each Microsoft Hyper-V system that you intend to back up from or restore to has the `MS Volume Shadow Copy Integration` component installed. If your Microsoft Hyper-V systems are configured in a cluster, they must be installed as cluster-aware clients. For details, see the *HP Data Protector Installation and Licensing Guide*.

    ZDB environments:

- If the virtual machine files are located on a disk array, ensure that you have configured and installed the corresponding VSS hardware provider.
- For VSS transportable backups, the `MS Volume Shadow Copy Integration` must also be installed on the backup system.

For details, see the *HP Data Protector Integration Guide for Microsoft Volume Shadow Copy Service*, chapter *Configuration*.

- Ports: Data Protector uses Windows Management Instrumentation (WMI) to locate Hyper-V resources. WMI uses port 135 on the target system to create a connection. After the connection is established an ephemeral port is used for the communication.
- For supported versions, platforms, devices, and other information, see the latest support matrices at http://support.openview.hp.com/selfsolve/manuals.

Limitations

- For restore to a directory (in which case, the backup host is used as the restore client), the application client and the backup host that you use must have the same operating system version installed.
- For VSS related limitations, see the *HP Data Protector Integration Guide for Microsoft Volume Shadow Copy Service*.
- For other limitations and recommendations, see the *HP Data Protector Product Announcements, Software Notes, and References*.

Before you begin

- Configure devices and media for use with Data Protector.
- To test whether the Cell Manager communicates with the Microsoft Hyper-V systems and the backup system properly, configure and run a Data Protector filesystem backup and restore on every Microsoft Hyper-V system and backup host in your environment.

Enabling automatic mounting of new volumes on Microsoft Hyper-V systems

To be able to perform online backups, enable automatic mounting of new volumes on all Microsoft Hyper-V systems by executing the `MOUNTVOL /E` command on each system.

Configuring Microsoft Hyper-V clusters

Before performing a backup in a Microsoft Hyper-V cluster environment, resolve every cluster node by executing the following command:

```
omnidbvss -resolve -apphost HyperVNode
```

The resolution needs to be performed sequentially and, normally, only needs to be performed once. For more information, see the *HP Data Protector Integration Guide for Microsoft Volume Shadow Copy Service*.

Importing and configuring Microsoft Hyper-V systems

The Microsoft Hyper-V systems need to be imported into the Data Protector Cell as **Hyper-V** clients.

Important: A client cannot be imported and configured as Hyper-V client, VMware vCenter client, and VMware vCloud Director client at the same time.

Note: Clustered environment: If your Microsoft Hyper-V systems are configured in a cluster, you need to import all cluster nodes and the virtual server as **Hyper-V** clients.

Prerequisites

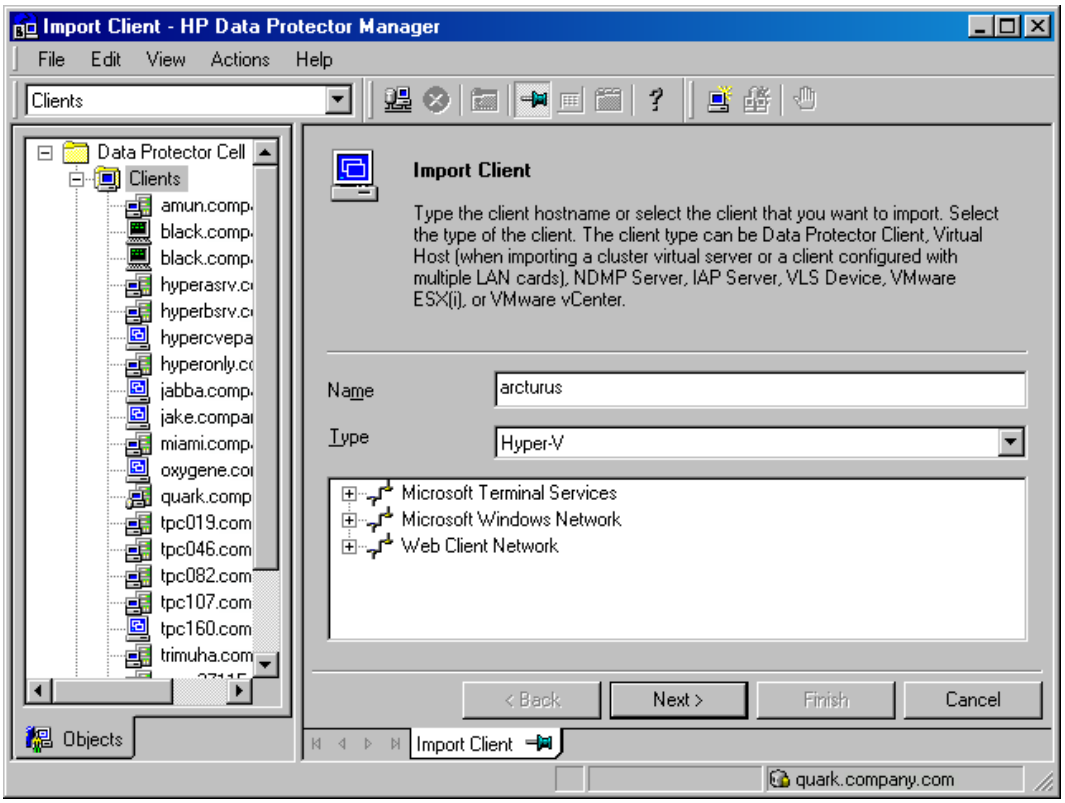
- The User Account Control on the Microsoft Hyper-V system must be configured to elevate user rights automatically.

Procedure

To import a client into a Data Protector cell:

1. In the Context List, click **Clients**.
2. In the Scoping Pane, expand **Data Protector Cell**, right-click **Clients**, and click **Import Client**.
3. In the Import client page, enter the client name in the **Name** option, select the **Hyper-V** type from the **Type** drop-down list, and click **Next**.

Figure 56: Importing a Microsoft Hyper-V client (Name and Type)



4. Specify login credentials:

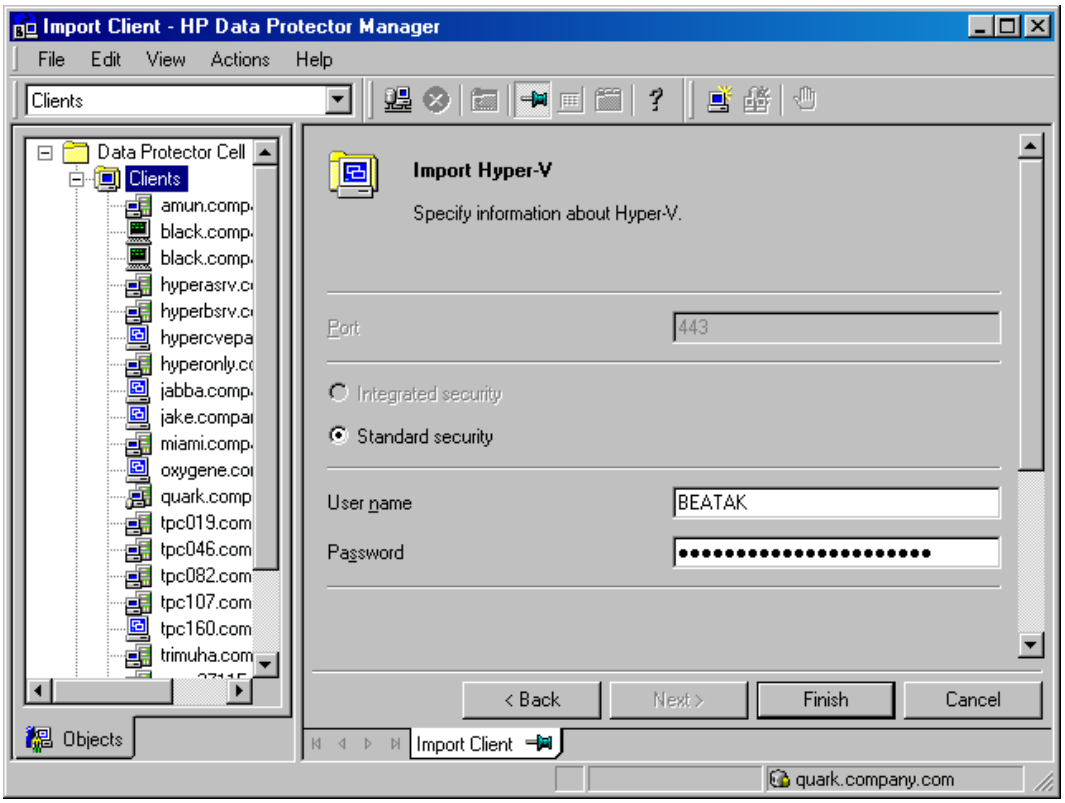
   Username and **Password**: Specify an operating system user account that has appropriate permissions to access the Microsoft Hyper-V WMI services. You can specify the user account in the following format:

   ```
   DOMAIN\Username
   ```

   If the domain is not specified, it is detected automatically. In case of a Microsoft Hyper-V cluster, both the domain and the username must be specified.

   Click **Finish**.

Figure 57: Importing a Microsoft Hyper-V client (Login credentials)



Note: For details of how to change the parameters later, see Changing the configuration of Microsoft Hyper-V systems below.

Changing the configuration of Microsoft Hyper-V systems

You can only change the credentials for connecting to a Microsoft Hyper-V system if you have the Data Protector `Clients configuration` user right. For details on the Data Protector user rights, see the *HP Data Protector Help* index: ”user groups”.

To change the login credentials, use the Data Protector GUI or CLI.

Using the Data Protector GUI

1. In the Context List, click **Clients**.
2. In the Scoping Pane, expand **Clients** and then select the client for which you want to change the login credentials.

3. In the Results Area, click the **Login** tab.
4. Update the credentials as needed and click **Apply**.

Using the Data Protector CLI

1. Log on to the backup host.
2. Open a Command Prompt window and change current directory to the directory of the `vepa_util.exe` command.

   For the command location, see the `omniintro` reference page in the *HP Data Protector Command Line Interface Reference* or the `omniintro` man page.
3. Execute:

   ```
   vepa_util.exe
   command
   --config
   --virtual-environment hyperv
   --host HyperVClient
   --username Username
   {--password Password | --encoded-password Password}
   ```

   The message `*RETVAL*0` indicates successful configuration.

   For option description, see the *HP Data Protector Command Line Interface Reference* or the `vepa_util.exe` man page.

Customizing the Data Protector behavior with omnirc options

The omnirc options are useful for troubleshooting or overriding other settings affecting the behavior of the Data Protector client. Options that apply to the Virtual Environment integration have the prefix `OB2_VEAGENT`.

For details on how to use Data Protector omnirc options, see the *HP Data Protector Help* index: “omnirc options”.

Backup

To back up virtual machines, create a backup specification and then start a backup session. For backup concepts, see Backup concepts on page 123.

Creating backup specifications

Create a backup specification using the Data Protector GUI (**Data Protector Manager**).

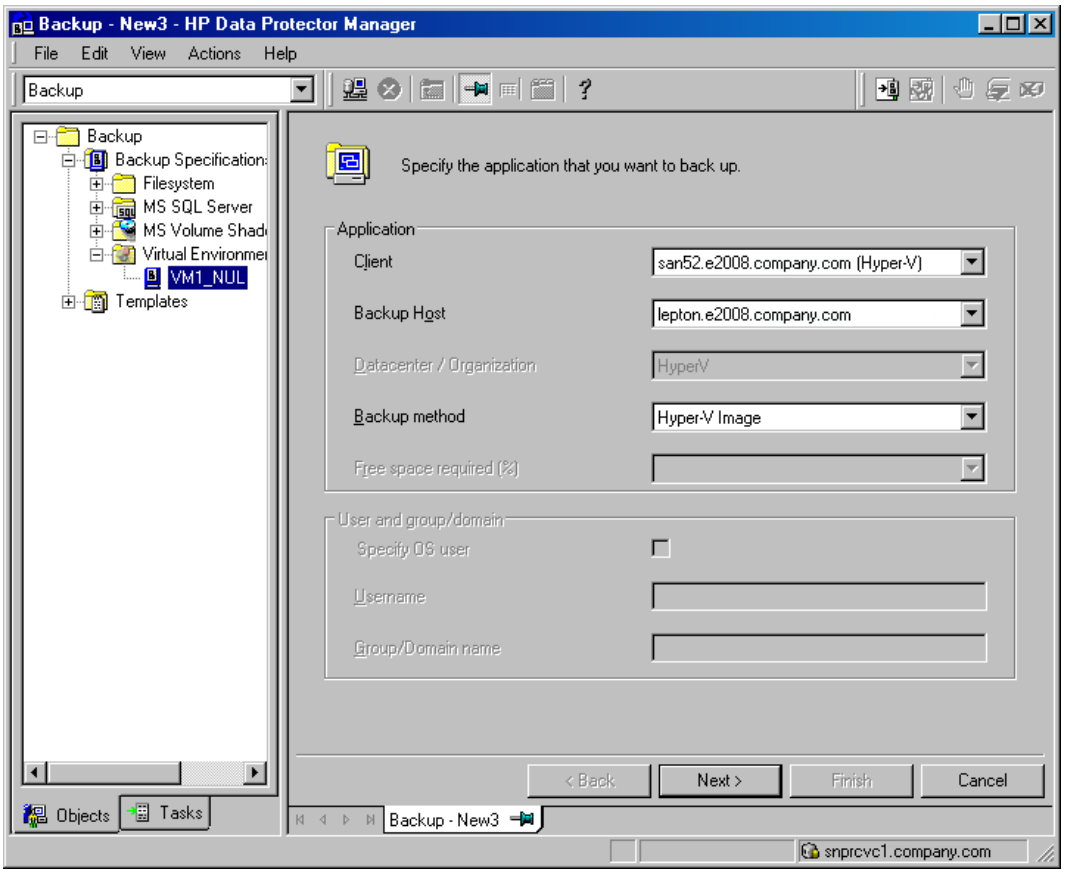
1. In the Context List, click **Backup**.
2. In the Scoping Pane, expand **Backup Specifications**, right-click **Virtual Environment**, and click **Add Backup**.
3. In the Create New Backup dialog box, specify the VSS backup type.

   Click **OK**.
4. From the **Client** drop-down list, select the Microsoft Hyper-V system that you want to back up data from. The list contains all clients that were imported into the Data Protector cell as **Hyper-V** clients.

   In a cluster environment, select any of the cluster nodes or the virtual server. Regardless of what part of the cluster you select, you will be able to back up all VMs residing in the cluster.

   From the **Backup Host** drop-down list, select a system to be used to control the backup. The list contains all clients that have the Data Protector `Virtual Environment Integration` and the Data Protector `MS Volume Shadow Copy Integration` components installed.

Figure 58: Selecting a client system and backup host

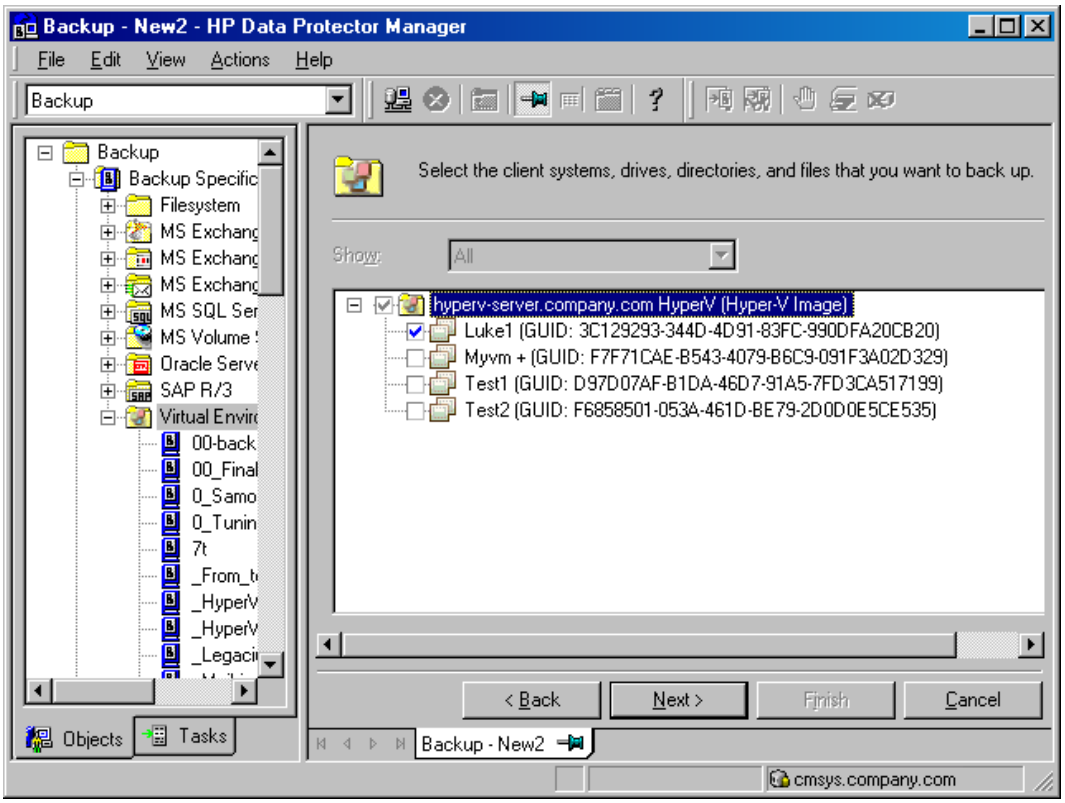


Click **Next**.

5. This step depends on the type of your environment:
   - With a non-ZDB environment, click **Next**.
   - With a ZBD environment, specify the following options:
     - For a *local or network backup*, select **Use hardware provider**.
     - For a *transportable backup*, select the **Backup system** from where the VSS shadow copies can be backed up to backup media or where you want your shadow copies to be presented and mounted after the backup. The VSS hardware provider is used automatically.
     - Specify other ZDB-specific options. For details, press **F1** or see the *HP Data Protector Integration Guide for Microsoft Volume Shadow Copy Service*. Note that the **Track the replica for instant recovery** option is not available since instant recovery is not supported.

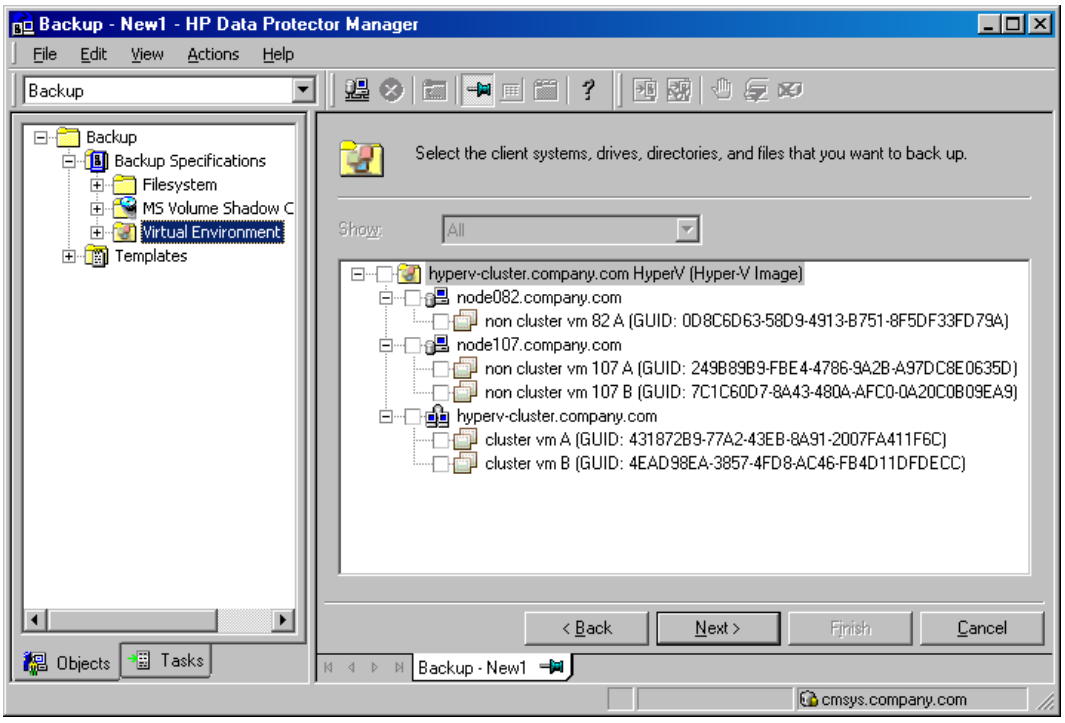
     Click **Next**.
6. Select the virtual machines you want to back up.

Figure 59: Selecting the backup objects



In a cluster, both non-cluster VMs and cluster VMs are displayed for all nodes of the cluster; non-cluster VMs are listed under their nodes and cluster VMs under their virtual server.

Figure 60: Selecting the backup objects in a cluster



Click **Next**.

7. Select the devices to use for the backup.

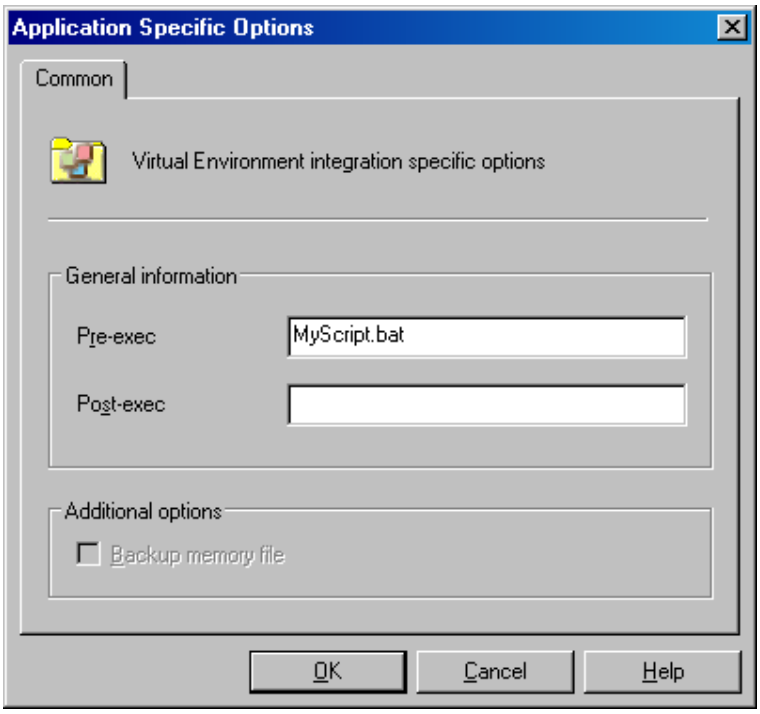
   To specify device options, right-click the device and click **Properties**. Set the device concurrency, media pool, and preallocation policy. For details, press **F1** or click **Help**.

   You can also specify whether you want to create additional copies (mirrors) of the backup during the backup session. Specify the desired number of mirrors by clicking the **Add mirror** and **Remove mirror** buttons. Select separate devices for the backup and for each mirror. For details, press **F1**.

   Click **Next**.

8. Set backup options. For information on backup specification options and common application options, press **F1**. For information on application-specific options, see Application-specific backup options on the next page.

Figure 61: Application-specific options



Click **Next**.

9. Optionally, schedule the backup. See Scheduling backup sessions on page 150.

   Click **Next**.

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

Table 15: Application-specific backup options

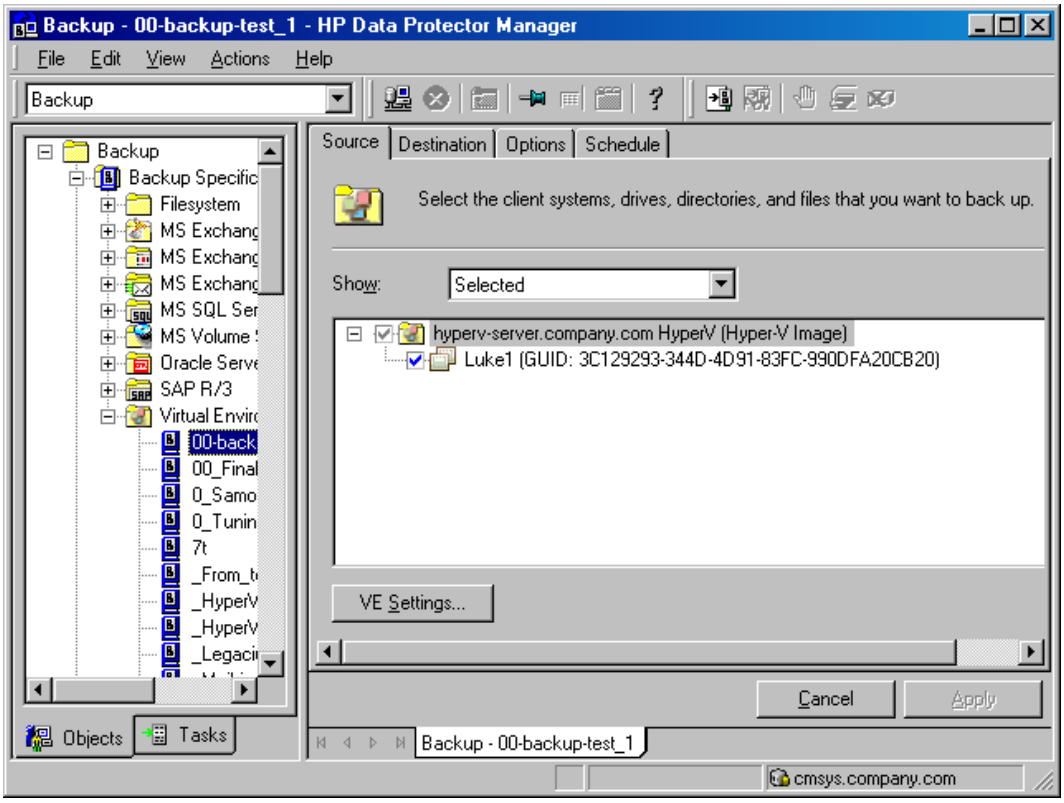
Option	Description
Pre-exec , **Post-exec**	Invoke the specified command, script, or application on the backup host before (**Pre-exec**) or after (**Post-exec**) the backup. In the specified command lines, do not use double quotes. Type only the name of the executable file and ensure that the file resides in the default Data Protector commands directory on the backup host.

Option	Description
Enable incremental backup of VM(s) *(available for systems that support incremental backup of Hyper-V virtual machines)*	Select this option and run a *full* backup session to enable Microsoft Hyper-V incremental backup sessions based on the Data Protector backup specification you are configuring. You can then choose between a full or incremental backup of Microsoft Hyper-V virtual machines later on when scheduling or starting a subsequent Data Protector backup session. Incremental backup can only be performed if the virtual machines to be backed up are properly prepared for it. It stores the changes made to the virtual machine after the last backup of any type, and is updated after each backup session. This option prepares all virtual machines that are included in the backup specification. When you clear this option and run a backup session, the virtual machine configurations with regard to incremental backup readiness are left intact. When this option is selected, the **Back up selected VM(s)** option is automatically selected, and the **Back up replica VM (s)** and **Use primary VM(s) if replication link is down** options are made unavailable. Default: not selected.
Back up selected VM(s) *(available for systems that support virtual machine replication)*	Select this option to back up the selected virtual machine (VM), regardless if it is a primary or replica VM. Default: selected.
Back up replica VM(s) *(available for systems that support virtual machine replication and when **Enable incremental backup of VM (s)** is not selected)*	Select this option to instruct Data Protector to always back up the replica VM even if a primary VM is selected. If the replication connection is down, the backup will fail even if a primary VM is selected. Default: not selected.
Use primary VM(s) if replication link is down *(available when **Back up replica VM(s)** is selected)*	Select this option to instruct Data Protector to back up the primary VM instead of the replica VM if the replication connection does not function. Default: not selected. Selected if **Back up replica VM(s)** is selected.

Modifying backup specifications

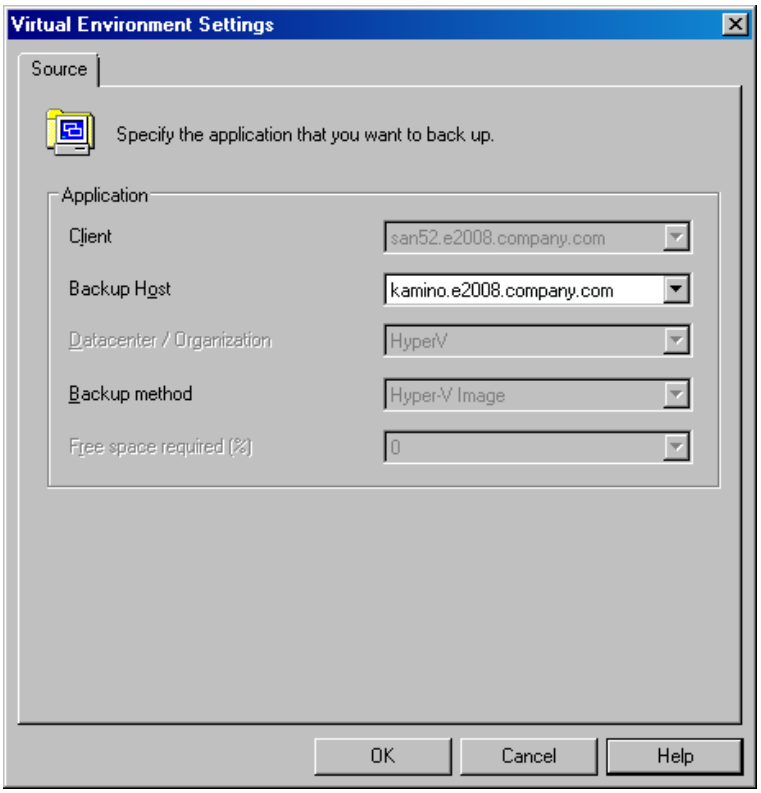
To modify your backup specification, select **Backup** in the Context List and click the backup specification name in the Scoping Pane. In the Results Area, click the appropriate tab and make the desired changes. When you are done apply them by clicking **Apply**.

Figure 62: Modifying a backup specification



To display the virtual environment settings, in the Results Area, click **VE Settings**. Not all settings can be modified.

Figure 63: Virtual environment settings



Note: To see all virtual machines in the source page, not just those you selected, select **All** from the Show list.

Scheduling backup sessions

You can schedule a backup session to start automatically at specific times or periodically. For details on scheduling, see the *HP Data Protector Help* index: “scheduled backups”.

Scheduling example

The following example applies to a Microsoft Hyper-V environment that supports incremental backup of virtual machines and to backup specifications in which the participating virtual machines are already prepared for Data Protector incremental backup sessions.

To schedule incremental backups at 8:00 and 13:00 and full backups at 18:00 each weekday:

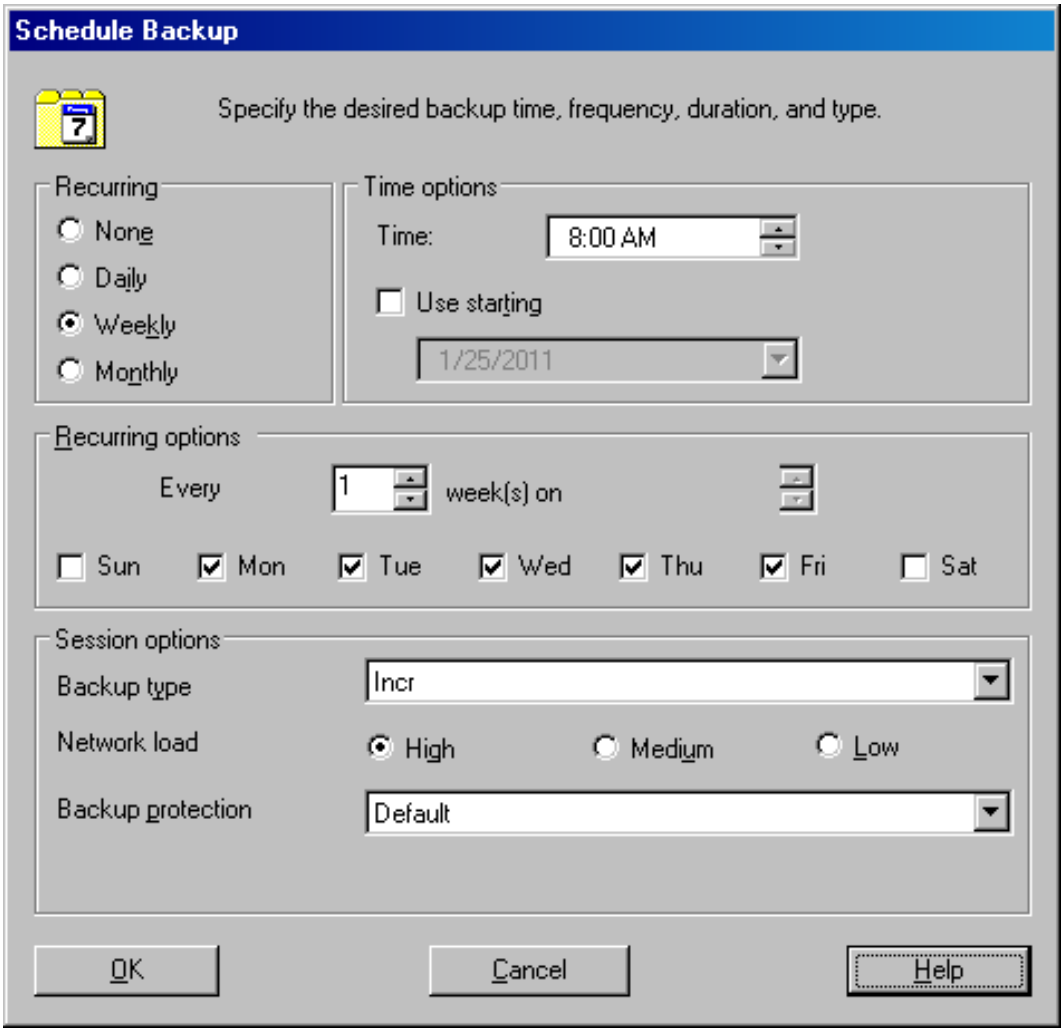
1. In the Schedule property page of the Backup wizard, select the starting date in the calendar and click **Add** to open the Schedule Backup dialog box.
2. Under Recurring, select **Weekly**. Under Time options, type **8:00** or appropriately change the

value in the Time box. Under Recurring options, select **Mon**, **Tue**, **Wed**, **Thu**, and **Fri**. Under Session options, select **Incr** from the Backup type list. See Scheduling backup sessions below.

Click **OK**.

3. Repeat Step 1 and Step 2 to schedule backups at 13:00 and 18:00, each time selecting the appropriate backup type.
4. Click **Apply** to save the changes.

Figure 64: Scheduling backup sessions



Starting backup sessions

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

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

Using the Data Protector GUI

1. In the Context List, click **Backup**.
2. In the Scoping Pane, expand **Backup Specifications** and then **Virtual Environment**.
3. Right-click the chosen backup specification and click **Start Backup**.
4. In the Start Backup dialog box, from the Backup type drop-down list, select either **Full** for full backup or **Incr** for incremental backup.
5. From the Network load drop-down list, select the desired network load for the session.
6. Click **OK**.

At the end of a successful backup session, the message `Session completed successfully` is displayed.

Using the Data Protector CLI

1. Log on to a Data Protector client where the Data Protector `User Interface` component is installed.
2. Open a Command Prompt window and change current directory to the directory of the `omnib` command.

   For the command location, see the `omniintro` reference page in the *HP Data Protector Command Line Interface Reference* or the `omniintro` man page.
3. Execute:

   `omnib -veagent_list` *`BackupSpecificationName`* `[-barmode` *`VirtualEnvironmentMode`*`]` `[`*`LIST_OPTIONS`*`]`

   where *`VirtualEnvironmentMode`* can be either `full` for full backup or `incr` for incremental backup.

   If the option `-barmode` is not specified, Data Protector attempts to start a full backup.

   For description of the option group *`LIST_OPTIONS`*, see the *HP Data Protector Command Line Interface Reference* or the `omnib` man page.

Examples

To start a full backup using the backup specification `MyVirtualMachines`, execute:

```
omnib -veagent_list MyVirtualMachines -barmode full
```

Restore

You can restore Microsoft Hyper-V virtual machines using the Data Protector GUI or CLI. For restore concepts, see Restore concepts on page 133.

Limitations

- **Windows Server 2008 systems:** If you perform a restore to a target storage path:
  - The option Power-on VM after restore is not supported. You must manually delete the saved states before you can power on the VM.
  - If the restored VM was part of a cluster and the cluster resource of the VM still existed at the begin of the backup, you must manually recreate the cluster resource after the restore.
- If you perform a restore to a different x64 platform, for example, if the backup was performed on an AMD system and you restore the VM to an Intel system, the system cannot be powered on. You must manually delete the saved states before you can power on the VM.
- Data Protector adds the original VM paths to the specified target storage locations. If the resulting file path is longer than 255 characters Hyper-V cannot access the files although the files are properly restored.

Finding information for restore

You can retrieve information about backup sessions (such as information on the backup media used and the messages reported during the backup) from the Data Protector Internal Database (IDB).

For retrieval, use the Data Protector GUI or CLI.

Using the Data Protector GUI

1. In the Context List, click **Internal Database**.
2. In the Scoping pane, expand **Objects** or **Sessions**.

   If you expand **Objects**, backup objects are sorted according to the Microsoft Hyper-V systems for which they were created.

   Note: The backup object name contains the virtual machine GUID.

   For example, the backup object for the database with the GUID `4844CA0C-E952-48D9-AE04-C68DDE08F1BR` is:

   ```
   /%2FHyperV/6/4844CA0C-E952-48D9-AE04-C68DDE08F1BR [VEAgent]
   ```

If you expand **Sessions**, backup objects are sorted according to the sessions in which they were created. For example, backup objects created in the session `2011/02/7–7` are listed under `2011/02/7–7`.

To view details on a backup object, right-click it and click **Properties**.

Tip: To view messages reported during the session, click the **Messages** tab.

Using the Data Protector CLI

1. Log on to a Data Protector client where the Data Protector `User Interface` component is installed.
2. Open a Command Prompt window and change current directory to the directory of the `omnidb` command.

   For the command location, see the `omniintro` reference page in the *HP Data Protector Command Line Interface Reference* or the `omniintro` man page.
3. To get a list of backup objects created in the backup session *`SessionID`*, execute:

   ```
   omnidb -session SessionID
   ```
4. To get details on the backup object *`BackupObjectName`*, execute:

   ```
   omnidb -veagent BackupObjectName -session SessionID -catalog
   ```

   Here is one example of a backup object name:

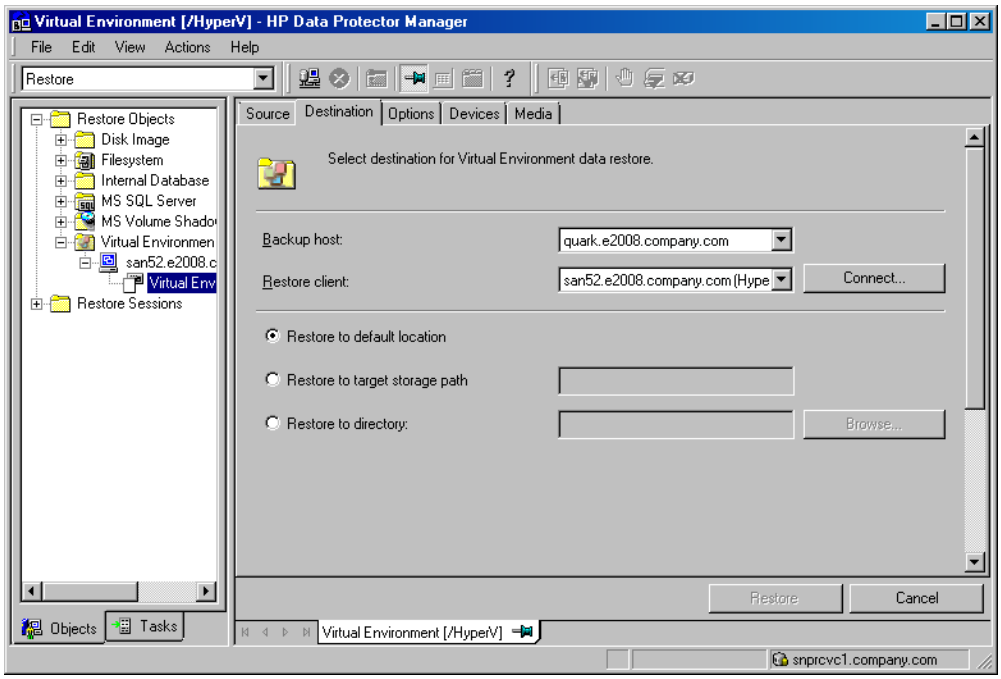
   ```
   quark.company.com:/%2FHyperV/6/4844CA0C-E952-48D9-AE04-C68DDE08F1BR [VEAgent]
   ```

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

Restoring using the Data Protector GUI

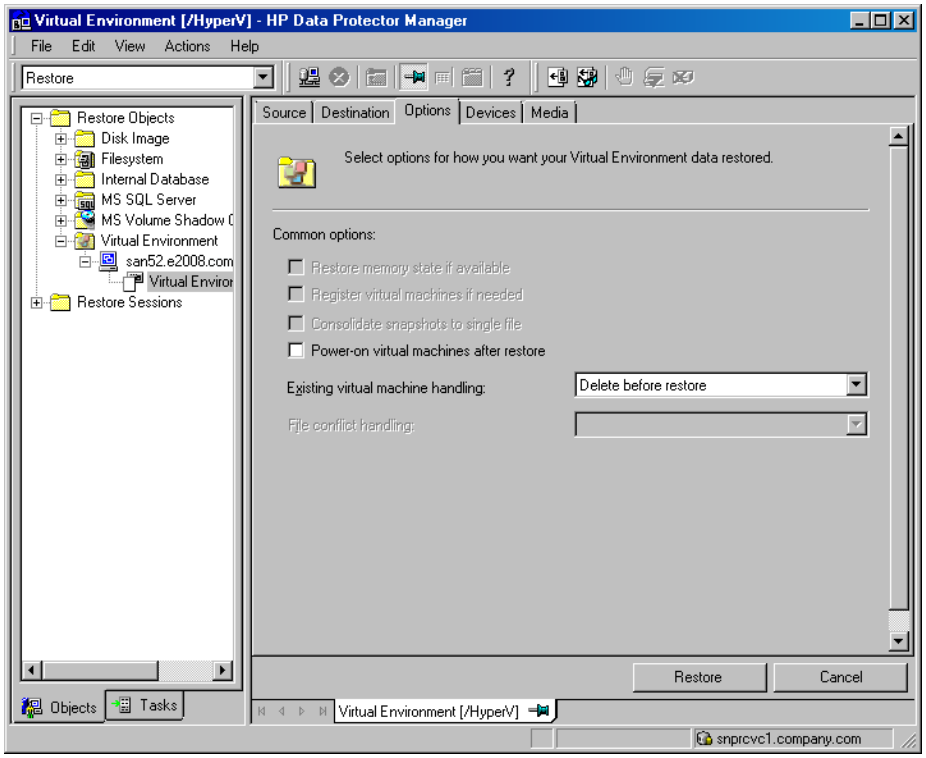
1. In the Context List, click **Restore**.
2. In the Scoping Pane, expand **Virtual Environment**, expand the client from which you want to restore, and click **Virtual Environment [HyperV]**.
3. In the Source page, select the virtual machines you want to restore.
4. In the Destination page, specify the restore destination. For details, see Restore destination on page 156

Figure 65: Restore destination



5. In the Options page, specify the restore options. For details, see Restore options on page 157

Figure 66: Restore options



6. In the Devices page, specify which devices to use for restore.

   For details, see the *HP Data Protector Help* index: “restore, selecting devices for”.

7. Click **Restore**.

8. In the Start Restore Session dialog box, click **Next**.

9. Specify the report level and the network load.

   Note: Select **Display statistical information** to view the restore profile messages in the session output.

10. Click **Finish** to start the restore.

    The statistics of the restore session, along with the message `Session completed successfully` is displayed at the end of the session output.

Note: When you restore a virtual machine to a directory and data from its incremental backup images is also restored during the session, to access folders and files in the restored virtual machine, you have to merge the virtual machine snapshots first. See Merging virtual machine snapshots manually on page 159.

Table 16: Restore destination

GUI option `omnir` command option	**Description**
Backup host `-barhost`	Select the Data Protector client that should control the restore. The drop-down list contains all clients that have the Data Protector `Virtual Environment Integration` and `MS Volume Shadow Copy Integration` components installed.
Restore client `-apphost`, `-destination`	Select the Microsoft Hyper-V client to which the selected virtual machines should be restored to. By default, the client from which the virtual machines were backed up is selected.
Restore to default location	Select this option to restore virtual machines to the original location on the selected restore client.
Restore to target storage path `-targetstoragepath`	Select this option to restore virtual machines to a different location on the selected restore client. All VMs are restored to a single volume, even if the VMs were originally on different volumes. For each VM, the original path is appended to the target storage path.

Restore to directory `-directory`	Select this option to restore virtual-machine files to a directory on selected restore client. You can use the Browse button to find the target directory.

Table 17: Restore options

GUI option `omnir` command option	**Description**
Power on virtual machines after restore `-poweron`	Select this option to power the virtual machines on once they are restored. This option is not available when restoring to a directory.

Existing virtual machine handling	Specifies Data Protector's behavior when restoring existing virtual machines.	
	Delete before restore `-deletebefore`	Select this option to delete an existing virtual machine before it is restored, and then restore it from new. Default (GUI): selected.
	Skip restore `-skip`	Select this option to skip the restore of an existing virtual machine. When restoring multiple virtual machines, selecting this option enables you to restore only the virtual machines that do not exist at restore time.

Restoring using the Data Protector CLI

1. Log on to a Data Protector client where the Data Protector `User Interface` component is installed.
2. Open a Command Prompt window and change current directory to the directory of the `omnir` command.

   For the command location, see the `omniintro` reference page in the *HP Data Protector Command Line Interface Reference* or the `omniintro` man page.
3. Execute:

```
omnir -veagent
       -virtual-environment hyperv
       -barhost BackupHost
       -apphost OriginalHypervClient
       [-session BackupID]
       -vm GUID [-vm GUID...]
```

```
[-destination DifferentHyperVClient]
[-targetstoragepath TargetStoragPathOfAllHyper-V-VMs|
-directory RestoreDirectory]
[-poweron]
```

For a description of all the options, see the *HP Data Protector Command Line Interface Reference* or the `omnir` man page.

Important: A backup ID is a point in time. All objects (backup data) created in a backup session have the same backup ID, which is the same as the session ID of the backup session.

Mirrored objects and objects created in an object copy session have the same backup ID as objects created in the original backup session. Suppose the media set created in the original backup session no longer exists, but the media set created in an object copy session still exists. To restore the objects, you have to specify the session ID of the original backup session (that is, the backup ID) and not the session ID of the object copy session.

The `omnir` syntax does not let you specify from which object copy to restore if several copies of the same object exist. This is only possible using the Data Protector GUI by setting the media allocation priority list.

Note: When you restore a virtual machine to a directory and data from its incremental backup images is also restored during the session, to access folders and files in the restored virtual machine, you have to merge the virtual machine snapshots first. See Merging virtual machine snapshots manually on the next page.

Example: Restoring virtual machines to a Microsoft Hyper-V system

Suppose you want to restore the virtual machines `VM1` with the GUID `62BD6C3C-D4BE-44F4-88D6-E439C96C4B0C` and `VM2` with the GUID `54C22930-E3B9-43AA-AFCD-1E90BB99F130`. At the time of backup, the virtual machines were running on the Microsoft Hyper-V system `hyperv1.company.com`. The virtual machines have been backed up with the `Hyper-V Image` backup method.

To restore the virtual machines to the Microsoft Hyper-V system `hyperv2.company.com` to the default location, using the backup session `2011/01/11-1`, and to power the newly restored virtual machines on, execute:

```
omnir -veagent -virtual-environment hyperv -barhost backuphost.company.com -
apphost hyperv1.company.com -session 2011/1/11-1 -vm 62BD6C3C-D4BE-44F4-88D6-
E439C96C4B0C -vm 54C22930-E3B9-43AA-AFCD-1E90BB99F130 -destination
hyperv2.company.com -poweron
```

Example: Restoring virtual machines to a different location

Suppose you want to restore the virtual machines `VM1` with the GUID `62BD6C3C-D4BE-44F4-88D6-E439C96C4B0C` and `VM2` with the GUID `54C22930-E3B9-43AA-AFCD-1E90BB99F130`. At the time of backup, the virtual machines were running on the Microsoft Hyper-V system

hyperv1.company.com. The virtual machines were backed up with the Hyper-V Image backup method.

To restore the virtual machines to the Microsoft Hyper-V system hyperv2.company.com to the location c:\machines, using the backup session 2011/01/11–1, and to power the newly restored virtual machines on, execute:

```
omnir -veagent -virtual–environment hyperv -barhost backuphost.company.com -
apphost hyperv1.company.com –session 2011/1/11-1 –vm 62BD6C3C-D4BE-44F4-88D6-
E439C96C4B0C –vm 54C22930-E3B9-43AA-AFCD-1E90BB99F130 -destination
hyperv2.company.com -targetstoragepath c:\machines -poweron
```

Example: Restoring virtual machines outside a Microsoft Hyper-V system

Suppose the virtual machines VM1 with the GUID 62BD6C3C-D4BE-44F4-88D6-E439C96C4B0C and VM2 with the GUID 54C22930-E3B9-43AA-AFCD-1E90BB99F130 that were backed up in the session 2011/02/12-5 from the Microsoft Hyper-V system hyperv.company.com, using the Hyper-V Image backup method. To restore the virtual machines outside the Microsoft Hyper-V system, to the directory C:\tmp on the backup host backuphost.company.com, execute:

```
omnir -veagent -virtual–environment hyperv -barhost backuphost.company.com -
apphost hyperv.company.com -session 2011/2/12-5 -vm 62BD6C3C-D4BE-44F4-88D6-
E439C96C4B0C -vm 54C22930-E3B9-43AA-AFCD-1E90BB99F130 -directory c:\tmp
```

Merging virtual machine snapshots manually

When a Microsoft Hyper-V virtual machine is restored to a directory and a restore chain is involved, Data Protector does not automatically merge the incremental backup images into their base backup image. Instead, Data Protector restores each backup image to a subdirectory of the selected target directory. To get the volumes of the virtual machine disks to the sate as they were at the time the last incremental backup session was run, and gain access to the contained folders and files, you have to manually merge the backup images.

Follow the steps:

1. In the subdirectories of the target restore directory on the backup host, enumerate all virtual hard disk files (files of the type *.vhd, *.vhdx, *.avhd, or *.avhdx) whose filenames do not contain the string ChildVhd. Copy all such files to a single directory.
2. Launch Hyper-V Manager. In the Actions pane, click **Edit Disk**.
3. In the Edit Virtual Hard Disk Wizard, click **Browse**.
4. In the Open dialog box, browse to the directory with the copied virtual hard disk files.
5. Select the oldest differential virtual hard disk file (file of the type *.avhd or *.avhdx) and confirm your selection.
6. In the Edit Virtual Hard Disk Wizard, select **Merge** and click **Next >**.
7. Select **To the parent virtual hard disk**, click **Next >**, and confirm you action by clicking **OK**.

8. Repeat steps Select the oldest differential virtual hard disk file (file of the type *.avhd or *.avhdx) and confirm your selection. on the previous page to Select To the parent virtual hard disk, click Next >, and confirm you action by clicking OK. on the previous page until all virtual hard disk snapshots are merged.
9. Right-click the virtual hard disk and select **Mount** to mount its volume to a drive letter or a directory.
10. Copy the folders and files you need.
11. Using the administrative tool Computer Management, dismount the virtual hard disk volume by right-clicking it and selecting **Detach VHD**.

Restore of cluster virtual machines

After a restore of a cluster virtual machine that was, for example, deleted, so no cluster resource for that virtual machine is available any more, the restored virtual machine becomes a local virtual machine running on a node. The reason is missing cluster resource configuration that cannot be restored by Data Protector. The virtual machine requires manual configuration to become a cluster virtual machine again, which is performed as follows:

1. Make sure the virtual machine is powered off.
2. In the Server Manager, expand **Features**, **Failover Cluster Manager**, and the virtual server, right-click **Services and applications**, and click **Configure a Service or Application**.
3. In the Select Service or Application page of the High Availability Wizard, select **Virtual Machine** and click **Next**.
4. In the Select Virtual Machine page, select the virtual machine you want to configure and click **Next**.
5. In the Summary page, review your planned changes and click **Finish**.

Restoring a replicated virtual machine

Re-enabling the replication

After restoring a VM (primary or replica VM), you must manually re-enable the replication:

1. Disable replication for the VM on the primary server. The replication state there will be `Failed`.
2. Enable replication for the VM on the primary server and in the Enable Replication wizard go to the page Choose Initial Replication Method and select **Use an existing virtual machine on the Replica server as the initial copy**.

Reverting a restored replica VM to an application-consistent recovery point

After the restore of a replica VM, the replication state of the VM is `FailedOverWaitingCompletion`. To revert the VM to a selected recovery snapshot:

1. Use the Hyper-V Manager or the Failover Cluster Manager to cancel the failover. If the latest VM state is the desired restore state, then the VM replication can be directly removed.
2. Initiate a new failover. In the Failover window, select the appropriate recovery point and click **Fail Over**. The VM is reverted to the selected recovery point and automatically started.

Restoring using another device

You can restore using a different device than used for the backup. For details, see the *HP Data Protector Help* index: “restore, selecting devices for”.

Monitoring sessions

You can monitor currently running sessions from any Data Protector client with the `User Interface` component installed, from the Data Protector GUI. When you run a backup or restore session, a monitoring window shows the session progress. Closing the GUI does not affect the session. You can also monitor sessions using the Monitor context of the GUI.

For details on monitoring, see the *HP Data Protector Help* index: “viewing currently running sessions”.

Troubleshooting

This section lists general checks and verifications, plus problems you might encounter when using the Data Protector Virtual Environment integration.

For troubleshooting information for the Data Protector Microsoft Volume Shadow Copy Service integration, see the *HP Data Protector Integration Guide for Microsoft Volume Shadow Copy Service*.

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

Before you begin

- Ensure that the latest official Data Protector patches are installed. On how to verify this, see the *HP Data Protector Help* index: “patches”.
- For general Data Protector limitations, as well as recognized issues and workarounds, see the *HP Data Protector Product Announcements, Software Notes, and References*.

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

Checks and verifications

If your browsing operation or a backup or restore session failed:

- Examine system errors reported in the `debug.log` located in the default Data Protector log files directory.
- Check if you can do a filesystem backup and restore on the problematic client. For information, see the *HP Data Protector Help*.

Problems

Problem

Backup session for a Microsoft Hyper-V virtual machine fails

When backing up a Microsoft Hyper-V virtual machine, the session ends unexpectedly with an error similar to the following:

```
[Major] From: OB2BAR_VSSBAR@computer.company.com "MSVSSW"
Time: 2/1/2011 11:29:03 AM [145:575]
Writer 'Microsoft Hyper-V VSS Writer' failed to prepare files
for backup:
      Reported state:      VSS_WS_FAILED_AT_POST_SNAPSHOT
      Expected state:      VSS_WS_WAITING_FOR_BACKUP_COMPLETE
      Failure code:        VSS_E_WRITERERROR_NONRETRYABLE
```

The following are possible causes:

- Automatic mounting of new volumes is disabled on the Microsoft Hyper-V system. For details, see http://support.microsoft.com/kb/2004712.
- There are issues inside the virtual machine, such as insufficient storage space for shadow copies, usage of a non-NTFS filesystem, and so on.

Action

Check if automatic mounting of new volumes is enabled on the Microsoft Hyper-V system. For example:

```
diskpart.exe
Microsoft DiskPart version 6.1.7600
Copyright (C) 1999-2008 Microsoft Corporation.
On computer: TPC021

DISKPART> automount
Automatic mounting of new volumes enabled.
```

If automatic mounting is disabled, enable it by executing the following command:

```
MOUNTVOL /E
```

If the issue persists even though automatic mounting is enabled, check the application log files inside the virtual machine to determine the cause.

Problem

In a CSV environment, a backup session fails

When backing up virtual machines with files located on Cluster Shared Volumes, the session fails with an error similar to the following:

```
[Major] From: OB2BAR_VSSBAR@tpc049.company.com "HyperV"  Time: 2/18/2011 3:53:09
PM
        Cannot perform backup of:
        /Microsoft Hyper-V VSS Writer/Virtual Machines/Backup Using Child
Partition Snapshot\vmw39192',
        which contains data in:
                C:\ClusterStorage\Volume3\vmw39192\Virtual Machines\1FC08961-
08B8-4AC5-BDE8-AF4E2AAA07E8.xml
                C:\ClusterStorage\Volume3\vmw39192\Virtual Machines\1FC08961-
08B8-4AC5-BDE8-AF4E2AAA07E8\*
                C:\ClusterStorage\Volume3\vmw39192\vmw39192.vhd
[Major] From: OB2BAR_VSSBAR@tpc049.company.com "HyperV"  Time: 2/18/2011 3:53:09
PM
        There is no data to be backed up.
```

This problem appears if two sessions attempt to back up virtual machines from the same CSV at the same time. Since the first session locks the CSV, the second session cannot access the CSV and consequently fails.

Action

Run the sessions one after the other.

Problem

Browse operation or a backup or restore session fails due to a wrong password

When the application system and the backup host are the same system, the configuration check of the username and password is not performed. Actually, in such a setup, the configuration check always appears to succeed even when the credentials are invalid, and the subsequent browse, backup, and restore operations will function. However, when a non-local connection is established, for example, when a different backup host is used, the operations will fail due to a wrong password.

Action

Configure backup host that is not the application system at the same time.

Problem

The Data Protector Inet service configuration is missing

During a restore session, a message similar to the following is reported in the session output:

```
[Warning] From: INET_thread_vepa_bar.exe@tpc040.company.com
"tpc040.company.com"  Time: 2/18/2011 5:24:05 PM
        No data for user ADMINISTRATOR@DOMAIN in Inet's impersonation
configuration.
```

Action

None. You can safely ignore the message.

Problem

Data Protector cannot restore a file

During a restore session, a message similar to the following is displayed:

```
[Major] From: OB2BAR_VSSBAR_COMP@tpc021.company.com
"HyperV"  Time: 3/3/2011 2:05:35 PM
Cannot restore file
'C:\ProgramData\Microsoft\Windows\Hyper-V\Virtual Machines
\8F74F8EE-E93A-4CD3-998F-3324784ED932.xml'.
Failed with error: '[33] The process cannot access the file because
another process has locked a portion of the file.'

[Major] From: OB2BAR_VSSBAR_COMP@tpc021.company.com "HyperV"
Time: 3/3/2011 2:05:35 PM
[145:221]   Restore of component
'/Microsoft Hyper-V VSS Writer/Virtual Machines/
Backup Using Child Partition Snapshot\VM_name' failed.
```

Action

Restart the restore without cleaning up the files that have already been restored.

Problem

During restore of data on CSV, data is sent through the LAN instead of the SAN

Due to a Microsoft limitation, during restore of virtual machine files on Cluster Shared Volumes (CSV), in some cases data is sent through the LAN instead of the SAN, which may increase the restore time. This happens when a node other than the coordinator node is used for data transfer.

Action

Before starting a restore, make sure the coordinator node is used for the restore. Perform either of the following:

- In Windows Server Manager, check which node is currently the coordinator node, and select that node for the restore in Data Protector.
- In Windows Server Manager, manually switch coordination to the node you wish to use for the restore.

Problem

Warning event ID 5605 is logged in the Windows Application Event Log

The warning appears when the Virtual Environment integration for Microsoft Hyper-V connects to the cluster namespace. The session completes successfully nevertheless.

Action

None. You can safely ignore the warning. For details, see the Microsoft KB article 2590230 at support.microsoft.com/kb/2590230.

Problem

After a backup session, the VM replication state is "Error" and health is "Critical"

During a Data Protector backup session the Hyper-V service locks the virtual machine to prevent inconsistencies. On the primary Hyper-V server it logs an error and a warning in the Windows Event Log:

```
Hyper-V failed to replicate changes for virtual machine 'vmw38078' (Virtual
Machine ID FBCDBFDF-ACBD-4A01-BA8D-A4A9CF597651). Hyper-V will retry replication
after 5 minute(s).
```

On the replication server side, the Hyper-V service logs multiple errors in the Windows Event Log:

```
Hyper-V failed to apply replication logs for 'vmw38078': Operation aborted
(0x80004004). (Virtual Machine ID FBCDBFDF-ACBD-4A01-BA8D-A4A9CF597651)
```

By default, the Hyper-V service retries the replication every five minutes for a maximum of one hour. If it is not possible to perform a successful replication within this time frame because the backup of the VM takes longer than that, the replication remains in the `Error` state and with health status set to `Critical` and the Hyper-V service no longer attempts to automatically resynchronize the VMs.

Action

Change the time interval in which Hyper-V is allowed to automatically resynchronize replica VMs.

For example, to change the interval to five hours, execute the following PowerShell command:

```
Set-VMReplication –VMName VMName -AutoResynchronizeEnabled $true -
AutoResynchronizeIntervalStart 00:00:00 -AutoResynchronizeIntervalEnd 05:00:00
```

Problem

Backup session fails when triggered after a restore session that involves a restore chain

After you start a Data Protector session that restores data from incremental backup images, a subsequent backup session fails after reporting an error similar to the following in the session output:

```
[Major] From: OB2BAR_VSSBAR@computer.company.com "HyperV"  Time: 5/14/2012
10:50:18 AM
[145:575]      Writer 'Microsoft Hyper-V VSS Writer' failed to prepare files for
backup:
```

```
Reported state:      VSS_WS_FAILED_AT_POST_SNAPSHOT
Expected state:      VSS_WS_WAITING_FOR_BACKUP_COMPLETE
Failure code:        0x80042336
```

When you inspect the operating system's event log, there is an event of the Windows Logs category with ID `10145` logged in it.

The root cause of the failure may be Data Protector's prevention of inconsistent data from being backed up. When Data Protector processes a Microsoft Hyper-V restore chain, thus one or more incremental backup images, data from each such image is merged into the base backup image. The automatic merge process is performed by Microsoft Hyper-V and is asynchronous to the Data Protector restore session. It may continue to run in the background after the session finishes. When a backup session for the involved virtual machines is invoked before merging is complete, Data Protector detects it and aborts the process to avoid inconsistencies in the backup image.

Action

Restart the problematic backup session at a later time or adjust the session schedule accordingly.

Problem

Restore session fails when restoring to an SMB share with insufficient privileges

When restoring to an SMB file share Data Protector needs sufficient privileges to change the owner of files on the File Server. If the Data Protector agent is not allowed not modify the owner, then an error is reported similar to the following:

```
[Major] From: OB2BAR_VSSBAR_COMP@hyperv.example.com "HyperV" Time: 5/13/2013
3:23:09 PM

Cannot restore file '\\fileserver.example.com\share4vms\local_vm\Virtual
Machines\A9321AEE-EC69-4F79-BB34-59BA97D83CAC.xml'.

Failed with error: '[1307] This security ID may not be assigned as the owner of
this object.'
```

Action

Run the Data Protector Inet service on the Hyper-V host under a domain user with sufficient privileges, or add the computer account of the Hyper-V host to the Administrators group of the File Server.

Part 3: Citrix XenServer

Data Protector offers a script solution to back up Citrix XenServer data online.

- ***Data Protector Citrix XenServer script solution***

  This solution is based on the standard Data Protector filesystem backup functionality.

  See Data Protector Citrix XenServer script solution on page 168.

Note: You can also back up Citrix XenServer virtual machines using the common Data Protector filesystem backup functionality, which operates on the file level. Consequently, the smallest object that you can back up or restore is a file. However, to ensure data consistency, you must take virtual machines offline before starting a backup session.

Chapter 3: Data Protector Citrix XenServer script solution

Introduction

This chapter describes a script based solution that, when used together with standard Data Protector functionality, enables online and offline backup and restore of **Virtual Machines** hosted on a **Citrix XenServer**. For the supported version of Citrix XenServer for your version of Data Protector, see the latest support matrices at http://support.openview.hp.com/selfsolve/manuals.

Integration concepts

Types of backup

Using this integration, you can perform both online and offline backups. In both cases, only full backups of virtual machines are available.

Online backup

Online backups are performed without stopping the virtual machines concerned, using the snapshot functionality available on the Citrix XenServer. By creating a snapshot of a virtual machine, a copy of the whole virtual machine is created, using the capabilities of the underlying storage repository and is saved as a template virtual machine. This template can subsequently be used to restore the disks of the original virtual machine, or to create new virtual machines as exact copies of the original at the time of the snapshot.

- **online** . The user selects which virtual machine, or virtual machines, Data Protector should back up without disturbing their power state(s).
- **allOnline** . Data Protector backs up all virtual machines present in the XenServer without disturbing their power states.

Note: The types of storage repositories for which online backup is supported is dependent on the version of XenServer that you are using. See Special considerations on page 185.

Online backup is available for Virtual Hard Disk (VHD), Netapp and EqualLogic storage repositories.

Offline backup

Offline backups are performed after first shutting down the virtual machines concerned. The complete virtual machine is then saved as an `.xva` file using the Citrix export functionality. This file

can subsequently be imported into any XenServer to create a new machine equivalent to the one exported.

- **offline** . The user selects which virtual machine, or virtual machines, should be suspended and backed up.
- **allOffline** . All the virtual machines present in the XenServer are sequentially suspended and backed up.

Disaster recovery

For disaster recovery, you need a backup of the disks that a virtual machine uses plus the metadata for the virtual machine. With this integration, this is only possible with offline backup.

Backup processes

Online backup

The process used by the integration script for an online backup is as follows:

1. Check that snapshot operation is allowed for all the disks of the virtual machine.
2. Snapshot the virtual machine.
3. Export the snapshot to the temporary backup folder as an `.xva` file.
4. Delete the snapshot.

After the script has finished, the contents of the temporary backup folder are backed up to the backup device using standard Data Protector functionality.

Offline backup

The process used by the integration script for an offline backup is as follows:

1. If the virtual machine to be backed up is running, stop it.
2. Export the virtual machine to the temporary backup folder as an `.xva` file.
3. If the virtual machine was running before the backup, restart it.

After the script has finished, the contents of the temporary backup folder are backed up to the backup device using standard Data Protector functionality.

Note: The file type of the exported file for offline backup is the same as that for online backup, but it is possible to differentiate between offline and online backups from the filename. See Specifying a restore on page 183.

Types of restore

The type of restore that can be performed is dependent on the type of backup that was performed: Restore from online backup requires a different process to restore from offline backup.

The following restore possibilities are available:

- **Restore from online backup** . In a similar way to online backup, this has two options available:
  - **online** . This mode allows a user to restore the disks of selected virtual machines that were backed up in a session using backup mode `online` or `allOnline`.
  - **allOnline** . This mode allows a user to restore the disks of all the virtual machines backed up in a session using backup mode `online` or `allOnline`.
- **Restore from offline backup** . In a similar way to offline backup, this has two options available:
  - **offline** . This mode allows a user to restore selected virtual machines that were backed up in a session using backup mode `offline` or `allOffline`.
  - **allOffline** . This mode allows a user to restore all virtual machines that were backed up in a session using backup mode `offline` or `allOffline`.

Note: The disks or virtual machines available for restore can be influenced by selections made within the Data Protector GUI. See Selection of files to restore on page 184.

Restore processes

Restore from online backup

First, Data Protector restores the selected contents from the relevant backup session to the temporary backup folder.

Then, the integration script uses the following process to perform the restore from online backup:

1. Ensure that the virtual machine is present and stopped.
2. Delete the old disks of the virtual machine.
3. Import the `.xva` file containing the snapshot from the temporary backup directory.
4. Restore the disks of the virtual machine using the disks from the snapshot.

Restore from offline backup

First, Data Protector restores the selected contents from the relevant backup session to the temporary backup folder.

Then, the integration script uses the following process to perform the restore from offline backup:

1. If present, ensure that the virtual machine is stopped.
2. Delete the old virtual machine.
3. Import the `.xva` file from the temporary backup directory, activating the restore option.

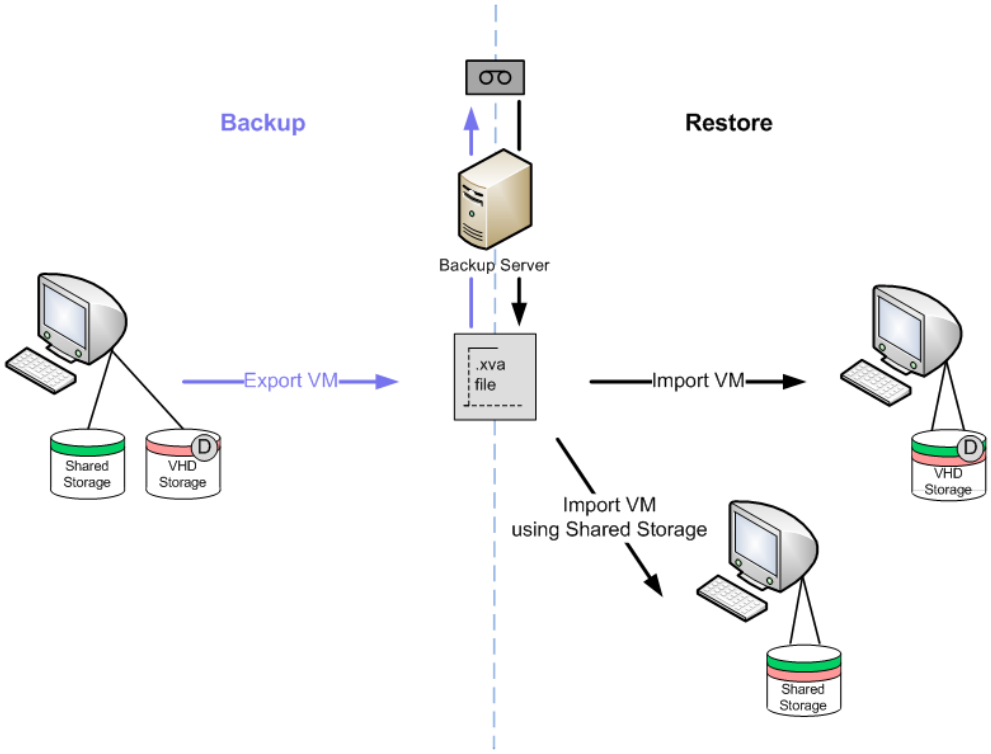
   The import operation of XenServer converts the `.xva` file into a virtual machine and sets the virtual machine in the same power state as it was during the export. When the restore option is set to true, the MAC of the old virtual machine is preserved

Note: The file type of the backup file for offline backup is the same as that for online backup, but it is possible to differentiate between offline and online backups from the filename. See Specifying a restore on page 183.

Restore considerations

When a restore is performed, the original storage repositories used by the virtual machine are not known, so the user must specify in which storage repository the restore should be performed. If no storage repository is specified, the virtual machine will be restored in the default storage repository. Consider Example backup and restore on the next page.

Figure 67: Example backup and restore



On the left side is a virtual machine with two disks: One disk uses the shared storage repository and the other the default storage repository.

When this virtual machine is backed up, an `.xva` file is produced.

When the virtual machine is subsequently restored, two options are available:

- A storage repository is not specified. In this case, both disks are restored into the default storage repository.
- A storage repository is specified. In this case, both disks are restored into the specified storage repository. For example, if the Shared Storage repository is specified, both disks are restored into the Shared Storage repository.

This means that the virtual machine can be restored successfully, but it is only possible to restore the disks to a single storage repository, regardless of the original configuration.

Main integration components

To function, this integration requires the following components:

- Supported Citrix XenServer
- HP Data Protector client(s) with:

- Disk Agent
- Media Agent

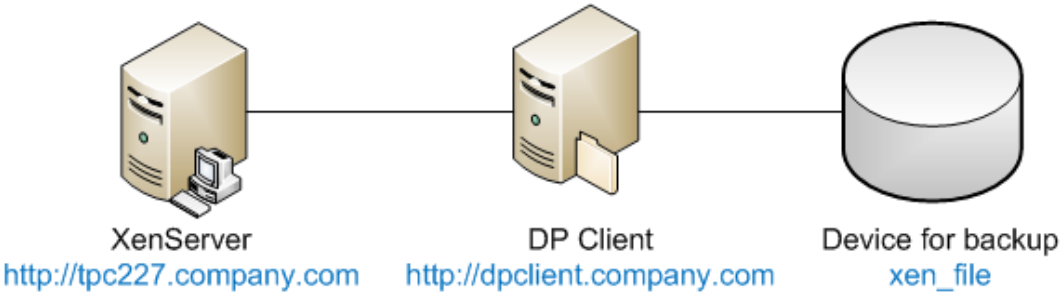
- Integration scripts

A simple example layout for these components (with both Disk Agent and Media Agent on the same Data Protector client) is shown in Example layout below.

No scripts are installed on the Citrix XenServer, but its export facility is used by the integration scripts. The integration scripts themselves are all installed on the Data Protector client with the Disk Agent installed.

During backup, virtual machines, or virtual machine disks, are exported to the Disk Agent host and backed up using Data Protector. The device used for the backup can be any device supported by Data Protector for file-system backup.

Figure 68: Example layout



Installation of the integration

This section gives detailed instructions for the installation of the XenServer integration.

Prerequisites

The machine on which the integration is to be installed must be a Data Protector client (shown as DP Client in Example layout above) with the Data Protector Disk Agent installed and must be a member of a Data Protector Cell. For further details, see the *HP Data Protector Installation and Licensing Guide*.

The Data Protector Disk Agent must be installed first, since other software must be installed in specific Data Protector directories.

The following software must then be installed on the Disk Agent host:

- Python version 2.5.x or 2.6.x (available from http://www.python.org/download). This must be installed first. (Also, see the note regarding Pycurl below.)

  Install the software in the following directories:

Windows systems: *Data_Protector_home*\bin

Linux systems: /opt/omni/bin

- Curl with libcurl version 7.18.x or 7.19.x (available from http://curl.haxx.se/download.html).

  Note that the package installed must contain libcurl.

- Pycurl (available from http://pycurl.sourceforge.net/).

  If you prefer there are some compiled versions available from:

  Windows systems: http://pycurl.sourceforge.net/download/

  Linux systems: http://rpm.pbone.net/index.php3

  Note: The installers may require a Python version earlier than the latest available, so it is best to check the situation before installing Python. For example, the fact that the pycurl-ssl-7.18.2.win32-py2.5.exe contains the string py2.5 implies that python 2.5 is required.

- xenAPI.py for the version of XenServer that you are using (available from http://community.citrix.com/display/xs/Download+SDKs)

Tip: Note the full installation directory of python. You will need this later when calling the Data Protector Pre-exec and Post-exec scripts. For this documentation it is assumed to be:

Windows systems: *Data_Protector_home*\bin\Python25\

Linux systems: /opt/omni/bin/Python25/

Installation of the integration scripts

The following scripts are supplied for the integration:

- DPxen_config.py
- DPxen_operations.py
- DPxen_backup.py
- DPxen_restore.py
- DPxen_postbackup.py

They are available as follows:

- For Data Protector 8.10, on the Data Protector 8.10 installation DVD-ROM in the directory:

  Windows systems: `Windows_other\Xen_sup`

  Linux systems: `Xen_sup`

- For other versions of Data Protector for which the integration is supported, as an installation package that can be downloaded:

  a. Go to http://www.hp.com/go/dataprotector.

  b. Click **SUPPORT & DRIVERS** at the top of the webpage.

  c. On the Support & Drivers webpage, click **Drivers & Software**.

  d. In the text box, enter Data Protector and click **SEARCH**.

  e. In the search results list, click the Data Protector version with which you will be using the integration.

  f. Select **Cross operating system (BIOS, Firmware, Diagnostics, etc.)**

  g. In the Software – Solutions section, click **Data Protector Release <Version> / Xen Server integration packet** and download the installation package from the subsequent page.

- When you have obtained the scripts, install them as follows:

1. If you have downloaded the package, unzip `xenServer_backup_solution.zip`.
2. Copy all of the scripts to your preferred location on the Data Protector Disk Agent host. For security reasons, the following locations are recommended:

   Windows systems: *`Data_Protector_home`*`\bin`

   Linux systems: `/opt/omni/bin`

   Make a note of this location: You will need it later.

3. If you do not already have the `xenAPI.py` file:

   a. Go to http://community.citrix.com/display/xs/Download+SDKs.

   b. Go to the download section for the version of XenServer that you are using.

   c. Download the `XenAPI.py`.

4. Copy `XenAPI.py` to the same location as the integration scripts.
5. Create a folder with read and write permissions, for temporary use during backup. Create the folder as follows:

Windows systems: `C:\tmp\backup\`

Linux systems: `/tmp/backup/`

Important: It is the contents of this directory that will actually be backed up to the backup device by Data Protector. It must therefore have enough space available to cope with your largest likely backup. For instance, if you want to be able to back up all the virtual machines on your XenServer in one operation, there must be enough space for all of them. The folder will be referred to as the **temporary backup folder** in these instructions.

Integration script functions

The integration components, supplied in the `xenServer_backup_solution.zip` file, and their purposes are described below:

- **DPxen_config.py** - This is the default configuration file for backup and restore operations using the integration. It is the only file that should be changed by the user, to match particular work scenarios. For details of setting up its contents, see Updating configuration script DPxen_config.py for backup on the next page and Updating configuration script DPxen_config.py for restore on page 181.

  For convenience, you can create your own versions of this file, with your own names, for instance myBackupConfig and myRestoreConfig, and specify these when calling the main scripts `DPxen_backup.py` and `DPxen_restore.py`.

- **DPxen_operations.py** - This contains same auxiliary functions that are used during backup and restore, for example, functions to import or export a virtual machine, to find a virtual machine by name, and so on.

- **DPxen_backup.py** - This controls obtaining the files to back up from the XenServer, according to the parameters specified in the configuration file, and writing them to the temporary backup folder ready for backup by Data Protector. If snapshots are created during the backup process it also deletes them afterwards.

  This script can be called with the name of the configuration file as an argument, which allows you to use your own configuration file. If called without an argument, the default configuration file, `DPxen_config.py` is used.

- **DPxen_restore.py** - This restores the files saved during the backup in the XenServer. It also deletes all the auxiliary elements created during a restore in the XenServer. The files restored by Data Protector to the temporary backup folder are not deleted by this script. This script also accepts as an argument the name of the configuration file to use.

- **DPxen_postbackup.py** - This can be used to delete the contents of the temporary backup folder. It should be run after completion of a backup session as a cleanup operation. Alternatively, it could be used to delete the contents of the temporary backup folder before a restore session.

Backup using the integration

To produce a backup using the integration, you need to perform the following operations:

1. Update the configuration script `DPxen_config.py`, or your own equivalent.
2. Ensure that the temporary backup directory is empty.
3. Set up a Data Protector backup specification.
4. Run the backup specification (or schedule it in the specification).

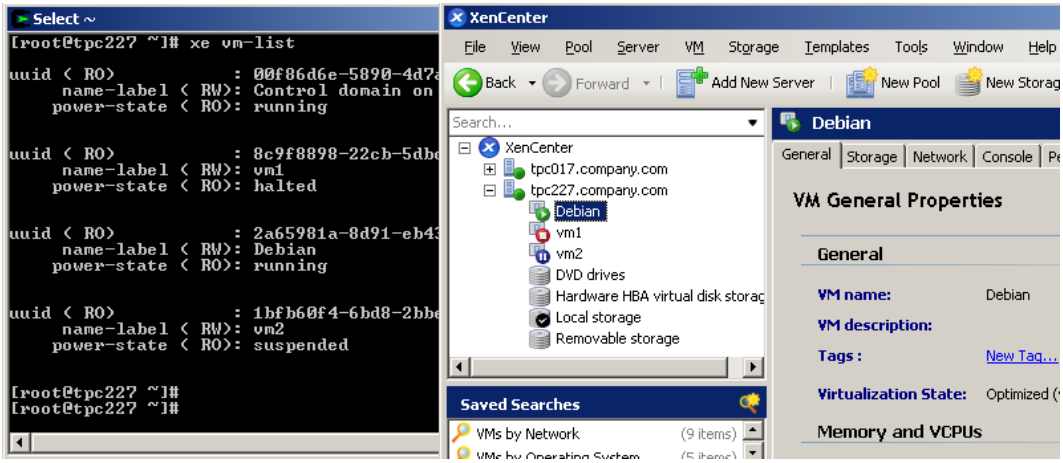
These operations are described in this section.

Updating configuration script DPxen_config.py for backup

In the configuration file `DPxen_config.py`, or a configuration file with a name of your own, you can specify the following parameters required to perform the backup:

Mode	The type of backup to be used and whether all, or only specified virtual machines are to be backed up. Valid options are: `online`, `allOnline`, `offline`, and `allOffline`. For explanations of these options, see Integration concepts on page 168.
url	The URL of the XenServer containing the virtual machines to be backed up.
username	The username of a user with the required access rights to the XenServer.
password	The password of the user specified in *username*.
vmName	A list containing the names of the virtual machines to be backed up. If you specify `online` or `offline` for the Mode parameter, you must specify the names of the individual virtual machines that you want to back up. The format of the list is: `["name1", "name2",...]` The names can be obtained from the command line interface on the XenServer (running the `xe vm-list` command) or from the XenCenter interface, as shown in Obtaining the names of the virtual machines on the next page. If you specify `allOnline` or `allOffline` for the *Mode* parameter, this parameter will be ignored.
debug	A Boolean value that should be set to `True` if you want to create a debug file during the backup.
sr	This parameter is used for restore only. It is ignored during backup operations and can be left out for backup, if preferred.

Figure 69: Obtaining the names of the virtual machines



Once you have all the information for those parameters you can proceed to change the `DPxen_config.py` file or create a new configuration file.

Example backup configurations

- Suspend and backup the Debian virtual machine, without creating a debug file.

```
Mode = "offline"
url = "http://tpc227.company.com"
username = "user"
password = "myPassword"
vmName = ["Debian"]
debug = False
sr = ""
```

- Suspend and backup all the virtual machines present in the XenServer and create a debug file. The debug file will be created in `/tmp/` or `C:/tmp/`.

```
Mode = "allOffline"
url = "http://tpc227.company.com"
username = "user"
password = "myPassword"
vmName = []
debug = True
sr = ""
```

- Backup the virtual machines Debian and vm2 in hot mode, creating a debug file.

```
Mode = "online"
url = "http://tpc227.company.com"
username = "user"
password = "myPassword"
vmName = ["Debian", "vm2"]
```

```
debug = True
sr = ""
```

- Backup all the virtual machines present in the XenServer, without changing their power state. When the *Mode* selected is `allOnline` or `allOffline`, the value of the *vmName* parameter is ignored so its value is not important. In this example a debug file will not be created.

```
Mode = "allOnline"
url = "http://tpc227.company.com"
username = "user"
password = "myPassword"
vmName = []
debug = False
sr = ""
```

Creating a backup specification

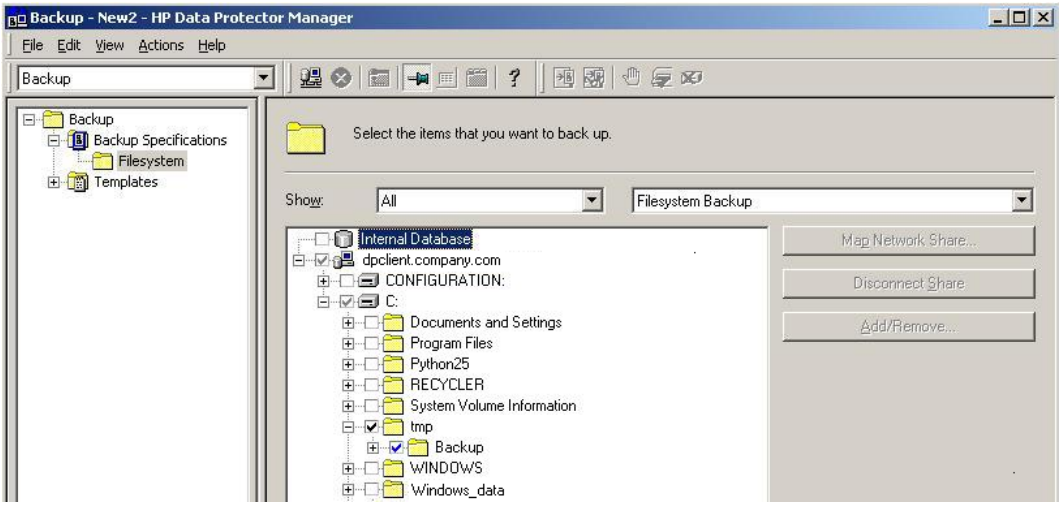
In the Data Protector GUI, create a filesystem backup specification:

1. Select the **Backup** context and expand **Backup Specifications**.
2. Right click on **Filesystem** and select **Add Backup**.
3. Select a **Blank Filesystem Backup** template and click **OK**.
4. Select the item to be backed up. In this case, you must select the temporary backup folder that was created during the installation process:

   Windows systems: `C:\tmp\backup`

   Linux systems: `/tmp/backup`

   Figure 70: Temporary backup folder selection



5. Click **Next**.
6. Select the backup device on which the backup will be performed and click **Next**.
7. In Backup Specification Options, click **Advanced**.
8. In the Backup Options window, make the following entries in the Pre-exec and Post-exec sections:

   Pre-exec: *PythonDirectory*\python.exe *ScriptPath*\DPxen_backup.py [*ConfigFile*]

   On client: myDPClient.com

   Post-exec: *PythonDirectory*\python.exe *ScriptPath*\DPxen_postbackup.py

   On client: myDPClient.com

   where:

   - *PythonDirectory* is the name of the directory containing the python interpreter, for example, Python25. Python must be installed in the correct location, as described in Prerequisites on page 173.

     Note: If the integration scripts have been installed on the Cell Manager, the *full* path must be given. For example, *Data_Protector_home*\bin\Python25.

   - *ScriptPath* is the full path of the integration scripts, for example, *Data_Protector_home*\bin
   - *ConfigFile* is an optional parameter for specifying a configuration file with a name of your own. If this is omitted, the default configuration file DPxen_config.py is used.
9. Click **OK** and then **Next**.
10. Schedule the backup in the normal way for a Data Protector backup. Select a backup type of **Full**. Even though incremental backups are shown as available, only full backups are supported for this integration.
11. Click **Next**
12. After reviewing the specification, click **Next**. Note that if you click **Properties** on the review panel, the options tab contains object options, not backup options, so your pre-exec and post-exec entries are not displayed.
13. Click **Save as...**, enter a name for the specification and click **OK**

Restore using the integration

To restore a backup using the integration, you need to perform the following operations:

1. Update the configuration file `DPxen_config.py`, or your own equivalent.
2. Ensure that the temporary backup directory is empty.
3. Specify a Data Protector restore.
4. Perform the restore.

These operations are described in this section.

Updating configuration script DPxen_config.py for restore

In a similar way to with backup, the configuration file `DPxen_config.py`, or a configuration file with a name of your own, must be used to specify the parameters required to perform a restore:

Mode	The type of restore to be performed and whether all, or only specified virtual machines are restored. Valid options are: `online`, `allOnline`, `offline`, and `allOffline`. For explanations of these options, see Integration concepts on page 168.
url	The URL of the XenServer to which virtual machines are to be restored.
username	The username of a user with the required access rights to the XenServer.
password	The password of the user specified in *Username*.
vmName	A list containing the names of the virtual machines to be restored. If you specify `online` or `offline` for the *Mode* parameter, you must specify the names of the individual virtual machines that you want to restore. The format of the list is: `["name1", "name2",..]` If you specify `allOnline` or `allOffline` for the *Mode* parameter, the *vmName* parameter is ignored.
debug	A Boolean value that should be set to `True` if you want to create a debug file during the restore.
sr	The name of the storage repository to which you want to restore the virtual machine (s) specified in the *vmName* parameter. This does not have to be the same storage repository as the one in use when the virtual machine was backed up. If the specified value is blank (`sr = ""`) the restore is performed to the default storage repository. **Important:** You must have a default storage repository defined if you leave this parameter blank for a restore, otherwise the restore will fail.

Example restore configurations

- Restore the Debian virtual machine, which was backed up using `offline` mode, into the default storage repository. Create a debug file.

```
Mode = "offline"
url = "http://tpc227.company.com"
username = "user"
password = "myPassword"
vmName = ["Debian"]
debug = False
sr = ""
```

- Restore all the files backed up in the selected session into the default storage repository. The backup was performed in `offline` mode. Create a debug file.

```
Mode = "allOffline"
url = "http://tpc227.company.com"
username = "user"
password = "myPassword"
vmName = []
debug = True
sr = ""
```

- Restore the virtual machines Debian and vm2, which were backed up in `online` mode, into the default storage repository and create a debug file.

```
Mode = "online"
url = "http://tpc227.company.com"
username = "user"
password = "myPassword"
vmName = ["Debian", "vm2"]
debug = True
sr = ""
```

- Restore all the virtual machines present in the XenServer, without changing their power state. Create a debug file.

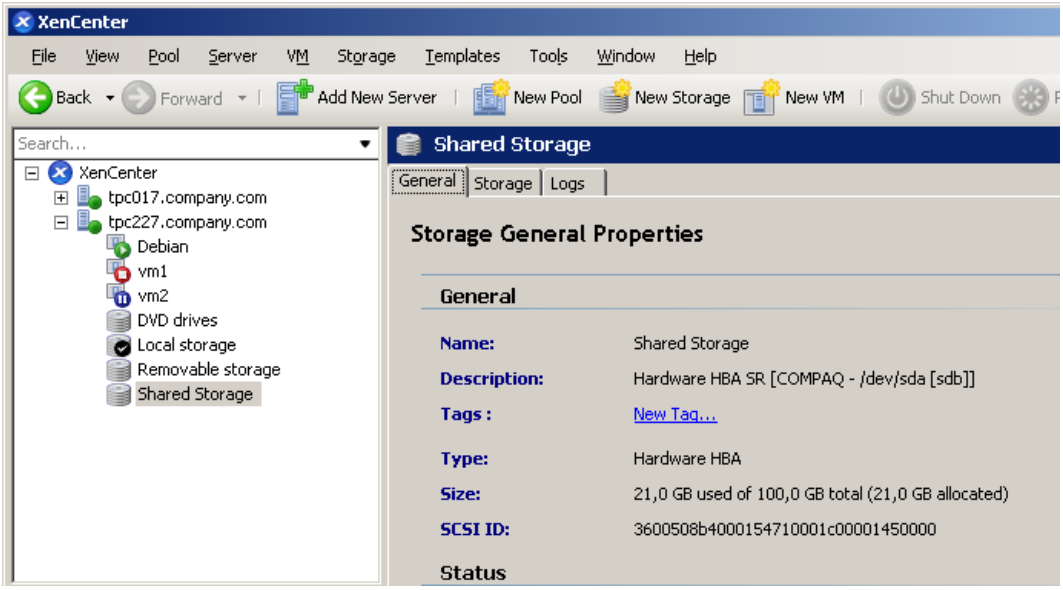
```
Mode = "allOnline"
url = "http://tpc227.company.com"
username = "user"
password = "myPassword"
vmName = []
debug = False
sr = ""
```

- Restore the Debian and vm2 virtual machines, which were backed up using the `offline` mode,

into storage repository "Shared Storage" (see Available storage repositories below). Create a debug file.

```
Mode = "offline"
url = "http://tpc227.company.com"
username = "user"
password = "myPassword"
vmName = ["Debian", "vm2"]
debug = True
sr = "Shared Storage"
```

Figure 71: Available storage repositories



- Restore the Debian virtual machine, which was originally backed up using the `online` mode, into the "Removable storage" storage repository. Do not create a debug file.

```
Mode = "online"
url = "http://tpc227.company.com"
username = "user"
password = "myPassword"
vmName = ["Debian"]
debug = False
sr = "Removable storage"
```

Specifying a restore

1. In the Context List, click **Restore**.
2. In the Scoping Pane, expand **Restore Sessions** to display clients and then the object backed

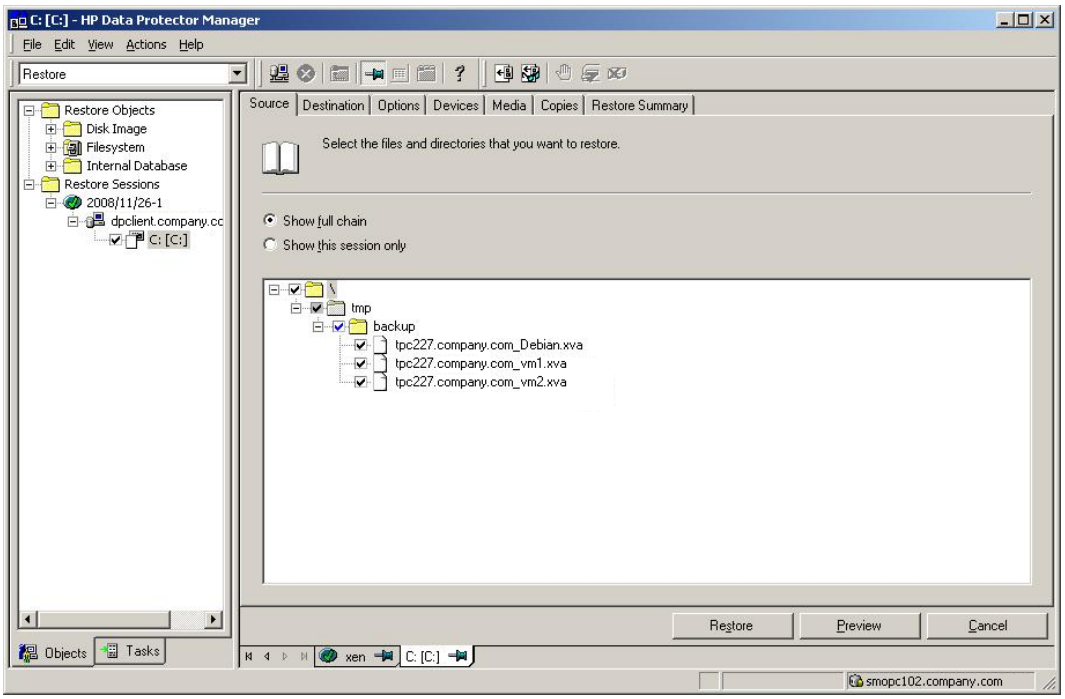
up on those clients (The mount point containing the temporary backup directory you created during the installation process).

3. Click the object to open the property pages.
4. In the Source tab, select the temporary backup directory to view the files available for restore. Note that the filename formats indicate the mode of the backups in the folder, as follows:

   - `offline` or `allOffline`: *`servername_vmName`*`.xva`
   - `online` or `allOnline`: *`servername_vmName`*`_Snapshot.xva`

   Check the file format, to decide the mode of restore required, (it must be equivalent to the type of backup). See Selection of files to restore below.

Figure 72: Selection of files to restore



Important: The Source tab shows the contents of the temporary backup folder when the backup session was performed. It does not show the current contents of the folder. It is important to ensure that the temporary backup folder is empty before performing a restore.

During a restore, the files selected in this tab are first restored to the temporary backup folder. Only files selected here are subsequently available for the restore of virtual machines using the `DPxen_restore.py` script (provided the temporary backup folder was empty beforehand).

5. In the Options tab, in the **Post-exec** field, specify the `DPxen_restore.py` script as follows:

PythonPath\python.exe *ScriptPath*\DPxen_restore.py [*ConfigFile*]

where:

- *PythonPath* is the *full* path of the python interpreter, for example, *Data_Protector_home*\bin\Python25
- *ScriptPath* is the full path of the integration scripts, for example, *Data_Protector_home*\bin
- *ConfigFile* is an optional parameter for specifying a configuration file with a name of your own. If this is omitted, the default configuration file DPxen_config.py is used.

Note: The restore mode specified in the configuration file must be suitable for the filename format of the files in the folder. See the previous point.

6. Click **Restore** and check that the conditions for the restore, summarized in the **Start Restore Session** panel, are correct.
7. When you are sure that the restore is correctly specified, click **Finish** to start the restore.

Notes on restore

- It is possible to perform the restore without specifying a post-exec. In this case, the .xva file is restored to the temporary backup folder only. You can then run the script independently.
- After the restore has completed, the files in the temporary backup folder are not deleted automatically. If you don't require them for any other purpose, it is advisable to delete them.
- When you restore a virtual machine, its UUID changes.

Special considerations

- The online backup performs a snapshot of the virtual machine, but this operation is not always allowed. For XenServer 5.0, at the time of writing, snapshots were supported with VHD, Netapp, or EqualLogic storage repositories only. Any attempt to perform an online backup of a virtual machine that uses a different storage repository will fail and the error message, At least one sr used by *vmName* does not support snapshot, will be displayed in the monitor. If you are performing a backup of multiple virtual machines, only the virtual machines that allow snapshot operation will be backed up.

  For the latest snapshot support with your XenServer version, see the XenServer documentation.

  If you want to convert your default storage repository to file-based VHD-on-EXT3, follow the instructions given in the Citrix forum at http://support.citrix.com/article/ctx116324.

- When you perform an online backup, only the disks of the virtual machines are available for restore, not the metadata. To be able to restore the disks and the metadata, you need to perform an offline backup. The best practice is to perform an offline backup after the metadata of a virtual machine has changed, for example after installing a new application. The rest of the time it is sufficient to perform online backups.

  If only the disks of a virtual machine have been corrupted you only need to restore your latest online backup. If the metadata is corrupted you need to first restore your latest offline backup and then your latest online backup, if newer.

- Before performing a backup, ensure that there is enough space on the Disk Agent host. If there is not enough space, the backup will fail.

Further information

For further information, see http://www.hp.com/go/dataprotector.

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 Integration Guide for Virtualization (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.


Java™
COMPATIBLE