HP StorageWorks EBS Solutions guide for VMware Consolidated Backup with HP Data Protector

Executive summary

This white paper provides technical information and best practices for planning or deploying VMware Consolidated Backup with HP StorageWorks tape libraries.

This white paper is not designed to replace documentation supplied with individual solution components but, rather, is intended to serve as an additional resource to aid the IT professionals responsible for planning a VMware Consolidated Backup environment.

This white paper contains planning information that can help when deploying a VMware Consolidated Backup environment running on HP ProLiant servers, HP blade servers, and HP StorageWorks storage solutions.

Prior to reading this white paper, the reader should understand the architecture of the VMware ESX server and how it virtualizes the hardware (for the architecture guide, information about VMware Consolidated Backup, and for more about how ESX works, see: http://www.vmware.com/products/vi/esx/).

Many of the HP guides, white papers, and technical documents for VMware can be found at http://www.hp.com/go/vmware. This white paper can also be found at http://www.hp.com/go/ebs.

IMPORTANT: The best practices described in this white paper are offered as recommendations, not requirements. The implementation of these best practices has no impact on whether or not your system may be supported by HP. Some of these best practices may not apply to your particular environment.

Audience

The solutions contained in this white paper are intended for solutions architects, engineers, and project managers involved with HP StorageWorks tape libraries with virtualization solutions. The reader should be familiar with networking in a heterogeneous environment, virtualized infrastructures, and have a basic knowledge of VMware Consolidated Backup and HP ProLiant servers, HP StorageWorks products, HP element managers, and ProLiant Essentials products.

The reader should understand the architecture of VMware ESX server 3.0.2 and how this product is able to virtualize hardware as outlined in the *VMware Infrastructure Architecture Overview*, available at: http://www.vmware.com/pdf/vi_architecture_wp.pdf.

Information not provided

This white paper does not provide information on the following:

- Installing and configuring VMware Consolidated Backup—for more information on installing and configuring HP storage hardware or administration software, see the VMware documents titled *Installation and Upgrade Guide* at: http://www.vmware.com/pdf/vi3_installation_guide.pdf and the *Server Configuration Guide* at: http://www.vmware.com/pdf/vi3_server_config.pdf.
- Installing and configuring HP servers and HP StorageWorks tape libraries—for more in-depth information, see the *HP StorageWorks SAN design reference guide* at: http://h20000.www2.hp.com/bc/docs/Support/SupportManual/c00403562/c00403562.pdf and the *HP StorageWorks EBS design guide* at: http://www.hp.com/go/ebs.

Introduction

A key component of an Enterprise Backup Solution (EBS), as envisioned by HP, is to maximize the use of shared resources and consolidation. This section provides more information on these concepts.

HP Enterprise backup environment

Implementing an Enterprise Backup Solution (EBS) can be challenging. HP understands that for any given Storage Area Network (SAN) environment there may be one or more vendor's hardware and software present. Each of these components, including software, servers, interconnects, and target devices must work together. HP EBS is dedicated to providing thorough integration testing of industry standard, heterogeneous, and multi-vendor SAN environments. The output of this work can be found at http://www.hp.com/go/ebs in the *HP StorageWorks Enterprise Backup Solution (EBS) Hardware/Software Compatibility Matrix*, the *HP StorageWorks Enterprise Backup Solution design guide*, and the various software guides and white papers, such as this one.

Virtual infrastructure

The primary benefit to virtualization may indeed be consolidation; however, a virtualized infrastructure can be beneficial in many other ways. For example, because an entire operating environment can be encapsulated in several files, that environment becomes easier to control, copy, distribute, and so on. If an organization virtualizes an operating system, its applications, configuration settings, and other desirable elements, that entire operating environment—known as a Virtual Machine (VM)—can be rolled out anywhere in the organization to maintain business continuity. To maximize availability, emerging technologies can allow VMs to migrate automatically from a potentially failing host to another virtualized platform—this happens with little or no user intervention.

Virtual infrastructure components

VMware ESX server

VMware ESX server is virtual infrastructure software for portioning, consolidating, and managing computing resources. ESX server installs on the "bare metal" and allows multiple, unmodified operating systems and their applications to run in virtual machines that share physical resources.

VMware Virtual Machine

VMware Virtual Machines (VMs) run on ESX servers and emulate various servers based on different operating systems (Windows, Linux, and Solaris). Each virtual machine represents a complete system with processors, memory, networking, storage, and BIOS.

VirtualCenter server

The VirtualCenter server runs a Windows service. The service acts as a central administrator for VMware ESX servers that are connected on a network. VirtualCenter directs actions on the virtual machines and the ESX servers.

VMotion

VMotion is a feature that enables you to move running virtual machines from one ESX server to another without service interruption. All VMotion activities are coordinated by the VirtualCenter server.

VMware Consolidated Backup

VMware Consolidated Backup (VCB) offloads backup responsibility from ESX servers to a dedicated backup proxy (or proxies). This reduces the load on ESX servers. VCB provides full-image backup and restore capabilities for all virtual machines and file-based backups for virtual machines running the Microsoft® Windows® operating systems.

Using VMware Consolidated Backup with HP StorageWorks tape/VTL libraries

VMware ESX server currently does not support SAN-shared tape devices. However, Windows-based VCB proxy servers do provide this functionality and allow the ESX server's data to be backed up to shared tape devices.

Backup and recovery strategy with VMware

VMware adds levels of complexity to existing backup and recovery strategies which lead to questions that should be answered prior to choosing the correct strategy (there may be more questions, depending on a particular environment).

The types of questions that should be asked are:

- Is file-level recovery required?
- Is there application data to back up, such as a database?
- Can the application on the VM be shut down during backup?
- Is there a backup window?
- Is there a locally attached tape device?
- Is there a SAN tape device?
- Are there large numbers of VMs to back up?
- Is VMotion used in the VMware environment?

The following table shows which backup method to use when answering these questions:

Table 1 Backup method to use

	A. ESX virtual disk backups—local tape	B. VM file backups—local tape	C. VCB proxy backup server	D. ESX virtual disk LAN backups to media host	E. VM LAN backups to media host
Requires file-level recovery	No	Yes	Yes (Windows)	No	Yes
Database to back up	Yes (cold)	Yes (hot/cold)	Yes (hot*/cold)	Yes (cold)	Yes (hot/cold)
Backup windows required	Yes	Yes	No	Yes	Yes
Locally attached tape drive	Yes	Yes	No	No	No
SAN-attached tape drive	No	No	Yes	Yes	Yes
Large number of VMs to back up	Not suggested	Not suggested	Yes	Not suggested	Not suggested
VMotion enabled	No	No	Yes	No	Yes

*scripted solution

Integration of tape in VMware data protection processes

Some common methods for integrating tape devices into the VMware data protection process are:

Note: ESX server 3.0.2 does not currently support SAN tape devices on virtual machines.

Note: As of the printing of this document, VMware Consolidated Backup (VCB) only supports VCB proxy on Windows.

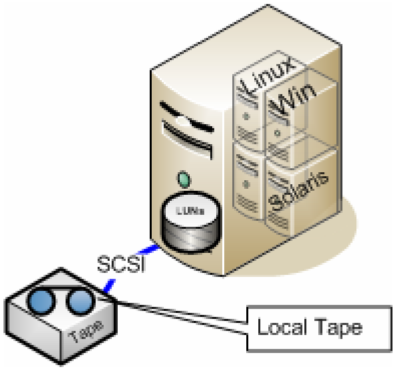
ESX server media host with a local (non-SAN) tape device

With a local tape drive attached to an ESX server media host, the following backup types are recommended:

- Virtual disk backups—ESX server utilities are used to:
  - Take a snapshot of a virtual machine or suspend a virtual machine located on a virtual disk.
  - Back up the snapshot or suspended virtual machine.

The following figure is an example of an ESX server media host with a local tape device:

Figure 1 ESX server media host with a local tape device



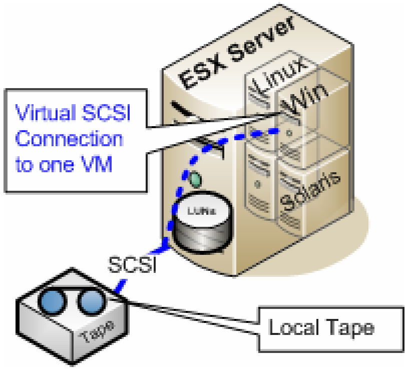
Virtual machine media host with a local (non-SAN) tape device

With a local tape drive presented to a virtual machine, the following backup types are recommended:

- Regular file system backups—Backups are written directly to the local tape drive.

The following figure is an example of a virtual machine media host with a local tape device:

Figure 2 Virtual machine media host with a local tape device



VCB proxy with a local or SAN tape device used as dedicated media host

With a dedicated physical media host, the following backup types are recommended:

- VMware Consolidated Backup (VCB) virtual disk backups—Backups are written to the VCB proxy tape device by using VCB to:
  - – Take a snapshot of the virtual machines located on the virtual disk.
  - – Present the snapshot to the VCB proxy.
  - – Back up the snapshot.

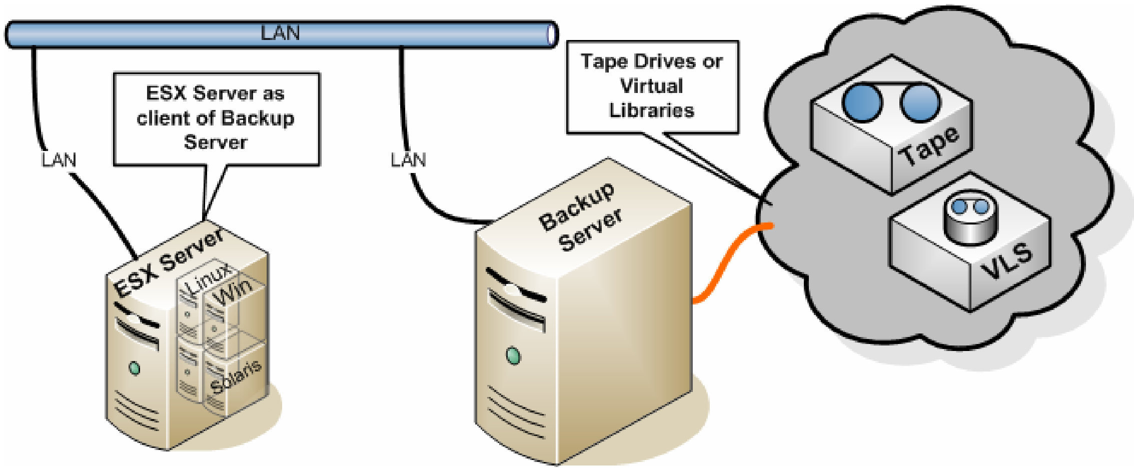
See Figure 5 on page 9 for an example of a VMware Consolidated Backup (VCB) environment.

Virtual disk LAN backups

ESX server virtual disk backups can be accomplished by sending the data over the LAN to a media host.

The following figure is an example of a virtual disk LAN backup:

Figure 3 ESX server virtual disk LAN backup

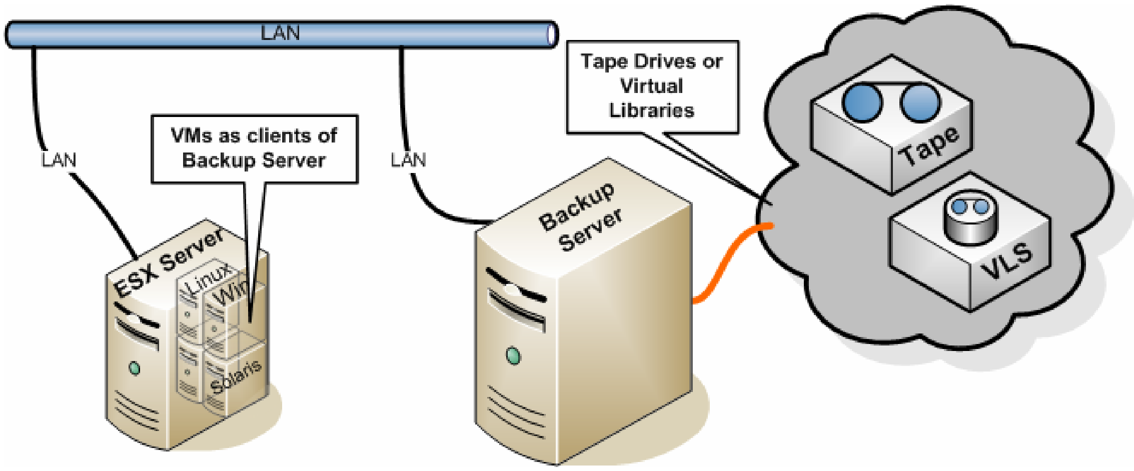

LAN
LAN
ESX Server as client of Backup Server
LAN
Tape Drives or Virtual Libraries
Tape
VLS
Backup Server
ESX Server
Linux
Win
Solaris

Virtual machine LAN backups

Virtual machine file system backups can be accomplished by sending data over the LAN to a media host.

The following figure is an example of a virtual machine LAN backup:

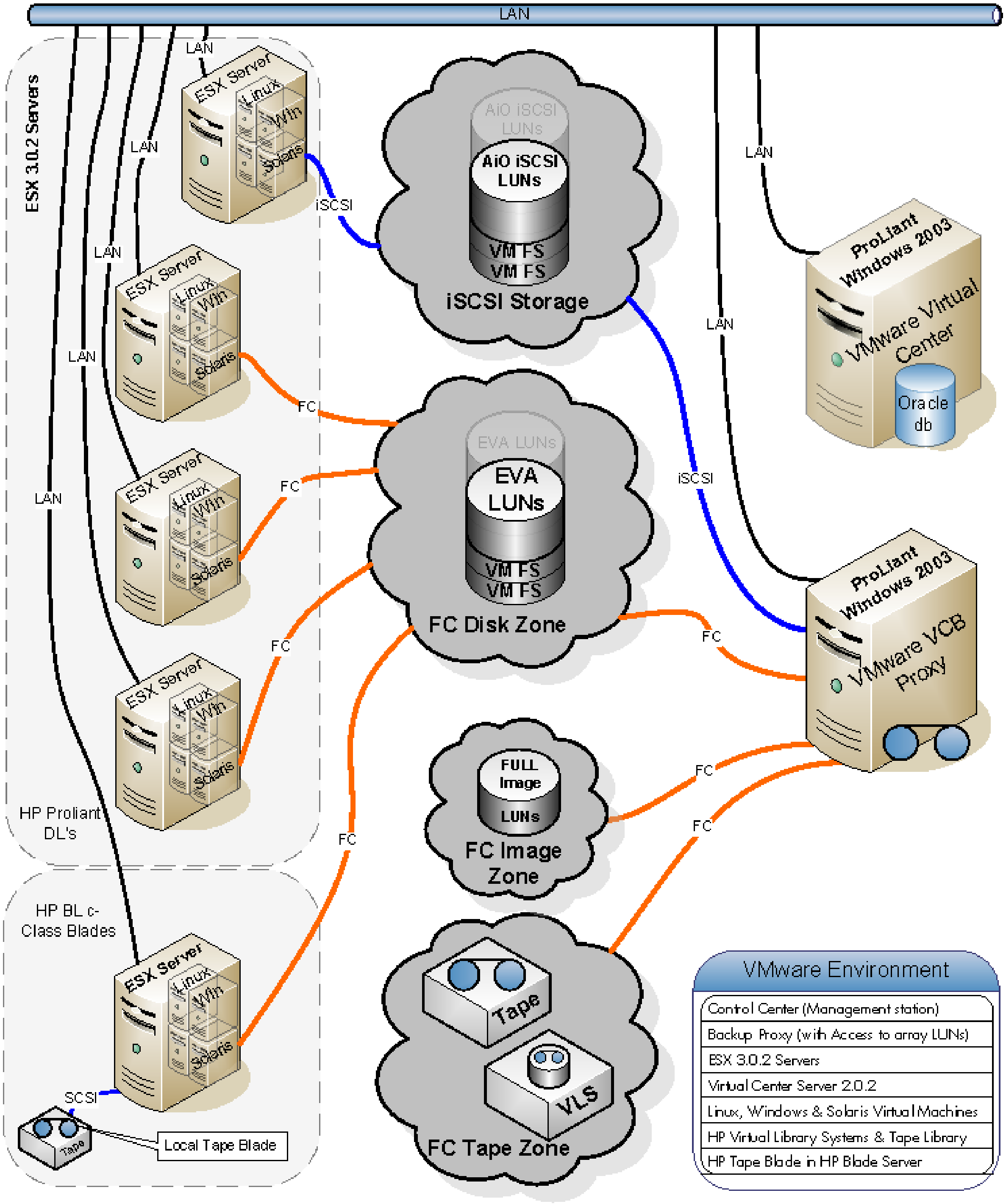
Figure 4 ESX server virtual machine LAN backup


LAN
LAN
VMs as clients of Backup Server
LAN
Tape Drives or Virtual Libraries
Tape
VLS
Backup Server
ESX Server
Linux
Win
Solaris

Test environment

To test the methods listed above, an environment was created that included the latest version of ESX server, a Windows Server 2003 VCB proxy, and virtual machines running Windows, Linux, and Solaris. Figure 5 shows the topology layout of the test environment.

Figure 5 VMware ESX Consolidated Backup environment



Hardware

Table 2 shows the operating systems and HBAs used in the test environment.

Table 2 Operating systems and HBAs in the test environment

Model	Operating system	HBA
HP ProLiant DL380 G4	Windows 2003 (32 bit)	AB379A
HP ProLiant DL380 G4	ESX server 3.0.2	AB379A
HP ProLiant DL380 G5	ESX server 3.0.2	FC2143
HP ProLiant DL380 G5	ESX server 3.0.2	FC2243
HP ProLiant BL460c	ESX server 3.0.2	LPe1105-HP

Table 3 shows the tape libraries and devices used in the test environment.

Table 3 Tape libraries and devices used in test environment

HP StorageWorks model	HP tape drives/quantity
MSL6000	Ultrium 460/2
VLS6000	Virtual Ultrium 960/2
Ultrium 448c tape blade	Ultrium 448 SAS/1

The virtual machine file systems and the virtual machine full images used in the test environment resided on an HP StorageWorks EVA storage array and HP StorageWorks All-in-One iSCSI storage.

Data protection application/software

- Data Protector 6.0 was used as the backup application and was installed on the VCB proxy, ESX servers, and virtual machines.
- VMware Consolidated Backup (VCB) 1.0.3 for ESX server 3.0.2 was installed on the VCB proxy.
- VMware tools were installed on each virtual machine.

Detailed testing of methods

A. ESX server media host virtual disk backups with a local (non-SAN) tape device

An ESX server may have backup application media host software installed. Configured this way, the ESX server can perform backups and restores to a local tape device. An HP test environment was set up to test this type of configuration.

Note: The VMware ESX 3.x integration packet is required for ESX server virtual disk backup with Data Protector. The integration packet can be downloaded from http://www.hp.com/go/dataprotector. Once on the Data Protector website, click on Patches & utilities > Data Protector 6.0 Software > Cross Operating system, and then download the integration packet.

The Data Protector Disk and Media Agents were installed on the ESX server using a Linux Data Protector installation server. To install Data Protector on an ESX server, Secure Shell (ssh) is required and is set up as follows:

1. A public-private key pair must be generated on the installation server by entering:
   ```
   # ssh-keygen -t rsa
   ```
2. The */etc/ssh/sshd_config* file on the ESX server must be modified to permit *root* login by setting *PermitRootLogin* to *yes*.
3. The SSH server service was enabled on the ESX server by entering (this service may already be enabled, in which case the *sshd PID* needs to be sent the *kill -HUP* signal):
   ```
   # excfg-firewall -e sshServer
   ```
4. The public key must be copied from the installation server to the ESX server. The key generated in step 1 was created as */root/.ssh/id_rsa.pub* on the installation server. This key must be copied to the ESX server as */root/.ssh/authorized_keys* by running the following on the installation server:
   ```
   # scp /root/.ssh/id_rsa.pub <ESX_Server>:/root/.ssh/authorized_keys
   ```
5. The ESX server must be added to the SSH list of known hosts on the installation server by running the following on the installation server:
   ```
   # ssh root@<ESX_Server>
   ```
6. The *OB2_SSH_ENABLED omnirc* variable must be set to *1* on the installation server in */opt/omni/.omnirc*.
7. The omni service must be restarted as follows:
   ```
   # service omni stop
   # service omni start
   ```
8. Port 5555 must be opened on the ESX server for incoming and outgoing Data Protector traffic as follows:
   ```
   # esxcfg-firewall –o 5555,tcp,out,DP
   # esxcfg-firewall –o 5555,tcp,in,DP
   ```

After properly configuring SSH, the Data Protector Disk and Media Agents can be installed on the ESX server following standard Data Protector installation server procedures.

Instructions in the HP Storage Data Protector white paper *VMware ESX server 3.x virtual disk snapshot capabilities integrated with Storage Data Protector 5.5 and 6.0* were followed to integrate virtual machine snapshots with Data Protector.

Backups were run as follows:

- A Data Protector backup specification pre-processing script was run on the ESX server to:
  - Suspend the virtual machine or prepare the virtual machine for a hot backup.
  - For a hot backup, take a snapshot of the virtual machine.
- The virtual machine image was copied to the local tape device using Data Protector.
- A Data Protector backup specification post-processing script was run on the ESX server to:
  - Destroy the snapshot for a hot backup.
  - Take the virtual machine out of suspended mode or hot-backup mode.

Restores were run using the ESX server to read the Data Protector backup image directly from the local tape device. To restore a virtual machine from a restored image, the following was performed:

- The virtual machine was powered off.
- The entire virtual machine was recovered to the point in time of the backup.
- The virtual machine was powered on.

Advantages of ESX server local tape device virtual disk backup and restore

- Point-in-time image: A point-in-time image allows a virtual machine to be easily restored to a known good point in time.
- Backup application not needed on virtual machine: Because the ESX server takes the image and that image is backed up, a backup application does not have to be installed and maintained on the virtual machine.

Disadvantages of ESX server local tape device virtual disk backup and restore

- File-level backup and restore is not possible: The image is a complete image of a virtual machine at a point in time. The entire virtual machine must be recovered to the point in time of the image when being restored.
- Heavy use of ESX server resources: Creating a snapshot and backing up multiple virtual machines on the same ESX server in parallel can use a lot of ESX server resources.

B. Virtual machine media host file system backups with a local (non-SAN) tape device

Virtual machines running on an ESX server may have backup application media host software installed, just as any other server. Configured this way, the virtual machines can perform backups and restores to a local tape device. An HP test environment was set up to test this type of configuration.

- The Data Protector Disk and Media Agents were installed on the virtual machine using a Data Protector installation server.
- A backup specification was created on the Data Protector Cell Manager for running file system backups of the virtual machine. The backup specification was created as a normal file system backup with the virtual machine local tape device selected as the destination.
- Backups were run using Data Protector to send data from the virtual machine directly to the local tape device.
- Restores were run using Data Protector on the virtual machine to read data directly from the local tape device.

Advantages of virtual machine local tape device backup and restore

- Frees LAN for other purposes: Data is written directly to a local tape device so the LAN is not overburdened.
- No dependency on an external media host: The virtual machine acts as its own media host.

Disadvantages of virtual machine local tape device backup and restore

- Heavy use of ESX server resources: Backing up virtual machines to local tape devices can use a lot of ESX server resources.
- No tape device sharing: Only one virtual machine may use the local tape device. To allocate the tape device to another virtual machine, the current virtual machine must be powered off, and the tape device must be removed.

C. VCB proxy with a local or SAN tape device used as dedicated media host

VCB provides a way to take a snapshot or full-image copy of a virtual machine and present the snapshot or copy to a Windows VCB proxy, which can back up the data to a local or SAN tape device. Virtual machine backups run with minimal impact on the virtual machine and ESX server. A Windows virtual machine backup can be a full-image or file system backup. File system backups allow file-level restore. Currently, only full-image backup is available for UNIX virtual machines.

Note: The VMware Consolidated Backup (VCB) integration packet is required for using VCB with Data Protector. The current integration packet (September 12, 2007 packet or later for VCB 1.0.3) can be downloaded from http://www.hp.com/go/dataprotector. Once on the Data Protector website, click on Patches & utilities > Data Protector 6.0 Software > Cross Operating system, and then download the integration packet.

An HP test environment was set up to test this type of configuration.

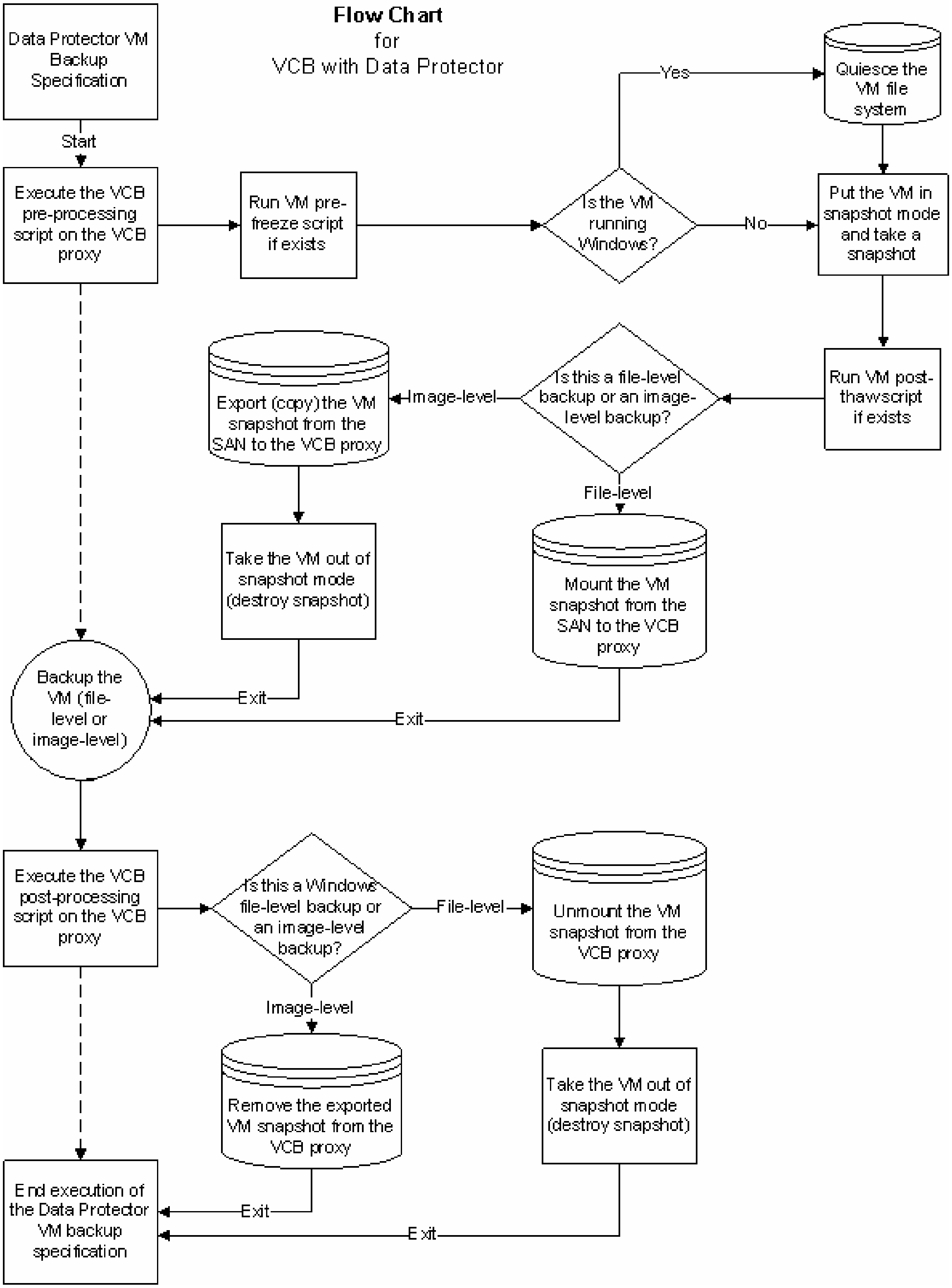
- The Data Protector Disk and Media Agents were installed on the Windows VCB proxy using a Windows installation server.
- Instructions in the HP Storage Data Protector white paper *VMware Consolidated Backup integrated with Data Protector 5.5 and 6.0* documents were followed to integrate virtual machine snapshots with Data Protector.
  - In the "Data Protector integration with Consolidated Backup" section of the white paper, instructions are provided for creating the *vmware_passwd* file.
  - The *vmware_passwd* file is used by the VCB proxy to scan the VirtualCenter server or each ESX server listed in the file to find the location of the virtual machine to back up.
  - It is recommended to scan the VirtualCenter server to locate the virtual machine. For this method, enter the VirtualCenter server hostname, username, and password only in the *vmware_passwd* file. ESX server information should not be added to the file.

Note: It is best to create a Windows user account specifically for VCB on the VirtualCenter server. The user account does not require administrator privileges. VMware specific roles and permissions for the VCB user account can be created within the VirtualCenter console to allow the user to create, modify, and remove virtual machines. Once created, the VCB user account should be used in the vmware_passwd file instead of the administrator account. This will keep the administrator account password from being exposed in a text file.

- The Data Protector Disk Agent was installed on the virtual machine for restore purposes only.

The following flow chart illustrates the Data Protector VCB process:

Figure 6 VCB with Data Protector


Flow Chart
for
VCB with Data Protector
Data Protector VM Backup Specification
Start
Execute the VCB pre-processing script on the VCB proxy
Run VM pre-freeze script if exists
Is the VM running Windows?
Yes
No
Quiesce the VM file system
Put the VM in snapshot mode and take a snapshot
Run VM post-thawscript if exists
Is this a file-level backup or an image-level backup?
Image-level
File-level
Export (copy) the VM snapshot from the SAN to the VCB proxy
Take the VM out of snapshot mode (destroy snapshot)
Mount the VM snapshot from the SAN to the VCB proxy
Exit
Exit
Backup the VM (file-level or image-level)
Execute the VCB post-processing script on the VCB proxy
Is this a Windows file-level backup or an image-level backup?
File-level
Image-level
Unmount the VM snapshot from the VCB proxy
Remove the exported VM snapshot from the VCB proxy
Take the VM out of snapshot mode (destroy snapshot)
End execution of the Data Protector VM backup specification
Exit
Exit

To restore a VCB snapshot (file-level) backup of a virtual machine, the following was performed:

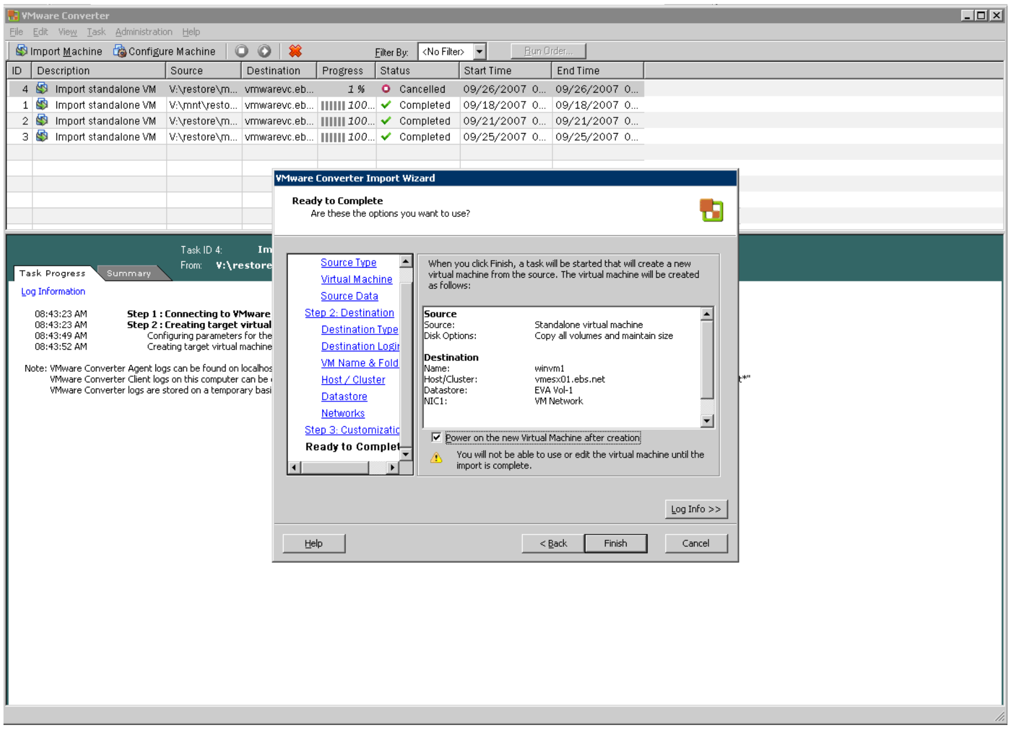
- Data Protector Disk Agent was installed on the virtual machine.
- Data Protector was used to restore the selected directories and/or files, using the Restore to new location option, directly to the virtual machine over the LAN.

To restore a full-image backup of a virtual machine, the following was performed (in this example, the following servers were used—Virtual Machine: winvm1; VCB Proxy Server: vcbProxy; Virtual Center Server: vcServer.):

- The virtual machine was powered off.
- Data Protector was used to restore the full-image backup to a file system on the VCB proxy.
- Three methods are suggested for recovering the virtual machine after the full image backup has been restored to the VCB proxy:
  - VMware Converter—Import the VCB backup image to the ESX server.
  - vcbRestore with NFS (NFS is included with Windows 2003 R2)—Share the VCB proxy restore drive to the ESX server, then use vcbRestore.
  - vcbRestore with a Windows share—Share the VCB proxy restore drive to the ESX server, then use vcbRestore.

Recover the virtual machine using VMware Converter

- VMware Converter was started on the VCB proxy (VMware Converter was previously installed on the VCB proxy) and Import Machine was selected.
- The following VMware Converter import selections were chosen:
  - Source
    - Standalone virtual machine, backup or disk image.
    - The recovered virtual machine image residing on the VCB proxy was selected.
    - Import all disks and maintain size.
  - Destination
    - VMware ESX server or VirtualCenter virtual machine.
    - Login information was entered for the VirtualCenter.
    - The original virtual machine name was entered.
    - The original ESX server was chosen as the destination.
    - The original datastore on the ESX server was chosen to store the virtual machine (use the Advanced option if the virtual machine has multiple disks on multiple datastores).
    - The number of virtual NICs was chosen.
    - Customize was not chosen (the virtual machine was recovered with its original configuration).
- The selections were verified and the Finish button was pressed to start the import.



ID	Description	Source	Destination	Progress	Status	Start Time	End Time
4	Import standalone VM	V:\restore\m...	vmwarevc.eb...	1 %	Cancelled	09/26/2007 0...	09/26/2007 0...
1	Import standalone VM	V:\mnt\resto...	vmwarevc.eb...	100...	✓ Completed	09/18/2007 0...	09/18/2007 0...
2	Import standalone VM	V:\restore\m...	vmwarevc.eb...	100...	✓ Completed	09/21/2007 0...	09/21/2007 0...
3	Import standalone VM	V:\restore\m...	vmwarevc.eb...	100...	✓ Completed	09/25/2007 0...	09/25/2007 0...

Task ID 4: Im
From: V:\restore

```
08:43:23 AM        Step 1 : Connecting to VMware
08:43:23 AM        Step 2 : Creating target virtual
08:43:49 AM             Configuring parameters for the
08:43:52 AM             Creating target virtual machine

Note: VMware Converter Agent logs can be found on localhos
      VMware Converter Client logs on this computer can be
      VMware Converter logs are stored on a temporary basi
```

Ready to Complete
Are these the options you want to use?

When you click Finish, a task will be started that will create a new virtual machine from the source. The virtual machine will be created as follows:

Source
Source: Standalone virtual machine
Disk Options: Copy all volumes and maintain size

Destination
Name: winvm1
Host/Cluster: vmesx01.ebs.net
Datastore: EVA Vol-1
NIC1: VM Network

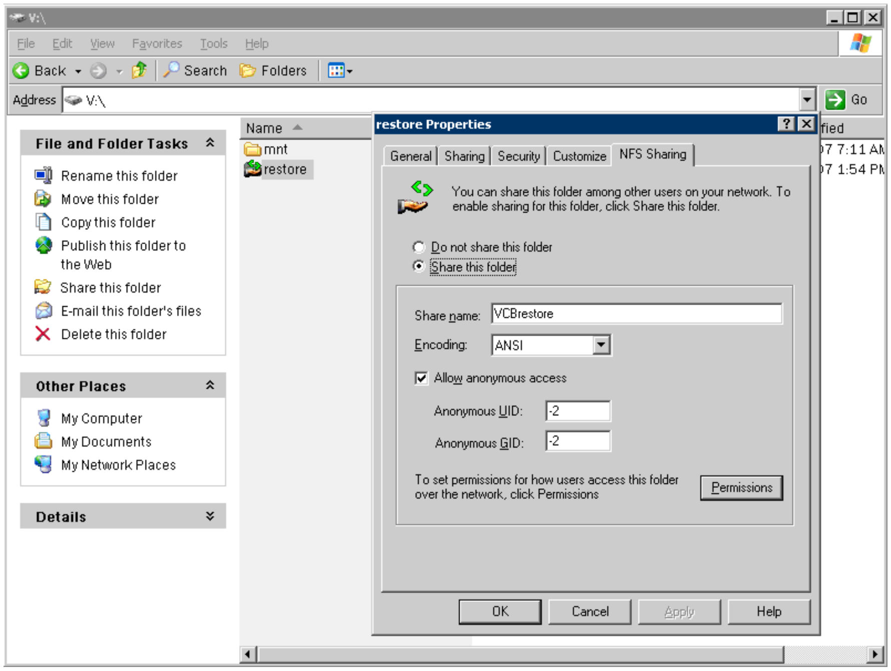
☑ Power on the new Virtual Machine after creation

You will not be able to use or edit the virtual machine until the import is complete.

Recover the virtual machine using vcbRestore with NFS

- The VCB proxy file system holding the restored image was mounted on the ESX server as follows:

1. An NFS share was created for the VCB file system folder containing the restored image (see Windows 2003 R2 documentation for installing and configuring NFS).



restore Properties — NFS Sharing

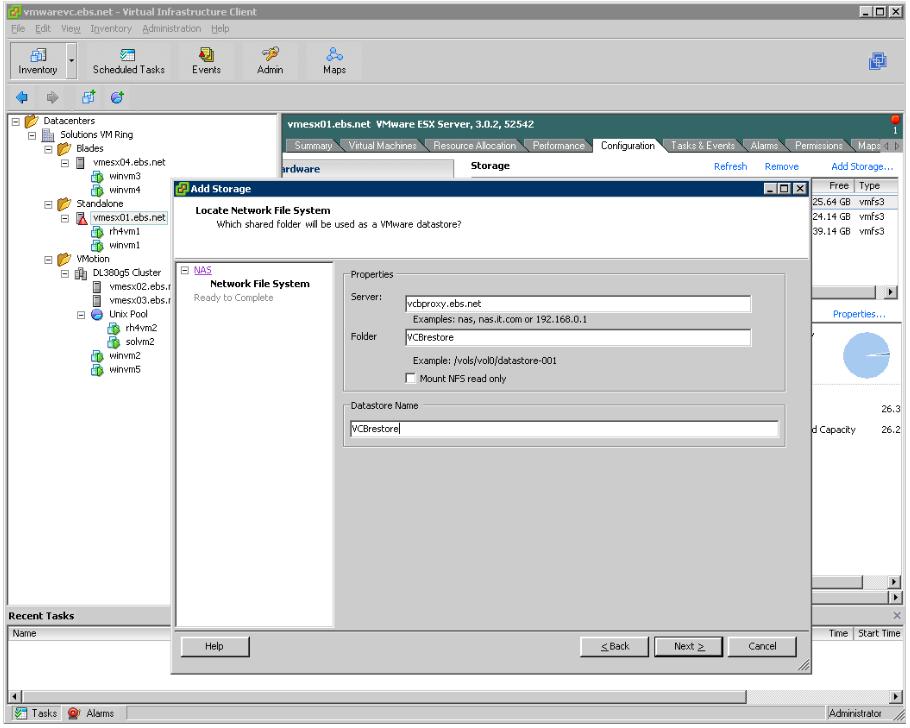
You can share this folder among other users on your network. To enable sharing for this folder, click Share this folder.

○ Do not share this folder
● Share this folder

Share name: VCBrestore
Encoding: ANSI
☑ Allow anonymous access
Anonymous UID: -2
Anonymous GID: -2

To set permissions for how users access this folder over the network, click Permissions

2. The NFS share was added as a datastore on the ESX server.


vmwarevc.ebs.net - Virtual Infrastructure Client
File Edit View Inventory Administration Help
Inventory Scheduled Tasks Events Admin Maps
Datacenters
Solutions VM Ring
Blades
vmesx04.ebs.net
winvm3
winvm4
Standalone
vmesx01.ebs.net
rh4vm1
winvm1
VMotion
DL380g5 Cluster
vmesx02.ebs.
vmesx03.ebs.
Unix Pool
rh4vm2
solvm2
winvm2
winvm5
vmesx01.ebs.net VMware ESX Server, 3.0.2, 52542
Summary Virtual Machines Resource Allocation Performance Configuration Tasks & Events Alarms Permissions Maps
Storage Refresh Remove Add Storage...
Free Type
25.64 GB vmfs3
24.14 GB vmfs3
39.14 GB vmfs3
Properties...
Recent Tasks
Name
Time Start Time
Tasks Alarms
Administrator
NAS
Network File System
Ready to Complete
Help < Back Next > Cancel

Add Storage

Locate Network File System

Which shared folder will be used as a VMware datastore?

Properties

Server: vcbproxy.ebs.net

Examples: nas, nas.it.com or 192.168.0.1

Folder: VCBrestore

Example: /vols/vol0/datastore-001

□ Mount NFS read only

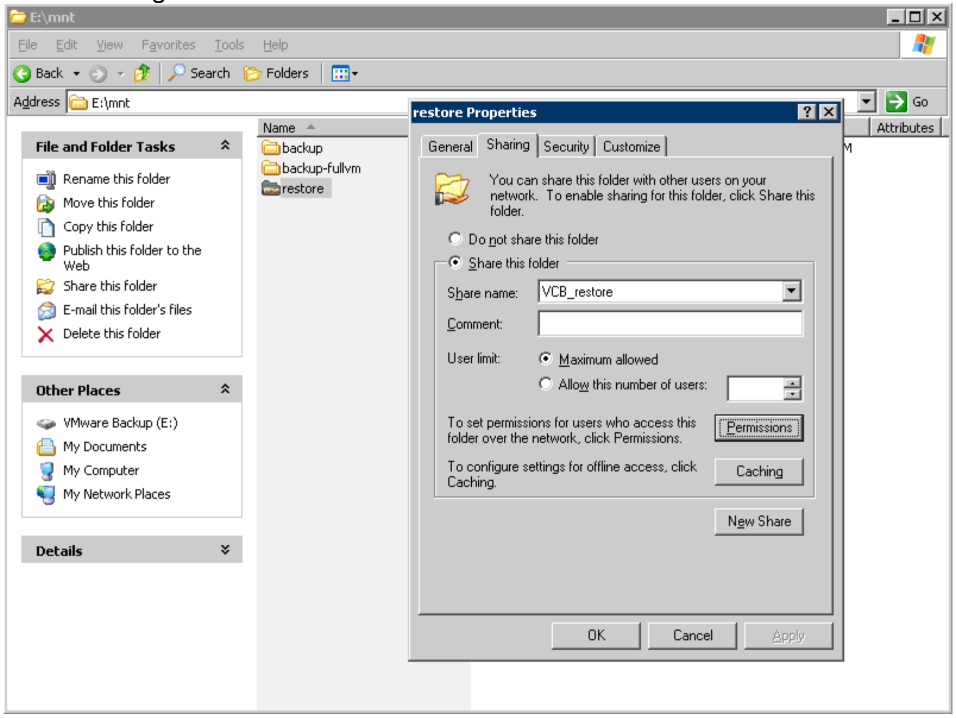
Datastore Name: VCBrestore

- The entire virtual machine was recovered to the point in time of the full-image copy using the vcbRestore utility on the ESX server:

```
# vcbRestore -h vcServer -u User -p Password \
-s /vmfs/volumes/VCBrestore/mnt/backup-fullvm/winvm1 -b overwrite
```

Recover the virtual machine using vcbRestore with a Windows Share

- The VCB proxy file system holding the restored image was mounted on the ESX server as follows:
  1. A Windows share was created for the VCB proxy file system folder containing the restored image.



You can share this folder with other users on your network. To enable sharing for this folder, click Share this folder.

○ Do not share this folder

● Share this folder

Share name: VCB_restore

Comment:

User limit: ● Maximum allowed

○ Allow this number of users:

To set permissions for users who access this folder over the network, click Permissions.

To configure settings for offline access, click Caching.

  2. The share was mounted on the ESX server:

```
# esxcfg-firewall -e smbClient
# mount //vcbProxy/VCB_Restore /vcb/restore
# mount | grep vcbProxy
//vcbProxy/VCB_Restore on /vcb/restore type smbfs (0)
```

- The entire virtual machine was recovered to the point in time of the full-image copy using the vcbRestore utility on the ESX server:

```
# vcbRestore -h vcServer -u User -p Password \
-s /vcb/restore/mnt/backup-fullvm/winvm1 -b overwrite
```

Advantages of a dedicated physical media host VCB proxy

- Frees ESX server for other purposes: The data backup is performed by a VCB proxy, so the ESX server is free to perform other tasks.
- Windows servers can do file level or full-image backups.
- Data Protector is not required on the ESX server: The backups are run on the VCB proxy, and restores are run on the VCB proxy or virtual machine, so Data Protector is not required on the ESX server.
- SAN tape devices can be used: The VCB proxy is a standard Windows server which may use SAN tape devices.

Disadvantages of a dedicated physical media host VCB proxy

- Requires a dedicated VCB proxy: A dedicated VCB proxy must be available for the virtual machine backups.
- Restores can be complicated: Full-image restores are multi-step processes that require installing VMware Converter on the VCB proxy, or finding a way to get the data to the ESX server prior to using the `vcbRestore` utility. Restores require the LAN for moving data to the virtual machine.

D. Virtual disk LAN backups with a dedicated physical media host

An ESX server without a local tape device may be set up to do backups over the LAN to a media host. Configured this way, the ESX server can perform backups and restores to a remote tape device. An HP test environment was set up to test this type of configuration.

Note: The VMware ESX 3.x integration packet is required for ESX server virtual disk backup with Data Protector. The integration packet can be downloaded from http://www.hp.com/go/dataprotector. Once on the Data Protector website, click on Patches & utilities > Data Protector 6.0 Software > Cross Operating system, and then download the integration packet.

In the HP test environment, this type of backup was set up much the same as the "ESX server media host virtual disk backups with a local (non-SAN) tape device" previously covered in this document. The two changes in the setup for LAN backup are:

- Only the Data Protector Disk Agent is installed on the ESX server.
- In the Data Protector backup specification, a remote media host tape device is selected for the backup.

Advantages of virtual disk LAN backup and restore

- Point-in-time image: A point-in-time image allows a virtual machine to be easily restored to a known good point in time.
- Backup application not needed on virtual machine: Because the ESX server takes the image and that image is backed up, a backup application does not have to be installed and maintained on the virtual machine.
- Local tape device not needed on ESX server.

Disadvantages of virtual disk LAN backup and restore

- File-level backup and restore is not possible: The image is a complete image of a virtual machine at a point in time. The entire virtual machine must be recovered to the point in time of the image when being restored.
- Heavy use of ESX server resources: Creating snapshot and backing up multiple virtual machines on the same ESX server in parallel can use a lot of ESX server resources.
- Remote media host is required: There must be a remote media host to send data to.
- Heavy LAN usage: This type of backup may require a dedicated LAN for good data throughput.

E. Virtual machine LAN backups with a dedicated physical media host

A virtual machine without a local tape device may be set up to do backups over the LAN to a media host. Configured this way, the virtual machine can perform backups and restores to a remote tape device. An HP test environment was set up to test this type of configuration.

- The Data Protector Disk Agent was installed on each virtual machine using a Data Protector installation server following the standard Data Protector installation server procedures.
- Backup specifications were created on the Data Protector Cell Manager for running file system backups of each virtual machine. The backup specifications were created as normal file system backup specifications with the media host tape library devices selected as the destination.
- Backups were run by sending data from the virtual machine over the LAN to the media host, which then wrote the data to a tape device.
- Restores were run using the media host to read data from the tape device, which then sent the data over the LAN to the virtual machine.

Advantages of virtual machine LAN backup and restore

- Simple setup: There are no add-ons to install and configure, so it is the same as setting up any LAN client.
- File-level backup and restore.
- Any Data Protector media host can be used: Any Data Protector host in the cell that is running a Media Agent can be used for writing the data to a tape device.

Disadvantages of virtual machine LAN backup and restore

- Data must be sent over the LAN: Configurations with large amounts of data may result in slow backups and restores.
- Heavy use of ESX server resources: Care must be taken to set up backup specifications so that multiple virtual machines on the same ESX server are not running backups and/or restores in parallel due to the ESX server I/O resources required.

Appendix

ESX server disaster recovery

An HP test environment was set up to test the recovery of an ESX server from the complete loss of the server and the server disk storage. The following procedure was used to recover the ESX server:

- It is vital to keep good records of the ESX server configuration. The following information was recorded, in detail, for reconfiguring a failed ESX server:
  - Virtual disk storage—disk storage name, size, location.
  - Networking—vSwitch name, physical adapter, port, and port groups created.
  - Licensing—license server, all license types enabled.
  - Virtual machines—list of virtual machines to be recovered, if necessary.
  - Any other information that may be important for disaster recovery.

Note: Some environments might require additional information not listed in the above steps.

- Restore the ESX server:
  1. Resolve all hardware issues that resulted in the server failure.
  2. Do a fresh install of the server using the ESX server 3.0.2 installation CD (follow the same procedure used for the initial server installation).
  3. After the new installation completes, log in to the ESX server, configure the ESX server firewall and other files necessary to enable the server to function as before.
  4. Use the Virtual Infrastructure client to set up the following items the same as they were prior to the ESX server failure:
     - Reconnect the ESX server to the Virtual Infrastructure client—this was done by disconnecting and then connecting the ESX server.
     - Set up the ESX server disk storage names.
     - Set up the ESX server networking.
     - Set up the ESX server licensing.
     - Set up any other necessary items.
- Restore the virtual machines following the steps in the “Dedicated physical media host VCB proxy with a local or SAN tape device” section of this document (in this example, all of the virtual machines were backed up using a VCB).

For more information

For more information about Enterprise Backup Solutions (EBS), see:
http://www.hp.com/go/ebs

For information on HP Data Protector software, see:
http://www.hp.com/go/dataprotector

HP StorageWorks SAN design reference guide:
http://h18006.www1.hp.com/storage/saninfrastructure/index.html

For information on the HP StorageWorks Modular Smart Array (MSA), see:
http://www.hp.com/go/msa

For information on the HP StorageWorks Enterprise Virtual Array (EVA), see:
http://h18006.www1.hp.com/storage/arraysystems.html

For information on HP StorageWorks XP arrays, see:
http://h18006.www1.hp.com/storage/xparrays.html

For information on the HP StorageWorks Command View EVA, see:
http://h18006.www1.hp.com/products/storage/software/cmdvieweva/index.html

For more information on HP StorageWorks Command View XP, see:
http://www.hp.com/products1/storage/products/disk_arrays/xpstoragesw/commandview/index.html

To view the VMware Hardware compatibility list, see:
http://www.vmware.com/pdf/vi3_san_guide.pdf

To access the VMware SAN configuration guide, see:
http://www.vmware.com/pdf/vi3_server_config.pdf

For access to VMware Infrastructure 3 documentation, see:
http://www.vmware.com/support/pubs/vi_pubs.html

Contact HP

For worldwide technical support, telephone numbers are listed on the HP support website at:
http://welcome.hp.com/country/us/en/contact_us.html

4AA1-3470ENW, October 2007