BEST PRACTICES

VMware Consolidated Backup

Best Practices and Deployment Considerations for SAN Environments

vmware®

Contents

Introduction

VMware Consolidated Backup (VCB) enables you to perform virtual machine backup at any time. It provides a centralized backup facility that leverages a centralized proxy server and reduces the load on production ESX Server hosts.

VCB is part of the VMware Infrastructure suite of products. VMware Infrastructure builds on the virtualization capabilities of VMware ESX Server, which abstracts server processor, memory, storage, and networking resources into multiple virtual machines.

VCB is the preferred method of protecting your virtual machines in a VMware infrastructure environment. This deployment guide is designed to help you use VCB effectively in a datacenter environment, where one or more ESX Server hosts run virtual machines stored on a SAN. It highlights important configuration details for VMware Infrastructure and VCB, helps you analyze your infrastructure to achieve optimum backup performance, and guides you through the basic steps you should follow to troubleshoot any issues you encounter when you run VCB in your environment. This guide supplements the installation and configuration information in the *Virtual Machine Backup Guide*, available from the VMware Web site.

VMware Consolidated Backup Refresher

VCB offers many benefits for protecting virtual machines in a VMware Infrastructure environment. These include:

- Offloading the backup workload from production ESX Server hosts and consolidating it on one or more dedicated backup proxy servers
- Reducing administrative overhead by centralizing backup management on the backup proxies and eliminating the need for backup agents in each virtual machine
- Eliminating the need for a backup window by using VMFS snapshot technology to keep virtual machines running while you back them up
- Eliminating network traffic on the network by backing up virtual machines over the storage network
- Allowing efficient incremental backups of Windows virtual machines using file-level backup
- Allowing online backup of all virtual machines (including file-level backup of Windows virtual machines and image backup any virtual machines)
- Integrating with current backup software to back up virtual machines

VCB uses VMware Tools to quiesce the file system inside the virtual machine, ensuring that when the snapshot is taken, all pending data changes have been written to disk so the snapshot contains consistent data. VCB also facilitates running scripts before and after the backup, so you can freeze and quiesce applications, then unquiesce them after the snapshot is taken.

Once the snapshot is taken, a separate physical machine — the backup proxy — mounts the base disk as if it were a locally attached file system so a backup agent running on the proxy can read and back up the files using the same features the agent makes available for backing up physical drives, as shown in Figure 1.

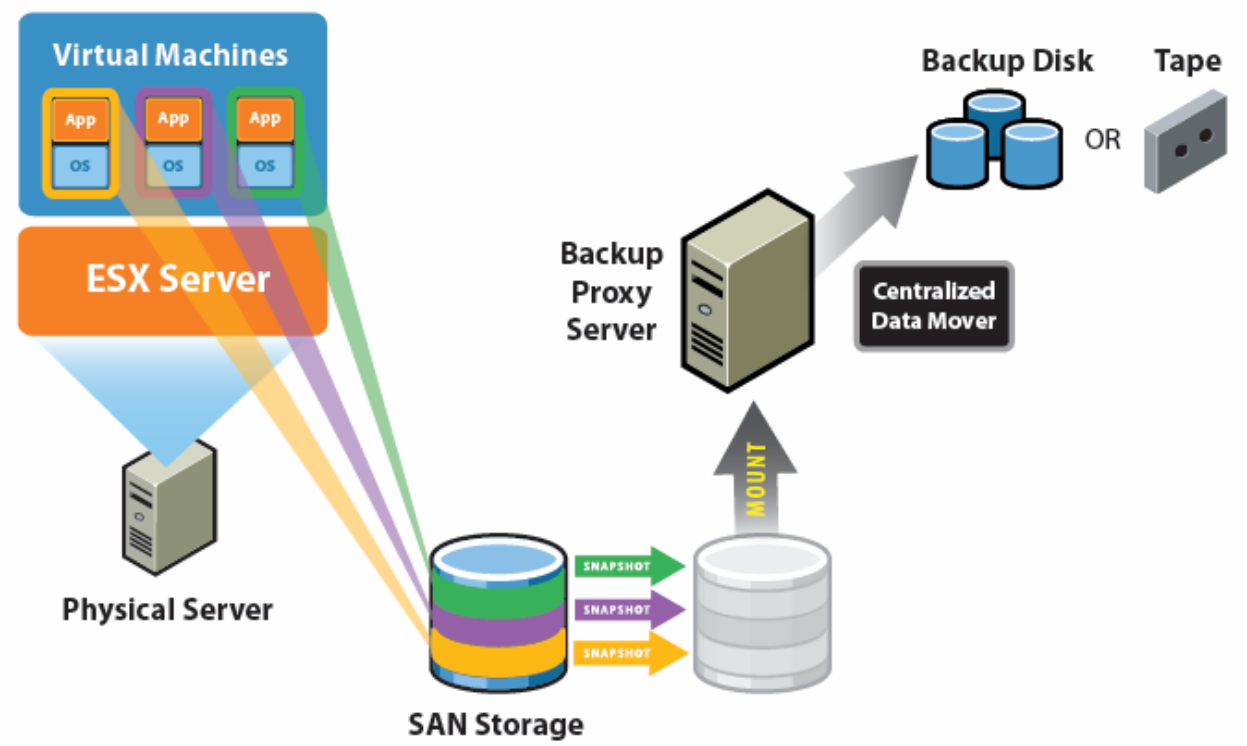

Figure 1: How VMware Consolidated Backup works

Full-Image Backup

Using VCB and your backup client, you can back up a full image of any virtual machine, whatever guest operating system it uses. In an image backup, your backup client software makes backup copies of all virtual disks and configuration files associated with a virtual machine. You can use an image backup to restore an entire virtual machine — for example, to recover from hardware failure or accidental deletion of the virtual machine. You can restore an image back up using VMware Converter or using the `vcbRestore` utility on the ESX Server service console.

File-Level Backup

File-level backup is an option for virtual machines running Windows guest operating systems. Using VCB and your backup client, you can back up individual files and directories from a virtual disk, much as you would if you were running the backup client inside a virtual machine. You can use the capabilities of your backup client to perform a full file backup, a differential backup, or an incremental backup. Using file-level backups, you can restore files or directories individually — for example, to recover an accidentally deleted file.

Requirements

When you plan your VCB configuration, be sure to consider the following requirements:

- For enterprise installations using SAN storage, the backup proxy server must be on a separate physical machine running Windows Server 2003 Service Pack 1 or Windows Server 2003 R2. Depending on the size of your environment, you may need more than one backup proxy server.
- The backup proxy server needs network connectivity to VirtualCenter Server — or, if you have only one ESX Server host and are not using VirtualCenter, the proxy server needs network connectivity to the ESX Server host.
- The backup proxy server must use Fibre Channel HBAs to connect to the SAN on which virtual machines reside.
- The ESX Server hosts that run the virtual machines you want to back up must be configured according to the instructions in the *Virtual Machine Backup Guide*. The ESX Server components of VCB are already installed on each host when you install ESX Server.
- The virtual machine should be stored on a VMFS 3 datastore on the SAN. It is also possible to store virtual machines using raw device mapping (RDM) SAN volumes when used in virtual compatibility mode.
- You must use compatible backup software. For details, see the *VMware Infrastructure 3 Backup Software Compatibility Guide* on the VMware Web site.

Third-Party Integrations

All major backup vendors fully support using VCB to protect virtual machines. You can integrate VCB with your backup software to provide a non-disruptive backup solution. Backup software in a VCB environment continues to handle backup scheduling, reporting, and data movement between the proxy server and secondary storage. VCB enables backup software to automate the task of making virtual machine disk images available to the proxy server for backup.

For the latest information on supported backup software, see the release notes for VMware Consolidated backup on the VMware Web site.

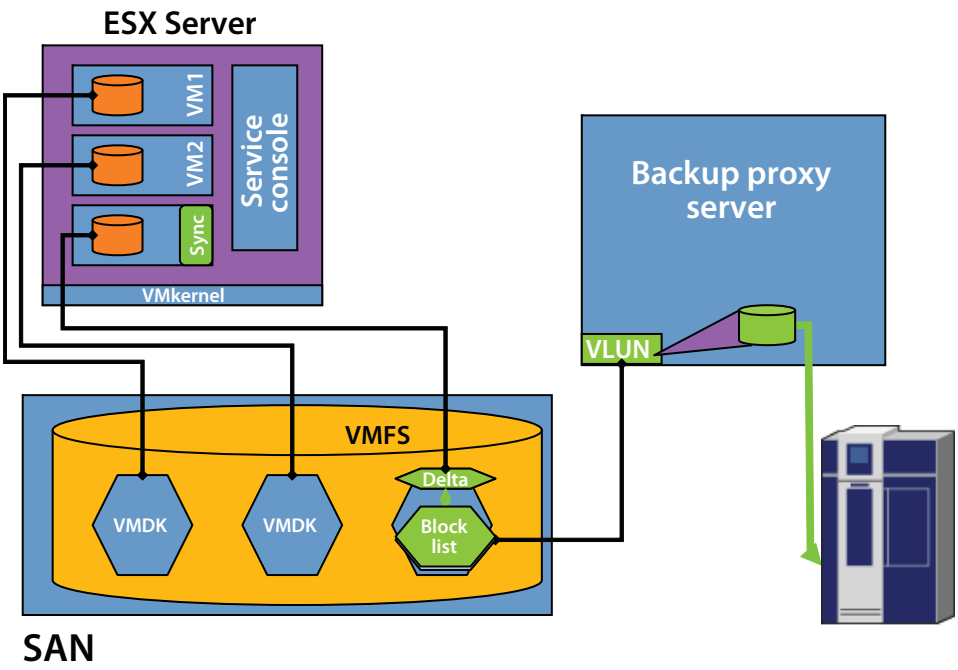

Figure 2: Using the ESX Server snapshot capability to enable backups while the virtual machine runs

Virtual Machine Storage and Snapshots

ESX Server uses the VMware Virtual Machine File System (VMFS) to store virtual machines. This high-performance file system is optimized to store large files, such as virtual machine disk images (`.vmdk` files). Each virtual machine contains one or more disk images.

When you take a snapshot of an ESX Server virtual machine, the system creates a point-in-time image of the virtual machine instantaneously. As the virtual machine continues to run, ESX Server stores all changes to the virtual disk in a separate storage area, labeled Delta in Figure 2, so the point-in-time image is not affected. Then, when you remove the snapshot, ESX Server consolidates the changes into the base virtual disk file.

VCB takes advantage of this snapshot capability when it backs up virtual machines. In each virtual machine, it quiesces applications and flushes pending writes to disk, takes a snapshot, then within a few seconds allows the virtual machine to resume normal operations. VCB uses the point-in-time image created by the snapshot as the basis for your backup. If you are performing an image backup, VCB copies the files that make up the point-in-time image to a "holding tank" on the backup proxy server, then hands control to your backup software so it can back up those files. If you are performing a file-level backup, VCB mounts the virtual disk files that are part of the point-in-time image, then hands control to your backup software so it can back up the appropriate files inside the virtual disks. When the backup is complete, VCB removes the snapshot and ESX Server consolidates any changes into the base virtual disk files.

Another important component of VMware Infrastructure is VirtualCenter. VirtualCenter manages ESX Server hosts and the virtual machines running on them. For example, VirtualCenter sends ESX Server the commands that initiate snapshot operations. When you use VCB to back up virtual machines running on multiple ESX Server hosts, the backup proxy server must be able to communicate with the VirtualCenter Server host that controls them.

Sizing Considerations for VCB

When you plan your configuration for VCB, you must be sure you have the resources you need to back up your virtual machines in the amount of time your schedule allows. To determine what resources you need, you must analyze a variety of factors, some directly related to your VCB configuration, others related to potential bottlenecks elsewhere in your environment. This section provides a guide to the factors you should consider.

VCB uses a snapshot mechanism that enables efficient movement of backup data over a storage area network. Many system components are involved in transferring data from an ESX Server host to a backup proxy server.

Sizing the VCB Environment

Many factors affect the decisions you make when sizing your backup environment. You might be bound by service level agreements to provide backups and finish them in a limited amount of time. You might have business needs to finish all backup activity within a certain amount of time. Or you might have limited resources for performing the backups. In general, you want to finish backups as efficiently as possible given your time and resource limitations.

The number of virtual machines in the environment that need protection is the main driving factor determining the time it might take to perform the backup. The backup infrastructure and storage area networking interconnects, such as switches and HBAs, also affect the efficiency of backup operations, and you must consider them carefully when you set up your backup infrastructure.

Factors That Affect Performance

To plan your backup configuration, you must evaluate a variety of components in your environment and identify which components are most likely to become bottlenecks when you run backups. Factors you should consider include:

- Number of virtual machines: The greater the number of virtual machines you must protect, the larger your backup infrastructure must be. If there are a great many virtual machines, you must either allow longer backup times or allocate a significant amount of resources to meet time constraints. You should carefully consider not only the existing size of your virtual infrastructure, but also possible growth that you will need to accommodate.
- Amount of data: The total size of the data you must protect is very important when you decide the appropriate size of the backup infrastructure. This parameter influences the number and data transfer capacity of your proxy servers and the size of the secondary storage. Together with the number of virtual machines, the amount of data also helps determine how you plan for parallelism.

  If you are performing file-level incremental backups of your virtual machines, only the data that is changed is backed up. The size of this data change is an important consideration when yousize the backup infrastructure.
- Parallelism: All backup products allow you to do more than one backup job in parallel to make efficient use of all resources and to reduce the time it takes to back up your data. Because it maximizes utilization of the entire infrastructure, parallelism is very desirable. But if too many jobs are started at the same time, overall backup speed might be adversely affected. Parallelism can also hurts backup performance. You must plan and configure your environment carefully to implement parallelism.

  VCB enables parallelism by letting you snapshot and mount multiple virtual machine images at the same time. The VCB best practices section recommends steps to make backups more efficient using parallelism.

- I/O activity inside the virtual machine during backup operations: All writes that take place during the backup operation are saved on the VMFS file system. The space for these writes is not allocated in advance. The VMFS allocates space as needed to accommodate the writes. Even though they do not have any negative performance impact on the virtual machine itself, VMFS metadata operations might slow down backup performance. Limiting parallel jobs to fewer than 10 virtual machines per VMFS file system helps avoid the problem completely.
- Fibre Channel setup: Backup is a heavy user of SAN infrastructure. Especially when backing up multiple virtual machines at once, you can easily use Fibre Channel capacity to its maximum. You need to consider various factors about your Fibre Channel infrastructure.
    - Spare IOPs available on LUNs: Configured LUNs of storage arrays can supply only to a certain I/O bandwidth. If you plan to back up virtual machines while they are in active use, pay close attention to the availability of spare I/O that your backups can use before you hit bandwidth limits on your LUNs.
    - Spare Fibre Channel capacity: VCB utilizes capacity on the Fibre Channel network to move data between the SAN array and the proxy server, then to secondary storage. If you are simultaneously using the storage network for normal operation, the network must have spare capacity to handle the backup operation. SAN infrastructure capacity is determined by two key parameters. The speed of the HBAs in the backup proxy server limit the maximum throughput that backups can achieve. The number of HBAs in the backup proxy server affects the capacity of the Fibre Channel network. To increase the capacity, add more HBAs to the backup proxy.
- Throughput available to the holding space: When you perform full image-level backups of virtual machines, data migration speed is dependent on both the read speed of the image, and also the speed with which exported virtual machines are written to the holding tank. Follow the best practices recommendations in this guide when implementing image-level backups using VCB.
- Fibre Channel switches: Modern switches rarely become gating factors for data transfer. But you must pay careful attention to switches and interconnects so they are not over-utilized. Some factors that may help you determine the maximum speed of the FC switches are:
    - Fibre Channel port speed
    - Speed of the service processor in the switch
- Proxy server configuration: When designing a VCB setup, pay close attention to the transfer speeds that your backup proxy can support. Even though speed and number of HBAs inside the proxy have the greatest impact on transfer speeds, the number of CPUs and amount of memory will also affect backup performance. Pay close attention to CPU utilization on the backup proxy server.

  Number of HBAs: Typically, the number of HBAs you use in a backup proxy server depends on such factors as the speed of your secondary storage, then number of parallel jobs, and the spare IOPs available on the SAN for use during backups. The number of HBAs in the proxy server is an important consideration that can have a big impact on backup performance.
- Backup software: You must properly size backup software as well as hardware. Backup software comes with its own tunables and best practices recommendations. Be sure to pay attention to those factors. Also, if your backup software allows you to install media servers on the proxy server, consider that possibility, as well. Consider the following backup software parameters when sizing your backup environment:
    - Streaming speed to secondary storage devices
    - Use of buffers when backing up data
    - Number of simultaneous backup streams

The most accurate data comes from your own tests in your own environment, if you have such test data. Otherwise, consult the documentation provided by the vendors for these components of your system.

Best Practices Using VCB

The guidelines provided in this section can help you adjust your VCB configuration for best performance.

Optimizing the VCB Proxy

The backup proxy server runs the VCB framework software, your third-party backup software, and an integration module that ties the two together. The backup proxy server moves the data during backup operations. When you configure your backup proxy server, follow the guidelines in this section to protect your data and ensure best performance.

- In a SAN environment, the backup proxy server must run on a separate physical machine.
- Be sure the machine you use as the backup proxy server is running a supported operating system — Windows Server 2003 Service Pack 1 (32-bit or 64-bit) or Windows Server 2003 R2 (32-bit or 64-bit). See the VMware Web site for the most current list of supported operating systems..
- VMware recommends that you use the backup proxy server as the backup or media server for your backup software.
- VMware recommends that you install third-party backup software appropriate for the operating system — 32-bit backup software on a 32-bit operating system or 64-bit backup software on a 64-bit operating system.
- Your third-party backup software controls most data-transfer operations on the backup proxy server. Consult your backup software vendor's documentation for guidance on sizing and tuning the backup software for best backup streaming speed.
- Be sure to disable automatic drive letter assignment on the backup proxy server, following the detailed instructions in the *Virtual Machine Backup Guide*. Failure to perform this configuration step can cause data corruption for virtual machines using raw device mapping.
- If you are using your third-party backup software to write to tape, try running multiple jobs in parallel if your backup software supports parallel jobs. Check the backup software documentation for guidance on the number of parallel jobs you can run with good performance.
- If you are performing full image backups — or if the target too which you are writing backup data is a disk — consider putting the target volume on your SAN rather than on a local disk. When data is coming from a relatively fast SAN to a slower local disk, writes to the local disk become a bottleneck. Also consider dedicating different HBAs for reading data from the VMFS and writing it to the holding tank, as discussed in the "HBA Setup" section.
- Be sure you configure the file `config.js`, following the detailed instructions in the *Virtual Machine Backup Guide*. Some third-party backup software can configure the VCB backup environment for you. Refer to the integration module documentation for your particular backup software for more details.

HBA Setup

Installing multiple HBAs in your backup proxy server and scheduling backups to use these HBAs as efficiently as possible can yield significant performance benefits.

As shown in Figure 3, full-image backups first copy a virtual machine's files from the VMFS datastore to a "holding tank" on an NTFS partition, then transfer the files from the holding tank to tape or another backup medium.

Because I/O throughput, not CPU load, is the likely bottleneck on the backup proxy server, the configuration shown in this example uses six HBAs and coordinates backups of virtual machines on multiple ESX Server hosts in such a way that data moves in only one direction through a particular HBA at a given time.

The first data transfer copies the files of a virtual machine running on ESX Server host 1 from the VMFS datastore to the NTFS holding tank. Then, while your backup software is copying the first virtual machine's files to tape, it is simultaneously copying the files of a second virtual machine, which runs on ESX Server host 2, from its VMFS datastore to an NTFS holding tank.

The configuration shown in this example has an additional benefit. They minimize the demands on any one VMFS datastore. Although the snapshot process used by VCB is quick, VMFS can process only one snapshot operation at a given time. Other snapshot requests to the same VMFS are queued until the first request is processed, and a queue of pending snapshot requests can affect performance of the datastore.

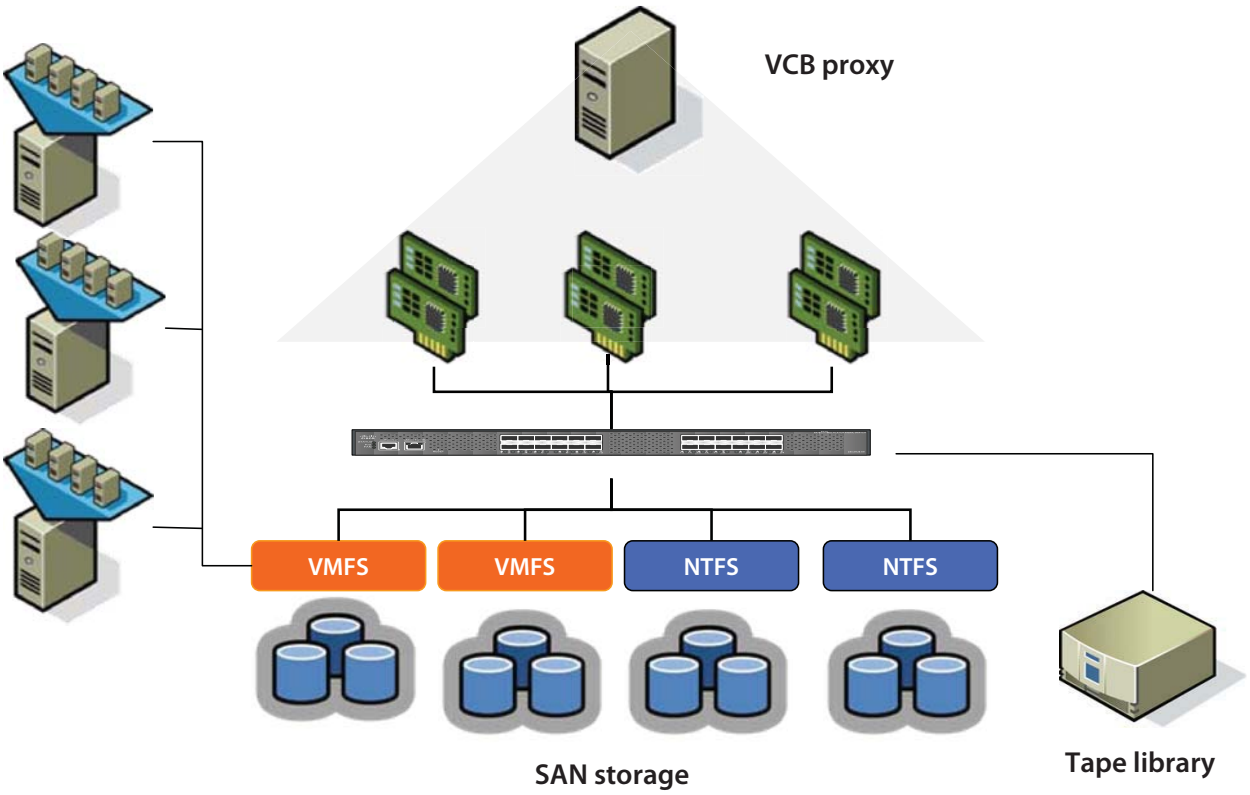

Figure 3: Using multiple HBAs in the backup proxy for more efficient backups

VirtualCenter

VCB communicates with VMware VirtualCenter to send commands to ESX Server hosts during the backup process. For best security, you should take the steps described in this section.

- Set up a special user account for VCB in VirtualCenter. In VirtualCenter 2.5, use the predefined role called VMware Consolidated Backup User. If you are using an earlier version of VirtualCenter, create a `vcbuser` role and give that role the following privileges:

  VirtualMachine > Configuration > DiskLease

  VirtualMachine > State > CreateSnapshot

  VirtualMachine > State > RemoveSnapshot

  VirtualMachine > Provisioning > Allow Virtual Machine Download

In VirtualCenter 2.5, you can use a predefined role called VMware Consolidated Backup User. Figure 4 shows the role as defined in VirtualCenter. Only a few privileges in the Virtual Machine category are enabled for this role. For additional details, see the *Virtual Machine Backup Guide*.

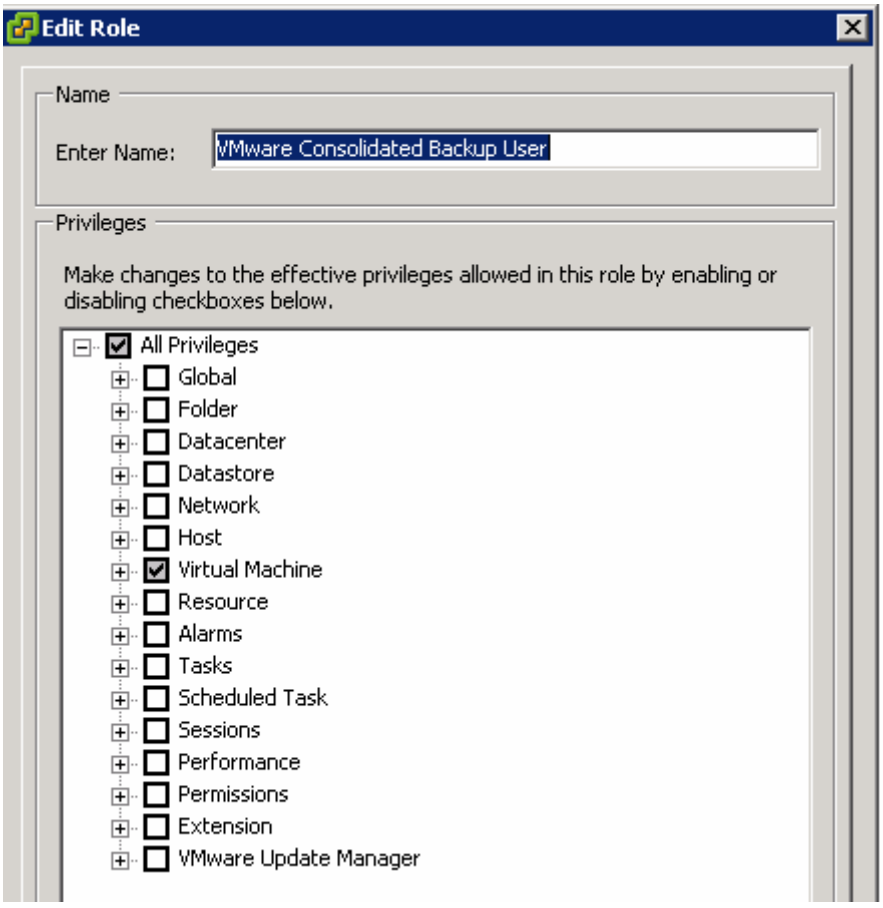

Figure 4: The built-in VCB User role in VirtualCenter.

Configure VCB to use the credentials of this special user. Include the `vcbuser` user name and password in the `config.js` file on the backup proxy server for automated login to VirtualCenter, as described in the *Virtual Machine Backup Guide*.

You should also lock down the backup proxy server itself, following these guidelines:

- Create a new VCB user with minimal privileges. Assign the VMware Consolidated Backup role in VirtualCenter to this user. Consider disabling such services as remote control and terminal services profile for this account for added security. Specify this user's credentials in `config.js` to initiate backups from your backup software.
- Use local authentication — The backup proxy server should not use any form of network authentication when using credentials to initiate the backup. This guideline protects against the possibility that other users might log in to the machine, a possibility that is greater if any network authentication is used.
- Restrict access to the proxy server —You should not use the backup proxy server as a general purpose server.
- The person who uses the `vcbuser` role on the VirtualCenter Server host should be the same person as the administrator of the backup proxy server. If these are separate people, the administrator on the backup proxy server can easily get access to the password for the `vcbuser` role.
- If you have multiple backup proxy server hosts, use different `vcbuser` accounts with different passwords for each host.
- Rotate the `vcbuser` account's password regularly.

ESX Server Host

When you schedule your backups, be sure to consider which ESX Server hosts are running the virtual machines you plan to back up at a given time. If you back up multiple virtual machines simultaneously, pick virtual machines on different VMFS datastore.

VCB takes advantage of the snapshot capabilities of VMFS when it backs up virtual machines. It is essential that you configure your SAN to work properly with ESX Server so that VCB can perform correctly.

- If you have many virtual machines in your environment, spread them across multiple VMFS volumes for best snapshot performance.
- VCB takes advantage of VMFS snapshots to perform virtual machine snapshot operations. Schedule your backups so you do not put more than six to eight virtual machines into snapshot mode at once on a single VMFS. You can achieve parallelism by batching virtual machines from different VMFS file systems together and creating subsequent batches of the virtual machines to be backed up.
- If you want to use VCB to back up a virtual machine using raw device mapping (RDM), you must create the RDM using virtual compatibility mode. This is the only mode supported with VCB.

For a more detailed discussion of SAN environment considerations, see the *SAN System Design and Deployment Guide*.

Virtual Machines

The configuration and operation of particular virtual machines affect your backup planning in various ways. Some configuration decisions affect the efficiency of backups. Other configuration decisions can make it impossible to use VCB with particular virtual machines. Keep the following points in mind as you set up your virtual machines and plan your backup strategy:

- Be sure all virtual machines you want to use with VCB have the latest version of VMware Tools installed. VMware Tools provides capabilities critical to such operations as quiescing virtual machines in preparation for backup.
- Be sure to quiesce all applications running inside the virtual machine before you take a crash-consistent snapshot. VCB can quiesce file systems automatically. In addition you can write scripts that are called at the appropriate time in the backup process to quiesce applications running inside the virtual machine for application-consistent snapshots. For more information, see the *Virtual Machine Backup Guide*.
- Although VCB works with virtual machines that are in snapshot mode, this approach may have unexpected effects and is not recommended. The reason is that VCB uses the most recent snapshot as the basis for the backup. If that snapshot is not the one created by the backup process — for example, if the most recent snapshot was created because someone is testing a service pack, hot fix, or upgrade that is later discarded — restoring from that backup might give you a virtual machine that contains unwanted data.
- VMware recommends that you use DNS in your infrastructure. Reverse name lookup makes it easier to manage the backup and restore process using DNS entries. DNS also removes the risk of human errors.
- If you use the `ipaddr` option for identifying virtual machines for VCB to back up, be sure you have powered the virtual machine on at least once and installed VMware Tools. These steps are needed to make the virtual machine's IP address available to VCB. If `ipaddr` fails, change the `VM_LOOKUP_METHOD` setting.

Troubleshooting Guidelines for VCB

If you encounter problems configuring or using VCB, the information in this section can help you identify and resolve the issues. Start with the flowchart in Figure 5, then refer to other information in this section for tips on particular issues and troubleshooting tools.

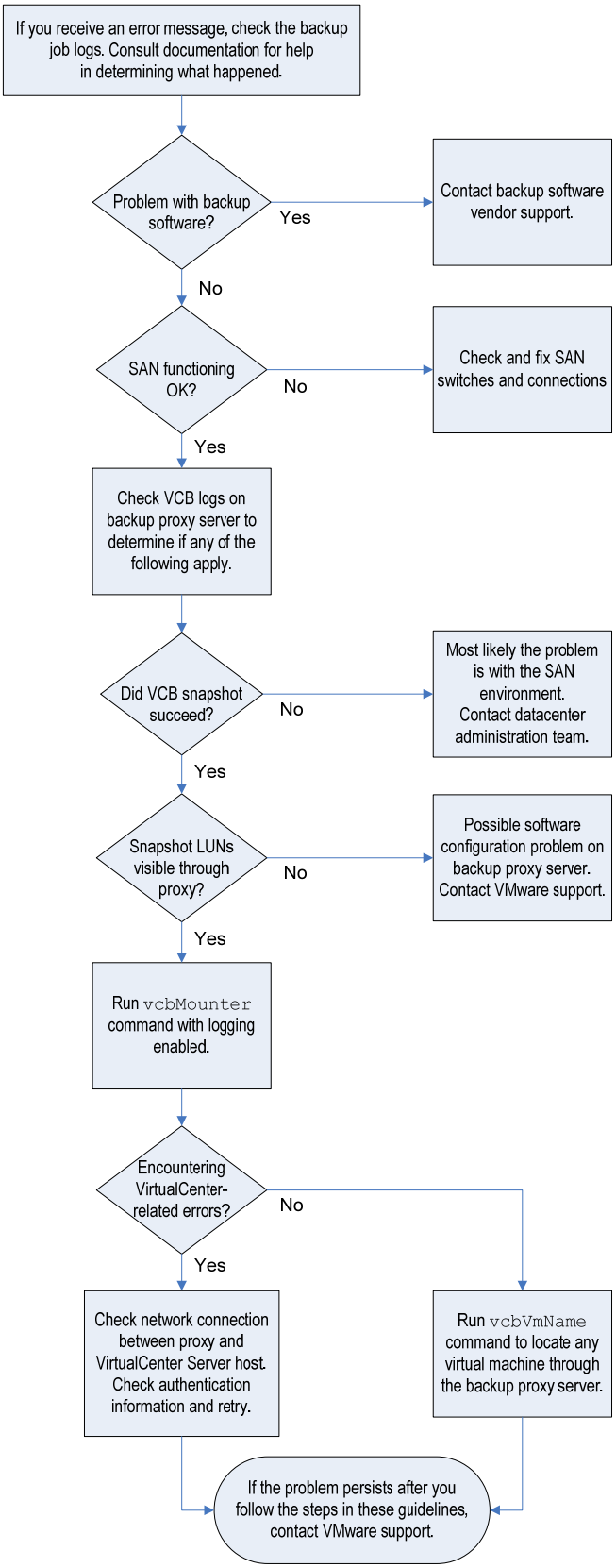

Figure 5: Troubleshooting flow chart

Problems with Backup Software

If you encounter problems with a backup operation, the first place you are likely to see evidence of the problem is in the interface of your third-party backup software.

First, check the logs of your backup software. Log files for the backup software are often found in `C:\Documents and Settings\Administrator\Local Settings\Temp`. See the documentation for your backup software for details.

If you determine that the error was not in your backup software and you suspect VCB errors, review the problems outlined in the following sections.

Snapshot Problems

Review the relevant log files and determine whether the snapshot of the virtual machine was successful.

The key sources to check for snapshot information are the log files for the `vmount` and `vstor` services. These logs are on the backup proxy server in the following files:

```
C:\WINDOWS\Temp\vmware-vmount*.log
C:\WINDOWS\Temp\vmware-vlun*.log
```

SAN Problems on the Proxy Server

If SAN connections are not working or are working only intermittently, the log files for the ESX Server host or the SAN switch should show evidence of the problem.

Be sure you can see the snapshot LUN from the backup proxy server. To do so, go to **Start** > **Settings** > **Control Panel** > **Administrative Tools** > **Computer Management** and choose **Disk Management**. (You can also get to this control panel by choosing **Start** > **Run Command** and entering `diskmgmt.msc`.) The control panel should show the LUN as `Healthy (Unknown Partition)`. If it shows the LUN as any other type, you have a problem with LUN presentation in your server.

Check your SAN configuration to determine whether you are using any multipathing software or have any zoning issues

If the Disk Management control panel shows a do not enter icon for the snapshot LUN as shown in Figure 6, you might have software conflicts with dynamic disk or volume management software. Disk 13 in Figure 6 is a snapshot. The Disk Management utility shows it as Not Initialized because some program other than the VCB VLUN driver is using it. Check with your storage administrator or system administrator or with VMware support for help resolving the problem.

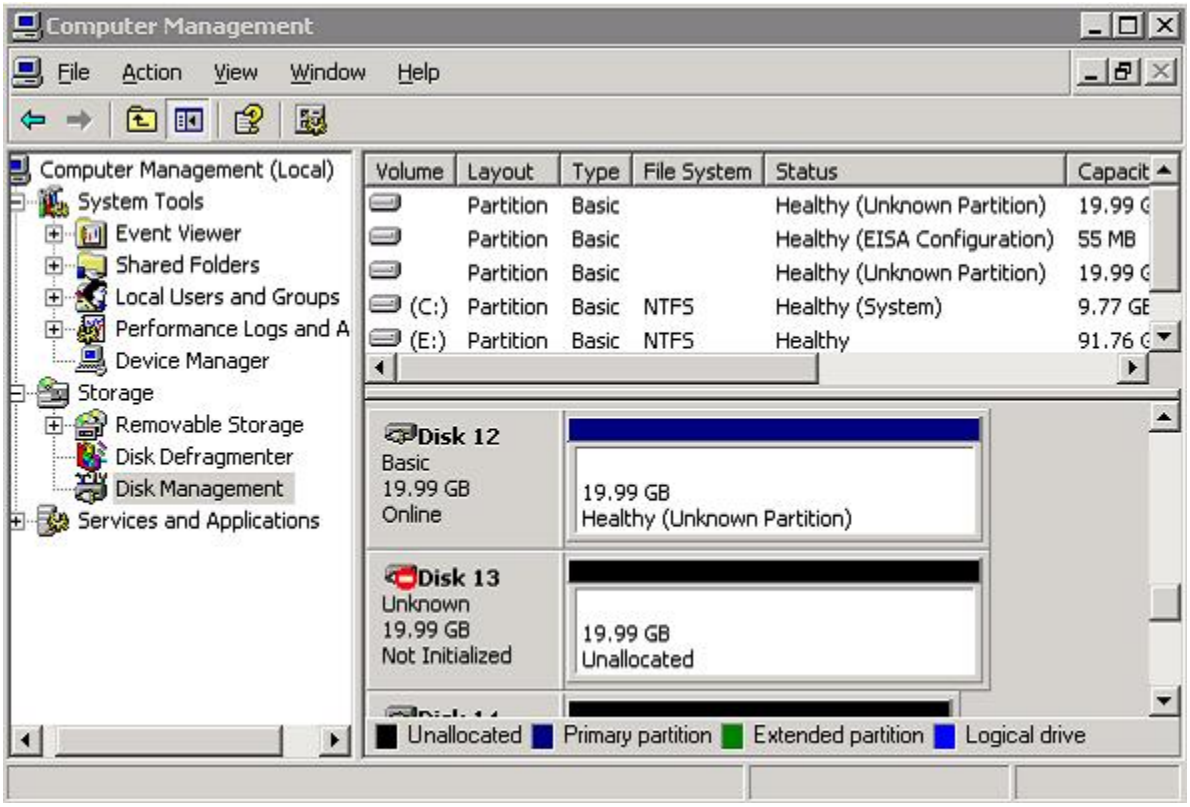

Figure 6: The Disk Management control panel showing a snapshot in use by some other program

Using vcbMounter for Testing

If you confirm that the snapshot is taken and is seen through the Disk Management control panel, your SAN is working and the backup proxy server is configured correctly.

Attempting a snapshot backup from a command prompt on the backup proxy server, as shown in Figure 7, can help you identify where the process fails. For this testing, use the vcbMounter command, which takes a quiesced snapshot of the virtual machine and exports the point-in-time image of the virtual machine as a set of files.

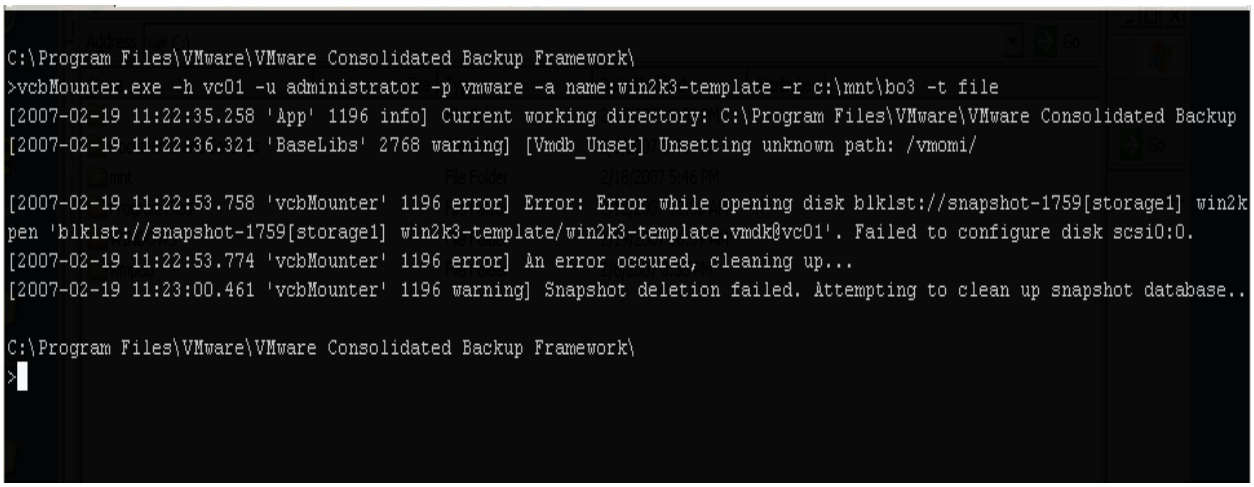

Figure 7: Running a snapshot backup from a command prompt

For detailed instructions on using `vcbMounter`, see the *Virtual Machine Backup Guide*.. Use `vcbMounter` with the `–L 4` option for a useful level of logging (`-L 6` provides the most verbose logging).

The tests with vcbMounter can help you identify problems with connections between the VirtualCenter Management Server host and other computers involved in the backup operations, problems with the VirtualCenter database of virtual machines, and user names and passwords, among other issues.

Problem Reaching the Virtual Machine

When you attempt a snapshot backup, you may receive an error message saying the command cannot reach the virtual machine. There are a number of possible reasons for this error message. Sometimes, the virtual machine is not properly registered with the VirtualCenter database, or the virtual machine might not receive an IP address before the backup begins.

To test for these problems, run the `vcbVmName` command from the service console of the ESX Server host or from a command prompt on the backup proxy server, as shown in Figure 8.

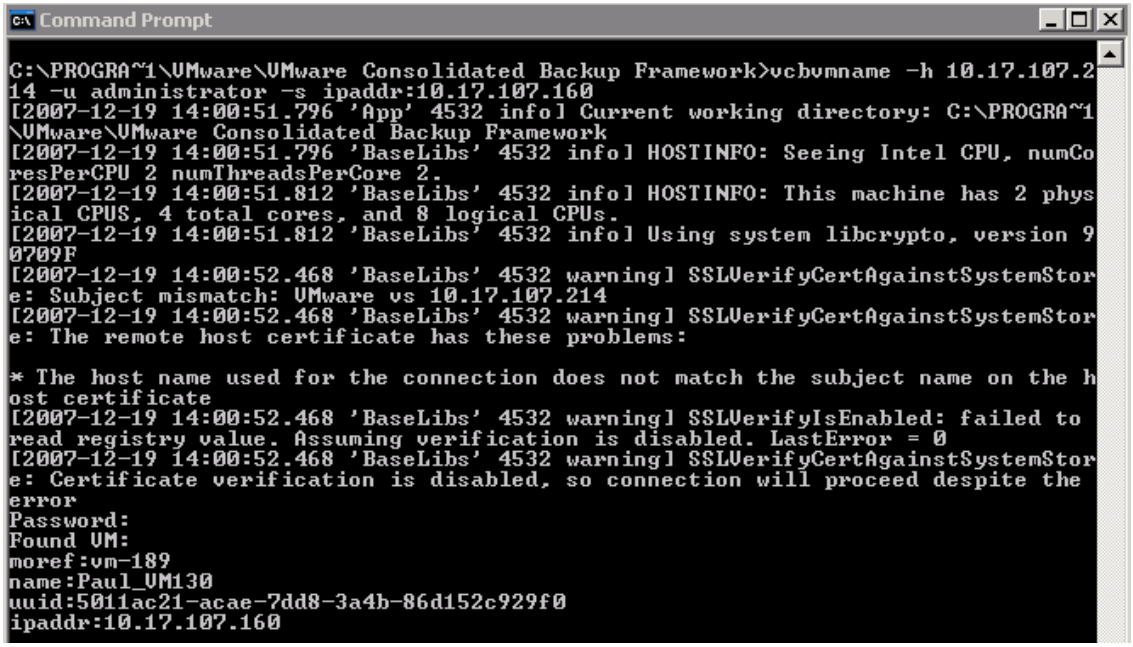

Figure 8: Running the vcbVmName command

The following examples illustrate how to use `vcbVmName`:

- `vcbVmName -s powerstate:on` — Lists all powered on virtual machines.
- `vcbVmName -s any:` — Lists all known virtual machines.
- `vcbVmName -s ipaddr:vm37.company.com` — Displays information about the virtual machine with the specified address.

The following example illustrates the output of `vcbVmName`:

```
bash #vcbVmName -s name:vm37.company.com
Found VM:
moref:192
name:Virtual Machine 37
uuid:564d78a1-8c1c-59b4-fa02-be14138797be
ipaddr:10.17.5.31
```

Compare the IP address reported by `vcbVmName` with the address shown in the VI Client. The two should be the same. If they are not, it might indicate that your VirtualCenter database is not current and that some of the virtual machine information in the database is inaccurate. If there is a mismatch, it might indicate a VMware Tools failure. Make sure the version of VMware Tools installed in the virtual machine is up-to-date.

Contacting VMware Support

If you cannot resolve the problem using these troubleshooting measures, contact VMware support

Log Files

When you run a backup job using VCB, various VMware programs, your custom scripts, and your third-party backup software all write details of their operations to log files. If you encounter problems, you can often identify the component where the problem occurred and the nature of the problem by reviewing these log files. Check the following locations for useful log files.

Log Files on the VCB Backup Proxy Server

- Logs from the `vmount` service
  `C:\WINDOWS\Temp\vmware-vmount*.log`
- Logs from the `vstor` service
  `C:\WINDOWS\Temp\vmware-vlun*.log`
- Logs from scripts that run before and after a backup operation
  `C:\WINDOWS\Temp\pre_<jobname>.log`
  `C:\WINDOWS\Temp\post_<jobname>.log`
  `C:\WINDOWS\Temp\browsestart_<jobname>.log`
  `C:\WINDOWS\Temp\browseend_<jobname>.log`
- Logs generated by third-party backup software
  `C:\Documents and Settings\Administrator\Local Settings\Temp`

If the log files collected on the VCB backup proxy server are too terse, you can enable more verbose logging by setting a higher debug level in the `config.js` file.

Open the `config.js` file in a text editor such as Notepad. Change the logging level by uncommenting the following line:

```
//LOGLEVEL=6
```

To uncomment the line, remove both leading forward slashes, so the line looks like this example:

```
LOGLEVEL=6
```

Change the logging level to the desired number. To disable logging again, add the two leading slashes to the line.

Log Files on the VirtualCenter Management Server Host

- Information on `getinfo` and disk leases
  `C:\WINDOWS\Temp\vpx\vpxd-*.log`

Log Files on the ESX Server Host

- Logs from `hostd`
  `/var/log/vmware/hostd-*.log`
- Logs from `vcbSnapAll`
  `/var/log/vmware/vcbSnapAll-*`
- General SCSI messages
  `/var/log/messages`

Restoring VCB Backups

Most organizations perform backups routinely, following a predictable schedule. Restores are unpredictable, and when the need arises, you must restore data very quickly and reliably. You thus need to pay close attention to restorability of data when you select backup tools and methods.

Because your restore requirements depend on the type of data loss, you must typically be aware of the uses and limitations of a variety of restore methods.

Besides the nature of the data loss, you need to consider ease of management of the restore process, flexibility of the process, and costs.

Selecting a Restore Method

Restore requirements drive the method used for restoring data. For example, if you lose a datastore on an ESX Server host, you must quickly restore entire sets of virtual machines. In this case, it is much more efficient to restore full virtual machine images than to re-create virtual machines and restore individual files. When a user accidentally deletes files from a virtual machine, on the other hand, you need to restore only those files. It would be wasteful to restore a full virtual machine image, then select only the deleted files.

Organization size also affects your approach to restores. If your organization is small, one IT staff member can manage restores for the entire organization. In medium to large businesses, groups within the organization must manage their own restores. The appropriate people within each group need access to the backup infrastructure so they can restore the required data.

You can perform two types of restores from VCB backups. One is full image restore. The other is file-level restore. VMware Converter Enterprise for VirtualCenter 2.5 is the best tool for restoring entire virtual machines from full backup images.

Both methods are discussed in detail in this section.

The following table shows various methods of restoring data from VCB backups.

Goal	Type of Backup	Tools/Agents	
Restore an entire virtual machine	Full virtual machine image	▪ Backup agent on proxy ▪ VMware Converter	**Steps** ▪ Restore VCB image files on proxy ▪ Using converter, restore the virtual machine to the original or alternate location on the ESX Server host **Advantages** ▪ Ease of management ▪ Simple disaster recovery ▪ Easy deployment ▪ Provision multiple virtual machines using single backup image **Disadvantages** ▪ Must have full backups present
Restore individual files and directories (with shared drive)	File-level backup	▪ Backup agent on proxy or inside one single virtual machine ▪ CIFS (shared drive)	**Steps** ▪ Traverse the backed up data and select the files and directories to restore ▪ Restore them directly on the target's shared drive **Advantages** ▪ Ease of management ▪ Restore from Incremental backups **Disadvantages** ▪ Must have CIFS with shared drives
Restore individual files and directories (without shared drive)	File-level backup	Backup agent inside each virtual machine	**Steps** ▪ Traverse the backed up data and select the files and directories to restore **Advantages** ▪ Direct restore **Disadvantages** ▪ Management of agents

Full Virtual Machine Restore Using VMware Converter

VMware Converter Enterprise for VirtualCenter is a plug-in for VirtualCenter that you can use to restore from VCB full image backups. You can also use the free VMware Converter, which does not plug into VirtualCenter, to restore VCB images. You do not need to purchase VMware Converter Enterprise for this purpose. You can use Converter to provision new virtual machines from a single VCB full image backup, too, as well as restore virtual machines to alternate locations.

For more information about VMware Converter, go to the VMware Web site.

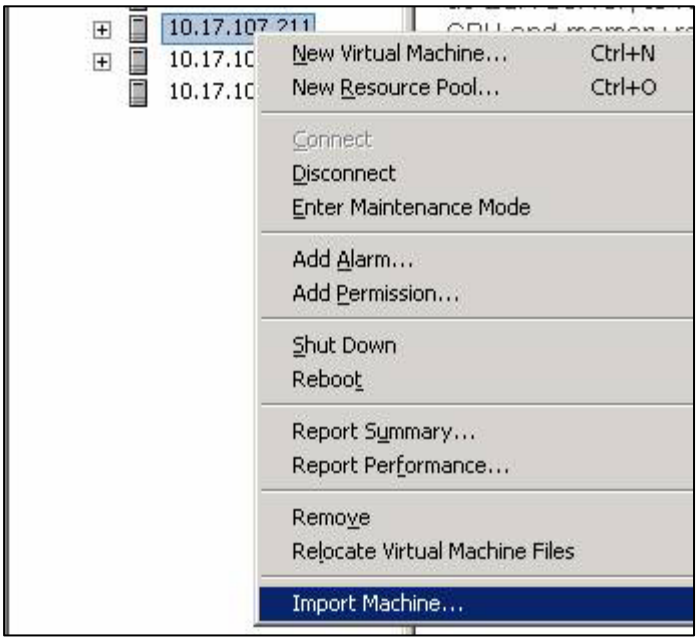

Figure 9: Preparing to import a virtual machine using VMware Converter Enterprise

To work with VMware Converter Enterprise, you install a server component on the VirtualCenter Management Server host and the plug-in client software on the machine running the Virtual Infrastructure Client. You can then initiate the virtual machine import process from the VI Client, as shown in Figure 9 above.

VCB makes full virtual machine image files available to the third-party backup vendors' backup agents on the VCB proxy server. In a typical backup process, you first create these backup image files on hard disk storage, then move them from the disks to a secondary backup medium, such as tapes. This allows you to remove image files from the disks to make efficient use of the disk space.

Before you can use VMware Converter Enterprise, you must restore the images from tape to disk. You can restore these images to any disk, but the VMware Converter Enterprise client must have network access to the files. Figure 10 shows the source input needed for Converter to begin the process of restoring a virtual machine from a VCB image.

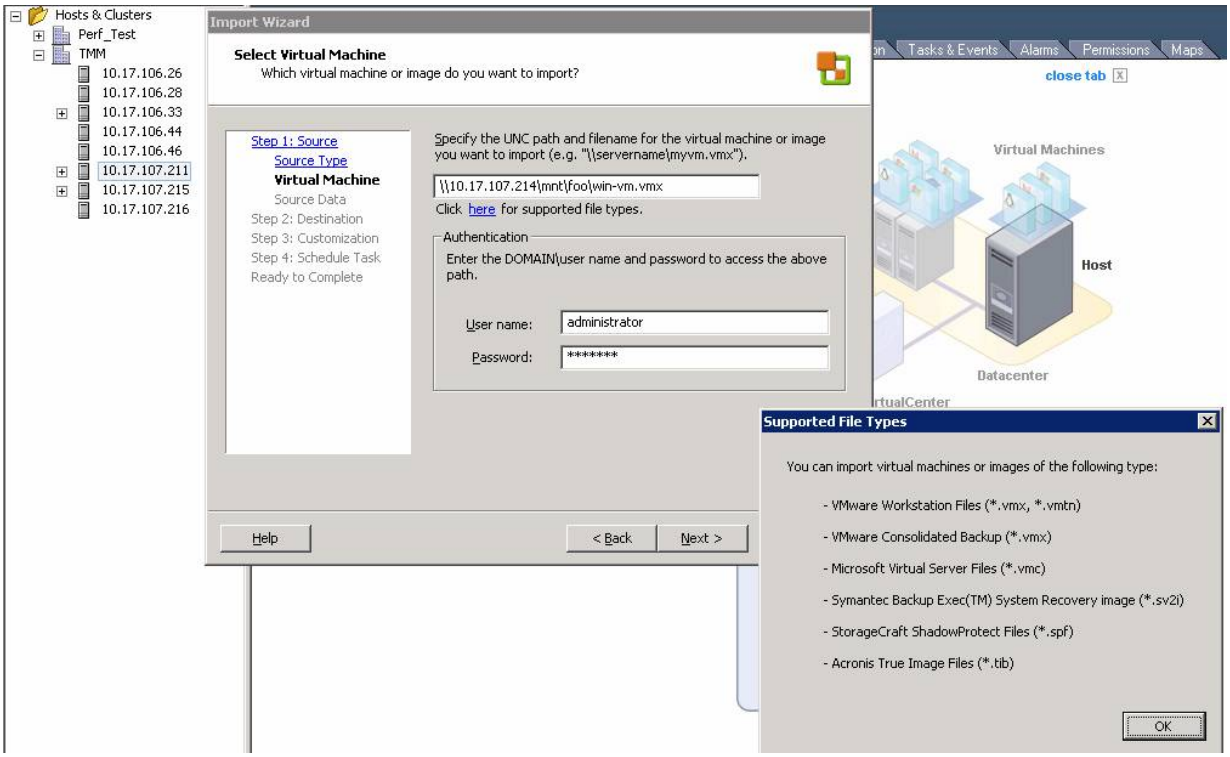

Figure 10: Preparing to restore a virtual machine from a VCB image backup

After you specify the image from which you want to restore, you can customize parameters such as the name of the virtual machine, its datastore location, and networking parameters. You can then submit the job for immediate execution or schedule it for a more appropriate time. You can carry out all the steps in the VI Client or script them for batch processing.

One key advantage of this method is that you can use VMware Converter Enterprise as a simple-to-use, rudimentary disaster recovery tool. Because Converter restores the virtual machine directly to the ESX Server host and adds it to the VirtualCenter inventory, the restore process requires minimal manual intervention once you submit the job.

Restoring Individual Files from File-Level Backups

User errors and media failures can cause individual files or directories on a volume to become corrupt or unavailable. The most efficient way to respond to this kind of data loss is to restore only the lost files.

You can recover the files from a VCB file-level backup in two ways. In the first method, the backup software agent is installed on the proxy or in only a limited number of virtual machines. In the second, backup software agents are installed in each virtual machine.

Agent on Proxy or a Few Virtual Machines

With this method, you use the backup software agent on the proxy server or a select few virtual machines to restore files from the backup to the location where the software agent is running. After you restore the files to that location, you can use CIFS shares to transfer the files to the target virtual machine.

This method enables you to save on the management overhead of installing, configuring, and maintaining backup agents on individual virtual machines. You also do not have to license as many copies of the backup agents as you would if you installed agents in every virtual machine.

Usually for a small to medium-sized business, one or more proxy servers can act as restore nodes for the organization. After they are configured with appropriate CIFS shares, you can perform restores locally on the servers. Target virtual machines can then use the shares to get the files.

For large corporations, each department in the company can have one or more of these restore nodes. You can perform restores on these servers, then use CIFS shares as before to transfer the files to the target virtual machines. You can easily tailor this process to mesh with corporate workflow systems. Users can open trouble tickets to restore files. A backup administrator then locates the correct tapes and restores the files on one of the restore nodes. The user is then alerted to copy the files from the restore node to the target virtual machine.

Agent on Each Virtual Machine

With this method, you install a backup software agent in each virtual machine. You delegate the entire responsibility for the restore process to a user who has access to that virtual machine. Usually this means that once the IT staff member or backup administrator has installed and configured the agent, users can traverse the backup catalog, locate the files they want to restore, then restore the files themselves.

If you use this method, all users must be properly trained to use the backup software to locate the right files and restore them. The architecture for this approach might involve using secondary disks to store backup images and configuring robust access control so users cannot access each other's data.

Once implemented, this method allows administrators to stop worrying about restores.

Note that in both these methods, you use the backup agent software to traverse the backup catalog to locate the files or directories that need to be restored. File-level restores on virtual machines are very similar to file-level restores on physical systems, because all the data transfer takes place over the network between the backup software and the guest operating system.

Resources

- *SAN System Design and Deployment Guide*
  http://www.vmware.com/support/pubs/vi_pages/vi_pubs_35.html
- VMware Consolidated Backup 1.1 Release Notes — navigate to notes from
  http://www.vmware.com/support/pubs/vi_pubs.html
- VMware Converter
  http://www.vmware.com/support/pubs/converter_pubs.html
- *VMware Infrastructure 3 Backup Software Compatibility Guide*
  http://www.vmware.com/support/pubs/vi_pages/vi_pubs_35.html
- *Virtual Machine Backup Guide*
  http://www.vmware.com/support/pubs/vi_pages/vi_pubs_35.html

Revision: 20071221 Item: BP-037-PRD-01-01

VMware, Inc. 3401 Hillview Ave. Palo Alto CA 94304 USA Tel 650-475-5000 Fax 650-475-5001 www.vmware.com