Best Practices Guide for VMware® ESX Server™ Backup
This documentation and any related computer software help programs (hereinafter referred to as the “Documentation”) is for the end user’s informational purposes only and is subject to change or withdrawal by CA at any time.

This Documentation may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA. This Documentation is confidential and proprietary information of CA and protected by the copyright laws of the United States and international treaties.

Notwithstanding the foregoing, licensed users may print a reasonable number of copies of the Documentation for their own internal use, and may make one copy of the related software as reasonably required for back-up and disaster recovery purposes, provided that all CA copyright notices and legends are affixed to each reproduced copy. Only authorized employees, consultants, or agents of the user who are bound by the provisions of the license for the product are permitted to have access to such copies.

The right to print copies of the Documentation and to make a copy of the related software is limited to the period during which the applicable license for the product remains in full force and effect. Should the license terminate for any reason, it shall be the user’s responsibility to certify in writing to CA that all copies and partial copies of the Documentation have been returned to CA or destroyed.

EXCEPT AS OTHERWISE STATED IN THE APPLICABLE LICENSE AGREEMENT, TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS DOCUMENTATION “AS IS” WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT. IN NO EVENT WILL CA BE LIABLE TO THE END USER OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF CA IS EXPRESSLY ADVISED OF SUCH LOSS OR DAMAGE.

The use of any product referenced in the Documentation is governed by the end user’s applicable license agreement.

The manufacturer of this Documentation is CA.

Provided with “Restricted Rights.” Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

Copyright © 2006 CA. All rights reserved.
# Contents

## Chapter 1: Introduction 5

- How You Can Administer Virtual Machines to Manage Backup Operations .......................... 5
- About this Best Practices Guide  .......................................................................................... 6

## Chapter 2: Protecting Virtual Machines as Physical Servers 7

- Back Up the ESX Server Individual VMs as Physical Servers ........................................... 7
- Network Architecture - VMs as Physical Servers ................................................................. 9
- Restore the ESX Server Individual VMs as Physical Servers ............................................ 11

## Chapter 3: Protecting Virtual Machines as Virtual Disks 13

- Back Up the Individual VM Virtual Disks as Separate Files ................................................ 13
- Network Architecture - VM Virtual Disks as Separate Files ............................................... 14
- How You Can Use Perl Scripts to Manage VMware Servers .............................................. 15
- Requirements for Backing Up Data ..................................................................................... 16
  - Set Up the VMware ESX Server Pre and Post Scripts ...................................................... 16
  - Configure the Client Agent Configuration File ............................................................... 17
- VMware ESX Server 2.5.X and ESX Server 3.0.X Protection ................................................. 18
  - Backup Planning - Files You Will Need ........................................................................... 18
  - Back Up Data Using This Solution ................................................................................. 19
  - Restore Data Using This Solution .................................................................................. 21

## Chapter 4: Protecting Virtual Machines from a Proxy Using VCB 27

- Back Up VM Images or Files from a Proxy .......................................................................... 27
- Network Architecture - Backing Up VM Images or Files Using a Proxy ............................. 29
- Set Up Backing Up Using a Proxy ....................................................................................... 30
- Configure the CAVCB Configuration File for Proxy Backups ............................................ 32
- Create a Backup Job ........................................................................................................... 34
- How to Protect Multiple ESX Servers .................................................................................. 39
- How to Restore Data ............................................................................................................ 39
  - Restore File-Level Data ................................................................................................... 40
  - Restore Image-Level Data ............................................................................................... 41
- Limitations .......................................................................................................................... 42
Appendix A: Using VCB Pre and Post Scripts to Protect ESX Server Virtual Machines

Usage for pre_backup.wsf ................................................................. 43
Usage for post_backup.wsf ............................................................. 44
Chapter 1: Introduction

This section contains the following topics:

How You Can Administer Virtual Machines to Manage Backup Operations (see page 5)
About this Best Practices Guide (see page 6)

How You Can Administer Virtual Machines to Manage Backup Operations

Many professionals in the IT industry have realized the tangible benefits of leveraging virtual environments. Along with these benefits come challenges in this relatively new and ever changing arena. In this document we will present solutions to help ensure that virtual machines (VMs) are protected as securely as any physical machine.

VMware ESX Server and BrightStor ARCserve Backup have flexible capabilities that lead to many backup scenarios. With customers' choices for data backup being as broad and varied as that of ESX Server site configurations, this puts the coverage of all possible VM backup scenarios outside the scope of this Best Practices Guide. However, this document will cover the most common methods used for data backups on virtual machines, and any considerations relating to the different methods.

In most instances, best practices documents cover a single topic. However, in the storage industry, there is no uniform solution when it comes to backing up machines within the VMware ESX Server environment. For this reason, this Best Practices Guide covers the two most common backup methods and a method that uses VMware Consolidated Backups (VCB) on the proxy system. We do not propose that these are the only backup methods, rather the most functional for many situations. If your environment does not fit the most common methods, you can explore other methods or modify the suggested methods to suit your needs.

Note: Throughout this best practices guide, we will refer to VMware Consolidated Backup as VCB.
About this Best Practices Guide

The different VM backup and restore solutions discussed in this guide are as follows:

- Solution 1--Protecting VMs as physical servers (see page 7).
- Solution 2--Protecting VMs as virtual disks (see page 13).
- Solution 3--Protecting VMs from a proxy system using VCB (see page 27).

**Note:** Refer to Figure 1 (see page 9) for an illustration of how you can configure your environment to backup and restore data using a networked BrightStor ARCserve Backup server.

For more information about planning your backup using virtual machines, see the VMware web site at http://www.vmware.com/pdf/ESXBackup.pdf.
Chapter 2: Protecting Virtual Machines as Physical Servers

The solution discussed in the following sections describes how you can back up and restore the individual virtual machines in an ESX Server as a physical server.

**Note:** The information contained in these sections applies to ESX Server 2.5.X and ESX Server 3.0.X systems.

This section contains the following topics:
- Back Up the ESX Server Individual VMs as Physical Servers (see page 7)
- Network Architecture - VMs as Physical Servers (see page 9)
- Restore the ESX Server Individual VMs as Physical Servers (see page 11)

Back Up the ESX Server Individual VMs as Physical Servers

**Question:**

When would I want to back up and restore virtual machines (VMs) as I would backup and restore my physical servers?

**Answer:**

You would want to back up and restore VMs as you would back up and restore physical servers under the following circumstances:

- You have policies and procedures in place that standardize the backup process in your infrastructure, and you do not want to introduce additional complexities into the environment.
  
  This method fits very comfortably into the BrightStor ARCserve Backup software solution. It allows the software to handle most of the basic backup and restore procedures.

- You need to restore data at the file level.
  
  If you incur frequent requests to restore individual files, this method lends itself nicely to this situation. BrightStor ARCserve Backup tracks the location of data on media down to the file level. This capability assists in the process of restoring data.
**Advantages:**

This method:

- Lets you back up as you would any physical server; no additional expertise needed.
- Lets you perform file-level backups and restores.

**Disadvantages:**

This method:

- Is not as simple as a single file copy of the VM file as we will discuss in Solution 2.
- Adversely affects the performance of the virtual machine and the host operating system input and output. As a result, other virtual machines using the same host operating system may also experience poor performance.
Network Architecture - VMs as Physical Servers

To use this solution in your environment, you can use an external backup server and a disk or tape device (library) to backup as you would any physically connected server. Then you should:

- Install the BrightStor ARCserve Backup agents, options, or both that are necessary to your server specific needs.
- Schedule backup jobs to run as appropriate for your needs.

In this configuration, you can back up the ESX Server in two or more instances (one for host and one for each guest operating system). The VMs are backed up as if they were physical servers in the backup domain (agents running to assist in the process of backing up and restoring data to an external backup server).

The following graphic illustrates a network-based backup that resides on a private network.

![Network Backup on Private Network](image)

The private backup network keeps the backup data off of your production network congestion.

**Figure 1**

In the method shown above, the ESX Server system contains the service console and one or more virtual machines. The BrightStor ARCserve Backup Client Agent for Linux is installed on the ESX Server Host to assist with backups of the host. This is necessary because the ESX Server Host is a slightly customized version of Red Hat Linux and has access to the special file system called VMFS. The VMFS file system is used to provide high performance access to large files: the disks of the VMs by VMware ESX Server.
The backup is done across the network (10/100 MB or GB). A separate backup server with the current release of BrightStor ARCserve Backup is installed and configured with a destination backup device such as a tape library or a file system device.

**Example: External Network Backup Server Configuration**

The following graphic illustrates a network-based backup that resides on a network-based backup server.

You can back up the ESX Server Host by running one backup job that consists of two sessions. The BrightStor ARCserve Backup Client Agent for Linux lets the backup server detect the following directories on the target system:

/ (root)
/boot
/vmfs
/home

To back up the Service Console, back up the / (root), /boot, and /home directories by scheduling a job.

**Note:** The ESX Server system usually stores the image and data of the VM in the /vmfs directory. Therefore, you do not need to back up the /vmfs directory. The data in this directory is protected by the agents that you install on the respective virtual machines.
BrightStor ARCserve Backup handles the backup of the virtual machines just as it would any physical machines. Backup jobs are scheduled; the client and database agents on the virtual machines handle the backup operations as normal.

**Important!** The importance of staggering backup time becomes magnified when you back up virtual machines. In a single-server environment, a small additional load may not affect the traffic in your network. However, when multiple VMs on the same host are backing up data simultaneously, the performance of your network can be adversely affected.

If you are familiar with standard backup routines, the techniques in Solution 1 may fit most readily into your backup methodology.

**Considerations:**

Although you can install the BrightStor ARCserve Backup server software onto a VM, attach a tape device physically to the ESX Server, and dedicate the tape device to the BrightStor ARCserve Backup VM, we do not recommend that you use this configuration for several reasons.

- Additional load is placed on the ESX Server system.
- In the event of a catastrophic failure on the ESX Server, you will need to reinstall the ESX Server and the VMware host. You must then restore the BrightStor ARCserve Backup server before you can attempt to restore data.

**Note:** For more information, see the document titled "Backup Planning" on the VMware web site.

**Recommendations:**

Due to the nature of backups, creating a network load when run over a production link, you can consider using a private backup network as illustrated in Figure 1 (see page 9) to reduce bandwidth usage.

**Restore the ESX Server Individual VMs as Physical Servers**

This solution lets you restore the ESX Server data via an external network backup server. Based on current backup and restore technology, this restore method is the most conventional method of restoring data.

**Note:** For more information about backing up and restoring data, see the BrightStor ARCserve Backup documentation.
To restore data, the basic steps are as follows

1. From the BrightStor ARCserve Backup Restore Manager, locate the data that you wish to restore.
2. Define the destination location where to restore the data.
3. Schedule the date and time for the restore.

You can restore the Service Console itself by restoring the following directories:

/ (root)
/boot
/home
Chapter 3: Protecting Virtual Machines as Virtual Disks

The solution discussed in the following sections describes how you can back up and restore virtual machines as separate files.

**Note:** The information contained in these sections applies to ESX Server 2.5.X and ESX Server 3.0.X systems.

This section contains the following topics:

- Back Up the Individual VM Virtual Disks as Separate Files (see page 13)
- Network Architecture - VM Virtual Disks as Separate Files (see page 14)
- How You Can Use Perl Scripts to Manage VMware Servers (see page 15)
- Requirements for Backing Up Data (see page 16)
- VMware ESX Server 2.5.X and ESX Server 3.0.X Protection (see page 18)

Back Up the Individual VM Virtual Disks as Separate Files

**Question:**

When would I want to use VMs virtual disks to manage backup and restore operations?

**Answer:**

You would want to back up and restore virtual machine, virtual disks under the following scenarios:

- Your backup and restore needs are based on the possibility of a disaster occurring to the ESX Server.
- Your environment needs to be readily scalable.

This method lets you capture the state of a virtual machine at a particular point in time and encapsulate the virtual machines into a single file. It allows you to take the VM's file to a separate ESX Server. For example, at a disaster recovery site - where it will run exactly as it did on the original machine.

**Advantages:**

The main advantage to this method is its simplicity. Moreover, by backing up virtual disks with this method, you gain the opportunity to copy the VM to another ESX Server in the event of a disaster, or other catastrophic failure.
Disadvantages:

To restore an individual file, you would need to do the following:
1. Restore an entire VM to a different ESX Server, or the same ESX Server with a different name.
2. Restore the failed server.
3. Copy the files from the new VM to the original VM using network file transfer utilities.
4. Delete the new VM.

This method is an inefficient and time consuming process. A full-system restore can become a prolonged process, depending upon the size of the VM.

Important! The ESX Server creates one or more virtual disk files for each virtual machine virtual disks. These files can be backed up conventionally, as single files. The actual backup and restore process is very simple and easy to use, however, the initial setup can be complex. We have therefore built the necessary scripts (via the VMware Perl API) to simplify this process for you.

Network Architecture - VM Virtual Disks as Separate Files

To preface this backup process, virtual disk files can only be backed up using the following two methods:

- The VM is stopped and the VM is backed up. This method is impractical for most production systems.
- The virtual disk is placed in a snapshot mode, which allows the VM to operate normally while the backup process occurs in the background. This method allows the backup process to access the normally locked files and back them up without interrupting the normal operations of the VM.

To help automate this process, Perl API scripts are necessary to place these virtual disks (at least one per VM) into a snapshot condition. When the backup is complete, the VM can be removed from the snapshot mode.

For this configuration, this backup procedure is identical to that of backing up a physical server.

Note: For more information about backup jobs, see the BrightStor ARCserve Backup documentation.

When setting up this backup job, you need to select each virtual disk that you want to back up. The virtual disks will be located in the /vmfs directory, along with any existing associated .REDO log or delta file. The REDO log or delta file contain all the changes made to the VM’s virtual disk since the last time the VM's REDO log was committed or the delta file was merged.
The following graphic illustrates how you can back up individual virtual disk files via a network backup.

The Perl script pre_backup.pl performs several system checks before creating the necessary REDO logs or VM snapshots.

Since this script and the post_backup.pl are called by the BrightStor ARCserve Backup Client Agent for Linux, the pre_backup.pl script places the corresponding VMs on the server into snapshot mode so that all VMs can be backed up.

After the data is backed up, the BrightStor ARCserve Backup Client Agent for Linux calls the post_backup.pl script. This action commits all the pre_backup.pl created REDO logs or snapshots, thus capturing all the changes that occurred on the VMs during the backup process.
Requirements for Backing Up Data

To back up data using this solution, the following requirements apply:

- The BrightStor ARCserve Backup Client Agent for Linux needs to be installed on the system hosting ESX Server and configured to use pre and post scripts.
  These scripts can be used with ESX Server 2.5.X and ESX Server 3.0.X.
- You should install all of the default packages for ESX Server 2.5.X or ESX Server 3.0.X, and Perl 5.6.1.
- The tasks you must perform include the following:
  1. Install the most current version of the BrightStor ARCserve Backup Client Agent for Linux from the distribution media.
  2. Configure the Client Agent configuration file.
  3. Set up the VMware ESX Server pre and post scripts.

More information:

Set Up the VMware ESX Server Pre and Post Scripts (see page 16)
Configure the Client Agent Configuration File (see page 17)

Set Up the VMware ESX Server Pre and Post Scripts

To set up VMware ESX Server pre and post scripts, you must copy the pre_backup.pl pre script, the post_backup.pl post script, and the supporting files listed below to the BABuagent directory, and give execution permission to all the copied files.

Note: The permissions given should be similar to the permissions given to the Agent for Linux executable (labeled "uagentd") residing in the BABuagent directory.

- cavm.cfg
- env_var.pm
- err_msg_set.pm
- debug_msg.pm

You can obtain the above-mentioned scripts and related files from the appropriate distribution media.
Configure the Client Agent Configuration File

**Important!** To configure and enable the capabilities described in this section, the most current version of the BrightStor ARCserve Backup Client Agent for Linux must be installed in your system.

To configure the Client Agent for Linux, you must modify the BrightStor ARCserve Backup for Linux agent configuration file labeled UAG.CFG, which, by default, is located in the BABuagent home directory.

```
/opt/CA/BABuagent
```

The UAG.CFG file lets the Client Agent for Linux do the following:

- Launch the pre_backup.pl script before the backup job starts to place the virtual machine disk files into snapshot mode.
- Launch the post_backup.pl script to commit the changes made to the virtual disks while the backup job is running.

To enable these capabilities, open the UAG.CFG file using a text editing application and add the following three lines to the bottom of the file:

```
-P n
-Prebackup <<Uagent directory>>/pre_backup.pl
-Postbackup <<Uagent directory>>/post_backup.pl
```

Where:

- **-P n**

  Indicates the number of minutes in which to run the prescript before the backup job begins (typically two minutes).

  You can determine this time based on the number of running VMs selected for backup under the ESX Server and the time each VM disk takes to add REDO log file.

  **Important!** If you are not certain about what value to use for this argument, specify 0 (zero) as the value of n. A zero value directs the Client Agent to let the script complete the task before the process of backing up data starts. If you specify a value that is greater than zero, the backup operation starts shortly after the prescript finishes or the timeout value specified elapses, whichever is less.

- **<<Uagent directory>>**

  Indicates the home directory of BABuagent.
VMware ESX Server 2.5.X and ESX Server 3.0.X Protection

On ESX Server 2.5.X, VMware has provided the Perl API’s to add a VM in Snapshot mode by adding the REDO log file. The REDO log file captures the changes on the virtual machine as you are backing up VM files. The changes captured in the REDO log file are merged to the VM image by committing the REDO log.

If you are running ESX Server 3.0.X on your systems, VMware provides you with a utility called vcbSnapshot that you can use to create a snapshot of the VM. The snapshot detects changes to the VM during the backup operation and captures the details in a snapshot delta file. After the backup is complete, the changes captured in the snapshot delta file are merged into the VM image.

Backup Planning - Files You Will Need

ESX Server 2.5.X Systems
To protect a virtual machine and the VM files in ESX Server 2.5.X environments, you will need to gather a list of all files that relate to the VM. The list of files must include the following:

- Disk files--These files include one or more .vmdk files. The disk files are located in the VMFS volumes (for example, /vmfs/vmhba2:0:0:7/).
- Configuration files--These files include the VM configuration files labeled with a .vmx file extension. The configuration files are provided when you create the virtual machine and are located in the directory that you specified during configuration.

ESX Server 3.0.X Systems
To protect a virtual machine and the VM files in ESX Server 3.0.X environments, you simply need to select the corresponding VM folder.

Important! You cannot back up VMs with virtual disks that are either physically or virtually compatible Raw Device Maps (RDM).
Back Up Data Using This Solution

After you gather a list of files that you need to protect, you can back them up from the BrightStor ARCserve Backup server. The BrightStor ARCserve Backup Client Agent for Linux facilitates the backup.

The following graphic illustrates that you can select the following disk file in the Backup Manager in an ESX Server 2.5.X environment:

```
/vmfs/vmhba2:0:0:7/RHEL3-1.vmdk
```
From the same backup job you can select multiple files and directories, select the configuration file (for example, /root/vmware/linux/RHEL3-1.vmx), and select the disk file (for example, /vmfs/vmhba2:0:0:7/RHEL3-1.vmdk).

Before you back up data, verify the following:

- The VMware tools are installed on the ESX Server.
- If there is a firewall running on the ESX Server, ensure that you allow the BrightStor ARCServe Backup Client Agent for Linux to communicate using the proper port.

To back up VM data in an ESX Server 3.0.X environment, you can select a complete directory for a VM.

The following graphic illustrates that the VM directory /vmfs/volumes/445577ed-4af9e884-abbf-000bdb959e33/WIn-2kP-1 is selected.

**Important!** You should not change the power state of the VM while a backup job is in progress.
**Restore Data Using This Solution**

The process of restoring data using this solution is identical to that of a file-level restore on a physical server.

**Note:** For more information about restoring file-level data on a physical server, see the BrightStor ARCserve Backup documentation.

The following sections describe scenarios that you should consider and additional tasks that you may need to perform when you want to restore all disk and configuration files to their original or proper location and recover the VM on the ESX Server.

**Considerations**

- Before you start the restore job, the VM must be stopped so that the restore process can update the disk files.
- This solution lets you perform the following types of restore operations on ESX Server systems:
  - VM disk restore
  - Full VM restore

**Considerations for VM Disk Restores**

- If you performed image-level backups without the VM configuration file (.vmx), you can restore the virtual disk of a VM file (.vmdk).
- You can restore VM disks and create a VM manually using the VMware tools and the .vmdk files.
  
  This mechanism is supported on ESX Server 2.5.X and ESX Server 3.0.X environments.
Considerations for Full VM Restores

The following sections describe considerations for performing full VM restores on ESX Server 2.5.X and ESX Server 3.0.X environments.

**Considerations for Restoring ESX Server 2.5.X Environments**

- All of the disk files must be restored to the VMFS volume.
- You can restore the VM configuration file to any directory.
- After you restore the data, you may need to perform the following tasks:
  - Register the virtual machine.
  - Optionally, commit the REDO log file.
    **Note:** This step is required only if a REDO log file was present when you restored the VM files.

**Considerations for Restoring ESX Server 3.0.X Environments**

- The entire directory containing the VM files must be restored to the VMFS volume.
- After you restore the data, you may need to perform the following tasks:
  - Register the virtual machine.
  - Delete the snapshot labeled CA_SNAP, if it exists.
    **Note:** CA_SNAP is a snapshot that is created when you back up VM data.

More information:

- [Register a Virtual Machine](#) (see page 23)
- [Commit the REDO Log File](#) (see page 23)
- [Delete the CA_SNAP Snapshot](#) (see page 24)
Register a Virtual Machine

The following procedure can be used on ESX Server 2.5.X and ESX Server 3.0.X systems.

To register a virtual machine

1. Register the VM (if it does not exist) to the ESX Server system using the VM configuration file and the utility provided by VMware.

   **Note:** If the VMFS volume name was changed, you must modify the configuration file to reflect these volume name changes before you can register the VM.

   **Example:**
   ```
   /usr/bin/vmware-cmd -s register <config_file_path>
   ```

2. If backed up VM configuration files do not exist (you have VM disk files only), you can create a new VM configuration file using one of the following applications to provide the existing disk files.

   - ESX Server 2.5.X--VMware Management Console
   - ESX Server 3.0.X--VMware Virtual Infrastructure Client

Commit the REDO Log File

The following procedure is optional and can be used on ESX Server 2.5.X systems.

A REDO log file contains the details about changes made to the VM's virtual disk since the last time the VM's REDO log was committed. If you restore data relating to a virtual disk that contains an updated REDO log file, you will need to manually commit the REDO log file.

To commit the REDO log file with VM disk files

1. Ensure that the corresponding VM is not running.

2. Restore the VM.vmdk and the VM.vmdk.REDO files to the same location in the /vmfs directory.

   The REDO log file can be committed manually as described in the next step. Otherwise, if you leave the REDO file as is, you will be asked to commit the REDO log file when the VM is turned ON.
3. Run the VMKFSTOOLS from ESX Server Service Console using the following syntax:

   `vmkfstools -m /vmfs/<SCSI device name> (e.g. vmhba0:0:0:6)/<vmname>.vmdk.REDO`

   (e.g. ESXserver01.vmdk.REDO)

   **Example:**

   `vmkfstools -m /vmfs/vmhba0:0:0:6/ESXserver01.vmdk.REDO`

   "This will commit ESXserver01.vmdk.REDO to its parent disk. Commit it (y/n)?
   "y"

4. Select y (yes) to commit the REDO log file.

   The REDO log file is committed.

**Delete the CA_SNAP Snapshot**

The following procedure is optional and can be used on ESX Server 3.0.X systems.

A snapshot labeled CA_SNAP is created when the power state of a VM is **On** or **Suspended** during backup operations. The snapshot can be deleted using the VMware Snapshot Manager during restore operations.
**To delete the CA_SNAP snapshot**

Edit the VM configuration file labeled *VMName*.vmx as described in the following examples:

**Example 1:**

Consider the following environmental configuration:

- A VM is labeled WIN2KP-1.
- WIN2KP-1 contains two hard disks, WIN2KP-1.vmdk and WIN2KP-1_1.vmdk.
- WIN2KP-1.vmdk and WIN2KP-1_1.vmdk are connected to the SCSI device as scsi0:0 and scsi0:3 respectively.
- Neither disk contains a snapshot or delta file immediately before the backup operation starts.

The restored .vmx file for the VM will contain entries that are similar to the following:

```
scsi0:0.fileName = "WIN2KP-1-000001.vmdk"
scsi0:3.fileName = "WIN2KP-1_1-000001.vmdk"
```

Modify the above-described text as follows:

```
scsi0:0.fileName = "WIN2KP-1.vmdk"
scci0:3.fileName = "WIN2KP-1_1.vmdk"
```

Delete WIN2KP-1-000001.vmdk and WIN2KP-1_1-000001.vmdk, which are available inside the VM folder.
Example 2:

Consider the following environmental configuration:

- A VM is labeled as WIN2KP-1.
- WIN2KP-1 contains two hard disks, WIN2KP-1.vmdk and WIN2KP-1_1.vmdk
- WIN2KP-1.vmdk and WIN2KP-1_1.vmdk are connected to the SCSI device as scsi0:0 and scsi0:3 respectively.
- Both disks contain a snapshot and a delta file immediately before the backup operation starts.
- The last snapshot disk file is WIN2KP-1-000002.vmdk and WIN2KP-1_1-000002.vmdk. The corresponding delta file is WIN2KP-1-delta-000002.vmdk and WIN2KP-1_1-delta-000002.vmdk respectively.

The restored .vmx file for the VM will contain entries that are similar to the following:

```plaintext
scsi0:0.fileName = "WIN2KP-1-000003.vmdk"
scsi0:3.fileName = "WIN2KP-1_1-000003.vmdk"
```

Modify the above-described text as follows:

```plaintext
scsi0:0.fileName = "WIN2KP-1-000002.vmdk"
scsi0:3.fileName = "WIN2KP-1_1-000002.vmdk"
```

Delete WIN2KP-1-000003.vmdk and WIN2KP-1_1-000003.vmdk, which are available inside the VM folder.
Chapter 4: Protecting Virtual Machines from a Proxy Using VCB

The solution discussed in the following sections describes how you can back up and restore VMs from a proxy system using VMware Consolidated Backup (VCB).

Note: The information contained in these sections applies to ESX Server 3.0.X systems.

This section contains the following topics:

- Back Up VM Images or Files from a Proxy (see page 27)
- Network Architecture - Backing Up VM Images or Files Using a Proxy (see page 29)
- Set Up Backing Up Using a Proxy (see page 30)
- Configure the CAVCB Configuration File for Proxy Backups (see page 32)
- Create a Backup Job (see page 34)
- How to Protect Multiple ESX Servers (see page 39)
- How to Restore Data (see page 39)
- Limitations (see page 42)

Back Up VM Images or Files from a Proxy

Question:

When would I want to back up VMs from a proxy using VCB?

Answer:

You would want to back up VMs using VCB under the following circumstances:

- You want to reduce resource contention in the ESX Server.
- You do not want to deploy a backup agent on your virtual machines.
- Your environment consists of a SAN fabric setup and your VMs reside on a SAN storage LUN.
- You need to restore data at the file-level or raw image-level.
Advantages:

This method lets you:

- Offload your backups to one or more dedicated backup proxy systems and removes the load from the ESX Server host system.
- Perform file-level backups and restores using a VM running any Windows operating system.
- Perform raw image-level backups and restores using a VM running any operating system.
- Perform LAN-free backups.
- Back up a VM, regardless of its power state.
- Reduce administration overhead by centralizing backup management on backup proxy systems. This method does not require you to deploy backup agents on the VMs.
Network Architecture - Backing Up VM Images or Files Using a Proxy

This solution can be used for VM raw-image backups and file-level backups.

**Note:** To perform a file-level backup, a Windows operating system must be running on the VM.

When you deploy this configuration in your network:

- The VM raw image backup method makes a copy of all of the disk and configuration files associated with the particular VM, thus allowing you to restore the entire VM.
  
  You can use this method for disaster recovery.

- The file-level backup method lets you make a copy of individual files contained on the disk in a VM, which can include all files.
  
  You can use this method for situations that involve restoring files that were accidentally deleted or corrupted.

The following diagram illustrates the network architecture for backing up VM images or files using a proxy system.

![Network Architecture - Backing Up VM Images or Files Using a Proxy](image)

**Figure 4** Note: The LUNs containing VMs must be accessible by the proxy in addition to ESX Server.
Set Up Backing Up Using a Proxy

*Note:* For additional information about VCB, see the document titled "Virtual Machine Backup Guide" on the VMware web site.

**Set Up Backing Up Using a Proxy**

This section describes how to install and set up your environment to back up VM images and files using a proxy.

**To set up backing up using a proxy**

1. Install ESX Server 3.0.X.

   *Note:* The VMs must reside on a SAN storage LUN.

2. Install VCB on the backup proxy server under the following environmental conditions:
   - Windows 2003 Server must be the operating system running on the backup proxy server.
   - The backup proxy server must be able to access to the SAN storage LUN.

   *Note:* For information about VCB installation, setup, and limitations, see the *Virtual Machine Backup Guide* on the VMware web site.

3. Install BrightStor ARCserve Backup on the backup proxy server.

4. Install the BrightStor ARCserve Backup patch for VCB. The patch contains the following files:
   - Readme.txt
   - pre_backup.wsf
   - post_backup.wsf
   - cavcb_config.js

5. Copy the sample configuration file labeled cavcb_config.js to the BrightStor ARCserve Backup configuration directory on the backup proxy server.

   `<BAB_HOME>\config`
6. Copy the scripts labeled pre_backup.wsf and post_backup.wsf to the root of the BrightStor ARCserve Backup installation directory.

< BabHome>

**Note:** For more information about the pre_backup.wsf and post_backup.wsf scripts, refer to the appendix "Using VCB Pre and Post Scripts to Protect ESX Server Virtual Machines."

7. Modify the cavcb_config configuration file as described in the section Configure the CAVCB Configuration File for Proxy Backups.

**More information:**

Configure the CAVCB Configuration File for Proxy Backups (see page 32)
Configure the CAVCB Configuration File for Proxy Backups

The CAVCB configuration file is a JavaScript (.js) file that has the generic information about the ESX server that is needed by VCB while mounting or unmounting the VM. You can use separate configuration files for each ESX server. If you use separate configuration files, you must pass the specific ESX server configuration file as first parameter to the pre and post scripts. Separate configuration files let you run multiple jobs on different ESX servers.

The CAVCB file should be saved in the config folder in the BrightStor ARCserve Backup home directory, as shown in the following example:

<BAB Home directory>\config\cavcb_config.js

To configure the CAVCB configuration file for proxy backups

1. Open cavcb_config.js and edit the following variables as necessary:

   **VCB_PATH**="VCB home directory";
   
   This variable has no default value. You must specify a value for this variable.
   
   Example:
   
   VCB_PATH="C:\Program files\VMware\VMware Consolidated Backup Framework";

   **BACKUPROOT**="Mount root directory";
   
   This variable represents the absolute path to the mount point root directory. The default value is:
   
   "c:\mnt"
   
   Example:
   
   BACKUPROOT="c:\mnt";

   **Note:** The mount point root directory should exist or be created before backup process starts.

   **HOST**="ESX server host name";
   
   This variable has no default value. You must specify a value for this variable.
   
   Example:
   
   HOST="CAVMWARE";

   where CAVMWARE is the host name of the ESX server that has the VMs to be backed up.
PORT ="902";
This variable represents the port number of the authentication daemon on the ESX Server or the Virtual Center server.
Default value:
"902"

USERNAME="username";
This variable represents the User Name of the ESX Server Host mentioned in the HOST that has the privileges required to access the VM image for read/write operation.
Note: This is a required variable.

PASSWORD="password";
This variable represents the password associated with the USERNAME variable.
Note: This is a required variable.

VM=[<VMname/IP>,<Mount type>,...,<VMname/IP>,<Mount Type>];
This variable string represents the VM host name or IP address and the mount type of all of the VMs in the host ESX Server.
Notes:
- This field is a required variable string.
- You can specify the name of the VM or the corresponding IP address followed by mount type.
- The mount type is case-sensitive. The value of the mount type can be "fullvm" (for all operating systems) or "file" (for all Windows operating systems). The mount type "fullvm" represents a raw image-level backup of a VM. This mount type can be used for disaster recovery. The mount type "file" represents a file-level or directory-level backup of a VM. This mount type can be used to restore an individual file or directory in a VM.
- The Windows operating system that you are running must support file-level mount. For more information, see the VMware VCB documentation.
- The VM image should be available in the SAN storage LUN and should be accessible to the ESX Server and the proxy machine.

2. Close and save cavcb_config.js.
Create a Backup Job

The section describes how to submit a backup job to back up VMs on ESX Server 3.0.X systems using VCB.

**To create a backup job**

1. Configure the CAVCB configuration file for "file" or "fullvm" protection of the VMs.
   
   **Note:** For more information, refer to the section Configure the CAVCB Configuration File for Proxy Backups (see page 32).

2. Open the Command Line utility and execute the pre script as shown:
   
   ```bash
   cscript <BAB home directory>\pre_backup.wsf <cavcb_config file>
   ```
   
   **Important!** This step is required only if "file" level protection is configured for some of the VMs in your environment, or if you do not want to back up all of the VMs that are specified in the CAVCB configuration file.

3. Open the Backup Manager.

   From the Backup Manager directory tree, expand the contents of the VCB Backup Proxy machine.

   **Note:** You can select the files or folders that you need from within the VM by traversing the VM directory.

   You can create the file-level backup job using the Backup Manager. The VM folder, which is labeled as the name of the VM or the IP address of the VM, is available inside the root mount point that you specified in the configuration file.

   **Important!** Optionally, you can select the mount point, c:\mnt, to protect all of the VMs (specified in the configuration file).
Create a Backup Job

The following graphic illustrates C:\ volumes on the Windows VM with an IP address is 192.168.0.0.

4. After you create the job, execute the post script as shown:
   
cscript <BAB home directory>/post_backup.wsf <cavcb_config file>

   **Important!** This step is optional. You must perform this step only if you executed the pre_backup.wsf script as described in Step 2.

5. Specify the destination or staging options required for the job.

6. Specify the scheduling options required for the job.
7. Specify Pre/Post options by doing the following:
   a. Open the Backup Manager and click the Options toolbar button. The Global Options dialog opens.
   b. Select the Pre/Post tab.

   The Pre/Post options appear as illustrated by the following graphic:
c. In the Run Command Before Job section, select the text box that appears after line “Enter the name of the file/application to execute before the job starts” and edit it based on the following:

**Syntax:**

cscript <BAB home directory>\pre_backup.wsf <cavcb_config file>

**Example:**

cscript “C:\Program Files\CA\BrightStor ARCserve Backup\pre_backup.wsf”
cavcb_config.js

**Notes:**

- cscript (cscript.exe) is a command-line version of the Windows Script Host that provides command-line options for setting script properties. With cscript, you can run scripts by typing the name of a script file at the command prompt.

- pre_backup.wsf is the pre script. It should be represented as an absolute path, which lets you mount the image or file system (Windows) of the VM in the proxy.

- Check the On Exit Code check box and set its value as 1. Also, you should check the Skip Job and Skip Post Application check boxes. With these options enabled, when the pre script returns error code 1, the job and the post script will be skipped.

- The Root Mount point in the proxy should not have any existing folder or already mount point having the name of the IP/VM of the VM to be backup.

**Exceptions:**

The script will fail under any of the following conditions:

- The path to the VCB specified in the configuration file is not correct.

- There was no argument specified. The value of the argument should be the file name of the cavcb configuration file.
d. In the Run Command After Job section, select the text box that appears after line “Enter the name of the file/application to execute after the job” and edit it based on the following:

**Syntax:**

cscript <BAB home directory>\post_backup.wsf <cavcb_config file>

**Example:**

cscript “C:\Program Files\CA\BrightStor ARCserve Backup\post_backup.wsf” cavcb_config.js

**Notes:**
- cscript (cscript.exe) is a command-line version of the Windows Script Host that provides command-line options for setting script properties. With cscript, you can run scripts by typing the name of a script file at the command prompt.
- post_backup.wsf is the post script. It should be represented as an absolute path, which lets you unmount or delete the VM folder in the proxy machine.

**Exceptions:**
The script will fail under any of the following conditions:
- The path to the VCB specified in the configuration file is not correct.
- There was no argument specified. The value of the argument should be the file name of the cavcb configuration file.
- The mount point of the VM is not present.

e. In the Run Before/After Command As section, specify the User Name and Password associated with the job.

Click OK.

The Pre/Post options are applied for the job.

8. Start the job as required.

**More information:**

Configure the CAVCB Configuration File for Proxy Backups (see page 32)
How to Protect Multiple ESX Servers

As mentioned previously, all ESX Servers should have separate configuration files available inside the config folder of <BAB_Home> directory. You can protect multiple ESX Servers by running multiple backup jobs.

If you want to protect multiple ESX Server systems using a single backup job, the best solution is to create your own pre and post scripts to call the pre_backup.wsf and post_backup.wsf for each ESX Server system that you want to protect. In this scenario, you must also create separate and unique configuration files for each ESX Server system.

Notes:

- You can create a mechanism that directs the pre_backup.wsf and post_backup.wsf scripts to skip the job, based on an exit code. The Exit Code is discussed in the section Create a Backup Job.
- The pre and post application command Edit box will contain a user-created pre and post script without a configuration file.

More information:

Create a Backup Job (see page 34)

How to Restore Data

When you back up a VM using ARCserve on the proxy system, you can restore the following types of data:

- File-level backups
- Image-level backups

More information:

Restore File-Level Data (see page 40)
Restore Image-Level Data (see page 41)
Restore File-Level Data

This section describes best practices that you can use to restore data that was backed up at the file-level using BrightStor ARCserve Backup. For more information about VMware restore mechanisms, see the VMware VCB documentation.

To restore file-level data

1. Restore the data to the proxy machine (local restore).

   Copy the files to the original location in the VM (in the case of VM files restore).

   Use the Common Internet File System (CIFS) for remote access, file sharing protocol, or remote file transfer method to copy the data to the VM based on your needs.

2. Install the appropriate agent on the VM, and then restore the data to the respective location.

   Important! BrightStor ARCserve Backup does not support backing up data using a Windows agent and then restoring the data using a non-Windows agent. If a situation such as this occurs, you must first restore the data to the proxy machine and then use remote file transfer to transfer the data to the destination machine.

Note: For more information about restore mechanisms, refer to the VMware VCB documentation.
How to Restore Data

Restore Image-Level Data

When you need to restore image-level data, you must first restore the images to the proxy system and then copy the images from the proxy system to the destination ESX 3.0.X Server system.

To restore image-level data

1. Restore the VM to its original ESX Server system.

   After the backup directory of the VM is present in its original ESX Server system, (where the VM was present) or in a remote server system, you can use the VMware provided vcbrestore command line utility to restore the VM. However, before you run the vcbrestore utility, you must update the configuration file labeled backuptools.conf stored in the following directory:

   /etc/vmware

   Syntax:

   vcbRestore -s <backup_directory>

   Examples:

   The following example describes the syntax required to restore the VM to a directory that is local (/home/VM/WIN_VM1) to the ESX Server system:

   vcbRestore -s /home/VM/WIN_VM1

   The following example describes the syntax required to restore the VM from a server that is remote (host_name.ca.com) to the local ESX Server system:

   vcbRestore -s scp://root@host_name.ca.com:/home/VM/WIN_VM1

   Note: The backup should be a complete VM image backup. It should include the VM folder that contains all the resource and configuration files for the VM (for example, \vmfs\volumes\Volume name\VM-folder).

2. Restore the VM image to an alternative location using the service console.

   You can use the catalog file for the VM to restore the VM to a location other than its original location (where the VM was not already present) and to a different ESX Server host. This process involves updating the values of the variables, data stores, folder paths, and resource pools. For more information, see the documentation on the VMware web site.
Limitations

When you use the VCB Proxy Consolidated Backup in your environment, consider the following limitations:

- You cannot back up VMs with virtual disks that are physically compatible Raw Device Maps (RDM).
- To back up VMs, VM disk images must be stored on the SAN storage LUN. The LUN should be accessible to the Backup Proxy.
- To back up data, VMs must have an IP address or a domain name server (DNS) association.
- To back up an individual file or directory, a Windows-based operating system should be running on the VM.
- You cannot back up VMs that reside on NAS/NFS or iSCSI storage devices.
- The VCB utility supports mounting up to 60 concurrent VM volumes.

Examples:
- 60 VMs with one C:\ drive
- 30 VMs with two VM volumes: one C:\ drive and one D:\ drive
Appendix A: Using VCB Pre and Post Scripts to Protect ESX Server Virtual Machines

The following sections describe how to setup, configure, and use the pre and post scripts provided by CA to protect your ESX Server environments that run on proxy systems.

This section contains the following topics:

Usage for pre_backup.wsf (see page 43)
Usage for post_backup.wsf (see page 44)

Usage for pre_backup.wsf

The pre_backup.wsf file is a Windows Script file (.wsf) that lets you mount the user-specified VM in the proxy.

**Note:** This operation can be at the file level or image level. However, it operates based on the criteria that you specify.

Optionally, you can place this file inside the BrightStor ARCserve Backup installation home directory. The script requires the following input parameters at runtime.

**Syntax:**

```
pre_backup.wsf <cavcb config file.js>
```

**Example:**

```
pre_backup.wsf cavcb_config.js
```

**Notes:**

- The script requires one parameter (the configuration file).
- Use quotation marks for the parameter that has space (for example, "c:\program files").
- You should save the cavcb_config.js file in the following directory:
  
  <BAB_HOME>/config
Usage for post_backup.wsf

- **Script Return codes:**
  
  **Code 0**
  
  Indicates a successful attempt to mount or export of all the VMs, as specified in the cavcb_config.js file.

  **Code 1**
  
  Indicates an unsuccessful attempt to mount or export the VMs, as specified in the cavcb_config.js file.

  **Code 2**
  
  Indicates a partially successful attempt to mount or export the VMs as specified in the cavcb_config.js file.

**More information:**

[Configure the CAVCB Configuration File for Proxy Backups](#) (see page 32)

**Usage for post_backup.wsf**

The post_backup.wsf file is a Windows Script (.wsf) file that will unmount or delete the user-specified VM that is mounted, exported, or both, in the proxy. The mount may be a file-level or image-level, based on what you specify. This file can be placed inside the <BAB_Home> directory (not compulsory). The script requires the following input parameters at runtime.

**Syntax:**

post_backup.wsf <cavcb config file.js>

**Example:**

post_backup.wsf cavcb_config.js
Notes:
- The cavcb_config.js file should have the same variable definitions as the configuration file passed to the pre script.
- Script Return codes:
  
  **Code 0**
  
  Indicates a successful attempt to unmount or delete of all the VMs (as specified as a parameter in the pre script).
  
  **Code 1**
  
  Indicates an unsuccessful attempt to unmount or delete the VMs (as specified as a parameter in the pre script).
  
  **Code 2**
  
  Indicates a partially successful attempt to unmount or delete the VMs (as specified as a parameter in the pre script).