WHITE PAPER: SYMANTEC SOLUTIONS FOR WINDOWS

Confidence in a connected world.

Comprehensive Backup and Recovery of VMware Virtual Infrastructure

Symantec Backup Exec™ 12.5 for Windows Servers

White Paper: Symantec Solutions for Windows

Comprehensive Backup and Recovery of VMware Virtual Infrastructure

Contents

Executive summary 4

VMware Virtual Infrastructure 3 backup and recovery challenges 4

VMware architecture overview 6

Addressing the VMware VI3 backup and recovery challenges 7

Traditional VMware Virtual Infrastructure (ESX) 3 backup methods 8

Traditional agent-level backup 8

Advantages of traditional agent-level backup of guest VMs 8

Disadvantages of Backup Exec Agents in guest VM backup 8

Service Console backup and recovery of .vmdk files with RALUS 9

Disadvantages of backups with RALUS in Service Console 10

Backing Up the ESX Service Console itself 10

Basic script-level VMware Consolidated Backup (VCB) backup 10

Advantages of basic script-level VCB backup 10

Disadvantages of basic script-level VCB backups 11

Optimizing VMware Virtual Infrastructure (ESX) 3 backup and recovery 12

Backup Exec 12.5 AVVI features and benefits 13

Using Backup Exec 12.5 Agent for Virtual Infrastructure (AVVI) 13

VMware backup method comparison chart 17

Licensing Backup Exec 12.5 Agent for VMware Virtual Infrastructure 19

Contents *(cont'd)*

AVVI system requirements 19

Software installation requirements 19

Backup Exec 12.5 AVVI software installation locations 20

VMware Data Protection best practices with Backup Exec 12.5 21

Backup configuration 21

Restores 22

Summary 23

Reference materials 23

Appendix A: VMware Virtual Infrastructure (ESX) 3 backup terminology 24

About Symantec 26

Executive summary

Server virtualization is quickly becoming a standard technology in many data centers today. While VMware augments hardware utilization significantly through the use of server virtualization, VMware's Virtual Infrastructure (ESX) 3 also introduces new issues concerning the backup and recovery of virtual environments.

It is important to remember that it is just as critical to protect data created and utilized in virtual machines as it is to protect the data that is located in a single physical machine. This paper describes several approaches that can be used to back up VMware ESX Server 3.x and its underlying components using Symantec Backup Exec 12.5 for Windows Servers and the Backup Exec Agent for VMware Virtual Infrastructure (AVVI). This paper also discusses the relative advantages and disadvantages of each method.

Key benefits

- Offers online, off-host protection of all Windows® and Linux® guest virtual machines through VMware Consolidated Backup (VCB) without scripting
- Integrates with VMware VirtualCenter for automated discovery of VMware installations
- Enables single-pass backups for complete virtual machine recovery or individual file-/folder-level recovery
- Provides online protection for entire guest systems running VSS-aware applications such as Exchange, SQL, and SharePoint
- Offers integration with Backup Exec to allow protection of physical and virtual systems

VMware Virtual Infrastructure 3 backup and recovery challenges

As server consolidation continues to accelerate, placing larger and larger numbers of VMware "guest" virtual machines in a single virtualized environment, planning backup, restore, and disaster recovery of the virtual environment is becoming an essential requirement of managing your virtual infrastructure. VMware Virtual Infrastructure 3 (VI 3) has quickly become an industry standard for organizations that want to virtualize their IT environments.

Companies are becoming dependent on efficient backup and quick recovery of their virtual systems—and the host systems they run on—to maintain business productivity and gain the cost savings that server virtualization delivers. This includes not only the guest virtual machines but also the applications that have been installed on them, such as Microsoft® Exchange®, SQL, and SharePoint Server. A lost ESX Server could impact multiple departments' productivity for up to several hours, or even days, as the IT administrator struggles to recover the virtual environment and the individual guest virtual machines.

Administrators who are looking to protect their VMware environment quickly come to understand the frustration and time involved with backup technologies that are not built specifically for protection of virtual environments. Administrators and companies who have not had the experience of recovering a guest virtual machine using basic backup and recovery tools will face several limitations in recovering their data with older backup tools that were designed only for physical systems, including the need to:

- Install a backup agent inside of each guest virtual machine—or directly on the ESX Server
- Perform a time-consuming recovery of the entire guest virtual machine to recover a single file
- Perform separate backups for system-level and individual file–level recoveries
- Take guest virtual machines offline during backup in order to protect them completely
- Ensure that applications running inside the guest virtual machines can be recovered
- Use separate backup products for physical and virtual machines

Traditionally, these problems have been overcome through the use of VMware utilities that allow third-party backup software to perform backups within the ESX Service Console of live guest virtual machines. Unfortunately, performing live or “hot” backups of guest virtual machines using these utilities can require the use of scripts and Linux-based tools that usually require Linux scripting experience.

Additionally, these types of backups on the ESX Server can place an additional performance load on the entire ESX Server during backup, affecting all guest virtual machines on that ESX Server as well as all of the users connected to those guest virtual machines. Performing a hot backup can be difficult or impossible to manage manually. In addition, it is only cost-effective if it is both centralized and usable by the staff who need it.

VMware Virtual Infrastructure 3 introduces a new technology, VMware Consolidated Backup (VCB), to help overcome some of the challenges associated with the traditional backup methods of virtual machines. However, VCB also introduces some backup and recovery challenges of its own that need to be considered by any organization that plans to implement it. These challenges include:

- Management of cumbersome and complicated VCB "scripts" to integrate with existing backup products
- Installation of proprietary VCB "integration modules" that require additional testing and setup
- The need for separate backups for system-level and individual file–level recovery of a single file from a virtual machine disk format (.vmdk) file

This paper attempts to explore these topics, discuss how Backup Exec 12.5 can help address these unique challenges, and ultimately provide sufficient information to help administrators make a decision on what Backup Exec solution is right for them.

VMware architecture overview

Planning your backup and recovery procedures for an ESX Server system should include identifying the items that need to be available for recovery in your environment *before* a recovery is required. Typically, with VMware Virtual Infrastructure 3 (VI3), three major components need to be considered for backup (see figure 1):

- Virtual disks
- Virtual machine configuration files
- The configuration of the ESX Server system itself

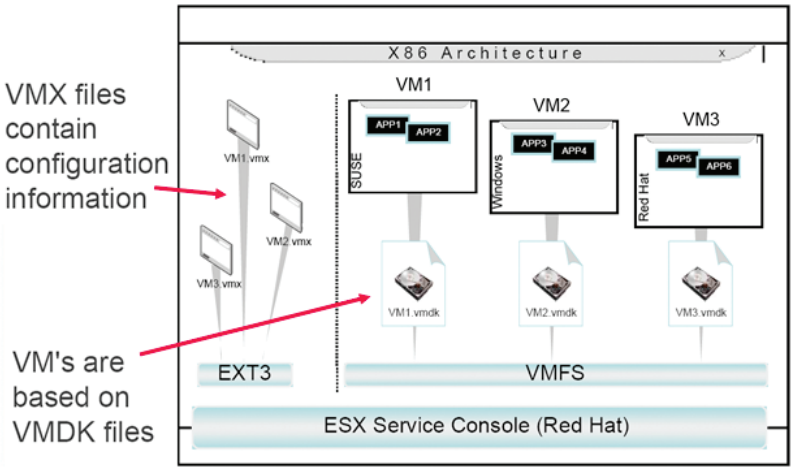

Figure 1. VMware Virtual Infrastructure (ESX) 3 architecture

Addressing the VMware VI3 backup and recovery challenges

As discussed earlier in this paper, while virtualization can provide enhanced server utilization and flexibility, it also introduces unique backup and recovery challenges. There are several ways that Backup Exec 12.5 can be configured to safely protect VMware environments. Before planning the backup and recovery processes for your virtual environment, you should consider several questions, including:

- Do you want to back up the individual virtual machines as normal clients for file-level and application-level recovery, or do you want back up the underlying .vmdk files on which the virtual machines are based for complete volume- or system-level recovery only?
- When one virtual machine is backed up, what is the performance impact on other virtual machines hosted on the same physical ESX 3 server during the backup?
- What are the relative advantages and disadvantages of each of these backup techniques?
- What are the relative advantages and disadvantages in terms of recovery of the ESX Server and the guest virtual machines?
- How would you ensure disaster recovery of an entire guest virtual machine?
- Does a combination of these backup methods make sense for your environment?

Taking into account these issues, we discuss these methods in detail and provide a comparison chart later in this paper.

Traditional VMware Virtual Infrastructure (ESX) 3 backup methods

Traditional agent-level backup

In this method, you are essentially treating each virtual machine as if it were a traditional physical system. In each case, a Backup Exec Remote Agent (for Windows or Linux) must be purchased and installed in each guest VM (see figure 2). The guest VM backup is then scheduled and performed as would a backup of any other Backup Exec protected system on your network.

Advantages of traditional agent-level backup of guest VMs

The virtual machines will appear to Backup Exec as normal physical systems. Restores of data contained inside guest virtual machines are done just like any standard Backup Exec restore job.

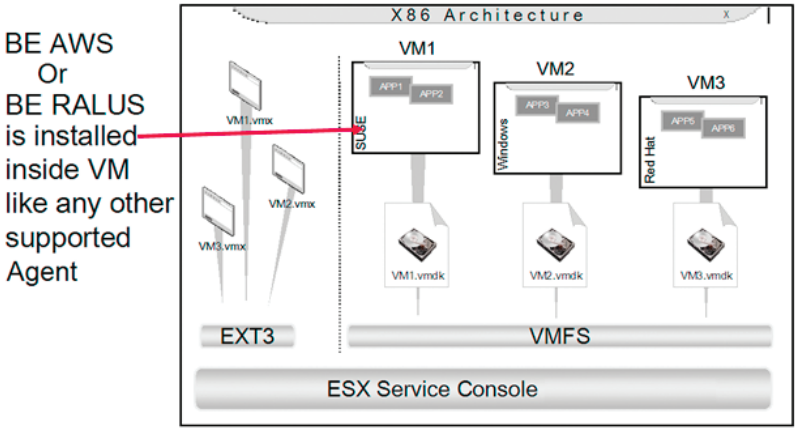

Figure 2. Installing Backup Exec Agents inside VMware guest virtual machines

Disadvantages of Backup Exec Agents in guest VM backup

For many organizations, installing an Agent in each of the guest VM systems can be cost-prohibitive both in terms of money and in relation to I/O performance on the ESX Server. Existing Backup Exec licensing applies to VMware environments. Backup Exec and its Agents are licensed

on a per-server basis regardless of whether they are physical or virtual servers. For example, three guest virtual machines running Windows 2003 being protected by a Backup Exec 12.5 Media Server would require:

- One Backup Exec for Windows Servers 12.5 Media Server license
- Three Backup Exec Agent for Windows Systems (AWS) 12.5 licenses (Agent for Windows Systems licenses include both a Continuous Protection Agent license and a Remote Agent for Windows Systems license)

Service Console backup and recovery of .vmdk files with RALUS

The Backup Exec 12.5 for Windows Servers Remote Agent for Linux and UNIX Servers (RALUS) can be installed directly on the ESX 3 Service Console to protect the .vmdk and .vmx files on the VMware supported file systems, including EXT3 and VMFS (see figure 3).

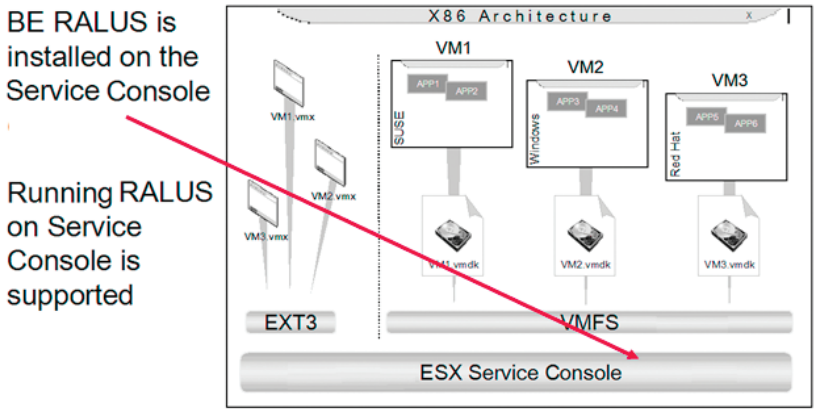

Figure 3. Installing RALUS in the VMware ESX 3 Service Console

Disadvantages of backups with RALUS in Service Console

Care needs to be taken when backing up these files to make sure that they are backed up in a consistent manner and to ensure that restored files are not corrupt. Before the .vmdk files are backed up, all I/O operations to these files must be halted. This can be done either by:

- Shutting down each guest virtual machine prior to the backup
- Performing snapshots of the virtual machines that can be used for backup

Either of these commands can be used by Backup Exec in a backup job automatically as a pre- or post-job command. For complete documentation of all vcbMounter and vcbRestore commands, please see your ESX documentation on www.vmware.com.

Note: The Backup Exec 12.5 for Windows Servers RALUS Agent requires ESX 3 or later and will not install or support ESX 2.x server.

Backing up the ESX Service Console itself

The service console itself (excluding .vmx and .vmdk files) does not typically change often, so the ESX Service Console OS does not need to be backed up very frequently. In addition, ESXi versions no longer even include the Service Console. However, in the event of an ESX system failure, restore operations of the Service Console configuration files may be facilitated if a current backup of the service console is available. As a point of clarification, the backup of the service console described in this section would not typically include the .vmx and .vmdk files associated with a guest OS. These files would be protected separately, as described in the previous section of this paper, “Service Console backup and recovery of .vmdk files with RALUS.”

Basic script-level VMware Consolidated Backup (VCB) backup

The traditional practice of placing backup agents on the virtual machine to perform daily backups puts extra load on the ESX Server and can impact performance for that ESX Server and all the users connected to virtual machines hosted on that ESX Server.

Advantages of basic script-level VCB backup

For a wide range of ESX Server virtual machines, VCB can accomplish two types of separate backups of guest VM data:

- **File-level backup**—This type of VCB backup will result in the entire file-system contents of the .vmdk files to be mounted as a local directory (i.e., a mount point) on the VCB Windows 2003

Proxy Server, which can then be protected by Backup Exec through a normal file system backup of the VCB Proxy Server.

- **Image-level backup**—This type of VCB backup will result in snapshot copies of the virtual machine .vmdk files being copied from the ESX 3 server's VMFS volumes to the VCB Windows 2003 Proxy Server as complete .vmdk disk file images.

These file- or image-level backups by can be done on a separate server from the ESX Server (i.e., "off-host") using a centralized Windows 2003 machine as the off-host VCB Proxy Server. VCB is then used by Backup Exec, via pre- or post-job "scripts," during a backup of an ESX Server to perform file-level or image-level backup (or a combination of both) of the guest virtual machines by exporting either the file-level data or the complete image-level data (.vmdk, .vmx, and .log files) to the off-host Windows 2003 Proxy Server (see figure 4).

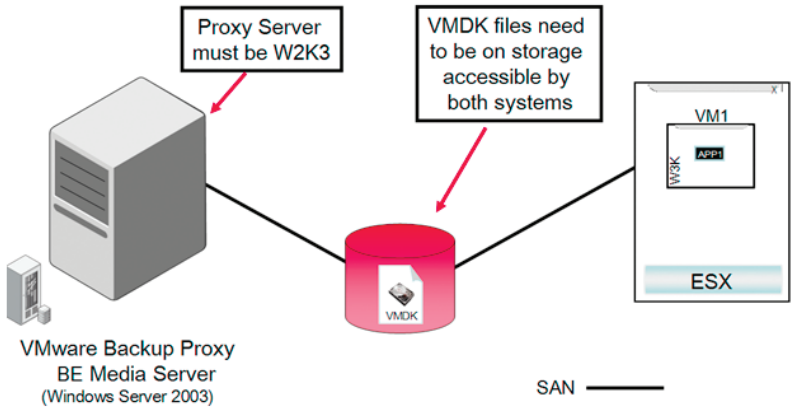

Figure 4. VCB Proxy Server backup configuration

Disadvantages of basic script-level VCB backups

It is important to understand that both image- and file-level VCB backups must be performed separately to obtain both complete backup of a guest virtual machine and individual file recovery. This "two-step" process results in double the backup time, double the disk or tape backup media storage, and twice the backup administrator's time to ensure that both backups run successfully.

In addition, you must download, install, configure, and manage the VMware created VCB scripts for Backup Exec 12.5 in order to perform these functions. You can obtain VCB and the VCB interoperability modules specifically for Backup Exec directly from VMware at http://www.vmware.com/download/download.do?downloadGroup=VCB.

Optimizing VMware Virtual Infrastructure (ESX) 3 backup and recovery

Backup Exec 12.5 Agent for VMware Virtual Infrastructure (AVVI) brings the advantages of VCB—such as off-host backup—while removing some of the challenges of implementing a script-based VCB-based backup solution. Improvements have been made in several key areas over just basic VCB script-level integration. AVVI efficiently:

- Integrates with key VMware APIs to ensure that VCB "scripting" or "integration modules" are not required
- Eliminates separate VCB backups for system-level vs. individual file-level recovery to recover a single file from within a .vmdk file
- Protects VSS-aware applications such as Exchange, SQL, or SharePoint as part of the entire guest virtual machine (see "Best Practices").

AVVI itself requires no "agent" to be installed on the ESX Server, and no configuration is required for VCB backups to take place. All of the support necessary to perform backups of the VMware Virtual Infrastructure is included (see figure 5).

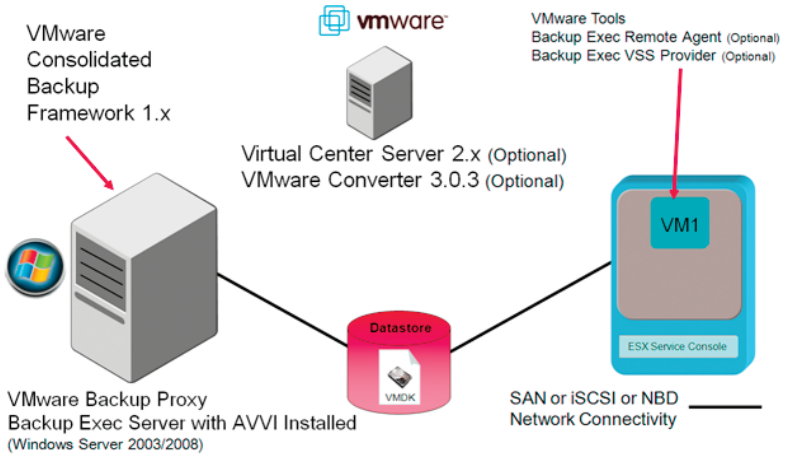

Figure 5. Backup Exec 12.5 AVVI configuration

Backup Exec 12.5 AVVI features and benefits

AVVI Features	Benefits
Integration with VMware Virtual Infrastructure 3 (VI3)	AVVI supports and integrates with all key VMware technologies, including VCB, VirtualCenter, VMotion, VMware Converter, ESX/ESXi, and VMware Tools.
"Scriptless" VCB integration with Backup Exec	AVVI is integrated directly into the Backup Exec 12.5 console and does not require VCB "scripts" or "integration modules" to protect a VMware environment.
"Agentless" guest VM backup	Backups can be done without installing a Backup Exec Agent inside guest virtual machines or on the ESX host server. The AVVI license is simply activated through the media server, and Backup Exec can automatically discover the VMware Virtual Infrastructure, including VMware ESX servers and guest machines, via VMware's VirtualCenter.
Simplified licensing and pricing	A single AVVI license can protect all Windows and Linux guest VMs on an ESX Server. Simply purchase an AVVI license for each ESX Server in your environment. A single AVVI license includes the ability to protect an unlimited number of guest VMs on the ESX host.
Embedded Granular Recovery Technology (GRT)	Included GRT technology provides the ability to restore individual files and folders inside of guest virtual machine without restoring the entire guest virtual machine (Windows guest machines only)
Application protection via VSS	When protecting the entire Windows Guest VM, AVVI can provide protection of applications via Microsoft's Volume Shadow Copy Services (VSS). This allows the entire server and application to be recovered together.
Integrated with Backup Exec to enable protection of virtual and physical systems	Backup Exec 12.5 AVVI can automatically discover your VMware virtual environment next to your physical environment to provide seamless protection for both.

Using Backup Exec 12.5 Agent for Virtual Infrastructure (AVVI)

Once the Backup Exec Agent for VMware Virtual Infrastructure license has been installed on the Backup Exec server, the easy-to-use Backup Exec interface can communicate with VMware's VirtualCenter or with individual ESX Servers to walk administrators through the process of identifying the necessary ESX hosts, groups, and guest virtual machines for fast and simple backup and recovery (see figure 6).

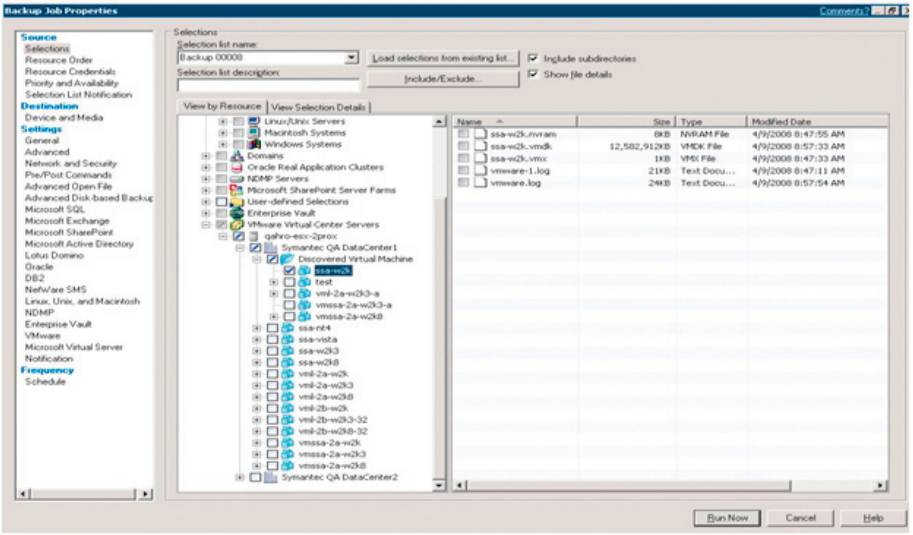

Figure 6. Discovering and selecting guest VMs

The entire guest VM and all of its necessary components are automatically selected for backup, including the guest VM's .vmdk files, .vmx, .log files, and .nvram files (see figure 7).

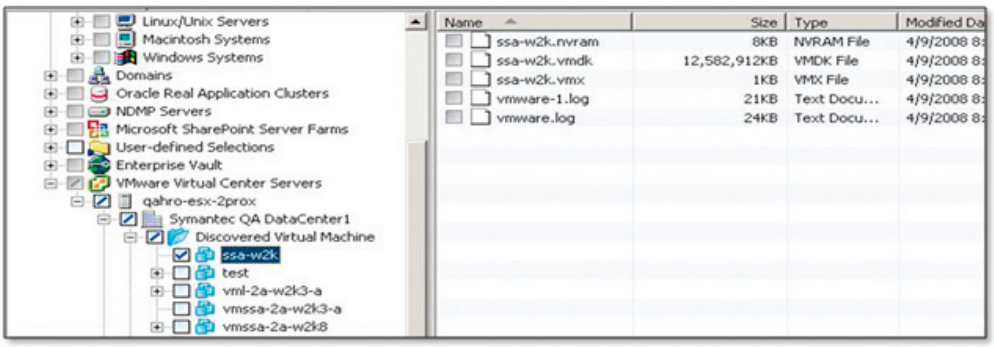

Figure 7. Protecting guest VMs

When the need arises to recover and entire guest VM, simply browse to your protected guest VM systems in the Backup Exec console to restore the entire guest VM or individual .vmdk files (see figure 8).

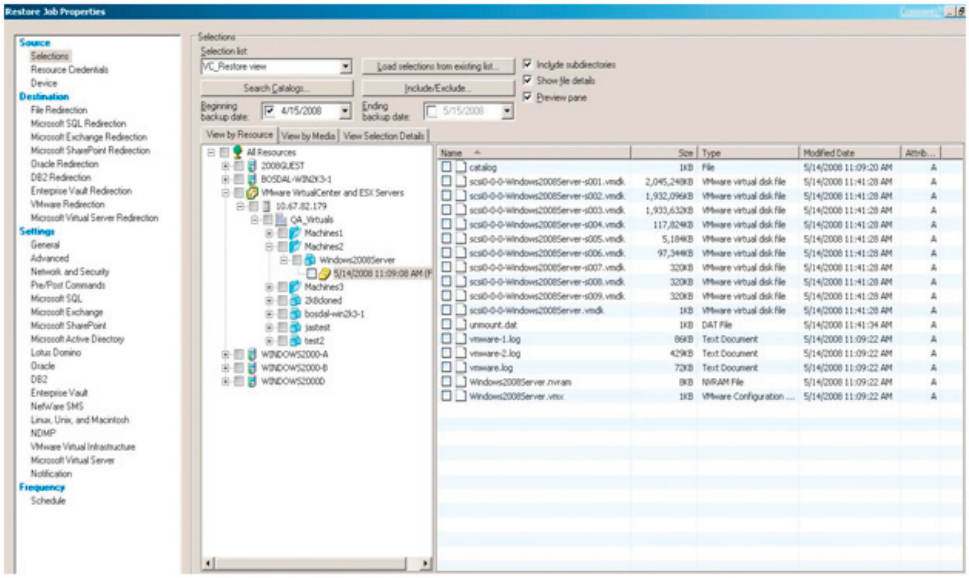

Figure 8. Restoring guest VMs

Alternatively, use Backup Exec's built-in Granular Recovery Technology (GRT) to allow an individual file or folder to be recovered from within a .vmdk file ***without*** having run a separate backup of the file or folder (see figure 9).

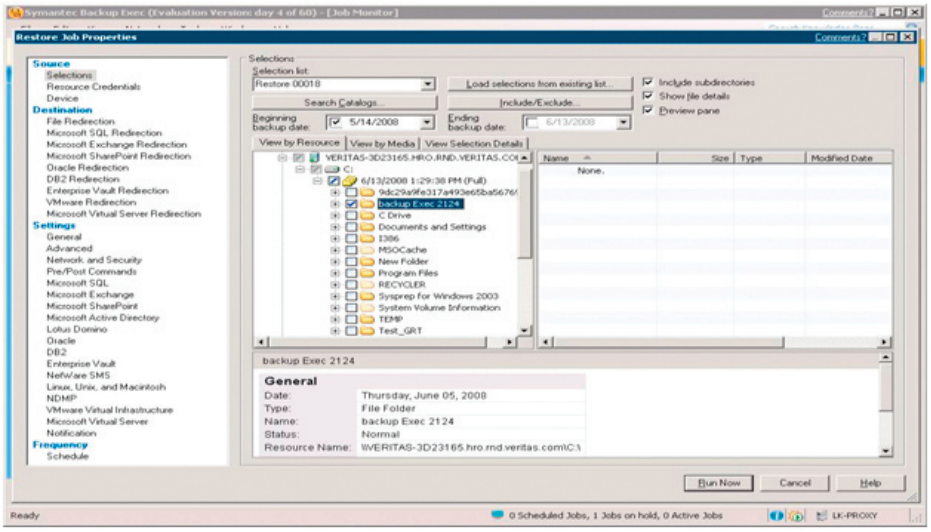

Figure 9. Restoring individual files and folders

Backups can be restored to their original locations or to alternate locations, including alternate datastores, host ESX Servers, different virtual machine names, and different virtual networks (see figure 10).

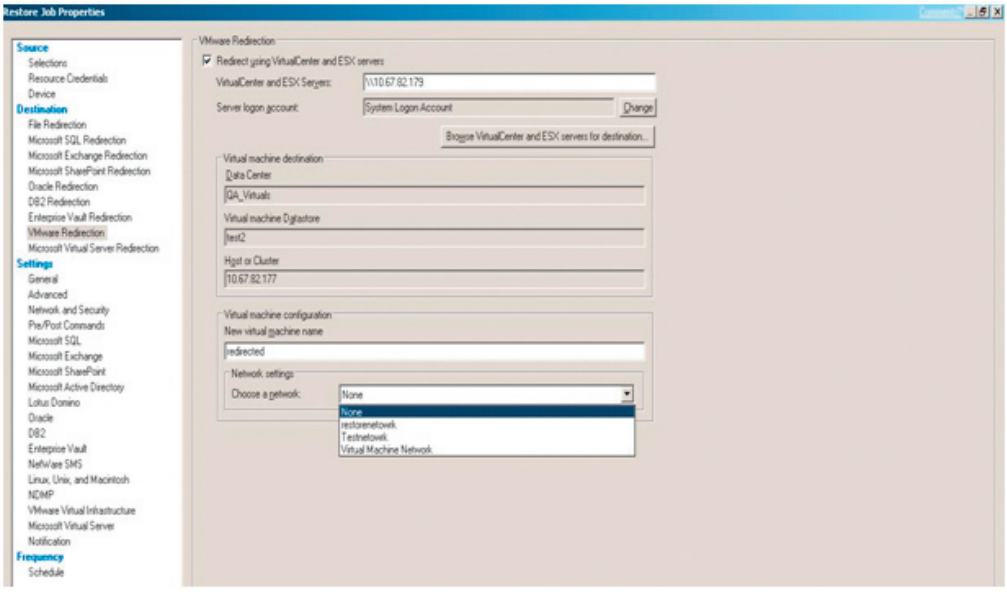

Figure 10. Restoring to original or alternate locations

VMware backup method comparison chart

The following table provides a comparison of the VMware backup methods described in this document.

Table 2. VMware backup methods

Feature	Backup Exec 12.5 Agent for VMware Virtual Infrastructure (AVVI)	Agent Level Guest VM Backup	Scripted VCB Off-Host Proxy Level Backup	Service Console Backup via RALUS*
Integrated with VMware VCB backup framework	YES Support for VMware's VCB framework has been integrated into the backup console without any scripting or integration modules required	NO There is no integrated support for VMware's VCB framework when Agents are installed inside the guest VMs	NO Requires separate scripts or integration modules for VMware VCB support as pre-/post-job scripts	NO No support for VMware's VCB framework
Individual file-level and folder recovery from a single-pass image-level backup of a guest VM (.vmdk)	YES AVVI uses Backup Exec's Granular Recovery Technology (GRT) to recover individual files, directories, or entire volumes ***without*** restoring the entire guest VM .vmdk	NO Individual files, directories, or entire volumes can only be selected for restore for a guest virtual machine when a Backup Exec Agent is used for backup	NO Individual files, directories, or entire volumes can only be selected for when a separate 2nd pass file-level VCB backup has been performed	NO The entire .vmdk file must be restored; individual files from within the .vmdk cannot be restored separately
Integrated with VMware VirtualCenter	YES AVVI can communicate directly with VMware VirtualCenter to automatically discover and display your VMware environment	NO Individual files, directories, or entire volumes can only be selected for restore for a guest virtual machine when a Backup Exec Agent is used for backup	NO Individual files, directories, or entire volumes can only be selected for when a separate 2nd pass file-level VCB backup has been performed	NO The entire .vmdk file must be restored; individual files from within the .vmdk cannot be restored separately
Agentless backup of guest virtual machines	YES AVVI allows Backup Exec to communicate directly with VirtualCenter or individual ESX Servers to provide protection of guest VMs without installing an Agent on the ESX or guest VM	NO Individual guest VM backup requires an Agent to be installed inside each guest VM	YES Provides basic backup without requiring an Agent to be installed inside each guest VM	NO Requires Agent to be installed on ESX Service Console (not possible with ESXi) and does not offload backup I/O
Off-host backup processing	YES AVVI uses VMware's VCB to offload backup tasks from ESX Server systems to one or more dedicated backup VCB Proxy Servers, reducing the load on the ESX Server systems	NO Off-host backups are not currently supported with Agent-level backups of guest virtual machines	YES Provides basic script-level VCB backup support for off-host backups	NO Backups of the .vmdk and .vmx files with the RALUS Agent must be done on-host on the VMware ESX 3 server to a remote Backup Exec 12.5 server

Comparison Chart continued

Feature	Backup Exec 12.5 Agent for VMware Virtual Infrastructure (AVVI)	Agent Level Guest VM Backup	Scripted VCB Off-Host Proxy Level Backup	Service Console Backup via RALUS*
Included application support	YES AVVI included VSS support to protect VSS-aware applications (such as Microsoft Exchange, Microsoft SQL, Microsoft SharePoint, etc.) when protecting the entire guest VM	YES Backups of applications are available via the corresponding Backup Exec Agent when installed inside the guest virtual machine running the application	YES VCB 1.5 does support the backup or recovery of online application data beyond a crash-consistent file system backup of the .vmdk file	NO RALUS does not currently support the backup or recovery of online application data beyond a crash-consistent file system backup of the .vmdk file
Leverages VMware Converter for customized guest virtual machine restores	YES AVVI leverages VMware Converter to restore Guest VM's backup to their original or alternate location with different virtual machine name and/or different network	NO VMware Converter integration is not available	YES A SAN is required to perform VCB off-host proxy backups	NO VMware Converter integration is not available
Online backups of guest virtual machine	YES AVVI leverages VMware VCB to communicate with VirtualCenter or individual ESX Servers to perform online off-host backups of guest VMs	YES The Backup Exec 12.5 Agent for Windows Servers (AWS) and the Backup Exec System Recovery 7.0 Option (BESRO) can both be installed into the guest virtual machine to take online backups without being shut down	YES VCB enables online backups of guest virtual machines	YES Backup Exec 12.5 Remote Agent for Linux and UNIX (RALUS) can use the vcbMounter and vcbRestore VMware tools to perform online backups of guest virtual machines
Supports all VMware storage configurations	YES AVVI can support all current storage infrastructures of VMware including SAN, iSCSI, NBD/NFS, and local storage	NO A SAN is not required to perform Agent-level backups of each guest virtual machine	YES VCB scripting can support multiple storage infrastructures including SAN, iSCSI, NBD/NFS, and local storage	NO Public folders can be restored directly by Backup Exec 12.5 GRT-enabled backups to original or redirected locations

*** Backup Exec Remote Agent for Linux and UNIX Servers (RALUS) does not support ESX 2.x. It is compatible with ESX 3.x servers only.**

Licensing Backup Exec 12.5 Agent for VMware Virtual Infrastructure

The Backup Exec Agent for VMware Virtual Infrastructure is designed to accommodate the needs of large and small deployments—whether it is a single ESX host or a robust, multi-ESX, VirtualCenter managed environment. It is licensed simply on a per-ESX host basis.

Table 3. Licensing requirements for Backup Exec 12.5 AVVI

Scenario	Customer Environment	Licensing
Protecting three (3) ESX hosts with eighteen (18) guest virtual machines total	Three (3) ESX host systems with eighteen (18) shared guest virtual machines ten (10) running Windows and eight (8) running Linux	**Qty: 3 Backup Exec 12.5 Agent for VMware Virtual Infrastructure licenses** **Note:** No Agent for Windows Systems or Agent for Remote Linux/UNIX Servers license is required for any guest virtual machine hosted on the protected and licensed ESX host. However, application-level or granular application-level recovery requires a separate Backup Exec Application or Database Agent. Please see "Integrated data protection".

AVVI system requirements

Software installation requirements

The following components are required to support Backup Exec 12.5 AVVI:

- VMware ESX 3.0.2, 3.0.3, 3.5, or later
- VMware Converter 3.0.3 or later
- VMware VirtualCenter 2.5 or later
- VMware VCB 1.1, 1.5 or later
- VMware Tools (must be installed on guest virtual machines)

Check the Backup Exec 12.5 Software Compatibility List at www.backupexec.com for the most current information.

Backup Exec 12.5 AVVI software installation locations

Installation of AVVI is simple and does not involve installing any software on the ESX server. The following section describes what components of Backup Exec and VMware Virtual Infrastructure are installed, and where they are installed (see figure 11):

- One or more backup proxy systems must be installed, running Microsoft Windows 2003 SP1 or later and having network connectivity to the VirtualCenter Server managing your ESX cluster (or to the ESX server system, if you are not using VirtualCenter and have only one ESX server system) and containing a Fibre Channel host bus adapter (HBA).
- For best performance, it is recommended that Backup Exec 12.5 for Windows Servers be installed on the VCB Windows 2003 Proxy Server to perform the backups of the exported data from the ESX 3 servers.
- VCB 1.1 or later software from VMware must be installed on the Windows 2003 VCB Proxy Server.
- VMware Converter 3.0.3 can be installed on the VCB Proxy Server or other Windows location that is accessible by the Backup Exec server.
- To protect VSS-aware applications such as Exchange, SQL, SharePoint, and Active Directory, a Backup Exec VSS Provider can be installed inside the guest VM. (This VSS Provider is located on the Backup Exec 12.5 CD.) Alternatively, VCB 1.5 also includes a VSS component that can be used in place of the one provided with Backup Exec AVVI. It is important to ensure that both are not used together. See the Backup Exec 12.5 Administrator's Guide for more details on installation of the VSS component.

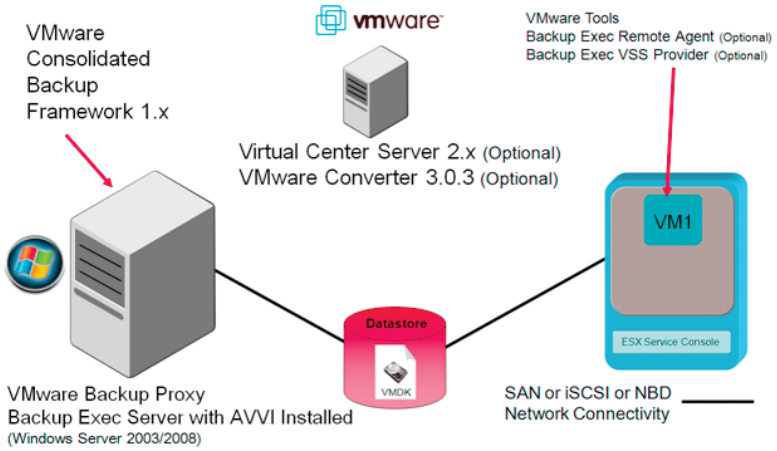

Figure 11. Backup Exec 12.5 AVVI software installation locations

VMware Data Protection best practices with Backup Exec 12.5

Backup configuration

- For best performance, it is recommended that Backup Exec 12.5 for Windows Servers be installed on the VCB Windows 2003 Proxy Server to perform the backups of the exported data from the ESX 3 servers. If Backup Exec is installed on a separate server from the VCB Proxy Server, Backup Exec 12.5 for Windows Servers or the Backup Exec 12.5 for Windows Servers Agent for Windows Systems (AWS) must be installed on the Windows 2003 VCB Proxy Server.
- When performing VCB image-level backups, care must be taken to ensure that sufficient disk space exists on the VCB Proxy Server for all .vmdk files that will be copied directly to it for off-host backup.
- Do not use both the Symantec Backup Exec VSS Provider and the VCB 1.5 VSS Requester together on the same guest VM system. Only install one or the other.
- VSS-enabled backups via VCB of guest VMs that contain applications such as Microsoft Exchange, SQL, SharePoint, and AD are NOT intended to replace traditional application- or database-level backups via Backup Exec Application/Database Agents. VCB backups with VSS enabled do not support application- or database-level full, incremental, or differential backup methods. The Backup Exec backup methods supported with VCB VSS backups are COPY backups that do not truncate log files of the application or provide application granular recovery.

- For SAN backups, the off-host VCB Proxy Server will need to be zoned properly to see the VMFS LUNs that the ESX servers use. VCB will mount a VM's .vmdk file to a directory on the centralized Windows VCB server and allow the contents of the .vmdk to be backed up.
- To avoid snapshot-associated issues, backups should be scheduled during times of relatively low I/O activity on the VM. Reducing the number of simultaneous backups (and, in turn, VCB snapshots) can help with this as well.
- Upgrade to the latest version of VMware Virtual Infrastructure. This includes the latest version of ESX Server, Virtual Center Server, and VCB Framework. Newer versions of Virtual Center components typically have enhancements that improve VCB snapshot reliability.
- Once a VCB snapshot is created, data is transferred from the VM datastore to the Backup Proxy mount point. The completion speed of the snapshot process can be significantly enhanced if care is made to ensure that the data path from the datastore to the snapshot mount point is as fast as possible. The snapshot mount point should be configured over as many dedicated spindles as possible.
- RDM disks are not currently supported through VCB backups and will be automatically skipped.

Restores

- VCB provides no direct-restore capability to individual guest VMs. A Backup Exec Agent for Windows Systems (AWS) is to be installed on the target guest VM to perform Granular Recovery Technology–enabled restores of individual files and folders. Alternatively, an alternate client restore can be performed to a Windows share, and the restored files may be accessed and transferred to the VM through this share.
- Granular recovery of individual files and folders from within a .vmdk file works best when restoring from a disk-based backup. While granular recovery from a tape-based backup is supported, it does require temporary staging of the entire .vmdk file to a disk location during the restore; the staged file will then be removed. Please ensure that there is sufficient disk space on the temporary staging location specified in the restore job properties to recover the entire .vmdk file.

Summary

Server virtualization has quickly risen to mission-critical status in many companies—therefore, keeping it highly available and protecting its data is not an option, but a business requirement. Consequently, backup and recovery, including full disaster recovery, are among the most critical processes of data centers that contain virtualized servers. Backup Exec 12.5 introduces a number of new and powerful capabilities to protect your VMware environment as part of your overall backup strategy—and it maintains the ease of use that has made Backup Exec the solution of choice for thousands of IT administrators for more than 15 years.

For more information on Backup Exec 12.5, please visit www.backupexec.com.

Reference Materials

Title: Consolidated Backup in VMware Infrastructure 3
Description: Covers the VMware Consolidated Backup functionality that was introduced with ESX Server 3
URL: www.vmware.com/pdf/vi3_consolidated_backup.pdf

Title: ESX 3.x Backup Compatibility Guide
Description: Backup software compatibility for ESX Server 3.x
URL: http://www.vmware.com/pdf/vi3_backup_guide.pdf

Title: Virtual Machine Backup Guide
Description: ESX Server 3.01 and VirtualCenter 2.01 virtual machine backup guide
URL: http://www.vmware.com/pdf/vi3_30_20_vm_backup.pdf

Appendix A: VMware Virtual Infrastructure (ESX) 3 backup terminology

Term	Description
AVVI	Backup Exec 12.5 Agent for VMware Virtual Infrastructure.
.VMDK	All the information of a physical server, including the operating system, applications, and data, is included in a VMware virtual disk file or files. Each VMware guest virtual machine has at least one physical disk file associated with it. VMware places these files on top of VMFS and adds a ".vmdk" extension to each file.
Guest VM	Guest virtual machine running in a VMware environment that includes .vmdk file, which represents virtual hard disks, and .vmx files, which represent the system configuration.
VCB	VMware Consolidated Backup (VCB) is a set of command line executables developed by VMware and designed to offload backups of guest virtual machines on the ESX Server to a separate VCB Windows 2003 Proxy Server.
VCB Proxy Server	A physical machine running Microsoft Windows 2003, Consolidated Backup, and third-party backup software (in this case Backup Exec) that is used to perform off-host file-level and full virtual machine backups of VMware virtual machines.
Backup Exec RALUS	Backup Exec Remote Agent for Linux and UNIX Servers. This is not a VMware term, but is important to understand for the purposes of this paper. This Agent is available for purchase separately for Backup Exec 12.5 for Windows Servers to enable the remote backup of Linux and UNIX servers—in this case VMware ESX 3 servers when installed into the ESX 3 Service Console.
VCB file-level backup	A file-level backup is a backup of individual files contained on the disks within a virtual machine. It can include all files and/or directories, or just selected files and/or directories. In addition, incremental or differential backups can be performed to protect only those files that have changed since a previous backup (full, differential or incremental file backups). File-level backups allow files or directories to be restored individually, which is often desirable in the case of file corruption or accidental file deletion. File-level backups can be done with either VCB or via Backup Exec Agents installed within guest virtual machines.
VCB image-level backup	A virtual machine image backup includes of all the disk (.vmdk) and configuration (.vmx) files associated with a particular virtual machine, allowing the entire virtual machine to be restored to a state just as it was at the time the backup was made. It is a complete volume-level backup. This capability is important for rapid and efficient disaster recovery of entire .vmdk files. Image-level backups can either be done via VCB or RALUS backups within the ESX Service Console.
VMFS	VMware VMFS is a high-performance file system on physical SCSI disks and partitions, including SAN and iSCSI storage systems. ESX Server uses the VMware VMFS file system for storage of virtual machines.

About Symantec

Symantec is a global leader in providing security, storage, and systems management solutions to help businesses and consumers secure and manage their information. Headquartered in Cupertino, Calif., Symantec has operations in more than 40 countries. More information is available at www.symantec.com.

For specific country offices and contact numbers, please visit our Web site. For product information in the U.S., call toll-free 1 (800) 745 6054.

Symantec Corporation
World Headquarters
20330 Stevens Creek Boulevard
Cupertino, CA 95014 USA
+1 (408) 517 8000
1 (800) 721 3934
www.symantec.com

Copyright © 2007, 2008 Symantec Corporation. All rights reserved. Symantec, the Symantec Logo, and Backup Exec are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Linux is the registered trademark of Linus Torvalds. Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Other names may be trademarks of their respective owners.
09/08 14547361