VMWARE VIRTUAL MACHINE PROTECTION

DELL POWERVAULT DL 2000 POWERED BY SYMANTEC

VMware Virtual Machine Protection

The PowerVault DL2000– Powered by Symantec Backup Exec offers the industry's only fully integrated backup-to-disk solution with software factory installed. Dell and Symantec have co-developed this offering to give you easier management capabilities of the backup-to-disk environment. It's an ideal way for any IT department to achieve faster, more reliable backups and restores. In addition, the appliance simplifies the backup and recovery of VMware based virtual environments by integrating with VMware Virtual Center, VMware Consolidated Backup, and VMware Converter.

Server virtualization is quickly becoming a standard technology in many data centers today. While VMware significantly augments hardware utilization through server virtualization, VMware's Virtual Infrastructure (ESX) 3 introduces new issues related to protecting and recovering virtual environments.

Data created and utilized in virtual machines is no less important than data 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 Backup Exec for Windows Servers and the Agent for VMware Virtual Infrastructure (AVVI). This paper also discusses the relative advantages and disadvantages of each method.

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 an essential requirement of managing your virtual infrastructure. VMware's Virtual Infrastructure 3 (VI 3) has quickly become an industry standard for organizations looking 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 cost savings that server virtualization delivers. This includes not only the Guest virtual machines, but also the applications that have been installed on those Guest virtual machines such as Microsoft Exchange, SQL, and SharePoint Server. A lost ESX server could impact productivity up to several hours, or even days, for multiple departments while the IT administrator struggles to recover the virtual environment and the individual Guest virtual machines.

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

- Having to install a backup agent inside of each Guest virtual machine or on the ESX server directly
- Recovery of a single file typically requires a long restore of the entire Guest virtual machine
- Separate backups for system level vs. individual file level recovery
- Taking Guest virtual machines off-line during backup in order to protect them completely
- Concerns about ensuring applications running inside of the Guest virtual machines can be recovered
- Having to use separate backup products for physical vs. virtual machines

Traditionally, this problem has been overcome with the use of VMware utilities that allow 3rd party backup software to perform backups within the ESX Service Console of running Guest virtual machines. Unfortunately, performing the live or "Hot" backups of running Guest virtual machines using these utilities can require using 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 and all of the users connected to the Guest virtual machines on that ESX server. Performing a hot backup can prove to be difficult or impossible to manage manually and certainly is not cost effective if it's not centralized and useable by the necessary staff.

VMware Virtual Infrastructure 3 introduces new technology, VMware Consolidated Backup(VCB), to help overcome some of these challenges with the traditional backup methods of virtual machines, but it also introduces some backup and recovery challenges of its own that need to be considered for all environments planning on implementing it including:

- Managing cumbersome and complicated VCB "scripts" to integrate with existing backup products
- Installation of proprietary VCB "integration modules" that require additional testing and setup
- Separate backups for system level vs. individual file level recovery to recover a single file from a .vmdk

This paper attempts to discuss these topics, how Backup Exec can help address these unique challenges, and ultimately provide sufficient information to administrators to 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, you should identify the items that need to be addressed for recovery in your environment before a recovery is required. Typically, with VMware's Virtual Infrastructure 3 (VI3), the major components that need to be considered for backup are (see Figure 1- VMware Virtual Infrastructure 3 ESX Architecture):

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

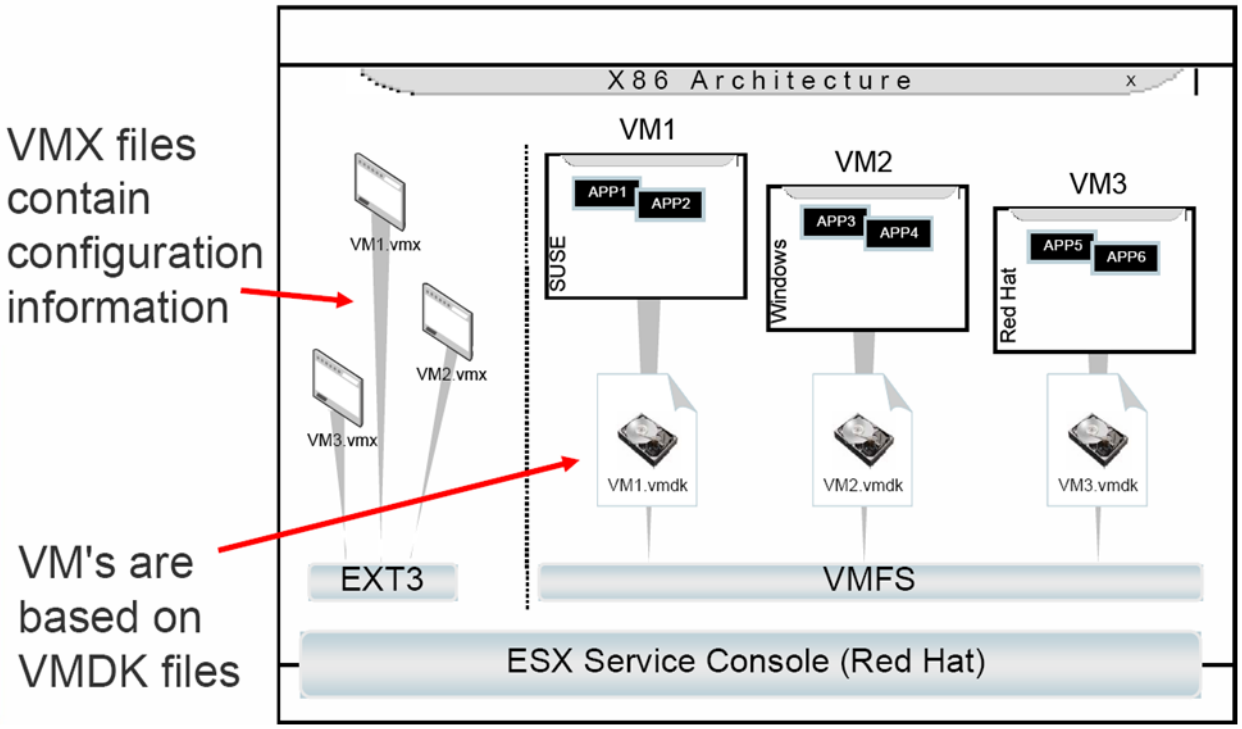

Figure 1. VMware Virtual Infrastructure (ESX) 3 Architecture

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 can be configured to safely protect VMware environments. Before planning your backup and recovery processes of your virtual environment you should consider several questions first, 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?
- While one virtual machine is being backed up, what is the performance impact on additional virtual machines hosted on the same physical ESX 3 server during the backup?
- What are the relative advantages\disadvantages of each of these backup techniques?
- What are the relative advantages\disadvantages in terms of recovery of the ESX server and the guest virtual machines?
- How would you perform a disaster recovery of an entire Guest virtual machine?
- Does a combination of these backup methods make sense for my 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 Backups
- Installing Linux Agent on ESX Server
- Basic Script-level VCB Integration

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 is required to be purchased and installed in each Guest VM (see **Figure 2- Installing Backup Exec Agents inside VMware Guest Virtual Machines**). The Guest VM backup is then scheduled and performed as you would with any other Backup Exec protected system on your network.

Advantages of Traditional Agent-Level Backup of Guest VM's

The virtual machines will appear to Backup Exec as normal physical systems. Restores of data contained inside of the Guest virtual machines are done the same as they would be for any standard Backup Exec restore job.

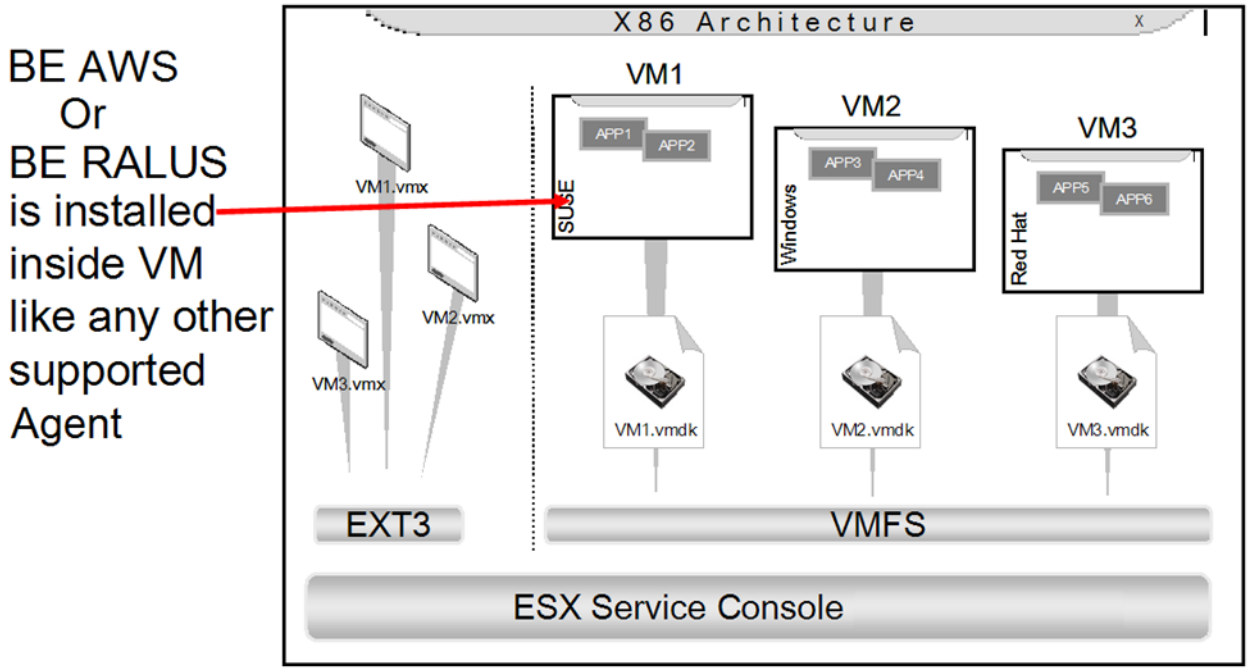

Figure 2. Installing Backup Exec Agents inside VMware Guest Virtual Machines

DISADVANTAGES OF BACKUP EXEC AGENTS IN GUEST VM BACKUP

Installing an Agent in each of the Guest VM systems can be cost prohibitive for many organizations in terms of both money and 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, if three Guest virtual machines running Windows 2003 being protected by a Backup Exec Media Server would require:

- 1 Backup Exec for Windows Servers Media Server License
- 3 Backup Exec Agent for Windows Systems (AWS) Licenses (Agent for Windows Systems licenses include both a Continuous Protection Agent and a Remote Agent for Windows Systems license)

SERVICE CONSOLE BACKUP AND RECOVERY METHOD OF .VMDK FILES WITH

The Backup Exec 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- Installing RALUS in the VMware ESX 3 Service Console**)

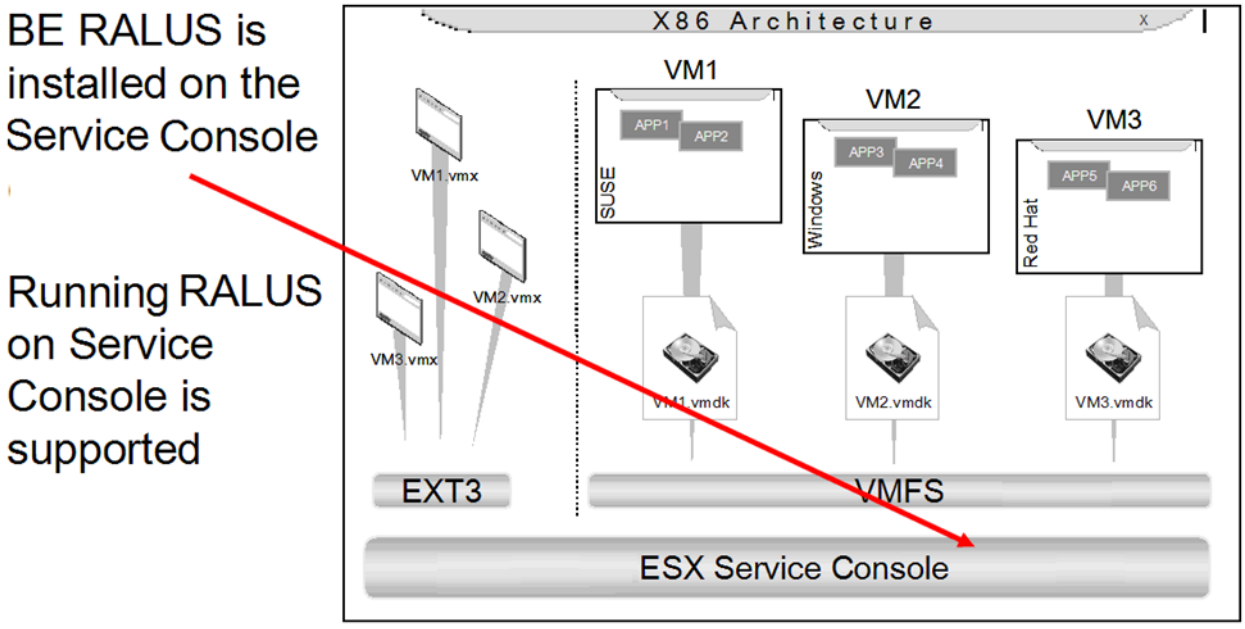

Figure 3. Installing RALUS in the VMware ESX 3 Service Console

DISADVANTAGES OF BACKUPS WITH RALUS IN SERVICE CONSOLE

Care needs to be taken when backing up these files to make sure they are backed up in a consistent manner, assuring that restored files are not corrupt. Before backing up the vmdk files, 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

These commands can be used by Backup Exec in a backup job automatically as a pre\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 for Windows Servers RALUS Agent requires ESX 3 or later and will not install or function correctly on an 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 backing up the service console OS does not need to occur very frequently. Additionally, 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 could be facilitated if a current backup of the service console was 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 mentioned in the previous section

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 for all of the users connected to virtual machines being hosted by that ESX server.

ADVANTAGES OF BASIC SCRIPT LEVEL VCB BACKUPS

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

File Level

- This type of VCB backup will result in the entire file system contents of the .vmdk files to be mounted as local directory (i.e. mount point) on the VCB Windows 2003 Proxy Server that can then be protected by Backup Exec via a normal file system backup of the VCB Proxy Server.

Image Level

- 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 Level 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\post job "scripts", during a backup of an ESX server to perform File Level or Image Level (or a combination) backup of the guest virtual machines by exporting either the File Level data or complete Image Level data (.vmdk, .vmx, and .log files) to the off-host Windows 2003 Proxy Server. (**see Figure 4- VCB Proxy Server Backup Configuration**)

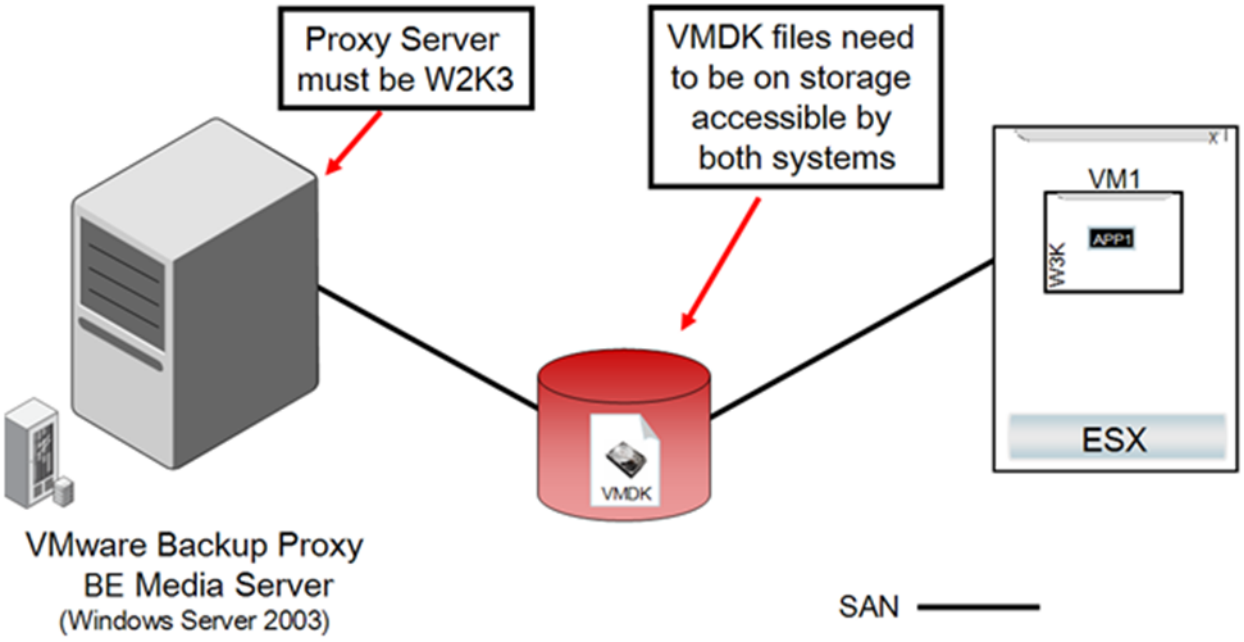

Figure 4- VCB Proxy Server Backup Configuration

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 VM and individual file recovery. This "two-step" process results double the backup time, double the disk or tape backup media storage, and twice the backup administrator's time to ensure both backups run successfully. Additionally, you must download, install, configure, and manage the VMware created VCB scripts for Backup Exec 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

IMPROVING VMWARE VIRTUAL INFRASTRUCTURE (ESX) 3 BACKUP AND RECOVERY

Backup Exec Agent for VMware Virtual Infrastructure (AVVI) takes 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 including;

- Integration with key VMware API's to ensure 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
- Protecting **VSS-aware applications such as Exchange, SQL, or SharePoint as part of the entire Guest virtual machine (**see Best Practices section below)
-

AVV itself requires no "agent" to be installed on the ESX and nothing to be configured for VCB backups to take place. All of the support necessary to perform backups of the VMware Virtual

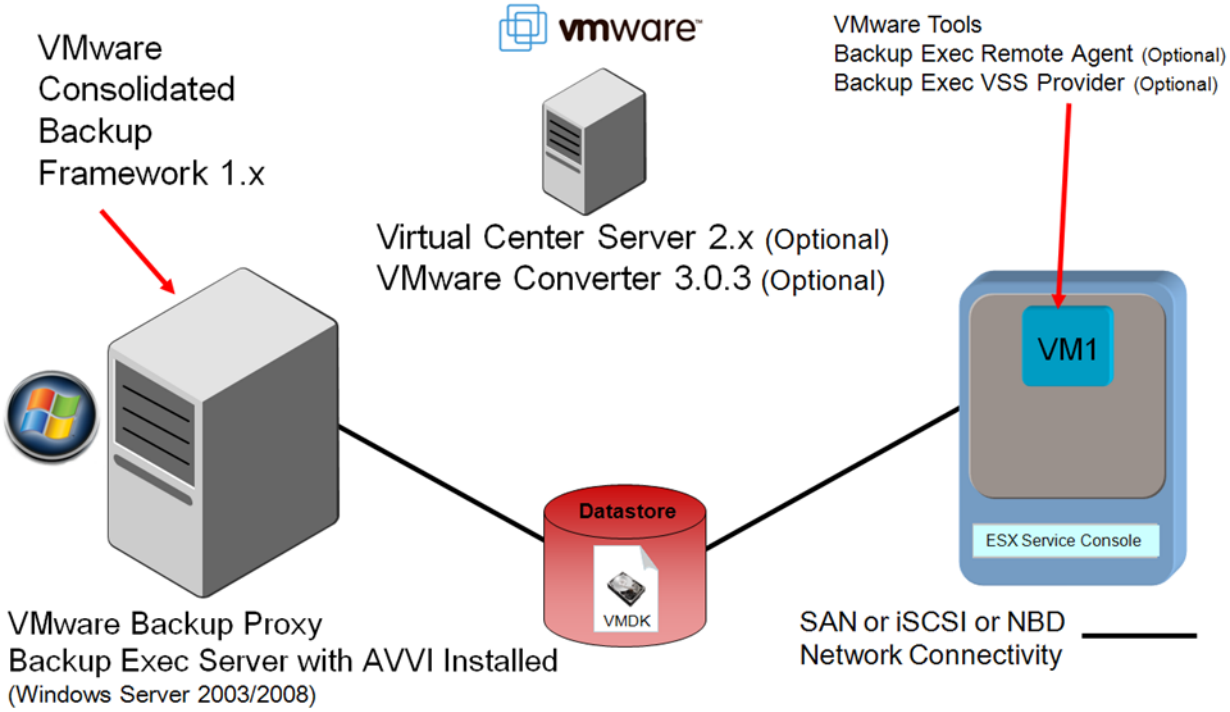

Figure 5- Backup Exec AVVI Configuration

BACKUP EXEC AVVI FEATURES AND BENEFITS

AVVI Features	Benefits
Integrated with VMware Virtual Infrastructure 3 (VI3)	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 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 of Guest virtual machines or on the ESX host server.
Simplified Licensing and Pricing	A single AVVI license can protect all Windows and Linux Guest VM's 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 VM's on the ESX host.
Embedded Granular Restore 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 for the entire server and application to be recovered together.
Restore Anywhere Features	Restore Guest VM's to their original or alternate Datastore locations including specifying different virtual machine name and virtual network to be used after the restore
Integrated with Backup Exec To Enable Protection of Virtual and Physical Systems	Backup Exec AVVI can automatically discover your VMware virtual environment next to your physical environment to provide the seamless protection of both.

USING BACKUP EXEC AGENT FOR VIRTUAL INFRASTRUCTURE (AVVI)

Once the 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- Discovering and Selecting Guest VM's)

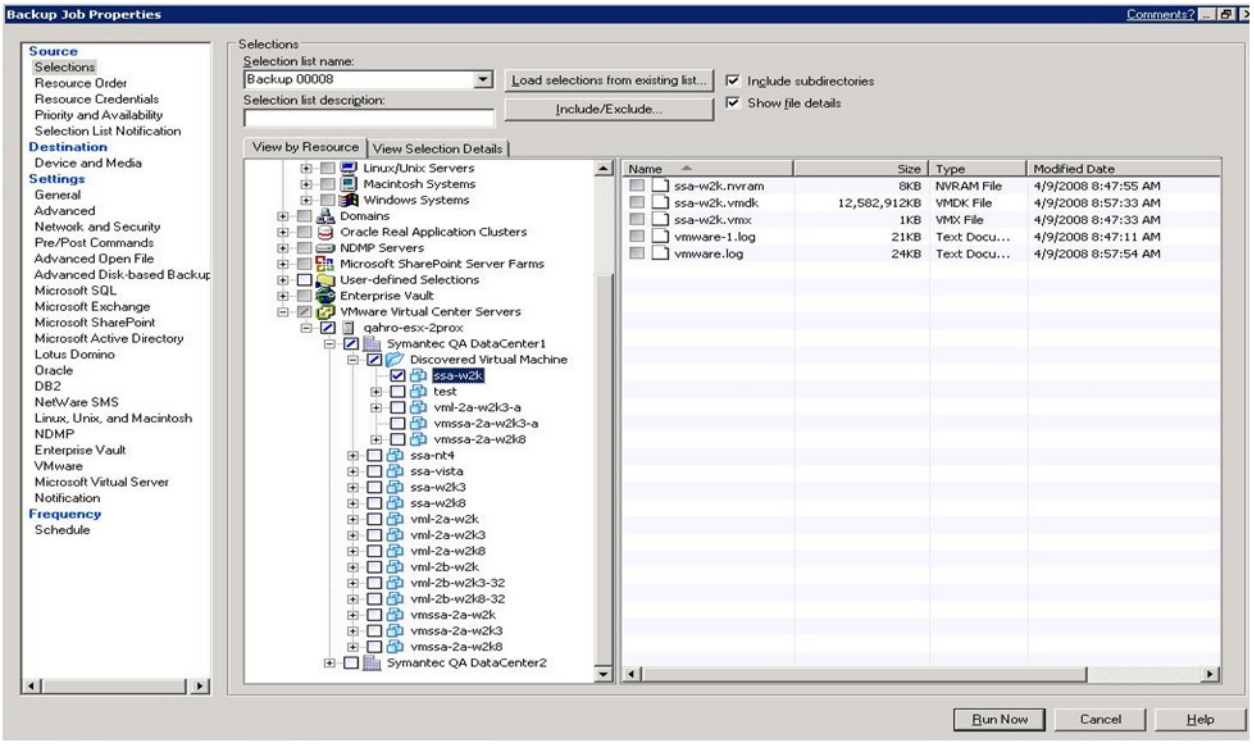

Figure 6- Discovering and Selecting Guest VM's

The entire Guest VM and all of it's necessary components are automatically selected for backup including the Guest VM's .vmdk files, .vmx, .log files, and .nvram files (see Figure 7- Protecting

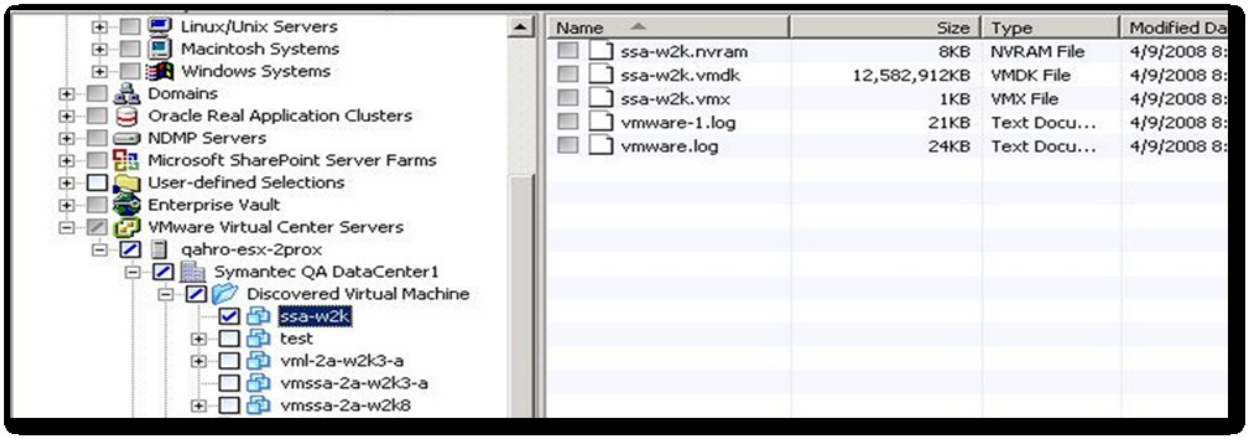

Figure 7- Protecting Guest VM's

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- Restoring Guest VM's)

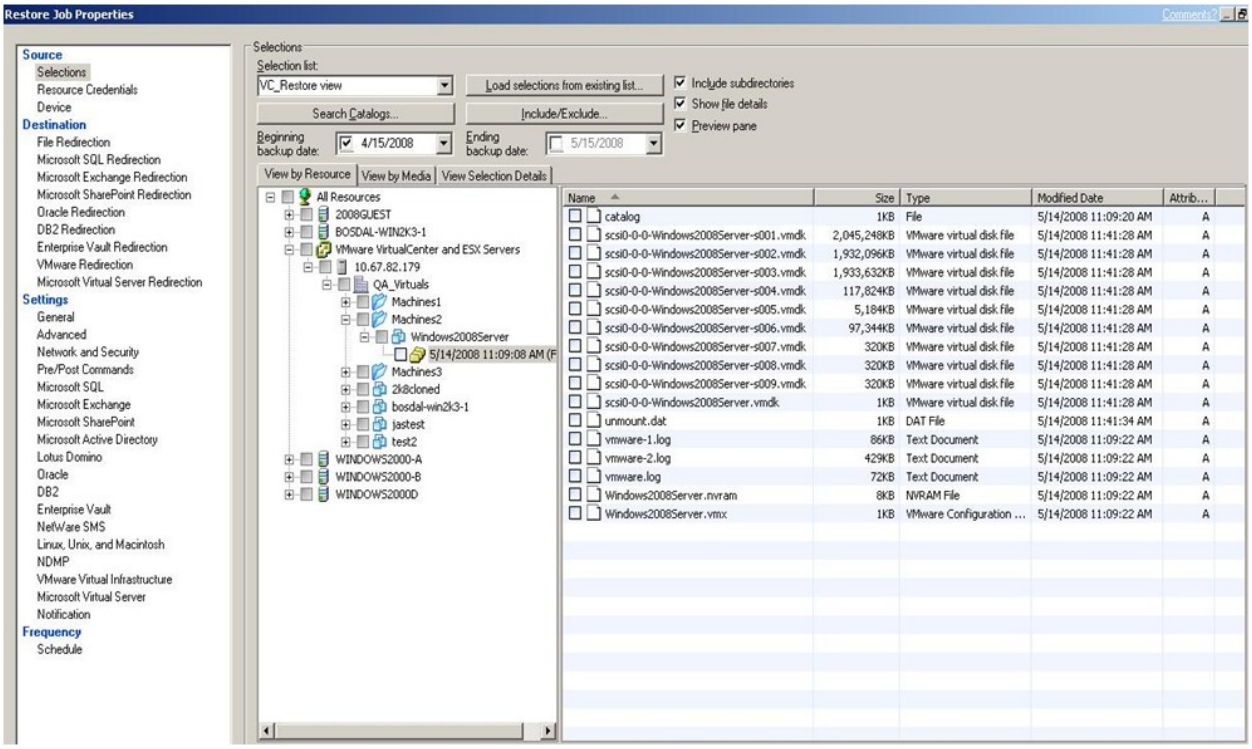

Figure 8- Restoring Guest VM's

Or use Backup Exec's built-in Granular Recovery Technology (GRT) to allow individual file/folder recovery from within a .vmdk file without having to run a separate backup of them. (see Figure 9- Restoring Individual Files and Folders)

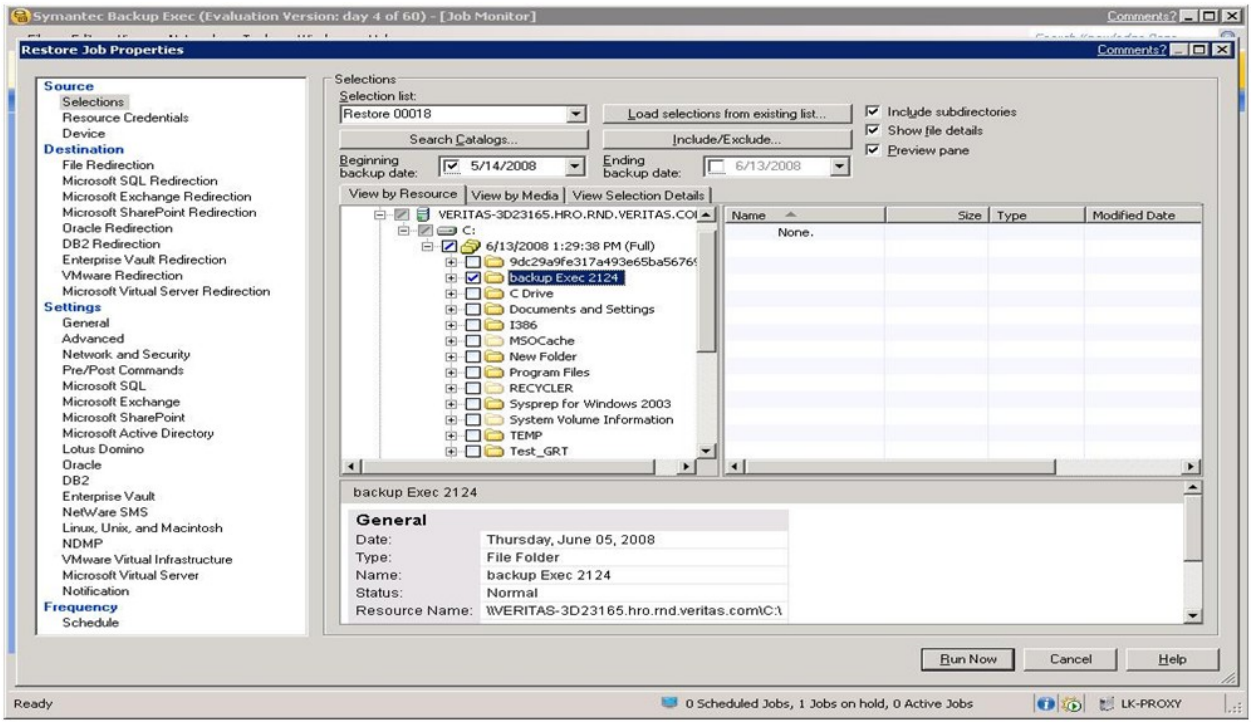

Figure 9- Restoring Individual Files and Folders

Backups can be restored back to their original locations or to alternate locations, including alternate datastores, host ESX servers, with different virtual machine names and to different virtual networks. (see Figure 10- Restoring to Original or Alternate Locations)

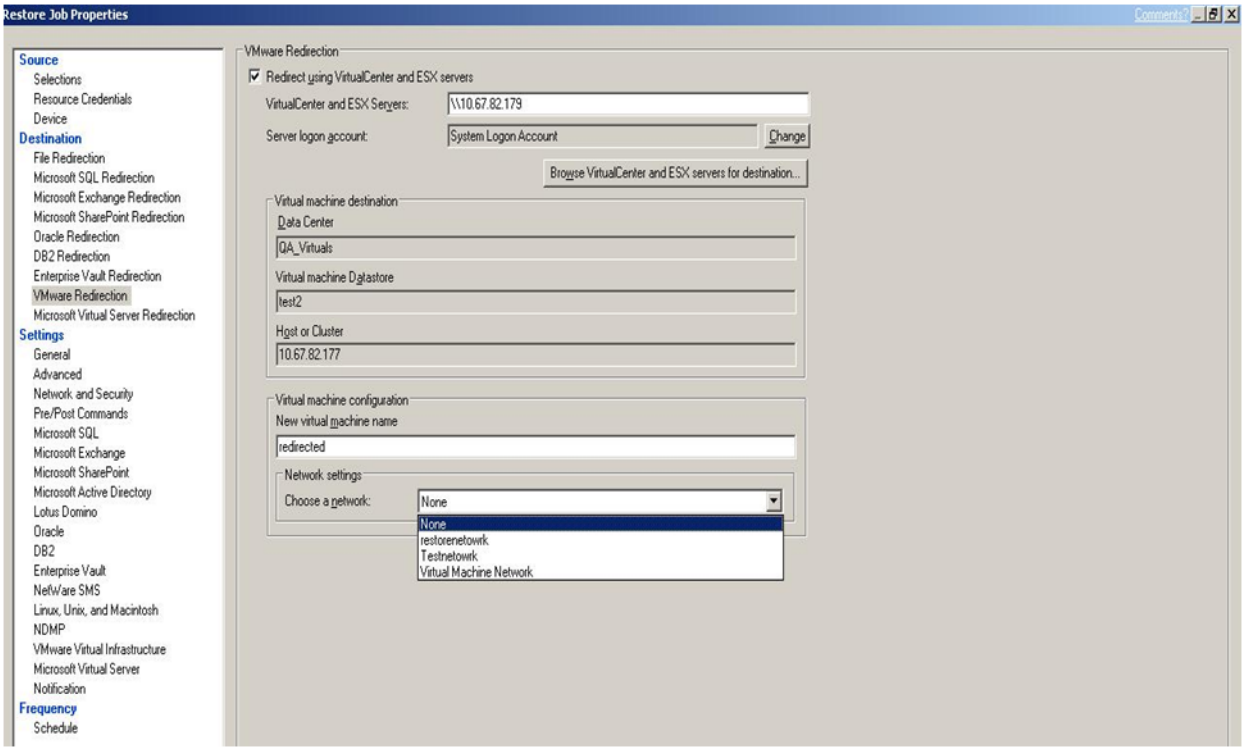

Figure 9- Restoring to Original or Alternate Locations

VMWARE BACKUP METHOD COMPARISON CHART

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

Feature	Backup Exec 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 Agent's are installed inside of the Guest VM's	**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 can be restored ***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 was 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's 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 was 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 VM's without installing an Agent on the ESX or Guest VM	**NO** Individual Guest VM backup requires an Agent to be installed inside of each Guest VM	**YES** Provides basic backup without requiring an Agent to be installed inside of each Guest VM	**NO** Requires Agent to be installed on ESX Service console (not possible with ESXi) and does not off-load 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 Server

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

VMWARE BACKUP METHOD COMPARISON CHART (CONT.)

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

Feature	Backup Exec 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 of 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 VM 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
Leverages VMware Converter for Customized Guest VM 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 VM's	**YES** The Backup Exec 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 shutdown	**YES** VCB enables online backups of Guest virtual machines	**YES** Backup Exec 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 GRT-enabled backups to original or redirected locations.

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

LICENSING BACKUP EXEC 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's a single ESX host or a robust, multi-ESX, VirtualCenter managed environment. It is licensed simply on a per-ESX host basis.

Scenarios	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 of Backup Exec Agent for VMware Virtual Infrastructure licenses**. **Note- No Agent for Windows Systems license or Agent for Remote Linux/Unix Servers 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 the **Integrated Data Protection Section** below

AVVI SYSTEM REQUIREMENTS

To support Backup Exec AVVI, the following components are required:

- 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
- Guest virtual machines are required to have VMware Tools installed on them
- Check the Backup Exec Software Compatibility List for the most current information at www.backupexec.com

LICENSING BACKUP EXEC AGENT FOR VMWARE VIRTUAL INFRASTRUCTURE

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 where. (see Figure 11 below - Backup Exec AVVI Software Installation Locations)

- One or more backup proxy systems running Microsoft® Windows 2003 SP1 or later, 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 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 of the Guest VM. This VSS Provider is located on the Backup Exec 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 Administrator's Guide for more details on installation of the VSS component.

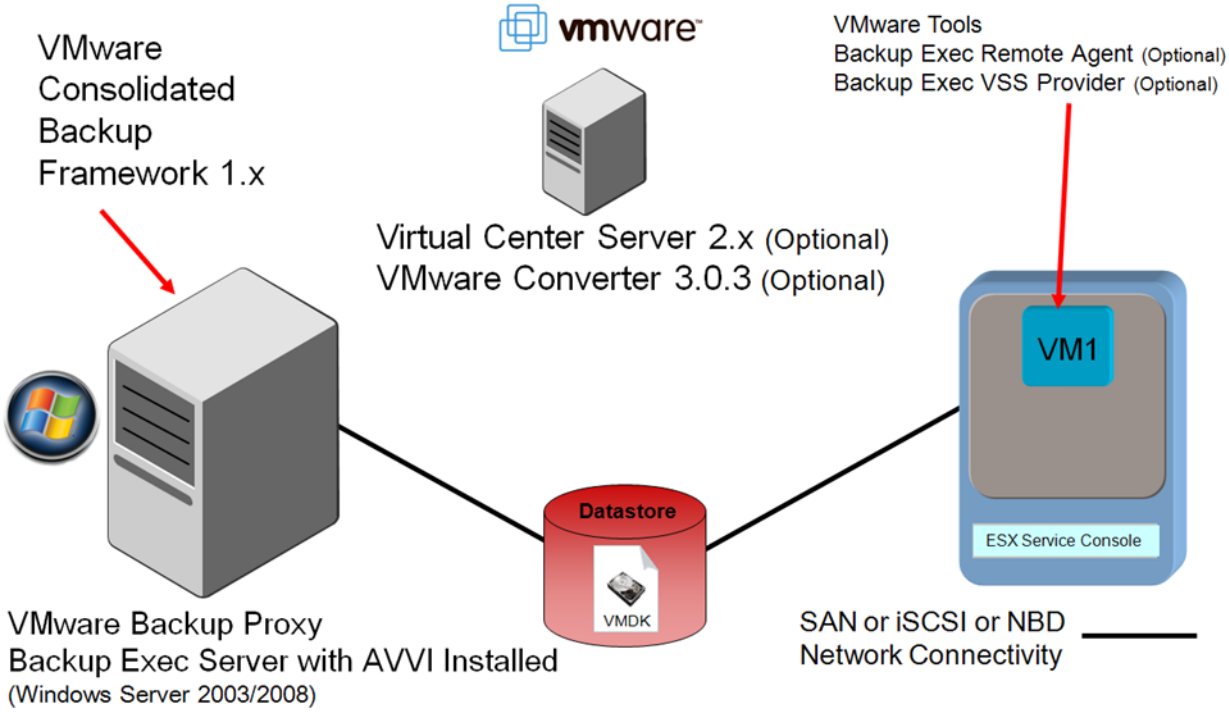

Figure11 - Backup Exec AVVI Software Installation Locations

VMWARE DATA PROTECTION BEST PRACTICES WITH BACKUP EXEC

Backup Configuration

- For best performance, it is recommended that Backup Exec 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 for Windows Servers or the Backup Exec 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 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 VM's that contain applications such as Microsoft Exchange, SQL, SharePoint, and AD are NOT intended to replace traditional application/database level backups via Backup Exec Application/ Database Agents . VCB backups with VSS enabled do not support application/ database level Full, Incremental, or Differential backup methods. The following Backup Exec backup methods are 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 VM's. A Backup Exec Agent for Windows Systems (AWS) 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 file 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 and is then removed. Please ensure sufficient disk space exists 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 datacenters that contain virtualized servers. Backup Exec introduces a number of new powerful capabilities to protect your VMware environment as part of your overall backup strategy while maintaining the ease of use that has made Backup Exec the solution of choice for thousands of IT administrators for over 15 years.