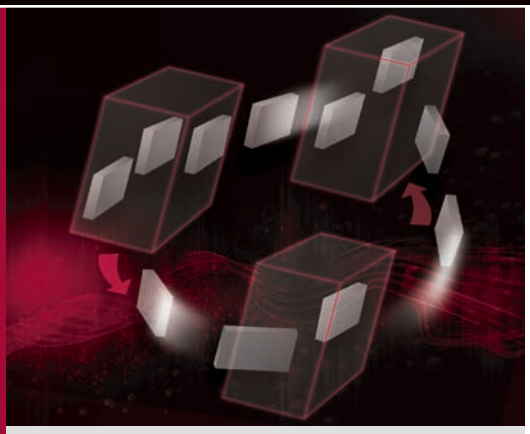

BEST PRACTICES FOR PROTECTING VMWARE INFRASTRUCTURE 3 WITH SYMANTEC BACKUP EXEC

Effectively protecting virtualized environments using traditional backup tools can be both difficult and time-consuming. Symantec® Backup Exec™ 12.5 software, part of the new Dell™ PowerVault™ DL2000 – Powered by Symantec Backup Exec, is designed to provide powerful, simplified backup and recovery for VMware® virtualized environments.

Related Categories:

Backup

Data consolidation and management

Dell PowerVault storage

Symantec

Virtualization

VMware

Visit DELL.COM/PowerSolutions for the complete category index.

Server virtualization is quickly becoming a key element of enterprise data centers, offering advantages ranging from efficient resource utilization to reduced hardware and operational costs. But although data created and utilized in virtual machines (VMs) is typically no less important than data in a single physical server, effectively protecting and recovering data in VMs can be a significant challenge—especially when trying to do so using traditional backup tools not designed for virtualized environments.

Symantec Backup Exec 12.5, part of the new Dell PowerVault DL2000 – Powered by Symantec Backup Exec,[1] introduces several features designed specifically to help protect virtualized environments based on the VMware Infrastructure 3 suite, including the new Agent for VMware Virtual Infrastructure (AVVI). Using these features and following best practices can help organizations overcome some of the challenges of protecting virtualized environments to help implement powerful, simplified backup and recovery.

VIRTUALIZATION BACKUP AND RECOVERY CHALLENGES

As hardware consolidation continues to accelerate, planning backup and recovery strategies for virtualized environments becomes an essential part of data protection. Enterprises are becoming increasingly dependent on efficient backup and quick recovery of their virtual systems and the host systems they run on to help maintain the productivity and cost savings server virtualization can deliver. These virtual systems include not only the VMs themselves, but also the applications that have been installed on those VMs, which might include Microsoft® Exchange, Microsoft SQL Server®, and Microsoft Office SharePoint® Server software. A failed virtualized server could affect productivity for up to several hours, or even days, in multiple departments while administrators struggle to recover the virtualized environment and the individual VMs.

Protecting a virtualized environment with backup technologies not built specifically for virtualization can be both frustrating and time-consuming, typically requiring the following:

- Installing a backup agent inside each VM or directly on a virtualized server
- Taking time to restore an entire VM just to recover a single file
- Maintaining separate backups for system-level and individual file-level recovery
- Taking VMs offline during backup operations to help provide comprehensive protection
- Ensuring that applications running inside VMs can be recovered

[1] For more information on the Dell PowerVault DL2000 – Powered by Symantec Backup Exec, see "Simplified Data Protection with Disk-Based Backup from Dell and Symantec," by Sanjeet Singh and Charles Butler, in *Dell Power Solutions*, November 2008, DELL.COM/Downloads/Global/Power/ps4q08-20080444-Symantec-M.pdf.

- Requiring separate backup products for physical and virtual systems

The VMware Infrastructure suite has quickly become an industry-standard virtualization platform. VMware Infrastructure 3 introduced VMware Consolidated Backup (VCB) to help overcome some of these challenges. But VCB can also introduce challenges of its own that administrators should consider before implementing it—including potentially requiring them to manage cumbersome and complicated scripts to integrate with existing backup systems, install proprietary integration modules that require additional testing and setup, and continue maintaining separate backups for system-level and file-level recovery.

SYMANTEC AGENT FOR VMWARE VIRTUAL INFRASTRUCTURE

The Symantec Backup Exec 12.5 AVVI is designed to provide the advantages of VCB, such as off-host backup, while removing some of the challenges of implementing scripted VCB-based backup systems. Beyond basic VCB script-level integration, it provides integration with key VMware application programming interfaces to help avoid the need for VCB scripting or integration modules, helps eliminate separate VCB backups for system-level and file-level recovery from VMs, and helps protect Microsoft Volume Shadow Copy Service (VSS)–aware applications such as Exchange, SQL Server, and SharePoint as part of a VM.

The AVVI does not require an agent to be installed on a VMware ESX server, and no additional configuration is necessary for VCB backups to occur. All support necessary to perform backups of the virtualized environment is included (see Figures 1 and 2).

After administrators have installed the AVVI license on the Backup Exec server, the simplified Backup Exec interface can communicate with VMware VirtualCenter or with individual ESX servers and guide administrators through the process of identifying the necessary ESX hosts, groups, and VMs for fast, simplified backup and recovery (see Figure 3). The VM and its necessary components—including the .vmdk files, .vmx files, .log files, and .nvram files—are automatically selected for backup.

When administrators must recover an entire VM, they can browse to protected VM systems in the Backup Exec console to restore the entire VM or individual .vmdk files. As an alternative, they can use the built-in Granular Recovery Technology (GRT) in Backup Exec to recover individual files and folders from within a .vmdk file without needing to run a separate backup. Administrators can restore backups to their original locations or to different locations—including alternate data stores, host ESX servers, and virtual networks—and can use the original VM name or a different name.

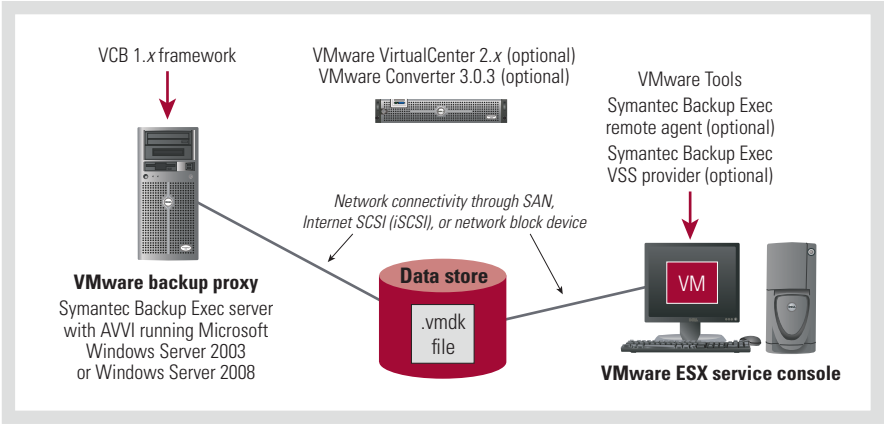

Figure 1. *Example environment using the Symantec Backup Exec 12.5 Agent for VMware Virtual Infrastructure*

Integration with VMware Infrastructure 3	The AVVI supports and integrates with key VMware tools and features, including VCB, VirtualCenter, VMotion™, VMware Converter, ESX and ESXi, and VMware Tools technologies.
Integration with Symantec Backup Exec	The AVVI can automatically discover both VMware virtualized environments and physical environments to help provide seamless protection for both.
Scriptless VCB integration with Symantec Backup Exec	The AVVI integrates directly into the Backup Exec 12.5 console, and requires neither VCB scripts nor integration modules to help protect a VMware virtualized environment.
Agentless VM backup	Backups can be performed without installing a Backup Exec agent inside VMs or on an ESX server.
Simplified licensing and pricing	A single AVVI license supports protection for an unlimited number of Microsoft Windows and Linux® OS–based VMs on an ESX server.
Embedded GRT	GRT technology enables recovery of individual files and folders inside a Windows-based VM without needing to restore the entire VM.
Application protection with Microsoft VSS	When protecting an entire Windows-based VM, the AVVI can also protect applications through VSS—enabling the entire server and application to be recovered simultaneously.
Flexible recovery	Flexible recovery features enable administrators to restore VMs to their original or alternate data store locations, including specifying a different VM name and virtual network use after the restore.

Figure 2. *Key advantages of the Symantec Backup Exec 12.5 Agent for VMware Virtual Infrastructure*

BEST PRACTICES FOR USING SYMANTEC BACKUP EXEC 12.5

Best practices such as the following can help ensure successful backup and recovery in VMware environments:

- To perform backups of exported data from ESX servers, install Backup Exec

12.5 for Windows Servers on a Microsoft Windows Server® 2003 OS–based VCB proxy server. 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 a Windows Server 2003–based VCB proxy server.

- When performing VCB image-level backups, 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.
- Install either the Backup Exec VSS provider or the VCB 1.5 VSS requester on a given VM; do not use both.
- Keep in mind that VSS-enabled VCB backups of VMs that contain applications such as Exchange, SQL Server, and SharePoint should not replace traditional application- or database-level backups through Backup Exec application or database agents. VSS-enabled VCB backups do not support application- or database-level full, incremental, or differential backup methods; these backups are copy backups that do not truncate application log files or provide granular application recovery.
- For storage area network (SAN) backups, ensure that the off-host VCB proxy server is zoned properly to enable it to see the Virtual Machine File System (VMFS) logical units (LUNs) used by the ESX servers. VCB mounts a .vmdk file to a directory on the centralized Windows Server–based VCB server and enables backup of the .vmdk file contents.
- To help avoid snapshot-related problems, schedule backups during times of relatively low I/O activity on the VM. Reducing the number of simultaneous backups (and, in turn, VCB snapshots) can help avoid problems as well.
- Upgrade to the latest version of the VMware Infrastructure suite, including the latest versions of ESX, VirtualCenter, and VCB. Updated versions of VirtualCenter components can often enhance VCB snapshot reliability.
- Configure the snapshot mount point over as many dedicated spindles as possible. After a VCB snapshot is created, data is transferred from the VM data store to the backup proxy mount point, and ensuring that the data path from the data store to the snapshot mount point is as fast as possible can help significantly accelerate the completion of the snapshot process.
- Keep in mind that raw device mapping (RDM) disks are not currently supported through VCB backups, and are skipped automatically.

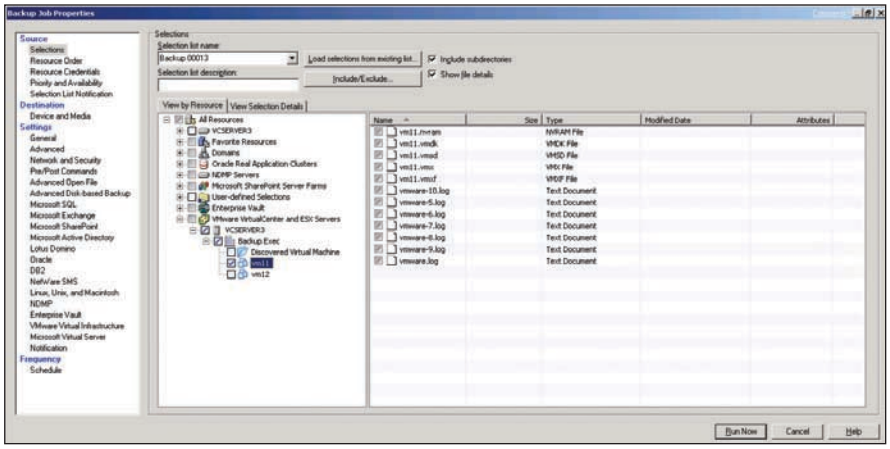

Figure 3. *Virtual machine discovery and selection in Symantec Backup Exec 12.5*

Administrators should also keep the following in mind regarding data recovery:

- VCB does not enable direct recovery of individual files and folders to individual VMs. Administrators must install the Backup Exec AWS on the target VM to perform GRT-enabled recovery of individual files and folders. Alternatively, they can perform a client recovery to a Microsoft Windows® OS–based share, then access the restored files and transfer them to the VM through this share.
- Granular recovery of individual files and folders from within a .vmdk file typically works best when restoring from a disk-based backup. Although granular recovery from a tape-based backup is supported, it requires administrators to temporarily stage the entire .vmdk file to a disk location during the restore process and then remove it. To recover the .vmdk file, sufficient disk space must exist on the temporary staging location specified in the Restore Job Properties window.

SIMPLIFIED DATA PROTECTION FOR VIRTUALIZED ENVIRONMENTS

The Symantec Backup Exec 12.5 software in the new Dell PowerVault DL2000 – Powered by Symantec Backup Exec introduces a variety of flexible capabilities to help protect VMware virtualized environments as part of an overall backup strategy. Taking advantage of features such as the Symantec Backup Exec AVVI and following best practices can help organizations implement powerful, simplified backup and recovery for their VMware virtualized environments.

MORE ONLINE
DELL.COM/PowerSolutions

QUICK LINKS

Symantec Backup Exec:
www.backupexec.com

Dell PowerVault DL2000:
DELL.COM/DL2000