WHITE PAPER

Addressing the Top Data Protection Challenges in Mixed Physical and Virtual Server Environments:

Symantec Backup and Recovery Solutions for Physical and Virtual Servers

By Lauren Whitehouse, Analyst

February, 2009

Table of Contents

Introduction

IT organizations are well-versed in protecting their physical infrastructure and data from interruptions. Most, if not all, organizations employ some level of data protection to minimize downtime and data loss in the event of a disruption. Just as introducing multiple operating systems created complexity and challenges, as these organizations incorporate virtual servers in their environment, new challenges are developing for protecting the mix as a whole.

As deployments of server virtualization proliferate and new server virtualization technology becomes available, the combination of new and incumbent vendors adds yet another dimension to the heterogeneity of the environment. Workloads running on different operating systems and on physical and virtual servers add a new level of complexity for operational and disaster recovery.

Symantec is responding to mixed environment data protection requirements with enhanced solutions for system and data protection. Backup Exec and Backup Exec System Recovery have been recently updated to provide comprehensive data and system protection of physical and virtual environments for multiple vendors' platforms and hypervisors. These solutions provide a single-source solution for protection of business-critical and business-supporting workloads.

The Impact of Server Virtualization

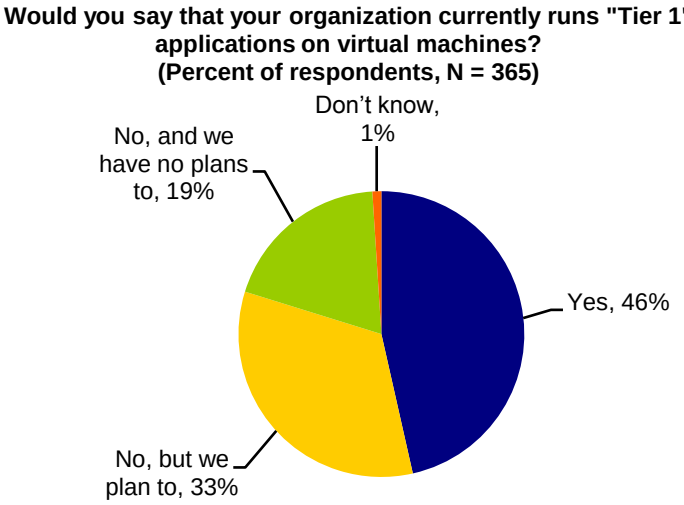
In the past, IT organizations could only come close to guaranteeing a service level for a specific application by deploying a dedicated silo infrastructure for the application—isolated from any potential outside impact. The downside of this approach was poor resource utilization, additional costs for high availability, workload spikes, and an environment that was inflexible and unable to accommodate or adapt to change or growth. Server virtualization—running multiple virtual machines on a single physical server—enables dynamic flexibility and eliminates the economic and operational issues of infrastructure silos while also introducing several benefits to IT organizations, including improved hardware utilization, physical server consolidation, increased availability, operational agility, and lower data center operating costs through optimized power, cooling, and space efficiency.

Server virtualization introduces big benefits, but also introduces vulnerabilities. In a physical server environment, loss of a single server has significantly less impact than in the virtual world where, depending on the workloads, the consolidation ratio of virtual machines running on a single physical server could be in the 20x range since server virtualization has increased the amount of applications and data that would normally be kept on a single physical server. A physical server failure can affect all of the virtual machines and applications running on that piece of hardware. The complexity of this scenario grows as organizations standardize on server virtualization and deploy Tier 1 applications in a virtual server environment.

Server virtualization vendors, aware of this vulnerability, have introduced some platform-specific features for business continuance. However, features such as an automated restart process are not adequate for applications that cannot tolerate any amount of downtime. Since more and more organizations are choosing to run business-critical Tier 1 applications in virtual machines—ESG research discovered that 46% of respondents surveyed run "Tier 1" applications on virtual machines[1]—it's important to implement safeguards to prevent unplanned downtime.

[1] Source: ESG Research Report, *The Impact of Server Virtualization on Storage*, December 2007.

FIGURE 1. TIER 1 APPLICATION USAGE ON VIRTUAL MACHINES

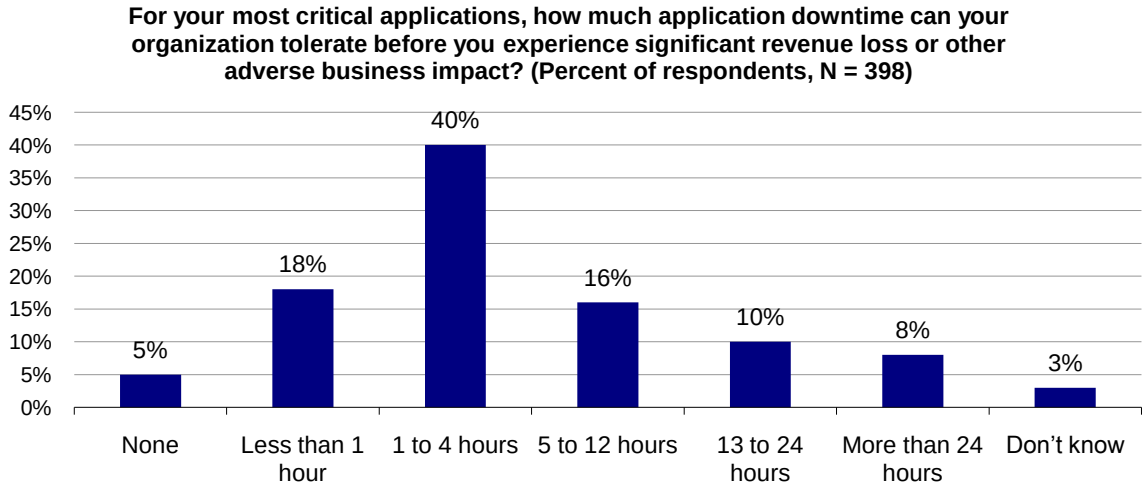


Source: Enterprise Strategy Group, 2007

Guarding Against Unplanned Downtime

Interruptions—such as computer viruses, disk failures, data corruptions, software faults, human errors, and disasters—can upset normal business activities by introducing unplanned downtime. Downtime could in turn result in productivity loss, customer service issues, or irreparable damage to the business' reputation or financial assets. ESG research found that 63% of organizations surveyed could withstand only four hours or less of downtime before experiencing adverse affects to their business[2] (see Figure 2).

FIGURE 2. DOWNTIME TOLERANCE



Source: Enterprise Strategy Group, 2008

To guard against downtime in a physical or virtual environment, organizations implement measures to protect systems, applications, and data. It may be feasible to acquire new hardware and reinstall applications, but data

[2] Source: ESG Research Report, *Data Protection Market Trends*, January 2008.

and entire server systems cannot be easily recreated. That's why organizations back up and replicate data and server systems to disk or tape storage. The two metrics used to evaluate the effectiveness of the data protection process are recovery time objective (RTO), which is the measure of time between outage and resumption of operations, and recovery point objective (RPO), which is the measure of the amount of data that may be lost during the outage or recovery process.

Applying these metrics involves evaluating the criticality of an application, data, or complete system and the time and cost of recovering it. For example, more critical data will be copied with greater frequency, requiring more accessible storage and faster recovery to ensure minimal impact on the business.

An organization's recovery strategy involves two main components:

- **Operational recovery:** Protecting systems and data to facilitate rapid on-premise recovery, minimizing downtime.
- **Disaster recovery:** Protecting systems and data to facilitate rapid off-premise recovery in the event of a primary site outage or comprehensive virtual to physical and physical to virtual conversion capabilities to quickly restore an entire physical or virtual server in the event of a catastrophic server loss.

Protecting Physical Server Systems and Data

Data and system protection strategies are based on the workload's aforementioned recovery objectives—RTO and RPO. The components to consider with physical server data and system protection are:

- **How the physical server and configuration will be protected**
  In the event of a hardware failure, replacing hardware (possibly with dissimilar hardware) and rapidly restoring systems to their pre-failure states is often a concern. Having the ability to quickly recover a physical server to dissimilar hardware or to a virtual environment enables flexible recovery options that can dramatically minimize system downtime.
- **How a copy of the data will be made**
  Performing file-based backup/recovery creates a copy of specified files and enables recovery of a single file or a collection of files. Snapshot backup creates a usable copy of a data set that represents an image of the data as it appeared at the time the copy was initiated.
- **The frequency of copies**
  Creating snapshots in several intervals during a 24-hour period generates multiple recovery points—addressing more stringent RPOs. Continuous data protection (CDP) involves saving changes in real-time to disk. With infinite recovery points, this method supports the most aggressive recovery point and recovery time objectives.
- **The type of onsite storage that will be used for operational recovery**
  The choice of onsite storage for the copy could include disk or tape. The selection of the onsite medium is often based, again, on the RTO for each workload. While both are reliable mediums, disk may edge out tape as better performing due to the handling, sequential read/write nature, and performance capabilities associated with tape drives, among others.
- **The type of offsite storage that will be used for disaster recovery**
  While tape media has traditionally been the offsite storage medium for many organizations, improvements in bandwidth, bandwidth optimization, and distance replication have made it more feasible to electronically vault backup media to disk storage at offsite locations.

Protecting Virtual Server Systems and Data

Organizations face several challenges when it comes to protecting a server virtualization environment. First, server virtualization increases the amount of data and files that would normally be kept on a single physical server—which could impact the backup window. Second, since physical resources are finite and backup processes can be resource-intensive when it comes to I/O and network resources, backup operations could affect the performance on other virtual machines sharing the same system resources. Finally, since the virtual

machine is an encapsulation of the operating system, applications, and data, protecting a production virtual disk (the .vmdk or.vhd file on local disk, RAID, or a SAN) is vital.

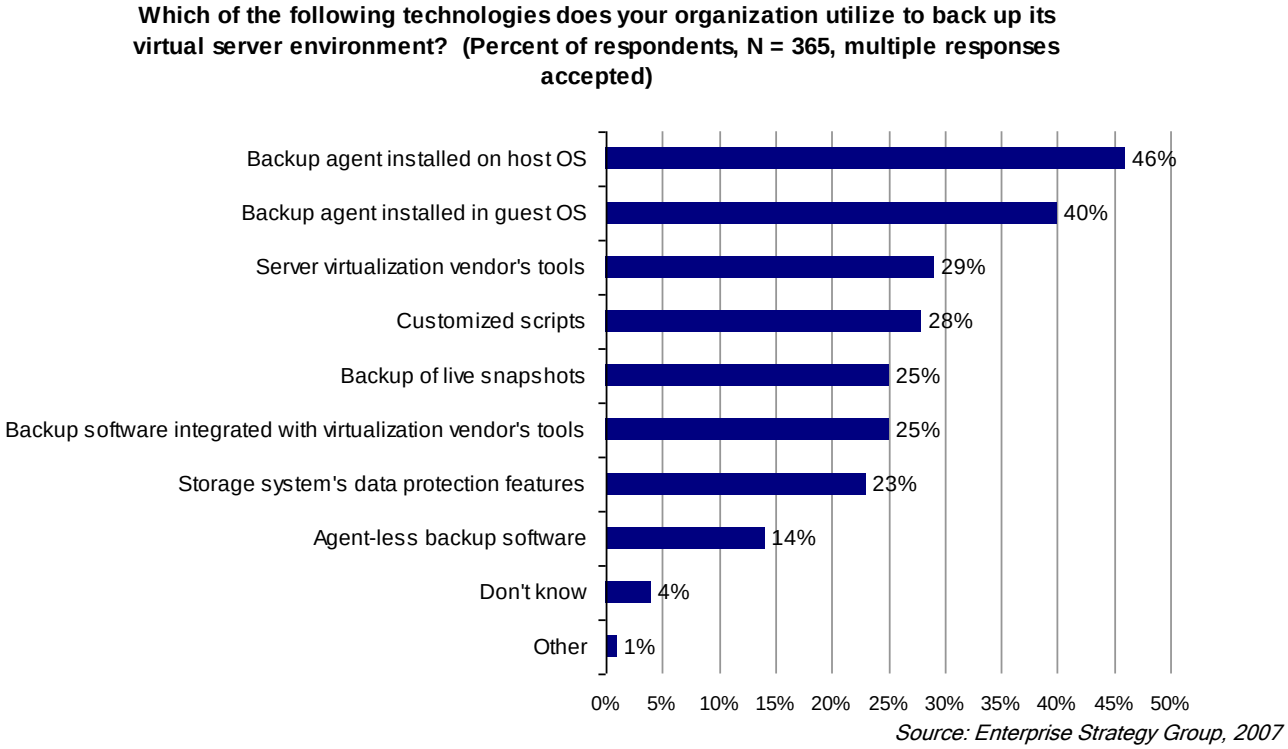
Multiple hypervisors in a single environment creates a level of complexity not unlike having mixed operating systems. The backup application has to understand the nuances of each hypervisor in order to effectively and efficiently protect the environment. Combine a mix of virtual and physical machines (and multiple operating systems) and the situation becomes even more of an ordeal.

Organizations with this level of heterogeneity will quickly realize the frustration of supporting backup and recovery. This will be glaringly evident the first time they attempt to recover a single file and realize they need to recover an entire virtual machine first, or when they realize they need to perform image-level backups for rapid whole virtual machine recovery and file-based backup for recovery of individual files. In some cases, there may even be a need to restore a virtual environment back to a physical system if problems arise with the virtual environment.

Approaches to Protecting Virtual Servers

There is no "one-size-fits-all" approach to protecting virtual servers. In a recent ESG Research survey, respondents noted several methods of backing up virtual machines. Installing traditional backup agents in the host or guest operating system were noted as the most popular approaches[3] (see Figure 3). However, as organizations gain comfort and maturity with their hypervisor, there can be a shift from the most-familiar to the more-efficient approaches.

FIGURE 3. APPROACHES TO BACKING UP VIRTUAL SERVER ENVIRONMENTS



Source: Enterprise Strategy Group, 2007

[3] Source: ESG Research Report, *The Impact of Server Virtualization on Storage*, December 2007.

VMware ESX

Backup Agent in Guest Operating System

Backing up at the guest operating system level is a relatively well understood approach. A backup vendor's client agent technology resides in the virtual machine and communicates with the backup server engine residing on the network. This method supports full and incremental backups of all guest operating system types, as well as application-specific backups for granular recovery of data. However, there are a few disadvantages. This method may be burdensome on the host's shared resources, especially if multiple virtual machines sharing the same host resources are scheduled for backup at the same time. It may be necessary to establish backup scheduling and policies for each virtual machine, as well as acquire a client agent license for each virtual machine. This method lacks bare metal recovery options, so a virtual machine cannot be restored as a whole—the operating system must be restored before virtual machine files can be restored.

Backup of a Running Virtual Machine

Another approach is the direct backup of the virtual machine disk image. VMware introduced VMware Consolidated Backup (VCB) to simplify data protection by offloading backup from ESX Servers and consolidating backup on one or more centralized proxy servers. At a scheduled time dictated by the backup application, VCB is instructed to initiate a backup. The operating system is quiesced and a snapshot of the virtual machine is performed. This allows a live system image to be captured without disrupting the virtual machine-resident applications or overwhelming the host's CPU. Backup occurs off-host and the need for a "backup window" is eliminated. This method also removes the need for an agent in every virtual machine (along with the cost and configuration/setup); allows for full, incremental, and differential strategies when the mounted image is backed up by the backup agent residing on the proxy system; and provides bare-metal recovery. Finally, capturing live system images (.vmdk) can enable conversion capabilities between physical and virtual (P2V and V2P) systems.

There are a few drawbacks to note with this approach. This method doesn't support file-level backup of non-Windows-based virtual machines. It also provides only limited support for enterprise applications such as Exchange, Oracle, and SQL Server. Application-specific backup can't be performed and, therefore, granular recovery for these applications typically cannot be performed. There are a few required infrastructure components, including:

- For application-data consistent backup, VSS is needed to quiesce supported applications prior to backup
- A license for VCB
- Networked storage[4]
- VCB-specific integration modules, special manual scripts, or new backup agent technologies that provide an integrated solution without VCB-specific integration modules or special manual scripts.

Image-Level Backup

Image-level backups typically take a full backup of an entire VMware guest machine—including data, applications, and systems—to ensure complete guest machine recovery or file and folder level recovery. Image-level backup solutions can also provide the benefit of P2V and V2P conversion capabilities that aid in server consolidation efforts, migration, testing, and disaster recovery practices. This is especially useful in a mixed physical and virtual server environment when a physical server needs to be recovered and no physical hardware is available.

Microsoft Hyper-V

Microsoft standardized on the use of Microsoft Volume Shadow Copy Service (VSS) snapshots to back up and recover all Windows Server 2008 services, including Hyper-V, as it guarantees complete protection for the platform. This provides a point-in-time copy of the active system's volume that helps protect all of the data required to fully restore the server. Microsoft exposed its VSS Writer interface, enabling ISVs to integrate their solutions with VSS. Therefore, the backup application must be compatible with the Hyper-V VSS writer.

[4] Note: local storage devices or NAS can be used to store virtual machine disks in environments running ESX 3.5 or ESXi 3.5 and Virtual Center 2.5, and provided each virtual disk is no larger than 1 TB.

Backup Within a Guest OS

There may be situations where installing a backup agent in the guest operating system is the only course available, such as backing up data from storage that is not supported by the Hyper-V VSS writer. One such use case involves virtual machines that use raw physical disks directly attached to a virtual machine (also known as "pass-through disks").

Backup of a Running Virtual Machine

Virtual machines running files on the host's file system consist of data (in memory and on disk), system configurations, and more. This makes performing an online backup tricky. To ensure backup consistency and prevent downtime, Microsoft allows for backup of running virtual machines with an operating system that supports the backup application's use of VSS. With this approach, a full server backup—including the virtual hard disks (.vhd), the associated configuration files, and the snapshots associated with the virtual machines—is performed through a host-based backup agent. It also automatically quiesces VSS-aware applications, such as SQL and Exchange, in guest operating systems before initiating backup. This approach does not replace the need for traditional application backup solutions to truncate log files and perform database consistency checks. However, it makes it easier to recover the whole system (you won't have to re-create the virtual machines or system settings), including the entire application. One drawback of this method is that, unlike VMware's VCB technology, the Hyper-V VSS writer does not natively support off-host backup of virtual machines to address the impact of backup I/O. Another is that recovering only a portion of the virtual machine—such as an individual file—cannot typically occur. As with VMware's VCB, the simplicity of recovery is dependent on the backup application's integration with Hyper-V. Finally, another limitation to note is that if the virtual machine is not running an operating system that supports VSS, then a backup of the virtual machine via the VSS writer will save the state of the virtual machine, snapshot the disk on the host, and restore the virtual machine state—costing some amount of downtime (typically minutes). In this case, the shadow copy will contain the state of the virtual machine at the time of the backup.

Image-Level Backup

Similar to how it works with VMware, in a Windows environment, image-level backups take a full backup of an entire Microsoft Hyper-V guest machine including data, applications, and systems to ensure complete guest machine recovery or file and folder level recovery. Image level backup solutions can also provide the benefit of P2V and V2P conversion capabilities that aid in server consolidation efforts, migration, testing, and disaster recovery practices. This is especially useful in a mixed physical and virtual server environment when a physical server needs to be recovered and no physical hardware is available.

Symantec's System and Data Protection

Backup Exec

Symantec Backup Exec provides disk-to-disk-to-tape backup and recovery for physical and virtual systems. It protects systems running Windows, Linux, Macintosh, UNIX, and NetWare, as well as VMware and Microsoft virtual machines. The backup application is differentiated from other solutions through its ability to:

- Perform backup in batch or continuous intervals—and therefore offer multiple recovery points.
- Execute image-based capture of virtual or physical machines with either whole server recovery or granular-level recovery of data.
- Provide backup to disk, tape, or "cloud" storage targets, offering multiple approaches for operational and disaster recovery strategies.

Backup Exec Support for VMware Infrastructure Environments

For environments based on VMware server virtualization, SymantecBackup Exec 12.5 for Windows Servers now offers multiple approaches for protection of VMware environments:

Backup Exec Agent in Guest Operating System

As previously noted, leveraging a backup agent in the guest operating system is a popular approach. A Backup Exec agent is installed in each virtual machine and policies and a schedule are set for each. Data is backed up and recovered in the same way it is in physical systems. When item-level recovery is needed, the application-specific Backup Exec agent installed in the virtual machine is the recommended approach.

Backup Exec's Agent for VMware Virtual Infrastructure

Backup Exec's Agent for VMware Virtual Infrastructure brings a number of improvements to manual scripting of VCB-based off-host backup. The new Backup Exec 12.5 Agent for VMware Virtual Infrastructure improves on the VCB method of backup while eliminating any need for manual VCB integration scripts or modules and ensures the entire backup process is easily completed while the VMware infrastructure remains online. The new agent supports an unlimited number of virtual machines on a VMware ESX host without requiring an agent to be installed on the ESX host or virtual machines. The benefits of file-level and image-level recovery are delivered from a single-pass VCB image-level backup—it's no longer necessary to perform separate VCB system- and file-level backups in order to recover a single file within a virtual disk image. Individual files can be recovered directly from an image-level backup within the Backup Exec console. Finally, the Agent for VMware Virtual Infrastructure protects VSS-aware applications—such as Microsoft Exchange, SQL, and SharePoint in a Windows virtual machine—allowing the entire server and applications to be recovered together. While traditional backup via database/application agents of applications such as SQL, Exchange, and SharePoint are still needed for transaction log truncation and consistency checks, the complete guest virtual machine can be protected and recovered in a single pass. Overall, the new Backup Exec Agent for VMware Virtual Infrastructure allows administrators to easily back up and recover physical and virtual server environments from a single console with granular recovery from image-level backups–saving time and money.

Backup Exec Support for Microsoft Virtual Server and Hyper-V Environments

For environments based on Microsoft virtualization software, Backup Exec has an Agent for Microsoft Virtual Servers. Like its VMware counterpart, the agent supports an unlimited number of Windows or Linux virtual machines on a host server. Supporting both Microsoft Virtual Server[5] and Microsoft Hyper-V, the agent also enables Backup Exec to provide image- or file-level recovery without a two-pass process—Windows guest operating systems are protected using Microsoft VSS snapshot technology while still allowing for individual file/folder recovery from inside the virtual machine. The Agent for Microsoft Virtual Servers also protects VSS-aware applications—such as Microsoft Exchange, SQL, and SharePoint in a Windows virtual machine—allowing the entire server and application to be recovered together. However, for optimal data protection and granular recovery of application-specific components (Exchange, Active Directory, SharePoint, for example) an application-aware agent is recommended to ensure log truncation, consistency checks, and more comprehensive overall backup and recovery of an application residing on a virtual machine.

Backup Exec System Recovery Support for Virtual Server Environments

Symantec Backup Exec System Recovery responds to organizations' need to rapidly recover from a complete server or desktop/laptop system loss or disaster, including recovering to dissimilar hardware or virtual server disaster recovery environments, using a technology called Restore Anywhere. When Backup Exec System Recovery is installed within any Windows guest virtual machine or physical machine, it captures live Windows system images (operating system, applications, system settings, configurations, and data files) in increments as often as every 15 minutes (with little impact on production systems) and stores them locally or remotely—on disk,

[5] Virtual Server 2005 R2 SP1

removable media, or at an FTP location. The result is that complete systems (OS, hardware configuration, user data, settings, and applications) are captured, providing a complete point-in-time image of the system. This is very similar to how both VMware and Hyper-V virtualize complete systems into .vmdk or .vhd files today. Not only does the saved image provide rapid and complete bare metal recovery, but granular recovery of data out of the complete system image is also possible.

In the event of a physical system failure, Backup Exec System Recovery can be used to rapidly restore the system recovery point of choice to a local or remote (even unattended) location. This saves organizations valuable time, eliminating the need to re-install the operating system and applications, re-configure settings, apply the necessary patches/updates, and recover data. Granular recovery of Exchange messages, attachments, folders. and mailboxes; SharePoint documents; or individual files/folders is available through the Granular Restore Option without having performed a granular-level backup process.

Symantec Backup Exec System Recovery 8.5 also provides physical to virtual (P2V) as well as virtual to physical recovery (V2P) capabilities to aid in server consolidation efforts, migration, testing, and disaster recovery practices. The solution includes a conversion wizard to facilitate the capture and encapsulation of a physical system into a recovery point which can be seamlessly and automatically converted to a VMware .vmdk file or Microsoft .vhd file format for instant disaster recovery on a VMware or Hyper-V platform. This is especially useful when recovery hardware is not available as the converted .vmdk or .vhd files can be brought online instantly for recovery. Backup Exec System Recovery 8.5 native image format (.v2i) can even be opened directly via VMware Server or VMware Workstation without the need for conversion, saving even more time during a disaster. Backup Exec System Recovery 8.5 now includes the capability to schedule the P2V conversions directly to a .vmdk or .vhd file, enabling immediate system recovery. Backup Exec System Recovery also makes it easy to perform even the most complicated conversion: going from a virtual environment back to a physical one (V2P) where the destination hardware and drivers are not similar to the original. The Restore Anyware technology in Backup Exec System Recovery automatically ensures that critical Windows drivers and components necessary to boot properly on the physical system (e.g., the mass storage controller and hardware abstraction layer) are in place to ensure a smooth recovery even when the hardware has dramatically changed.

Summary

Server virtualization is pervasive in data centers of medium-size to larger organizations. As these organizations leverage server virtualization for Tier 1 applications, it becomes even more critical to ensure availability and protection of systems and data as physical hardware failures can impact numerous workloads.

Data protection is often complicated by the complexity of mixing physical and virtual servers, multiple operating systems, and hypervisors. A single-source solution for addressing this level of heterogeneity in data protection delivers economies of scale, as well as operational benefits.

Symantec Backup Exec and Symantec Backup Exec System Recovery directly address these needs, providing comprehensive features to protect systems and data in physical and virtual, mixed operating system, and hypervisor environments. The solutions provide significant flexibility in protecting workloads—depending on the RTO and RPO requirements for operational and disaster recovery. Features such as continuous protection, granular recovery, P2V and V2P conversion, and more save valuable time for administrators and reduce the risk of downtime.

20 Asylum Street
Milford, MA 01757
Tel: 508-482-0188
Fax: 508-482-0218

www.enterprisestrategygroup.com