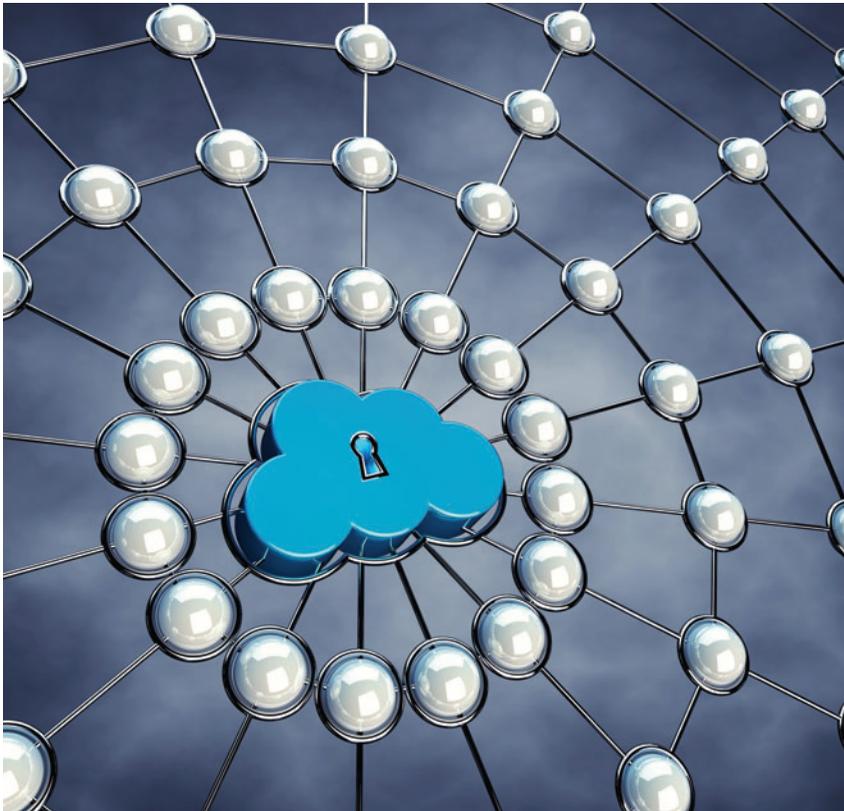


## IT MANAGER'S GUIDE TO **Protecting Virtual Servers**



Backing up and restoring a virtual machine that has far more moving parts than a physical server is a complex operation. If your storage doesn't keep up with your dynamic virtual servers, your data, your business and your job might be exposed. **By Doug Barney**

**A**s shops move from physical to mixed physical and virtual servers—and even purely virtual datacenters—storage infrastructure must move along. For the best protection, storage shouldn't just go along in lockstep, but should be ahead of the curve.

The only way to be truly safe in a virtual server world is to have backup, recovery and disaster recovery in place before the move is made.

Understanding this new world means broadening your storage horizons. "The widespread deployment of virtual machines [VMs] has created a whole new set of backup

issues," says Deni Connor, founding analyst of Storage Strategies NOW, an analyst firm in Austin, Texas. "Different virtual machine managers, or hypervisors, have different levels of support for backup. Likewise, different backup systems take different approaches to VM backups."

On the simplest level, your solution has to accommodate both physical and virtual systems during the migration. And because nearly no one goes fully virtual, you'll need to continue supporting both.

That leaves two choices. You can have two silos and one backup and recovery product for each server type, or a single tool that handles both. A single tool is great as long as it handles your needs with top marks. It's far simpler to buy and manage.

### SERVER PREP

You may not realize it, but you might need far more server overhead to properly back up VMs. "One purpose of virtualization is better utilization of hardware resources," Connor explains. "This means VM hosts are typically running closer to maximum CPU, memory and I/O capacity than physical—non-VM—servers. Backup also tends to use a lot of CPU, memory and I/O resources, so it can impact the performance of a busy VM host. In addition, backing up multiple VMs means encountering most or all of the issues encountered when backing up multiple physical servers, including scheduling issues and completing backups within the available backup window."

## VIRTUAL MACHINE BACKUP OPTIONS

- Run the backup from the virtual machine (VM) host or a proxy, and back up the files that contain the VM and its definitions from the host. In most cases the VM must be shut down during backup.
- Back up the contents of the VM as if it were a physical machine. This approach usually requires an agent running in the guest VM. Database applications must be quiesced with the same techniques used for applications on physical servers.
- “Hot” snapshot the VM—that is, create an image of the VM while it’s running. Because the backup application is running on the VM host or a proxy, there must be some degree of coordination between the backup system and database applications running in the VM to make sure they are in a consistent, stable state.

SOURCE: STORAGE STRATEGIES NOW

## GETTING REQUIREMENTS IN ORDER

Before you get in too deep into virtualizing your datacenter, you must figure out requirements for protecting your VMs (which you probably have already done for your physical servers). For instance, can you back up VMs in the same window as your physical servers, and still meet your recovery time objective? Similarly, can you restore VMs as fast as your physical servers? While both of these goals may sound like no-brainers, they aren’t.

And here’s another requirement: “Those managing VM backups should make sure that the entire VM as well as individual files and directories can be restored quickly and easily,” Connor advises. “Depending on the hypervisor being backed up, a variety of backup techniques may be necessary to achieve this goal.”

The key to making sure all this works is testing potential storage solutions to confirm they can meet your backup- and restore-window objectives. Other objectives should include pinpointing apps that need protection, and ascertaining what level of granularity they require.

## KEEP IT SIMPLE

Because virtualization makes server computing complicated, it makes sense to keep storage as simple as possible, both during the migration from physical to virtual and afterward. Multiple vendors mean multiple licenses, installs,

integrations, interfaces, upgrades, patches and support relationships.

Once you’re committed to virtual computing, maintain discipline. VM sprawl happens because it’s so easy to spin up VMs. The consequence is that all VMs—which are so simple to create—need backup. This complicates your storage infrastructure and stresses your storage compute infrastructure.

VM sprawl creates network bottlenecks, harms server performance, makes management more difficult and increases the risk of failure. And your storage licensing costs will likely go up as your number of VMs rises.

Meanwhile, backup windows for virtualized servers increase because you’re essentially using one server to back up machines that used to be hosted on a whole bunch of separate servers. The same applies to the reverse process of restoration.

## BASICS DON’T CUT IT

Platform vendors usually provide just the basics. Windows has bare-bones backup built-in through Microsoft Security Essentials and Windows Defender, a form of antivirus and anti-malware.

The same is true of hypervisor providers, which offer standards and components that support backup and restore, as well as some base-level tools to help you perform the backup and restore. (For more on hypervisor providers, see “Backup Strategies for 3 Key VM Platforms,” opposite page.)

There are a few concerns with these basic tools. The tools are proprietary and they only work with VMs. That leaves IT with inferior point products alongside all its other storage tools. And it’s easy to argue that built-in platform tools are almost never as good as dedicated third-party tools.

“Backing up multiple VMs means encountering most or all of the issues encountered when backing up multiple physical servers.”

*Deni Connor, Founding Analyst, Storage Strategies NOW*



Choosing the right tool is also critical for an easy and safe migration to the virtual world. Some storage software makes this easy: It takes an image of your Windows server and turns it into either a Microsoft Virtual Hard Disk file or a VMware VM Disk file.

As with any backup and protection strategy, it’s important to ensure that the technologies used are appropriate and address the challenges in your environment. For protecting virtual servers, there are several specific challenges that any solution must be able to meet. These include selecting the right level of



“Those managing VM backups should make sure that the entire VM as well as individual files and directories can be restored quickly and easily.”

*Deni Connor, Founding Analyst, Storage Strategies NOW*

protection, providing for granular recoveries, managing large data volumes and backup performance, and automating as much of the backup and protection process as possible.

For virtual servers, it's essential to select an appropriate protection level that meets your recovery objectives.

## DOWN TO BUSINESS

Backups must meet two seemingly contradictory requirements: they must be broad-based but also granular. Host-based backups handle the broad-based part by backing up the entire host server, which includes all the virtual servers. When it comes time to restore, all those files, apps or VMs may not come back in a granular way.

Application-level backups protect software such as SQL Server and Exchange. These backups run inside VMs and restore apps in a granular way.

Then there are guest-level backups, which are designed to granularly bring back data from individual VMs (but not on a per-application basis).

A single-pass backup tool can apply all these techniques in one pass to a virtual server or VM, making sure all the data is backed up and restorable on both a broad and granular basis.

The other thing to look for is whether you can restore to a bare-metal machine. This machine can be a dissimilar server, so you don't have to stock identical servers (which grow obsolete as soon as you buy them) just for backup.

## AUTOMATION TO THE RESCUE

In the world of physical servers, the number of machines is out of control. Falling hardware costs, shrinking sizes due to rack-mounting and other techniques, and growing user demand all lead to an explosion in the use of virtualization.

Given all that, the watchword for protecting VMs—in both backup and recovery—is automation. As new VMs are spun

## BACKUP STRATEGIES FOR 3 KEY VM PLATFORMS

**The VMware Way** In VMware systems, backup uses either the VMware Consolidated Backup (VCB) application or the more recent VMware vStorage APIs for Data Protection. VCB is a standalone application that can be called by other backup software. The vStorage APIs, however, are effectively file system drivers that allow access to VMware from Windows or Linux applications.

Applications can also access proprietary VMware Virtual Machine File System files from within the VMware ESX service console. Safely backing up database applications usually requires an agent running within the virtual machine (VM). A recent VMware product, VMware High Availability (HA), which is part of VMware Infrastructure, provides the ability to create high-availability clusters without a dedicated failover server. HA provides automatic detection and failover of a VM host server. In the event of a failure, HA initiates the affected VMs on other servers in the cluster.

**The Hyper-V Way** Backup applications for Microsoft Hyper-V typically use Microsoft Volume Shadow Copy Service (VSS). VSS operates at the block level and allows VMs to be backed up from the Hyper-V host. It also allows VSS-aware applications within a VM to be properly quiesced for backup. VSS-based backups are point-in-time consistent at the VM level and transactionally consistent at the application level. VSS backs up the entire VM as an image (snapshot), but allows file-level restores. VSS backups of Hyper-V use one of two methods: Saved State or Child VM Backup.

The Saved State method takes the VM briefly offline while it prepares the VM for backup. Snapshots are taken of the appropriate volumes and then the VM is returned to its previous state. Saved State can only be used with running VMs. The Child VM Backup, which requires the installation of Hyper-V Integration Services in each VM, doesn't require taking the VM offline. It can also back up both running and not-running VMs. VSS-based backups of VMs and their applications do not require agents.

**The XenServer Way** Citrix XenServer backups are typically performed using snapshots or backup agents. Depending on the software and backup method used, VMs can be backed up online or offline. For online backups, Citrix provides the XenServer VSS Provider (Windows-only), which provides for backups that maintain a consistent state with supported Windows OSes and applications. The XenServer VSS Provider is included with XenServer Tools, which must be installed in each XenServer VM.

SOURCE: STORAGE STRATEGIES NOW

out, the backup tool should recognize them, and storage policies such as backup windows should be automatically applied. If a VM goes down, you should have automatic failover with Live Migration, a cloud standby or some other predefined technique such as a virtual standby. •

---

*Doug Barney is editor in chief of Redmond.*

# AVOID THE HIDDEN COSTS OF VIRTUALIZATION

**Virtualization could be costing you more than you think!**  
Dedicated point solutions are often inflexible and expensively complex to implement and maintain. And maintaining a separate physical environment for key applications creates a costly and inefficient two-tier level of management and storage.

The CA ARCserve r16 Family of Products is the ONE solution that can seamlessly protect your systems, application and data in physical, virtual and cloud environments – simplifying management, accelerating transformation, optimizing efficiency and reducing downtime.

Visit [www.arcserve.com](http://www.arcserve.com) now to find out more and activate a free trial.

