VEEAM
IT JUST WORKS!™

# VMware vSphere Backups: What are you Missing?


## Greg Shields

Microsoft MVP and VMware vExpert


**Modern** Data Protection
Built for Virtualization | **#1 VM Backup**

Backups used to be easy. Just check the time stamp or the archive bit. If it changed, then back up the file.

Suddenly virtualization became popular, as did server applications. The unstructured data inside files and folders found itself sharing the datacenter with all manner of applications and databases. Virtual machines (VMs) joined physical machines as the method of delivering IT services.

*And, suddenly, backups became complex.*

The old file-and-folder approach just stopped being effective. Using date stamps and archive bits meant backing up any file that changed, no matter how large. An application's database might be gigabytes in size, but that file needed to be backed up. Even virtual disks became a problem. Not unlike small databases themselves, the virtual disks used by VMs created big problems in the file-and-folder days of data protection's past.

Fixing those problems is the reason why you see more content, thought leadership, research and product announcements from today's data protection vendors. Replacing the file-and-folder approach with something better—that fits the needs of applications and virtual machines alike—has become big business in the IT industry.

# Deconstructing the vSphere backup

IT shops also see the need to fix these problems, but figuring out exactly *what you're missing* can be tough considering today's complex and multifaceted datacenter environments. To help you fill that gap, let's explore in detail what exactly can happen when you've implemented a modern vSphere backup solution. The following deconstruction will take you through all the communication that must occur for a backup to complete successfully.

Use this as a guide to help you figure out what your environment is still missing.

### Step #1: Kicking off the Backup

The first step in backing up a vSphere VM starts with you, the administrator, and a specially configured VM[1]. This data protection VM, which is highlighted in Figure 1, serves three roles: It contains the backup solution itself, it exists as a backup "proxy" for moving data and it hosts the repository of backed up data.

*1. It is worth noting that this can be a physical machine, although for simplicity we'll discuss only the VM use case here.*

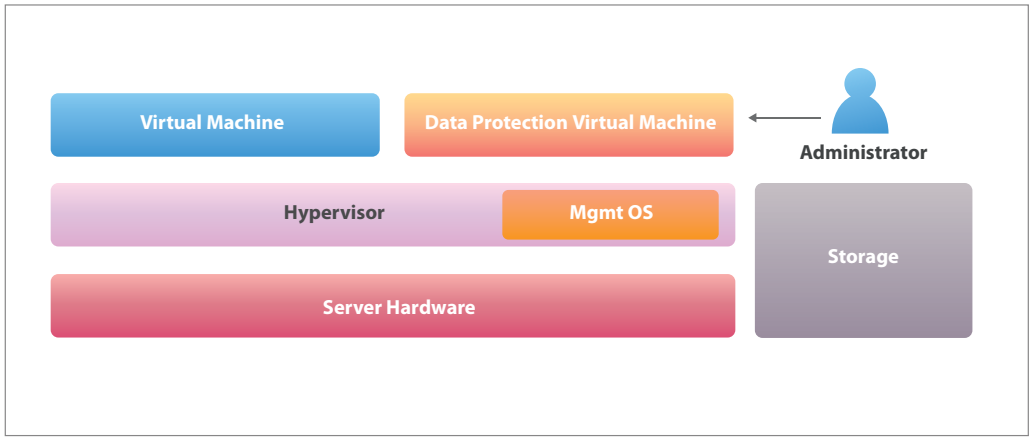


*Figure 1: Kicking off the backup with the data protection virtual machine.*

Serving in these three roles, this data protection VM delivers the management user interface for the administrator. It serves as the conduit for transferring VM disk files to storage. It also becomes the source for accessing those backed up VMs when later restores become necessary.

> **All for one, many for all**
>
> It is worth noting that a single data protection VM offers only the simplest of backup and recovery architectures. Larger and/or more complex environments will find value in separating these three roles onto individual virtual or physical machines. In some circumstances, even using a VM for the repository host may be an overly heavyweight approach. If your storage can also serve up shares to the network, those shares alone may well serve the need for a repository host.

With this architecture in place, the first step in any backup starts with an administrator kicking off the process. What happens next digs deeper into other areas inside the virtual infrastructure.

## Step #2: Orchestrating the virtual environment

Virtual environments are a complex web of interconnected servers and services, each relying on the others for various functions. For this reason, the next step in a vSphere backup requires orchestrating the backup activity across those components.

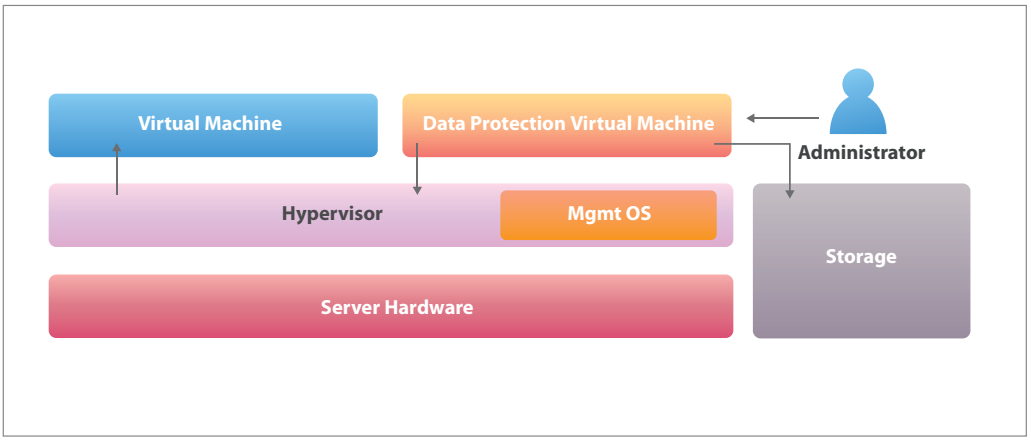


*Figure 2: Orchestrating the virtual platform components.*

Figure 2 shows a graphical representation of what goes on. The data protection VM informs the vSphere platform that a backup needs to occur. vSphere in turn notifies the VM—a process that can occur with the assistance of vSphere's preinstalled VMware Tools. Finally, the data protection VM's proxy and repository roles make ready the storage for receiving backup data.

At the conclusion of this step, vSphere and the other datacenter components are ready to start the backup. What's not yet ready is the VM itself

### Step #3: Orchestrating the virtual machine

As mentioned earlier, a VM's virtual disk files are not unlike small databases. Similar to databases, they contain data that's constantly in motion and requires quiescence in order to successfully capture a backup. Orchestrating the virtual environment ensures that the quiescence process happens correctly.

But VMs aren't the only databases around. Installed into many VMs are applications and other databases that themselves require additional quiescence. Neglecting that step would create a backup that wouldn't be trivial to restore. As a consequence, additional orchestration is required *inside the VM* to ensure every form of data gets captured correctly.

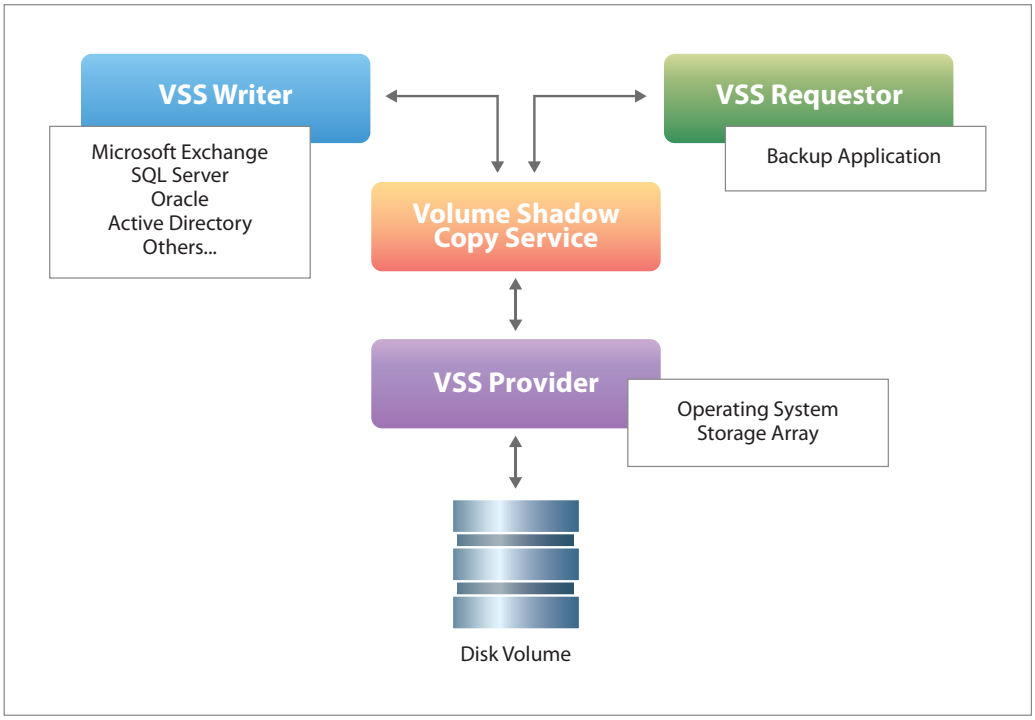


*Figure 3: Orchestrating the VM with VSS.*

Microsoft Windows uses the native Volume Shadow Copy Service (VSS) to orchestrate the activities inside a VM. Figure 3 shows the three parts that make up the solution. On the right, the backup activity begins with the VSS Requestor. That requestor receives the instruction from your backup solution that a backup is about to begin.

The requestor then notifies the VSS Writer, which is responsible for managing the before, during and after activities of each registered application. These activities can be the running of scripts or other commands that prepare each application for backup.

Once all applications are prepared, the requestor and writer work with the VSS Provider. The provider creates and manages the shadow copies that are used in the execution of the backup. The provider also interacts with whatever storage is being used during the backup.

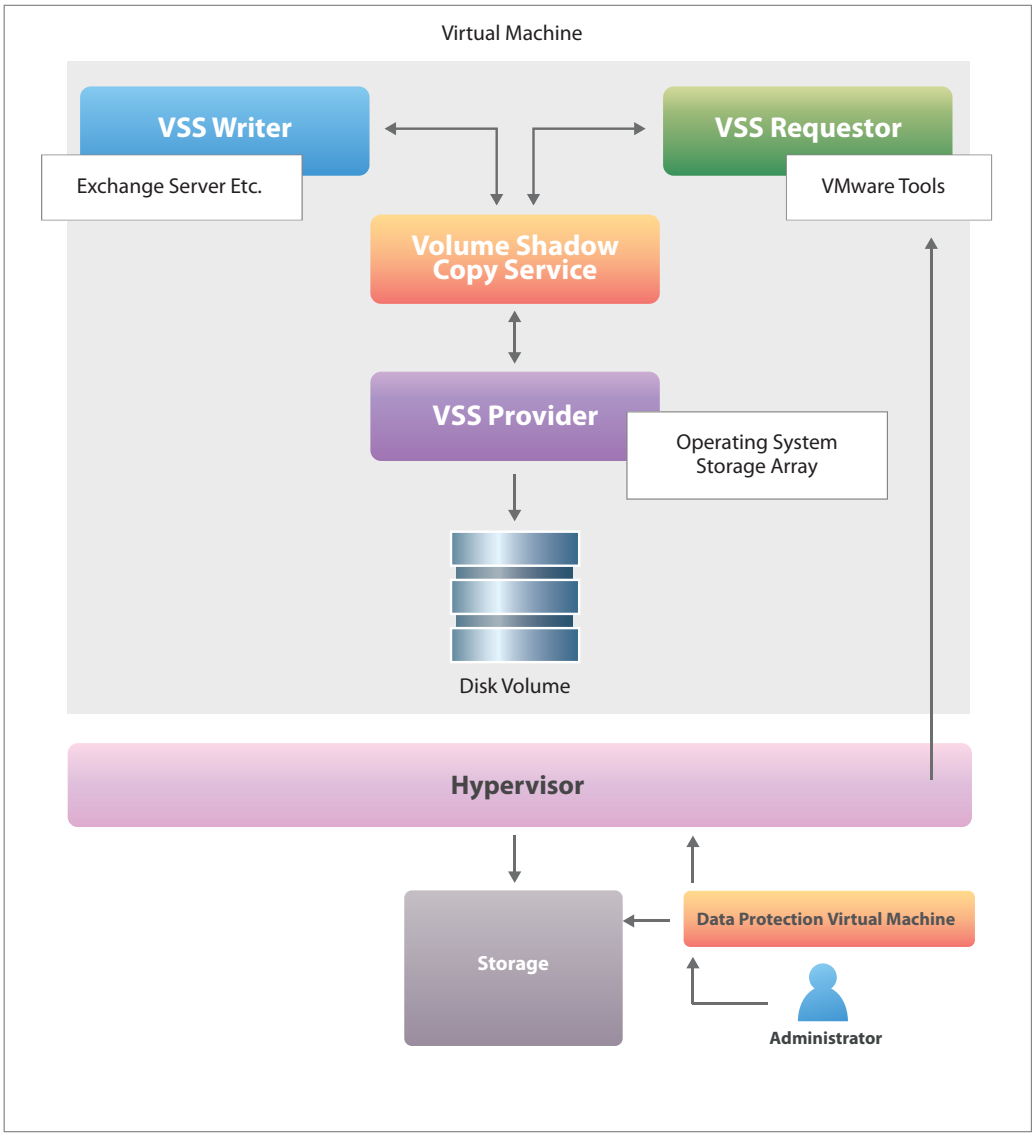


*Figure 4: VSS in the vSphere environment.*

## Step #4: Backing up

The integration between the three-part communication in Step 3 and the activities of Step #2 happens generally as a function of the VMware Tools that are installed into each VM. In addition to its other functions, the VMware Tools can serve as a VSS Requestor, where it enables the entire orchestration to occur among the data protection VM, storage, vSphere platform and the contents of each VM, as shown in Figure 4.

Once everything is ready, a backup can commence.

# So…what are you missing?

This guide's explanation of the vSphere backup process should help illuminate which pieces you have and which you don't. You've already implemented a virtual platform, and odds are good you've implemented that platform atop some kind of shared storage. You have VMs, and those VMs are serving up applications and data to users.

*But do you have effective data protection?*

Can your existing backup solution capture files and folders, application objects and entire VMs all at once? Can that solution restore any of those items with minimal effort? Are your backups still focused on late-night windows, or are they constantly capturing changes in near real-time? And can your backup solution replicate everything it captures elsewhere, to ensure that even the biggest of disaster events won't be a disaster for your business?

If not, what you've got are backups *that are complex*. What you're missing is the right data protection solution for all your VMware vSphere needs.

# About the Author

**Greg Shields**, Microsoft MVP and VMware vExpert, is an independent author, speaker, and IT consultant, as well as a Partner and Principal Technologist with Concentrated Technology. With 15 years in information technology, Greg has developed extensive experience in systems administration, engineering, and architecture specializing in Microsoft OS, remote application, systems management, and virtualization technologies.

# About Veeam Software

Veeam® is Protection for the Modern Data Center™ - providing powerful, easy-to-use and affordable solutions that are Built for Virtualization™ and the Cloud. Veeam Backup & Replication™ delivers VMware vSphere backup, Microsoft Hyper-V backup, recovery and replication. This #1 VM Backup™ solution helps organizations meet RPOs and RTOs, save time, eliminate risks and dramatically reduce capital and operational costs. Veeam Backup Management Suite™ provides all the benefits and features of Veeam Backup & Replication along with advanced monitoring, reporting and capacity planning for the backup infrastructure. Veeam Management Pack™ (MP) extends enterprise monitoring to vSphere through Microsoft System Center and also offers monitoring and reporting for the Veeam Backup & Replication infrastructure. The Veeam Cloud Provider Program (VCP) offers flexible monthly and perpetual licensing to meet the needs of hosting, managed service and cloud service providers. VCP currently has over 4,000 service provider participants worldwide. Monthly rental is available in more than 70 countries from more than 50 Veeam aggregators.

Founded in 2006, Veeam currently has 23,000 ProPartners and more than 91,500 customers worldwide. Veeam's global headquarters are located in Baar, Switzerland and the company has offices throughout the world. To learn more, visit http://www.veeam.com.

VEEAM

IT JUST WORKS!™

# Protection for the **Modern** Data Center


To learn more, visit **http://www.veeam.com/backup**