

CommVault Galaxy Enhances Data Protection

for VMware ESX Server Virtual Machines

CommVault® Galaxy® software is a powerful suite of Unified Data Management™ capabilities optimized for large-scale, enterprise deployment. This suite includes capabilities for data backup, recovery, replication, snapshots, and archiving. These capabilities can be used to help manage data in VMware® ESX Server™ virtualized environments.

BY KELLY HARRIMAN-POLANSKI

Related Categories:

CommVault

Storage

Storage software

Virtualization

VMware

Visit www.dell.com/powersolutions
for the complete category index.

Backup, restore, and disaster recovery are crucial considerations when managing data center operations. This is no less true for virtualized servers. Traditional backup and recovery methods can be used to protect data in virtualized environments. However, IT organizations should also consider using additional methods for protecting data on virtual machines (VMs) such as those provided by CommVault Galaxy software.

Data protection needs of VMware-based environments

VMware software enables enterprise IT organizations to virtualize their computing, storage, and networking systems and manage them centrally through the creation of enterprise-class VMs. These virtual environments can help increase physical server utilization, performance, and

system uptime cost-effectively. When deployed on Dell™ PowerEdge™ servers, VMware ESX Server virtual infrastructure software enables IT administrators to create multiple VMs on a single physical server, each of which can run a separate OS and applications without interfering with other VMs on the physical server. VMware VirtualCenter management software provides a central point of control for a data center's virtual computing resources. This highly scalable, cost-effective VMware virtualization platform is designed to provide advanced resource management capabilities for today's enterprise IT environments.

CommVault software can provide additional data protection and management capabilities in a VMware-based environment. By integrating data backup and recovery with replication, snapshots, and archiving—all of which can be managed from a single console—CommVault software

offers cost-effective, scalable, and easy-to-use data management with a range of options for reliably protecting VMware-based environments. CommVault Galaxy software can help protect and manage data residing on VMware-based systems by providing the following capabilities:

- Object-level backup and recovery of file system data residing in guest-hosted VM environments
- Granular backup and recovery of application data residing in guest-hosted VM environments
- Deployment options for placement of the backup server components—within a VM and on a separate server
- Crash-consistent protection of VMs

Disk structure of VMware ESX Server

VMware ESX Server is a data center-class virtual infrastructure suitable for mission-critical environments. It boots from a version of the Linux 2.4 kernel on the x86 chipset. Because ESX Server runs directly on the server hardware, it is highly scalable and capable of running many more VMs than VMware GSX Server™ software, which runs on top of a host OS. The ESX Server system can guest-host VM environments running various operating systems, including Microsoft® Windows®, Red Hat® Enterprise Linux®, Novell® NetWare®, Novell SUSE® Linux, Sun Solaris, and other OS platforms (see Figure 1).

VMware provides its own file system—VMware File System (VMFS)—for storage of VMs. VMFS is optimized to store large files containing virtual disk images and memory images of suspended VMs. VMFS-2, used by ESX Server 2, may exceed 2 GB in size and can span multiple disk partitions across one or multiple logical units (LUNs) or physical disks.

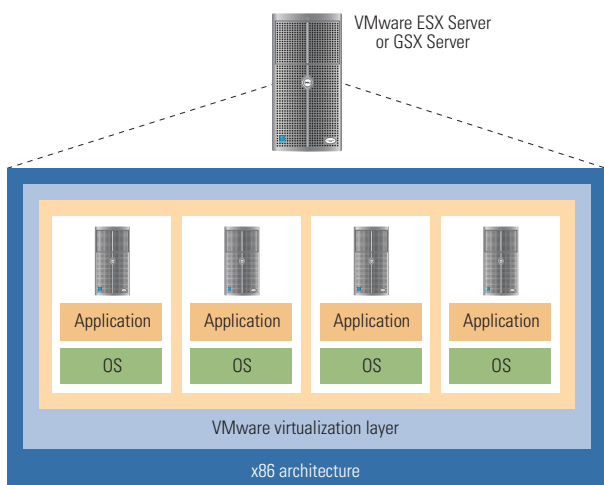


Figure 1. ESX Server environment with guest-hosted operating systems running as VMs

ESX Server captures and preserves the data residing on VMs in VMFS disk files. These files, which have .dsk or .vmdk file extensions, can be used to back up the entire VM. While the VM is in operation, these files remain open and in use. VMware provides various methods for gaining access to these files so that they are readily available for backup protection. One method for protecting the virtual disk file is to stop the VM while the file is being backed up. VMware also provides a procedure for releasing the disk file by first creating a redo file (log) to capture any changes, freezing the disk file, and then exporting a snapshot of the disk file. This snapshot image is then available for backup.

To help ensure effective recovery of an ESX Server system, administrators should protect three main components:

- Virtual disks—which contain the guest-hosted OS, applications, and the application data
- VM configuration files
- Physical machine configuration data

Options for protecting VMware ESX Server VMs with CommVault software

CommVault Galaxy backup and recovery software is flexible and modular—so enterprise IT organizations can customize the level of protection for their VMware-based environment. Administrators have two options for protecting data on VMs: treating the VMs as physical servers or treating them as files on an ESX Server system. For both options, Galaxy iDataAgent™ modules (iDAs) are used to implement data protection. These modules are designed to protect file systems in virtualized environments.

Protection option 1: Treating VMs as physical servers

IT administrators can deploy CommVault Galaxy software within VMware VMs just as if the VMs were separate physical servers. For example, administrators can install Galaxy iDAs within the VMs and then use a Galaxy CommServe™ module deployed on a separate physical system to protect those VM environments by sending backup data across the network. An advantage of this approach is the ability to run traditional incremental, differential, and synthetic full backups in addition to full backups. However, IT organizations cannot protect the entire encapsulated VM environment—that is, the VM configuration information in addition to the data residing on the VMs—for easy recovery.

Figure 2 depicts an ESX Server system with four VMs, each of which are protected by a Galaxy backup server running on a separate physical machine. The file systems and applications running within the VMs are protected via the Galaxy file system and application iDAs. Backup and recovery is performed using the normal Galaxy process, with each VM presented as a unique client system within the Galaxy unified console.

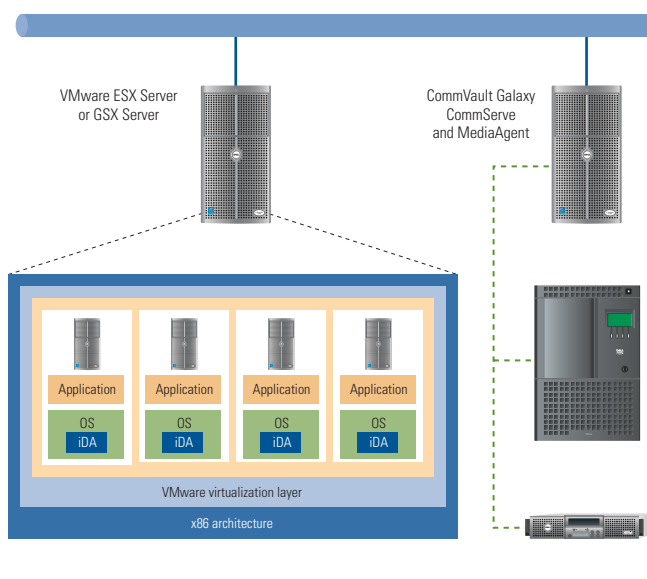


Figure 2. CommVault Galaxy software protecting an ESX Server VM environment

In this scenario, Galaxy software enables administrators to configure data movement from the virtual server environment to the backup server using standard Galaxy configuration options over the LAN. Backup devices, whether disk or tape, are configured and managed from the Galaxy MediaAgent™ component running on the backup server and can be shared among all VMs as well as other systems. These drives can also be specifically allocated to protect specific VMs, again using standard Galaxy configuration options.

Protect VM system state. In most methods for backing up VM data in a VMware-based environment, treating VMs as physical systems does not provide the added benefit of being able to protect and recover the VM configuration itself. Being able to protect and recover the encapsulated VM configuration is, therefore, described as a unique advantage of using virtual disk files to protect VM file system and application data, which is the other protection option (described in the next section). CommVault Galaxy provides full system state protection for both Windows and Linux file systems along with individual file protection and recovery—because CommVault builds system state protection into the file system iDA. Administrators do not need to protect the virtual disk files themselves to recover VMs at crash-consistent states.

Avoid sending backup copies across the network. IT administrators can avoid sending backup copies of VMs on an ESX Server system across the LAN. To do this, they can select a VM to deploy the Galaxy MediaAgent, which manages a backup device. Best practices recommend using a shared backup device for all VMs running on the ESX Server system. Alternatively, a MediaAgent can be run on more than one VM attached to more than one backup device, depending on factors such as how much data needs to be protected and how much load particular VMs need to support.

Protection option 2: Treating VMs as files on an ESX Server system

This option takes advantage of how ESX Server creates a file per VM disk device and keeps track of changes using redo logs. Backup and recovery using this method is simplified to the physical machine level and creates a crash-consistent recovery to a specific point-in-time.

For example, IT administrators can deploy a single Galaxy iDA for Linux file system protection to protect the entire ESX Server system and all of its guest-hosted VM environments. Then, when IT administrators need to recover a specific VM, the VM OS, file system data, applications, and application data are all recoverable to a consistent point in time.

Using this option means that IT administrators must plan to protect and recover very large files (typically more than 2 GB in size). In cases in which administrators need to recover a single file, they must first recover the entire disk file—which can take dramatically longer than recovering a single file, depending on the size of the virtual disk file.

Therefore, this option is well suited for small ESX Server implementations with file systems and no or few applications running. By definition, virtual disk files cannot be protected while the VM is running. To protect a virtual disk file, administrators must add a redo log, which makes the virtual disk file static and therefore available for backup. Administrators can also take a snapshot of the VM, creating multiple points in time—each of which can be backed up for crash-consistent recovery.

Effective backups for virtualized servers

As data needs continue to grow because of compliance regulations and end-user requirements, backup, restore, and disaster recovery are becoming crucial issues in today's data center operations. Virtualized servers such as VMware ESX Server systems require the same attention to backup strategies as physical systems. Together, CommVault and VMware can provide various options for effectively backing up and protecting the data in virtualized environments. [▶](#)

Kelly Harriman-Polanski is the director of product marketing for CommVault. Kelly recently joined CommVault and has worked in the storage software market for nearly 10 years, most recently at EMC/Legato. Her interests include data and information management, data archive, retrieval, compliance, data classification, and integrated snapshot and replication management. Kelly graduated magna cum laude and Phi Beta Kappa from Augustana College in Illinois.

FOR MORE INFORMATION

CommVault Galaxy:

www.commvault.com/backup_and_recovery.asp