commvault
solving forward®

A CommVault® White Paper

The Five Fundamentals of Virtual Server Data Protection

February, 2013

Contents

commvault

solving forward®

Data Protection and the Drive to Virtualization

The benefits of server virtualization are compelling and are driving the transition to large scale virtual server deployments. From cost savings recognized through server consolidation or business flexibility and agility inherent in the emergent private and public cloud architectures, virtualization technologies are rapidly becoming a cornerstone of the modern data center.

However, the lure of virtual server deployments is having unintended consequences for data storage and data protection. The consolidation of physical servers and networking is resulting in a massively converged IT infrastructure where already limited resources are being made even scarcer. Typical server consolidation ratios of 10 to 1 mean there are a fraction of the resources there once were for even routine IT management tasks like backup and recovery. In addition to fewer resources, massive data growth coupled with the expanding number of virtual machines is leading to an ever larger and more consolidated amount of data that must be managed and protected. The benefits of virtual servers in terms of cost savings, application flexibility and uptime are now driving customers to deploy more critical applications within a virtual machine context. These critical applications come with the most demanding SLAs for application uptime, granular recovery points, and rapid recovery times.

With this shift to virtualized data centers and round the clock operations, there is a need to rethink the traditional data protection techniques. Data protection and data recovery must have minimal front end impact and cannot exclusively rely on the legacy methods of streaming copying data from the production to the backend. A modern, effective solution minimizes the load on production systems, reduces administrative effort, enhances data protection and recovery, eases the transition to a virtualized data center, and will enable cloud-based options when they are desired.

The Fundamentals of Virtual Server Data Protection

Exploding Backup Windows: The combination of high server consolidation and high virtual machine (VM) density concentrates data ownership to a small number of physical servers with most resources dedicated for production workloads. There are few resources, if any, left for traditional management tasks, such as backup, which moves data over a network during a fixed window. In this new world of consolidated and virtualized environments, storage and backup teams are being asked to protect large and growing datastores with a fraction of the compute, network and storage resources and to do so in less time.

As server resources continue to consolidate and virtual environments become more concentrated, the amount of data owned by virtual machines is skyrocketing. This massive growth in the amount of data to be owned, managed and protected by the virtual environment is compounding what is already an untenable situation when using a traditional streaming backup approach. Cases are emerging where a successful backup of multi-terabyte datastores using a traditional streamed backup approach is exceeding a 24-hour window, far in excess of what the modern data center requires.

Every virtual machine is essentially a set of large files (VMDKs in a VMware context). These large files are stored on LUNs known as Datastores. Datastores can be configured on iSCSI or Fiber Channel block storage volumes or on NFS volumes. Traditional data protection techniques such as VMware's vStorage API for Data Protection (VADP), or VMware Consolidated Backup (VCB) rely on an external agent to protect VMDK files associated with virtual servers. Typical steps are as follows:

- Queisce virtual servers to get a consistent set of VM image files.
- Use the VADP enabled agent to read the VM image files from the Datastores.
- Copy the image files to a backup disk target.
- Release the Virtual Servers for normal operations.

While VADP brings much efficiency to this process, it is still a streaming method that moves the image files from the datastore to backup disk for protection. For environments with ever shrinking backup windows, there is simply not enough time or bandwidth to move all the VM data. Even if the infrastructure is available to copy all this data, it places a tremendous burden on the datastores as the data is read.

Unprotected Virtual Machine Data: The ease of deploying new VMs leads to a virtual machine sprawl, making it tedious and time consuming for administrators to keep track of new virtual machines and to ensure correct data protection and retention policies are applied to them. There is a major risk that important virtual machines may be created and never backed-up. Today, many administrators spend a significant part of their day tracking down new VMs and manually applying data protection policies. In the modern data center with hundreds or even thousands of virtual machines, this manual approach to ensuring VM protection policies is simply an unacceptable solution.

Application Integration: As more and more mission critical applications – like SQL, Exchange and Oracle – are virtualized, it is necessary to provide the same level of protection and recovery capabilities for these applications as they had in a purely physical server setting, while staying within the constraints imposed by a highly consolidated, virtualized environment. The modern data center now demands data protection solutions that deliver a level of application and virtualization platform awareness in order to provide concerted backup and restore capabilities that will ensure maximum uptime of these critical applications.

Delivering Recovery Points: With high data growth and change rate, relying on last night's backup for recovery is no longer sufficient. In addition, as organizations deploy more critical applications within a virtual server context, they are demanding Recovery Point Objectives (RPO) of hours. In other words, it is necessary to be able to recover to a few hours ago, not to last night's backup, in order to minimize data loss and the impact to the organization as a result of any disruption. Creating frequent recovery points without impacting production activity is a huge challenge.

Ensuring Restore Granularity: In order to further accelerate restores, organizations require an integrated approach to restoring data granularly at the volume, file or application object level. The ability to restore an individual email or file from within a virtual machine datastore is critical for ensuring application uptime and for meeting availability and uptime SLAs. Traditional approaches which require remounting an entire virtual machine datastore (such as a VMDK) and searching through the contents to find a single user email is simply too time-consuming and resource intensive to be a workable solution. Newer approaches are currently being introduced that enable file and object level restoration, however, they may require a second pass in order to generate that granular catalog. This unnecessarily adds additional processing time and consequent risk into the data protection process. A solution is needed that delivers granular restore options down to the file or object level and does so from a single pass backup operation.

Virtual Server Data Protection Solved with CommVault® Simpana® Software

CommVault® Simpana® software is a revolutionary data management solution that not only addresses the data protection and information management challenges arising out of limitations in legacy data center environments, but more importantly, that accelerates the shift into virtualized and cloud-enabled data centers. With Simpana® software, businesses can start to realize tangible benefits from day one of deployment as they transition from traditional environments to the modern data center. For example, by using new techniques that access data once, then reuse it for multiple protection operations, enterprises can bypass many of the pitfalls that arise from trying to force-fit legacy techniques or point solutions. With CommVault® Simpana® software you can:

- Protect hundreds of virtual servers in minutes with minimal impact on physical production servers.
- Securely and easily protect very large VMware environments with thousands of virtual machines
- Automate discovery and protection of new virtual machines for guaranteed protection with minimal administrator intervention
- Rapidly create and efficiently move secondary copies of data for retention and disaster recovery using embedded source side deduplication.
- Create 100% application consistent protection copies.
- Use granular protection to provide granular restores at the VM, volume, and file or application object level.

If you want to reap the benefits of virtualization for your organization you must overcome the challenges of virtual server protection. To do this, you need a new approach that will allow you to rapidly modernize your data protection and management. With CommVault Simpana software, you can take full advantage of the developments in virtualization technology and enable private and public cloud data centers while continuing to meet all your data management, protection and retention needs – both now and as they evolve over time.

About CommVault

A singular vision—a belief in a better way to address current and future data and information management needs—guides CommVault in the development of Singular Information Management® solutions for high performance data protection, universal availability and simplified management of data on complex storage networks. The CommVault exclusive single-platform architecture gives companies unprecedented control over data growth, costs and risk. CommVault Simpana software modules were designed to work together seamlessly from the ground up, sharing a single code and common function set, to deliver superlative Backup & Recovery, Archive, Replication, Search and Resource Management capabilities. More companies every day join those who have discovered the unparalleled efficiency, performance, reliability and control only CommVault can offer. Information about CommVault is available at www.commvault.com. CommVault's corporate headquarters is located in Oceanport, New Jersey in the United States.

For More Information on Virtual Server Data Protection:

http://www.commvault.com/simpana.html#t-0

http://www.commvault.com/solutions-virtualization.html

For more information about Simpana® software modules and solutions,
and for up-to-date system requirements, please visit www.commvault.com

www.commvault.com • 888.746.3849 • info@commvault.com
CommVault Worldwide Headquarters • 2 Crescent Place • Oceanport, NJ 07757
Phone: 888.746.3849 • Fax: 732.870.4525

CommVault Regional Offices: United States • Europe • Middle East & Africa • Asia-Pacific • Latin America & Caribbean Canada • India • Oceania