

A CommVault® White Paper

3 Questions Every CIO Should Ask About Virtual Server Data Protection

February, 2013

Contents

Why CIOs Care	3
What Every CIO Should Know	4
3 Questions to Ask	5
CommVault® Simpana® Software	6

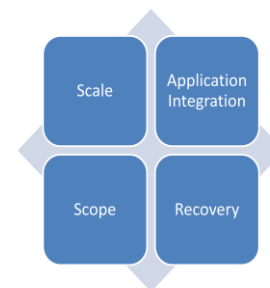
IT has reached an inflection point in the adoption of virtual server technologies. For example, Gartner recently forecast an expectation for x86 server virtualization to double from 40% in 2011 to 80% by 2016¹. Many organizations are no longer asking: “Why virtualize?”. The question has been flipped to: “Why not virtualize?” -- and rightly so. The benefits from virtualization now extend well beyond the benefits of cost savings through resource consolidation and reduction in operational overhead. Businesses now see that many applications can realize improvements in availability, reliability and even performance by running in a virtual context. As a result of this shift, many organizations are looking to rapidly scale out their virtual infrastructure to encompass most, if not their entire data center.

Why CIOs Care

A Poorly Architected Data Protection Solution Can Stop a Virtualization Deployment in Its Tracks

Data protection and management of the virtual environment continues to be a challenge for most organizations. Industry research has consistently ranked “Improve backup and recovery”² as one of the top initiatives for Virtual Infrastructure deployments. Why is that? Simply put, most existing tools for backup and data protection of virtual machines are limited either in terms of:

- Scale - most backup solutions do not adequately address the scale challenges of a deployment quickly growing into the hundreds of VMs and beyond.
- Recovery capabilities - they do not deliver adequate granular recovery options to support business requirements.
- Scope of support -they are limited to support for only a single virtual platform, such as VMware, whereas many organizations are looking at more than one platform due to cost and benefit profiles of the applications they want to virtualize.
- Application Integration – it is not enough to integrate with the virtual platform. The successful data protection solution should provide deep application integration to enable rapid recovery and meet the most stringent SLAs.



Data Protection Requirements for Rapid, Mass Adoption of Virtual Infrastructure

In fact, many traditional storage and backup vendors are simply force fitting legacy solutions into the new virtual environment hoping it will work. In each case, as virtual environments grow in scale and complexity, users continue to struggle with tools that are not optimized for these unique problems adding cost, increasing complexity and potentially increasing overall risk to the business.

Normally these challenges might remain under the purview of storage and backup teams within the IT organization. However, organizations are seeing the need to re-evaluate and re-architect legacy data protection strategies as the virtual infrastructure grows in scope and scale³. This can result in significant delays to the overall virtualization initiative as IT leadership is forced to take a step back and realign data management strategies with the burgeoning virtual infrastructure.

Like never before, IT leadership should be looking to storage and data management teams to ensure they are ahead of the challenges created by the tidal wave of consolidation and infrastructure convergence that is upon them in the form of server virtualization.

¹Gartner Inc., “Virtualization Key Initiative Overview”, Philip Dawson, Chris Wolf, July 2011.

² ESG, August 2012, Market Landscape Report: Navigating VMware backup and recovery solutions.

³ ESG, December 2010, the Impact of Server Virtualization on Data Protection.

What every CIO Should Know About Virtual Server Data Protection

Point Products Proliferate – adding cost, complexity and risk to the business

One of the biggest misconceptions in IT is the equation between “Best of Breed” and “Point Solution”. Virtualization data protection is a great example of this phenomenon (data deduplication is another). Recent years have seen an explosion in new products and new companies offering data protection solutions for the various virtual platforms, marketed under the heading of “purpose built” or “optimized” for the virtual world. But “purpose built” does not automatically equate to best of breed. The only way to truly discern the best approach is to go into the details to understand how the solution will meet the performance, scale, scope and recovery capabilities required of the business, both today and for what is expected in the future. You might be surprised by how few vendors are in a position to credibly address these concerns.

Beyond the claim of best of breed, the introduction of a point solution carries with it additional challenges in the form of added cost, complexity and ultimately risk to the business. By definition, a point solution is going to offer data protection for only a subset of the overall data center (in this case the virtual environment). Equally, it means these solutions lack support for what are potentially key elements of a comprehensive data protection strategy (this could even be as simple as lack of support for tape backups). Consequently, multiple solutions are required to ensure adequate data protection for the entire data center. This means added cost and complexity in the form of multiple product licenses and increased management overhead as admins must learn and manage multiple tools. It also means added complexity and ultimately additional risk to the business in the form of custom integration projects and scripting to ensure that the various tools work together as required.

“managers are unwilling to virtualize tier-one applications until they are certain that those applications are well protected and that they can recover VMs, files, applications or parts of applications in a timely fashion to meet stringent service level agreements (SLAs) required by mission critical applications.”

The 451 Group

The drive to virtual infrastructure is first and foremost about reducing cost by consolidating resources, maximizing utilization and centralizing management. It is thus counter-productive in the long run to completely contradict this strategy by adding multiple, complex solutions for data protection and management.

Methods Matter – the wrong method adds cost and risk

All data protection methods are not created equal. In this case, as with point products, simply marketing a solution as “purpose built” for the virtual platform is not the same as delivering capabilities that address the challenges in deploying and scaling out applications within a virtual infrastructure. Many purpose-built solutions run into real trouble when users attempt to scale beyond fifty or a hundred virtual machines, significantly impacting performance of production hosts and applications. Others lack the proper integration and application awareness to deliver the service level agreements (SLAs) required by business critical applications.

Choosing a solution that doesn’t understand the scale and performance requirements of the converged virtual infrastructure can result in unnecessarily expensive, over-designed solutions or in critical application and virtual machine data that are left unprotected.

Recoveries that match application and business requirements – mismatches can lead to increased business risk

By the end of 2012, it is estimated that 58% of all x86 server workloads were virtualized⁴. In essence this means many organizations have completed virtualization the “low hanging”. Areas like test and development, web servers and basic application servers have been fully virtualized. For most organizations, achieving the goal of a fully (or 100%) virtualized

⁴ Gartner, Sept 2012.



environment means targeting Tier 1 applications. This puts data management squarely in the critical path of the virtualization initiative. As the 451 Group recently put it: “managers are unwilling to virtualize tier-one applications until they are certain that those applications are well protected and that they can recover VMs, files, applications or parts of applications in a timely fashion to meet stringent service level agreements (SLAs) required by mission critical applications.”⁵

But why should the CIO care about these issues? Again, it comes back to the implications of not having a solution that understands the scope, scale, and recovery requirements of the virtual infrastructure. As organizations look to build out large private and hybrid cloud environments, the data protection and data management strategy must be ready for that level of scale and efficiency in order to avoid the costly re-architecture which many IT leaders are now realizing is needed.

3 Questions Every CIO Should Ask About Virtual Server Data Protection

IT leaders should be asking tough questions designed to ensure they have a data management strategy that comprehends the drive to a fully scaled out virtual infrastructure in order to avoid the need for a costly, time-consuming data management redesign. Here are the top three:

Does the solution align to the long term goals of the business?

The virtual platform and initiative is strategic. The supporting cast of infrastructure components and tools – including data protection – needs to align with this strategic direction. If the goal is to become 100% virtualized, and it is in an increasing number of organizations, the data protection solution must be ready to handle the scale, application integration, recovery, and access requirements to make this happen.

Does the solution help reduce cost?

Let’s face it, the primary objective of virtual platforms is to do more with less and ultimately reduce costs across the board. The data protection solution for the organization should align with that compelling vision. A data protection solution that spans the entire data center – physical as well as virtual environments – should help ease the transition from physical to virtual. Additionally, a data protection solution that is fully integrated from the ground up to deliver all the requirements of the virtual platform and does not require additional bolt-on components, 3rd party add-ons, or costly and complex scripting integration projects will help dramatically reduce the overall costs for protecting and managing data across the organization. CIOs should be looking to choose a solution that not only helps facilitate, but actually accelerates that transition by also delivering scale, scope and recovery in the virtual platform.

Does the solution help reduce business risk?

Beyond reducing costs, we’re now seeing that business can actually improve performance and flexibility and reduce business risk by virtualizing more workloads and centralizing management and operations. The same is true for data protection and data management. A centralized solution that spans the data center and encompasses all data protection and management requirements will eliminate the need for multiple point solutions that must be synchronized with complex scripts and manual intervention – ultimately resulting in more reliable data management processes that ensure information is where you need it, when you need it, and in this way, reduce risk to the business.

CommVault® Simpana® Software Solves Virtual Server Data Protection

⁵ The 451 Group, 2012, “Backup in a Virtual World”

CommVault® Simpana® software offers a completely fresh approach to data management that is optimized for the new challenges of the virtualized data center. CommVault's approach helps reduce both cost and risk by eliminating the need for multiple point solutions that require complex integration projects by delivering a fully integrated solution across physical, virtual (VMware and Hyper-V), and cloud-based components of the modern data center. This approach enables users to store, relate, classify, and search for all data across the enterprise. This results in IT that is more efficient in operations, disaster recovery, litigation, and compliance initiatives. On the back of this approach, CommVault has been positioned in the "Leaders" quadrant in Gartner's 2012 "Magic Quadrant for Enterprise Disk-Based Backup/Recovery" report⁶.

CommVault Simpana software is application, operating system, virtual platform, and disk-aware to efficiently generate copies that are highly available for rapid recovery through the use of integrated array-based snapshot and replication technologies. Retention copies are efficiently deduplicated and moved to appropriate tiers of storage (either disk, tape, or cloud). Data can be seamlessly retrieved from any tier for multiple uses, including disaster recovery, data mining, legal discovery, compliance or regulatory requirements. The convergence of these key technologies that integrate and span the entire data center and the various tiers of data make up a truly unique and modern approach to data management.

About CommVault

A singular vision—a belief in a better way to address current and future data 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. CommVault's exclusive single-platform architecture gives companies unprecedented control over data growth, costs, and risk. CommVault Simpana software was designed to work together seamlessly from the ground up, sharing a single code and common function set, to deliver superlative backup and 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.

CommVault® Simpana® software is a complete solution for modern data management and information governance that includes the following capabilities:

- ✓ Backup and recovery
- ✓ Snapshots
- ✓ Deduplication
- ✓ Replication
- ✓ Disaster recovery
- ✓ SRM
- ✓ Cloud storage integration
- ✓ Desktop and laptop protection
- ✓ Archiving
- ✓ Storage optimization
- ✓ Virtual server protection
- ✓ Cloud storage integration
- ✓ Retention lifecycle management
- ✓ Enterprise search
- ✓ Privacy violation management
- ✓ Records declaration
- ✓ Content organization
- ✓ Compliance
- ✓ eDiscovery

⁶ 2012 Gartner Magic Quadrant for Enterprise Backup/Recovery Software by Dave Russell, Alan Dayley, Sheila Childs, Pushan Rinnen, 11 June 2012. This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from CommVault. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.