WHITE PAPER:
TAKING THE LEAP TO VIRTUALIZATION

Security and Backup Considerations in the Virtual Environment

Taking the Leap to Virtualization

Who should read this paper

Midsized Business IT Directors, IT Managers and IT Administration (Security and Backup)

Confidence in a connected world. Symantec.

Taking the Leap to Virtualization

Security and Backup Considerations in the Virtual Environment

Contents

Overview

Many mid-market companies have invested significant time and resources to secure and back up their servers, client computers, data, and overall network infrastructure in the traditional client-server environment. Now, just when they thought they could relax and reap the benefits of these efforts, emerging new technologies such as cloud computing and virtualization have arrived on the scene, bringing both significant benefits and new challenges.

Cloud computing is essentially a shift to using relatively scalable and reliable, pay-per-use, third-party services over the Internet to do business, such as Software-as-a-Service (SaaS) and Infrastructure-as-a-Service (IaaS). Virtualization is the first step to cloud computing.

By using software to divide one physical server into multiple isolated virtual environments, virtualization enables a more efficient utilization of existing computing resources. It is also a key stepping stone for cloud computing, as it makes physical and logical resources available through a virtual service layer across the enterprise.

Virtualization offers companies the tantalizing promise of significant time and money savings, increased productivity, and enhanced customer service. Current servers are better utilized, old machines can be retired, floor space is freed up, and—with the need to power and cool fewer systems—energy costs plummet.

Virtualization also improves reliability and performance by ensuring high availability and load balancing between various physical hosts. In the event of physical server failure, recovery in the virtual environment is much faster. Virtual servers simply fail over to another machine with no impact to users and a single IT manager can manage far more servers in far less time.

While virtualization brings impressive benefits, it requires careful planning and management to ensure your data is safe from corruption and that access is suitably controlled. As you migrate to the virtualized environment, ask yourself the following questions to ensure the transition is well-managed and allow you to get the most out of your virtual environment:

- Will your existing security and backup tools work in the virtual environment?
- Are you forced to use separate security and backup tools for your virtual and physical environments?
- Are your security and backup solutions complicated to use?
- How does your backup software impact your storage requirements?
- Is your software tightly integrated with your virtual environment?
- Are policies in place to prevent unmanaged growth of the virtual environment?

Are you forced to use separate security and backup tools for your virtual and physical environments?

Virtualization should simplify, not complicate, your technology environment. The more software, appliances, and servers you install on your network, the more complicated the environment becomes, and the greater the maintenance and management required.

Businesses are now tasked with maintaining the same degree of security and protection they currently enjoy to secure, protect, backup, and recover their virtual machines. The right technology can offer visibility into the virtual environment so that businesses can virtualize and reap the benefits faster.

Sophisticated solutions designed for the virtual environment integrate security, storage, and backup. They also provide:

- The ability to manage physical and virtual systems data protection through one console.
- Backups that don't sacrifice file recovery or tax your infrastructure.
- Deduplication to avoid storing the same data multiple times (resulting in up to a 90 percent reduction in storage).
- Automated security to apply appropriate security policies and spot risks and threats immediately.
- Ensure that virtual machines (VMs) are updated and fully compliant with security policies before they can access your network.[1]

Integrated backup and security tools make it possible for busy IT staff to protect their infrastructure through one interface, from one vendor. If you are using multiple solutions to protect (secure and backup) your network, an integrated protection solution can greatly simplify your job.

Are your security and backup solutions complicated to use?

Since IT managers at midsized companies are often tasked with knowing a great deal of diverse technologies, your virtualization protection software should not be overly complicated. Look for automated solutions that are easy to use, with one console developed specifically for the virtualized environment. Avoid simplistic solutions that lack robust protection, as well as software that is so complicated it's a struggle to use.

The right solution can protect your data, reduce storage and management costs, and automate storage and management savings with efficient archiving, backup, and security, all through a single console. As you seek to secure your virtual environment, ensure your protection software is integrated, efficient, fast, and user-friendly, with strong security features.

How does your backup software affect your storage requirements?

If (or when) disaster strikes, your business must be able to recover quickly. Ironically, the number one mistake businesses make when backing up their virtual environments is failing to back up the virtual environment at all. In a recent blog post, based on a global survey of thousands of users, Symantec found that nearly two-thirds of virtual machines are improperly backed up, representing a significant business risk.[2]

Done poorly, server virtualization can actually increase storage requirements and inefficient storage management can wipe out the cost savings achieved through server consolidation. Storing multiple versions of one file is a good example of poor storage usage.

Sophisticated backup software "knows" when it is operating in a virtual environment and properly backs up data in each hypervisor. Advanced storage management solutions automatically deduplicate (store only one copy of each file), reclaim orphaned storage, and virtualize pooled storage to ensure that you reduce rather than increase your storage requirements. A solution that is optimized for the virtual environment will automatically provide the advanced security, backup, and storage management you need.

Is software tightly integrated with my virtual environment?

Since virtual machines operate in its own environments, it's possible to have multiple protection systems on each of them, which can be a real headache to manage. Traditional agent-based backup and recovery are unsuitable for the virtual environment. This is because agents, by their nature, lack cohesion—you must physically install and manage agents on each application within the virtual server, which is time- and labor-intensive and presents security risks.

1-(from Symantec website: www.symantec.com/connect/blogs/symantec-v-ray-end-dark-ages-virtualization)
2-http://www.symantec.com/connect/blogs/ten-backup-mistakes-virtual-environment-part-1

A sophisticated solution that recognizes and integrates with your virtual environment can discover new guest virtual machines (VM), centralize management, minimize job configuration and management, support multiple backup sets, and offer broad application and operating system support.

VM Blog writes that, "Virtualized environments are difficult to visually inspect, and due to virtual server mobility and related issues, they often have dynamic configurations and server populations. In this context, threats can easily spread, devices can be overlooked, and inappropriate activity can be concealed. To prevent configuration oversights, rogue devices, auditing omissions, and other issues, the security system should maintain persistent awareness of all virtualized devices, services, and communications."

In other words, if you're using protection systems that are unaware of the virtual environment, you're not protected.

Are policies in place to prevent virtual sprawl?

Virtual sprawl is what happens when the virtual environment grows out of control—administrators bring up virtual machines for every little task and are left with an unmanageable sprawl of virtual machines. Because they are so easy to implement, they are often deployed with little thought as to the impact they will have on network security and management. While deploying a virtual machine is often much easier than deploying a new physical machine, use common sense. Create, enforce, and audit virtual machine policies to keep the virtual environment steady.

So what does it all mean?

There's no doubt that virtualization offers dramatic benefits for midsize companies, including efficiency, cost savings, and increased reliability and performance. But in order to take advantage of these benefits, companies must properly adapt their best practices, policies, tools, and procedures to the virtual environment. With a little caution, planning, and common sense, your virtualization implementation can allow you to do more with less and free up IT staff to focus on strategic projects that help your company grow. To be able to finally harness the full power of IT for competitive advantage—now that's compelling.

About Symantec

Symantec is a global leader in providing security, storage, and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored. Headquartered in Mountain View, Calif., Symantec has operations in 40 countries. More information is available at www.symantec.com.

For specific country offices and contact numbers, please visit our website.

Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com

Symantec helps organizations secure and manage their information-driven world with **endpoint virtualization**, **server virtualization**, and **application virtualization**.

6/2011 21196714