PARTNER'S GUIDE TO Virtual Backup

SHUTTERSTOCK

The fast-paced expansion of cloud environments and services in recent years has ensured virtual servers and software increasingly take up a bigger portion of the IT landscape. Here's what partners need to know about virtual backup and why it's so important. **By Pedro Pereira**

As of 2013, virtual workloads have exceeded the number of physical ones, and if Gartner Inc. projections hold true, in 2016 virtual workloads will reach 86 percent of the overall total. And thanks largely to cloud computing, the global client virtualization software market will expand at a 46 percent annual clip from 2014 to 2018, according to firm Research and Markets.

Predictions aside, one fact is indisputable: Virtualization is here to stay. Though not always fully understood, it isn't exactly a new trend anymore. The fast-paced expansion of cloud environments and services in recent years has ensured virtual servers and software increasingly take up a bigger portion of the IT landscape.

The drivers of virtualization are essentially the same as those for cloud computing—the need to consolidate servers to control datacenter expansion and its associated costs, a desire to increase efficiency and productivity, easy scalability, and a democratization of IT that places some of the most advanced technology available within reach of small and midsize businesses (SMBs).

Enterprises, with their deep pockets, historically had a leg up on small competitors in adopting cutting-edge technology. Now that the landscape has changed, enterprise-size challenges can affect SMB companies just as they do large organizations. When it comes to virtualization, a major challenge for companies of any size revolves around backing up the ever-swelling volumes of data companies generate and store in the course of running their operations.

That is, in fact, one of the biggest headaches CIOs and IT professionals currently face. More than 80 percent of participants in an Enterprise Strategy Group study cited virtual backup as a top IT challenge.

To overcome the challenge, organizations need to ensure their virtual environments are properly backed up and easily available for recovery should they experience a data loss. Any organization that leverages virtualized systems must include a virtual component in their business continuity plan. Solution providers with expertise in virtualization, backup and recovery, or both, have an opportunity here to ensure clients have the right strategy and technology in place to back up virtual data. Solution providers that figure this out early stand to profit and cement client loyalty.

A VIRTUAL NECESSITY

The first thing to keep in mind regarding virtualized environments is backing up is just as necessary with virtual machines (VMs) as with physical systems. Interestingly, it's something even some IT professionals fail to grasp. A preponderance of them said in a 2013 survey they believed virtualized environments pose little risk of data loss. The survey by data recov-

ery vendor Kroll Ontrack revealed 80 percent of respondents didn't believe their virtual environments were at risk and, in fact, thought that storing data in virtual environments decreased data-loss risks.

The finding was all the more surprising when taking into account that 40 percent of the 724 poll participants said they had experienced data loss over the previous year in their virtualized storage environments. Storage virtualization pools multiple network storage devices into what appears to be a single storage unit controlled from a central console. In 2010, a similar poll found that 27 percent of respondents had suffered data losses in a virtualized environment.

The 2013 survey also found that 84 percent of corporations use virtual storage, with one-third of participants indicating virtual makes up 75 percent to 100 percent of their environments.

The study seems to point to a misconception among IT professionals that virtual environments are inherently safer than physical ones. This could be because redundancies are built into virtual servers, and some IT professionals believe that's all it takes.

However, complexity in virtual environments can increase data-loss causes, including file-system corruption, deleted VMs and internal virtual disk corruption. And the effects can be compounded because the amount of data stored in a virtual environment is often much greater than that stored on a single physical system.

VIRTUALIZATION CONUNDRUM

What makes virtual environments complex? For one thing, you're processing and storing data in a software representation of what traditionally has been a physical system, such as a desktop computer or a server. The VM runs programs much like a physical computer, but it functions more like an abstraction, which is hard to grasp unless you work in virtualized environments.

VMs need a physical server to operate. A hypervisor resides in the server to create and run the VM. In physical IT environments, one-to-one mapping between servers, applications and storage is the rule, but virtualized setups function on one-to-many relationships. A single physical server hosts multiple virtual servers and, typically, the ratio keeps growing as the environment expands.

This leads to what has become a bit of a virtualization paradox: Simplicity leads to complexity. One of the benefits of the technology is how easy it is to set up a VM. Unlike a physical server that requires hours or days to fire up, a virtual server can be up and running in less than an hour.

However, because VMs are so easy to create, they can multiply quickly in what is known as "VM sprawl." Unwanted and unintentional complexity is added to the IT environment, and if it gets bad enough, the whole infrastructure might become unmanageable.

So while backup and storage have always presented complications, it turns out that backing up data in a physical environment is a simpler proposition than setting up a backup solution for an environment with servers that host numerous VMs. Complicating things even further, most environments today are a combination of physical and virtual resources.

These mixed environments require a comprehensive approach to data backup. Backing up only the physical servers in the belief that virtualized systems are inherently safer is a recipe for disaster. If the data in a virtual server isn't replicated, it cannot be recovered. That means it could be lost forever if the server fails.

This is an area where solution providers can make themselves invaluable to clients. In proposing virtual backup solutions, solution providers can dispel myths surrounding virtual data loss, leaving no doubt that virtualization offers no inherent advantage. Providers need to emphasize the consequences of data loss: According to the Federal Emergency Management Agency (FEMA), 43 percent of businesses never reopen after a catastrophic data loss; three-fourths of businesses without a business continuity plan, including data backup, fail within three years of suffering a natural disaster.

5 Key Elements of a Business Continuity Plan

1. Identify key functions.

Ideally, everything would be recovered after a disaster, but realistically it's important to prioritize the most critical business data and functions.

2. Involve everybody.

Business continuity isn't just an IT problem. The goal is to save the business after a calamity, so every employee should know and understand their role in a business continuity strategy.

3. Keep systems running.

Technology is fundamental to business continuity, and that means all backup and recovery systems need to be healthy and functional. The need for routine updates and checkups is a given.

4. Review and revise.

Businesses evolve and continuity plans must evolve with them. The recovery plan must be updated with changes to workflows, applications and systems.

5. Test the plan.

You don't want to find out if the plan works after disaster already has struck. Tests and drills can ensure that the plan works.

—P.P.

A VIRTUAL OPPORTUNITY

As companies weigh virtual backup options, solution providers have an opportunity to guide clients through technology decisions and execute a strategy for backup and disaster recovery (BDR). For providers that already offer BDR services, adding a virtual component should be a natural fit, but the opportunity also extends to those willing to learn the ins and outs of virtual backups.

Providers, of course, need to have a strategy of their own for how to handle virtual backups—either by setting up a storage network infrastructure or by partnering with a vendor that offers cloud-based backup services. The latter may prove an easier course of action, especially for providers who already partner with vendors for services such as remote systems monitoring and management and patch management.

Here are seven important considerations for solution providers looking to add virtual backup services:

> The first thing to keep in mind regarding virtualized environments is backing up is just as necessary with virtual machines as with physical systems. Interestingly, it's something even some IT professionals fail to grasp.

1. Do your research.

Solution providers that already offer BDR need to ascertain whether their service or solution supports virtual backup. If it doesn't, you will have to consider the available options, such as a virtual backup appliance or a cloud-based service from vendors such as Intronis Inc., StorageCraft Technology Corp. and VMware Inc.

2. Pick the right vendor.

Solution providers need vendors that have a reliable partner support infrastructure, especially when delving into new service areas. Some cloud vendors do most of the work, including implementation and management, treating channel partners essentially as commissioned agents. That works for some providers, but not for those who prefer to handle all contact with customers. Therefore, it's crucial to understand up front the vendor's support strategy before sealing any partnerships.

3. Educate the client.

Even though virtualization has steadily gained traction for the better part of a decade, many clients still have a fuzzy grasp on the concept and the need to back up virtualized environments. It's up to solution providers to guide clients through the various options, such as cloud-based services, appliances or virtual SANs, and help them make the best decision for their needs.

4. Build trust.

Trust is essential in service relationships. Solution providers build trust with clients by delivering value and following through on their promises of high-quality service, be it virtual backup or anything else. In doing so, solution providers increase their chances of cementing their role as trusted IT advisors.

5. Deliver business continuity.

While some processes and infrastructure may change in a virtual environment, the concept behind backing up data is the same—ensuring businesses remain operational even after losing critical data. Replicating the data, and making it readily available for recovery, is just as essential in virtual as it is in physical environments (see "5 Key Elements of a Business Continuity Plan").

6. Differentiate yourself.

If you can tell clients you're equipped to back up virtual environments, you will be a step or two ahead of competitors that don't yet offer the service. Differentiation in IT services helps fight commoditization, which helps protect revenue and margins, while elevating a solution provider's image in the eyes of the customer.

7. Market the service.

A common mistake solution providers, or any business, make is to launch a service and do little or nothing to promote it. If customers don't know about it, they won't buy it, so it's important to market your virtual backup offering through your Web site, e-mail, social media and, of course, in face-to-face communications.

REAL PROFITS

From a solution provider's perspective, the ultimate goal is to increase profits, or at least remain profitable. Losing money leads to losing the business. But staying profitable in an industry with a penchant for commoditizing everything requires hard work and vision. Seizing an emerging opportunity such as virtual backup is a way for solution providers to protect their profitability. •

Pedro Pereira is a freelance writer based in Plymouth, Mass. He can be reached at pedrocolumn@gmail.com.

*Backup "Hoarders" Fail the Recovery Test, Aberdeen Group Research, March 2014.

Can your clients survive an attack of the costly Downtime Dragon?

In today's market, the Downtime Dragon can burn down the castle and everything in the storehouse if you and your clients are unprepared. In this **FREE** Aberdeen Group research report you'll learn how leading organizations slay the Downtime Dragon by taking a complete business continuity approach and focus on recovery to minimize downtime and maximize uptime and availability of their critical applications. Download this vital report forthwith!

FREE Aberdeen Research Report

Backup "Hoarders" Fail the Recovery Test

www.StorageCraft.com/DDRCP

STORAGECRAFT®

Backup Fast, Recover Faster