FIVE TIPS FOR CREATING A VIRTUAL SERVER BACKUP STRATEGY

Virtualization has become not just commonplace, but vital among enterprises–but what should a company know when architecting its virtual server backup strategy? Here are five tips, including knowing what to ask vendors and how to go about future-proofing your organization.

CONTENTS:

Now that virtualization has become such a critical component of so many corporate infrastructures, virtualization server backup has spawned an industry of its own. The competition among vendors in this arena has become fierce, with so many companies dead-set on distinguishing themselves from one another.

It's an exciting market that will continue to expand as hypervisor, virtualization management and cloud stack management tools continue to improve. At this point, there's no shakeout in sight. In order to help users navigate these roiling waters, we suggest the following five tips:

1 | KNOW WHAT TO ASK VIRTUAL SERVER BACKUP VENDORS.

David Davis is a leading authority on a wide variety of virtualization and cloud topics. He is the author of the best-selling VMware vSphere video training library from TrainSignal and has written innumerable articles and books on a wealth of technology trends. The first question he suggests is asking would-be vendors where they came from—i.e., did the company come from the physical world, or was its backup product created for only virtual infrastructures? Knowing if products are specifically virtual makes it possible to determine how an organization may have designed its tools and provides insight about its user base.

Getting right to the point, Davis says, "How do they back up the data? Do they do agentless backup going directly to the virtual infrastructure data stores and virtual machines, and back them up directly? Do they use agents inside each virtual machine or on each physical server, or do they have other backup methods, such as SAN-based backups?"

He says he would also ask if vendors use the VMware vCenter API for data protection, and if they change block tracking. This is important to know because changed block tracking can significantly speed up the backup process and reduce backup windows. Other questions to ask vendors include:

- What are their tested restore times for not just one virtual machine, but also for a mass restoration of virtual machines in the event that an entire storage area network goes down?
- What is their off-site backup storage method, and how do they recommend that users retrieve data from that site?
- Do they have replication, or do they support cloud-based off-site backup storage?
- Do their products support multi-hypervisor environments?
- What sort of insight do they have into applications? Can they restore an individual Exchange mailbox or SQL database?
- Do they have 24-hour support, and what is included with the purchase of a license?

2 | PICK THE RIGHT TOOL.

With so many virtual server backup tools available, honing in on the right one is no easy task. As is the case with many current IT infrastructures, there is a mix of physical and virtual environments. For those companies that are 100% virtual, a dedicated virtualization backup product may be the likely choice. For those with mixed environments, the right call is a backup system that can go back and forth between physical and virtual modes. One way or the other, Davis strongly discourages the use of multiple backup tools. "For the sake of simplicity and licensing costs, I strongly believe that companies shouldn't have multiple backup tools," he explains. "It just doesn't make sense."

Davis also urges users to test vendor offerings and take their time doing so. "Every tool offers a free trial period that allows you to test the product on your own infrastructure," he says. "Put those tools through their paces with your applications, and focus on features related to recovery. Remember, you aren't just getting a tool to back up your virtual machines; more importantly, you want them to be restored and restored very fast. Test things like multiple restores at a time, file-level restore, and application integrity after restore."

3 | MOVE YOUR DATA OFF-SITE.

It's not enough to simply back up data—for safety's sake, it needs to be relocated off-site. One common fault with many virtualization backup tools is they stop once data is backed up and provide little or no information about moving it off-site. Due to bandwidth restrictions, replication is not an option for many companies. One way or the other, users should create an automated, controlled capability to move data from the backup repository to a portable device for off-site storage in the event of a disaster.

The good news is that off-site replication is no longer just for the largest of companies with their own cross-country fiber networks. As Davis notes, "Thanks to advancements in backup technology–backing up only changed blocks, deduplication and compression—now moving replication data off-site is affordable and practical."

4 | SPEED IS KING

Vendors are never shy about claiming the speed and reliability of their backup products, but unless users test them and share their results, we are left with only murky, unsubstantiated promises. Unfortunately, because backup and disaster recovery testing is so rarely done—it is reportedly too expensive and time-consuming—we will continue to be in the dark, for the most part, about both speed and reliability. That means there are no good answers to questions like, "How quickly can it get your largest server running again if it is lost?" and "How quickly can it restore 20 servers at once?" Users should insist that vendors provide them with real, live customer experiences that map closely to their individual needs.

5 | FUTURE-PROOFING ISSUES

The biggest issues facing backup users going forward include keeping up with the demands of the business no matter what backup tool or hypervisor is in use. According to Davis, "Your infrastructure and backup solution needs to keep up with the ever-increasing number of virtual machines, demands and resource consumption that's going on in the infrastructure. I think that's something to keep in mind. Also, a lot of companies are moving to or at least considering testing multiple hypervisors and also private or public cloud." He goes on to note that due to the more complex architectures being built by users, backup vendors face unusual circumstances, such as users splitting up their infrastructures across a hybrid cloud to a public service provider.

As Davis puts it, "Suddenly now, the backup vendors might be faced with 'OK, this is what we did. Now tell me how I'm going to back this up.' I think they'll be pushed by the market and by end users to keep pace." Users take note: Keep pushing those vendors for the information you need.