CHAPTER 1

VIRTUALIZATION CONCEPTS IN DISASTER RECOVERY

Virtualization is changing the disaster recovery landscape. Rethinking your hardware and software, testing methods and performance requirements is key.

EDITOR'S NOTE:

How virtualization changes the game

UPHEAVAL AND CHANGE are par for the course in the IT sector, but occasionally, a new technology comes along that profoundly changes the game. Virtualization is one such technology.

Virtualization lets IT departments decouple their services and resources from the underlying hardware for greater infrastructure flexibility and utilization. This translates to more bang for the buck.

This e-book is a beginners' guide to virtualization with chapters on disaster recovery (DR), test and development, server consolidation, high availability, storage, security and key technologies including VMware ESX, Microsoft Hyper-V and Citrix XenServer.

Virtualization simplifies DR. A physical or virtual server working in the primary data center can be copied into a virtual instance on almost any other server hardware located at the DR site. The DR site can run the virtual instance regardless of differences in the remote server's hardware. We'll explain how all this works in the chapter on DR.

Server consolidation and test and development are the meat and potatoes of virtualization. When developers were frustrated that they couldn't obtain the hardware needed to test their software, VMware was born. This is still where most IT departments start out with virtualization, and where much of the gains can be realized.

Heartened by the ability to run multiple machines on a single server, administrators often skip the effects to security and storage infrastructure. Fixing these problems after the fact is a headache.

The security chapter explains best practices for securing virtual machine guests on a single server as well as meeting various compliance issues.

The last chapter of this e-book covers three main server virtualization technologies—VMware ESX, Microsoft Hyper-V and the open source platform, Citrix XenServer, as well as the pros and cons of each.

Each chapter gives you all you need to know to enter the virtualization game. Once you've downloaded this entire e-book, you'll be ready for our Advanced Enterprise Virtualization seminars.

Jo Maitland
Executive Editor

Virtualization concepts in disaster recovery

Virtualization technology is changing the face of disaster recovery (DR). Traditional DR-based backup and restoration techniques typically imposed high IT costs as administrators anguished over delicate hardware dependencies—often driving some companies to ignore or overstate their DR preparedness.

While virtualization itself adds complexity to the environment, it also brings consolidation and flexibility that allows organizations to copy live storage and server workloads between remote sites running radically different hardware.

Virtualization is changing DR and, with that, altering the way that data center administrators look at basic hardware and software considerations, testing and performance. Concerns for regulatory compliance and security may also enter into the equation as virtualization continues to evolve.

VIRTUALIZATION'S EFFECT ON DISASTER RECOVERY

It might seem like a simple matter to back up a workload and restore it to another machine, but there practical concerns that further complicate this objective. Central issues are disruption, hardware dependencies and cost implications of both. First, migrating copies of workloads between physical hardware is disruptive, limits application and database availability and can potentially result in lost productivity or sales.

In addition, workloads and storage volumes are notoriously sensitive to physical hardware—the slightest difference could easily cause operational problems with workloads at the warm/hot remote site, as well as problems restoring them to the primary site.

Errors can dramatically extend recovery beyond the anticipated recovery time objective (RTO) and stress out an already overworked IT staff. In response, companies typi-

cally absorbed the cost of duplicate hardware and upgrade expenses. Some organizations have tried to mitigate this cost by omitting non-critical workloads from the DR plan, relying instead on the availability of common backups for later restoration.

Although virtualization seems to be mostly beneficial, no technology is perfect. Data center professionals must consider all sides in their DR plan.

The pros: There are several benefits to virtualization, the most important of which is hardware independence. Virtualization creates a layer of software abstraction—the virtual operating system or hypervisor—between the workload and its underlying hardware. This decouples the two and allows workloads to reside or operate in a virtual instance unrelated to the server and storage hardware underneath. Now a physical or virtual server working in the primary data center can be copied into a virtual instance on almost any other server hardware located at the DR site. This site can run the virtual instance without concern for differences in the remote server's hardware. It then can be restored to the original physical server or migrated to another virtual server.

Such flexibility enhances server availability. When a fault occurs on one virtual server, workloads can be migrated to another available server. Server virtualization also enables hardware consolidation, allowing multiple virtual instances to operate on a properly configured server.

A company can use different servers in the DR site and can manage with fewer physical servers if each one is running multiple virtual instances. The benefit of reduced hardware becomes more obvious when the primary site is also virtualized. There will be fewer servers at the primary site and virtual workloads can be moved non-disruptively. Synchronization can occur between sites

What is Recovery Time Objective?

THE RECOVERY TIME objective (RTO) is the maximum tolerable length of time that a computer, system, network or application can be down after a failure or disaster occurs. The RTO is a function of the extent to which the interruption disturbs normal operations and the amount of revenue lost per unit time as a result of the disaster. These factors in turn depend on the affected equipment and application(s). The RTO is measured in seconds, minutes, hours or days, and is an important consideration in disaster recovery planning (DRP). —WHATIS.COM

without affecting applications and data availability.

"Storage virtualization can be included in a virtual DR environment, but it's not a requirement for DR," said Ray Lucchesi, president and founder of Silverton Consulting, an independent technology consultant headquartered in Broomfield, Colo. Lucchesi said that many enterprise-class network-attached storage (NAS) and Fibre Channel (FC)

Minding your Ps and Vs

AS VIRTUALIZATION TECHNOLOGY garners greater attention in disaster recovery (DR) plans, you must understand the differences between physical and virtual data migrations.

With a **physical-to-virtual (P2V)** approach, physical servers or storage volumes at the primary site are replicated to VMs or virtual storage volumes at the DR site. This includes migrating operating systems, applications and data.

P2V is used most often in organizations that want to reduce the server or storage system count at the secondary site, allowing complete replication of the primary environment onto radically different hardware. However, restoring VMs or storage volumes back to physical counterparts can be problematic if any hardware changes take place at the primary site.

Virtual-to-virtual (V2V) is the most flexible approach, allowing VMs and storage volumes to be replicated between (and within) the primary data center and DR site, regardless of the underlying physical hardware involved. V2V DR supports operating systems, applications and data; recovery is simplified because it's not necessary to meet specific hardware requirements. Tools like VMware's VMotion can automate the process.

In a **virtual-to-physical (V2P)** environment, the OS, applications and data of a VM or storage volume are migrated to a physical counterpart at the DR site. V2P may appear in any number of backup scenarios, such as restoring a tape backup or virtual entity, to a physical server or disk array. It may be difficult to run the virtual workload on the physical machine, unless that physical server or storage system meets minimum hardware and configuration requirements. ■

storage subsystems natively support data replication.

Storage virtualization certainly improves flexibility in the creation, control and non-disruptive migration of storage volumes, but it doesn't offer the consolidation found in server virtualization. One TB of storage at the primary site still requires 1 TB of storage at the DR site.

The collective benefits of virtualization bring cost savings to an organization. There are fewer physical systems to contend with, reduced server hardware costs, reduced switch port counts, less wiring and floor space as well as lower power and cooling demands. Virtualization allows you to reallocate older servers or storage systems from a technology refresh at the primary site to the DR site, saving additional hardware capital expense.

Virtualization's hardware-agnostic and flexible nature eliminates most recovery problems and aids availability, minimizing downtime and the burden on IT staff. Hardware savings easily make up for the cost to license and maintain virtualization software.

The cons: Although there are few disadvantages to virtualization, you still must consider them in your DR planning. The abstraction layer needed for virtualization will add some complexity to the environment, which requires more management and may complicate troubleshooting since it can be difficult to track virtual problems to a physical source.

Consolidation is an even bigger issue; a fault on one physical server will affect all virtual machines (VMs) running on that server. High-availability architectures such as server clustering may be needed to guard against hardware faults.

Servers hosting multiple VMs must be configured with CPU, RAM, I/O and network resources adequate enough to support expected utilization. Otherwise, all VM performance on the server will suffer. This may not be a serious concern for a DR site that is simply used for restoration. "They [administrators] could potentially get by with less processing power at the secondary site and less operational costs," Lucchesi said. "But they spend a bit more on [virtualization] software to support that."

SUPPORTING VIRTUALIZATION IN DISASTER RECOVERY

Successful DR doesn't happen by accident. Actual infrastructure requirements can vary dramatically depending on DR goals and corporate budgets. Success requires careful consideration of several factors: network, server, storage and software resource considerations.

LAN/WAN resources: An infrastructure evaluation normally begins with network resources (LAN/WAN) that connect primary and secondary

EDITOR'S NOTE
VIRTUALIZATION CONCEPTS IN DR
PROS AND CONS
INFRASTRUCTURE
CASE STUDY
TESTING AND PERFORMANCE

sites. RTO influences bandwidth needs.

Synchronous replication duplicates each write between sites and maintains real-time site synchronization. However, this bandwidth-intensive approach generates the highest costs and is limited in distance. Asynchronous replication provides periodic synchronization between sites as time permits. This can achieve acceptable results over greater distances using lower-cost WAN connections like T1 (or slower), though more time must be allocated for the recovery point objective (RPO).

When evaluating bandwidth, remember that replication processes shouldn't impair user access or other daily network performance. "If you're doing several writes at the primary site, the workload across the network increases," Luchessi said. If the DR site will run "hot" to support actual users, there should be enough bandwidth and network connectivity to support anticipated user load.

Fibre Channel over Ethernet (FCoE), which is designed to support IP and storage traffic on the same interface, can also influence virtualization. Not only does FCoE promise to simplify storage networking, it can also reduce interface costs through the use of integrated adapters such as the Emulex LP21000 series.

"We're talking about combining a fiber HBA and a network card in one interface at the server and the switch level," said Pierre Dorion, data center practice director at Long View Systems, an IT solutions and services company headquartered in Denver. Dorion pointed out that using fewer network adapters simplifies server hardware requirements and reduces power consumption. He added that network virtualization can further enhance the flexibility of a virtualized data center or DR site.

Server size and performance: While there are no definitive requirements for a virtual server, you must size the server's resources—CPU, memory, I/O, and network connectivity—according to the number of virtual workloads that will reside on it. Experts recommend testing a VM setup prior to an actual rollout to ensure that application performance remains acceptable on the target hardware. Once this is determined, administrators can recommend hardware upgrades or test various configuration or resource throttling options to ensure that each VM runs properly.

Backups can hinder virtual server performance, so evaluate the machine's application performance while replicating VMs in a DR setting. "Backup is probably the most I/O-intensive operation you can subject a server to," Dorion said. "If you're running 15 servers at a time on one physical system, you can really bring a

(Continued on page 9)

CASE STUDY:

Prudential eases DR with virtualization

HIGH POWER AND cooling costs convinced Prudential Fox & Roach Realtors, based in Devon, Pa., to consolidate and virtualize half of its server infrastructure and, in the process, simplify its DR operation.

The firm replaced nearly 100 HP servers with an IBM BladeCenter system running VMware ESX virtualization software. Web servers, intranet servers, custom real estate applications, file and print servers and monitoring systems now run on virtual machines (VMs). With substantially fewer physical servers, the company expects to save $60,000 a year on power and cooling costs.

Prudential Fox & Roach Realtors runs four BladeCenter H chassis in its central data center as well as one BladeCenter S chassis in a separate location to support all of its remote offices. This secondary site acts as a DR facility.

The company replaced Sun Microsystems' tape storage equipment with IBM N-Series NAS to securely and centrally manage company assets and client data. Prudential takes snapshots of all its VMs and stores them on the N-Series at the secondary site.

"By bringing backup online and getting rid of tape, we can rebuild machines in minutes instead of days," said Tory Skyers, IT consultant for Prudential. Previously, the firm had to rebuild the operating system manually and would need a person in the secondary data center to install the backup client, perform the restore from tape or disk and reconnect the new server to the shared storage.

Now, recovery at the DR site involves creating a new VM and redeploying the virtual machine disk format (VMDK) over the network to this machine, while restoring the data from the snapshot. The VMDK file contains the whole operating system environment to enable simple loading and saving of the VM. Not only does this file contain the image of the operating system and application code, but it also describes the required configuration of the VM, including virtual processors, memory and devices.

This serves as a simple and portable single file that contains everything needed to describe the server environment and the actual code and data that makes up that server.

The new DR strategy was put to the test when a virus brought down one of the firm's servers. A snapshot of the server existed at the secondary site, and it was brought back online within two hours. "We can conduct business if one data center goes down without breaking the bank," Skyers said. **—J.M.**

(Continued from page 7)
physical server to its knees."

The performance implications of backup/recovery processes can radically affect consolidation choices for an enterprise. For example, five VMs might run well on one physical server, but it will slow to an unacceptable crawl during a backup. Dorion noted that there's nothing wrong with hosting a single VM such as a SQL Server on a single physical machine, which still produces non-disruptive migration.

Effects on storage: Virtualization adds flexibility and non-disruptive migration to storage, though virtual storage is not an essential element of virtual DR. There are no minimum storage virtualization requirements.

The DR site will require enough total disk capacity to hold storage volumes migrated from the primary site, but that storage does not have to be virtualized. Servers must have local storage large enough to retain all of the VM images intended for that physical system, so the DR servers and their local storage are almost always virtualized.

Third-party software tools: Software tools are essential for replicating VMs and storage volumes; many DR tools are available from the virtualization vendor. Citrix XenServer5 has built-in live migration and DR features. Other vendors like VMware provide separate free tools like VMware Consolidated Backup, which is designed to protect an entire VMware environment under VMware Infrastructure 3. VMware VMotion can move VMs non-disruptively between physical servers; even Windows Server 2008 R2 includes live migration of VMs between servers.

Are you ready for a DR SAN?

A VIRTUALIZED DR site is best served with a storage area network (SAN). The centralized high-performance storage provided by a SAN adds redundancy, rather than relying on individual disks within physical servers. It also enables the rapid migration of virtual images between systems. Cost-conscious organizations, though, may be reluctant to fund a conventional FC SAN for a remote DR site. Instead, organizations may consider an iSCSI SAN deployment to support storage and IP traffic on the same network. For many organizations, iSCSI running on a 1 GB Ethernet network strikes an acceptable balance between affordability and performance. ■

EDITOR'S NOTE
VIRTUALIZATION CONCEPTS IN DR
PROS AND CONS
INFRASTRUCTURE
CASE STUDY
TESTING AND PERFORMANCE

Server clustering software can also play a role in a virtualized data center or DR environment; Veritas Cluster Server from Symantec Corp. is just one example. Clustering enables physical servers to work in conjunction with each other, sharing their collective computing resources to handle more workloads or improve performance. Clustering also supports high availability—if one physical server fails, the remaining cluster elements take control and continue processing.

Other third-party software, such as vFoglight from Vizioncore Inc., can further enhance a virtualized environment by monitoring VM performance. Vizioncore's vReplicator can also enhance DR and high availability within a VMware environment.

TESTING AND IMPROVING PERFORMANCE

One of the principle weaknesses with DR is inadequate testing. Traditional DR required that recovery occur to a working environment. This resulted in unacceptable disruptions at the primary site, especially if recovery errors happened. The alternative was to attempt recovery to a test site, but recreating and maintaining additional redundant recovery hardware proved cost-prohibitive. When virtualization is used to consolidate servers in the DR site, it's simpler to test the recovery of many VMs to a

VIRTUAL DR CHECKLIST

Test DR regularly: Virtualization simplifies the DR-testing process. Take every opportunity to test and verify disaster readiness.

Don't ignore upgrades: Hypervisors and other software residing on servers at the DR site must be included in regular patch/update cycles.

Choose servers carefully: Select servers with computing power (CPU, memory, I/O and network connectivity) adequate enough to support the intended number of VMs and users.

Back up the backup: Protect VMs at the DR site using a SAN, or back up VMs using other storage like NAS or tape.

Balance virtualization with performance: Rather than back up multiple VMs simultaneously, stagger the process or reduce the number of VMs to manage the added I/O strain.

Look beyond servers: Look for opportunities to leverage other technologies such as network virtualization or desktop virtualization. ■

EDITOR'S NOTE
VIRTUALIZATION CONCEPTS IN DR
PROS AND CONS
INFRASTRUCTURE
CASE STUDY
TESTING AND PERFORMANCE

few extra virtual servers.

With an increasing number of "hot" DR sites, the availability of applications and data at the site itself is often taken as proof of DR readiness. For example, administrators can simulate a disaster at the primary site by rerouting DNS to the DR facility, and simply allowing users to work on the SAN and virtual servers there.

> Disk failure can cripple a physical DR server and leave many VMs inaccessible.

If that works, DR site content is replicated back to the production site (often non-disruptively), and the DNS is rerouted back to the main data center. DR in a virtualized environment can be tested more frequently with less effect on users. Administrators usually don't need to be at the DR site.

Regardless of the specific approach, testing a virtualized DR environment should extend beyond simply verifying recovery to include a performance evaluation. "Make sure that your DR environment can carry the processing load," Dorion said. "You may accept [your servers] running at a somewhat degraded level of service during a recovery effort."

Network monitoring tools can measure performance at the DR site, though actual end users can also provide solid feedback on performance snafus during a backup/restoration.

The proper use of storage in a virtual environment can improve DR. Dorion points out that disk failure can cripple a physical DR server and leave numerous VMs inaccessible. It's critical to protect VMs at the DR site with more traditional backups like tape.

"Virtualizing servers is no guarantee of reliability," Dorion said. "You still need to make sure that your data is adequately protected." Consider storing VM images on protected disk storage, such as RAID, in SAN or NAS arrays as an alternative. Centralizing the storage of VM images also allows more efficient reallocation from one physical server to another.

THE EVOLUTION OF VIRTUAL DR

Concerns about compliance and business continuance are driving the need for DR, but the landscape is still evolving. In addition to FCoE and network virtualization, ever-growing computing power and attention to security will influence the future of virtual DR.

The number of available processors limits server virtualization. Servers based on inexpensive two-core processors can easily migrate to more powerful four- or six-core processors like Intel's Xeon 7000 series or AMD's Opteron family. This is espe-

EDITOR'S NOTE
VIRTUALIZATION CONCEPTS IN DR
PROS AND CONS
INFRASTRUCTURE
CASE STUDY
TESTING AND PERFORMANCE

cially true for processors with "virtualization acceleration" technology, such as Intel VT or AMD-V capability. Eight-core platforms that use two four-core processors are cropping up, and "true" eight-core processors such as Sun Microsystems' UltraSPARC T2 will become more commonplace in the next 18 to 24 months.

Security will also play a vital role in future virtualization. Traditional security techniques generally monitor network traffic and its behavior. This is suitable with distinct physical servers and networking hardware, but when multiple servers are hosted on the same machine—along with network virtualization technologies like "soft switches"—virtual security must emphasize interprocess monitoring of VM interaction.

Virtualization security flaws also surface in server configuration and OS patching. It's much easier to overlook a configuration setting or OS patch level when there are dozens of VMs on a physical server. Hypervisors can also suffer from security flaws, potentially exposing the VMs that run under them. Virtualization users should add hypervisor patching/updating to their OS maintenance process.

The introduction of virtualization has dramatically changed the traditional data center environment. As this technology continues to evolve, so will virtual DR considerations and planning. Having a solid plan in place and examining each aspect will make all the difference. ■

ABOUT THE AUTHOR

Stephen J. Bigelow, Senior Features Writer, has more than 15 years of technical writing experience in the PC/technology industry. He has authored hundreds of articles and more than 15 feature books on computer troubleshooting, including *Bigelow's PC Hardware Desk Reference* and *Bigelow's PC Hardware Annoyances*. Contact him at sbigelow@techtarget.com.

SearchServerVirtualization.com

Cathy Gagne, Editorial Director, cgagne@techtarget.com; **Christine Casatelli**, Managing Editor, ccasatelli@techtarget.com; **Michelle Boisvert**, Features Editor, mboisvert@techtarget.com; **Martha Moore**, Copy Editor, mmoore@techtarget.com; **Linda Koury**, Art Director of Digital Content, lkoury@techtarget.com; **Marc Laplante**, Publisher, mlaplante@techtarget.com

- **Virtualization 101**
- **Using virtualization for testing and development environments**
- **What is Microsoft Hyper-V?**

About Dell Inc.:
Dell Inc. (NASDAQ: DELL) listens to customers and delivers innovative technology and services they trust and value. Uniquely enabled by its direct business model, Dell is a leading global systems and services company and No. 34 on the Fortune 500. For more information, visit www.dell.com, or to communicate directly with Dell via a variety of online channels, go to www.dell.com/conversations. To get Dell news direct, visit www.dell.com/RSS.