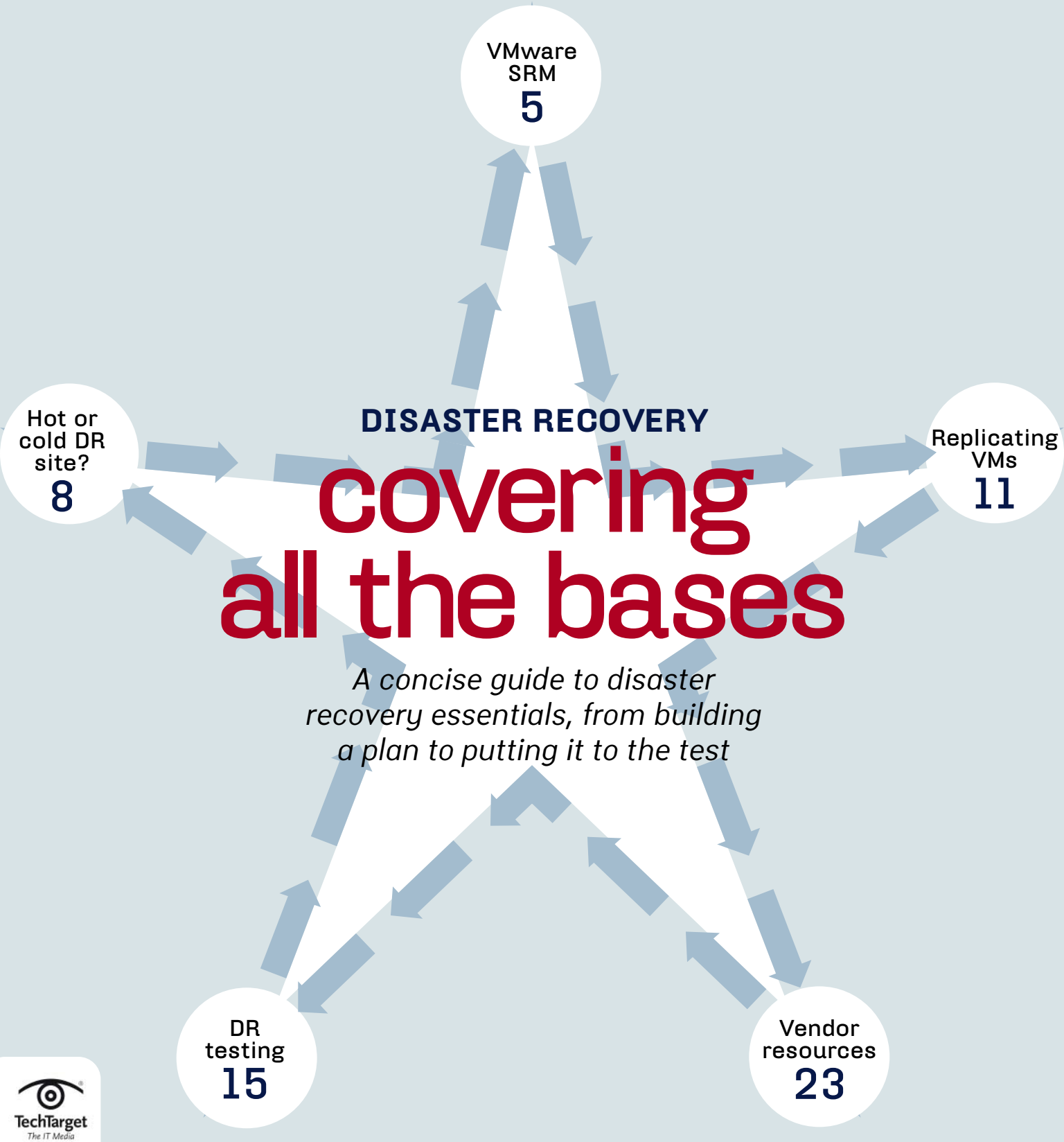
Managing the information that drives the enterprise

STORAGE



DISASTER RECOVERY

covering all the bases

A concise guide to disaster recovery essentials, from building a plan to putting it to the test

TechTarget
The IT Media ROI Experts

New tools, new challenges for DR

By Rich Castagna

In almost every conversation we have, and on every survey we run, disaster recovery (DR) is consistently the No. 1 priority for storage managers. When you think about it, that represents a startling turnaround. Only a few short years ago, DR was considered something of a luxury item, affordable by only the biggest companies with the fattest budgets. I don't have to run through the list of recent incidents that have put that theory to rest for good.

Today, the issue isn't whether or not you have a DR plan, but rather to have one that will work when needed. Effective testing and remediation is, of course, a requisite, but it's even more important to match up available technologies with corporate objectives. The good news is that today there are ample technology choices to employ in a DR plan. But that's the bad news, too, as storage managers are pressed to find the right combination of technologies and processes that will help ensure that their businesses can withstand and recover from an interruption in normal operations.

Today, the issue isn't whether or not you have a DR plan, but rather to have one that will work when needed.

Server virtualization is a good example. It offers a level of resiliency for recovering both physical and virtual servers that surpasses most other approaches. But its very flexibility poses a challenge to the storage team, requiring the same lithe response from storage systems in the event of a disaster. And the growing popularity of virtual machines brings along a new crop of recovery tools—tools storage managers will have to become intimately familiar with.

The high cost of replication services and the requirement of having a duplicate physical environment at the recovery site were key contributors to the notion that DR was out of reach for small or midsized firms. But, in addition to price drops, replication products are now available that bridge the gaps between unlike storage systems and allow data to be replicated among different systems.

And as we've all seen when monster storm systems take out huge swaths of geographic regions, it's not enough to ensure that your data is copied somewhere—you also need to be sure that "somewhere" is out of the path of whatever has brought your primary data center to its knees. Choosing the location of your recovery site might be the most important DR decision you make.

DR today is very much a good news/bad news story. The tools are better, but the challenges are greater than ever, especially with the kind of unabated data growth we've seen of late. We created this special guide to help you hone your DR skills, find the gaps in your DR plan and help build an effective testing plan. ⊙

Rich Castagna (rcastagna@storagemagazine.com) is Editorial Director of the Storage Media Group.

With disaster recovery,
speed is the name of the game.

vmware®

Take your business to a whole new level with VMware Infrastructure.

Disasters come in all shapes and sizes-and it's your job to be prepared for all of them. But until now, you didn't have an option that provided the speed and reliability you needed without prohibitive cost and complexity. That was before VMware.

With VMware virtualization, you get an automated solution that's easily tested, hardware-independent and offers complete infrastructure protection.

All of this, and more, with an unprecedented level of simplicity.

VMware Disaster Recovery. Sounds like a good day to be in IT.

Find out more at www.vmware.com/go/fast

VMware SRM

VMware Site Recovery Manager promises to change the way storage admins manage DR for their virtual server environments.

By Jerome M. Wendt

AUTOMATED DISASTER RECOVERY (DR), shortened downtimes and simplified business continuity are some of the benefits that VMware Site Recovery Manager (SRM) offers. Controlled by VMware VirtualCenter and working in conjunction with new storage replication adapters on storage systems, SRM stands poised to change how companies think about and manage DR and data backup for their VMware virtual server environments. However, for companies that lack a carefully planned and documented DR plan for their virtual servers, implementing SRM can be tricky.

There are five main components that must be in place prior to implementing VMware SRM:

1. VirtualCenter Server 2.5
2. Virtual Infrastructure (VI) Client 2.5
3. Oracle Database 11g or Microsoft SQL Server
4. Storage systems with a storage replication adapter (SRA) that appears on VMware's hardware compatibility list
5. VMware ESX Server 3.0.2 Update 1 or ESX 3.5 Update 1

But even with these building blocks in place, installing and using VMware SRM is still far from a turnkey operation. Chris McCall, senior product manager for LeftHand Networks Inc. (which has been acquired by Hewlett-Packard Co.), says that LeftHand has successfully tested SRM in its labs and demonstrated it at events such as VMworld Europe. However, McCall recommends that companies have a well-thought-out DR plan prior to installing.

VMware advises users to pay close attention to the following SRM configuration requirements: storage systems used with VMware SRM must be the same vendor's model at the production and DR site, replication should be integrated and certified with SRM and the storage replication adapter that's supported by SRM should be used. The storage replication adapter allows SRM to communicate with the storage system and manage the replication of data of the specific storage system's LUNs that SRM needs for the automated recovery at the second site.

Though the need for the storage system to appear on VMware's hardware compatibility list isn't explicitly stated as a prerequisite for SRM, companies should view it as one. LeftHand Networks has found that as many as three-quarters of companies won't implement storage hardware unless it appears on VMware's hardware compatibility list.

Even with building blocks in place, VMware SRM is still far from a turnkey operation.

Companies should also not assume that VMware SRM automatically recovers apps on the virtual machines on ESX hosts. SRM only recovers the virtual machines hosted on each ESX server, not necessarily the application that the virtual machine (VM) hosts. Unless the application happens to start as part of the boot-up process of the VM on the ESX Server at the DR site, companies will still need to put in place separate processes to recover these applications.

Glen Rhodes, CA's vice president of product marketing for recovery management and data modeling, points out that VMware SRM is focused on servers and storage—not the application layer. So if failures occur at the application layer of a virtual machine while the infrastructure layers remains operational, no failover to a secondary site will occur because SRM doesn't detect the application failure.

"Companies need application-aware software that automates the scripting and failover to bring the application back online on another [physical or virtual] server at the remote site," says Rhodes.

VMware SRM is a needed new feature for companies looking to automate disaster recoveries of their VMware virtual server environments. However, configuring it is not a quick and simple process. A company should devote a substantial amount of time to planning and documenting which VMs they want to recover and in what order. Only when that is done should companies contemplate implementing SRM in their environments. ⊙

Jerome M. Wendt is lead analyst and president of DCIG Inc.

Designed to:

- Improve performance.
- Tighten security.
- Extend disaster recovery.

All while helping to reduce costs.

With numerous accolades and many satisfied customers, **CA ARCserve® Backup and CA XOsoft™** will help ensure that your business-critical applications will be available when you need them.

Transforming IT Management®

See how easy it is to protect your business-critical applications with **CA ARCserve® Backup** and **CA XOsoft.™**

Get your FREE evaluation software today at ca.com/rm.

hot or cold DR site?

Getting your applications up and running after a disaster can be a painful task if you don't have a proper disaster recovery (DR) plan in place.

By Deni Connor

CHOOSING THE TYPE of protection you need in the event of a disaster depends on how long your business can sustain being down. Getting applications back in operation quickly can be an arduous process, especially if you don't have a DR process in place.

Consider Peter Haas, director of technology for the Supreme Court of Louisiana in New Orleans. Two years ago, after his offices were clobbered by Hurricane Katrina, Haas spent innumerable hours devising a DR plan.

During the aftermath of Katrina, Haas made several trips into the crime- and chaos-ridden city to retrieve servers, tapes and storage gear and to install them in a DR site several hours away from New Orleans.

"The biggest entity an organization needs to think about is: 'How long can I afford to be down?'" says Haas. "We asked ourselves that question, and after Katrina, we realized we can't afford to be down much at all."

Haas installed CA Inc. XOsoft Replication Option to replicate his Oracle databases and Microsoft Exchange and SQL servers in

real time to a location in Baton Rouge. “If we had a disaster right now, we could be back up in under an hour,” he says.

The hot site Haas implemented is fully equipped with all the server, network, storage gear and applications to continue operations essentially unabated. That is the most expensive of the DR options.

Instead of hot sites, some companies opt for less-expensive cold sites, in which they need to obtain, provision, install and configure all the equipment in the event of a disaster. In between the hot site and cold site, both in terms of availability and cost, is the warm site, where computers and network gear may be installed but not configured, upgraded or in operational readiness.

“It really comes down to the urgency a company needs to recover their environment,” says Jim Grogan, vice president of consulting product development for SunGard Availability Services. “If the recovery time objective [RTO] is measured in days, it is going to mean a customer needs to look at a hot site. If the RTO is measured in weeks, they might be in a position to look at the warm site. Only if the RTO goes beyond that is the cold site appealing.”

Some companies opt for less-expensive cold sites, in which they need to obtain, provision, install and configure all the equipment in the event of a disaster.

Grogan says that many organizations look at cold sites not so much as a place where they would recover, but as a place for ongoing operations in the event of a catastrophe that would require them to be out of their offices for several years.

Not unlike Haas is Brian Cutler, executive vice president and CTO for Arrow Financial Services. Cutler also chose a hot site that he manages himself rather than having a co-location service do it for him. Cutler’s DR site is outfitted with EMC Corp. Symmetrix gear from which he replicates data from one site to another site located 200 miles away.

The cost of not having a DR site, when systems are down, would be approximately $2 million a day for Arrow Financial Services. “The biggest factor [in choosing a hot, warm or cold site] is going to be the business decision—how much does it cost me to be down for a day, two days, three days, etc. That’s the key evaluation,” says Cutler. “You have spent a whole bunch of money, and if it doesn’t cost you that much for downtime, you are wasting your money to be hot.”

The Supreme Court of Louisiana’s Haas’ hot site isn’t the total answer to his DR plan. Upon his recommendation, IT personnel who work with Haas wear USB thumb drives around their necks. Stored on each thumb drive is the company’s DR plan, phone numbers of key personnel that play a part in the recovery process and other information and data files necessary for implementing the plan. Testing the plan is also crucial to the business. ⊙

Deni Connor is principal analyst for Storage Strategies NOW, an IT research firm in Austin, Texas. You can reach her at dconnor@ssg-now.com.

What Happens When SharePoint Goes Down?

You rely on MOSS to communicate, to action immediate service and to collaborate across the organization.

Without MOSS everything stops. Productivity dies, employees are isolated and information flow ends.

Keep Lines of Communication Open

The ability to collaborate within teams across geographic dispersion is vital. There is no acceptable downtime window for SharePoint, it must be available 24x7.

Planned maintenance, storage failures, power outages and user errors are all reasons for downtime. Factor these into service continuity plans.Service continuity plans should have protection of MOSS as a high priority. Projects and information sharing may depend on it.

Keeping SharePoint Available

Neverfail is an award winning solution to keep users connected to MOSS. Disaster recovery, high availability and data protection comes as standard. Out-of-the box your entire SharePoint farm is protected. Predictive monitoring ensures best practice. Replication ensures data is always protected. Automated failover keeps SharePoint available when things go wrong.

Can you afford to be without email for a day?

Visit www.neverfailgroup.com/resources/whitepapers.aspx for your copy of the Neverfail for SharePoint White Paper.

Or, better still, email us at info@neverfailgroup.com today or call 512.327.5777 to join organizations across the World who've chosen Neverfail for the most effective disaster recovery, data protection and high availability solutions in the industry.

EXCHANGE • SQL SERVER • FILE SERVER • IIS • SHAREPOINT • BLACKBERRY • LOTUS DOMINO • RIGHTFAX

replicating VMs

Server virtualization has the ability to simplify disaster recovery for enterprises as well as small- to medium-sized businesses.

By Arun Taneja

MPLEMENTING DISASTER RECOVERY (DR) solutions has been one of the most difficult tasks for IT departments over the past several decades. So it's not surprising that in a typical enterprise only the most mission-critical applications are protected via remote replication to a DR site. In a typical small- to medium-sized business (SMB), even fewer apps are protected in this manner.

Less than 20% of applications are protected by DR in a typical enterprise, and the number is smaller for a typical SMB. However, all of that is changing due to server virtualization's march into IT shops of all sizes and its inherent ability to simplify DR.

To protect data on a physical server, identical servers need to be available at the DR site and in the main data center. In a large majority of the cases, even storage has to be identical. Server settings need to be identical, including the operating system, driver and BIOS levels, Windows registry settings, and the host bus adapter (HBA) and network interface card models. The same goes for application version and security settings.

The expense associated with buying and maintaining identical pieces of gear on both sides is out of reach for many organizations. Out of necessity, DR is relegated to only those mission-critical applications that could jeopardize the company's existence if they weren't available. Financial data, customer orders, inventory and manufacturing status fall in this category.

Storage administrators have told me numerous times that they don't mind using an EMC Corp. Symmetrix for the primary site, but they ask,

"Why can't I use an EMC Clariion for the secondary [DR] site? I can deal with lower performance in case of a disaster as long as the systems are available." The same questions are asked about other vendors' storage gear.

Also, testing DR is disruptive to production and quite expensive because the recovery process is mostly manual. And, without up-to-date testing, there is no assurance that all systems are functional or that recovery will indeed occur.

THE BENEFITS OF SERVER VIRTUALIZATION

Enter server virtualization. By abstracting away the physical server components and representing everything in logical terms, server virtualization eliminates one of the biggest issues of DR: the need for exactly the same equipment at both sites. It allows all system elements and storage to be dissimilar, without jeopardizing recovery. Similarly, one is free to choose the style of replication, be it host-based, storage-based or network-based.

Additionally, server virtualization simplifies the recovery process by encapsulating not only the data (as done in a physical DR situation) but the entire system, including system configuration, OS, data and applications into a simple file or files, which can be easily replicated to the remote site. Recovery is achieved by simply running this file as a virtual machine (VM) in an appropriately configured physical server on the remote site.

Testing DR is disruptive to production and quite expensive because the recovery process is mostly manual.

By replicating this file on a periodic basis to the remote site, the recovery point objective (RPO) is improved. The fact that recovery is almost instantaneous means the recovery time objective (RTO) is also improved. But most importantly, the file can be run on the remote site anytime to test the viability of DR without impacting production on the primary site. Given the fact that systems on the remote site can be "lesser" than those on the primary site and can be of different makes/models, the IT organization can use existing equipment without worrying about patches and security levels. DR just got a lot simpler and less expensive.

Lower costs mean more applications can be protected. Of course, not all mission-critical applications are run on VMs, but server virtualization is a major step forward for DR.

According to VMware, more than 55% of VMware users are employing server virtualization to obtain DR benefits. In fact, DR and server consolidation are the two main reasons users deploy server virtualization. Server virtualization is bringing DR to the forefront and making it easier for companies of all sizes to enjoy the benefits of remote replication and DR.

DR is essential to protect against power failures, floods, earthquakes and other natural disasters, discounting human errors. The fact that DR

traditionally had been reserved for “elite applications” had nothing to do with the business’ need for protection. Instead, it had to do with the cost and difficulty of doing DR.

Server virtualization is in its infancy with less than 5% of the worldwide servers virtualized. The need to protect large numbers of applications from site disasters couldn’t be greater. The task of developing, implementing and testing a DR plan is now more feasible and affordable. The era of broad-based DR is upon us—and not a moment too soon.

Arun Taneja is founder and senior analyst at Taneja Group.

Special Report: Online Backup

Have you looked at Online Backup lately?

Visit the SearchDataBackup.com "Online Backup Special Report" to find out how online backup has evolved:
www.SearchDataBackup.com/online_backup

Sponsored by:

The Web's best storage-specific information resource for enterprise IT professionals

DR testing

In addition to periodically testing your disaster recovery (DR) site, DR testing tools can constantly monitor the site's readiness to recover from a disaster.

By Robert L. Scheier

TESTING THE STORAGE PORTION of your DR plan requires tools to ascertain if data was backed up properly. Proper testing may also require an application to constantly monitor the DR site's storage infrastructure—from the number of disks to the configuration of RAID arrays—to ensure it matches the storage configuration at your primary site.

The first place to look for confirmation that critical backups and data replications to the DR site took place is the backup and replication software you're using and the reports it generates. In addition, the same tools that storage admins use for day-to-day storage efficiency and management can help assess the health of their backup infrastructures, says John Sing, a senior consultant on business continuity strategy and planning at IBM Corp.

Next, test the recoverability of data and applications from the DR site. Many firms perform tests of one or several applications, or on selected portions of the backup environment, to reduce costs and avoid the risk of disrupting production applications.

Patrick Honny, departmental information systems manager for the County of San Bernardino Auditor/Controller-Recorder, performs an overall DR test once a year, based on the assumption that the entire primary site has failed. He also tests the storage portion of his DR plan monthly. "Basically, that's as simple as repointing production servers to the Isilon [Systems Inc.] SANs that are receiving replicated data and pulling up some files," he says.

PRODUCTION-LEVEL TESTING

Some users may want to test their DR environment under actual production-level conditions with, for example, the actual number of users an application supports and the level of transactions the application needs to process in specific time intervals. In those cases, automated software can be used to reduce the time, effort and expense required.

IBM's Sing, who uses automated testing tools, says he "can no longer afford to take five, 10 or 15 highly paid individuals off their jobs and dedicate them to two days of testing." Automated test tools en-

A sampling of backup reporting applications

Vendor/Product	*Capabilities*	*Platforms supported*
Aptare Inc. StorageConsole Backup Manager	Provides customizable portal, drill-down dashboard	Symantec Veritas NetBackup 3.2-6.5; Symantec Backup Exec 9.1, 11d; IBM Tivoli Storage Manager 5.2-5.4; EMC NetWorker 7.2-7.3; HP Data Protector 5.5-6.0; Sun StorageTek ACSLS Manager; Oracle Recovery Manager (RMAN)
Bocada Inc. Bocada Enterprise 5	Can report on success/failure, performance on SLAs and consumption of backup resources by business unit so costs can be allocated among units	Symantec, EMC NetWorker, IBM Tivoli Storage Manager, CA ARCserve and HP Data Protector
EMC Corp. Backup Advisor	Identifies the cause of current backup problems and highlights potential problems	Windows, HP-UX, AIX, Solaris and Linux; backup apps, including EMC's NetWorker and Avamar, CA ARCserve, CommVault Galaxy, Hewlett-Packard Data Protector, IBM Tivoli Storage Manager, and Symantec NetBackup and Backup Exec
Hewlett-Packard (HP) Co. Storage Essentials Backup Manager	Automatically discovers and reports on backup environment with configurable backup reporting dashboard	Most major server operating systems and storage hardware
Symantec Corp. Veritas NetBackup	Provides backup and recovery for heterogeneous operating environments; centralized reporting and service-level management of backup operations	Generates reports for Symantec Veritas NetBackup, Symantec Backup Exec, CommVault Galaxy, EMC NetWorker and IBM Tivoli Storage Manager
Tek-Tools Inc. BackupProfiler	Web-based reporting and analysis summarizing status of backups	Windows 2000/2003 Server or Pro, Linux, Solaris; supports backup software from CA, IBM, Syncsort, Symantec, BakBone Software and Sun StorageTek

TEST MORE OFTEN AND MORE THOROUGHLY

IN TESTING DISASTER RECOVERY (DR) PLANS, IT staffs often overlook how applications depend on each other for data, and they don't understand which related sets of data need to be backed up and restored to the same point in time, says Bill Peldzus, director of data centers, business continuity and disaster recovery at GlassHouse Technologies Inc., in Framingham, MA.

By failing to fully understand application dependencies and properly identify "consistency groups" (related sets of data which should be updated to the same point in time) organizations risk running DR tests that don't accurately reflect how well an application could be recovered after an actual disaster, he says.

For example, an order-entry system might have a recovery point objective (RPO) and a recovery time objective (RTO) of four hours. A customer database with which it shares data might have an RPO and RTO of 12 hours. When the data for both applications is restored in a test, "you have customers without orders and orders without customers because the data wasn't recovered in a consistent fashion," says Peldzus.

While many replication applications can identify consistency groups, they're much more difficult to use across different platforms, such as PC-based, minicomputer and mainframe servers, he says. Peldzus also recommends that companies test to see if they can recover all of their critical applications within the required time period, rather than (as is often the case) only testing the applications needed by one business unit or that serve one function, such as email.

Finally, he suggests testing critical applications most often. Applications with RPOs or RTOs of less than 24 hours are candidates for testing two to four times per year, rather than just annually, he says.

sure tests are done consistently and can be repeated over time, which makes them more useful for auditing purposes.

For example, Compuware Corp.'s Hiperstation line of software "records network traffic heading to and from the mainframe," says Mark Schettenhelm, Hiperstation product manager. It can then be used to access a remote site, "and it's as if you have a hundred people beating away at that system," he says.

WRITABLE CLONES

Any test requires accessing the replicated data, even if only to read or write to a few sample database fields. That access can interrupt the replication process, raising the danger that the replicated data would become out of date if disaster or hardware failure occurred during the DR test.

A number of vendors aim to solve that problem by creating replicas of data that can be written to and kept current. According to NetApp Inc., its FlexClones act as "a transparent writable layer" in front of the snapshot copy of the data in the DR facility, allowing the snapshot to be used for DR testing while remaining up to date in case of an actual disaster. Symantec Corp. has enhanced a similar feature called Fire Drill in the 5.0 release of Veritas Storage Foundation for Windows.

CA Inc. offers a similar capability with XOsoft Assured Recovery, which suspends the replication of data between a master and replica

copy. It spools changes made during a test and applies them to the replica only after the test is over and replication resumes. CA XOsoft Assured Recovery works in conjunction with the CA XOsoft Replication and CA XOsoft High Availability DR and business continuity software (formerly WANSync and WANSyncHA, respectively).

These writable replicas not only make it safer to do DR testing, but they make the replicated data available for other uses, such as data mining, and test and development.

STAYING IN SYNC

One major challenge in maintaining a DR site is configuring it exactly the same as the primary environment, so that when application servers link to the backup site they can connect to the appropriate storage and continue operation.

"With pressure on businesses to respond more quickly to customer demands, the IT infrastructure supporting the business changes on a daily basis," says Bob Laliberte, an analyst at Enterprise Strategy Group, in Milford, MA. "So any DR environment that was implemented and tested on day one could be at risk on day two. Unfortunately, that risk isn't discovered until a copy of the backup is needed or a DR test is run."

Jeff Pelot, chief technology officer at the Denver Health Hospital and Medical Center, saw how a seemingly minor change in the backup environment can cripple a DR effort after one of his LeftHand Networks Inc. IP SANs (LeftHand has been acquired by Hewlett-Packard Co.) failed to take over for another during a monthly DR test. "LeftHand was migrating from their iSCSI initiator to Microsoft's [iSCSI Software] Initiator ... and I guess we found a bug," he says. Pelot says he's now "fairly comfortable" his systems will work as needed, but he admits that "what I don't know is what scares me"—that any update by any vendor's product might introduce a similar bug that could crash his DR systems. For that reason, his staff carefully evaluates which upgrades are critical and applies them to one system in a cluster at a time to ensure they work before installing them on the other system, he says.

Many storage shops maintain a knowledgeable staff only at their production sites and not at their DR sites, says Dan Lamorena, senior product marketing manager at Symantec. That makes it harder to ensure that no critical data is lost during replication, and that the proper volumes and LUNs are configured in the right way at the DR site, he says.

MONITORING AND CONFIGURATION TOOLS

The difficulty of manually synchronizing a primary environment and a backup environment has led to the development of automated monitoring and configuration tools. The FlashSnap feature in Veritas Storage Foundation Enterprise enables admins to create application server groups that ensure the application servers are configured to connect to the appropriate backup storage in the event of a hardware failure in the primary data center, says Sean Derrington, Symantec's director of storage management. This eliminates much of the effort and error associated with manually configuring such servers, he says.

Continuity Software Inc.'s RecoverGuard continually checks to deter-

mine that all changes made to the primary site are reflected on the backup site, and identifies dependencies among servers, storage devices, databases and apps. It also automatically detects gaps, such as the passive node on a cluster not being mapped to the correct disk volume, which could cause a problem during a DR event.

RecoverGuard, which Continuity Software plans to offer as a service, currently supports EMC Corp. and NetApp arrays. Support for Hitachi Data Systems hardware is due to be released next.

EMC's WysDM for Backups continually monitors backup environments and provides customized policy-based alerts about problems that could affect the DR environment. It can report on servers that haven't been backed up within a given period of time, and backups that need to be rescheduled to meet service-level agreements, among other conditions.

BladeLogic Inc.'s Data Center Automation suite can monitor the configuration of backup data centers to see if they vary from corporate policies. Vick Viren Vaishnavi, BladeLogic's director of product marketing, says some customers are using the suite to help synchronize changes among sites.

Tracking such changes is much easier when a firm maintains the same hardware and software at both the primary and DR site and uses virtualization to mask any disparities between the two. Dick

Tools that report on the storage infrastructure

Vendor/Product	*Capabilities*	*Platforms supported*
Continuity Software Inc. RecoverGuard	Monitors storage, servers, database and replication infrastructure for configuration problems	EMC Symmetrix/DMX, SRDF, TimeFinder and Clariion; NetApp Data Ontap 6.5/7x
EMC Corp. ControlCenter	Maps and monitors performance of the storage environment	Arrays from EMC, IBM, Hitachi, HP and NetApp; Unix, Windows, VMware and mainframe operating systems
IBM Corp. TotalStorage Productivity Center Suite	Discovers, manages, configures and monitors storage devices	Fullest capabilities for IBM disk and tape products
Onaro *(now owned by NetApp)* Replication Assurance, Service Insight	Inventories all devices involved in replication and the type of replication being performed; verifies that replication services meet defined requirements	EMC SRDF Family, EMC TimeFinder Family
WysDM Software Inc. *(acquired by EMC)* WysDM for Backups	Reports on performance of backup operations; monitors backup environment for problems	Windows, Red Hat Enterprise Linux; Solaris and SUSE Linux Enterprise; most backup applications from CA, EMC, HP, IBM, NetApp, Oracle and Symantec

Cosby, systems administrator at Estes Express Lines, used system utilities for his firm's IBM System Storage DS8000 to mirror changes in data, as well as changes to the sizes of the underlying volumes and LUNs, between the Richmond, VA-based headquarters and a DR facility in Mesa, AZ. But Cosby says he wouldn't be able to rely on this integrated process if, for example, he introduced EMC storage into the environment.

CULTURAL CHANGES

Along with the right technology, storage admins need to put the proper processes in place to make sure their DR environments work as needed in an actual disaster. IBM's Sing recommends admins develop detailed schemas that specify what data is most important and needs to be recovered quickly. That will help them determine if they're backing up the right data to meet required recovery time objectives and recovery point objectives.

All too often, says Sing, "storage administrators don't have as much insight as they need about the business value of the data for which they're responsible." That makes it harder for them to restore the most crucial data the fastest. One shortcoming that often emerges during testing is the realization that the storage admin has backed up only the data files associated with an app and not the files needed to actually bring up the app at the DR site, says Greg Schulz, founder and senior analyst at StorageIO Group, in Stillwater, MN.

Some cultural changes can also ensure tests get done. Although EMC suggests customers test critical applications several times a year, many are still struggling to test once a year, says John Linse, EMC's director of business continuity services. A 2007 Symantec survey of more than 1,000 data center managers showed that lack of staff, fear of disrupting business as usual and lack of money are the most common barriers to running a full DR test. One reason, says Linse, is that "DR is sort of a second fiddle to operations" in many companies.

Educating others about storage's role in keeping vital apps running can ensure that staff members keep storage admins informed about changes that could affect DR, says Gil Hecht, CEO at Continuity Software.

He gives the example of a DBA who needs more disk space for a critical production app on a weekend, when the storage admin isn't available to provision it. The DBA might take unused space on a test-and-development system to keep the production app running and plan to tell the storage admin later. But if the DBA forgets, "the storage guy hasn't got a clue what his disk is being used for," says Hecht, or that the test and development system isn't replicated to a backup site and has thus invalidated the firm's DR plan.

Automated tools catch such changes, but Hecht says storage admins must educate other staffers about the need to communicate big and small changes, as even a small configuration change will affect the company's ability to plan for and recover from a disaster. ⊙

Robert L. Scheier is a freelance writer who covers storage and other technologies from his home in Boylston, MA.

Check out the following resources from our sponsors:

CA XOsoft Live Trial Download

CA ARCserve Backup Live Trial Download

"Take Off With CA Recovery Management" Mail-in Rebates (EU Rebates for ARCServe and XOsoft)

Neverfail for SharePoint

Neverfail's Vital Role in Server Virtualization

Business Continuity: Choosing the Right Technology Solution

VMware White Paper: Transforming Disaster Recovery—VMware Infrastructure for Rapid, Reliable and Cost-effective Disaster Recovery

Yankee Group: "Disaster Strikes! Is Your Business Ready? Disaster Preparedness for Mid-Sized Firms"