

Disaster Recovery

in the 21st Century

by Alan Mark



The formula for achieving a successful relationship is simple: you should treat all disasters as if they were trivialities but never treat a triviality as if it were a disaster.” (Quentin Crisp, *Manners from Heaven*, ch. 7.)

Crisp’s quip should be the foundation for business models as well as the foundation for human relationships. In theory, companies should be confident that despite any interruption—whether that interruption is due to a computer virus, a hurricane, a flood, an earthquake, a fire, or a bomb—business will continue as if nothing happened. To achieve this goal, companies must duplicate many aspects of their business to another location, and that duplication must include people as well as equipment.

Rather than asking your boss to start a human-cloning project, you should first determine how to effectively clone your company so it won’t go under if a disaster strikes. Over the past decade, the computing industry has built millions of information highways, but many of these highways have single points of failure. These electronic roads are similar to Germany’s autobahns, where speed is more important than safety. However, just like regular highways, electronic highways need police for protection and ambulances for cleaning up the mess if an accident occurs.

IT’S ALL RELATIVE

When I was young, my father always kept a spare pair of glasses in the glove compartment of his green Rambler. He explained that if his glasses were ever lost or broken, he wouldn’t have to walk around nearly blind. I didn’t know how bad his eyesight was, but he certainly couldn’t drive without glasses.

One weekend my family drove from Los Angeles to San Diego. The first stop after the two-hour drive was an amusement park with a large wooden roller coaster. After we were strapped in the roller coaster, my dad took off his glasses and placed them in his shirt pocket. It wasn’t his brightest moment. When the ride was finished, his glasses had vanished. Fortunately, we went to the car, and he put on his spare glasses.

How does this story relate to disaster recovery? *Disaster* is a relative term. Having a vacation ruined because my father lost his glasses would have been a disaster for me as a young boy.

Your first step in creating a disaster recovery plan is to determine what *disaster* means to your company. For some companies, one hour of downtime is a disaster. Internet-focused companies consider 13 seconds of downtime a disaster because customers grow impatient after that time and may switch to a competitor.

In the business world, companies are talking about disaster recovery like never before. For many companies, it’s almost a mission to get a plan in place in case something bad happens again.

This article explains the basic steps you should take to prevent total disaster from happening to you or your company. Depending on the size of your company, you may implement only some of these measures. The worst mistake you can make, however, is to dismiss this discussion altogether. Proper planning will not only protect your company but will also help you sleep better at night.

KEEPING YOUR COMPANY RUNNING

According to the American Red Cross, 40 percent of small businesses that suffer a disaster won’t reopen for business, and 29 percent of small businesses that do reopen close within two years. (See “Business and Industry Guide” at www.redcross.org/services/disaster/beprepared.) Whether you use the term *disaster recovery planning* or *business continuity planning*, there has been no better time to start implementing solutions to keep your company functioning during a disaster. Floods may happen only once a century, but computer hackers can destroy your business at any moment—and try to destroy businesses as often as they can.

In disaster recovery planning, you may be tempted to focus only on server hardware, backup tapes, and redundant cabling. You may even pay a consulting firm to store spare systems. These steps are important to any disaster recovery plan, but you need to do much more.

When you evaluate why companies fail after a disaster, it's generally because they can't quickly relocate equipment, employees, and, in some cases, employees' families. For example, what happens if no one is available to run your redundant systems? Keeping employees educated and cross-trained is important. Management often ignores cross-training because it appears unproductive.

Of course, this belief is absurdly short-sighted. As you know only too well, network administrators are often asked to install and maintain systems but don't have adequate training to perform these tasks. Having a well-trained staff is advantageous to both employees and managers. Employees have better morale when they get training on a regular basis. If a key employee is sick or on vacation, procedures don't have to wait until that employee returns.

Disasters can occur if key employees are lost. Each year, Novell receives many support calls because an employee left a company on bad terms and no one else knows the password to the Novell eDirectory administrator account. In the World Trade Center attacks, some companies lost 100 percent of their Information Services (IS) employees. Many of these companies may never recover.

Even if all of the key employees are still working for the company and are still available, the systems themselves may be inaccessible. Buildings can be quarantined or inaccessible for various reasons, so you must plan for such situations. Analysts call this the "snowstorm" scenario, but you could update it to include anthrax scares.

In case a disaster happens to your company, you need alternate routes to link your company's network to the outside world. Severed links and down backbones can take hours or days to fix.

You also need to plan how users and network administrators will access the network from a remote location. Your plans should include a quick setup of wireless environments in remote offices. You should ensure that the IS staff understands how to configure the wireless systems and to connect them to a LAN.

You may also want to create a portal solution for your company. Portal solutions help employees access information even if some systems have been subjected to a nasty virus. A well-designed portal system has alternative entry

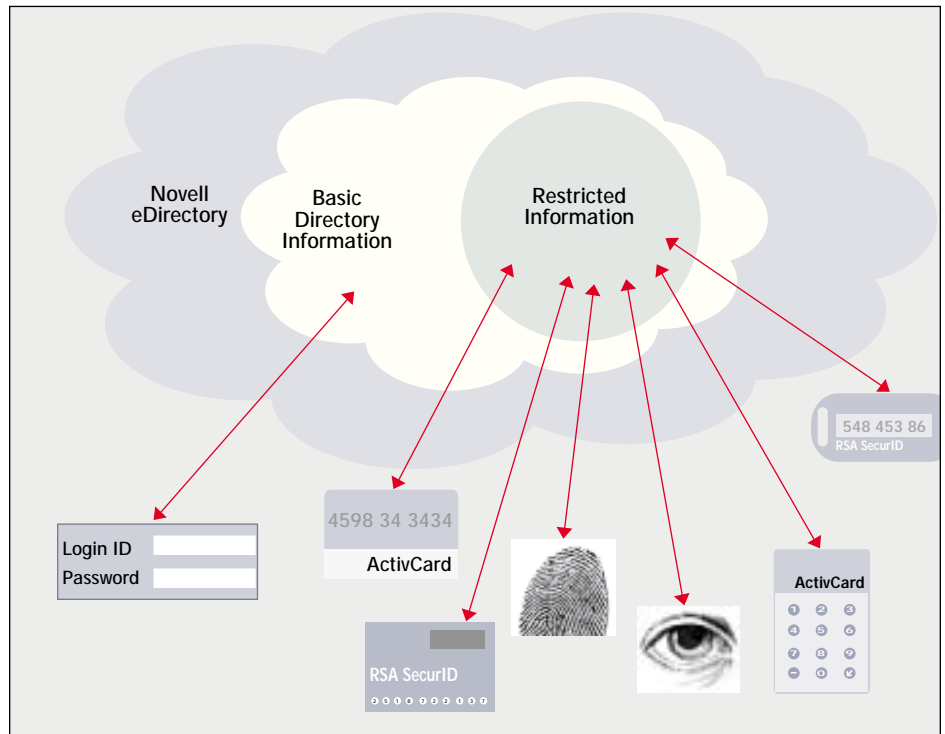


Figure 1. With Novell Modular Authentication Service (NMAS), you can require multi-factor authentication before users are allowed to access restricted information.

points for users to access. For example, suppose your company's data center in London hosted services for European employees. If something happened to those routers or servers, your Internet Service Provider (ISP) could route all requests to a backup site in Milan. Of course, employees would not even know a problem had occurred.

If air travel were suspended as it was in the United States last September, how long would it take to restart your company if the main office became incapacitated? To provide this capability, you may want to consider retaining a consulting firm near your backup data center.

Are any of your company's offices at particular risk from terrorists? Many large companies have increased security at some offices. You should ensure that your disaster recovery plans include these offices that are at increased risk.

You should also educate all department managers so they know what to expect during a catastrophe. Some department managers may think your suggestions are overkill, so be ready to supply cost estimates of implementing a disaster recovery plan versus having the company shut down for a period of time.

And don't forget to evaluate time-critical tasks, such as payroll, and ensure

Visit our advertiser,
Beginfinite, at
www.beginfinite.com.

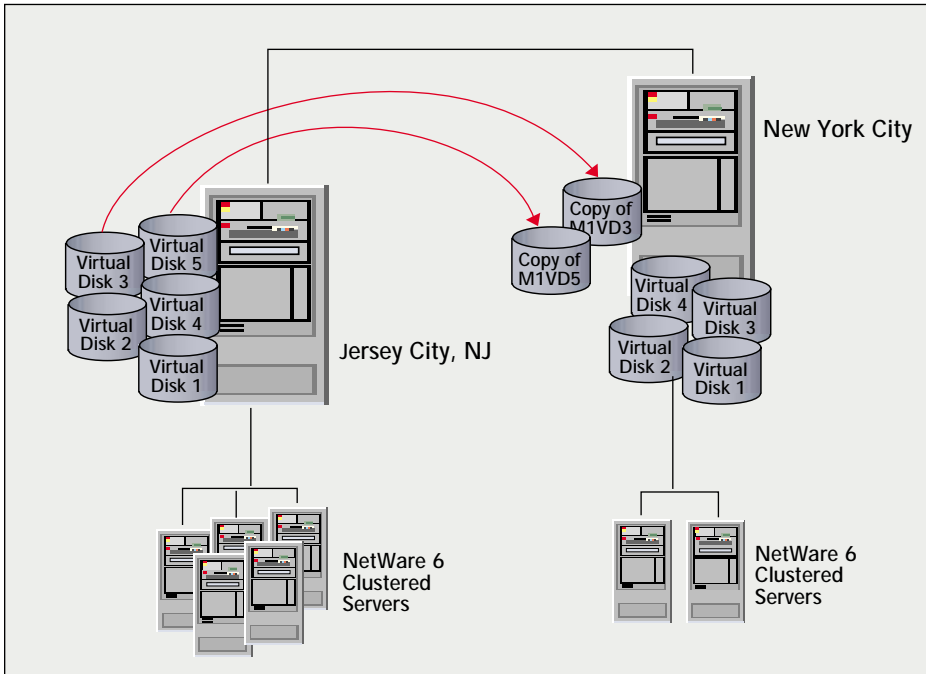


Figure 2. With Novell Cluster Services, you can provide failover protection and redundancy over long distances. For example, servers in New York City can provide services if servers in Jersey City fail for any reason.

that the services required to complete these tasks are available even if the primary systems are destroyed. For example, if your company uses an electronic system for time cards, you may want to suggest a manual process that will be used if a disaster occurs.

In the event of a disaster, it is imperative that the business has 24 x 7 guaranteed access to the records. Consider storing printed reports at an alternate location. Off-line data storage companies offer such facilities.

Is your documentation current? Although writing procedures and guidelines isn't glamorous (in fact, it's hard work), such documentation is essential when disaster hits. As an IS professional, you may sometimes forget that although information is available at your fingertips, finding and correlating that information may not be easy. Installations and configurations differ from system to system, and too many times the tips and tricks you discover through trial and error are lost because they aren't recorded.

You may want to hire a temporary employee to document all of the systems on your company's network. Although most managers think in terms of immediate profits, this task is a wise investment for the future.

Tips

The following are some general tips for keeping your company running after a disaster occurs:

- Create a duplicate hardware and software environment away from the main office.
- For smaller companies, create a backup environment in someone's home (such as the owner's or a trusted employee's home). Make sure that passwords are recorded, stored in a secure place, and tested periodically. You should also ensure that the backup system is physically secured and protected.
- Cross-train employees on key systems.
- Document procedures for key systems, including any tricks that you have learned.
- Outsource some services, especially web-based applications.
- Periodically update software and hardware in backup environments, and test these systems by simulating a disaster.
- If budgets allow, have a wireless system available to provide in-house communications.

SERVER BACKUP AND RESTORE

My cousin owns a small accounting firm near Wall Street. His office, which is just two blocks from the World Trade

Center, was closed for nearly three weeks after the attacks on September 11. The most important thing for my cousin was to keep his business alive during those troubled weeks. Before that time, the words *disaster recovery* and *redundancy* had never entered his mind, other than performing periodic tape backups and duplexing the disks on his NetWare server.

Fortunately, my cousin was able to perform a final backup of his NetWare 5.1 server while other people were evacuating the area on September 11. By the time my cousin left his office, it was five hours after the attacks. He drove home, called Hewlett-Packard (HP), and requested a replacement server to set up in his house.

Three days later the server arrived, but the new tape unit was incompatible with his backup tapes. My cousin then ordered a new tape drive. On Monday, one week after the attacks, he assembled the server. To restore the tape, however, he had to install NetWare. And where was his license disk? You guessed it—in his office.

I sent my cousin a demo CD, which contained a three-user license of NetWare 5.1. He restored the image in 15 minutes and then tried to restore the backup tape. However, he needed new LAN, disk, and tape drivers. After installing these new drivers, he was finally able to get his server running.

As this example demonstrates, creating a fully redundant environment isn't easy if you don't plan ahead. Part of this planning must be keeping current hardware and software.

I've been working in the computing industry a long time. The phrase *network backup* is as misused as the phrase *government surplus*. Let's face it: Backup is boring. Ever look at your tape backup logs? Probably only if a sleeping pill doesn't work.

The true test is when the epinephrine gets pumped into your arteries if you actually need to restore data. If any part of the restore process fails, you better be ready for some managerial yelling.

Spare yourself the anxiety. Once a week, restore your company's data onto a similar system. Time how long a complete restore takes, and check the contents—especially infrastructure components such as eDirectory, digital certificates, and hardware-specific configurations (such as IP addresses and LAN drivers).

A quick way to restore a basic server is to use imaging software, such as DeployCenter (formerly known as Drive Image Pro) from PowerQuest (www.powerquest.com). DeployCenter is not only useful for new server deployments but also for emergency server installations. You can also use Storage Manager from Portlock Software (www.portlocksoftware.com).

The trick is to create a generic server with all possible drivers on the disk and then save the image to CD or DVD. You can then keep the CD or DVD with your tape backups off site.

PowerQuest also offers ServerMagic for NetWare, which allows you to copy complete volumes and partitions from one system to another across the wire. You may already be using ServerMagic to move data to new servers.

ServerMagic can also help with disaster recovery plans. For example, you can use ServerMagic to periodically duplicate volumes from primary to secondary systems. To do this, you must down the server. However, this procedure virtually guarantees that data are consistent between systems.

On systems with hot-swappable drives, you may want to consider periodically removing the mirrored drives and storing them off site. After you install the mirrored drive in the off-site backup server, restoring data from tape or disk is faster because there are less data to transfer. This solution is adequate for small environments, but impractical for larger ones because there are too many drives to remove.

Although creating redundant systems is necessary, they also increase your company's vulnerability. That is, if your backup tapes or systems are hacked or stolen, all of your company's information may be exposed. It's important to password-protect the backup servers and tapes and to ensure that they are stored in a safe and protected environment.

You should keep important notes, keys, and passwords locked in a safe at both the primary and secondary locations. Even the best backups in the world won't help your company get back on its feet if the backup tape password isn't known or if the server can't be powered on.

You may want to consider implementing other authentication methods for key systems such as eDirectory. If you use Novell Modular Authentication Service

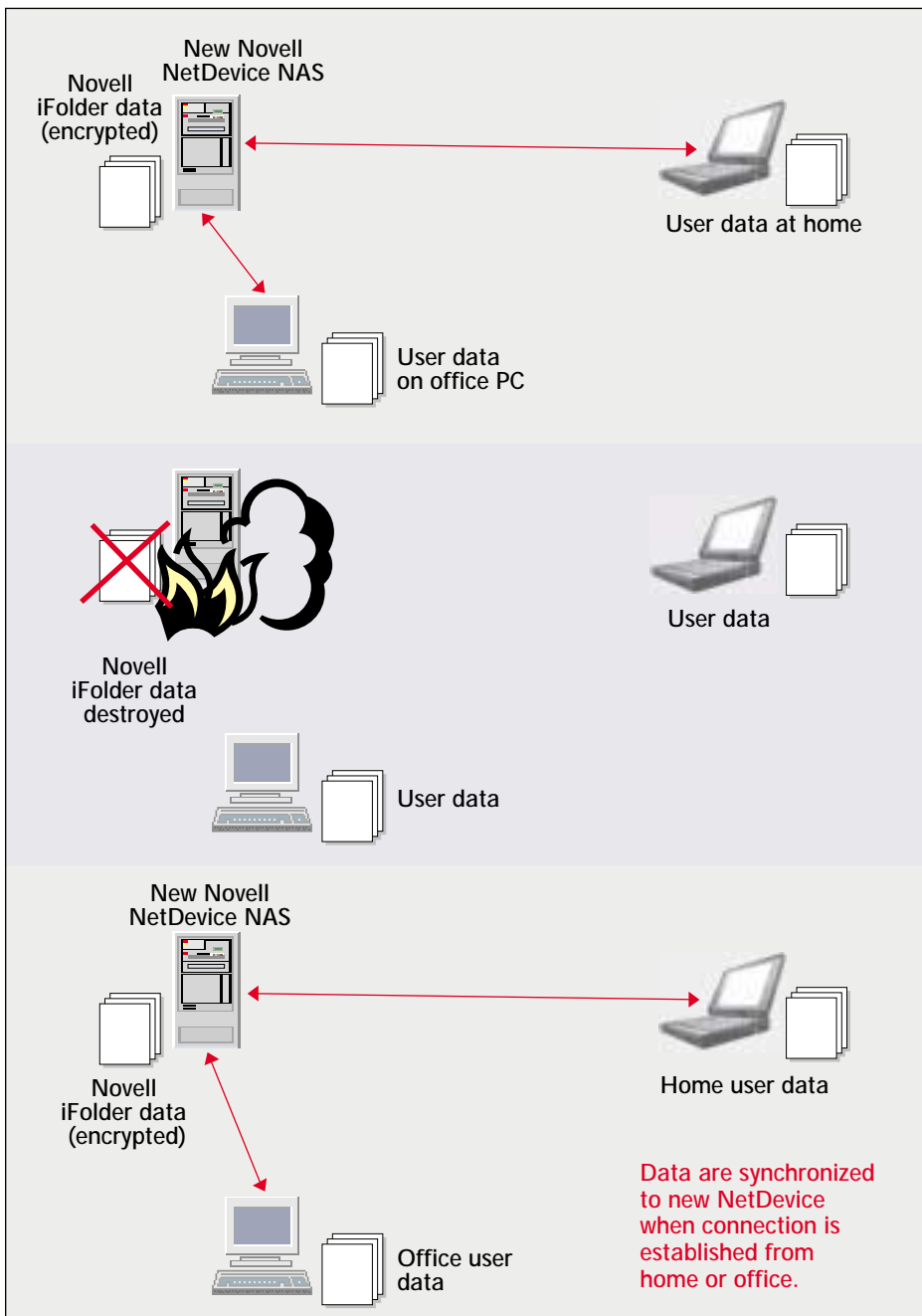


Figure 3. The branch office of this fictitious company uses Novell iFolder and Novell NetDevice NAS to store data. If the NetDevice is destroyed, the employees' data are not lost because iFolder synchronizes data between workstations and the iFolder server. When the company installs a new NetDevice with iFolder, that data are still available on laptops and are synchronized to the new NetDevice.

(NMAAS), users can use tokens, biometric devices, or smart cards to access their accounts. (See Figure 1 on p. 27.) You can even require two authentication methods, such as a fingerprint (biometric) and a smart card. (For more information about NMAAS and the third-party products that work with NMAAS, visit www.novell.com/products/nmas.)

Tips

The following are some tips for backing up servers:

- Test the backup system by periodically restoring data.
- Create basic server images on a bootable CD or DVD that is ready to install.

Olympic Security

What does Olympic security have in common with network security? As a volunteer for the 2002 Olympics in Salt Lake City, I had a lot of time to think about the similarities. I drove athletes from the Olympic Village, where the athletes stayed, to various Olympic venues. (See Figure 5 on p. 31.) As you probably know, security for the Olympics was the tightest ever. But how can anyone, even the U.S. government, protect 900 square miles, a dozen venues, and mountains that peak at 12,000 feet? Given enough money and resources, it's possible to keep the bad guys away.

Security plans for the Salt Lake Olympic games were being devised four years before September 11, 2001. After that disaster, however, the U.S. Secret Service took over the operations. More than 10,000 law enforcement and military personnel were placed in the Salt Lake area. An additional 5,000 people had security responsibilities. That means the ratio of security personnel to athletes was 5 to 1.

The upside to all of this is that the Olympics were safe—although some people groused at the inconvenience that safety caused. Spectators were advised to arrive three hours before an event began. Twice I waited an hour to enter a venue. In comparison, when I attended the 1984 Olympics in Los Angeles, I walked into venues without a hitch. However, the world is different today, and delays to enter public arenas will be commonplace.

Some of the details provided here were confidential before the Olympics. Each Olympic driver was given a handbook of driving routes to venues scattered across the Salt Lake region. Each primary route had a secondary and tertiary route. For security reasons, drivers were asked not to show the handbook to anyone, including family.

In the Village, where each route originated, I saw more police, Secret Service agents, and FBI agents than athletes. The challenge was to drive a secure vehicle from the 70-acre Village to

any Olympic venue in a 50-mile radius. The task is really just like moving secure data from a data center over the Internet to a workstation somewhere in the world. At the Olympics, however, the "data" (3,500 athletes, officials, and coaches) were watched as they moved from place to place.

The Olympics had two types of security zones. The "soft" zone allowed only certain accredited vehicles and persons to enter, but there was no rigid screening if the vehicle came from a secure area. In this case, military personnel performed a level 3 inspection. They examined all parts of the vehicle. Authorized vehicles had a placard; authorized persons displayed an ID badge.

If someone entered the vehicle en route or if the vehicle didn't arrive from a secure location, military personnel performed a level 1 inspection: Each passenger and all contents of the vehicle were screened.

All fences surrounding the soft zone were armed with sensors and cement bases, and police were stationed so that no part of the fence was unseen by human eyes. In addition, cameras were mounted on light posts. To reach the high security, or "hard," zone, all persons went through metal detectors, had their badges electronically verified, and their bags x-rayed.

The hard zone was also fenced, which created a kind of DMZ. Anyone or anything between the soft and hard zones was called *dirty*.

The Village was a hard zone. Even athletes, their bags, and their equipment were inspected. Everyone in the Village was required to display an ID at all times. Any miscellaneous items entering the hard zone were examined in the materials transfer area (MTA). This was a "guarded" zone—a place for items to be held before entering a soft or hard zone. The challenge came when the biathlon athletes brought their guns to the village; military personnel developed a special procedure to move the guns to an armory for safekeeping.

Is your data center this secure?

continued on page 31

- Store keys and passwords in a safe place.

REAL-TIME RECOVERY

Over the past 30 years, the computing architecture has undergone several evolutions: The 1970's computing model was centralized with a few large systems serving many terminals. In the 1980s and early 90s, the computing model changed: Data were distributed across many inexpensive servers. Because servers became capable of serving so many clients, the computing model was centralized again in the late 90s.

This computing architecture is now adapted to the Internet. Today's web applications can leverage both the client and server, depending on which is more practical.

After September 11, however, we need to carefully evaluate which

services should be run on standalone computers and which should be provided by centralized systems. Certainly, it's hard to ignore the fact that today's PCs have more memory, storage, and processing power than servers had just five years ago. And with the Internet Printing Protocol (IPP), printing isn't even tied to servers. Why shouldn't users do all their work on an inexpensive PC and use a server only for e-mail? Having servers run only basic services is efficient.

The key point to remember is that the role of servers has changed. Servers are not so much about file and print as they are about providing web-based services that gather data from other systems.

As you make disaster recovery plans for your company, you should factor in each server's role in providing services to

users. For example, if a portal server goes down, users can't access e-mail, databases, reports, or other information. When you positively cannot face any downtime, you must create real-time failover systems.

Novell Cluster Services (www.novell.com/products/clusters/ncs) provides failover services for up to 32 systems. If a server crashes, the client will access services on another server. During the switchover, the user is unaware that any problem has occurred. Clustering allows you to create a scalable and redundant network environment.

With Novell Cluster Services, the servers in a cluster can be located many miles away, depending upon the hardware used. (The latest fibre and repeaters provide high-speed data services among systems.) If those servers handle web-based applications, you can provide

continued from page 30

Initially, each vehicle was swept for explosives. Once cleared, the vehicle was inspected before being allowed into a soft zone.

All persons—including volunteers, police officers, athletes, and coaches—had background checks. Work schedules and IDs were coordinated with a PC-based system and handheld badge scanners. Each badge had an entry code for specific venues. For example, if I tried to enter the ice arena to see a hockey game, I'd be refused. I had to pay the high price of admission like all of the other spectators.

All drivers followed the same procedure when driving athlete van shuttles. Each driver inspected the vehicle for possible problems, including mechanical problems. Having a breakdown was a security risk.

Each driver was given a two-way radio and cell phone. If a problem occurred, we could use either the radio or the cell phone to signal for help. We could also push a panic button.

Police cars and unmarked Secret Service vehicles were stationed along driving routes, and each van had a homing device that allowed the Secret Service to monitor its position and speed. We were told that police response would be swift. If a van was caught off route, the driver was called. If the driver used a special panic word, it signified trouble.



Figure 5. The layout of the Olympic Village and other venues

Was all of this security overkill? Remember rule 1: Security is never 100 percent. Stuff happens, as they say in Utah, and no one wanted a repeat of the tragedies of September 11. As the Secret Service agent in charge of Olympic security said, "There is always something new . . . to examine. We try to look at every possible scenario and learn something from it." (*Salt Lake Tribune*, Jan. 30, 2002.)

Once at the venue, vans entered the soft zone. Military personnel used mirrors to look under and over the vehicle. After the engine and gas tanks were inspected, drivers could drop off the athletes. On the return trip, the security steps happened all over again at the Village.

When you think about this process, it is just like using Secure Socket Layers (SSL) in a browser to access secure data over the insecure Internet. There are at least two exceptions, of course: In the electronic world, we don't care if someone intercepts the data because it's encrypted. When driving athletes along Utah's roadways, we did care if a vehicle is intercepted.

Although Internet users don't track each packet's route, the Olympic security team did indeed care what route its vehicles took. No van was allowed to make unnecessary stops, even if a passenger had a "mother nature" call. This rule prevented something unsecure from being placed inside the van.

While driving some athletes to Deer Valley, I made a wrong turn. In less than two minutes, I received a phone call, asking me if there was a problem. Not wanting anxious-looking police officers hunting me down, I quickly got back on course.

Another driver decided to stop at Burger King for lunch. Within minutes, the Secret Service surrounded him.

With all of the money spent on the Olympics, could someone have circumvented security? Let's just say it might have been possible—with a little charm. (I plead the Fifth.) In the end, no matter how much money is used to secure something, nothing beats the system like charm—a fact you may want to impress upon your company's users.

One point I must mention: the military and law enforcement people at the Olympics were top-notch professionals. They were always courteous and performed their often-mundane tasks with enthusiasm. How would you like to work the graveyard shift patrolling a chain-linked fence in the 15-degree February cold? Or slide yourself under countless vans and trucks to inspect their gas tanks? These hard-working people deserve much credit for keeping the Olympics safe. ●

highly reliable web services. (See Figure 2 on p. 28.)

Both NetWare 6 and NetWare 5.1 support Novell Cluster Services. In fact, NetWare 6 (www.novell.com/products/netware) includes a four-node license of Novell Cluster Services.

Creating data redundancy with Storage Area Networks (SANs) is another way to protect data during disasters. Vendors such as IBM, Compaq, EMC, and HP offer solutions that manage terabytes of data. With SANs, many servers attach to many disks, and the

cluster of disks creates a unified way to manage data. If data access is interrupted, communication can be transferred via an alternate path. Ideally, that path can be outside of the data center at an alternate site.

Most SAN vendors use Fibre Channel for their SAN solutions. Fibre Channel provides data rates of 100 Mbps or more and supports several topologies, including point-to-point, token ring-like loops, and Ethernet-like packet switching. Although SANs can run over copper, copper has a 30-meter maximum

cable length. With fiber optic, distances of 10 km or more are possible.

For example, the EMC Clarion Storage System (www.emc.com) supports 7.3 TB of storage with data transfer rates of 1 Gbps. This system uses fully redundant power supply, drives, storage processors, and fans. XIOTech (www.xiotech.com) offers mirrored storage solutions that, when combined with third-party fibre channel extenders, allow connections up to 120 km.

Novell's Guide to Storage Area Networks and NetWare Cluster Services is

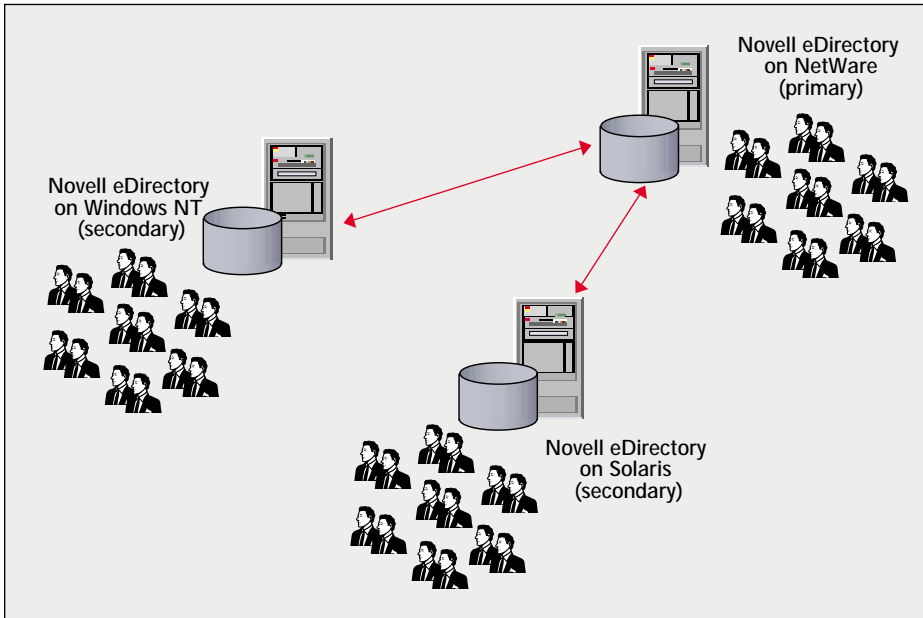


Figure 4. You can use Novell DirXML to synchronize the data between two Novell eDirectory trees, thereby providing a backup of the information in each tree.

a great resource for using SANs in a Novell environment. In this book, authors Stephen C. Payne and Robert Wipfel take you through all the steps of designing and implementing SANs and clusters. (To find the latest SAN solutions that work with NetWare, visit <http://developer.novell.com/yespgm>.)

Novell NetDevice NAS (www.novell.com/products/netdevice) is a departmental network attached storage (NAS) product. Using NetDevice, you can essentially turn any computer into a NAS device. Combined with Novell Native File Access Pack (www.novell.com/products/nfa), NetDevice provides seamless access to Macintosh, Windows, and UNIX clients. (Novell Native File Access Pack allows users to access files on servers or a NetDevice without having to run Novell or third-party client software. For more information, see "Native File Access Wanted: Client Software Need Not Apply," *Novell Connection*, Nov. 2001, pp. 6–26. You can download this article from www.ncmag.com/past.)

What does a NAS device have to do with disaster situations? Suppose that a small sales office in the Bahamas (the office that you never get to visit) was using Novell NetDevice NAS and Novell iFolder (www.novell.com/products/ifolder) to back up data. (See Figure 3 on p. 29.) When users worked on their laptop, office workstation, or

home workstation, iFolder automatically synchronized that data with the data stored on the NetDevice.

Now suppose that NetDevice was destroyed by fire. With relative ease, you can send the sales office a new NetDevice and have a storage system up and running minutes after it is powered on. Because users' data are merely replicated to the NetDevice, the synchronization process begins once users log in to iFolder. Data from users' local drives are encrypted and stored on the NetDevice. (See Figure 3 on p. 29.)

Hierarchical storage is another option for more efficient data backup. Hierarchical storage segments data into active and historical data. (As the name suggests, historical data have not been accessed recently.) Historical data are moved to off-line storage devices, resulting in improved storage management and lower hardware costs. For example, CaminoSoft StorageServer HSM (www.camino.com) archives data on NetWare servers to off-line storage.

Another CaminoSoft product, Managed Server HSM, moves little-used data to central NetWare servers, which act as NAS devices. CaminoSoft estimates that about 10 percent of all server data is used on a daily basis. That means 90 percent of data simply sits, consuming valuable storage space. Using the rules that you define, Managed Server HSM moves the data to less expensive storage

devices. These two solutions provide good ways to archive historical data, and to offload little-used data such as Group-Wise mailboxes. (For more information, visit www.camino.com/cs.faq.main.html.)

Other clever backup solutions on the market can save your company time and money. For example, FDR/Upstream from Data Processing (www.innovationdp.fdr.com) moves data from NetWare servers to MVS mainframes.

The older-than-dirt approach to data redundancy is disk mirroring and duplexing. These features have been a part of NetWare since version 2.x. Although mirroring and duplexing require twice the storage to achieve redundancy, they provide onsite redundancy and protection against disk failure.

Mirroring and duplexing also allow whole chunks of data to be moved to an alternate site. How? As mentioned earlier, you can remove a mirrored disk and replace it with a new disk. You need experience and expertise to attempt this task, although it is easier if the server has hot-swappable disks. After the mirror link is broken, you can remove the mirrored (secondary) disk. You then insert a new disk, and the mirror link is reestablished. (Incidentally, I often recommend this technique when upgrading the network operating system, since a full backup of the original disk is always available.)

Another approach to data redundancy is Redundant Array of Independent Disks (RAID), which spreads data across several disks for better speed and reliability.

What about using directory-based policies to distribute data to servers? Rick Cox wrote an excellent article, "ZENworks for Servers 2: Consolidating Data From Many Servers to One," which explains how you can use ZENworks for Servers 2 (www.novell.com/products/zenworks) to move data among servers. (See *Novell Connection*, July 2001, pp. 30–34. You can download this article from www.ncmag.com/past.)

If something does happen to your primary systems or if your Internet links are unavailable, it's a good idea to have a communication backup plan. Then if a problem occurs, your company's ISP can simply advertise your domain names with different IP addresses, and customers will be automatically redirected

to the alternate site. In addition, you should give users instructions on how to connect to alternate Virtual Private Network (VPN) servers or other internal devices.

Because eDirectory controls most aspects of the Novell environment, you absolutely must back it up. There are many approaches to backing up eDirectory. For example, besides the obvious tape backup, you should always have at least three copies of a replica ring. That means at least three servers contain the same information; one holds the master replica, the other two hold read-write replicas. (See Blair Thomas and Jeffrey Hughes, *Four Principles of NDS Design* [Novell Press], 1996, p. 135.)

There is a new method to backup eDirectory in real time. Version 8.6.1 and above include a live continuous backup feature that uses Novell DirXML technology. (For more information about DirXML, visit www.novell.com/products/edirectory/dirxml.) This feature synchronizes eDirectory data between two or more directories, even if the operating systems are different. That means all directory objects and attributes on a UNIX host can be sent to a NetWare server, making the two trees appear identical. (See Figure 4.) eDirectory 8.6.1 also includes enhanced scalability and reliability.

Tips

The following are tips for real-time recovery:

- If uptime is critical, implement a cluster of servers.
- If uptime is critical, implement SANs, with data duplicated at primary and alternate sites.
- For small offices, prepare a NAS device that's ready to roll out on a moment's notice.
- Use hierarchical storage management products to efficiently manage your company's data.
- Use disk mirroring, disk duplexing, or RAID systems for basic data redundancy.
- Consult with your ISP to establish failover communication links.
- Use Novell DirXML to synchronize eDirectory objects and attributes between two or more eDirectory trees.

PROTECTING THE WORKSTATIONS

As mentioned earlier, disasters come in all sizes. Having an enterprise server explode because someone's coffee spilled into the power supply is a big disaster. Having a laptop stolen seems minor but can be a major catastrophe to the user or even to the company, depending on what data is stored on that laptop and when the laptop was last backed up.

You can quickly restore a new workstation in at least two ways: You can use a disk image application, such as PowerQuest DeployCenter or Symantec Ghost, to make a disk image. With this approach, the biggest hurdle to overcome is making sure that the image will work on the new workstation. Although Windows has gotten better at recognizing new hardware, it's not a foregone conclusion that an image created on one workstation will work on another. Creating corporate standards for hardware and software purchases can alleviate this problem. Microsoft also provides some tools to help configure imaged systems.

You can also use ZENworks for Desktops' Preboot Services, which rely on directory-based policies to define how new workstations should be configured. After identifying a new workstation, ZENworks for Desktops (www.novell.com/products/zenworks) uses this policy to copy a predefined image to the workstation and to install new applications and policies. ZENworks for Desktops can also enable virus checking and backup services on workstations.

Few people back up their personal systems, even if company policy dictates it. Fewer users are also storing data on servers because their local drives have so much free storage. So what's the answer?

Novell iFolder gives users the best of both worlds. Data is stored locally and on a server. The transmission is via HTTP over IP, so data is sent to a network drive from any location. Because all information is encrypted when sent and stored, prying eyes can't view that information. Even network administrators cannot view iFolder information.

When users see the value of iFolder, they'll want to use it. Data is accessible from any browser and can be synchronized to multiple computers. For example, if I modify a document in my office, that document is available on my home PC

when I connect to the Internet.

You can use ZENworks for Desktops to create a workstation policy that ensures Novell iFolder is installed on each user's workstation. You can further configure iFolder so that any data stored in the My Documents directory is automatically replicated to a server. This makes iFolder seamless to users.

How important is printing to your company? With Novell iPrint (www.novell.com/products/netware/printing), printing is as easy as clicking a picture in a browser window. If a printer is unavailable or a whole office needs to be relocated due to a disaster, users can easily select a new printer by IP address, by Domain Naming System (DNS) name, or from a map. (Novell iPrint is included with NetWare 6 and is available for NetWare 5.1.)

Finally, you should make sure that you have a central web site for users to download the latest software. For example, Novell used Novell Portal Services to create a site called *Desktop Depot*. Users access this site to download the

Visit our advertiser,
Wired Red, at
www.wiredred.com.

Visit our advertiser, Novell
eDirectory, at
www.novell.com/edirectory.

Visit our advertiser, Novell
eDirectory, at
www.novell.com/edirectory.

The Personal Side of Disasters

While you are making plans to protect your company in the event of a disaster, you may want to make similar plans to protect your personal life. For example, what items do you want to protect in case of tragedy? What passwords unlock the systems that protect your valuables?

My most prized possessions are my photographs. In the past three years, I've accumulated more digital images than film images. However, I still have quite a collection of film-based photographs.

Although I used to store negatives for these photographs in a fireproof safe, I discovered, after talking to a fireman, that these safes are "hot spots" during a fire. When putting out a fire, firemen attack such hot spots with water, foam, and axes. Although a fireproof safe is built to withstand fire, it may not be equipped to resist water, foam, and axes. You may want to think twice about using a fireproof safe to store critical documents.

A better alternative is to copy all documents and photographs and then send these copies to friends or relatives for safekeeping. You may even want to take the electronic approach: Scan those items and store the images on a CD or DVD.

If you want to password-protect these items, make sure that others outside of your immediate family know your password. Write down common passwords to online banking systems or

encrypted documents. Seal the paper in an envelope, and give it to a close relative or friend.

Here is my approach to backing up all of my data, including photographs.

I have a NetWare 5.1 server with three disks: 18 GB, 40 GB, and 80 GB. To provide redundancy, I mirror the 18 and 40 disks to the 80 GB disk. Periodically, I use Windows briefcase to back up data from my laptop. This way, only changed files are copied. (If you are using only Windows computers, you can use Novell iFolder to back up your data. iFolder synchronizes data between your workstations and the iFolder server.)

I have divided my data into three parts: corporate (corp), personal data (data), and photos. I do three individual syncs to the briefcases. I could have combined all the data into one briefcase, but I have an awful lot of data. On occasion, Windows cannot open the briefcase, so I must manually copy over all the files.

I have a copy of the data on my laptop, on the primary server disk, and the mirrored disk. I then use a Macintosh computer that has a Superdrive to burn several DVDs (4.3 GB). I give the DVDs to my friend in Los Angeles.

I'm still working on scanning all of my photos. It's a Herculean task. I'm also scanning my tax returns and other documents. One thing is clear: I need a long vacation to duplicate all of my stuff. ●

latest corporate applications. If a disaster occurs, employees can use this web site to quickly set up new workstations.

Tips

The following are tips for protecting workstations:

- Create images of workstations so that new machines can easily be configured.
- Use ZENworks imaging for policy-based configuration of new machines.
- Use iFolder to backup user's files.
- Use iPrint for printer redundancy.
- Create a living document and download site for users to get the latest software. Make sure the site is redundant.

CONCLUSION

According to a report by David Smith, assistant professor of Economics at Pepperdine University, 4.6 million incidents of lost data occur each year. The average cost of each incident is about U.S. \$2,500. Much of that amount represents the data itself, not the downtime. ("The Cost of Lost Data," Sept. 1999. You can download this report from <http://portal1.legato.com/resources/whitepapers/W052.pdf>.)

The hourly cost of downtime is significant, reaching millions of dollars per hour for some industries. (See "Data Recovery Center" at www.ontrack.com/datarecovery/cost.asp.) In addition, a various surveys show hundreds of thousands of attacks on organizations.

If you want to protect your company but don't have enough personnel to create a disaster recovery plan, many Novell consulting partners specialize in security and business continuity planning. To locate these partners, visit www.novell.com/consulting. Many managed security firms also provide outsourced mission-critical services. To locate these firms, and enter MSSP in an Internet search engine.

If you think your company will never experience a disaster, then please call this number: 1-555-GET-REAL. Seriously, we all purchase health, car, and home insurance to protect us from the unknown. Insurance companies know that, in due course, something will happen to our property or to us. They know the odds and charge us accordingly.

You should also ask who's guarding the guards. Because your company's network is an invaluable asset, the people running that network have a lot

of power to help or harm your company. For example, Timothy Lloyd was sent to prison for nearly 3 1/2 years and ordered to pay U.S. \$2 million in restitution for planting a time bomb that destroyed the manufacturing software developed by his employer. (See "Net Saboteur Faces 41 Months," *NetworkWorld Fusion*, Mar. 4, 2002. You can download this article from www.nwfusion.com/news/2002/0304lloyd.html.)

What happens if a bad apple spoils your data systems? You should set up a system of checks and balances to ensure that your company's network is protected from an errant employee.

In some cases, recovering from a disaster will take some time. In other cases, the disaster could cause so much loss that the company has to start from scratch. In any case, having a disaster recovery plan will ease the pain in the event of a tragedy. The rewards of your planning won't be evident until a disaster actually strikes. Before and after a disaster occurs, it's your role as a network administrator to ensure that recovery process is a smooth as possible.

Alan Mark is the chief security strategist for Novell. He has worked at the company for 11 years and frequently speaks to large organizations around the globe. ●