



BUSINESS CONTINUITY

USING NETWARE 6.5 TO DEVELOP A SOUND BUSINESS CONTINUITY SOLUTION

BY PETER CLEGG

It gnaws at you constantly. That uncomfortable feeling that you're hangin' out—exposed—vulnerable, and lucky to have survived another day without some executive asking, “So how safe is our IT network if we were to experience a natural disaster or the side effects of terrorist violence?” If you're feeling unprotected, you're not alone. A recent Gartner survey of 205 companies showed that one-third were at risk of losing capital data or operational capabilities in a terrorist attack. Business continuity has become a top-level priority for chief information officers and according to Business Week, “most companies are still unprepared for the worst” (*“The Business-Continuity Imperative,” Business Week, May 13, 2003*).

If the distance between just keeping your network operational and a fully redundant, automatic failover, multiple site-protection strategy seems as vast as the Sahara, take heart! The business continuity technologies included with NetWare 6.5 provide you the tools necessary to create a state-of-the-art, disaster-resistant network that will ensure IT availability and business viability in the event of an unplanned emergency or disaster. The great news is that all of this capability comes at very little incremental cost in the way of equipment, software or training. You too can have redundant sources of data, automatic failover systems, distributed geo-site coverage and continuous network access from remote locations—all with just what's included in the NetWare 6.5 box. In this article, we'll roll up our sleeves, open the box and see just what's available to help you be prepared for the worst.

BUSINESS CONTINUITY — WHAT IS IT?

What is business continuity? It's whatever it takes to ensure that your business can survive through any type of disruption including—but not limited to—categories of natural disasters, hardware and communication failures, internal or external sabotage, acts of terrorism or the failures of supply chain and sales affiliate organizations. Although what might be required for a good business continuity solution varies from company to company, it basically boils down to ensuring that whatever your organization needs to avoid capital loss is in place.

You can implement business continuity at any one of several levels depending on the needs of your organization. Let's look at three general types of protection that are most likely required for any company: data access and recovery, organization intelligence and business operation tools. NetWare 6.5 includes solutions for each category.

DATA ACCESS AND RECOVERY

Data is the lifeblood of many organizations. It may consist of database files, documents, correspondence, transaction records, history or Web content. It may be located in any number

of locations including central IT facilities, remote or branch offices, personal workstations or mobile notebook computers, and even at service provider or business affiliate sites. Your job is to make sure there are multiple copies (data is redundant) and that it is accessible through multiple access channels. NetWare 6.5 includes several data-access and recovery solutions to help you build protection. Starting with a central IT facility, data redundancy can be created through the use of iSCSI SANs, clustering and Snapshot Backup.

iSCSI SANs—storage area networks (SANs) let you pull data which may exist on several servers in several locations to a central virtual point for management. iSCSI is an emerging standard for SCSI block storage protocols networked over high-speed TCP/IP networks. Commodity Ethernet hardware is used with standard interoperability between SCSI storage servers or targets. This iSCSI support enables you to deploy a SAN for up to one tenth the cost of Fibre Channel. SANs can be centralized, distributed over multiple

geographical locations or configured as distributed mirrors so that one SAN continues in the event of failure of the other.

Implementing a NetWare iSCSI solution is simple. Initiator software is installed and configured on servers in the SAN that will be used to access shared storage (initiators can be individual or cluster servers). Initiators use the iSCSI protocol to communicate with an iSCSI storage or target server over a TCP/IP network. Target software is installed on a NetWare server and provides access to shared disks through the iSCSI protocol. iSCSI target software enables the target server to function as a disk controller for the shared disk system.

iSCSI SANs ensure data access and recovery in three ways. First, SANs allow you to consolidate data from multiple locations to a central location, which eliminates multiple points of failure. There's no running from server to server to make sure there are current backups. Second, centralized (or virtually centralized) data simplifies storage

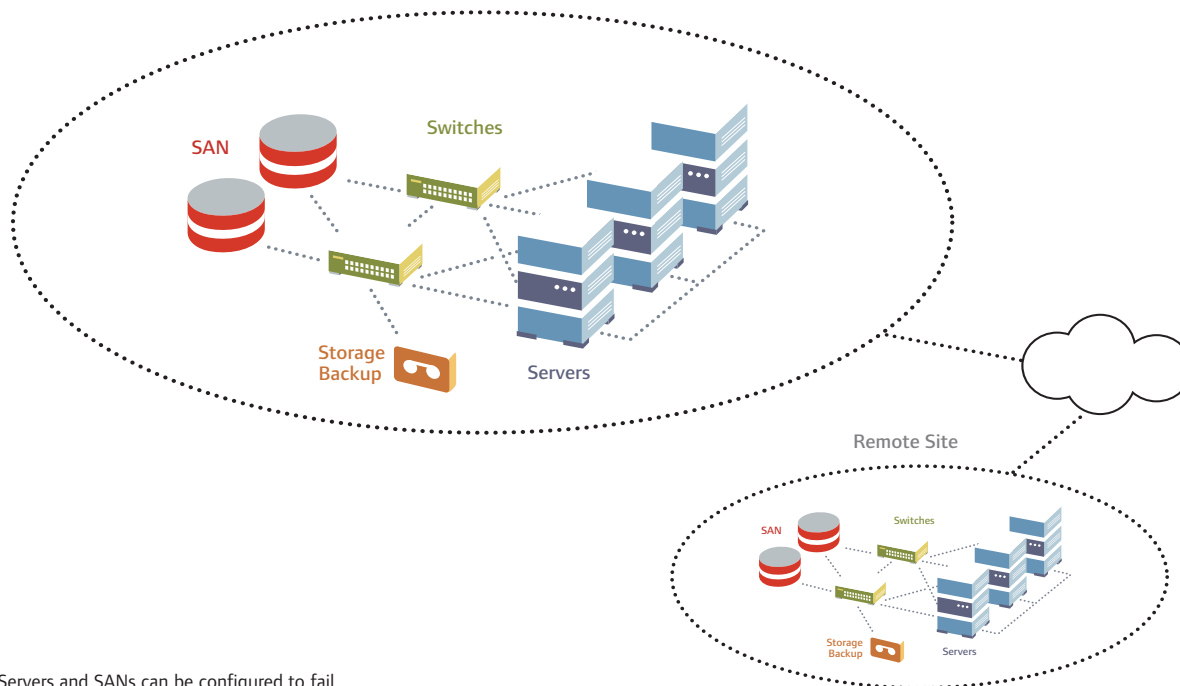
management. Backups are more comprehensive and complete; new capacity can be added without disruption; and as an administrator, you can monitor all your data storage at a glance. Third and most important, SANs can be configured as redundant and geographically separate storage repositories. If one location experiences failure, all data mirrored at the alternate location is seamlessly substituted, often transparently to end-users and without the need to reconnect. And keep in mind that all the benefits of a clustered SAN have also been available using Fibre Channel technology since NetWare 5.1 and continues with version 6.5.

Clustering—Novell Cluster Services can be an integral part of data access and recovery if automatic failover is required. (For more information, see *Novell Cluster Services* on pg. 32.)

DATA OUTSIDE THE NOC

A good IT manager knows where the company gold is stored. In most cases, there's a fair amount of float with critical

GEO-SITE FAILOVER ARCHITECTURE



Servers and SANs can be configured to fail over to remote sites during an emergency.

FIGURE 1

data existing only on workstations, mobile notebooks and in branch or remote offices around the company. Novell's business continuity solution provides security and access for this information as well through features in iFolder and Nterprise Branch Office.

Nterprise Branch Office—If you're in a remote or branch office, it can be like being marooned on an island without IT. Solving the simplest problems like printing, file storage and access to applications takes weeks, requires a visit from corporate support, or—as is often the case—just doesn't get taken care of. Novell Nterprise Branch Office is like having a virtual IT department right in your office. IT tasks such as file storage management, backups, printer configuration, portal management and application access are all handled by corporate IT but the connections, modifications and access are all reflected immediately at the remote or branch office.

HERE'S HOW IT WORKS: An Nterprise Branch Office appliance is located at the branch office. All that's required is a network connection (slow or fast) with Internet access. The Nterprise Branch Office appliance links to corporate with a virtual umbilical cord that makes sure that directory, file, print and authentication information is always synchronized between the two. The relationship between the remote office and corporate is designed to be "loose" so that if the connection between them fails or resources at either end are down, users continue to work uninterrupted. Nterprise Branch Office provides redundancy of file, directory, print and portal access information so that if there is an outage or disaster at either site, users can still be productive. (See Figure 2.)

NOVELL IFOLDER—Novell iFolder provides data redundancy for workstations and laptops—multiple instances

of files in multiple locations ensures redundancy. Novell iFolder provides individuals with an easy solution for automatically managing personal backups and ensuring that their files will always be accessible, no matter where they go or what happens to a particular workstation.

HERE'S HOW IT WORKS: An iFolder server sits at some point on the network. A small piece of client software is installed on each workstation that a user wants to protect (i.e., desktop computer at the office, desktop at home, mobile notebook, etc.). A directory on each workstation is designated as the iFolder directory and any files and subfolders contained in it are automatically synchronized to a user-specific directory on the iFolder server. Synchronization can take place automatically at user-defined intervals or manually any time the user chooses to synchronize. If they have updated files while disconnected, synchronization will

NOVELL NTERPRISE BRANCH OFFICE

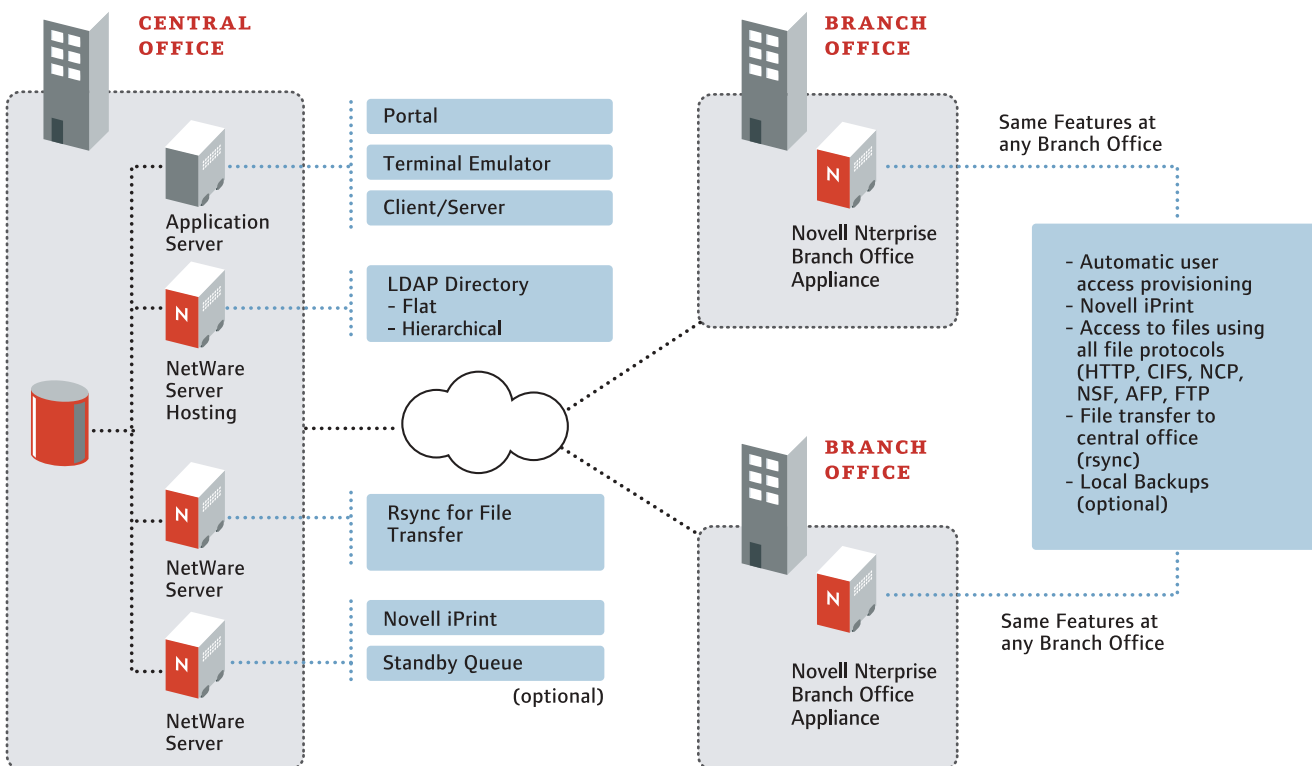


FIGURE 2

occur the next time a connection to the Internet is established. Users can also access files located in their iFolder server directory from any standard Internet browser.

A simple scenario illustrates the process. Jill works from her office desktop, a notebook and sometimes through a Web portal from a client's computer. She makes changes to a presentation on her desktop and saves them in the iFolder-specified directory. At home, she connects to the

presentation either on her other machine or the iFolder server that didn't fail. iFolder provides her with assurance that there is always a current file available and gives her added flexibility when on the move.

NOVELL ARCHIVE AND FILE

VERSIONING—One more valuable NetWare 6.5 feature for end users when it comes to recovering data is Archive and File Versioning. The archive and file

What is business continuity?
It's whatever it takes to ensure that your business can survive through any type of disruption including—but not limited to—categories of natural disasters, hardware and communication failures, internal or external sabotage, acts of terrorism or the failures of supply chain and sales affiliate organizations.

Internet with her notebook and the new changes are immediately synchronized on that machine. She makes additional changes and saves them. The next day, at a client site, she uses one of their workstations to access the latest copy of the presentation using a Web browser. Not once did she have to transfer a file, e-mail herself or insert a floppy.

If anything happens to any of Jill's machines—or the iFolder server—she still has at least two other updated copies of her

versioning server is able to take file-based snapshots of volumes and store them either locally (on the volume it is acting on) or remotely. The system administrator determines the snapshot interval and where the archived files are to be stored. Because Novell archive and file versioning operates at the file system level, administrators have granular control over the archive and the data that are being versioned. The system can be restricted to archive and version-specific subsets (e.g.,



Q: Still sweating your incredibly vanishing backup and restore windows?

A: Get CaminoSoft and sweat no more!

Managed Server HSM™ for NetWare delivers exceptional value for your organization:

- proactive centralized storage management with file retention and deletion policy for NetWare 4/5/6 servers.
- virtual elimination of "out-of-disk-space" conditions—your infrequently accessed files are moved to lower-cost storage, automatically per your policy.
- vastly reduced time required for backup and disaster recovery since only the active files require restoration in primetime.

For more details or to order your comprehensive Data Insurance Policy,™ contact CaminoSoft today!

+1 (805) 370-3100
info@caminosoft.com



©2003 CaminoSoft Corporation. CaminoSoft, the CaminoSoft Logo, Managed Server HSM, and Data Insurance Policy are trademarks of CaminoSoft Corporation. All other trademarks, trade names, and logos referenced herein are the property of their respective owners.



How to Ensure Data Recovery

First rule of disaster recovery is to have something to recover. Following are several methods and a summary of steps to implement them that will ensure you have a spare copy of what you need.

1 File Level Protection

iFOLDER—

Set up iFolder server and clients. Requires iFolder server (dedicated or as a process running on a server) and an IP connection. Users access iFolder server via browser to create an account and download iFolder client. Once client is installed, user selects local iFolder directory and places files to be synchronized in this folder. Repeat process on other workstations if desired.

ARCHIVE AND FILE VERSIONING—

Set up Archive and File Versioning Server. Administrator specifies file/directory/volume for snapshot and specifies interval. Files are accessible to users over the network through file management tools.

ENTERPRISE BRANCH OFFICE—

Set up Branch Office appliance at remote site and connect to corporate.

Failure at branch office, files/authentication/printing recovered from corporate.

Failure at corporate, users work from branch office appliance.

2 Disk or Volume Level Data Protection

STORAGE AREA NETWORK—

Create SAN using iSCSI or Fibre Channel. Use hardware level RAID or software level RAID included with NetWare 6.5. RAID level 1 provides for mirrored drives; RAID level 5 for striping across disks with parity rebuild.

3 Server Level Data and Server Protection

CLUSTERED SERVERS—

Create a cluster with two servers and mirrored drive. On failure of one server, the other server assumes operation.

4 Site Level Data and Server Protection

DISTRIBUTED CLUSTERS—

Create a clustered cluster with servers and SANs in multiple locations. Data transactions are kept current at both sites. Partial failure at one site is recovered by cluster servers and mirrored or RAID drives. Full site failure is recovered by second site. (See Figure 1.)

only .doc files in one subdirectory), or can be expanded to cover all files on all volumes of a server. The resulting archive can be stored on the same server, or can be located across the LAN or WAN on a different server.

Archiving and versioning are a valuable emergency recovery bonus for users. If a file is modified or updated and an earlier version is needed, users simply go to the archive directory, right click on the file and see all previous versions. They select the version to restore—even if the file was renamed, deleted or modified by someone else on their team. There's no need for IT support or the necessity to fumble through backup tapes.

BUSINESS OPERATION TOOLS

Having continuous access to data is only valuable if the tools to access and manipulate that data are also available. Most information is only accessible if business applications such as databases, Web servers, e-mail servers, application servers and ERP/CRM/Supply Chain programs are operational. With the increased use of portals and inter-business communications, ensuring that online business processes are functional in the event of disaster is absolutely critical. In upcoming issues of Novell Connection we'll also cover open source technologies and Web application services supported in NetWare 6.5 which are also a critical part of a solid disaster-recovery plan.

Key technologies included in NetWare 6.5 that ensure that business operation tools continue to function and are easily managed are Novell Clustering Services and Novell iManager.

NOVELL CLUSTER SERVICES—

In addition to providing excellent data recovery support, Novell Cluster Services can be used to guard against failure of business operation tools such as databases, application servers and Web servers. Clustering allows administrators to create a group of servers performing various functions (e-mail, Web, application, database, etc.). If any one of these servers fail, then its processes, IP addresses, drive

mappings, trustee rights, etc., will be automatically and immediately assumed by one of the other servers in the cluster. The cluster can be separated geographically, creating the option for continued operation in the event that one site is disabled. Using SAN replication technologies, the data blocks for Novell services are completely portable between sites. This means that service configuration data and storage metadata, including all security rights, are portable between geographically separated

Mesaba also uses host shadowing as an ideal backup method. Each time the server writes data to a storage box at the airline's data center in Minneapolis International Airport, it simultaneously writes to another storage box at the disaster recovery site 20 miles away, ensuring double protection of airline data.

NOVELL iMANAGER—Many business continuity and disaster recovery solutions require a separate system that comes with

If a file is modified or updated and an earlier version is needed, users simply go to the archive directory, right click on the file and see all previous versions.

clusters. Multiple dispersed data centers may be clustered into a global high availability system which becomes immune to regional outages. If a tornado eliminates one data center, the application services automatically fail over to other data centers positioned in different geographies. In essence, the solution is a cluster of clusters on a global level.

Here's how it worked for Mesaba Airlines, the fourth largest regional airline in the US. Originally, all mission critical resources—flight information, airplane tracking, parts inventories—were on one system and if it failed, flight delays, cancellations and financial loss were the results. After moving to Novell Cluster Services, if one network server in the cluster fails, other server nodes in the cluster automatically take over the failed node's responsibility, guaranteeing continuous, uninterrupted system operation, ensuring employees have reliable access to essential resources.

its own administration interface and management paradigm—not NetWare. All aspects of a Novell continuity solution, including SANs, clusters, archives, backups and eDirectory, are manageable through one consistent interface, Novell iManager. iManager is a browser-based console that provides administration control of resources from any Web location. iManager's remote management gives administrators the ability to monitor and manage NetWare server health from any location on the Internet. Once securely authenticated, administrators have access to server processes and statistics, volume/directory/sub-directory inventory features, and the GUI server console. NetWare 6.5 includes a new set of storage management tools which allow administrators to view storage consumption trends graphically. Managers can easily spot high disk usage and determine usage rate increases by file types or users.



Q: Still sweating the availability of your vulnerable mission-critical servers?

A: Get CaminoSoft and sweat no more!

StandbyServer™ for NetWare 4/5/6 delivers high availability and data replication for multiple NetWare servers. By monitoring the health and mirroring the volumes of your primary servers, it provides both automatic failover and data access if storage becomes unavailable.

OFFSite Archive™ for NetWare 4/5/6 provides data replication and rapid recovery for multiple NetWare servers. Point-in-time “snapshots” of your data are sent to a safely located remote server, facilitating centralized backup plus quick disaster recovery.

For more details or to order your comprehensive Data Insurance Policy™, contact CaminoSoft today!

+1 (805) 370-3100
info@caminosoft.com



©2003 CaminoSoft Corporation. CaminoSoft, the CaminoSoft logo, and Data Insurance Policy are trademarks of CaminoSoft Corporation. StandbyServer, OFFSite Archive, and all other trademarks, trade names, and logos referenced herein are the property of their respective owners.



Novell BrainShare Europe

BARCELONA, SPAIN, SEPTEMBER 7 - 11, 2003

If you missed the fun in Salt Lake City, be sure to join us in Barcelona.

We are pleased to announce that our 13th Annual BrainShare Europe event will be held at the Palau de Congressos de Catalunya in Barcelona, Spain.

REGISTER NOW! www.novell.com/brainshare/europe

THINGS TO DO AND SEE

one Net Solutions Lab:

One-stop shop for all Novell solutions and those of our strategic partners!

BrainShare Network:

PCs located throughout the conference center keeping you connected.

Over 100 Technical Sessions:

Developer code breaks, real-world case studies, technical tutorials and business solutions.

Novell Developer Den:

More content to help developers deliver one Net solutions than ever before.

Evening Events

Welcome Reception

Kick off BrainShare Europe 2003 with a bang.

Meet The Experts

Mingle with top Novell engineering, product, solutions and consulting experts.

The Conference Party

We're keeping the details a surprise, but will be dropping hints on the fantastic party we have lined up for you over the coming months!

For a distributed system with geo-site failover capabilities, the ability to manage from a remote office or emergency command post is imperative in the event that the central facility becomes inaccessible. Novell iManager provides this type of access for pooled, clustered, remote, synchronized and redundant systems throughout the network.

ORGANIZATION INTELLIGENCE

Even though data is secure and tools are available, your organization is still dangerously vulnerable if proper authorization and security is not maintained. Preserving the organizational intelligence of who (individuals, groups, departments) has access to what (files, applications, networked resources) is a mandatory requirement for protecting data and ensuring business continuity. Novell eDirectory is the world's leading solution for the safekeeping and management of company authorization and intelligence information.

eDirectory was engineered as a high-level, fault-tolerant solution. While it is tightly integrated to control access to all resources, it is not tied to a specific server or machine. eDirectory provides a virtual security umbrella without the need to be anchored to one specific processor or location. Because of this linked association (integrated but not dependent), eDirectory continues to retain information and control access even when individual servers or groups of servers go down or offline. eDirectory's capability is due to partitioning and replication. Partitioning allows the directory database to be split into smaller portions for better client support and performance. Replication allows distributed directory databases to update each other quickly in the background for increased security, ensuring changes in one portion of eDirectory become available to the entire network as quickly as possible.

In most enterprise organizations, there are other directories (often application specific) are in operation, in addition to eDirectory. Not to worry. Using the

NOVELL CORPORATE EVENTS CALENDAR

DATES	SHOW	LOCATION	URL
August 5-7	LinuxWorld	San Francisco, CA	http://www.linuxworldexpo.com
August 12-14	HP World	Atlanta, GA	http://www.hpworld.com
October 7-9	Catalyst Conference Europe 2003	Hotel Rey Juan Carlos, Barcelona, Spain	http://www.burtongroup.com/catalyst/cateu03/
November 4-6	BrainShare Latin America	Sao Paulo, Brazil	http://www.novell.com/brainshare/

DirXML Starter Pack included with NetWare 6.5, you can keep this business intelligence secure as well. DirXML provides a synchronization mechanism between directories of varying types, keeping identity information consistent in multiple disparate formats.

Using eDirectory, any and all resources can be managed from a single point no matter where they are physically located or at what location the management takes place. This distributed, replicated management model

With NetWare 6.5, you can implement data redundancy on a sliding scale anywhere from good backup to mirrored servers, auto failover, and redundant data at remote locations. During a complete site disaster, you can still continue operations without a hiccup. Users in remote offices are covered, business operation tools remain viable, and you can manage the network from a remote office—or wherever you may be.

The best part of this is that you can provide this capability without spiking

With NetWare 6.5, you can implement data redundancy on a sliding scale anywhere from good backup to mirrored servers, auto failover, and redundant data at remote locations. During a complete site disaster, you can still continue operations without a hiccup.

ensures that the remaining network resources and applications will still be manageable—and secure—in the event that sections of a network are rendered inoperable. No one is going to gain unauthorized access during an outage and managers will still be able to control the surviving portions of the network. All organizational intelligence is securely maintained.

SUMMARY

So now, if that executive asks about your business continuity contingencies, you can feel confident and frankly even a little bold.

your IT budget. Everything comes with NetWare 6.5—Nterprise Branch Office, iFolder, iSCSI, Novell Cluster Services, NSS, archive and file versioning, eDirectory and more—right in the box. You can put in place a failproof system using the same people, with their existing networking knowledge, on the same equipment that you already have. So after explaining this to your executive, you might just feel bold enough to ask for some extra time off! After all, the network will be fine without you—even if something does happen. **N**

The best
insurance
policy for
NetWare
is **FREE.**

Prior to installing your next Service Pack or NetWare upgrade, use the Evaluation version of Portlock Storage Manager to image the booting DOS partition and SYS volume. If the upgrade fails, purchase a license and then restore the server exactly as it was prior to the upgrade.



PORTLOCK

Contact Your NetWare
Insurance Agent @

sales@portlock.com

www.portlock.com