

Business Continuity and Disaster Recovery

White Paper

Novell, Inc

Overview

If you scan the last year's headlines for business disrupting events, you will find the list is extensive. Businesses in various parts of the world have experienced downtime and data loss due to storms, energy shortages, earthquakes, volcanoes, accidents and even terrorist violence. Through these events, companies have experienced everything from minor inconvenience to complete dissolution. With the random and unpredictable possibility of natural, accidental or terrorist disaster always on the horizon, how do companies optimally prepare to prevent or minimize the effects of these occurrences?

Novell, through a combination of products and partners, provides a comprehensive business continuity and disaster recovery solution for any organization interested in preparing for, guarding against, and recovering from unplanned disruptions. The Novell solution consists of several elements for creating and implementing a business continuity and disaster recovery plan including:

- *Plan Preparation and Development* - By conducting an in depth risk and recovery capabilities assessment, organizations can discover areas of vulnerability and strength in guarding against and recovering from an unplanned disruption.
- *Preventative Safeguards* - Established policies combined with strong security and specific product technologies provide a secure line of defense that can avert a high percentage of common crises.
- *Appropriate Architecture* - Implementing a secure architecture with failsafe, redundant, and distributed elements can minimize or eliminate disruptions. An appropriate architecture ensures continued communications as well as easy data recovery and access.
- *Recovery Accommodations* - In the event of crisis, recovery accommodations enable IT staff and employees to be back to full productivity as quickly as possible. This includes full restoration of management features, workspace, information, and organization intelligence.

This white paper outlines the services, architecture, products, features and benefits that are available from Novell and its partners for a complete business continuity and disaster recovery solution. In addition to peace of mind and reduced loss from downtime, the greatest benefit is that a comprehensive and robust solution can be implemented with very little incremental expense. Almost all of the features that are required for disaster prevention and quick recovery come with standard Novell products at no extra charge.

The Need

Any IT manager considering business continuity and disaster recovery scenarios doesn't need much of an imagination to understand the critical need after this last year's world events. "The September 2001 attack on the World Trade Center in New York City tested the contingency plans of companies to an unanticipated degree. Companies that had business continuity plans and contracts in place with vendors of recovery services were able to continue business at alternate sites with minimum loss of data and minimum downtime. Business survival necessitates planning for every type of business disruption including—but not limited to—categories of natural disasters, hardware and communication failures, internal or external sabotage or acts of terrorism; and the failures of supply chain and sales affiliate organizations." (source: GartnerGroup)

Other pertinent disaster planning and recovery statistics indicate:

- Two out of five (40%) of enterprises that experience a disaster will go out of business in five years. In some cases, the disruption of normal business operations causes the customer to lose confidence in the viability of the enterprise. In other cases, the cost of recovery is simply too great. (source: GartnerGroup)
- While 85% of Global 2000 enterprises have established a disaster recovery plan for core technology and infrastructure, only 15% have a full-fledged business continuity plan. This is dangerous: enterprises must shift from a disaster recovery focus to business continuity because most, if not all, stages of the business life cycle now totally depend on IT services. (source: GartnerGroup)
- By 2005, more than 70% of large enterprises will have invested in business continuity planning compared to fewer than 25% today. (source: GartnerGroup)

According to InformationWeek, a business continuity and disaster recovery plan must address five specific areas in order to be effective. These include 1) facilities (employees need a place to work); 2) connectivity (multiple connection options for access); 3) IT applications (access to business critical applications); 4) business partners (ensuring continued communication and information flow among supply chain partners); and 5) people (coordinating and communicating with people in the event of a disaster).

By using products and services from Novell and its partners, enterprise companies can effectively combine existing business intelligence and policies with state-of-the-art technology to address all five of these areas and ensure business continuity in the event of an unplanned crisis or disaster. Novell's business continuity and disaster recovery solution includes both strategy and technology. Novell and its partners offer an integrated approach that addresses each of the following areas.

- Preparedness Planning
- Preventative Security Measures
- Communication Restoration
- Data Recovery and Access Restoration
- Workspace Recovery
- Recovery Expertise and Skills

Be Prepared

A few simple preventative measures can mean the difference between a temporary glitch and total debilitation—being prepared isn't just for Boy Scouts. But with an intense and complex IT installation, how can you spot vulnerabilities or know where a system will fail in the event of a crisis? Novell customers can leverage partnerships with leading business continuity and disaster recovery consulting firms to make assessments and implement an effective and comprehensive plan based on proven best practices.

Novell and Goliath Networks have pooled resources to provide a Risk Assessment/Disaster Recovery Planning offering that combines the technology expertise of Novell with the business assessment and planning expertise of Goliath Networks. This security assessment looks at every aspect of a company's infrastructure and ability to deter or withstand a crisis. The issues examined include:

- *Security Protections* - Are there adequate safeguards in place to prevent any unauthorized access? An effective analysis includes an assessment of access methods, security barriers, authentication schemes, connection safety and physical facility security.

- *Communications Infrastructure* - The communications aspect of continuity and recovery has two facets. The first is the ability for administration personnel to continue communications in the event of a crisis and during the recovery process—facilitating communications through the recovery period is critical. The second is the ability to continue or restore communications for system subscribers. A good assessment will determine what elements are required to enable a certain level of continued communication through a crisis and what processes must engage to quickly restore general communications shortly thereafter.
- *Workspace Recovery* - System users have customized environments that include all of the elements (applications, peripherals, connections, references, files, etc.) required for them to perform their jobs. An effective assessment will quantify and qualify the elements that must be available after a crisis for continued business operation and outline the methods for ensuring quick and effective recovery.
- *Data Access and Recovery* - At the heart of any IT infrastructure is the protection and security of data. At the simplest level, a data recovery plan “backs up” data so it can be manually restored if needed. A business continuity and recovery assessment will help determine the value of data and how it should be protected and stored so that some or all of it is available in the event of a crisis. Fail-over, mirroring, near-line/offline, Web-enabled, Web-hosted—all of these technologies are possible elements of an effective continuity and recovery plan.

In summary, devising an effective strategy is not a simple process. Professional planners like Goliath Networks and Novell have had years of experience in managing infrastructures and providing solutions that minimize or eliminate the potentially devastating effects of unplanned emergencies.

Robust Security

Adequate protection requires several layers of security before, during and after a crisis. An effective strategy to protect digital assets will include a bulwark of safeguards in three major areas: access security, connection security, and failsafe security administration. Novell effectively addresses all three areas with a combination of directory service technology and security specific products.

Access security ensures that only those with the right credentials or identity are able to access authorized resources. Resources can be anything including files, applications, peripherals, Web content, computers, messages, media streams, etc. Effective authorization takes into account who a user is, their identity characteristics, the context of their relationships with other resources and users, and the business policies and rules that must be adhered to in order to ensure proper access. Access security is particularly important in the event of a crisis as disasters are often followed by an increase in criminal activities.

At the heart of an effective access security solution is Novell's eDirectory™. As a state-of-the-art, distributed, flexible, and secure authentication service Novell eDirectory provides an identity based security infrastructure that can be leveraged to accommodate all types of access security. Each of the following solutions helps eliminate one of the primary sources of IT crisis—unauthorized access. Effective authentication management can prevent intruders before, during and after an unplanned disruption.

- **SecureLogin** - Novell SecureLogin consolidates usernames and passwords from multiple applications or authorization directories to single instance. Applications, databases, and other processes that require a username/password sequence for

authentication can check these against a single source—users only need one set of credentials, eliminating possible security breaches from floating, multiple or duplicate IDs.

- **iChain™** - Novell iChain provides identity-based Web security services that control access to application and network resources across technical and organizational boundaries using Internet protocols. iChain separates security from individual applications and Web servers, enabling single-point policy-based management of authentication and access privileges throughout the Internet. Users can access a multitude of resources with a single signon.
- **BorderManager™** - Novell BorderManager is a suite of network services that enables IT to securely connect the network to the Internet or any other network. BorderManager improves security and performance at the borders between networks and provides the following features: control outside access to an intranet; control user access to the Internet; provide remote access to the intranet and the Internet; establish Virtual Private Networks (VPNs); and accelerate access to the intranet and Internet.
- **Novell Modular Authentication Services™** (NMAS) enables multiple authentication methods for stronger security including digital certificates, smart cards and biometrics.

Connection security involves the protection of data as it is transmitted though the network or across the Internet. Several Novell technologies are applied to ensuring that communication connections are secure, robust, and efficient. Novell's implementation of the Internet Protocol (IP) includes the highest levels of encryption; Novell Web service connections are encrypted using SSL; Novell BorderManager includes VPN capabilities for secure connections across a WAN.

The complexity of a security management system can be a factor in how safe a system is. With complex management and limited staff, more doors for security breach may be left open. Novell eDirectory combines security management for all resources into a single interface that is graphical, intuitive, and easy to use. eDirectory's powerful hierarchical management architecture combined with strong policy and rules capabilities make it very easy to strongly manage a vast collection of users and resources with a minimum of effort. **Novell Account Management** unifies the management of user profiles on NetWare®, Windows™ 2000, Windows NT, Solaris™ and Linux™ networks, making it easy to securely manage cross-platform environments.

Restore Communications

Since disasters can occur at any scale, disaster preparedness should include provisions for facilitating disruptions at multiple levels. An effective system will inherently accommodate localized or individual events automatically without the need for IT intervention. For large-scale disruptions, failsafe and emergency plans should include alternate systems, methods for crisis management communications and procedures for quick restoration of full services. Effective disaster preparedness must accommodate cascading levels of crisis, all the way from a single user losing an e-mail link to having the mail server taken out along with the entire data center. Novell provides continuity and crisis solutions across the entire spectrum with products such as GroupWise™, eGuide, and Novell Portal Services.

As a complete communications and collaboration solution, **GroupWise** is a leading choice among enterprise companies. Integrated e-mail, calendaring, scheduling, workflow and document management is available across the network and the Internet for employees and

partners from wired or wireless devices. GroupWise features that contribute to rapid recovery in the event of a crisis include caching and Web access.

GroupWise architecture is inherently scalable and distributed. If eDirectory is the underlying directory service, contact information resides in a virtual workspace that is shared among many GroupWise post offices which means that one location or server can go down without affecting any other. Directory information is always available through replicas. In addition, GroupWise data is “chunked” rather than streamed enabling GroupWise servers to continue communications without timing out. If one domain goes down, messaging and collaboration between other domains is uninterrupted enabling the rest of an organization to continue working.

GroupWise caching mode replicates an individual’s message store to a local hard drive. This allows them to continue working as if they were connected and then resynchronizes when the connection is restored. Users can continue working uninterrupted through temporary outages due to downed post offices, network connection failure, and even power outages if they are working from a laptop.

GroupWise also provides for emergency replacement post offices at alternate locations. In the event of a complete post office failure, all users on one system can be communicating again within an hour. If the reverse occurs and a user location or workspace is inoperable yet the post office is intact, users can still have full GroupWise functionality available through Web access. E-mail, calendaring, scheduling and workflow are available to any authorized user from any Web-enabled workstation at any location.

Other Novell technologies facilitate emergency response and communications infrastructures during and after a crisis including eGuide and Novell Portal Services. **eGuide** provides a virtual list of the latest contact and organizational information on employees from backed-up network and HR directories. As organizational relationships and identity information in a company change, information is recorded automatically in eGuide. In the event of a crisis, information such as home numbers, contingency contacts, supervisors, group memberships and more is easily accessible to authorized individuals. This information is searchable by attribute such as location, manager, responsibility or relationship.

Using **Novell Portal Services**, a virtual command center can be created for access by employees from any location using any device. Updates and instructions are quickly and easily available to employees, customers and partners keeping businesses operational and providing status. Using the organizational information available through eDirectory, information can be specifically targeted to and only accessible by specific individuals or groups. General updates from management can be disseminated to everyone across all portal sites with specific content such as IT status going only to the IT group or customer service instructions going only to employees facing external customers.

Recover Data and Restore Access

Successful recovery after a crisis has at least three prerequisites—good backups, one or more systems for quick restoration, and management tools that facilitate recovery. Solutions from Novell and its partners comprehensively cover each of these areas.

Good Backups

An effective plan includes several levels of backup data to accommodate different degrees of crisis. Novell solutions provide a broad range of options from iFolder and Web access for individual user backups to complete server mirroring at remote locations for network fail-over.

For individual users with one or more workstations, **Novell iFolder™** is an online storage repository and synchronization engine. Users can store files on a local machine—just like they have always done—and automatically these files and any changes are replicated to a central server over the network or the Internet. These files and changes will automatically be updated on any other machines that the user has subscribed to iFolder. Novell iFolder provides an incremental and automatic backup (and possibly multiple copies) of any new or modified file on a user workstation. If the workstation or laptop is damaged, stolen, or inoperative for any reason, the user can immediately resume work from another machine and still have the latest data.

NetWare™ 6 has several inherent backup features that ensure availability of data in the event of crisis including Storage Management Services (SMS) and Novell Cluster Services. **Novell Cluster Services™** is a server clustering solution that supports fail-over, fail-back, and migration (load balancing) of individually managed cluster resources. NetWare 6's clustering system ensures high availability and manageability of critical network resources, including data (volumes), applications, server licenses, and services from remote/distant locations. Novell Cluster Services uses off-the-shelf server and storage area network (SAN) hardware to provide mirrored storage that is geographically separated by up to 10 kilometers on up to 32 servers. Hierarchical Storage Management (HSM) provides the ability to segment data into "active" and "historical" data, which results in improved storage management and lower hardware costs.

Novell Storage Management Services™ (SMS) is a flexible backup solution that enables administrators to target specific devices and databases for information backup and retrieval. By loading the appropriate Target Service Agent (TSA), it is possible for SMS to back up a variety of different databases on the local server, remote servers, or even on network clients.

Novell partners provide excellent solutions for the storage and access of data. Legato provides two products, SnapShotServer™ for NetWare and OFFsite Archive™ for NetWare.

SnapShotServer for NetWare provides disk imaging and centralized control of the backup process. It creates an image of live volumes at designated intervals and either holds them or presents these frozen images to any standard backup utility. Legato **OFFSite Archive for NetWare** is a disaster recovery solution that creates a point-in-time recovery image of data at another location. In the event of a local disaster, the remote system can be used to quickly recover the primary server's critical data and network services. OFFSite Archive functions with or without Legato StandbyServer™ and provides for local high availability and OFFSite Archive for distance disaster recovery.

Alternate Access

Disruption may not always occur at the heart of a network but at the periphery with workstations or printers. NetWare features such as Novell iPrint and Web Access provide solutions for these situations. **Novell iPrint™** connects geographically dispersed printers through the network or the Internet providing multiple options for printing in the event that a printer or location goes offline. Using a Web interface and physical map, users can locate printers in other locations, install print drivers and access them as if they were directly attached to their workstations. In the event a printer is no longer accessible, another can be easily located and printed to.

NetWare Web Access allows users to instantly access data files via the Web should other network connections become unavailable. Files can be uploaded, downloaded, viewed and deleted from any device with a standard Web browser. NetWare still enforces the same levels of security and authentication that are in place with a network workstation client.

Remote management is also a critical 'must have' for disaster recovery. All Novell services, including directory and network management, are available through a remote Web interface using a standard browser. Novell Remote Management allows IT to perform critical server management functions via the browser without having to be onsite if local staff is unavailable or if an area is restricted due to contamination or infection.

Server Management and System Recovery

Another important aspect of disaster preparedness is preventative and recovery operations for network and application servers. Using Novell **ZENworks™ for Servers**, complete groups of servers can be configured, modified and managed simultaneously. ZENworks for Servers enables IT to quickly and easily distribute content across multiple servers and to reconfigure them exactly as they were before any unplanned failure. ZENworks Synergy provides disaster prevention by immediately distributing critical new virus protection software to protect all servers as well as desktops. And, as with most Novell solutions, ZENworks can be administered remotely.

Adequate storage is also a critical component of any preparedness or recovery plan. Modular, snap-in storage is valuable for storing backups and system images as a precautionary measure. In addition, having easily expandable storage capacity available during recovery and rebuild can facilitate data organization and reconfiguration. Novell's **NetDevice™ NAS** (Network Attached Storage) provides snap-in, online storage that can be remotely located but centrally administered. NetDevice NAS can be used to keep a remote office going if the corporate net goes down or as snap-in storage to accommodate a new or recovering system.

In addition to restoring mission critical data, a recovery plan should include provisions to restore second and third-tier data applications as well. **Novell DirXML™** enables automatic synchronization of identity data across other applications and databases. This can be extremely valuable when authoritative identity sources have changed between the time when a disaster occurs and second and third-tier systems are later brought online. DirXML ensures that a consistent authoritative identity source is available and used across all applications—even when these applications vary in identity format.

Recover Workspace

Getting communication connections and data back on line is still only part of the recovery task. In order for users to be productive again, they must have access to applications that they use on a regular basis. Whether a user requires spreadsheets, e-mail, database, word processing or specialty line-of-business applications, a workspace environment must be available that applies these applications to restored data. Again, Novell solutions can assist in rapidly recovering user workspace or providing temporary workspace so that users can be productive immediately.

ZENworks™ for Desktops enables IT administrators to deploy and configure multiple desktops simultaneously. Using group and profile information from eDirectory, workstations can be automatically configured with individual preferences and customized according to area of responsibility or assignment. Hundreds of workstations could be installed or reconfigured with a few simple operations. New services and applications can be made available on a permanent or temporary basis.

Again, **Novell Remote Access** can be a valuable workspace recovery tool, enabling temporary or displaced workers to connect to various Web applications, peripherals, data and organizational resources. Novell Remote Access leverages the Internet as a connectivity backbone without the need to establish (or reestablish) internal networks or expensive VPN connections. **ZENworks Synergy** delivers content and applications across the Web to

individuals based on directory profiles and business rules to any Web-enabled device. Employees can work from any location using whatever device they have access to, whether that be from temporary office space, home, on a borrowed machine, at an Internet kiosk, or from a personal digital assistant (PDA).

Recovery Expertise

In the event of a crisis or disaster, Novell customers are not left on their own to deal with it. Novell experts are available worldwide who architect and implement disaster plans as well as facilitate recovery in the event of a crisis. For customers desiring additional support, Novell offers Premium 600/700 support services as well as access to the global community of certified Novell professionals.

With various levels of **Novell Premium Service** available, customers are able to choose programs that meet unique needs—whether that ranges from occasional support to ongoing access to a Dedicated Support Engineer (DSE) and Service Account Manager (SAM), 24 hours a day, seven days a week. All of these options can help an IT department keep operations running at maximum efficiency in the event of unplanned emergency or disaster. During the September 2001 New York/Washington disaster, Novell support engineers were immediately deployed onsite for recovery work with government and financial customers. Novell's support services are ranked among the best in the world with dedicated and proactive support contacts and powerful support tools.

In addition, there are more than 600,000 professional Novell certifications worldwide. Using the Novell Partner Locator, customers in need can quickly access skill sets that may be lost or unavailable in a disaster. Each year, Novell certifies thousands of professionals all over the world to manage or support its information technology (IT) products. The real-world certification requirements, performance-based testing and quality reputation of Novell certified professionals ensure that resources are available and qualified to manage or assist in a recovery effort.

The Benefits

Using solutions from Novell and its partners, it is entirely possible that if a catastrophic event disabled one entire data center, servers and storage would be made immediately available from another data center without IT intervention and transparent to the users. Whether the unplanned disruption is just a failed laptop hard drive or the loss of an entire data center, Novell products and services ensure that critical business systems are up and running without interruption to employees, customers or partners. Knowing a system is secure and an effective plan is in place provides one of the most desired benefits—peace of mind. IT professionals and line of business managers can rest assured that adequate precautions have been taken at every level and that if a major disaster does occur, systems are in place for fail-over and complete recovery.

Another significant benefit to a Novell-centric business continuity and disaster recovery solution is that it hardly costs anything extra. The same systems and products that are implemented for routine operations often have features built in and included at no extra charge that facilitate crisis management. Emergency functionality is available at no additional cost.

To illustrate, eGuide isn't just used for emergencies. A comprehensive online company directory available from any device with controlled access by attribute is valuable for any

company. The fact that it can be securely available in the event of a crisis with protected organizational and individual information is an incremental benefit at no extra charge. Novell Portal Services have vast application in everyday operations for application and data access; the fact that they can facilitate ongoing work in an emergency is a no extra charge feature. Other benefit examples include the capabilities of ZENworks for Servers and Desktops and NetDevice NAS; these products deliver value and huge savings in everyday use. Novell's licensing scheme also makes implementing disaster services inexpensive as licensing "user based". Extra licenses for Novell servers are not required for dedicated backup, cluster, mirror or storage systems. In short, most of the services described in this paper are available and part of the standard set of products and services offered by Novell.

The summary of benefits to implementing Novell solutions for business continuity and disaster recovery includes:

- *Security Confidence* - Businesses can rest assured that adequate security and preparedness measures are in effect. There is no taking chances on matters of intrusion, identity theft, digital asset loss, or unauthorized access.
- *Retained Intelligence* - Solutions from Novell uniquely enable companies to collect and retain intelligence such as business policies, rules, organizational structure as well as access rights and authorities. In the event of a crisis, this intelligence can be recovered without loss or the need to reimplement.
- *Quick Recovery* - With a distributed and flexible solution, full IT capabilities with data and application access can always be available, even if disasters eliminate physical facilities.
- *Ongoing Business Value* - A Novell solution not only enables capability in time of crisis but provides business value everyday. Novell's ability to enable and manage diverse and complex systems simplifies the task of management and enables users and employees to be more efficient and productive.
- *Cost Savings* - Implementing Novell's business continuity and disaster recovery solution can be accomplished with little or no incremental cost. In most cases, an effective solution can be implemented using existing infrastructure and configuring familiar products. There is little need for retraining or extensive rip and replace configurations.

Putting in place a comprehensive and complete business continuity and disaster recovery solution provides tangible and intangible benefits for organizations and businesses of all sizes. And if by fortunate circumstance nothing happens, there is still the benefit of piece of mind.