



Cases in Point

Business continuity/disaster recovery plans should consider a variety of possible scenarios and deployment options, including:

- Co-locating with the primary server for onsite redundancy in case of a localized server hardware or database failure
- At a peer or redundant data center that would be robust enough to operate in redundant mode when one of the data centers is offline for a significant period
- At a geographically distant, disaster-recovery company that specializes in helping customers prepare for and recover from cataclysmic events

Network Performance Management and Your Disaster Recovery Plan

nGenius® Performance Manager Standby Server Delivers Business Continuity

Introduction

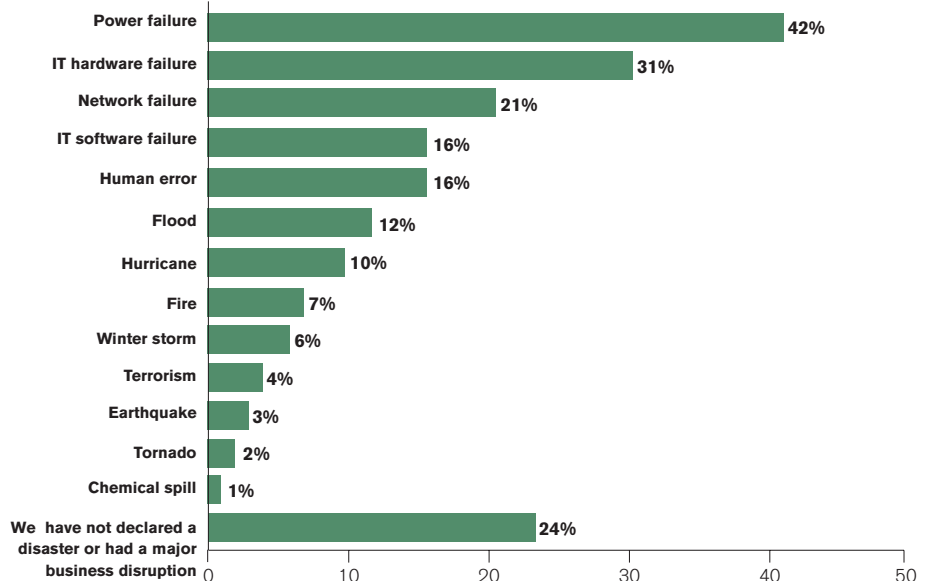
The disasters of 9/11 started the steady drum beat in many corporate boardrooms regarding the value and need for disaster recovery plans. A number of serious hurricanes (Katrina, Rita, Gustav, etc), tornados, and other natural disasters, as well as a variety of power interruptions from rolling brown outs and black outs on the West Coast to a multi-day power outage that hit the Northeast and Canada, have all served to punctuate the need that a strong disaster recovery plan is essential to maintaining business continuity.

Challenges

Today's data centers, trading floors, and manufacturing facilities depend on continuous operation and availability to earn revenue, maintain profitability and sustain customer loyalty. According to the Forrester/Disaster Recovery Journal October 2007 Global Disaster Recovery Preparedness Online Survey, 76% of companies have declared a disaster or experienced a major business disruption in the past five years.

The most common cause of a declared disaster or major business disruption is a power failure, followed by IT hardware failures and network failures (see Figure 1).

Figure 1. "What was the cause(s) of your most significant disaster declaration(s) or major business disruption?"



Base: 250 disaster recovery decision-makers and influencers at businesses worldwide (multiple responses accepted) (Does not include those who answered "other" or "Don't know")

Source: Forrester/Disaster Recovery Journal October 2007 Global Disaster Recovery Preparedness Online Survey

To successfully secure funding to support disaster recovery preparedness, IT must work with business owners to calculate the cost of downtime, define recovery objectives, identify the likeliest risks, and select the most cost-effective technologies and services. Management is much more likely to approve funding when IT leads with a business case and business metrics.

Business continuity/disaster recovery plans should consider a variety of possible situations:

- Are we protected if the application server experiences a failure?
- What happens if we lose our primary Internet connection?
- What if the power goes out for a significant period of time, such as a four-hour window during peak business hours?
- Do we have an alternative if our data center is inoperable for an extended period of time?

Some of the solutions devised to address the challenges and questions above could include:

- Physically deploying backup servers alongside all application servers that would maintain a back-up copy of the database and/or take over operations in the event of a server failure.
- Creating and maintaining two or more data centers that would be robust enough to operate in redundant mode in situations where one of the data centers is offline for a significant period.
- Contracting with a disaster-recovery company that specializes in helping customers prepare for cataclysmic events with more sophisticated and expensive “mirroring” in which remote centers simultaneously run the same operations as a company’s primary computers. These sites can host services after such monumental events for weeks or even months.

Performance Management Aids Business Continuity

Organizations rarely question adding redundant servers for revenue-generating or customer resource management applications as maintaining order processing and customer service during challenging conditions will continue to be essential. With the nGenius Standby Server, NetScout makes it possible for IT organizations to ensure that the functions and benefits of the nGenius Performance Management System are available in disaster situations – when they may be needed most. Network and application performance management tools such as the nGenius Solution help maintain close tabs on network and application activity during a crisis by showing which systems and applications are online, which sites and users can continue to conduct business, and how business services are performing on backup or redundant networks and systems. This information will help IT professionals decide where to deploy disaster assistance or even if they need to notify local authorities for assistance.

Business continuity plans and disaster recovery back up services represent a substantial investment to any company. Failures in execution or holes in coverage may reduce the effectiveness of the entire plan. After-the-fact network and application activity reporting from performance management tools like the nGenius System can help validate the investment, demonstrate its success or failure, or identify areas to improve in overall disaster recovery operations.

Case Study

A European-based fixed-line operator and wireless provider (PTT) with stakes in telecom operations and mobile phone carriers throughout Central and South America began an MPLS roll out. Their challenge was creating and securing service assurance as they converted the network and moved customers to the new MPLS network, while simultaneously migrating corporate employees to the MPLS network for inter-company communications. This challenge was compounded by the necessity of maintaining “five 9’s” availability in a “high availability and reliability” industry.

The PTT chose the nGenius Solution because of its carrier-class, highly scalable three-tier architecture that would support multiple nGenius Performance Manager Servers deployed in a distributed manner as well as companion nGenius Standby Servers as part of the business continuity plan. When implemented, the information between the Global Manager (master), the Local Servers (slaves) and their respective nGenius Standby Servers can be shared and accessed seamlessly.

Meeting the Need

The nGenius Server, built on highly scalable architecture for supporting multiple nGenius Performance Manager Servers, is often deployed in a distributed manner. When implemented, the Global Manager serves as the master to the local servers or slaves where information between the two (or more servers) can be shared and accessed seamlessly to provide both real-time analysis and historical reports. Most importantly, the integrated nGenius Solution lets IT professionals carry out critical performance management tasks, including performance analytics, application and network monitoring, capacity planning, network troubleshooting, fault prevention, and service-level management. The nGenius Standby Server acts as a backup to the primary nGenius Server, allowing you to continue to monitor your network's performance in the event the primary nGenius Server fails.

How It Works

As noted previously, the nGenius Standby Server implementation includes a primary and backup nGenius Server. Every fifteen minutes, all the monitored elements and configuration settings are replicated from the primary server to the backup server, including settings for devices, users, global settings, and other configuration data. Historical data for reports is submitted to the backup server on a 15-minute basis while property files are copied to the backup server once a day.

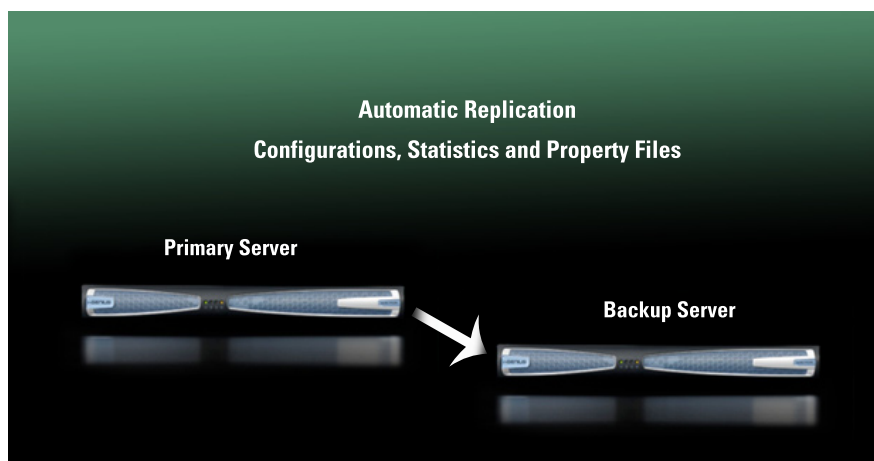
Should the primary server fail or go offline for any reason and the Standby Server does not receive its regularly scheduled 15 minute update, it sends an alert to the designated network managers. If the network manager determines that the primary server is inoperable, the standby server can be engaged to carry out all of the primary server's responsibilities without any loss of service or data that the primary server routinely logs and stores.

Deployment Options

The nGenius Performance Manager Standby Server supports several different deployment scenarios. Some of the potential disaster recovery scenarios include positioning the Standby Server:

- At a peer or redundant data center or a backup network operations center to which IT staff shift control and management of their networks and IT systems during a disruptive event, e.g., a power outage, natural disaster or other site-level failure
- At a geographically distant third-party back-up site hosted by a business continuity service provider
- Co-located with the primary server for onsite redundancy in case of a localized server hardware or database failure

Figure 2. How Standby Server Works



While maintaining normal network and application performance management activities, the Standby Server engages in periodic look backs to the primary server. If it detects that the primary server is on-line, it alerts the network team to make the decision of when to return ongoing operations to the primary server.



About NetScout Systems

NetScout Systems provides advanced network and application service assurance solutions that deliver complete visibility into real-time, packet/flow-based operational intelligence. IT operators at the world's largest enterprises, government agencies, and service providers use the Sniffer and nGenius solutions to troubleshoot service degradations faster and more efficiently in order to reduce MTTR.

Our world-renowned Sniffer and nGenius solutions include:

- Intelligent Data Sources for high capacity, deep-packet recording and monitoring
- Analysis Software for real-time and historical network and application performance management, troubleshooting, capacity planning, and reporting
- Advanced Intelligence for early detection and in-depth analysis of complex or specialized application services
- Comprehensive, global support, consulting and training services

Corporate Headquarters

310 Littleton Road
 Westford, MA 01886-4105
 Phone: 978-614-4000
 Toll Free: 888-999-5946
www.netscout.com

European Headquarters

NetScout Systems (UK) Ltd.
 100 Pall Mall
 London SW1Y 5HP
 United Kingdom
 Phone: +44 (0)20 7321 5660

Asia/Pacific Headquarters

Room 105, 17F/B, No. 167
 TunHwa N. Road
 Taipei, Taiwan
 Phone: +886 2 2717 1999
www.netscout.cn

©2008 NetScout Systems, Inc. All rights reserved. NetScout, the NetScout logo, Network General, the Network General logo, nGenius, Sniffer, InfiniStream, Business Container, Business Forensics, NetVigil and Quantiva are trademarks or registered trademarks of NetScout Systems, Inc. Other brands, product names and trademarks are property of their respective owners. NetScout reserves the right, at its sole discretion, to make changes at any time in its technical information and specifications, and service and support programs. AN0908-11revA