

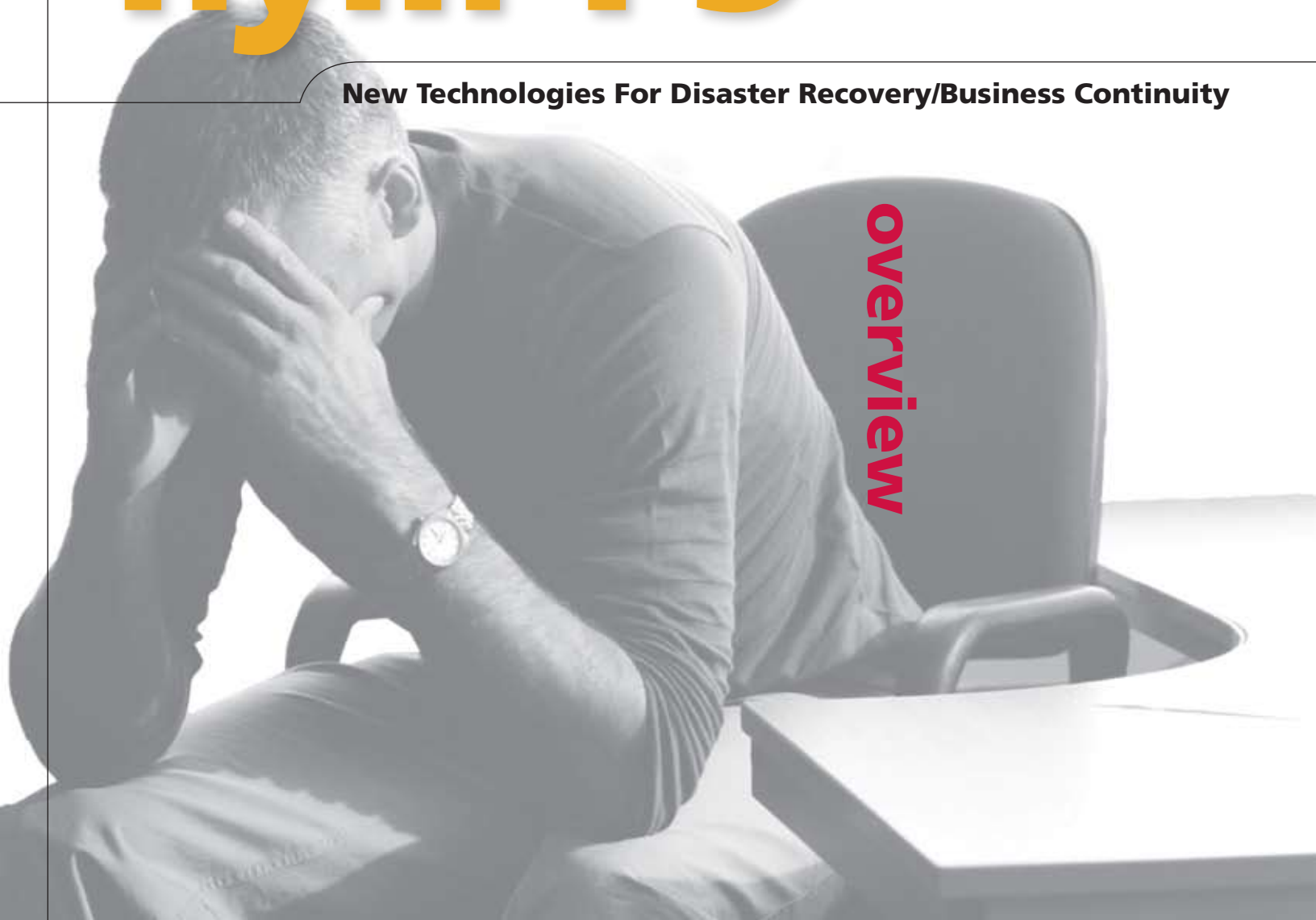


courtesy of
F5 NETWORKS

f.y.i. F5 | guide 1

New Technologies For Disaster Recovery/Business Continuity

overview



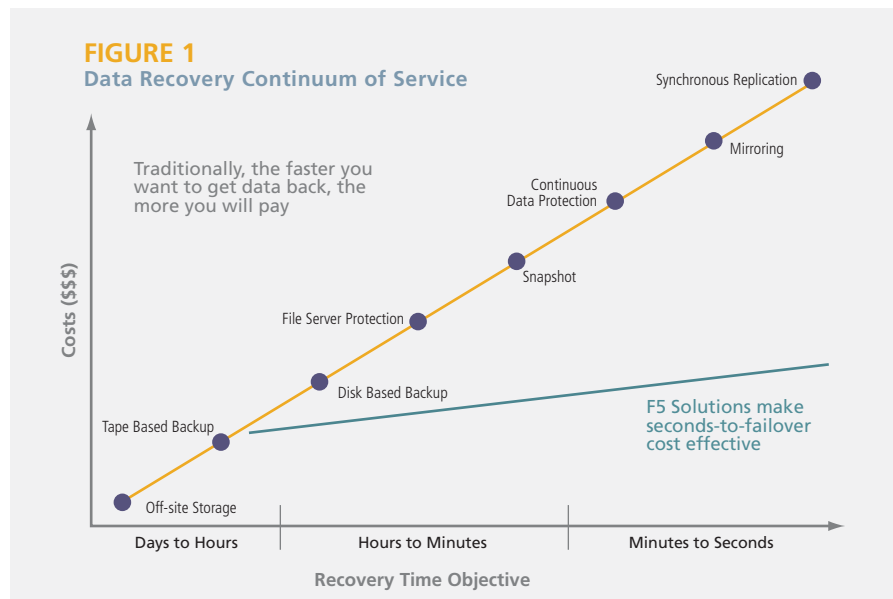
Business Continuity, Disaster Recovery and Data Center Consolidation

IT managers today must be ready for the unexpected, especially in consideration of new industry and government rules concerning data protection and disaster recovery. Disaster recovery initiatives, of course, have been around for some time; however, it is only recently that several new technologies have emerged that are changing the way we think about disaster recovery and business continuity planning. These technologies focus on WAN optimization, traffic redirection, data replication, and secure remote access. Together, they represent a new methodology for organizations seeking to consolidate cost and equipment, reduce management time, and ensure applications are always available when disaster strikes.

The Recovery Time and Recovery Point Objective

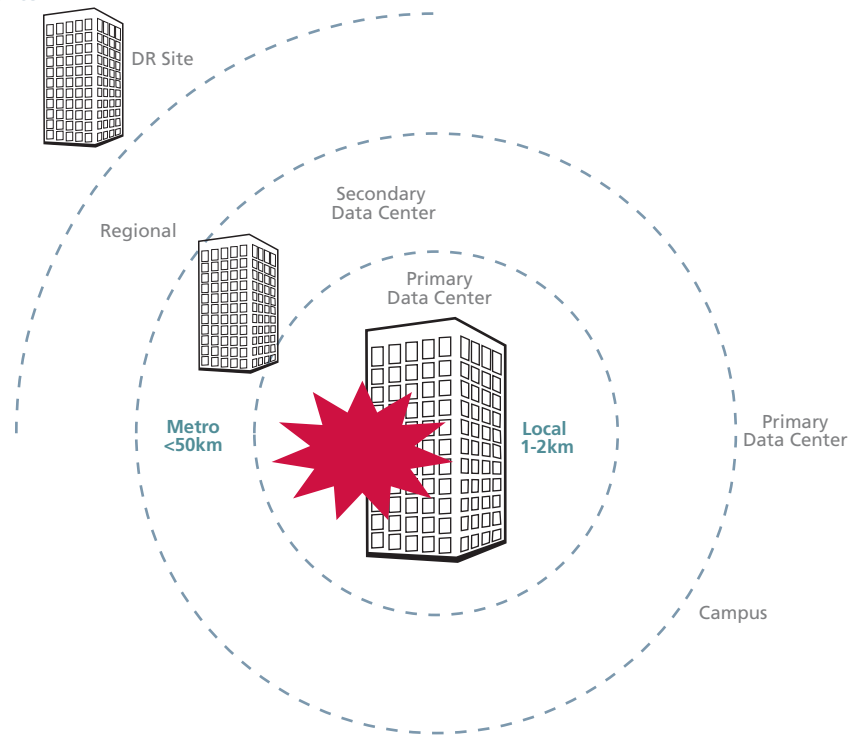
What You Need To Know

The recovery time objective (RTO) is the maximum allowable downtime after an outage for recovering systems, applications, and functions (see Figure 1). RTO provides the basis for developing cost-effective recovery strategies and for determining when and how to implement these recovery strategies during a disaster situation.



Source: Network World, The New Face of Disaster Recovery, 050806

FIGURE 2
The Disaster Radius of a Data Center



The Disaster Recovery Continuum of Service – The Faster You Want Data Back, The More You’ll Pay

The recovery point, for example, defines how current the data is after a disaster. The **recovery point objective** (RPO) is the earlier point in time to which systems and data must be recovered after an outage. RPO defines the maximum amount of data that your organization is willing to sacrifice after a disaster; i.e. a zero RPO business continuance solution can survive a disaster without any loss of data.

Together, RTO and RPO provide a measurable target for your business continuance and disaster recovery solution to achieve. Improving RTO and RPO requires increasing your investment in networking and storage technologies and processes. Also, the physical distance between your data centers and how well your applications tolerate network latency affects how close you can get to zero RPO. That is why you should limit your RTO and RPO to whatever levels your organization can effectively tolerate.

Disaster Radius

The probable distribution of a disaster, called the *disaster or threat radius*, also affects the business continuance solution. The probability and extent of damage from earthquakes, floods, fires, hurricanes, cyclones, or terrorist threats varies according to the region in which the data center physically resides. To be effective, the backup site must not be within the disaster radius (see Figure 2).

Defining the disaster radius may be more complicated than identifying a limited geographic region. For example, an earthquake might destroy both primary and secondary data centers if a major fault line connects them, even though they are geographically separated. Many enterprises adopt a multi-hop strategy to be safe, using two data centers separated by metro distances and a third site located out of the region.

Many enterprises adopt a multi-hop strategy to be safe, using two data centers separated by metro distances and a third site located out of the region.

Business Continuity Planning

Trends You Should Be Aware Of

The results from both a 2004 IDC study and a current study highlight a continuing trend among companies looking to reduce overall downtime and increase overall availability. Through business continuity planning, the change in downtime over a four-year period has dropped more than 53% from 20.4 hours in 2003 to an expected 9.5 hours in 2007. This converts to a shift in availability from 97.2% to 98.7% over the same period. When these results are viewed with regard to business impact, adding nearly 11 hours of monthly “uptime” converts to 132 hours annually, or 5.5 24-hour days. This additional amount of time could translate to a significant amount of potential revenue loss were your company not able to meet these higher-availability requirements.

Additionally, as you look to increase the availability of your IT environments and business processes, you will need to integrate more advanced means of achieving these results. The impact of reaching these high-availability goals will likely require greater levels of expertise, automation, and, ultimately, capital investment.

Disaster Recovery Planning

What Should Your Plan Include?

A Disaster Recovery Plan covers the data, hardware and software critical for a business to restart operations in the event of a natural or human-caused disaster. It should also include plans for coping with the unexpected or sudden loss of key personnel. The analysis phase in the development of a BCP (Business Continuity Planning) manual consists of an impact analysis, threat analysis, and impact scenarios with the resulting BCP plan requirement documentation.

Impact Analysis

An impact analysis results in the differentiation between critical and non-critical organization functions. A function may be considered critical if the implications for stakeholders of damage to the organization resulting are regarded as unacceptable. Perceptions of the acceptability of disruption may be modified by the cost of establishing and maintaining appropriate business or technical recovery solutions. A function may also be considered critical if dictated by law.

Next, the impact analysis results in the recovery requirements for each critical function. Recovery requirements consist of the following information:

Threat analysis

After defining recovery requirements, documenting potential threats is recommended to detail a specific disaster’s unique recovery steps. Some common threats include the following:

- Natural disasters
- Fire
- Power failure
- Terrorist attacks
- Organized or deliberate disruptions
- System and/or equipment failures
- Human error
- Computer viruses
- Legal issues
- Worker strikes

Impact Scenarios

All threats in the examples above share a common impact: the potential of damage to organizational infrastructure, except one (disease). The impact of diseases is initially purely human, and may be alleviated with technical and business solutions. During the 2002-2003 SARS outbreak, some organizations grouped staff into separate teams, and rotated the teams between the primary and secondary work sites, with a rotation frequency equal to the incubation period of the disease. The organizations also banned face-to-face contact between opposing team members during business and non-business hours. With such a split, organizations increased their resiliency against the threat of government-ordered quarantine measures if one person in a team contracted or was exposed to the disease.

60 percent of enterprise data is being stored outside the data center and up to 75 percent of that data is unprotected.

Data Center/Server Consolidation

Overview and Benefits To Your Business

Data Center Consolidation is an approach to optimizing technologies in one or more data centers to achieve cost savings, improve performance, and mitigate risk. This approach involves planning, optimization and physical migration of systems and facilities.

Data Centers and the Data Storage Dilemma

A recent study conducted by Santa Barbara, California-based Strategic Research Corporation revealed that over 60 percent of enterprise data is being stored outside the data center and up to 75 percent of that data is unprotected. According to the study, this is a risky practice because "edge data" can be as critical to a company's survival as its more closely managed centralized data. Finding an efficient and effective way of protecting data at remote offices has been one of the most difficult issues facing IT managers to date. Some of the major issues in this area include:

The high cost of maintaining tape devices, including:

- Tape hardware and software, which may range from \$5,000 to \$20,000 or more
- Operational costs of maintaining remote backup equipment
- Third-party services to manage tapes and the backup process

Inconsistent backup execution:

- Remote employees are not professional IT staff
- Remote office employees are busy with full-time jobs
- Remote employees may not be able to execute the backup process consistently

The difficulty of implementing network-based backup:

- Existing WAN links too slow
- Too much data in remote servers
- Network-based backup causes network congestion, slowing down main application servers

Leading drivers for server consolidation have been:

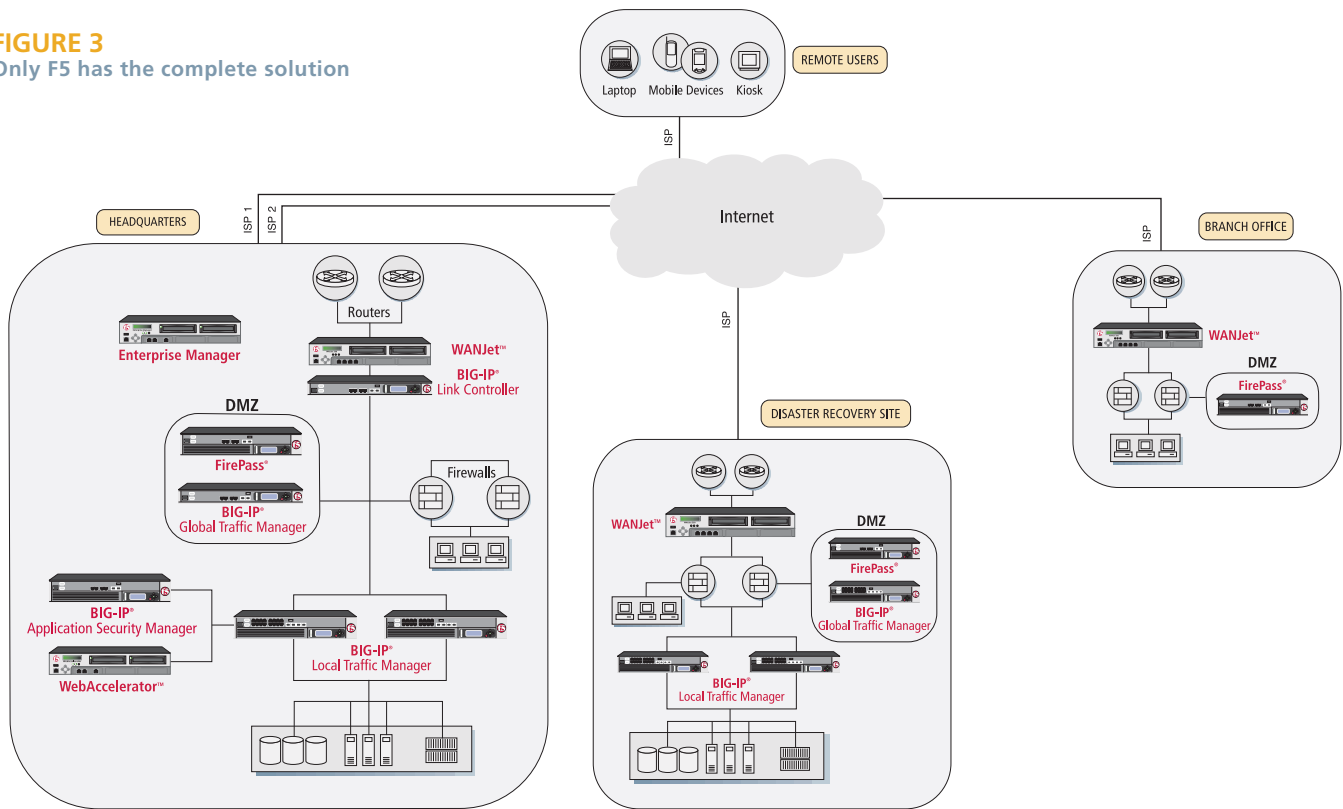
- Improving TCO and taming server sprawl
- Easier day-to-day management of upgrades, reconfigurations, fixes, workload balancing and backup, coupled with more-effective use of CPUs and storage
- Business unit management is also providing an impetus toward consolidation. Many distributed systems are managed part-time by end users, causing end-user frustration and negatively affecting end-user productivity levels.

Although reduced TCO remains a major reason for server consolidation, we are seeing a change indicating there is more interest in consolidation to provide better service, systems management and improved agility. Unconstrained storage growth, increasing retention periods, and low utilization rates have brought storage provisioning to the forefront of operational problems. Consolidating storage moves provisioning from the server to the application or infrastructure.

This creates enormous opportunities for improving staff productivity asset management and meeting ever more stringent service level agreements (SLA) and regulatory requirements. It also provides the predicate for IT organizations to evolve from an infrastructure centric focus to a more services oriented focus. Externalizing storage eliminates the "busy work" associated with doing server upgrades configured with internal storage.

The bottom line? You need to ensure that the major reasons for your server and/or storage consolidation project are clearly understood so that proper goals and objectives are defined and appropriate measurement objectives are set to measure your success against your objectives.

FIGURE 3
Only F5 has the complete solution



Putting It All Together

F5's portfolio of products represents a comprehensive solution that allows you to achieve their Business Continuity, Disaster Recovery, and Consolidation goals.

Business Continuity/Disaster Recovery

F5 products can be used in business continuity and disaster recovery plans. F5's BIG-IP Global Traffic Manager (GTM), BIG-IP Link Controller (LC), and BIG-IP Local Traffic Manager (LTM) are best-of-breed solutions for delivering failover of downed systems. This covers both intra-data center recovery and disaster recovery across multiple data centers. Deploying these solutions can help organizations achieve the best RTO (Recovery Time Objectives) and better RPO (Recovery Point Objectives).

In addition, F5's WANJet product provides speedy replication of data across data centers to ensure database and application integrity during failovers. And F5's FirePass SSL VPN provides remote access to users that typically access their "home" site, but due to the disaster now must remotely access the backup site.

Data Center Consolidation

Consolidation of servers requires effective and efficient load balancing of servers; F5 offers the BIG-IP LTM to achieve this. Increased availability is also key behind consolidation; F5 offers advanced high availability products including BIG-IP GTM, BIG-IP LC and BIG-IP LTM. Finally, increased security through consolidation means protecting the access to applications; F5 offers FirePass SSL VPN and the Application Security Module for these purposes.

Mitigating disaster – including natural disasters, fires, power failures, terrorist attacks, human error, and computer viruses – requires the deployment of mission critical applications in redundant data centers. At least two data centers, geographically distributed (i.e. one in the U.S., one in Asia) should be made available. Each data center should be multi-homed. Common product requirements include ones that provide Global Traffic Management, secure remote access for users, protection of applications exposed to public networks, timely application state sharing (i.e. database replication) between data centers, and LAN-like performance over the WAN.

Only F5 has a complete, comprehensive suite of solutions that mitigate the effects of disasters on enterprise networks.

Steps You Can Begin To Take Today

Applications represent the life blood of any business. There are several steps you can take to ensure a successful recovery of your business critical applications.

- Inventory your application and determine a Recovery Point Objective and Recovery Time Objective for each.
- Consider what the response would be to environmental disasters, disruption of services, loss of utilities and system failure.
- Select a person who will administer the disaster recovery and business continuity plan.
- Communicate and train staff on the business continuity process.
- Document the business continuity plan and store a copy in an off-site location.
- Test the disaster recovery plan, backups, and recoveries to ensure they work properly.
- Re-assess and update the plan regularly.

