Issue Date: Open Systems edition
June | July 2006

Making Preparations

Jaqui Lynch
jaqui.lynch@mainline.com

Disaster-recovery planning points to ponder

In the past few years, disaster recovery (D/R) has become more important than ever before to annual planning. We've always paid attention to it but now, given recent events and new laws, it has become more critical. This article outlines some of the basic points to consider before jumping into the technology behind D/R.

D/R is defined as the ability to meet your business needs for recovery in a predetermined manner and timeframe. This doesn't mean that every application or server has to fail - it means you must be able to conduct day-to-day business in some manner.

Issues to Consider

To have a decent plan, it's important to first analyze what level of D/R is needed by each component of the business. This means conducting a risk analysis for every function, including each individual application. For example, if business continuance depends on the ability to get a tape from your current datacenter to the D/R site, how are you going to accomplish that?

It's important to understand what you're trying to accomplish. If it only matters that you can take in cash and give out product, then the issues you have to consider are quite different than if you have to perform other functions. But, keep in mind you may have to move locations if the area is badly damaged, and you may also find that your employees are more concerned with protecting their families and finding food than they are with work. I've seen many D/R plans that depend on the ability to use current local employees, either by having them come into work locally or flying them to another datacenter. Yet, these plans fail to take into account what would happen if these people were unavailable or if there was no way to get them to work. These are important issues to consider for inclusion in a D/R plan.

Other areas where I've seen D/R plans fall down relate to money and legal issues. It's important to have access to cash in case you have to move people around or feed people, yet few companies have ready access to cash in these cases. In a true disaster, credit-card machines won't be operational and any vendors still functioning will require cash. Additionally, looters are a problem, so robust security is important.

Finally, many of us sign contracts with companies that make certain guarantees for equipment, etc., in the case of a disaster. However, it's important to make sure that you cover the following in those contracts: A) Where is your company in the priority scheme if this is a major disaster? B) Does the vendor have enough equipment to handle multiple companies at a time? C) What guarantees are the vendor making?

As far as the contracts go, it's important that copies are lodged with a lawyer somewhere near the D/R site and that those responsible for enacting the disaster plan know which law firm has the copies and where the firm is located. Further, the law firm must know it's authorized to act. These issues may seem obvious, but they're often forgotten because companies are so focused on the technology. In the long run, these issues are likely to cause more problems than the technology ever will.

D/R planning should also take into account planned and unplanned outages, not just full disasters. Servers require maintenance and firmware updates. These should be included in the plan, along with details on how to test after changes are made and how to recover if issues arise.

Disaster Recovery Types and Terminology

Even before you start to examine technology, it's important to understand the kind of D/R that will work for you. It's important to understand the different kinds of D/R that are available. D/R can be handled in many different ways - options include within a site and site-to-site. Within each of those, the D/R could be server-to-server or LPAR-to-LPAR. Additionally, sites can be cold sites with nothing except the required planning and basic infrastructure, warm sites with equipment that doesn't normally run anything, or hot sites where the equipment runs all of the time.

The highest and most expensive are fault-tolerant systems. These are extremely redundant and operate without interruption. When one site goes down, the other is already running and picks up the workload. This type of D/R requires a hot site where the failover servers are running the application live. It's rare to see this kind of D/R within a site - it's normally a site-to-site

D/R, although it may be server-to-server or LPAR-to-LPAR D/R between sites.

High availability (HA) clusters are the next level down. They use hardware and software to automate recovery with minimal downtime. Hardware is redundant and data is mirrored. Some companies implement HA clusters within a site and others use it between sites. Depending on the complexity and technology, an outage still occurs, but it can be as low as three minutes. HACMP* can now be integrated on the IBM* System p5* 590 or System p5 595 with capacity-backup solutions. In the case of the System p5 590, a server can be purchased for the D/R site that has four active and 28 inactive processors. The active processors can be used at all times, but the inactive ones can only be used in a disaster, for production role swapping during unscheduled outages or for failover testing. When combined with HACMP, the activation of the inactive processors during a failover can be automated. IBM offers several capacity-backup offerings for the System p5 595 with four active processors and either 28 or 60 inactive processors onboard.

At the lower end of the scale, the options include enhanced-standalone or pure-standalone recovery. This may be as simple as bringing up an LPAR and pointing it at a duplicate of the data if the storage area network (SAN) is replicated, or it may involve going to the last full backup.

Once the workloads are analyzed and the recovery type needed for each is known, it's wise to categorize the type of D/R necessary for each workload (see Table 1).

Consider All of the Factors

Clearly, many factors must be considered when planning for D/R. These include technological, personnel, financial and legal issues. A good disaster plan includes all of these factors, but also takes into account change control, backups, maintenance windows and a test plan. A D/R plan is only as good as its last successful test, so be sure to test your plan regularly. I recommend at least quarterly, but testing requirements vary from company to company. D/R planning and testing require a significant investment in time and money, but that investment will prove itself worthwhile if the plan ever has to be enacted.

Table 1

	Downtime	Data Available	Cost
Standalone	>=2 days	Last full backup	Inexpensive
Enhanced Standalone	>=2 hours	Last transaction	Relatively inexpensive
HA Clusters	About 3 minutes to 3 hours	Last transaction	Expensive
Fault Tolerant	Never stop	No loss	Extremely expensive

Jaqui Lynch, *a technical editor for* IBM Systems Magazine, Open Systems edition *and senior systems engineer focusing on System p5 and Linux at Mainline Information Systems, has worked in the IS industry for more than 26 years.*