Disaster Recovery Requirements Analysis

By Stan Stringfellow - Special to Sun BluePrints™ OnLine

Sun BluePrints™ OnLine - July 2000

http://www.sun.com/blueprints

Sun Microsystems, Inc.
901 San Antonio Road
Palo Alto, CA 94303 USA
650 960-1300 fax 650 969-9131

Part No.: 806-6196-10
Revision 01, July 2000

Please
Recycle

Disaster Recovery Requirements Analysis

This article is derived from the upcoming Sun BluePrints™ book *Business Continuity Planning with Sun Microsystems Technologies*.

Scenario

A disaster recovery plan typically involves deploying a remote failover architecture which allows a secondary datacenter to take over mission-critical operations in the event that a disaster strikes the primary datacenter. There are many technologies that can be used to implement a remote failover architecture including tape shipments, campus clusters, and WAN replication on the database transaction level or disk I/O level. Typically, IT offers a variety of solutions that can be tailored to the needs of individual business units and negotiated on an application-by-application basis. IT must carefully and exhaustively analyze disaster recovery requirements to assure that its service level agreements can be met.

This article provides a form that IT can ask its customers to fill out. This form can serve as the basis for an iterative negotiation process that helps all parties to arrive at realistic expectations and well-understood disaster recovery service level agreements.

Disaster Recovery Service Levels

Disaster recovery (DR) service levels establish priorities for recovering IT services in the event of a disaster. Typically DR service levels are negotiated on a per application basis. The service level classifications shown below are used by a major financial services corporation which is a customer of Sun Microsystems, Inc. The company asked to remain anonymous, so this article refers to it as the company.

TABLE 1 DR Service Levels

DR Classification	Time to Recover	Acceptable Data Loss (from Time of Failure)	Typical Implementation
AAA	Four Hours or Less	Maximum one hour	Database Replication and/or Network Mirroring
AA	Four to 12 Hours	Four hours	Standby Database or tape shipment
A	12 to 24 Hours	24 hours	Usually restore from offsite backup
B	24 to 72 Hours	24 hours	Always restore from offsite backup

For example, the company supports Web applications that interface with employees and customers. These applications are used for purposes such as training. The applications are distributed, and a user can simply be routed to a different datacenter in the event of a disaster. This is an example AAA application that supports virtually instantaneous failover.

The company uses a different type of AAA implementation to support applications such as Oracle® Payroll and Hughes Electronic Payroll. In these cases, production databases are deployed at one datacenter, and hot standby databases are setup at a remote datacenter. Archive logs are copied over via a WAN, and the standby databases are rolled forward to keep them about one hour behind the production database. In the event of a failure or disaster, the company can simply apply latest archive logs, and quickly failover the application to the DR site.

The company has very few AA applications. One example is a workflow system. The storage volumes—such as VERITAS Volume Manager volumes—are laid out in advance to support this application. IT keeps the application binaries synchronized across the sites. For example, when binaries are changed, the changes are implemented at both sites. Copies of tapes are shipped from the primary site to the DR site. But the company does not restore those tapes until a disaster occurs (or until the next DR validation test is performed). Note that this approach can only be

used if the data can be restored from tape quickly enough. For example, it may be necessary to restore from tape in less than eight hours in order to meet the 12 hour recovery time requirement. Thus, it might be necessary to use fast tape drives at the DR site, possibly in conjunction with striped tapes to increase the bandwidth.

For single A applications, IT does not necessarily lay out the storage volumes at the DR site. But, they keep current and accurate documentation at the DR site (in hard copy format) that describes the storage layout. The binaries for the operating system and applications are installed, although they may not be in use since the DR machines are normally used for other purposes such as software development. Tapes containing data that is current to within 24 hours are kept at the DR site (and at an offsite storage vendor). As with the AA solution described above, this approach can only be used if the data can be restored from tape quickly enough. For example, to restore the application to production status within 24 hours, it may be necessary to restore the data from tape in 12 hours.

For B applications, the binaries for the application and operating system may not be installed, and the storage volumes may not be laid out. But, IT keeps tapes at the DR site, or at an offsite vendor where the tapes can be transported to the DR site quickly. All procedures for re-installing and configuring the system are documented at the DR site (in hard copy format).

Requirements Analysis Form

The following form is used by the company to determine the disaster recovery requirements on an application-by-application basis when negotiating service levels with the business units. The goal is to determine all of the application requirements before the DR solution is deployed so that there are no surprises later. IT works through several iterations with the customer before implementing the solution. This has worked out well at the company. The comments embedded in this form convey the experiences of the company.

1. Which disaster recovery (DR) classification is required for this application?
   - AAA
   - AA
   - A
   - B

   Comments: It is important to establish the DR service level that will be required for the application. If the customer requires an AAA solution, IT must find a way to recover the data as quickly as possible. If the customer only requires a B solution, then IT attempts to find the most cost-effective solution that meets the requirements. After considering the real costs involved, the customer may find that they cannot afford the desired solution, and a lower service level may have to be negotiated.

2. How much data can the business afford to lose? That is, how current must the data be after it is recovered?

   Comments: This information determines the implementation method and whether additional network bandwidth will be required. This question helps IT to make decisions such as whether to deploy a standby database, a network replication technology, or a tape-based solution.

   Normally, the first two questions go hand in hand. For example, if the data is very critical, then the customer probably can't afford to lose any data at all.

3. How much degradation in performance is acceptable to the business during a disaster?

   Comments: This is important because IT doesn't want to support 100% of machine capacity at the DR site. Often, the answer is 50% of the production capacity. This is because a disaster is not considered likely to happen. If a disaster is declared, it is possible to temporarily run at 50% of the production level. For extended disasters, agreements can be put in place with external vendors to upgrade the systems as soon as possible—sometimes within 48 hours. It is also possible to use a "capacity on demand" approach—where servers are sold with greater capacity (e.g. more CPUs) than the customer needs to deploy initially, and the customer only pays for the capacity that they actually use. In this situation, servers at the DR site can be upgraded immediately in the event of a disaster.

4. When do you need DR to be in place for this application?

   Comments: This question is requesting a start date. Some application groups need to have DR in place the day the application goes into production. Other groups decide to wait until the bugs are found and fixed in the production system before implementing the DR solution. Why take the latter approach? Because the problems that are fixed in production system must also be fixed in the DR environment. Some application groups do not want to implement all such changes two times. They prefer to stabilize the production system before implementing DR.

   For example, if an application goes into production and problems are found with the database, it might be necessary to add tables, change the database structure, and so forth. If the application is implemented simultaneously on the production site and the DR site, this effort must be applied at both sites. Because of this, less concentrated resources are available for developing the production environment.

   On the other hand, senior management may demand that DR be put in place before an application is deployed. This depends on the business unit and how much they are willing to invest in the development effort. If a single person is implementing both the production and the DR version of the application, the DR effort is likely to be delayed because the business is waiting for the application to go to production. If more people can be allocated, it may be possible to implement both sites in parallel.

5. How often should IT validate the DR architecture for this application?
   - Quarterly
   - Semi-Annually
   - Annually

   Comments: Normally, DR is tested quarterly at the company. There are some applications of lower priority that are tested annually. This question is used to project the level of resources that must be allocated to DR testing for this application. DR testing requires is a very resource-intensive effort. It involves many groups: operating systems support, database support, middleware support, application support, personnel who monitor the batch cycle and support the scheduling system, and personnel who support the backup system. IT needs to know when testing will occur so that it is possible to schedule human resources appropriately.

6. Does this application send data to or receive data from other applications?
   - Where does the data come from or go to?
   - How is the data transported? (E.g., Ethernet, FDDI, Token Ring)

   Comments: Some applications at the company support transmission feeds between mainframes and UNIX® operating system, or between an external bank and the internal systems.

   Sometimes data might be exchanged via tape. The tape format must be supported on the DR machine. For example, if 9 track is used, the DR machine must support 9 track tape. If DLT is used, the DR machine must support DLT tape.

   Another way to exchange data is via a network, perhaps through Ethernet or Fast Ethernet using FTP. But, there are other applications at the company that exchange data with external banks through SNA, serial ports, and other types of networks. The required technology must be set up on the DR system, because there is no single card or adapter that will accommodate all of those types of feeds.

7. What kind of database does this application use? (E.g., Oracle, Sybase, Informix, DB2)

   Comments: This impacts the level of computing resources that must be allocated to the DR machine. It also has implications regarding the recovery method that can be used. For example, if the customer requests a standby database and the database is implemented in Informix, then IT might not accept this since they usually only support Oracle applications in standby mode.

8. How big is the database now? How much will it grow in the next six months?

   Comments: The six month period is used for near term growth. This is the normal planning process at the company. It requires a significant amount of time to acquire and configure storage products.

9. How does the database update its information? (E.g., Online, Batch, Feeds)

   Comments: The method that is used to update the database must be accommodated at the DR site. For example, if an application uses a batch cycle, the scheduling system must be setup to run the same cycle at the DR site. If the database is updated through a middle

tier or online client, then the same technologies must be available at the DR site. This is especially true for a middle tier service. Many of the clients at the company are desktops, and they access databases via a middle tier application server. Middle tier servers are often Web-based, and many tools are added in the middle to route transactions that originate from the online user. The implementation must be duplicated at the DR site.

10. If data loss occurs after a disaster, is there a way to re-enter the data into the database via OLTP, Batch, Feeds, or other methods?

11. If network bandwidth must be allocated to support a standby database, what is the average rate at which the archive log grows (in MBytes per hour)?

    Comments: The company typically sets up standby databases to use one archive log per hour. So if the answer to this question is 250 MBytes per hour, the network must provide that much bandwidth.

12. Which database instances must be recovered in a disaster scenario?

    Comments: Not all databases must be recovered for the business to continue functioning. For example, some applications at the company support a reporting database which can be easily recreated from the production database. The reporting database may be a read-only duplicate of the production database. So in DR scenario, the production copy of the database can also be used as the report database. Performance may be degraded somewhat in this situation, but this may be acceptable during a disaster.

13. What file systems are required by the application? (Include file systems for software products, application binaries, external feeds, and so forth)

14. How do clients access the production system? How should clients access the system in a disaster scenario?

    Comments: IT must understand how the client establishes a connection with the production site so that the DR site can be configured in the same manner (or in a way that is appropriate for a disaster scenario).

15. What software is required by the application? (E.g., Oracle, Syncsort, and so forth)

    Comments: This question is primarily concerned with software licensing issues for the DR site. Many vendors provide licenses for DR functions free of charge, but some do not.

16. Are there any unrecoverable database activities performed by the application that will prevent IT from restoring the database and rolling it forward?

    Comments: If unrecoverable commands are used in a batch cycle or in day-to-day operations, it is not possible to recover that database at the DR site. With Oracle, table truncation and table drop operations probably cannot be recovered at the DR site. There are two possible solutions. The developers may be able to recode the application. Alternatively, IT may have to create backups at very specific points in time to capture the data in a state that it can be replicated at the DR site. In most cases, if the application

performs unrecoverable actions, it is not possible to guarantee recovery of the database at the DR site. So, it is important to know this in advance, and to devise the DR architecture to address it.

Operations such as table drop are not recorded in Oracle archive logs, and are not reproduced when archive logs are rolled forward. Programmers may use these types of operations for performance reasons. For example, it is significantly faster to drop a table and recreate it, than it is to delete a large number of rows, since every deletion must be logged in the archive log. If the application drops a table at a certain point in time, it may be necessary to stop the application and capture a backup image at that point. There may be performance tradeoffs for any approach that is taken.

17. If developers normally use the machines that are designated as alternate servers for DR, will the development environment need to be up and running during a disaster.

    Comments: This affects system sizing. If the customer requires development and DR to run simultaneously, greater server capacity is required.

    In addition, some applications are not sophisticated enough to isolate development from DR or production. These applications might use the same filesystem name for development and production. In this case, when IT lays out the production environment on the DR machine, they overwrite the development environment. It is necessary to know about this in advance so IT can advise the customer to use different directory structures for development and production.

For your convenience, the following URL contains a printable version of the DR requirements analysis form, `www.sun.com/blueprints/tools`

Conclusion

To successfully implement a disaster recovery program, IT must negotiate realistic DR service levels with its customers on an application-by-application basis. This necessitates careful and exhaustive disaster recovery requirements analysis. We have looked at the definitions of typical DR service levels—AAA, AA, A, and B. And, we have examined a form that can be used to evaluate and negotiate DR costs and infrastructure requirements.

Author's Bio: Stan Stringfellow

Stan Stringfellow is an independent author, technical writer and software developer who is currently doing work for the Sun BluePrints program. He holds a B.A.C.S. from UC San Diego and has written many manuals including the original software manuals for the Sun Enterprise™ 10000 (also known as Starfire™) server. He may be contacted at stan@stringfellow.com.