Module 7: System Component Failure Contingencies

Introduction

The purpose of this module is to describe procedures and standards for recovery plans to be implemented in the event of system component failures. The procedures described provide a structured recovery plan that is well documented and ready for execution when such extraordinary events occur.

Note: This module is **not** intended to document disaster recovery plans for catastrophic situations at the Production Center at DB300.

In such a recovery plan, two elements are necessary:

1. The parties responsible for particular components must know what management and users expect of them.
2. Interdependent groups must know what their expectations of each other should appropriately be.

For a failure contingency plan to be effective, it needs to be well documented and tested so that less time is spent figuring out the best way to invoke the contingency. From time to time, it also needs to be tested with each institution during normal operations so that we can have confidence that the contingency works and all parties involved have worked out any kinks in the process.

Topics include:

- Servers
- System Software and Databases
- Networks
- Workstations
- Printers

Topic One: Servers

UNIX Servers

There are a total of six (6) Banner UNIX servers designated for Production Services, as shown in the figures below.

Comment: (Mark to provide updated dirgram for Banner environment.)

These machines are under a 24 hours a day, 7 days a week, maintenance agreement with a four hour response time.

In order to limit the impact that any hardware failure will have on production services, the servers are configured as follows:

1. Each server's system disk is mirrored onto a spare disk using Hewlett-Packard (HP)'s MirrorDisk/UX software.

2. Each server's database volumes are located on an EMC Symmetrix Enterprise Storage System, which internally mirrors those volumes.

3. Each server is connected to the EMC Symmetrix system by a redundant path. If one path to the EMC fails, the HP/UX operating system will automatically use the other.

4. A control and backup server has redundant connections to all of the EMC disk paths, which provides access to all of the server's databases from a central location.

5. All tiers of the application have automatic failover except the database tier. The firewall, the load balancer (F5), and application servers are all running on more than one device. If one of these devices fails the entire application will continue to run. In the case of the application servers, the load on the remaining servers will be higher and might cause some application slowness.

   If a database server fails, manual failover will be carried out. In the initial Banner Hosting configuration for 6 schools, there are two database servers. Each server runs 3 databases. If one server fails its three databases will be manually moved to the other database server. This will increase the load on the remaining database server but the application should continue to run.

6. System backups to tape are completed nightly, 7 days a week, 365 days a year.

7. The production Oracle instances are running in **archivelogmode**, where daily transactions are periodically saved throughout the day, which allows for recovery up to the current point in time. The combination of archive logs and routine backups provides numerous data recovery options. In the worst case, a full restoration of a daily backup may be required.

Comment: George to review and comment. George confirmed as accaurate.

8. User access to the databases is handled through DNS, so that databases can be moved from one server to another without any required changes to application configuration.

Comment: Mark to provide updated paragraph.

UNIX Server Backups

As noted above, the production Oracle instances are running in **archivelogmode**, where daily transactions are periodically saved throughout the day, which allows for recovery up to the current point in time. In addition, HP's Data Protector software runs nightly, 7 days a week, 365 days a year, to back up the UNIX servers.

Backups are divided into three groups, each with their own archive schedule:

1. Production Databases and Systems are scheduled as follows:
   - Daily Full Backup, each kept for 7 days
   - Weekly Full Backup, each kept for 4 weeks
   - Monthly Full Backup, each kept for 4 months

2. Non-Production Databases and Systems are scheduled as follows:
   Daily Full Backup, each kept for 7 days

This combination of archive logs and routine backups provides numerous data recovery options, up to and including a full restoration of an institution's daily transactions.
On a weekly basis, both Weekly and Monthly back-up tapes are moved to the UGA Data Center from the OIIT DB 300 Data Center, so that these back-up tapes will be in a location separate from the source data in case of an emergency.

Disaster Recovery for the Banner Environment

If one of the UNIX servers should suffer a hardware failure, we would take the following actions:

1. Evaluate whatever error messages were presented.

2. If the failure is not recoverable without HP support, we would call and provide them with all the information about this event.

3. If HP believes that a solution is available and can be implemented in a timely manner, we would follow their directions and implement the solution as quickly as possible.

4. If the nature of the problem or the application processing schedule does not allow timely HP repair, we would evaluate interim recovery options. Since the databases and other application files, as well as the operating system files on each server, are being backed up regularly, and the production Oracle instances are also running in the archive log mode, we have numerous data recovery options.

   These may include restoring data from tape and/or Oracle archive logs, moving Oracle database instances from one server to another, or reallocating disk assignments within the EMC array from one server to another.

5. In the event that we need to move Oracle database instances from one server to another, the Banner system administrators would present the disk space volume groups to the other production servers and make the appropriate DNS changes.

6. The DBAs would then begin the process for starting the databases. This would include the following:
   - Starting the listeners.
   - Starting the databases.
   - Starting the UNIX batch servers.

   Note: Because there is redundancy built into the load balancers, routing modules, web servers, and applications servers, no manual failover is required for these components.

We have successfully executed these contingencies in real emergency situations with other applications. However, we would not normally invoke such drastic options unless the recovery of the hardware would require more total downtime than alternative courses of action, or the application processing schedule would dictate that such extraordinary measures were necessary.

EMC Symmetrix Enterprise Storage Systems

Each of the UNIX database servers stores its databases on an EMC Symmetrix infrastructure. Through maintenance agreements, EMC provides proactive monitoring of this infrastructure 24 hours a day, 365 days a year, and dispatches service technicians to correct problems as necessary.

Symmetrix Enterprise Storage systems protect the largest relational databases and most demanding applications with the highest degree of data protection - continuous availability. These systems are fully protected against planned or unplanned disruption of information availability and accessibility. The architecture features Mirroring (RAID 1), hardware redundancy, and non-disruptive microcode and component replacement.

EMC's disk Mirroring provides the highest data availability for production-critical applications. By creating two copies of data on separate disk drives, Mirroring ensures both the highest availability and highest system performance. EMC TimeFinder™ software allows us to create independently addressable business continuance volumes (BCVs), which are copies of active production volumes that can be used to run simultaneous tasks in parallel with one another. This gives us the ability to do concurrent operations, such as data warehouse loads and refreshes or point-in-time backups, without affecting production systems. In addition, the systems support non-disruptive microcode update loading, so that we can remain online and unaffected even as the system gains the advantages offered by enhanced capabilities.

This architecture ensures data integrity during each step of the data transfer process, verifying the data from host to cache to disk and back, using the same data verification codes that are generated once at the entry point.

These systems also feature a full-system battery, which guarantees no lost writes and orderly transitions or shutdowns during power outages. Extensive proactive and predictive intelligent maintenance features, such as cache and disk scrubbing and an integrated Remote Maintenance Processor (RMP), add to the information protection and continuous information availability features.

Database Servers

Procedures for disaster recovery for the database servers are included in the published OIIT **Database Administration Policies and Procedures** document.

This document does not address information on database component failure because those scenarios are addressed as database recovery actions rather than disaster recovery. Database backups are kept for disaster recovery purposes, and are to be used to recover the entire database in the event of a failure. These backups are not intended to be used to recover specific data for an institution. However, standard database backup and recovery practices that include a combination of cold backups, exports, and archive log mode operations are being used as part of the database recoverability strategy.

Risk Assessment

Based on past history, failure events such as these may be most likely to occur:

1. Tape library system runs out of available tapes during backup procedures.
2. CPU failure in any one system.
3. Prolonged power outage at the OIIT DB 300 Data Center
4. System hard disk failure.
5. Primary network adapter failure.
6. Backup network adapter failure.
7. Tape drive device failure.

Recovery Scenarios

1. **Tape library system runs out of available tapes during backup procedures.**
   Scenario:
   When the tape library cannot find an available tape during backups, which occur during the hours of 11PM and 7AM, the backup system will issue a "mount request" and wait until a tape is made available. This will postpone the backup of a system or group of systems until the tape is made available.

   Response:
   System administrators are notified via pager and email at the time of the "mount request." System administrators can login the system remotely from their homes and solve the problem. If the problem requires an onsite visit to the machine room facility by the System Administrators, they will drive there in their personal vehicles.

2. **CPU failure in any one system.**
   Scenario:
   One of the systems experiences a CPU failure.

   Response:
   All systems have a minimum of two CPUs. Whether such an event would happen during the day or at night, the failure of one CPU would not necessarily cause the system to halt. In the event of a CPU failure, the system would use its other CPU (or CPUs). Event notification systems would alert the system administrators to this failure. HP hardware support would then be called and the CPU would be replaced later that day during maintenance hours. This type of hardware replacement generally takes one to two hours, leaving plenty of time in the remainder of the maintenance window for system backups to run and complete.

3. **Prolonged power outage at the OIIT DB 300 Data Center.**
   Scenario:
   DB 300 loses power for an extended period of time, exceeding one hour.

   Comment: Mark to provide revised paragraph.

   Response:
   The Banner Hosting systems are supported by the UPS at the DB300 data center. The UPS can most likely support the servers long enough for the system administrators to perform emergency shutdown procedures gracefully.

4. **System hard disk failure.**
   Scenario:
   One of the two system disks in any of the Banner Hosting systems experiences a failure.

   Response:
   This type of failure would not cause an interruption in service. All system hard disks are mirrored to a separate physical hard disk. System administrators would be notified of the failure via pager. Hardware support would be called to replace the disk. In general system disks can be replaced and mirroring reestablished without any downtime for the server. In rare cases, replacing a disk will cause downtime for the system.

5. **Primary network adapter failure.**
   Scenario:
   A primary network adapter fails.

   Response:
   System administrators would be notified via pager. To get the system back as quickly as possible, the network adapter usually used for backups would manually be turned into the primary adapter. This would take less than an hour. Hardware support would be called and downtime scheduled to replace the adapter as soon as the situation warranted. In the meantime, backups will impact performance.

6. **Backup network adapter failure.**
   Scenario:
   A backup network adapter fails.

   Response:
   In the event of such a failure, normal connectivity from the institution would continue without interruption. HP hardware support would be called and replacement of the interface would be performed during the maintenance hours (11PM-7AM). This type of maintenance would be carried out in one to two hours, leaving plenty of time for a daily backup to be carried out in the remainder of the maintenance window.

7. **Tape drive device failure.**
   Scenario:
   A tape drive device fails in the tape library.

   Response:
   The tape library has a sufficient number of tape drives so that, in the event of a tape drive failure, the tape library can perform its required backups to the remaining functional tape drives in the same given backup time frame.

Responsibilities

For any server problem, whether it is something small or something catastrophic, contact the **OIIT HELPDESK**, as noted in Module 8, Section 1.

Topic 2: System Software and Databases

In the event of massive data corruption, System Administrators are prepared to replace any and, if required, all of the system and database software components listed below. Brief procedural descriptions are provided.

Operating System

OIIT/EIS (Enterprise Infrastructure Systems) release of HP-UX would be installed via the network. This would not only provide the base operating system, but it would also contain base layered packages such as SSH and other security oriented packages such as TCP Wrappers.

The Symmetrix disks would be configured for a particular client system. The Symmetrix database would be used to determine which Symmetrix volumes would be assigned to which specific client systems. The Symmetrix database is stored on both the Symmetrix system and on the UNIX system hosting the Symmetrix management software.

Backup Software - Server

The Data Protector server would be installed from the original source (CD/DVD or downloaded images) or restored from a trusted HP Recovery image. All Banner Hosting servers routinely update a Recovery backup image that can be used to restore the system files without Data Protector.

The Data Protector database would then be restored from tape. This database contains specific information about the data contained on the tapes in the tape library. Data Protector makes backups of this database to a pre-identified set of tapes.

Once the server is reinstalled and the Data Protector database has been restored, all of the backups for the Banner Hosting systems can be identified and retrieved.

Banner and Oracle Base Systems

There are two ways to restore the Banner and Oracle base systems.

1. Once the Data Protector server and client have been installed, the Banner and Oracle base systems could be restored from Data Protector tape.

Databases

A list of available backups would be presented to OIIT/EAS/TS. OIIT/EAS/TS would choose a specific backup based on the dates of the available backups. The selection of which backup to use would be left up entirely to OIIT/EAS/TS.

The file systems specific to a database would be created based on naming configuration and sizes that were recorded for the selected backup.

System Administrators would use Data Protector to restore the database data to the file systems. Database Administrators would take appropriate action as needed to verify the successful start-up and availability of the restored database server.

Responsibilities

For any database, application server, or process scheduler technical problem, whether it is something small or something catastrophic, contact the **OIIT HELPDESK**, as noted in Module 8, Section 1.

Topic 3: Networks

Local Area Networks (LAN's)

It is the responsibility of each institution to operate and maintain its own Local Area Network(s).

Wide Area Network

Connectivity from each campus to its hosted Banner Environment is provided by PeachNet, the statewide communications network supporting all University System of Georgia (USG) Information and Instructional Technology (IIT) efforts. In the event of a PeachNet outage at a site not currently engineered with redundant capability to restore connectivity, PeachNet will work with the site to provide operational network connectivity as soon as possible.

Comment: Mark to update diagram

Responsibilities

For any network technical problem, whether it is something small or something catastrophic, contact the **OIIT HELPDESK**, as noted in Module 8, Section 1.

Topic 4: Printers

Note: Please refer to Module 1, Topic 6, starting on page **Error! Bookmark not defined.**, for specific information regarding printing options and recommendations for check and report printers.

Comment: Jeff: See SSC Printing section

Responsibilities

For any printer technical problem, whether it is something small or something catastrophic, first contact the local Workstation Support personnel at your institution.

Comment: Mark to check with Glenn for revision of this section

If the problem cannot be solved at your institution, contact the **OIIT HELPDESK**, as noted in Module 8, Section 1.