Disaster Recovery Implementation for SAP and Related Systems

Bhasker Ravikanti
Information Technology Fellow
Honeywell Aerospace
Agenda

- Introduction to Honeywell
- SAP at Honeywell Aerospace
- DR Concepts
- Honeywell DR Evolution
Great Positions in Good Industries

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Fire Protection &amp; First Responder</td>
<td>Automotive &amp; Transportation</td>
<td>Efficiency, Energy &amp; Utilities</td>
<td>Healthcare &amp; Medical</td>
</tr>
<tr>
<td>Industrial Process Control</td>
<td>Manufacturing</td>
<td>Oil &amp; Gas, Refining, Petrochemicals &amp; Biofuels</td>
<td></td>
</tr>
<tr>
<td>Safety &amp; Security</td>
<td>Scanning &amp; Mobile Productivity</td>
<td>Energy, Safety &amp; Security</td>
<td></td>
</tr>
</tbody>
</table>
Honeywell’s Businesses

- $35-36 billion* in revenues, 50% outside of U.S.
- Nearly 130,000 employees operating in 100 countries
- Morristown, NJ global corporate headquarters

Aerospace

Automation & Control

Specialty Materials

Transportation Systems
Aerospace

Developing innovative safety products, driving the modernization of global air traffic management, revolutionizing combat technology and committed to improving operational efficiencies.

Products:
• Integrated avionics
• Propulsion engines
• Aircraft and engine systems
• Full-service solutions for airliners, business and general aviation aircraft, military aircraft and spacecraft.

Businesses:
• Air Transport & Regional
• Business & General Aviation
• Defense & Space

- Phoenix, AZ headquarters
- 38,000 employees at nearly 100 locations
SAP at Honeywell Aerospace

- Number of users in SAP: 22,500
- Number of countries: 12
- Number of plants: 66
- SAP revenues are now at 81%
- 36,000+ batch program run every 24 hours
- App server workload segregated into Dialog and Batch
- Single Global Instance for all of Aerospace
- Multiple landscapes – ECC, Global Trade System, PI, and All
- Supporting landscapes include Content Server, Solution Manager, SLD and Java
- Primary Database size: 18 TB (growing at 350 GB/Month)
Disaster Recovery Definition

• Disaster recovery is the process, policies and procedures related to preparing for recovery or continuation of technology infrastructure critical to an organization after a natural or human-induced disaster. Disaster recovery is a subset of business continuity. While business continuity involves planning for keeping all aspects of a business functioning in the midst of disruptive events, disaster recovery focuses on the IT or technology systems that support business functions.

-- Wikipedia.org
Natural Disasters – Earthquakes

• Fukushima Daiichi earthquake (April 2011)
Natural Disasters – Forest Fires

• Wallow Fire (Arizona, June 2011) – 519,319 acres burned (source azcentral.com)
Natural Disasters - Hurricanes

- Irene
Human-Induced Disasters

3 Alleged PlayStation Network hackers arrested in Spain

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>LulzSec</th>
</tr>
</thead>
<tbody>
<tr>
<td>Motto</td>
<td>&quot;The world's leaders in high-quality entertainment at your expense&quot;</td>
</tr>
<tr>
<td>Formation</td>
<td>May 2011</td>
</tr>
<tr>
<td>Type</td>
<td>Hacking</td>
</tr>
<tr>
<td>Affiliations</td>
<td>Anonymous, LulzPatt, AntiSec</td>
</tr>
<tr>
<td>Volunteers</td>
<td>6</td>
</tr>
<tr>
<td>Website</td>
<td>lulzsecurity.com</td>
</tr>
</tbody>
</table>
DR Concepts

- Recovery Point Objective (RPO)
- Recovery Time Objective (RTO)
- Business Data loss
  - Infrastructure Recovery
  - Database / File Recovery
  - Application Recovery
  - Application Testing / Configuration and Business Continuance
DR Concepts

Data + Infrastructure + People + Documentation
DR Concepts – Data protection

A. Tape
   • After backing up primary systems, tapes are duplicated and sent to a bunker site (in town) for retention. They get rotated back into the system based on the retention policy.

B. Remote tape backup
   • Tape backup is duplicated directly at a DR hosting company’s facility.

C. Application Replication
   • Oracle data guard uses archivelogs to maintain a copy of the database at the remote site.
   • Rsync can be used to maintain non-database files at the remote site.
   • SAP replication can be used for SLD.
DR Concepts – Data protection

D. SAN replication
   • Direct to DR site using asynchronous updates.
   • Synchronous replication from primary to bunker site (up to 300 KM), cascaded to DR site (asynchronous, unlimited distance) using Journal Space at the bunker site.
DR Concepts - Infrastructure

A. external
   • Pre-arranged agreement allows use of infrastructure at the hosting company’s facility at the remote location.

B. Internal
   • Dedicated infrastructure exists at the company’s remote facility.
   • Dedicated network for replication, so that normal business applications are not impacted.
   • OS synchronization using Image Restore.
     – OS installed on internal drives
     – Not compatible with remote data center policies
     – Host name conflicts
   • Maintain Separate Installation in each data center.
     – Good with OS policies
     – Local files need to be maintained by hand (/etc/services for example)
DR Concepts - Recover Point Objective (RPO)

• RPO: How much loss of data (from the time of the event) can your business afford? Measured in time. Directly depends on the technology used for data protection:

A. Tape: It is the time when the last backup was completed and the tapes were sent to offsite.
  • Oracle database – Last database backup + Archivelogs on offsite tape. Flat file timestamp could dictate Oracle point in time recovery.
  • Other files – Last backup on offsite tapes.
DR Concepts - Recover Point Objective (RPO)

B. Application Replication: Oracle data guard + rsync: Time when the last log switch occurred. Also consider the time it takes for that log to get replicated to the DR site.
   • Not an issue for an active database. Three minutes or less.
   • Inactive database – can trigger a log switch every RPO minutes (say 5 minutes).
   • Rsync is used for non database file sync between the sites. It should be run every RPO minutes at the least.

C. SAN replication:
   • Could be up to 15 minutes. Can be reduced by using a bunker site.
DR Concepts - Recover Time Objective (RTO)

• RTO: How long it takes to recover? Also measured in time. Directly depends on technology used, people skills and documentation:

A. Tape based: Shipping tapes from offsite to the DR site plus the restore time.
   • Oracle database – Directly proportional to the size of the database and the number of tape drives available.
     – 24 hours for Next Business Day shipment.
     – 24 to 36 hours for 8 to 10 TB database.
DR Concepts - Recover Time Objective (RTO)

B. Application Replication: Oracle dataguard + rsync: Time to activate the standby database.

- About 15 minutes for the database.
- About 15 minutes for the Central Instance.
- About 60 minutes for all the APP servers to be brought online.
- Repeated for each landscape.
C. SAN replication:

- Hitachi Universal Replicator:
  - Pause Replication – 15 minutes
  - Present the LUNs to the host – 15 minutes
  - Scans the LUNs – 15 minutes
  - Assemble VG/DG – 15 minutes
  - Mount the filesystems – 15 minutes
  - Start the Oracle database – 15 minutes

- About 15 minutes for the Central Instance.
- About 60 minutes for all the APP servers to be brought online.
- Repeated for each landscape.
DR Concepts - Recover Time Objective (RTO)

D. Include travel time for the technical teams if remote access to DR site is not possible.

E. Hosted DR site:
   • Host OS installation will be an add on.

F. Documentation is crucial to reduce RTO.

G. Trained and Rehearsed team of people are also crucial to reduce RTO.
Honeywell DR Evolution – Tape: External Site

A. Recovery Testing at a hosted company’s site:

• Tapes are sent to offsite retention facility daily.
• Recovery at a hosted companies site.
• Given 48 hours to recover during a test.
• Most of the time was spent in recovering servers (Operating System)
• Not enough time to recover SAP.
Honeywell DR Evolution – Tape: Internal Site

A. Dedicated DR infrastructure at the company’s secondary data center.

B. DR Infrastructure is designed for 70% of primary system capacity.

C. Tape Recovery onto existing hardware:
   • Operating System recovery using image restore on tape.
   • SAP restore from backup tapes.
   • OS image not compatible with secondary site’s template.
   • Configuration information was lost when OS was restored.
   • Consistent recovery across multiple landscapes was too complex.
Honeywell DR Evolution – Application Replication

A. OS is pre-staged and not part of recovery plan:
   • Compatible with local datacenter guidelines.
   • Configuration information is preserved.

B. Database, OS, and SAP replication:
   • Database replication using Oracle dataguard.
   • rsync for non database files.
   • SAP replication for SLD.
   • Consistent recovery across multiple landscapes was better than tape but still complex due to the use of multiple technologies.
Honeywell DR Evolution – SAN Replication

A. Identical Universal Storage Platform V (USP-V) arrays in both data centers with Hitachi Universal Replicator (HUR) services:

• Multiple local and remote copies for protection for high availability (HA) and DR.
• DR Testing uses a copy of storage meant for DR.
• Consistent recovery across multiple landscapes without any issues.
Honeywell Aerospace SAP ECC Landscape
Honeywell Aerospace SAP Other Landscapes

Primary Data Center

DR Data Center

Storage Replication
SAP Storage Architecture with Multi Level Protection

- Use: Mission Critical – Core
- Virtualized: Yes
- Thin Provisioned: No
- Performance: Highest
- Availability: Highest
- Replication: Local & Remote
- Snapshots: 6 Rolling Copies Taken Every 4 Hours

Legend:
- Virtualization Logical Connection
- Async or Point-in-Time Copy
- Full Copy
- Space Efficient Copy
- Virtual Volume

NetApp 3160
Replication Architecture

Honeywell Replication Infrastructure
Hitachi Universal Replicator (HUR)
11/1/2010
Replication Management

Honeywell Replication Diagram
Recommended horcm configuration

horcm0 manages the P-Vols at DCW
horcm1 manages the S-Vols at DCE
horcm11 manages the P-Vols at DCE
horcm10 manages the S-Vols at DCW

Primary CCI Server
TC/IP Network
Secondary CCI Server

SAN
Command Devices
Data Volumes
Primary USP

SAN
Command Devices
Data Volumes
Recovery USP
## Honeywell DR Testing Experience

<table>
<thead>
<tr>
<th>Data Protection / DR component</th>
<th>Tape</th>
<th>Application Replication</th>
<th>SAN Replication</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>RPO</strong></td>
<td>24 hours (if tapes are sent to offsite daily)</td>
<td>30 to 45 min (based on 1 GB Oracle redolog)</td>
<td>15 min</td>
</tr>
<tr>
<td><strong>RTO</strong></td>
<td>60 hours (based on 9 TB Oracle database)</td>
<td>6 hours</td>
<td>4 hours</td>
</tr>
</tbody>
</table>
DR Testing, Managing, Documentation

A. Test once a year with teams traveling.
B. Test once a year without travel.
C. Project Management is very critical to the successful testing of DR.
DR Testing, Managing, Documentation

Decision Criteria to Declare Plan Activation

1. **Incident**
   - Alert/Notification from Business, HITS, DR coordinator, or Infrastructure Service Delivery

2. **Initial Outage Assessment**
   - General Cause of Outage
   - Extent of Outage
   - Estimated outage time

3. **Assemble Team**

4. **Ensure authorized decision makers are present or delay decision**

5. **Review criteria**

6. **Determine Decision or when to re-assess situation**

   - Time to recover at original site hours
   - Time to recover at remote site hours
   - Time to bring back system hours

   **DECLARE DISASTER to Failover to DR site**

   - No
     - Re-assess situation
DR Testing, Managing, Documentation

Initial Response Actions After Declaration Declared

1. DECLARE DISASTER to Failover to DR Site
2. Activate the conference bridge
3. Notify and Brief Recovery team members
4. Begin Failover Recovery Procedures
5. Begin Application Validation and User Testing
6. Re-assess situation with key resources and authorized decision makers
7. Activate DR site as primary system location for business
8. Decision for Planned Failback to normal operations at Primary Site
9. Begin Failback Recovery Procedures to Primary Site (follow procedures contained in this plan)
10. Assemble recovery team to IT Emergency Operations Center
11. Disaster Recovery Coordinator will initiate notification and coordinate arrangements with DR Site, Suppliers, Tape Site
DR Testing – Lessons Learned

A. Firewall Rules for the DR site.

B. Remove network routing on the DR servers so that they can’t reach real production servers.

C. Not all dependent applications may be on the DR plan.

D. Change DNS entries to minimize access issues for end users and external applications.
Feedback

A. Please complete a session evaluation for this session!
B. Session ID:
C. Title: Disaster Recovery Implementation for SAP and Related Systems
D. Speaker: Bhasker Ravikanti
Transforming the Information Infrastructure: Build, Manage, Optimize.