Zero Data Loss Recovery Appliance: Maintenance & Operational Best Practices

MAA Best Practices Team
Server Technologies
April 2021
Agenda

1. Understand Requirements First
2. RA Deployment Decisions and Key Practices
3. RA Stay Healthy Plan
4. Best Practices Backup and Restore
5. Migration with ZDLRA
6. Oracle Support & Service Request
7. RA Roles and Responsibilities
MAA Recommendations

- One Recovery Appliance (RA) per data center
- Backup primary and standby databases to their respective local RA
- No RA replication for any database with a remote standby
- Restore operation can use any RA in any location
Do your business requirements call for multiple Recovery Appliances?

1. Do you need the ability to backup, restore and recover during RA planned maintenance windows (2-6 hours for major upgrades) versus waiting until the planned maintenance completes?  
   Yes/No

2. Do you require disaster recovery protection? (e.g. data center failure, power failure)  
   Yes/No

3. Do you require minimal data loss for all protected databases backing up to RA during its planned maintenance windows? (you don't need to restore/recover)  
   Yes/No

4. Do you require archive and backups operations to continue during RA planned maintenance windows (2-6 hours) versus waiting until the planned maintenance completes?  
   Yes/No

If you answered “Yes”, to any of these questions multiple Recovery Appliances are required.
Multiple Recover Appliances Required?

- Did you answer “yes”?
  - To ANY of the questions: You will need another Recovery Appliance
  - Yes to question #1 or #2: Use High Availability for Backup and Recovery
  - Yes to question #3 or #4 Only: Use Backup Failover to Alternate Appliance Solution

Note: Using Data Guard or GoldenGate?
Backup the production, standby or Golden Gate replica to their respective local RA.
RA Replica: System Outage / Disaster Protection

Recommended for Standalone (Non Data Guard) Databases

REPLICATION BENEFITS

- Protects data from Local or Site-wide failures
- Automated restore from Local Appliance or directly from Remote Appliance
High Availability for Backup & Recovery

RA Osaka normally replicates to RA Tokyo

When upstream appliance (RA Osaka) is not available, backups and redo are redirected to Remote appliance (RA Tokyo)

- Virtual fulls are created as normal
- Sizing DR appliance
  In general, size per Recovery Window Goal (RWG) business requirement:
  1x full backup + N RWG days of incremental and redo/arch log backups
  Bare minimum: 1x full backup + 1 day redo/arch logs backups.

When upstream is back online, DR appliance backups are transferred

- Backups are ingested and processed into virtual fulls
- Normal backups to upstream can be restarted immediately
- Virtual fulls for new backups are created after all transferred backups have completed processing
- Note: Redo Logs sent to the downstream are not automatically copied to the upstream. A restore/recover will pull the logs from the downstream as necessary.

Benefits

- Best practice to preserve HA during planned or unplanned downtime
- Database backup & restore/recoverability available from either upstream and downstream

Copyright © 2021, Oracle and/or its affiliates
Backup Failover to Alternate RA

Incrementals and Redo normally sent to Primary RA

Alternate RA serves as backup staging area when primary RA is unavailable, then syncs with primary RA afterwards
  • No virtual fulls created on alternate, hence recoverability not supported
  • Space sized for ‘n’ incrementals and archived log backups during primary downtime period

Benefits:
  • Preserves backup and redo shipment continuity during planned maintenance / upgrades
  • Prevents local Fast Recovery Areas from filling up with archived logs
  • Block Change Tracking continues

“BF_FORWARD” Policy on Alternate RA:
STORE_AND_FORWARD = ‘YES’
Backup Failover to Alternate RA - Continue

Backup and redo failover destination when primary appliance is unavailable

- Alternate appliance takes over backups and redo transport
- When primary appliance is back online, all interim backups are replicated from alternate and virtual full backups are created on primary
- Once all virtual fulls are completed, backups and redo transport can restart to the primary appliance
- Backup Failover” within the same data center requires both Recovery Appliances to be configured on the same replication subnet.

“BF_BACKUP” Policy on Primary RA

“BF_FORWARD” Policy on Alternate RA:
STORE_AND_FORWARD = ‘YES’
Recovery Appliance Solutions Summary

High Availability for Backup and Recovery (Non-Data Guard Databases)
• Backup and Redo to RA Replica during RA maintenance and unplanned downtime
• Restore from RA Replica
• More capacity required due to RA replication
• See: Configuring High Availability ZDLRA client for backup and restore (Doc ID 2432144.1)

Backup Failover to Alternate Appliance (Standalone/Primary/Standby Databases)
• Backups and Redo to Alternate RA during RA maintenance and unplanned downtime
• Restore from Alternate NOT available
• Less capacity required because RA replication was not setup
Recovery Appliance & Data Guard

MAA Recommendations:
• One Recovery Appliance (RA) per data center
• Backup primary and standby databases to the local RA
• No RA replication for any databases with a remote standby needed
• Restore operation can use any RA in any location

Active Data Guard License on primary and standby, is NOT required for using Fast Incremental and Real-time Redo exclusively to RA.

See: Licensing Documentation
Recovery Appliance and Data Guard

Maximum Availability Architecture (MAA) White Paper

Post Data Guard role transition

• No change in backup operations. Continue to backup both the primary and standby databases to the local RA

Deploying the Zero Data Loss Recovery Appliance in a Data Guard Configuration

Agenda

1. Understand Requirements First
2. RA Deployment Decisions and Key Practices
3. RA Stay Healthy Plan
4. Best Practices Backup and Restore
5. Migration with ZDLRA
6. Oracle Support & Service Request
7. RA Roles and Responsibilities
Network Configuration Options

ZDLRA Supports 10GigE / 25GigE and InfiniBand

- 10 GigE or 25 GigE is the recommended for protected database to RA connectivity
  - Ethernet based connectivity provides optimal backup and restore rates due to RA's resource management.

- Note: While IB connectivity is supported, be aware of the following:
  - IB will not realize the full IB network bandwidth due to RA resource management (managed throttling).
  - IB setup will introduce software update complexity.
  - Owner’s Guide, Chapter 9 has details on how to configure Backup Ingest over IB

- Note: Real-Time Redo Transport uses 10 GigE or 25 GigE network ONLY
Network Configuration Options - continue

VLAN for network isolation

- Backup and restore traffic from different VLANs is not routed.
- **Recovery Appliance supports VLAN tagging on the ingest network**
  - Protected DB hosts on different and isolated VLANs can be connected directly to the RA
  - Enabling 802.1Q VLAN Tagging in Zero Data Loss Recovery Appliance Over Ingest Networks (Doc ID 2047411.1)

Replication Network: Typically configured via OEDA before RA SW install

- Replication network configuration, post install
  - Post Install - Replication Network Configuration for ZDLRA (Doc ID 2126047.1)
- When Replication network is configured: VLAN tagging is not supported.
- Protected Databases must use the ingest network.
Recovery Appliance Security

Customers requiring end to end security

Client to Recovery Appliance, or Recovery Appliance to Client
- Upcoming: Security in Flight (TCPS, HTTPS) ➔ Provided upon request
- Adding a protected database Recovery Appliance VPC user credentials to an existing OID wallet (Doc ID 2211759.1)

Security in the Recovery Appliance
- Recovery Appliance administrators responsibilities
  - Create Virtual Private Catalog (VPC) User
  - Assign protected databases to a specific VPC User
  - The protected database administrator can see all databases that share a common VPC user
Agenda

1. Understand Requirements First
2. RA Deployment Decisions and Key Practices
3. RA Stay Healthy Plan
4. Best Practices Backup and Restore
5. Migration with ZDLRA
6. Oracle Support & Service Request
7. RA Roles and Responsibilities
Adjusting Default Settings

Do not make any changes to Recovery Appliance

- **IT’S AN APPLIANCE and it’s already optimized**
  - Restrictions and supported configuration exceptions in MOS note 2172842.1

If required, use **MAX_RETENTION_WINDOW** to enforce hard limits on data retention for all databases within a protection policy.

- **Use cases where there are stringent compliance / regulatory requirements**
  - Best practices is to set the value to 5 days or greater (50% above the Recovery Window for large ranges)
  - Backups are forcibly removed after exceeding window
  - Recovery Window Goals should be used to manage backup space consumption
  - Using an aggressive **MAX_RETENTION_WINDOW** (one not adhering to best practice) may delay backup processing and indexing due to increased and less efficient PURGE task jobs.
Use Recommended RA Software

• Subscribe to MOS alerts and refer periodically to the following notes:
  • Recovery Appliance Critical Issues MOS note for critical issues alerts (SUBSCRIBE NOW)
  • Recovery Appliance Supported Versions MOS note for latest software update

Use Recommended RA Software to avoid known critical issues
• Number 1 method to avoid problems: Upgrade to recommended software release
• Zero Data Loss Recovery Appliance Supported Versions (Doc ID 1927416.1)
• Zero Data Loss Recovery Appliance Upgrade and Patching (Doc ID 2028931.1)
• Patches are cumulative and include
  - Bug fixes (Avoid a bug before it happens)
  - Enhancements (Modification to RA process flow)

Coordinate with Platinum Patching
• Schedule early & Open Proactive SR
Don’ts

• Don’t ignore incidents:
  • Resolve and understand

• Don’t neglect the RA
  • Monitor the system

• Don’t Submit multiple request to Delete databases
  • Multiple – concurrent database deletions can have a negative impact on the RA
  • Avoid Delete Database commands as much as possible or limit deletions to 1 or 2 concurrently for large database deletions
  • Start with the smallest and work up, monitor for successful completion.
**Don’ts**

- Don’t repeat backup or recovery scripts after a failure
  - First troubleshoot the reason.
  - Typically a client side issue.
  - Rapid and repeated executions of a script may impact the RA.

- Don’t make modifications to the RA configuration
  - Zero Data Loss Recovery Appliance - Installing Third-Party Software and Modifying Internal Appliance Software (Doc ID 2014361.1) - (oratab, .zdlra env, databasemachine.xml)

- Don’t take periodic Level 0
  - Virtual Level 0 requires only one level 0 followed by level 1s
  - Note: A level 0 may be requested
    - By Support
    - To preserve recoverability in event of backup corruption detected on the RA
Don’ts

- Don’t backup a Data Guard primary & standby to the same RA
  - See Deploying the Zero Data Loss Recovery Appliance in a Data Guard Configuration

- Don’t register databases with identical DBIDs to the same RA
  - See Cloning a Protected Database within the ZDLRA Protected Database Configuration Guide

- Don’t backup to another media
  - Switching to another media can impact past and future backups made to the RA

- Dual backup strategies are complex and should be avoided if possible
  - Dual backup strategies are designed for migration
  - Dual Backup Strategy MOS Notes:
    - Implementing a Dual Backup Strategy with Backups to Disk and Recovery Appliance (Doc ID 2154461.1)
    - Implementing a Dual Backup Strategy with Backups to Tape and Recovery Appliance (Doc ID 2154471.1)
Dos

• Validate the backup/restore network first:
  • Use Zero Data Loss Recovery Appliance Network Test Throughput script (Doc ID 2022086.1)
    • requires qperf, NOT OS agnostic
  • How to measure network performance from RMAN for ZDLRA or Cloud Backups (Doc ID 2371860.1) – uses RMAN’s “NETTEST” option, OS agnostic

• File a NEW SR for any new issue
  • Refer to Service Requests and Escalation Process section

• Set NLS_DATE_FORMAT before calling rman scripts
  • e.g. in Linux: export NLS_DATE_FORMAT="yyyy-mm-dd hh24:mi:ss"
Dos

• **Use Multi Section**: set Section Size to 64GB
  • Number of sections per datafile is limited to 256.
  • When a section size of 64GB is used:
    • Large datafiles > 16TB will automatically see > 64GB section size as determined by RMAN
      • if (sizeof(datafile) > 16TB), section size = sizeof(datafile) / 256
    • Small datafiles < 64GB will not have sections
  • A 64GB section size: allows for efficient processing in ZDLRA’s flash cache
    • Forces filesperset to 1

• **Use the latest libra** (The RMAN client sbt library that supports ZDLRA)
  • Download the latest sbt library (libra module) (Doc ID 2219812.1)
  • For RAC: Distribute to ALL nodes in the cluster
  • Do NOT update the libra.so on the ZDLRA, unless directed by support.
Monitoring RA’s Health

Monitor the Appliance on a daily basis
  • EM Unified Management Dashboard
    • Review twice daily
  • System Activity Script (Doc ID 2275176.1)
    • Run daily and monitor trends
  • EM notifications
    • Review and act on notifications
  • Run exachk Monthly and review findings
    • How To update exachk outside ZDLRA Install, Patching and Upgrade (Doc ID 2399688.1)
      • Use diff to compare month to month
      • Run pre and post patching
  • Review Capacity Planning Report Monthly or Bi-Monthly
### Incidents and Events

#### Summary

<table>
<thead>
<tr>
<th>Incident</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ORA-45159</td>
<td>Recovery window goal is lost for database all caused by SYS.DBSYS_SYS_ERR.</td>
</tr>
<tr>
<td>ORA-45159</td>
<td>Recovery window goal is lost for database all caused by SYS.DBSYS_SYS_ERR.</td>
</tr>
<tr>
<td>ORA-45172</td>
<td>The validation task has not run recently for one or more databases. ORA-06512 at SYS.DBSYS_SYS_ERR.</td>
</tr>
</tbody>
</table>

#### Incident Details

<table>
<thead>
<tr>
<th>Target</th>
<th>Severity</th>
<th>Status</th>
<th>Escalation Level</th>
<th>Time Since Last Update</th>
</tr>
</thead>
<tbody>
<tr>
<td>ORA-45159</td>
<td>New</td>
<td>-</td>
<td>Incident</td>
<td>0 days 14 hours</td>
</tr>
<tr>
<td>ORA-45159</td>
<td>New</td>
<td>-</td>
<td>Incident</td>
<td>0 days 18 hours</td>
</tr>
<tr>
<td>ORA-45172</td>
<td>New</td>
<td>-</td>
<td>Incident</td>
<td>1 day 9 hours</td>
</tr>
<tr>
<td>ORA-45172</td>
<td>New</td>
<td>-</td>
<td>Incident</td>
<td>7 days 5 hours</td>
</tr>
<tr>
<td>ORA-45172</td>
<td>New</td>
<td>-</td>
<td>Incident</td>
<td>10 days 5 hours</td>
</tr>
</tbody>
</table>

#### Additional Details

<table>
<thead>
<tr>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal error detected in /u01/app/trace/16072910/ORA-45159 trace Flag. Match at timeline number Fri Jan.</td>
</tr>
</tbody>
</table>

**Updated in the last 31 days**

---

### Incidents and Events

#### Summary

<table>
<thead>
<tr>
<th>Incident</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ORA-04760</td>
<td>Database stuck in ordering wait state for over 2 days.</td>
</tr>
<tr>
<td>ORA-44748</td>
<td>Trace file writing initiated using debug flags.</td>
</tr>
<tr>
<td>ORA-46173</td>
<td>The checks file has not run recently for one or more storage locations.</td>
</tr>
<tr>
<td>ORA-45159</td>
<td>Unable to validate backup piece with ORA-06512. ORA-45159 is metadata for database, file is corrupt.</td>
</tr>
<tr>
<td>ORA-44737</td>
<td>Unable to copy a full backup of database to tape or replicated recovery appliance.</td>
</tr>
</tbody>
</table>

#### Incident Details

<table>
<thead>
<tr>
<th>Target</th>
<th>Severity</th>
<th>Status</th>
<th>Escalation Level</th>
<th>Time Since Last Update</th>
<th>Created</th>
</tr>
</thead>
<tbody>
<tr>
<td>ORA-04760</td>
<td>New</td>
<td>-</td>
<td>Incident</td>
<td>13 days 1 hours</td>
<td>Jan 6, 2018 9:1...</td>
</tr>
<tr>
<td>ORA-44748</td>
<td>New</td>
<td>-</td>
<td>Incident</td>
<td>13 days 23 hours</td>
<td>Jan 6, 2018 1:2...</td>
</tr>
<tr>
<td>ORA-46173</td>
<td>New</td>
<td>-</td>
<td>Incident</td>
<td>14 days 4 hours</td>
<td>Jan 6, 2018 11:1...</td>
</tr>
<tr>
<td>ORA-45159</td>
<td>New</td>
<td>-</td>
<td>Incident</td>
<td>15 days 15 hours</td>
<td>Jan 6, 2018 9:2...</td>
</tr>
<tr>
<td>ORA-44737</td>
<td>New</td>
<td>-</td>
<td>Incident</td>
<td>16 days 20 hours</td>
<td>Jan 6, 2018 4:8...</td>
</tr>
</tbody>
</table>

**Updated in the last 31 days**
Unified End-to-End Control

Recovery Appliance Admin centrally monitors and manages all database protection activity across all tiers.

Database Admin monitors the protection status of their database from disk, to tape, to replica.

- Offloaded replicas and tape backups appear in Recovery Catalog.
Best Practice – Unified Management Dashboard

1) Summary
   Shows the number of protected databases, and summarizes their health status, current activity, and activity within the last 24 hours. For more information, click the links in the Operation column: Backup, Copy-to-Tape, Replication, and Restore.

2) Protected Database Issues
   Highlights issues relating to backup and recovery status for protected databases. The View menu filters the data on key categories.

3) Data Sent/Received (Daily)
   Displays daily throughput over the past week.

4) Performance
   Charts performance statistics for Data Rate and Queued Data. The statistics are filterable by day, week, or month.

5) Media Managers
   Displays the configured media manager for copy-to-tape operations.

6) Storage Locations
   Summarizes total available space and usage by indicating how much has been consumed to meet the disk recovery window goal for all databases, and what percentage of total space is reserved space for databases backing up to the specified storage location.

7) Replication
   Lists the downstream Recovery Appliances to which this Recovery Appliance is replicating, and also the upstream Recovery Appliances from which this Recovery Appliance is receiving.

8) Incidents and Events
   Summarizes all warnings or alerts that have been generated by Cloud Control monitoring of all targets associated with the Recovery Appliance. From this section, drill down for further detail on the issues.

Copyright © 2021, Oracle and/or its affiliates
Best Practices – Unified Management Dashboard - Continue
Best Practices – Leverage OEM notifications

Recovery Appliance alert notification setup using Oracle Enterprise Manager (Doc ID 2262003.1)

Example of alerts and notification for old backups:

```
<table>
<thead>
<tr>
<th>Incidents and Events</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

Summary

- The last complete backup for database HENC was on 2017-05-28 08:00:04-07:00.
- The last complete backup for database YHNC was on 2017-05-28 08:00:02-07:00.
- The last complete backup for database CB1212 was on 2017-04-28 09:00:02-07:00.
- The last complete backup for database CB1211 was on 2017-05-09 10:01:50-07:00.
- The last complete backup for database MAACDB1 was on 2017-05-06 00:05:58-07:00.
- The last complete backup for database MAACDB1 is 2995 minutes old.

Host=example.com
Target type=Recovery Appliance
Target name=ZDLRA_Montreal
Category=Availability
Message=The last complete backup for database MAACDB1 is 2995 minutes old.
Severity=Critical
Event reported time=May 8, 2017 1:35:56 PM PDT
Operating System=Linux
Platform=x86_64
Associated Incident ID=27852
Associated Incident Status=New
Associated Incident Owner=
Associated Incident Acknowledged By Owner=No
Associated Incident Priority=None
Associated Incident Escalation Level=0
Event Type=Alert
Event name=Ora_backup_rule_name
Metric=Ora_backup_rule_name
Metric value=2995
Key Value=Ora_backup_rule_name
Key Column 1=db_unique_name
Key Column 2=policy_name
Key Column 3=Ora_backup_rule_name
Key Column 4=Ora_backup_rule_name
Key Column 5=Ora_backup_rule_name
Key Column 6=Ora_backup_rule_name
Key Column 7=Ora_backup_rule_name
Rule Name=rule_LAST_BACKUP_AGE
Rule Owner=SYSMAN
Update Details:
The last complete backup for database MAACDB1 is 2995 minutes old.
```
Zero Data Loss Recovery Appliance System Activity Script

Contains multiple queries, providing:

- Catalog version
- General state of the system
- Examination of running tasks on the system
- Task history for the last day
- Space usage
- Locking information
- Check status of replication server if it exists
- Incidents for the last five days
- Display each database's current progress processing their datafiles
- API commands over the last 2 weeks
- Notable config changes
Is the ZDLRA Healthy? System Activity Report

Items to watch for: Bad report

<table>
<thead>
<tr>
<th>TASK_TYPE</th>
<th>STATE</th>
<th>CURRENT_COUNT</th>
<th>LAST_EXECUTE_TIME</th>
<th>WORK_TYPE</th>
<th>creation_time</th>
</tr>
</thead>
<tbody>
<tr>
<td>CROSSCHECK_DB</td>
<td>EXECUTABLE</td>
<td>1</td>
<td></td>
<td>Maintenance</td>
<td>08-DEC-2017</td>
</tr>
<tr>
<td>PLAN_DF</td>
<td>EXECUTABLE</td>
<td>496,959</td>
<td></td>
<td>Maintenance</td>
<td>22-NOV-2017</td>
</tr>
<tr>
<td>UPDATE_INDEX</td>
<td>EXECUTABLE</td>
<td>228</td>
<td></td>
<td>Maintenance</td>
<td>09-SEP-2017</td>
</tr>
<tr>
<td>OPTIMIZE</td>
<td>EXECUTABLE</td>
<td>224</td>
<td></td>
<td>Maintenance</td>
<td>28-NOV-2017</td>
</tr>
<tr>
<td>OPTIMIZE</td>
<td>EXECUTABLE</td>
<td>98</td>
<td></td>
<td>Maintenance</td>
<td>22-NOV-2017</td>
</tr>
<tr>
<td>RESTORE_RANGE.PreparedStatement</td>
<td>EXECUTABLE</td>
<td>209</td>
<td></td>
<td>Maintenance</td>
<td>06-DEC-2017</td>
</tr>
<tr>
<td>RH_INC_FILES</td>
<td>EXECUTABLE</td>
<td>1</td>
<td></td>
<td>Maintenance</td>
<td>09-DEC-2017</td>
</tr>
<tr>
<td>OBSCURE_SBT</td>
<td>EXECUTABLE</td>
<td>1</td>
<td></td>
<td>SBT</td>
<td>22-NOV-2017</td>
</tr>
<tr>
<td>PURGE_DUP</td>
<td>EXECUTABLE</td>
<td>211</td>
<td></td>
<td>Work</td>
<td>13-NOV-2017</td>
</tr>
<tr>
<td>INDEX_BACKUP</td>
<td>EXECUTABLE</td>
<td>179,451</td>
<td></td>
<td>Work</td>
<td>04-DEC-2017</td>
</tr>
<tr>
<td>CROSSCHECK_DB</td>
<td>EXECUTABLE</td>
<td>10</td>
<td></td>
<td>Work</td>
<td>29-NOV-2017</td>
</tr>
<tr>
<td>BACKUP_ARCH</td>
<td>EXECUTABLE</td>
<td>1,072</td>
<td></td>
<td>Work</td>
<td>06-DEC-2017</td>
</tr>
<tr>
<td>PURGE_DP</td>
<td>EXECUTABLE</td>
<td>289,722</td>
<td></td>
<td>Work</td>
<td>06-DEC-2017</td>
</tr>
<tr>
<td>INDEX_BACKUP</td>
<td>ORDERING_WAIT</td>
<td>112</td>
<td></td>
<td>Work</td>
<td>13-NOV-2017</td>
</tr>
<tr>
<td>PURGE_DUP</td>
<td>RUNNING</td>
<td>1 09-DEC-2017 18:57:01</td>
<td>Work</td>
<td>12-NOV-2017</td>
<td></td>
</tr>
<tr>
<td>PURGE</td>
<td>RUNNING</td>
<td>3 09-DEC-2017 06:36:12</td>
<td>Work</td>
<td>08-DEC-2017</td>
<td></td>
</tr>
<tr>
<td>PURGE_DUP</td>
<td>TASK_WAIT</td>
<td>172,675</td>
<td></td>
<td>Work</td>
<td>31-DEC-2017</td>
</tr>
<tr>
<td>CHECK_FILES</td>
<td>TASK_WAIT</td>
<td>1</td>
<td></td>
<td>Maintenance</td>
<td>19-NOV-2017</td>
</tr>
<tr>
<td>VALIDATE</td>
<td>TASK_WAIT</td>
<td>1</td>
<td></td>
<td>Maintenance</td>
<td>12-JUN-2017</td>
</tr>
<tr>
<td>OPTIMIZE</td>
<td>TASK_WAIT</td>
<td>293</td>
<td></td>
<td>Work</td>
<td>09-NOV-2017</td>
</tr>
<tr>
<td>CROSSCHECK_DB</td>
<td>TASK_WAIT</td>
<td>218</td>
<td></td>
<td>Work</td>
<td>21-NOV-2017</td>
</tr>
<tr>
<td>PURGE_DP</td>
<td>TASK_WAIT</td>
<td>3</td>
<td></td>
<td>Work</td>
<td>09-DEC-2017</td>
</tr>
</tbody>
</table>

Watch for:

If there are tasks of WORK TYPE in RUNNING state and created a day earlier then investigate.

If there are tasks of MAINTENANCE or SBT TYPE present and their creation time is older than one week then it should be investigated.

A large number of task in executable state for the same task_type.

The same task type is increasing in the number of jobs (current_count) over time.

A system with ordering waits that are older than 1 day.

A system with tasks in stall_when_wait. This should only be seen if Oracle Support is troubleshooting the RA.
### The Good:

Minimum creation time for active tasks is within the last 24 hours for work tasks.

Task history state should indicate work is being completed.

Review other sections.

### Task history for the last day:

---

### Seeing what work has completed recently can be informative.

---

### It is a basic indication of what has happened.

#### Task Type: COUNT, MIN COMPLETION TIME, MAX COMPLETION TIME

<table>
<thead>
<tr>
<th>Task Type</th>
<th>State</th>
<th>COUNT</th>
<th>MIN COMPLETION TIME</th>
<th>MAX COMPLETION TIME</th>
</tr>
</thead>
<tbody>
<tr>
<td>DB States Refresh</td>
<td>Completed</td>
<td>131</td>
<td>10-Jan-2018 20:04:01</td>
<td>11-Jan-2018 20:04:04</td>
</tr>
<tr>
<td>Oemol</td>
<td>Completed</td>
<td>1</td>
<td>11-Jan-2018 00:10:31</td>
<td>11-Jan-2018 00:10:31</td>
</tr>
<tr>
<td>Purge Diff</td>
<td>Completed</td>
<td>268</td>
<td>11-Jan-2018 06:29:46</td>
<td>11-Jan-2018 06:29:51</td>
</tr>
<tr>
<td>Restore Back Refesh</td>
<td>Completed</td>
<td>28,737</td>
<td>10-Jan-2018 20:06:02</td>
<td>11-Jan-2018 20:06:02</td>
</tr>
<tr>
<td>SW Inc Files</td>
<td>Completed</td>
<td>131</td>
<td>10-Jan-2018 20:06:00</td>
<td>11-Jan-2018 20:06:07</td>
</tr>
</tbody>
</table>
Is the ZDLRA Healthy? exachk

Update exachk for RA:
• How to update exachk outside ZDLRA Install, Patching and Upgrade (Doc ID 2399688.1)
Determining whether unprocessed task list is growing (over 7 day period):

SELECT count(*)
FROM ra_task
WHERE archived='N';

Determine whether incidents are active for delays in performing busywork:

SELECT error_text
FROM ra_incident_log
WHERE status='ACTIVE'
  AND error_text like '%has not run%';

Tasks with highest numbers (RA_TASK.PRIORITY) are busywork tasks

- DB_STATS_REFRESH, RESTORE_RANGE_REFRESH, OPT_DF, OPTIMIZE, REBUILD_INDEX, VALIDATE, CHECK_FILES, CROSSCHECK_DB

How to Determine If ZDLRA Is Keeping up With Load

Problem: task queue growing over time
Action: review system activity report/EM open SR

Problem: Active incidents log indicates busywork not running
Action: Review system activity report/EM open SR
ORDERING_WAIT tasks

• Occurs when a backup piece won’t tile with existing Delta Pools

• Causes:
  • Unprocessed incrementals from polling directory
  • Missing incremental level 1 backup
  • Incremental level 1 backup taken against a level 0 backup that is not in Delta Pool (may be on local storage in Protected DB or replica or on tape
  • Missing datafile incarnation information: open resetlogs
  • Unsupported features used in backup piece:
    maxpiecesize, rman encryption, datafile copy
ORDERING_WAIT tasks -- investigating

Current script for investigating ORDERING_WAIT issues is available from support in a MOS note:

- Diagnostic SQL script for tasks in ORDERING_WAIT status on Recovery Appliance (Doc ID 2095949.1)
Lost RESTORE_RANGE

Uses of restore ranges:

- RECOVERY RANGE output from EM
- RA_<disk|sbt>_RESTORE_RANGE views
- UNPROTECTED_WINDOW information and alerts

For a restore range to be valid we need:

- Archivelogs to cover the range
- ZDLRA Disk file backups for all datafiles that were taken during the range
- Backup of controlfile
Diagnosing RESTORE RANGE problems

Compare restore range of ZDLRA storage against all storage

```sql
select * from ra_disk_restore_range
where db_key = <db_key> order by low_time;
```

```sql
select * from rc_restore_range
where db_key = <db_key> order by low_time;
```

- Make sure that the restore range has been recomputed

```sql
select count(*), max(completion_time) from ra_task
where task_type = 'RESTORE_RANGE_REFRESH' and archived = 'Y' and db_key=<db_key>;
```

- See what RMAN thinks about recovery of database

RMAN> restore preview database;
Diagnosing RESTORE RANGE problems (cont.)

Get list of logs to make sure that they tile

```sql
select thread#, first_change#, first_time, next_change#, next_time
from rc_backup_redolog join rc_backup_piece using (bs_key, db_key)
where db_key = <db_key> and ba_access='Local' and first_time > sysdate - <RWG>
order by thread#, first_change#;
```

Get list of datafiles to make sure that they overlap with archivelogs

```sql
select file#, checkpoint_change#, checkpoint_time, absolute_fuzzy_change#
from rc_backup_datafile join rc_backup_piece using (bs_key, db_key)
where db_key = <db_key> and ba_access='Local' order by file#, checkpoint_change#;
```

Get list of control files to make sure that one is usable

```sql
select c.completion_time
from rc_backup_controlfile c join rc_backup_piece using (bs_key, db_key)
where db_key = <db_key> and ba_access='Local' order by c.completion_time;
```
Recovery Appliance BI Reports

Reports are available to help the Recovery Appliance administrator understand resource utilization, alerts, and historical operations.

Reports examples include:

• Active Incidents
• API History
• Capacity Planning
• Recovery Window Summary
• Top 10 Databases by Data Transfer
• Protected Databases Details
• Chargeback Reports
Protected Database Report

Recoverability information per database!

Top section contains the following information:

- Protected Database
- Space Used
- RPO / Recovery Window
- Unprotected Window
- Last Backup time
- Last Tape Copy
- Last Replication

![Protected Database Report](Image)

Copyright © 2021, Oracle and/or its affiliates
Chargeback Report – Pay as RA Storage is Utilized (Least)

Charge for space as it is used on the Recovery Appliance

Recuer Appliance - Protected Database Chargeback Report

Scenario: Think of this as similar to an metered model where the customer only pays for utilization. The database being protected is charged only for the space utilized.

Example: A 6 month retention would ramp up in cost since utilization on month 1 is lower than month 6.
Chargeback Report - Pay as RA Storage is Utilized-cont’d

Monthly RA Storage space consumption for this database.

Display of RA space used to calculate the chargeback.

<table>
<thead>
<tr>
<th>Year</th>
<th>Month</th>
<th>Database</th>
<th>Maximum Current Space (GB)</th>
<th>Maximum Recovery Window Space (GB)</th>
<th>Maximum Reserved Space (GB)</th>
<th>Space Used for Chargeback (GB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017</td>
<td>03</td>
<td>T12E8K</td>
<td>3034.14</td>
<td>5323.82</td>
<td>2048</td>
<td>3034.14</td>
</tr>
<tr>
<td>2017</td>
<td>04</td>
<td>T12E8K</td>
<td>6087.21</td>
<td>4847.9</td>
<td>2048</td>
<td>4847.93</td>
</tr>
<tr>
<td>2017</td>
<td>05</td>
<td>T12E8K</td>
<td>9439.77</td>
<td>4352.21</td>
<td>2048</td>
<td>4352.21</td>
</tr>
<tr>
<td>2017</td>
<td>06</td>
<td>T12E8K</td>
<td>12558.35</td>
<td>4511.3</td>
<td>2048</td>
<td>4511.3</td>
</tr>
<tr>
<td>2017</td>
<td>07</td>
<td>T12E8K</td>
<td>12599.74</td>
<td>8053.57</td>
<td>2048</td>
<td>8053.57</td>
</tr>
<tr>
<td>2017</td>
<td>08</td>
<td>T12E8K</td>
<td>8971.02</td>
<td>4116.51</td>
<td>2048</td>
<td>4116.51</td>
</tr>
</tbody>
</table>
Monthly cost for this database on RA Storage.

<table>
<thead>
<tr>
<th>Year</th>
<th>Month</th>
<th>Database</th>
<th>Chargeback Amount</th>
<th>Chargeback Amount Delta</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017</td>
<td>03</td>
<td>T1ZE8K</td>
<td>$151.71</td>
<td>$0.00</td>
</tr>
<tr>
<td>2017</td>
<td>04</td>
<td>T1ZE8K</td>
<td>$202.38</td>
<td>$90.67</td>
</tr>
<tr>
<td>2017</td>
<td>05</td>
<td>T1ZE8K</td>
<td>$217.61</td>
<td>($24.77)</td>
</tr>
<tr>
<td>2017</td>
<td>06</td>
<td>T1ZE8K</td>
<td>$226.57</td>
<td>$7.96</td>
</tr>
<tr>
<td>2017</td>
<td>07</td>
<td>T1ZE8K</td>
<td>$402.68</td>
<td>$177.11</td>
</tr>
<tr>
<td>2017</td>
<td>08</td>
<td>T1ZE8K</td>
<td>$265.83</td>
<td>($196.85)</td>
</tr>
</tbody>
</table>
Chargeback Report- Pay as RA Storage is Utilized-cont’d

Monthly tape storage space consumption for this database.

<table>
<thead>
<tr>
<th>Year</th>
<th>Month</th>
<th>Database</th>
<th>Copy to Tape (GB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017</td>
<td>03</td>
<td>T12E8K</td>
<td>0</td>
</tr>
<tr>
<td>2017</td>
<td>04</td>
<td>T12E8K</td>
<td>0</td>
</tr>
<tr>
<td>2017</td>
<td>05</td>
<td>T12E8K</td>
<td>0</td>
</tr>
<tr>
<td>2017</td>
<td>06</td>
<td>T12E8K</td>
<td>345.6</td>
</tr>
<tr>
<td>2017</td>
<td>07</td>
<td>T12E8K</td>
<td>325.61</td>
</tr>
<tr>
<td>2017</td>
<td>08</td>
<td>T12E8K</td>
<td>327.53</td>
</tr>
</tbody>
</table>
Chargeback Report - Pay as RA Storage is Utilized - cont’d

Monthly cost for this database on tape.

![Copy to Tape Chargeback - Budgetary Breakdown](chart)

<table>
<thead>
<tr>
<th>Year</th>
<th>Month</th>
<th>Database</th>
<th>Chargeback Amount</th>
<th>Chargeback Amount Delta</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017</td>
<td>03</td>
<td>T12E8K</td>
<td>$0.00</td>
<td>$0.00</td>
</tr>
<tr>
<td>2017</td>
<td>04</td>
<td>T12E8K</td>
<td>$0.00</td>
<td>$0.00</td>
</tr>
<tr>
<td>2017</td>
<td>05</td>
<td>T12E8K</td>
<td>$0.00</td>
<td>$0.00</td>
</tr>
<tr>
<td>2017</td>
<td>06</td>
<td>T12E8K</td>
<td>$3.45</td>
<td>$3.45</td>
</tr>
<tr>
<td>2017</td>
<td>07</td>
<td>T12E8K</td>
<td>$3.26</td>
<td>($0.19)</td>
</tr>
<tr>
<td>2017</td>
<td>08</td>
<td>T12E8K</td>
<td>$3.28</td>
<td>$0.02</td>
</tr>
</tbody>
</table>
Agenda

1. Understand Requirements First
2. RA Deployment Decisions and Key Practices
3. RA Stay Healthy Plan
4. Best Practices Backup and Restore
5. Migration with ZDLRA
6. Oracle Support & Service Request
7. RA Roles and Responsibilities
Backup & Configuration Overview

Steps to Backup & Configure a Database using Enterprise Manager Cloud Control

- Create Protection Policy on Recovery Appliance (RA)
- Add Protected Database to RA
- Configure Backup Settings for Protected Database
- Schedule **ONE-TIME** Level 0 (Full) Backup with “Custom Backup”, then Level 1s with “Oracle-Suggested Recovery Appliance Backup”
What To Do With Existing Backups?

RMAN backups to disk or NFS share (including Data Domain share)
  • Can be imported into the Recovery Appliance via “polling”
  • Become part of the Incremental Forever strategy on the RA

Backups taken using 3rd party backup software
  • Leave the agent in place on the protected DB hosts until retention expires
  • Leverage dual backup (disk & tape) strategy if needed in interim
  • Removing agents saves system resources
Backup Best Practices

Use Transparent Data Encryption (TDE) instead of RMAN encryption
  • RMAN encryption will prevent ZDLRA from creating Virtual Full Backups (VB$).

Use native database compression instead of RMAN compression
  • RMAN compression will result in additional CPU utilization on the Protected Database client
  • RMAN compressed backups require decompression and recompression on the ZDLRA

Use block change tracking for all protected databases

```
rman target <target string> catalog <catalog string>
  backup  device type sbt
    cumulative incremental level 1
  filesperset 1  section size 64g  database
  plus archivelog  not backed up  filesperset 32;
```
Impact of TDE Encryption

Advanced Security Option requires a Level 0 when:

• first key (encrypt) a tablespace
• rekey a tablespace
• masterkey rotation

• If RA upgraded to 19.2.1.2-RELEASE or later ( RA takes a level 0 as needed )

When you first key (encrypt), rekey a tablespace or master key rotation
• The next L1 backup will automatically create the level 0 of datafiles required as necessary via Smart Incremental feature.

• If RA version is 12.2.1.2-201810-RELEASE (INTERIM 1) OCT 2018 PSU but less than 19.2.1.2-RELEASE

When you first key (encrypt) or rekey a tablespace or master key rotation
• The NEXT backup for that tablespace MUST be a level 0

Avoid RMAN compression against a TDE tablespace as RMAN encryption will be automatically enabled, preventing the RA from creating Virtual Backups.
Backup Best Practices – Cont.

Incremental level 0 (full) as first backup
Subsequent cumulative incremental level 1 backups “Incremental Forever”
Use section size of 64GB
Use filesperset 1 for one datafile per backupset
Limit channel allocation to 4 per node

Virtual Full Backup Creation Monitoring

• After a L1 incremental backup: RA indexes it and builds the corresponding Virtual Full. Check EM or SAR for error messages like “ORA-64760: Database XYZ has had tasks in ordering wait state for over X days.”
• Refer to MOS note: Diagnostic SQL script for tasks in ORDERING_WAIT status on Recovery Appliance (Doc ID 2095949.1)
Restore & Recovery Best Practices

Use RMAN Restore Database / Recover Database as you would today

- No new RMAN commands to learn. Intelligent built-in recovery catalog in RA
- RMAN is aware of the validated backups on disk, tape or replica. Restore is transparent and simple
- Restore directly from tape or RA Replica without staging on local RA if local disk backups are not present

Performance considerations

- Maximize # of RMAN channels for Restore: Consider other active databases on a target.
- Restore operations are always auto prioritized within RA without preventing other backup operations
- BCT: Works against the most recent VL Full. With cumulative, BCT will stop if VLF 7 days out.

Bigfile Tablespace Practices and Considerations (recall backup best practice using SECTION SIZE)

- Oracle 11g databases can restore initial L0 with SECTION SIZE to parallelize sections across channels
  - Restoring virtual fulls (created from L1s) does parallelize sections (As of RA Software 12.1.1.8.201710)
- Oracle 12c databases can restore L0 and virtual fulls with SECTION SIZE parallelism across channels
Agenda

1. Understand Requirements First
2. RA Deployment Decisions and Key Practices
3. RA Stay Healthy Plan
4. Best Practices Backup and Restore
5. Migration with ZDLRA
6. Oracle Support & Service Request
7. RA Roles and Responsibilities
Database Migration Process using ZDLRA

Cross Endian - Big Endian ↔ Little Endian

Uses Virtual Level 0 backup of source database and Restore/Recover on destination

Refer to MOS Note: Cross Platform Database Migration using ZDLRA (Doc ID 2460552.1)

Same Endian - Leverage Data Guard

Data Guard Support for Heterogeneous Primary and Physical Standby in Same Data Guard Configuration (Doc ID 413484.1)

Creating a Physical Standby Database in an 11.2, 12.1, 12.2 or later environment (Doc ID 2275154.1)

Source database backups available on the ZDLRA, instantiate new database on the destination platform using RMAN DUPLICATE FOR STANDBY

1When using RMAN to DUPLICATE a database, connect to the ZDLRA as CATALOG and configure the RMAN AUXILIARY SBT channels for the ZDLRA.
Cross Platform DB Migration using ZDLRA - Benefits

Primary benefits:
• Significant reduction in downtime (Potentially less than 2 hours of service downtime)
• Application service is Read Only during most of the service downtime
• New ZDLRA tool (dbmigusera.pl) simplifies cross platform migration by automating steps, especially useful for large databases
• Migration time is not impacted by the size of the database
• Supports migration to the same or higher DB version

Read Only downtime based on
• Final incremental backup & recovery step Incremental size < 5% of the database
• Final tablespace metadata export/import duration (only necessary for cross platform)
• Number of target tablespaces – import is done serially
• Application service switchover from source to destination database
Leverage Data Guard and ZDLRA - Benefits

Primary benefits:

• Near-Zero to Zero downtime during switchover to destination database
• Increased availability during the migration process vs transportable tablespace approach
• With Active Data Guard, standby database can be used to offload read-only activities from primary (e.g. reporting), until switchover is performed
Agenda

1. Understand Requirements First
2. RA Deployment Decisions and Key Practices
3. RA Stay Healthy Plan
4. Best Practices Backup and Restore
5. Migration with ZDLRA
6. Oracle Support & Service Request
7. RA Roles and Responsibilities
Opening a Service Request
Proactively update the SR with as MUCH details as you can
*** critical time-sensitive information might be lost! ***

1. Problem statement with Use Case, Timeline (before problem, any changes, when problem occurs)
2. Impact Analysis
3. Refer to MOS notes:
   - SRDC - Zero Data Loss Recovery Appliance (ZDLRA) Data Collection (Doc ID 2154189.1)
   - Zero Data Loss Recovery Appliance System Activity Script (Doc ID 2275176.1)
   - ZDLRA Detailed Troubleshooting Methodology (Doc ID 2408256.1)
   - How to create a Technical Service Request (SR) in My Oracle Support (Doc ID 1321379.1)
   - How to Create Service Requests for Software Issues Using a Hardware Support Identifier (Doc ID 1439980.1)
   - Who to contact to discuss details, corrections or changes to a Support Contract (Doc ID 1250376.1)
4. Remember to escalate an SR which is not progressing to your satisfaction. Escalation brings management attention to the issue. You can escalate an SR of any severity
Escalations: Bringing Management Attention to your Service Request

Asking to increase the severity of your service request is NOT an escalation, even though customers follow the same process.

An escalation is bringing Oracle Support Management’s attention to your service request:

- **Proactive reasons to escalate an issue:**
  - Communicate business issues to managers within Oracle Support

- **Reactive reasons to escalate an issue**
  - Encountering critical roadblocks
  - Dissatisfied with resolution or response

Describe Impact of Problem: Project deadlines?, Lost Revenue?, Government reporting? Increase in Recoverability and Data Loss Potential
How to Escalate or Change Severity

1. Call the 24x7 Support Hotline
   Toll Free: 0800.891.5899
   http://www.oracle.com/support/contact.html

2. Choose option #1 for an existing service request

3. Enter all digits of the SR number followed by #

4. Choose the option to **ESCALATE** the SR
   Do **NOT** choose the option to speak to the owning engineer, **you want to speak to an Escalation Manager** (formerly called Duty Manager) in order to escalate or change the severity of the SR. Always request a call back from the Escalation Manager when escalating an SR!

Engineered Systems Hardware Replacements:
   Choose the option for Field Delivery Dispatch to schedule, change or check the status of a Field Engineer visit for hardware replacement
When Calling for Engineered Sys. Support...

The following options will direct your call to the relevant team:

Press "1" for Existing Service Requests
• Enter Service Request#. If lookup is successful:
  • Press “1” to speak to the engineer working your service request
    • If Engineer is available, call will connect
    • If engineer is not available
      • Press “1” to leave VM or,
      • Press “2” to speak to the next available EEST engineer
  • If there is no FS Task, press “2” to Escalate the Service Request
  • If there is a FS task,
    • Press “2” for Field Delivery Dispatch
    • Press “3” for Escalation Request

Press “2” for New Service Requests
• Press “1” Engineered Systems
  • For Technical Product Issues Press “1”
  • For Non-Technical Issues such as My Oracle Support or Support Identifier Issues Press “2”
## Service Request Severity Levels

<table>
<thead>
<tr>
<th>Severity Level</th>
<th>Business &amp; Technical Impact</th>
<th>1st Response</th>
<th>Update Frequency</th>
<th>Resolution Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Mission Critical Business Impact</td>
<td>&lt; 1 Hour (telephone preferred)</td>
<td>Continual Updates 24x7</td>
<td>Co-Owned</td>
</tr>
<tr>
<td>2</td>
<td>Serious Business Impact</td>
<td>Communication Preference</td>
<td>Multiple Updates 24-48 hours</td>
<td>Co-Owned</td>
</tr>
<tr>
<td>3</td>
<td>Minor Business Impact</td>
<td>Communication Preference</td>
<td>Updates 2-3 Business Days</td>
<td>Co-Owned</td>
</tr>
<tr>
<td>4</td>
<td>No Business Impact</td>
<td>Communication Preference</td>
<td>Updates 3-5 Business Days</td>
<td>Co-Owned</td>
</tr>
</tbody>
</table>
**Platinum Support for Recovery Appliance**

**Integrated Support**
- 24/7 HW and SW support
- Consistent service across the stack from single vendor
- SW and OS updates included
- Integrated online support interface – My Oracle Support

**Proactive Support Tools**
- Personalized health checks
- Advanced knowledge sharing and communities
- Integrated stack delivery with Oracle Enterprise Manager
- Converged HW mgmt with Oracle Enterprise Manager Ops Center

**Monitoring & Patching**
- 24/7 remote fault monitoring
- Industry-leading response times:
  - 5-min fault notification
  - 15-min restoration or escalation to development
  - 30-min joint debugging
- Risk mitigation and business innovation through patch deployment

---

ORACLE PREMIER SUPPORT → PLATINUM
Agenda

1. Understand Requirements First
2. RA Deployment Decisions and Key Practices
3. RA Stay Healthy Plan
4. Best Practices Backup and Restore
5. Migration with ZDLRA
6. Oracle Support & Service Request
7. RA Roles and Responsibilities
Typical questions from new ZDLRA customers

1. **Who** will manage this?
2. **How** will my team support it?

This section provides information to help you answer these questions.
The Starting Point: A Set of Specialist Teams

- **Database Administrators**
- **Storage Administrators**
- **System Administrators**
- **Network Administrators**
- **Security Administrators**
Option 1: Multiple Specialist Teams *(status quo\(^1\))*

1. Each team is assigned a specific ZDLRA set of responsibilities.
Option 2: **Extended RA Team**

1. **Primary stakeholders**
   - Database Administrators
   - Storage Administrators

2. **Secondary stakeholders**
   - System Administrators
   - Network Administrators
   - Security Administrators

1. Perform main ZDLRA monitoring & administration activities.

2. Perform additional tasks required by the main stakeholders.
Option 3: RA Machine Administrator

Centralized stakeholders

1-Responsible for all ZDLRA activities including monitoring, administration and maintenance.

Database Administrators
Storage Administrators

System Administrators
Network Administrators
Security Administrators
## Operational Model 1: Multiple Specialist Teams

**RASCI Model - Multiple Specialist Teams**

### RACI Legend:
- **R** = Responsible
- **A** = Accountable
- **S** = Supportive
- **C** = Consulted
- **I** = Informed

<table>
<thead>
<tr>
<th>Task</th>
<th>DBA</th>
<th>SYSADMIN</th>
<th>NETWORK</th>
<th>STORAGE</th>
<th>CIO</th>
<th>SECURITY</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Day-to-day Operation</strong></td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>A</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td><strong>Testing</strong></td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>A</td>
<td>C/I</td>
<td></td>
</tr>
<tr>
<td><strong>Monitoring</strong></td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>A</td>
<td>C/I</td>
<td></td>
</tr>
<tr>
<td><strong>Configuration Management</strong></td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>A</td>
<td>C/I</td>
<td></td>
</tr>
<tr>
<td><strong>Patching</strong></td>
<td>R</td>
<td>C</td>
<td>R</td>
<td>A</td>
<td>C/I</td>
<td></td>
</tr>
<tr>
<td><strong>Storage Cells</strong></td>
<td>C</td>
<td>R</td>
<td></td>
<td>A</td>
<td>C/I</td>
<td></td>
</tr>
<tr>
<td><strong>InfiniBand</strong></td>
<td>C</td>
<td>R</td>
<td></td>
<td>A</td>
<td>C/I</td>
<td></td>
</tr>
<tr>
<td><strong>Cisco Public Network</strong></td>
<td>C</td>
<td>R</td>
<td></td>
<td>A</td>
<td>C/I</td>
<td></td>
</tr>
<tr>
<td><strong>Db Compute Nodes OS</strong></td>
<td>C</td>
<td>R</td>
<td></td>
<td>A</td>
<td>C/I</td>
<td></td>
</tr>
<tr>
<td><strong>Database</strong></td>
<td>R</td>
<td>A</td>
<td></td>
<td>A</td>
<td>C/I</td>
<td></td>
</tr>
<tr>
<td><strong>Back Up RA</strong></td>
<td>R</td>
<td>R</td>
<td></td>
<td>A</td>
<td>C/I</td>
<td></td>
</tr>
<tr>
<td><strong>Upgrading SW</strong></td>
<td>R</td>
<td>R</td>
<td></td>
<td>A</td>
<td>C/I</td>
<td></td>
</tr>
<tr>
<td><strong>Replacing HW</strong></td>
<td>R</td>
<td>R</td>
<td></td>
<td>A</td>
<td>C/I</td>
<td></td>
</tr>
<tr>
<td><strong>Metering and Charging</strong></td>
<td>R</td>
<td>R</td>
<td></td>
<td>A</td>
<td>C/I</td>
<td></td>
</tr>
</tbody>
</table>
## Operational Model 2: Extended RA Team (ERMA)

### RACI Legend:
- **R** = Responsible
- **A** = Accountable
- **S** = Supportive
- **C** = Consulted
- **I** = Informed

<table>
<thead>
<tr>
<th>Task</th>
<th>DBA</th>
<th>SYSADMIN</th>
<th>NETWORK</th>
<th>STORAGE</th>
<th>CIO</th>
<th>SECURITY</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Day-to-day Operation</strong></td>
<td>R</td>
<td>S</td>
<td>S</td>
<td></td>
<td>A</td>
<td>C</td>
</tr>
<tr>
<td>Testing</td>
<td>R</td>
<td>S</td>
<td>S</td>
<td></td>
<td>A</td>
<td>C/I</td>
</tr>
<tr>
<td>Monitoring</td>
<td>R</td>
<td></td>
<td></td>
<td></td>
<td>A</td>
<td>C/I</td>
</tr>
<tr>
<td>Configuration Management</td>
<td>R</td>
<td></td>
<td></td>
<td></td>
<td>A</td>
<td>C/I</td>
</tr>
<tr>
<td>Patching</td>
<td>R</td>
<td></td>
<td></td>
<td></td>
<td>A</td>
<td>C/I</td>
</tr>
<tr>
<td>Storage Cells</td>
<td>R</td>
<td></td>
<td></td>
<td></td>
<td>A</td>
<td>C/I</td>
</tr>
<tr>
<td>InfiniBand</td>
<td>R</td>
<td>S</td>
<td></td>
<td></td>
<td>A</td>
<td>C/I</td>
</tr>
<tr>
<td>Cisco Public Network</td>
<td>R</td>
<td>S</td>
<td></td>
<td></td>
<td>A</td>
<td>C/I</td>
</tr>
<tr>
<td>Db Compute Nodes OS</td>
<td>R</td>
<td>S</td>
<td></td>
<td></td>
<td>A</td>
<td>C/I</td>
</tr>
<tr>
<td>Database</td>
<td>R</td>
<td></td>
<td></td>
<td></td>
<td>A</td>
<td>C/I</td>
</tr>
<tr>
<td>Backing Up RA</td>
<td>R</td>
<td></td>
<td></td>
<td></td>
<td>A</td>
<td>C/I</td>
</tr>
<tr>
<td>Upgrading SW</td>
<td>R</td>
<td>S</td>
<td>S</td>
<td></td>
<td>A</td>
<td>C/I</td>
</tr>
<tr>
<td>Replacing HW</td>
<td>R</td>
<td>S</td>
<td>S</td>
<td></td>
<td>A</td>
<td>C/I</td>
</tr>
<tr>
<td>Metering and Charging</td>
<td>R</td>
<td></td>
<td></td>
<td></td>
<td>A</td>
<td>C/I</td>
</tr>
</tbody>
</table>
Operational Model 3: RA Machine Administrator (RAMA)

RASCI Model - RA MACHINE ADMINISTRATOR

<table>
<thead>
<tr>
<th>Task</th>
<th>DBA</th>
<th>SYSADMIN</th>
<th>NETWORK</th>
<th>STORAGE</th>
<th>CIO</th>
<th>SECURITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Day-to-day Operation</td>
<td>R</td>
<td></td>
<td>A</td>
<td>C</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Testing</td>
<td>R</td>
<td></td>
<td>A</td>
<td>C/I</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Monitoring</td>
<td>R</td>
<td></td>
<td>A</td>
<td>C/I</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configuration Management</td>
<td>R</td>
<td></td>
<td>C</td>
<td>A</td>
<td>C/I</td>
<td></td>
</tr>
<tr>
<td>Patching</td>
<td>R</td>
<td>C/I</td>
<td>A</td>
<td>C/I</td>
<td></td>
<td>C/I</td>
</tr>
<tr>
<td>Storage Cells</td>
<td>R</td>
<td>A</td>
<td>C/I</td>
<td>A</td>
<td></td>
<td>C/I</td>
</tr>
<tr>
<td>InfiniBand</td>
<td>R</td>
<td>C/I</td>
<td>A</td>
<td>C/I</td>
<td></td>
<td>C/I</td>
</tr>
<tr>
<td>Cisco Public Network</td>
<td>R</td>
<td>C/I</td>
<td>A</td>
<td>C/I</td>
<td></td>
<td>C/I</td>
</tr>
<tr>
<td>Db Compute Nodes OS</td>
<td>R</td>
<td>C/I</td>
<td>A</td>
<td>C/I</td>
<td></td>
<td>C/I</td>
</tr>
<tr>
<td>Database</td>
<td>R</td>
<td>A</td>
<td>C/I</td>
<td>A</td>
<td></td>
<td>C/I</td>
</tr>
<tr>
<td>Backing Up RA</td>
<td>R</td>
<td>A</td>
<td>C/I</td>
<td>A</td>
<td></td>
<td>C/I</td>
</tr>
<tr>
<td>Upgrading SW</td>
<td>R</td>
<td>A</td>
<td>C/I</td>
<td>A</td>
<td></td>
<td>C/I</td>
</tr>
<tr>
<td>Replacing HW</td>
<td>R</td>
<td>A</td>
<td>C/I</td>
<td>A</td>
<td></td>
<td>C/I</td>
</tr>
<tr>
<td>Metering and Charging</td>
<td>R</td>
<td>A</td>
<td>C/I</td>
<td>A</td>
<td></td>
<td>C/I</td>
</tr>
</tbody>
</table>

RACI Legend:
- R = Responsible
- A = Accountable
- S = Supportive
- C = Consulted
- I = Informed

Copyright © 2021, Oracle and/or its affiliates
Summary of **Staffing Models**

All three models will work.

You decide what is best in your organization.
OpenWorld Presentations & Resources for Recovery Appliance

OOW 2019:
• Zero Data Loss Recovery Appliance: Expanding Integration with Oracle Cloud
• Zero Data Loss Recovery Appliance: Latest Practices from Oracle Development

OOW 2018:
• Zero Data Loss Recovery Appliance: Leveraging Integration with Oracle Cloud
• Oracle Recovery Manager: Latest Generation Features for On-Premises and the Cloud

ZDLRA MAA Best Practices:
• https://tinyurl.com/zdlramaa

ZDLRA Documentation: