

Database

Level 200

Sanjay Narvekar

November 2018

Safe Harbor Statement

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

Database Service - Objectives

After completing this lesson, you should be able to:

- Describe and utilize the Database command line (CLI) on the Oracle Cloud Infrastructure (OCI) Database systems
- Backup a database and recover from a database backup
- Troubleshoot database backup failures
- Be aware of different database migration methods to move data into OCI Database Systems
- Use the MAA capabilities of OCI for DB Systems

dbcli on OCI Database Systems

- The database command line reference (dbcli) is a command line interface available on bare metal and virtual machine DB systems.
- After you connect to the DB system, you can use the database CLI to perform tasks such as creating Oracle database homes and databases.
- Scope of dbcli commands and operations
 - For the whole system, all homes
 - Backup configurations, operations
 - Database configurations and operations
 - Storage configurations and operations
 - Jobs
 - Object storage and swift configuration
 - Schedules
 - TDE configuration and reporting

dbcli on OCI Database Systems

- dbcli is on every OCI Database system under `/opt/oracle/dcs/bin/` directory.
- The dbcli commands must be run as the root user.
- Oracle Database maintains logs of the dbcli command output in the `dcsccli.log` and `dcs-agent.log` files in the `/opt/oracle/dcs/log/` directory.
- The database CLI commands and most parameters are case sensitive and should be typed as shown.
- The database CLI commands use the following syntax:

dbcli command [parameters]

where:

- command is a verb-object combination such as **create-database**.
- parameters include additional options for the command. Most parameter names are preceded with two dashes, for example, `--help`.
- User-specified parameter values are shown in red text within angle brackets, for example, `<db_home_id>`. Omit the angle brackets when specifying these values.
- The help parameter is available with every command.

dbcli on OCI Database Systems

CLI Update Command

Occasionally, new commands are added to the database CLI and other commands are updated to support new features. You can use the following command to update the database CLI:

cliadm update-dbcli

Use the cliadm update-dbcli command to update the database CLI with the latest new and updated commands.

Examples for dbcli commands

- dbcli create-database -n crmdb -hm <password> -cl OLTP -s odb2

This creates a database called crmdb of database class OLTP and using the odb2 database shape.

- dbcli create-dbhome -v 12.1.0.2

This creates an Oracle Database Home version 12.1.0.2

https://docs.cloud.oracle.com/iaas/Content/Database/References/dbacl.htm?TocPath=Services|Database|Bare%20Metal%20and%20Virtual%20Machine%20DB%20Systems|_____12

Database Sizing Templates

When you create a database using the `dbcli create-database` command, you can specify a database sizing template with the `--dbshape` parameter. The sizing templates are configured for different types of database workloads. Choose the template that best matches the most common workload your database performs:

- Use the OLTP templates if your database workload is primarily online transaction processing (OLTP).
- Use the DSS templates if your database workload is primarily decision support (DSS) or data warehousing.
- Use the in-memory (IMDB) templates if your database workload can fit in memory, and can benefit from in-memory performance capabilities.

https://docs.cloud.oracle.com/iaas/Content/Database/References/sizingtemplates.htm?tocpath=Services%7CDatabase%7CBare%20Metal%20and%20Virtual%20Machine%20DB%20Systems%7C_____13

Backing up to Oracle Cloud Infrastructure Object Storage

Backing up to OCI Object storage

This topic explains how to work with backups managed by Oracle Cloud Infrastructure. You do this by using the Console or the API.

Required IAM Policy

To use Oracle Cloud Infrastructure, you must be given the required type of access in a policy written by an administrator, whether you're using the Console or the REST API with an SDK, CLI, or other tool.

Prerequisites

- The DB system's cloud network (VCN) must be configured with either a service gateway or an internet gateway.
- Your DB system must have connectivity to the applicable Swift endpoint for Object Storage.
- Ensure that the database's archiving mode is set to ARCHIVELOG (the default).
- Ensure that /u01 directory on the database host file system has sufficient free space for the execution of backup processes.
- The .bash_profile file for the oracle user does not include any interactive commands (such as oraenv or one that could generate an error or warning message).

<https://docs.cloud.oracle.com/iaas/Content/Database/Tasks/backingupOS.htm>

Backing up to OCI Object storage

- (For automatic backups) No changes were made to the default WALLET_LOCATION entry in the sqlnet.ora file.
- No changes were made to RMAN backup settings by using standard RMAN commands.

Using the Console

- You can use the Console to enable automatic incremental backups, create full backups on demand, and view the list of managed backups for a database. The Console also allows you to delete full backups.
- The database and DB system must be in an “Available” state for a backup operation to run successfully.
- Oracle recommends that you avoid performing actions that could interfere with availability (patching, Data Guard operations).
- If an automatic backup operation fails, the Database service retries the operation during the next day’s backup window.
- If an on-demand full backup fails, you can try the operation again when the DB system and database availability are restored.

<https://docs.cloud.oracle.com/iaas/Content/Database/Tasks/backingupOS.htm>

Backing up to OCI Object storage

Automatic Incremental Backups

- When you enable the Automatic Backup feature, the service creates daily incremental backups of the database to Object Storage.
- The first backup created is a level 0 backup.
- Then, level 1 backups are created every day until the next weekend.
- Every weekend, the cycle repeats, starting with a new level 0 backup.
- The automatic backup process can run at any time within the daily backup window (between midnight and 6:00 am UTC).
- Automatic incremental backups are retained in Object Storage for 30 days.
- After 30 days, the system automatically deletes your incremental backups.

Note

You can enable the Automatic Backup feature on a database with the standby role in a Data Guard association. However, automatic backups for that database will not be created until it assumes the primary role.

<https://docs.cloud.oracle.com/iaas/Content/Database/Tasks/backingupOS.htm>

Backing up to OCI Object storage

On-Demand Full Backups

You can create a full backup of your database at any time unless your database is assuming the standby role in a Data Guard association.

Standalone Backups

When you terminate a DB system or a database, all of its resources are deleted, along with any automatic backups.

Full backups remain in Object Storage as standalone backups.

You can use a standalone backup to create a new database.

<https://docs.cloud.oracle.com/iaas/Content/Database/Tasks/backingupOS.htm>

Recovering a Database from Object Storage

Recovering a Database from Object storage

This topic explains how to recover a database from a backup stored in Object Storage. You can recover a database using the Console, API, or by using RMAN.

Required IAM Policy

To use Oracle Cloud Infrastructure, you must be given the required type of access in a policy written by an administrator, whether you're using the Console or the REST API with an SDK, CLI, or other tool.

Prerequisites

- The DB system's cloud network (VCN) must be configured with either a service gateway or an internet gateway.
- Your DB system must have connectivity to the applicable Swift endpoint for Object Storage.

Using the Console

You can use the Console to restore the database from a backup in the Object Storage that was created by using the Console or the API. You can restore to the last known good state of the database, or you can specify a point in time or an existing System Change Number (SCN). You can also create a new database by using a standalone backup.

<https://docs.cloud.oracle.com/iaas/Content/Database/Tasks/recoveringOS.htm>

Recovering a Database from Object storage

Note

- The list of backups you see in the Console does not include any unmanaged backups (backups created directly by using RMAN or dbcli).
- Restoring a database with Data Guard enabled is not supported. You must first remove the Data Guard association by terminating the standby database before you can restore the database.

Creating a New Database from a Backup

You can use a standalone backup to create a database in an existing DB system or to launch a new DB system.

Using an RMAN Backup

You can also recover a Recovery Manager (RMAN) backup stored in Object Storage.

<https://docs.cloud.oracle.com/iaas/Content/Database/Tasks/recoveringOS.htm>

Troubleshooting Database Backup Failures

Backup Failures

Database backups can fail for various reasons. Typically, a backup fails because either the database host cannot access the object store, or there are problems on the host or with the database configuration.

Determining the problem: In the Console, a failed database backup either displays a status of **Failed** or hangs in the **Backup in Progress** or **Creating** state. If the error message does not contain enough information to point you to a solution, you can use the database CLI and log files to gather more data.

Steps to identify the root cause of the backup failure

1. Log on to the host as the root user and navigate to the /opt/oracle/dcs/bin/ directory.
2. Determine the sequence of operations performed on the database.

```
dbcli list-jobs | grep -i <dbname>
```

Note the last job ID listed with a status other than **Success**.

3. With the job ID you noted from the previous step, use the following command to check the details of that job:

```
dbcli describe-job -i <job_ID> -j
```

Typically, running this command is enough to reveal the root cause of the failure.

Backup Failures

4. If you require more information, review the `/opt/oracle/dcs/log/dcs-agent.log` file.

You can find the job ID in this file by using the timestamp returned by the job report in step 2.

5. If the problem details suggest an RMAN issue, review the RMAN logs in the `/opt/oracle/dcs/log/<hostname>/rman/bkup/<db_unique_name>/rman_backup/<yyyy-mm-dd>` directory.

Note: If the database failure is on a 2-node RAC database, perform steps 3 and 4 on both nodes.

Backup failures due to database Service Agent Issues

The Oracle Cloud Infrastructure Database makes use of an agent framework to allow you to manage your database through the cloud platform. Occasionally you might need to restart the dcsagent program if it has the status of stop/waiting to resolve a backup failure.

Steps to restart the database service agent

1. From a command prompt, check the status of the agent:

```
initctl status initdcsagent
```

Backup Failures

2. If the agent is in the **stop/waiting** state, try to restart the agent:

```
initctl start initdcsagent
```

3. Check the status of the agent again to confirm that it has the **start/running** status:

```
initctl status initdcsagent
```

Backup failures due to Oracle Clusterware Issues

Oracle Clusterware enables servers to communicate with each other so that they can function as a collective unit. Occasionally you might need to restart the Clusterware program to resolve a backup failure.

Steps to restart the Oracle Clusterware

1. From command prompt, check the status of Oracle Clusterware:

```
crsctl check crs
```

```
crsctl stat res -t
```

Backup Failures

2. If Oracle Clusterware is not online, try to restart the program:

```
crsctl start crs
```

3. Check the status of Oracle Clusterware to confirm that it is online:

```
crsctl check crs
```

Backup failures due to Object Store Connectivity Issues

Backing up your database to Oracle Cloud Infrastructure Object Storage requires that the host can connect to the applicable Swift endpoint. You can test this connectivity by using a Swift user.

To ensure your database host can connect to the object store

1. Create a Swift user in your tenancy.
<https://docs.cloud.oracle.com/iaas/Content/Identity/Tasks/managingcredentials.htm#Working>
2. With the user you created in the previous step, use the following command to verify the host can access the object store.

```
curl -v -X HEAD -u <user_ID>:'<auth_token>' https://swiftobjectstorage.<region_name>.oraclecloud.com/v1/<tenant>
```

See <https://cloud.oracle.com/infrastructure/storage/object-storage/faq> for the correct region to use.

Backup Failures

3. If you cannot connect to the object store, refer to Prerequisites for how to configure object store connectivity.

<https://docs.cloud.oracle.com/iaas/Content/Database/Tasks/backingupOS.htm#Prerequi>

Backup failures due to Host Issues

One or more of the following conditions on the database host can cause backups to fail:

Interactive Commands in the Oracle Profile

If an interactive command such as `oraenv`, or any command that might return an error or warning message, was added to the `.bash_profile` file for the `grid` or `oracle` user, Database service operations like automatic backups can be interrupted and fail to complete. Check the `.bash_profile` file for these commands, and remove them.

The File System Is Full

Backup operations require space in the `/u01` directory on the host file system. Use the `df -h` command on the host to check the space available for backups. If the file system has insufficient space, you can remove old log or trace files to free up space.

Backup Failures

Incorrect Version of the Oracle Database Cloud Backup Module

Your system might not have the required version of the backup module (opc_installer.jar). See Unable to use Managed Backups in your DB System for details about this known issue. To fix the problem, you can follow the procedure in that section or simply update your DB system and database with the latest bundle patch.

Changes to the Site Profile File (glogin.sql)

Customizing the site profile file (\$ORACLE_HOME/sqlplus/admin/glogin.sql) can cause managed backups to fail in Oracle Cloud Infrastructure. In particular, interactive commands can lead to backup failures. Oracle recommends that you not modify this file for databases hosted in Oracle Cloud Infrastructure.

Backup failures due to Database Issues

An improper database state or configuration can lead to failed backups.

Database not running during backup

The database must be active and running while the backup is in progress.

See <https://docs.cloud.oracle.com/iaas/Content/Database/Troubleshooting/Backup/backupfail.htm> for steps to check the database is active and running.

Backup Failures

Archiving Mode Set to NOARCHIVELOG

When you provision a new database, the archiving mode is set to ARCHIVELOG by default. This is the required archiving mode for backup operations. Check the archiving mode setting for the database and change it to ARCHIVELOG, if applicable.

See <https://docs.cloud.oracle.com/iaas/Content/Database/Troubleshooting/Backup/backupfail.htm> for steps to check and set the archiving mode.

Stuck Database Archiver Process and Backup Failures

Backups can fail when the database instance has a stuck archiver process. For example, this can happen when the flash recovery area (FRA) is full.

Temporary Tablespace Errors

If fixed table statistics are not up to date on the database, backups can fail with errors referencing temporary tablespace present in the dcs-agent.log file

See <https://docs.cloud.oracle.com/iaas/Content/Database/Troubleshooting/Backup/backupfail.htm> for steps to check and fix the errors related to archiver process and temporary tablespace errors.

Backup Failures

RMAN Configuration and Backup Failures

Editing certain RMAN configuration parameters can lead to backup failures in Oracle Cloud Infrastructure.

See <https://docs.cloud.oracle.com/iaas/Content/Database/Troubleshooting/Backup/backupfail.htm> for RMAN configuration settings that should not be altered.

RMAN Retention Policy and Backup Failures

The RMAN retention policy configuration can be the source of backup failures. Using the REDUNDANCY retention policy configuration instead of the RECOVERY WINDOW policy can lead to backup failures. Be sure to use the RECOVERY WINDOW OF 30 DAYS configuration.

See <https://docs.cloud.oracle.com/iaas/Content/Database/Troubleshooting/Backup/backupfail.htm> for configuring RMAN retention policy setting.

Loss of Object store wallet file and Backup Failures

RMAN backups fail when an objectstore wallet file is lost. The wallet file is necessary to enable connectivity to the object store.

See <https://docs.cloud.oracle.com/iaas/Content/Database/Troubleshooting/Backup/backupfail.htm> to confirm that the object store wallet file exists and has the correct permissions.

Backup Failures

TDE Wallet and Backup Failures

Incorrect TDW Wallet Location Specification

For backup operations to work, the \$ORACLE_HOME/network/admin/sqlnet.ora file must contain the ENCRYPTION_WALLET_LOCATION parameter formatted exactly as follows:

```
ENCRYPTION_WALLET_LOCATION=(SOURCE=(METHOD=FILE)(METHOD_DATA=(DIRECTORY=/opt/oracle/dcs/commonstore/wallets/tde/$ORACLE_UNQNAME)))
```

See <https://docs.cloud.oracle.com/iaas/Content/Database/Troubleshooting/Backup/backupfail.htm> for steps to check the TDE wallet location specification.

Incorrect State of the TDW Wallet

Database backups fail if the TDE wallet is not in the proper state. The following scenarios can cause this problem:

- The ORACLE_UNQNAME environment variable was not set when the database was started using SQL*Plus
- A pluggable database was added with an incorrectly configured master encryption key

See <https://docs.cloud.oracle.com/iaas/Content/Database/Troubleshooting/Backup/backupfail.htm> for steps to fix this

Backup Failures

Incorrect Configuration Related to the TDW Wallet

Several configuration parameters related to the TDE wallet can cause backups to fail.

See <https://docs.cloud.oracle.com/iaas/Content/Database/Troubleshooting/Backup/backupfail.htm> to check configuration related to the TDW wallet.

Missing TDW Wallet File

The TDE wallet file (ewallet.p12) can cause backups to fail if it is missing, or if it has incompatible file system permissions or ownership.

See <https://docs.cloud.oracle.com/iaas/Content/Database/Troubleshooting/Backup/backupfail.htm> to check the TDW wallet file permissions.

Missing Auto Login Wallet File

The auto login wallet file (cwallet.sso) can cause backups to fail if it is missing, or if it has incompatible file system permissions or ownership.

See <https://docs.cloud.oracle.com/iaas/Content/Database/Troubleshooting/Backup/backupfail.htm> to check the Auto Login wallet file permissions.

Backup Failures

Other Causes of Backup Failures

Unmounted Commonstore Mount Point

The mount point /opt/oracle/dcs/commonstore must be mounted, or backups will fail.

See <https://docs.cloud.oracle.com/iaas/Content/Database/Troubleshooting/Backup/backupfail.htm> to check the commonstore mount point and confirm that ora.data.commonstore.acfs is online.

The Database is Not Properly Registered

Database backups fail if the database is not registered with the dcs-agent. This scenario can occur if you manually migrate the database to Oracle Cloud Infrastructure and do not run the `dbcli register-database` command.

To check whether the database is properly registered, review the information returned by running the **srvctl config database** command and the **dbcli list-databases** command. If either command does not return a record of the database, contact Oracle Support Services.

See [Registering the Database on the DB System](#) for instructions on how to register the database.

Collecting database and diagnostic information to resolve errors

See <https://docs.cloud.oracle.com/iaas/Content/Database/Troubleshooting/Backup/backupfail.htm> for information on collecting database and diagnostic information.

1. Database information for use in problem reports
2. Diagnostic information regarding failed jobs
3. DCS agent log files
4. Transparent Data Encryption (TDE) configuration details

Migrating Databases to Oracle Cloud Infrastructure

Migrate your existing Oracle Database to an Oracle Cloud Infrastructure DB System using a number of different methods that use several different tools

- **Migration Methods:** Several methods of migration are available, including Export/Import, Data Pump, Remote Cloning, RMAN, Unplug/Plug PDB, SQL Developer
- **Factors Considered During Migration:** downtime, database size, database versions, database options, database patches, database name, database upgrade (e.g., 11g->12c), Endian Changes, Character Set Matching, data encryption, database block size, database time zone, database multitenancy - CDB or non-CDB.
- **Connectivity:** Speed of connection between existing database and Oracle Cloud Infrastructure. Options include Fastconnect, IPSec tunnels and using the Internet Gateway
- **Bulk Data Transfer:** If database sizes are very large and bandwidth is limited **Bulk Data Transfer Services** for OCI is an option. The bulk data transferred can be resynced reducing overall data transfer bandwidth used.

Guidance for Migrating Databases to Oracle Cloud using object storage

When you want to transfer database backups to Oracle Cloud Infrastructure Object Storage, use the following guidance and options to help you plan and estimate the transfer.

Data Transfer Guidance

The following table provides some high-level guidance based on "theoretical minimums" from over-the-internet data transfer time calculators. Start with these estimates to evaluate the time it might take to transfer your data, but then be sure to test for the actual numbers based on your data volume, network bandwidth, and network reliability.

Note: If uploading data takes longer than 1 to 2 weeks, consider using the Data Transfer service option (see the following section).

	10 Mbps	50 Mbps	100 Mbps	1 Gbps	10 Gbps
5 GB	1+ hours	13+ mins	7+ mins	1+ mins	< 1 min
10 GB	2+ hours	27+ mins	13+ mins	1+ mins	< 1 min
100 GB	23+ hours	4.5+ hours	2.25+ hours	14+ mins	1+ mins
1 TB	9.5+ days	1.5+ days	1+ days	2.25+ hours	14+ mins
5 TB	48+ days	10+ days	5+ days	12+ hours	1.10+ hours
10 TB	100+ days	20+ days	10+ days	1+ days	2.20+ hours

Guidance for Migrating Databases to Oracle Cloud using object storage

Transfer options

Based on your data volume, network bandwidth, and network reliability, use one of the following options to upload the backups to Oracle Cloud Infrastructure (OCI) Object Storage.

Option	Transfer Mode	Options for Copying Data
Public internet	Online	OCI CLI, OCI API, OCI Console, rclone
IPSec VPN	Online	OCI CLI, OCI API, OCI Console, rclone
FastConnect	Online	OCI CLI, OCI API, OCI Console, rclone
Data Transfer service	Offline	cp/scp to NFS mount points
Storage Gateway	Sync	cp/scp to NFS mount points

Guidance for Migrating Databases to Oracle Cloud using object storage

Incremental Backups considerations

Based on your data volume, network bandwidth, and network reliability, you can also upload incremental backups to Object Storage by using the any of the preceding options.

As long as backups are complete and consistent, you can use a combination of transfer options, staggered over a period of time, to transfer the required backups to the target bucket. For example, say that you transferred the bulk of your data by using the Data Transfer service. The incremental backups that occurred since the last level 0 or level 1 backups shipped via the Data Transfer service can be uploaded by using different methods, such as the OCI CLI or rclone, to the same target bucket, which has another level 0/1 backups.

TDE Wallets considerations

As a best practice, we recommend that you do **not** upload TDE wallet files and backups to the same location.

Maximum Availability Architecture (MAA) for Oracle Databases on OCI

Maximum Available Architecture (MAA) Building Blocks in OCI

What's available where?

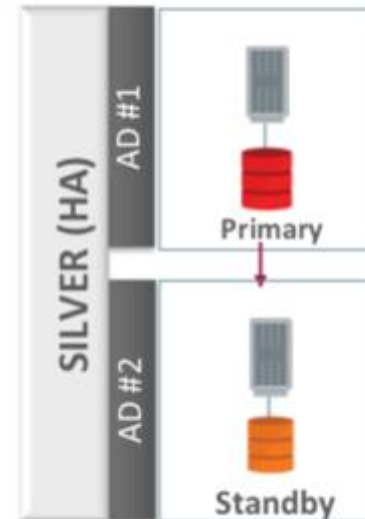
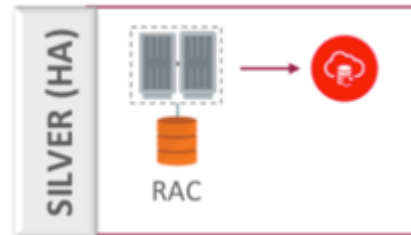
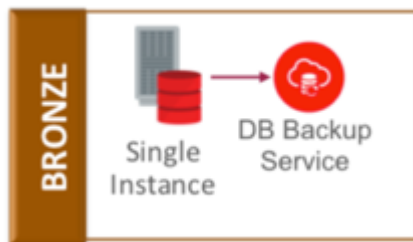
Cloud Infrastructure	Backup/Restore Options	RAC	Active Data Guard	Replication across ADs/Regions
OCI (Bare Metal)	Backup to OCI Object Storage (manual/automatic) Automatic backup copies across Availability Domains (ADs)		☐	Across ADs Across Regions via VCN peering
OCI (Virtual Machine) (with SI or RAC)		☐*	☐	
EXA-OCI (X6, X7)		☐	☐	

*In OCI, RAC VM nodes are now in separate fault domains

MAA Deployment Automation in the Cloud

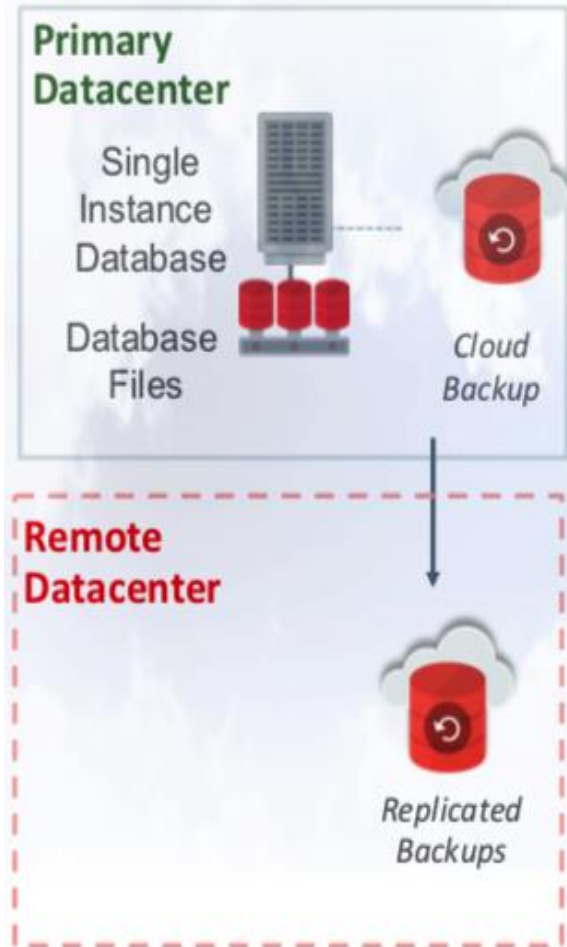
MAA Database Deployment Made Easy

- Databases are provisioned with MAA parameter configurations
- Simple UI / CLI / REST interfaces being configured for MAA topologies
- MAA made easy in the cloud



Bronze: Single Instance Database with Backups

Low cost MAA solution for customers that can tolerate higher RTO and RPO



Bronze Summary	<ul style="list-style-type: none">• Single instance database with backups & auto-restart capabilities with Oracle clusterware• Optional replication of backup• Restore from backup to resume service following unrecoverable outages
Features	<ul style="list-style-type: none">• Oracle Restart Capabilities (enable with Oracle clusterware)• Multitenant Database with PDB features (12c+ DBs)• Online Maintenance (available manually)• Corruption Protection (enabled on OCI)• Flashback Technologies (enabled on OCI)• Recovery Manager and Cloud Storage (all Oracle cloud)• Recovery Appliance (future, available for C@C)

*Backups stored in Object storage are available in the the region across availability domains

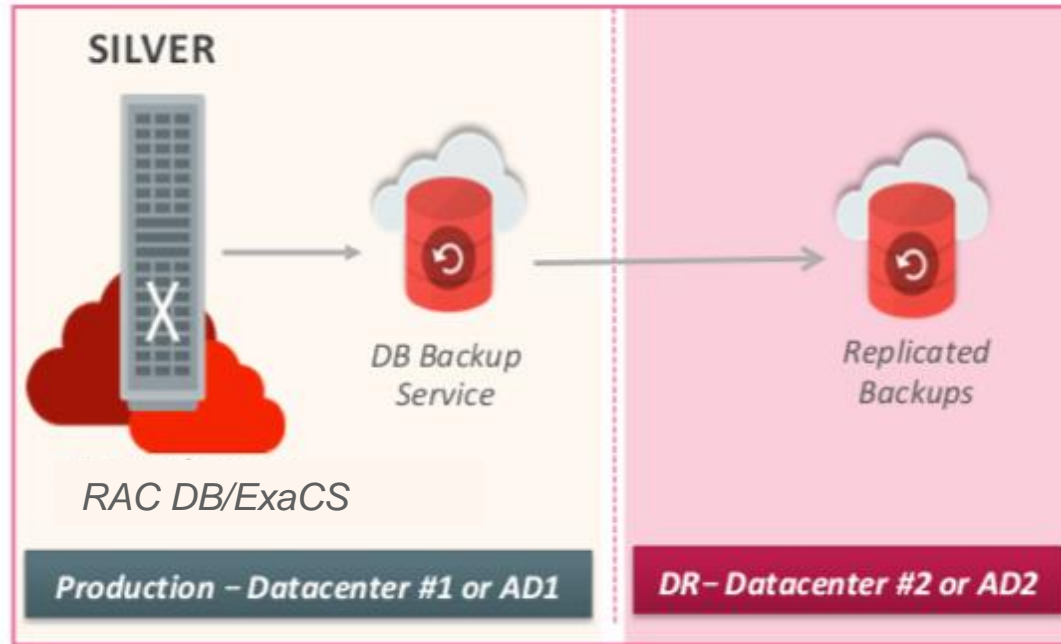
Unplanned Outages and Planned Maintenance

Bronze: Single Instance Oracle Database

	Events	Downtime (RTO)	Data Loss Potential (RPO)
Unplanned Outages	Recoverable Database instance failure	Minutes	Zero
	Recoverable server failure	Minutes to hour	Zero
	Data corruptions, unrecoverable instance, server, database or site failures	Hours to days	Since last backup
Planned Maintenance	Online file move, reorganization/redefinition, and certain patches	Zero	Zero
	Hardware or operating system maintenance and database patches that cannot be done online	Minutes to hours	Zero
	Database upgrades: patch sets and full database releases	Minutes to hours	Zero
	Platform migrations	Hours to a day	Zero
	Application upgrades that modify back-end database objects	Hours to days	Zero

Silver: High Availability with Fast Failover

RTO of Seconds for Server Failures



- Active-Active clustering with Oracle RAC
 - All nodes active at all times
 - Real-time failover
- Zero downtime rolling maintenance across RAC instances
 - Hardware and OS maintenance
 - Qualified Oracle Database patches
 - Follow Application Checklist for Continuous Service

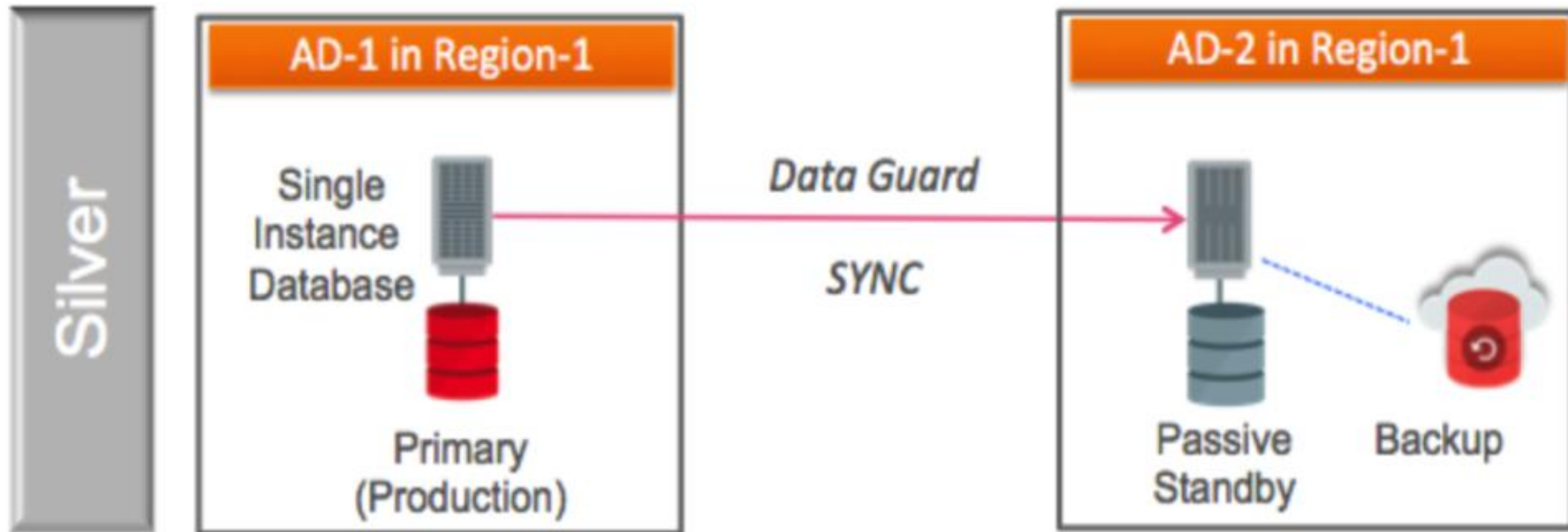
*In OCI, VM RAC instances are in different fault domains

Unplanned Outages and Planned Maintenance

Silver: High Availability with Fast Failover

	Events	Downtime (RTO)	Data Loss Potential (RPO)
Unplanned Outages	Recoverable or unrecoverable RAC instance failure	Seconds	Zero
	Recoverable or unrecoverable server failure	Seconds	Zero
	Data corruptions, unrecoverable database, Availability Domain or Region failure	Hours to days	Since last backup
Planned Maintenance	Online file move, reorganization/redefinition, and patching	Zero	Zero
	Hardware or operating system maintenance and database patches that cannot be done online but qualified for RAC rolling install	Zero	Zero
	Database upgrades: patch sets and full database releases	Minutes to hours	Zero
	Platform migrations	Hours to a day	Zero
	Application upgrades that modify back-end database objects	Hours to days	Zero

Silver Option 2: High Availability with Data Guard Fast Start Failover



Use of Active Data Guard and its real time apply and auto block repair is highly recommended

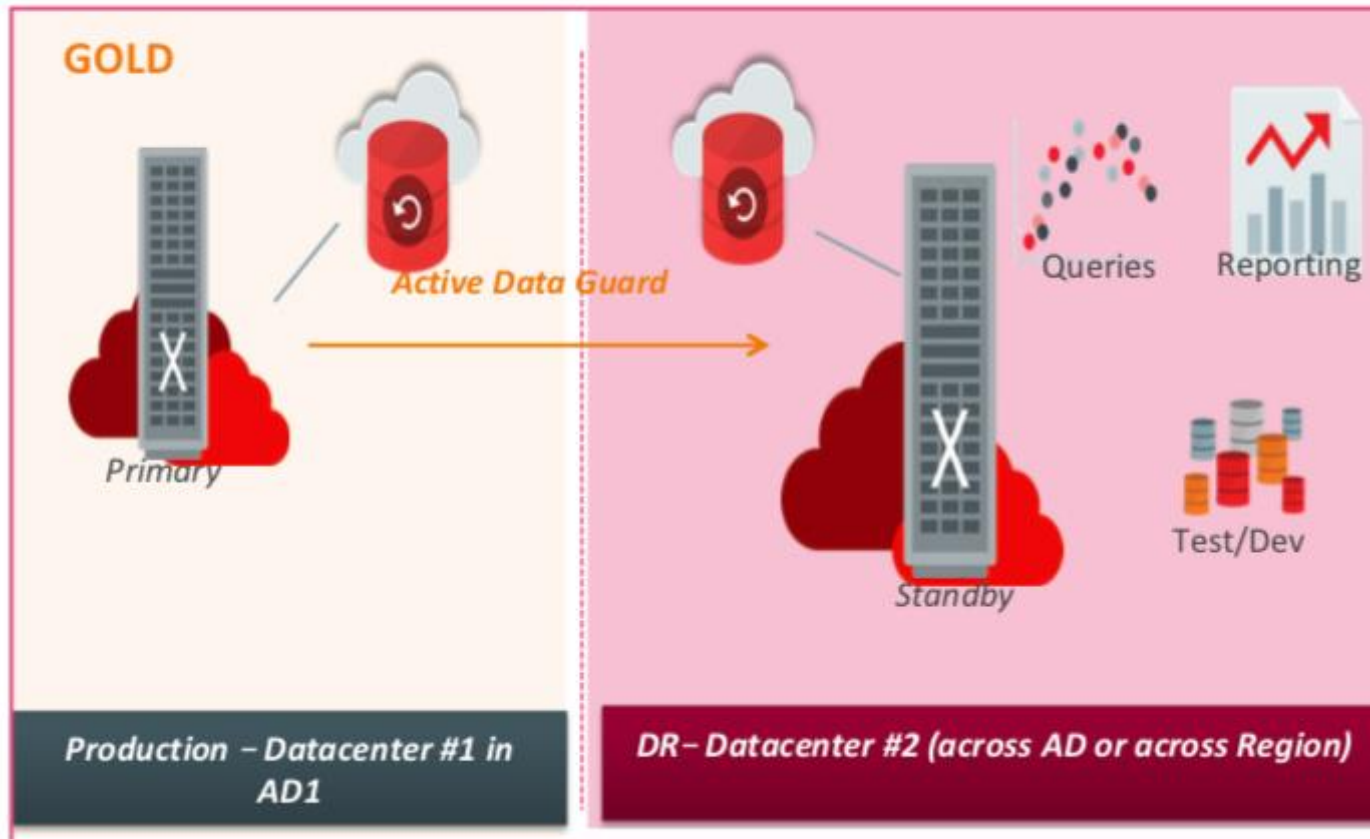
Unplanned Outages and Planned Maintenance

Silver Option 2: High Availability with Data Guard Fast Start Failover

	Events	Downtime (RTO)	Data Loss Potential (RPO)
Unplanned Outages	Recoverable or unrecoverable database instance failure	Seconds to Min	Zero
	Recoverable or unrecoverable server failure	Seconds to Min	Zero
	Data corruptions, unrecoverable database, Availability Domain or Region failure	Seconds to Min	Zero
Planned Maintenance	Online file move, reorganization/redefinition, and patching	Zero	Zero
	Hardware or operating system maintenance and database patches that cannot be done online	Minutes to hour	Zero
	Database upgrades: patch sets and full database releases	Minutes to hours	Zero
	Platform migrations	Hours to a day	Zero
	Application upgrades that modify back-end database objects	Hours to days	Zero

Gold: Comprehensive HA/DR

RTO of Seconds to minutes, RPO of Zero or Near-zero



- Real-time data protection, HA and DR using Active Data Guard
 - Best corruption protection
 - Zero or near-zero data loss
 - Automatic database failover with potential zero data loss
 - Offload read-only and backups
- Minimal Downtime for Database Upgrades using DBMS_Rolling or transient logical standby

Oracle Data Protection

Gold – Comprehensive Data Protection

	Capability	Physical Block Corruption	Logical Block Corruption
Manual	Dbverify, Analyze	Physical block checks	Logical checks for intra-block and inter-object consistency
	RMAN, ASM	Physical block checks	Intra-block logical checks
Runtime	Active Data Guard	<ul style="list-style-type: none"> • Continuous physical block checking at standby • Strong isolation to prevent single point of failure • Automatic repair of physical corruptions • Automatic database failover 	<ul style="list-style-type: none"> • Detect lost write corruption, auto shutdown and failover • Intra-block logical checks at standby
	Database	In-memory block and redo checksum	In-memory intra-block checks
	ASM	Automatic corruption detection and repair using extent pairs	
	Exadata	HARD checks on write, automatic disk scrub and repair	HARD checks on write

Unplanned Outages and Planned Maintenance

Gold: Comprehensive HA and Data Protection

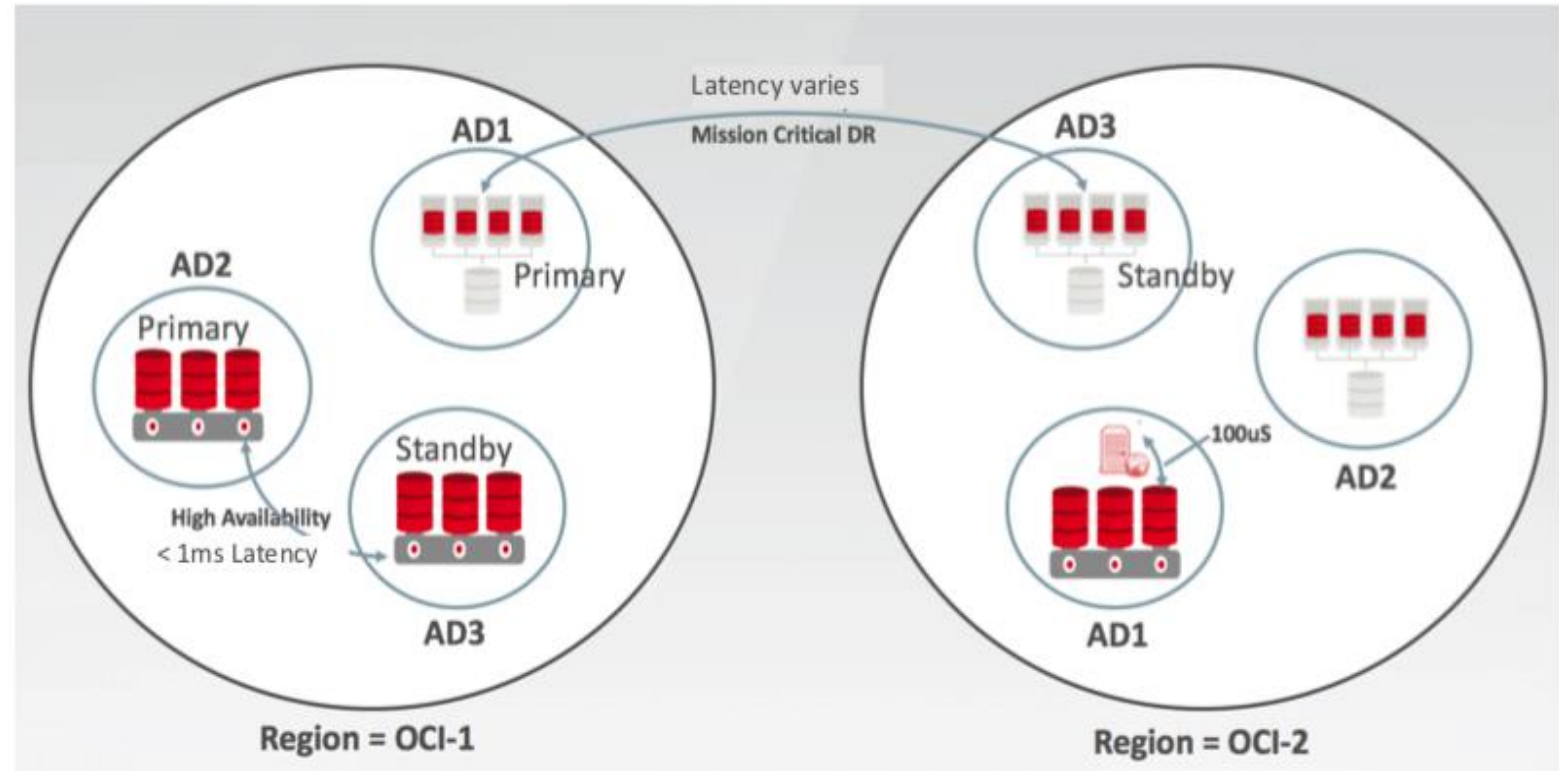
	Events	Downtime (RTO)	Data Loss Potential (RPO)
Unplanned Outages	Recoverable or unrecoverable RAC instance failure	Seconds (RAC)	Zero
	Recoverable or unrecoverable server failure	Seconds (RAC)	Zero
	Data corruptions, unrecoverable database, site failure	Seconds (Active Data Guard FSFO*)	Near-zero if ASYNC, Zero if SYNC or FAR SYNC
Planned Maintenance	Online file move, reorganization/redefinition, and patching	Zero	Zero
	Hardware or operating system maintenance and database patches that cannot be done online but qualified for RAC rolling install	Zero (RAC)	Zero
	Database upgrades: patch sets and full database releases	Seconds (Active Data Guard)	Zero
	Platform migrations	Seconds (Active Data Guard)	Zero
	Application upgrades that modify back-end database objects	Hours to days	Zero

*FSFO: Fast Start Failover

OCI Deployment Model

OCI deployment specifics

- Provides HA, data protection and fast failover for database across ADs
- DG synchronous mode possible due to < 1ms between ADs
- Data Guard Fast Start Failover is manual
- VCN Peering across Regions available today
 - PHX – IAD and LHR – FRA
 - Cannot provision across Regions, so no DR via cloud tooling



Database Service - Summary

In this lesson, you should have learned how to:

- Describe and utilize the Database command line (CLI) on the Oracle Cloud Infrastructure (OCI) Database systems
- Backup a database and recover from a database backup
- Troubleshoot database backup failures
- Be aware of different database migration methods to move data into OCI Database Systems
- Use the MAA capabilities of OCI for DB Systems

Additional References

<https://blogs.oracle.com/cloud-infrastructure/database-migration-to-oracle-cloud-infrastructure-blog-series>

<https://docs.cloud.oracle.com/iaas/Content/Database/Tasks/migrating.htm>

<https://www.oracle.com/technetwork/database/availability/database-rolling-upgrade-3206539.pdf> (Database Rolling Upgrades)

<https://www.oracle.com/technetwork/database/availability/maa-reference-architectures-2244929.pdf> (Oracle MAA Reference Architectures)



cloud.oracle.com/iaas

cloud.oracle.com/tryit