ORACLE University

Integrated Cloud Applications & Platform Services

Implement Database High Availability & Disaster Recovery on OCI

Student Guide

D105872GC10 | D106280

Learn more from Oracle University at **education.oracle.com**

ORACLE

Author

Soumyadeep Mitra

Technical Contributors and Reviewers

Sailaja Pasupuleti

Sharath Bhujani

Tatsuya Nomura

Naoki Kato

Graphic Editor

James Hans

Editor

Aju Kumar

Publishers

Syed Imtiaz Ali

Asief Baig

Michael Sebastian Almeida

1005282019

Contents

Objectives

After completing this lesson, you should be able to:

- Describe the scenario that will be used throughout this course
- Discuss the online retail company in the course scenario
- Identify the personas used throughout this course
- Explain the current state and the proposed state of the IT infrastructure of the online retail company

Course Scenario: Tween Corp

- Online retail company
- Customer base scattered all over the globe
- Operational Data Center in Ashburn, USA

Challenges with Current System:

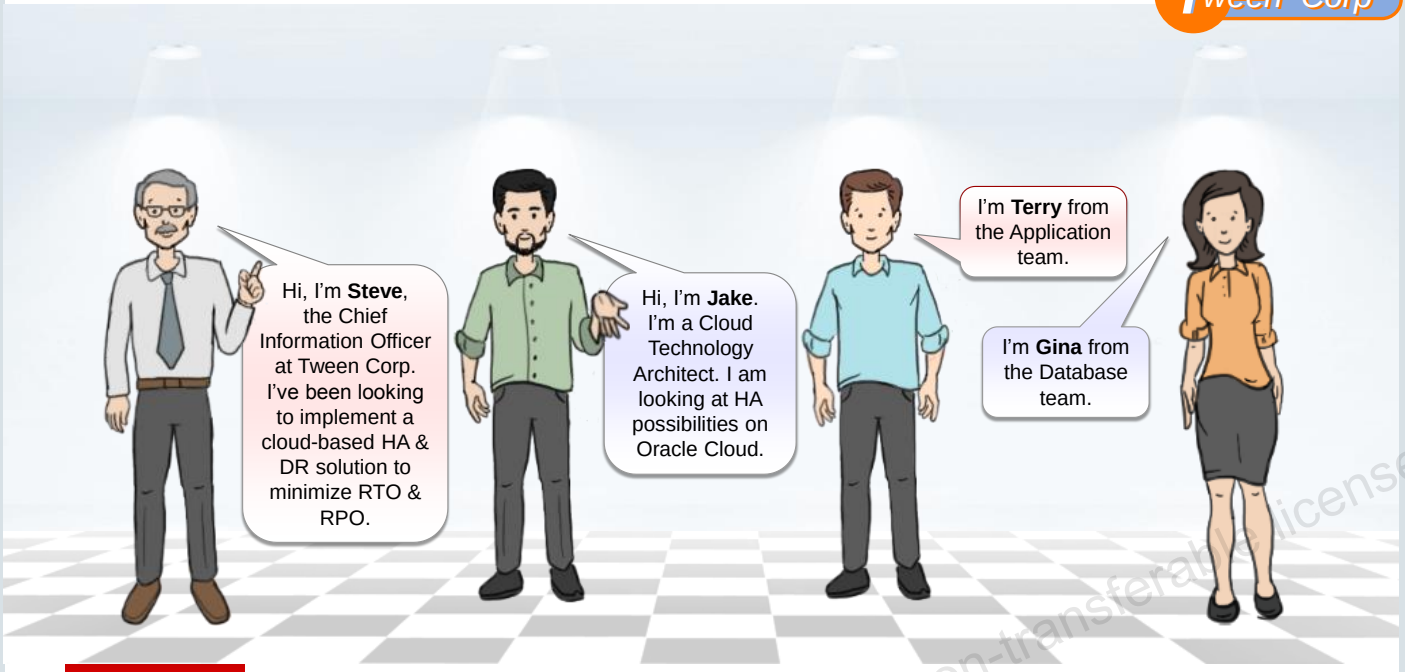
- End of life H/W
- Server sprawl
- Degrading performance on aging hardware
- Version de-support
- Licenses exposure
- Operational Efficiency and agility around provisioning
- Elasticity / scalability on-demand

Course Scenario: Tween Corp

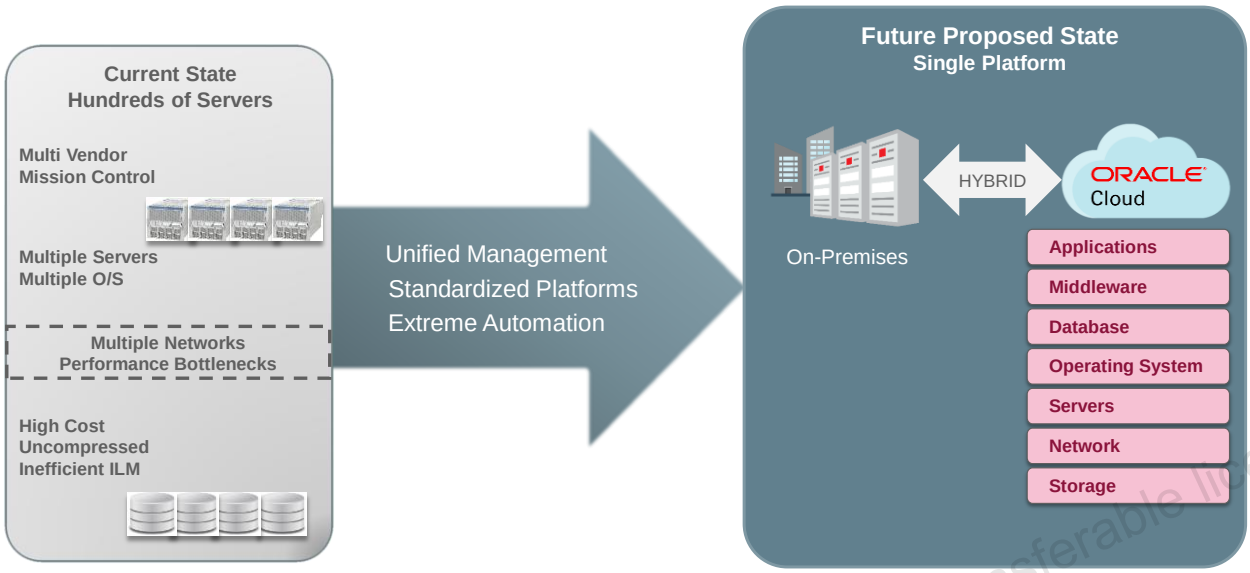
Tween Corp's Chief Information Officer is looking for a cloud-based high-availability solution because the hardware being used to host their application and databases are nearing end of life.

They plan to adopt Oracle Cloud Infrastructure for operational efficiency and agility around provisioning, elasticity/scalability on-demand, and minimize RTO and RPO by implementing High Availability (HA) and Disaster Recovery (DR)–based solutions.

Course Personas

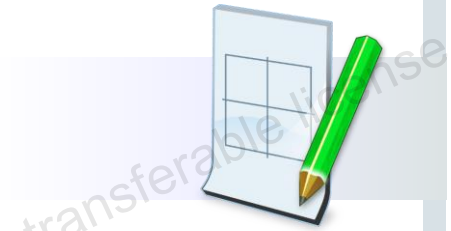


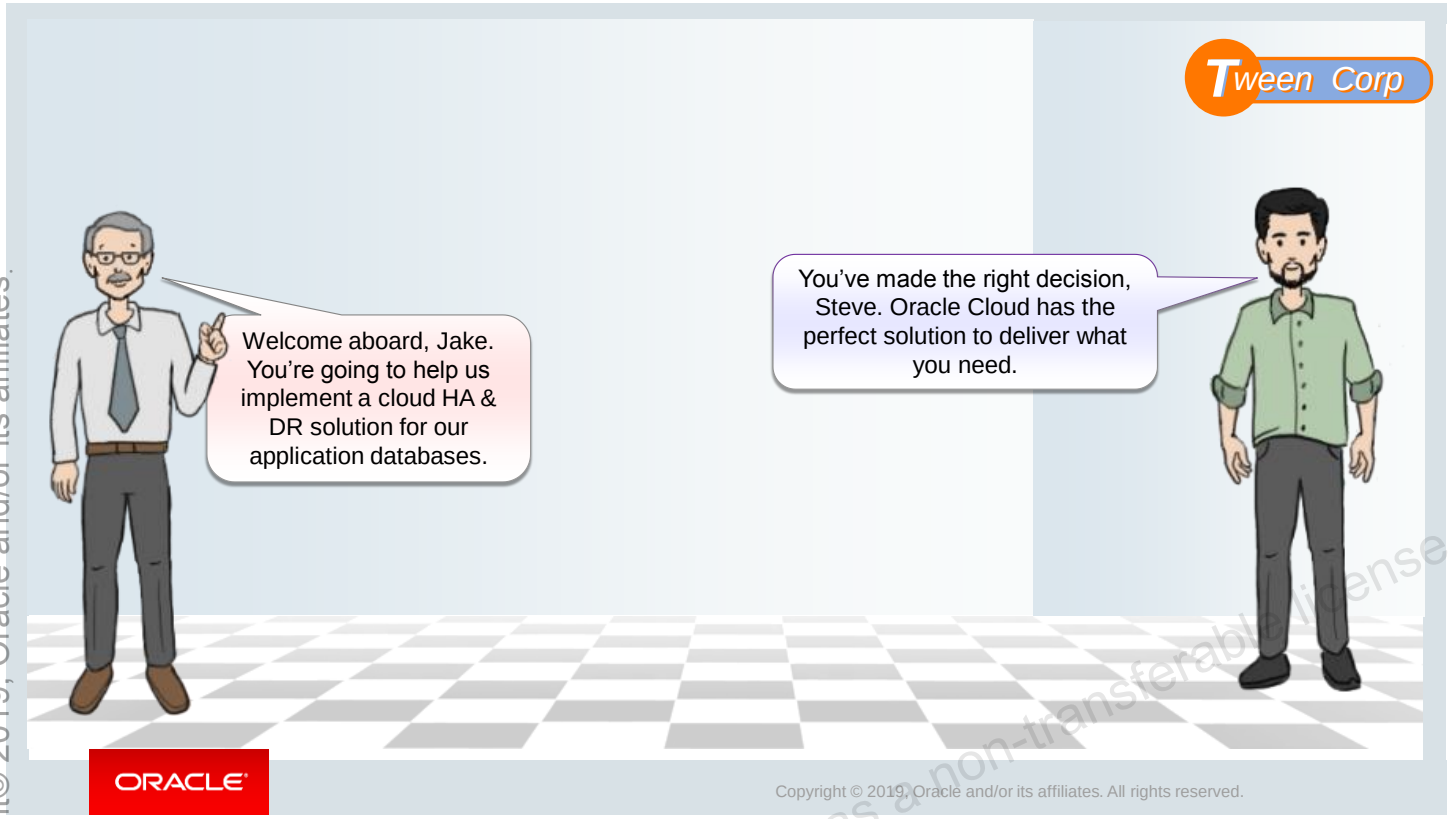
Current State Versus Future Proposed State



Practice 1: Overview

There are no practices for this lesson.





Tween Corp has many application databases with stringent RTO & RPO requirements. They have decided to implement HA & DR on Oracle Cloud.

RTO is Recovery Time Objective and

RPO is Recovery Point Objective

These two are the most important parameters of a Disaster Recovery plan and can guide enterprises in choosing an optimal backup plan.

Objectives

After completing this lesson, you should be able to describe:

- High Availability Building Blocks
- Oracle Maximum Availability Architecture on Oracle Cloud
- Database High Availability Reference Architectures on Oracle Cloud

High Availability Service

Designed for maximum potential uptime and accessibility

Three key elements for designing high availability architecture:

- Redundancy
- Monitoring
- Failover

A high availability service is designed for maximum potential uptime and accessibility. To design a high availability architecture, three key elements should be considered:

- Redundancy means that multiple components can perform the same task. The problem of a single point of failure is eliminated because redundant components can take over a task performed by a component that has failed.
- Monitoring checks whether or not a component is working properly.
- Failover is the process by which a secondary component becomes primary when a primary component fails.

High Availability Building Blocks

- **Availability Domain**
- **Fault Domain**

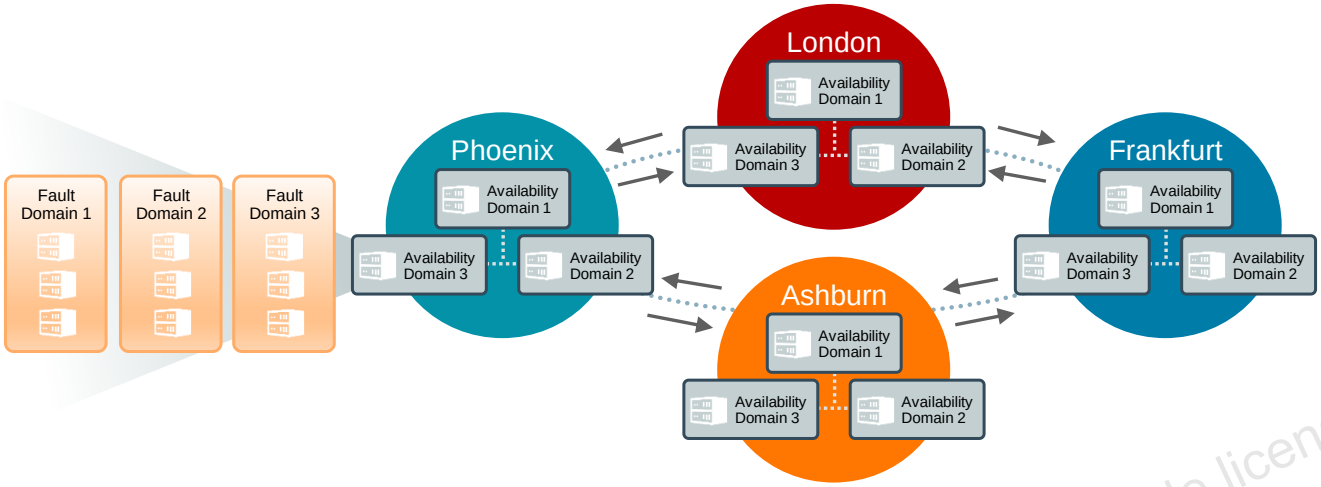
An Oracle Cloud Infrastructure region is a localized geographic area composed of one or more availability domains, each composed of three fault domains.

An availability domain is one or more data centers located within a region. Availability domains are isolated from each other, fault tolerant, and unlikely to fail simultaneously. Because availability domains do not share physical infrastructure, such as power or cooling, or the internal availability domain network, a failure that impacts one availability domain is unlikely to impact the availability of others.

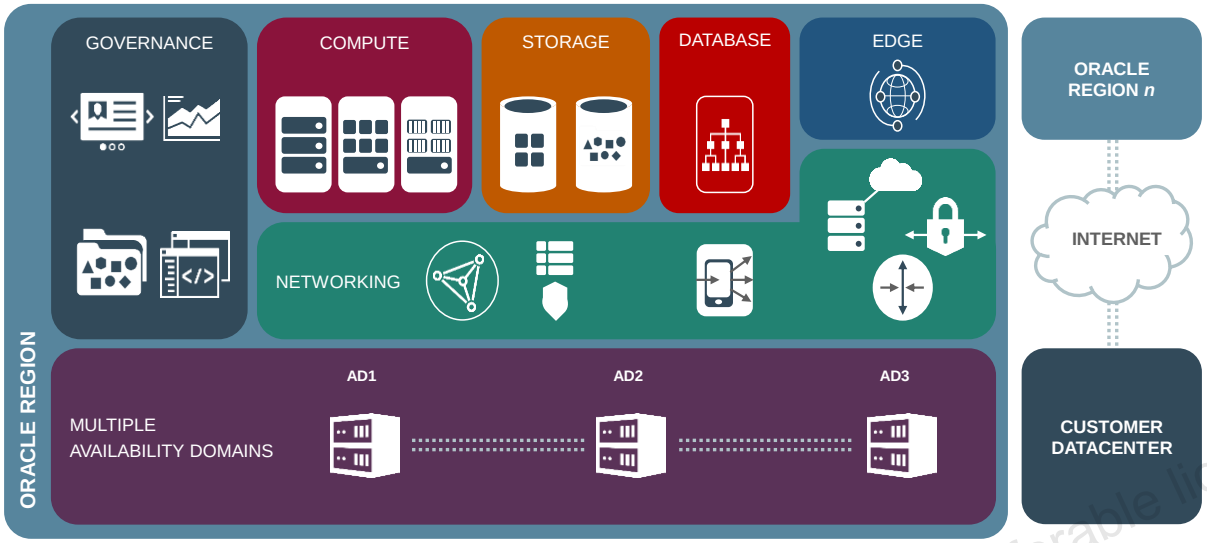
A fault domain is a grouping of hardware and infrastructure within an availability domain. Each availability domain contains three fault domains. Fault domains let you distribute your instances so that they are not on the same physical hardware within a single availability domain. As a result, an unexpected hardware failure or a Compute hardware maintenance that affects one fault domain does not affect instances in other fault domains. You can optionally specify the fault domain for a new instance at launch time, or you can let the system select one for you.

All the availability domains in a region are connected to each other by a low-latency, high-bandwidth network. This predictable, encrypted interconnection between availability domains provides the building blocks for both high availability and disaster recovery.

High Availability Building Blocks



Architecting High Availability Solutions



This section describes each Oracle Cloud Infrastructure layer and provides detailed best practices and design guidelines for architecting high availability solutions.

Compute High Availability Design

- **Elimination of a Single Point of Failure**
- **Single Availability Domain Deployment**

Single Availability Domain Deployment

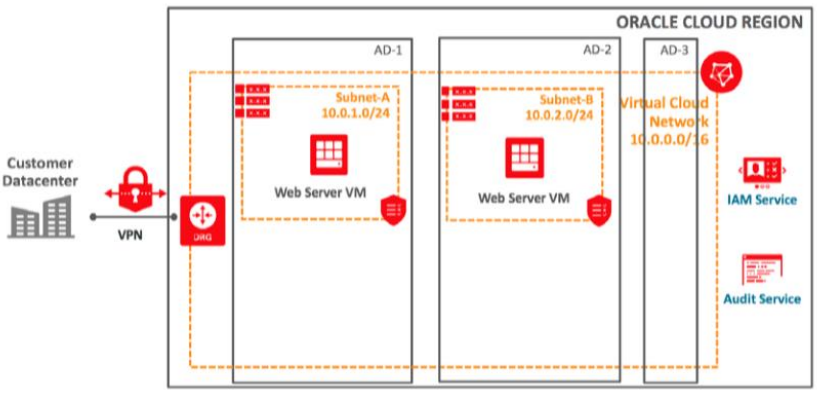
Each availability domain has three fault domains. By properly leveraging fault domains, you can increase the availability of applications running on Oracle Cloud Infrastructure.

Your application's architecture determines whether you separate or group instances by using fault domains.•

Scenario 1: Highly Available Application Architecture In this scenario, you have a highly available application—for example, two web servers and a clustered database. In this scenario, you group one web server and one database node in one fault domain and the other half of each pair in another fault domain. This architecture ensures that a failure of any one fault domain does not result in an outage for your application.

Scenario 2: Single Web Server and Database Instance Architecture In this scenario, your application architecture is not highly available—for example, you have one web server and one database instance. In this scenario, both the web server and the database instance must be placed in the same fault domain. This architecture ensures that your application is impacted only by the failure of that single fault domain.

Compute High Availability Design



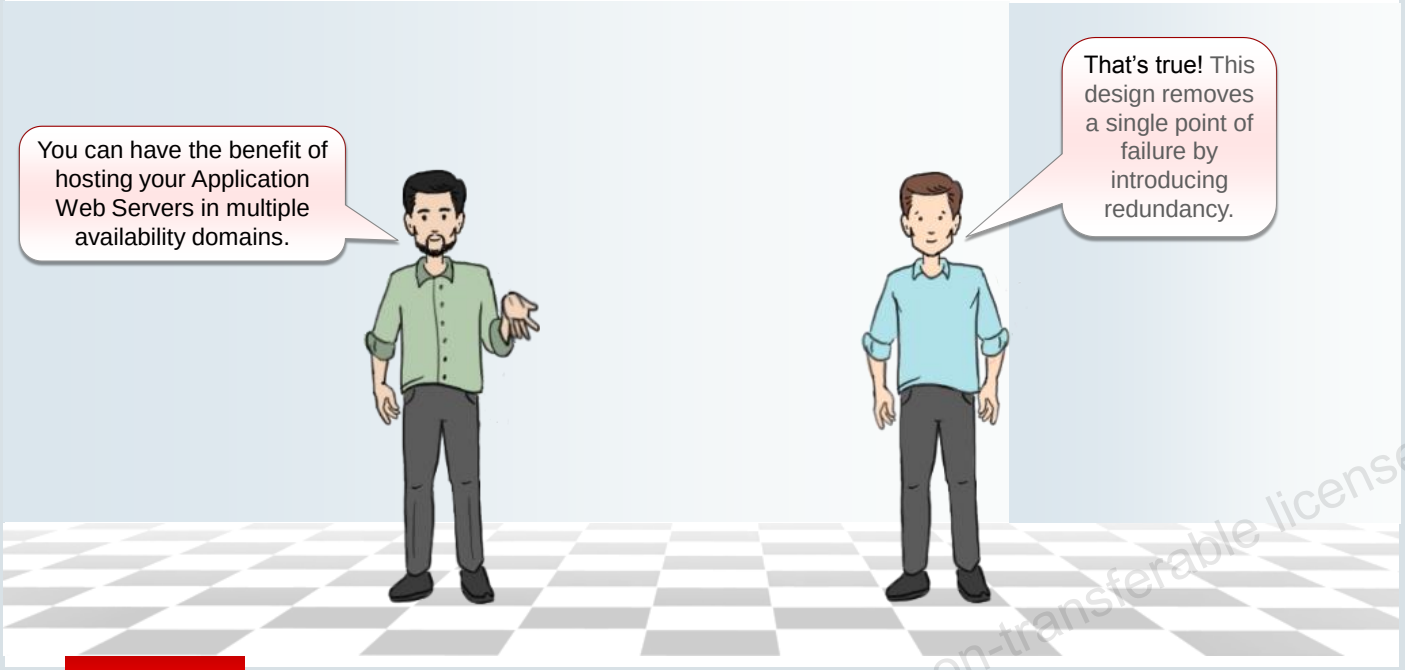
- **Multiple Availability Domain Deployment**

The following diagram illustrates web server VMs deployed in two availability domains to implement redundancy:

Depending on your system or application requirements, you can implement this architecture redundancy in either standby or active mode:

- In standby mode, a secondary or standby component runs side-by-side with the primary component. When the primary component fails, the standby component takes over. Standby mode is typically used for applications that need to maintain their states.
- In active mode, no components are designated as primary or standby; all components are actively participating in performing the same tasks. When one of the components fails, the related tasks are simply distributed to another component. Active mode is typically used for stateless applications.

Compute High Availability in Application Design



Floating IP Addresses

- Floating IP play a key role in high availability architecture design
- Compute instance with secondary private IP address
- Persistent reserved public IP address
- Leveraging Linux high availability services – Corosync, Pacemaker

ORACLE

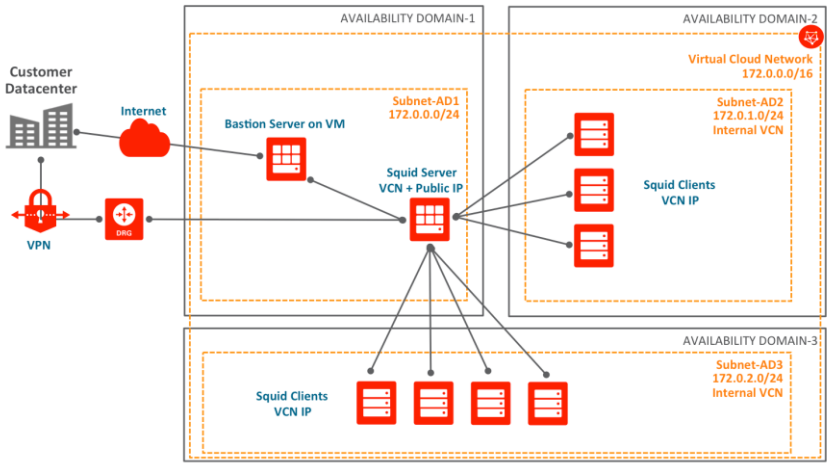
Floating IP addresses of Compute instances (either the secondary private IP address or the reserved public IP address) play a key role in high availability architecture design on Oracle Cloud Infrastructure.

A Compute instance can be assigned a secondary private IP address. If the Compute instance has problems, you can reassign that secondary private IP address to a standby instance in the same subnet to achieve instance failover.

A reserved public IP address can be persistent and exist beyond the lifetime of the Compute instance to which it's currently assigned. In the case of high availability and failover scenarios, you can unassign a reserved public IP address from the primary instance and then reassign it to standby instance.

You can automate this floating IP address failover by leveraging Linux high availability services, such as Corosync or Pacemaker.

Network High Availability Design



Set up:

- Virtual Cloud Network
- Subnet
- Internet Gateway
- Virtual Router
- Dynamic Routing Gateways

A VCN resides within a single region but can cross multiple Availability Domains.

Internet Gateway provides a path for network traffic between your VCN and the internet

A virtual router that provides a single point of entry for remote network paths coming into your VCN.

You can use DRG (Dynamic Routing gateways) to establish a connection with your on-premises network via IPSec VPN or FastConnect.

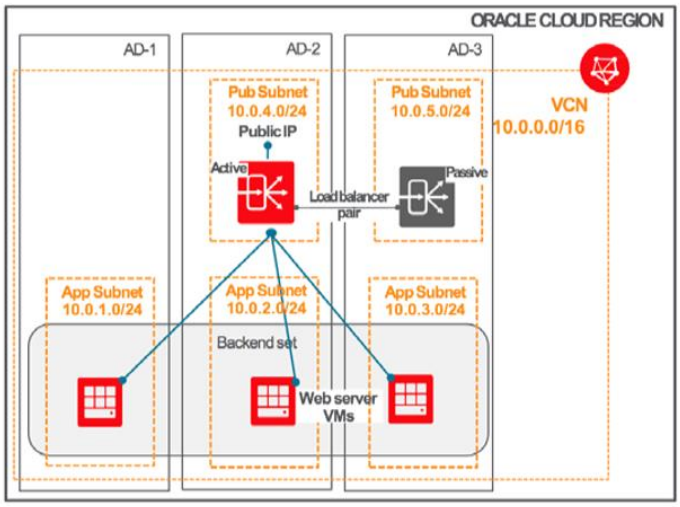
Load Balancing High Availability Design

- Provides automated traffic distribution
- Public or private IP address
- Provisioned bandwidth
- Supports routing incoming requests

- Provides automated traffic distribution from one entry point to multiple servers reachable from your VCN
- Comes with a public or private IP address and provisioned bandwidth
- Improves resource utilization, facilitates scaling, and helps ensure high availability
- Supports routing incoming requests to various back-end sets based on virtual hostname, path route rules, or a combination of both

Determining the Right Size of Subnets Each subnet in a VCN exists in a single availability domain and consists of a contiguous range of IP addresses that do not overlap with other subnets in the cloud network (for example, 172.16.1.0/24). The first two IP addresses and the last one in the subnet's CIDR are reserved by the Oracle Cloud Infrastructure Networking service. You can't change the size of the subnet after it is created, so it's important to think about the size you need before creating subnets. Consider the future growth of your workloads and leave sufficient capacity to meet high availability requirements, such as the need to set up standby Compute instances.

HA with Public Load Balancer



Public Load Balancer

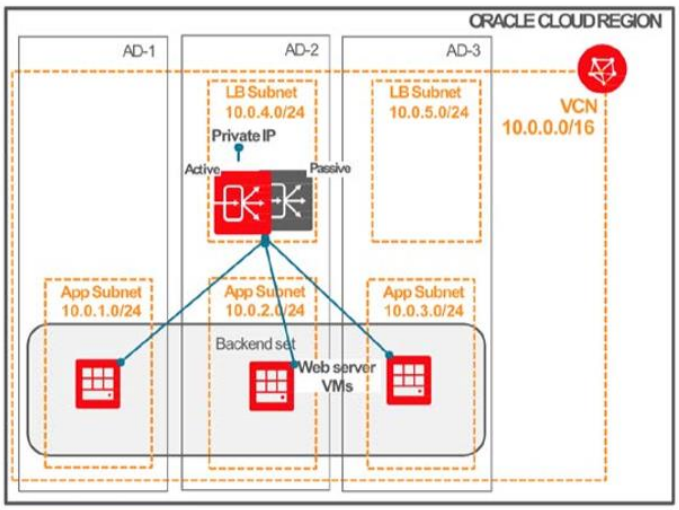
- Accept traffic from the internet
- Has a public IP address
- Entry point for incoming traffic
- Supports friendly DNS name

A public load balancer is regional in scope and requires two subnets, each in a separate availability domain. As a result, a public load balancer is inherently highly available across availability domains. To achieve high availability for your systems, you can put the systems behind a public load balancer. For instance, you can put your web server VMs as backend server sets behind a public load balancer, as illustrated in this diagram.

Public Load Balancer

- To accept traffic from the internet, you create a public load balancer.
- The service assigns it a public IP address that serves as the entry point for incoming traffic.
- You can associate the public IP address with a friendly DNS name through any DNS vendor.

HA with Private Load Balancer



Private Load Balancer

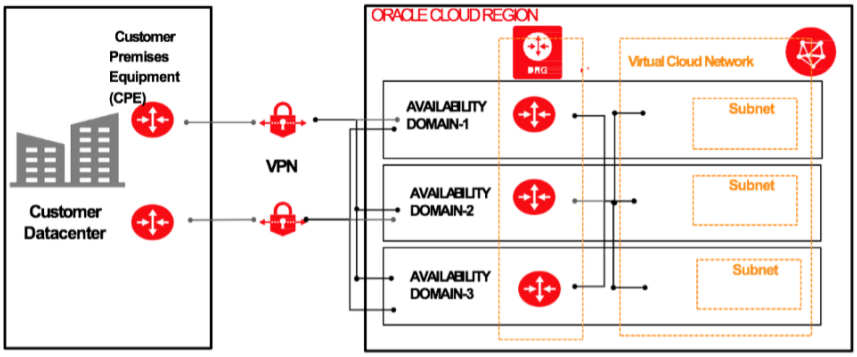
- Isolate load balancer from the internet
- Has a private IP address
- Entry point for incoming traffic

When you create a private load balancer, the service requires only one subnet to host both the primary and standby load balancers. In this case, private load balancer service is bounded within an availability domain.

Private Load Balancer

- To isolate your load balancer from the internet and simplify your security posture, you create a private load balancer.
- The Load Balancing service assigns it a private IP address that serves as the entry point for incoming traffic.

Network High Availability Design with IPSec VPN



IPSec VPN connections

- Enables redundancy
- Ensures high availability

Implement IPSec VPN connections to connect your data center to Oracle Cloud Infrastructure.

An IPSec VPN connection is easy to set up and cost-effective.

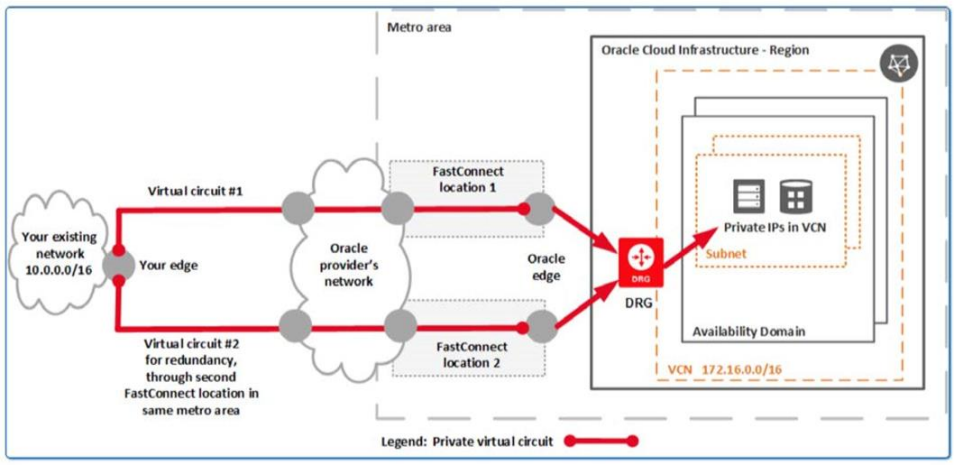
To enable redundancy, each Oracle Cloud Infrastructure dynamic routing gateway (DRG) has multiple VPN endpoints so that each IPSec VPN connection consists of multiple redundant IPSec tunnels that use static routes to route traffic.

To ensure high availability, you must set up VPN connection availability within your internal network to use either path when needed as illustrated in the diagram.

Implement IPSec VPN connections:

- To enable redundancy, each Oracle Cloud Infrastructure dynamic routing gateway (DRG) has multiple VPN endpoints.
- To ensure high availability, you must set up VPN connection availability within your internal network.

Network High Availability Design with FastConnect



- Dedicated private connection
- Higher-bandwidth
- Reliable and consistent
- Supports peering

- Dedicated, private connection between your data center and Oracle Cloud Infrastructure
- Higher-bandwidth options and a more reliable and consistent networking experience
- Use private peering, public peering, or both

Use private peering to extend your existing infrastructure into a virtual cloud network (VCN) in Oracle Cloud Infrastructure (for example, to implement a hybrid cloud, or in a lift-and-shift scenario). Communication across the connection is with IPv4 private addresses (typically RFC 1918).

Use public peering to access public services in Oracle Cloud Infrastructure without using the internet (for example, to access Object Storage, the Oracle Cloud Infrastructure Console and APIs, or public load balancers in your VCN). Communication across the connection is with IPv4 public IP addresses. Without FastConnect, the traffic destined for public IP addresses would be routed over the internet. With FastConnect, that traffic goes over your private physical connection.

You can either connect directly to Oracle Cloud Infrastructure routers in provider points-ofpresence (POPs) or use one of Oracle's many partners to connect from POPs around the world to their Oracle Cloud Infrastructure Networking resources. Oracle provides features that allow you to build fault-tolerant connections, including multiple POPs per region and multiple FastConnect routers per POP.

FastConnect Redundancy

Avoid a single point of failure with redundancy:

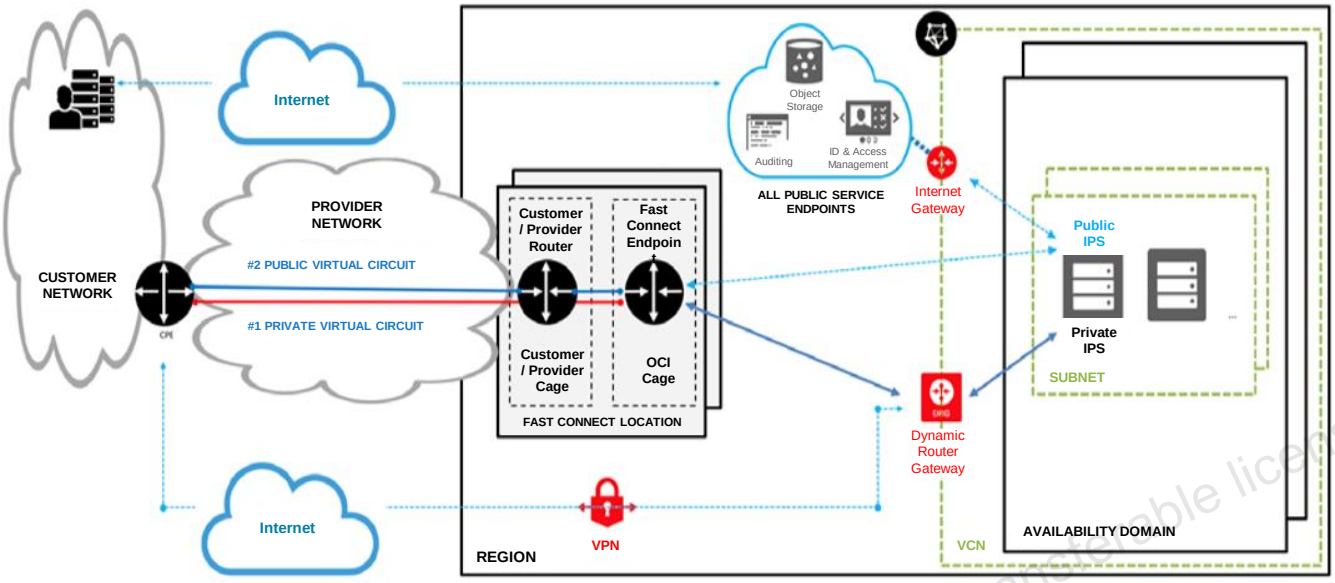
- Multiple FastConnect locations
- Multiple routers
- Multiple physical circuits

To avoid a single point of failure with redundancy, Oracle Cloud Infrastructure provides the following features:

- Multiple FastConnect locations within each metro area
- Multiple routers in each FastConnect location
- Multiple physical circuits in each FastConnect location
- Oracle handles the redundancy of the routers and physical circuits in the FastConnect locations.

Oracle's FastConnect partners have redundant links to the Oracle network. As a customer of the partner, you should have redundant links to the partner's network. These connections should be on different routers, both in your network and in the partner's network. When you provision virtual circuits, provision them across your multiple provider link.

Using Both IPSec VPN and FastConnect



To have an additional level of redundancy, you can set up both IPSec VPN and FastConnect to connect your on-premises data centers to Oracle Cloud Infrastructure. When you set up both an IPSec VPN connection and FastConnect virtual circuits to the same DRG, remember that the IPSec VPN uses static routes but FastConnect uses BGP. Oracle Cloud Infrastructure advertises a route for each of your VCN's subnets over the FastConnect virtual circuit BGP session, and overrides the default route selection behavior to prefer BGP routes over static routes if a static route overlaps with a route advertised by your on-premises network.

Storage High Availability Design

- Oracle Cloud Infrastructure Block Volume: Create, attach, connect, and move volumes as needed.
- Oracle Cloud Infrastructure storage services:
  - Block Volume
  - Object Storage
  - File Storage

Oracle Cloud Infrastructure Block Volume enables you to dynamically provision and manage block storage volumes. You can create, attach, connect, and move volumes as needed to meet your storage and application requirements.

Oracle Cloud Infrastructure provides the following storage services:

- Block Volume
- Object Storage
- File Storage

Storage High Availability Design

Recommendations to achieve high availability and durability:

- Object Storage to back up application data
- Block Volume policy-based backups
- Block Volume cloning feature
- Block volume with a read-only attachment
- File Storage
- GlusterFS on top of the Block Volume service

To achieve high availability and durability, Oracle recommends the following best practices for the storage layer:

- Use Object Storage to back up application data. Data is stored redundantly across multiple storage servers across multiple availability domains. Data integrity is actively monitored by using checksums, and corrupt data is detected and automatically repaired. Any loss in data redundancy is automatically detected and corrected, without any customer impact.
- Use Block Volume policy-based backups to perform automatic, scheduled backups and retain them based on a backup policy. Consistently backing up your data allows you to adhere to your data compliance and regulatory requirements.
- If you need an immediate, point-in-time, direct disk-to-disk copy of your block volume, use the Block Volume cloning feature. Volume cloning is different than snapshots because there is no copy-on-write or dependency to the source volume. No backup is involved. The clone operation is immediate, and the cloned volume becomes available for use right after the clone operation is initiated. You can attach and use the cloned volume as a regular volume as soon as its state changes to available.
- If you need to safeguard data against accidental or malicious modifications by an untested or untrusted application, use a block volume with a read-only attachment. A read-only attachment marks a volume as read-only, so the data in the volume is not mutable. You can also use read-only attachments when you have multiple Compute instances that access the same volume for read-only purposes. For example, the instances might be running a web front end that serves static product catalog information to clients.

- When your workload requires highly available shared storage with file semantics, and you need built-in encryption and snapshots for data protection, use File Storage. File Storage uses the industry-standard Network File System (NFS) file access protocol and can be accessed concurrently by thousands of Compute instances. File Storage can provide high performance and resilient data protection for your applications. The File Storage service runs locally within one availability domain. Within an availability domain, File Storage uses synchronous replication and high availability failover to keep your data safe and available.
- If your application needs high availability across multiple availability domains, use GlusterFS on top of the Block Volume service.
- Plan and size your storage capacity by considering future growth needs.

Database High Availability Design

- Using Exadata DB Systems
  - Built-in high availability capabilities
- Using 2-node RAC DB Systems
  - Deployed on Virtual Machine Compute instances
  - Built-in high-availability capabilities

The Oracle Cloud Infrastructure Database service lets you quickly launch an Oracle Database System (DB System) and create one or more databases on it.

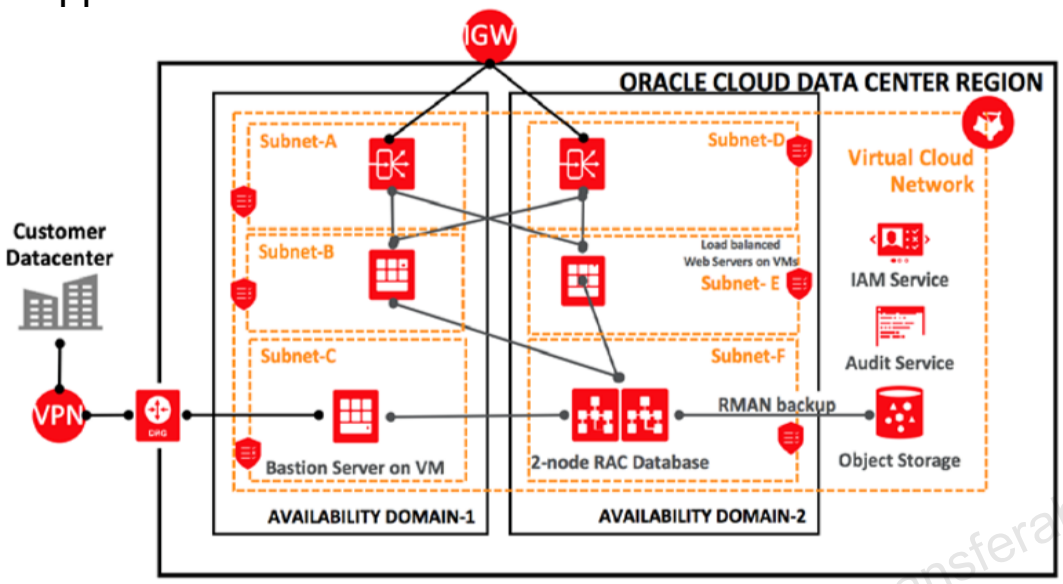
Using Exadata DB Systems

- Exadata DB systems provide built-in high availability capabilities.
- All the existing best practices with your on-premises Exadata DB systems are applicable.

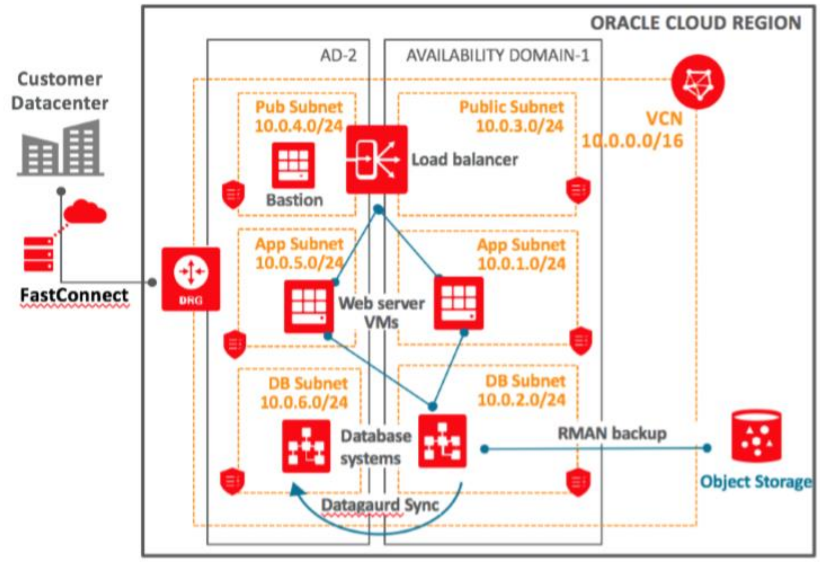
Using 2-node RAC DB Systems

- Oracle Cloud Infrastructure offers 2-node RAC DB Systems on virtual machine Compute instances.
- 2-node RAC DB systems provide built-in high-availability capabilities.

2-Node RAC DB System to Support High Availability of a Two-Tier Web Application



Using Data Guard for a High Availability Database Design



- For solutions with a single-node DB system
- Ensures:
  - High availability
  - Data protection
  - Disaster Recovery

ORACLE

For solutions with a single-node DB system, Oracle recommends using Oracle Data Guard to achieve high availability. Data Guard ensures high availability, data protection, and disaster recovery for enterprise data.

Implementation of Data Guard in the Oracle Cloud Infrastructure Database service requires two databases, one in a primary role and one in a standby role. The two databases compose a Data Guard association. Most of your applications access the primary database. The standby database is a transactional consistent copy of the primary database.

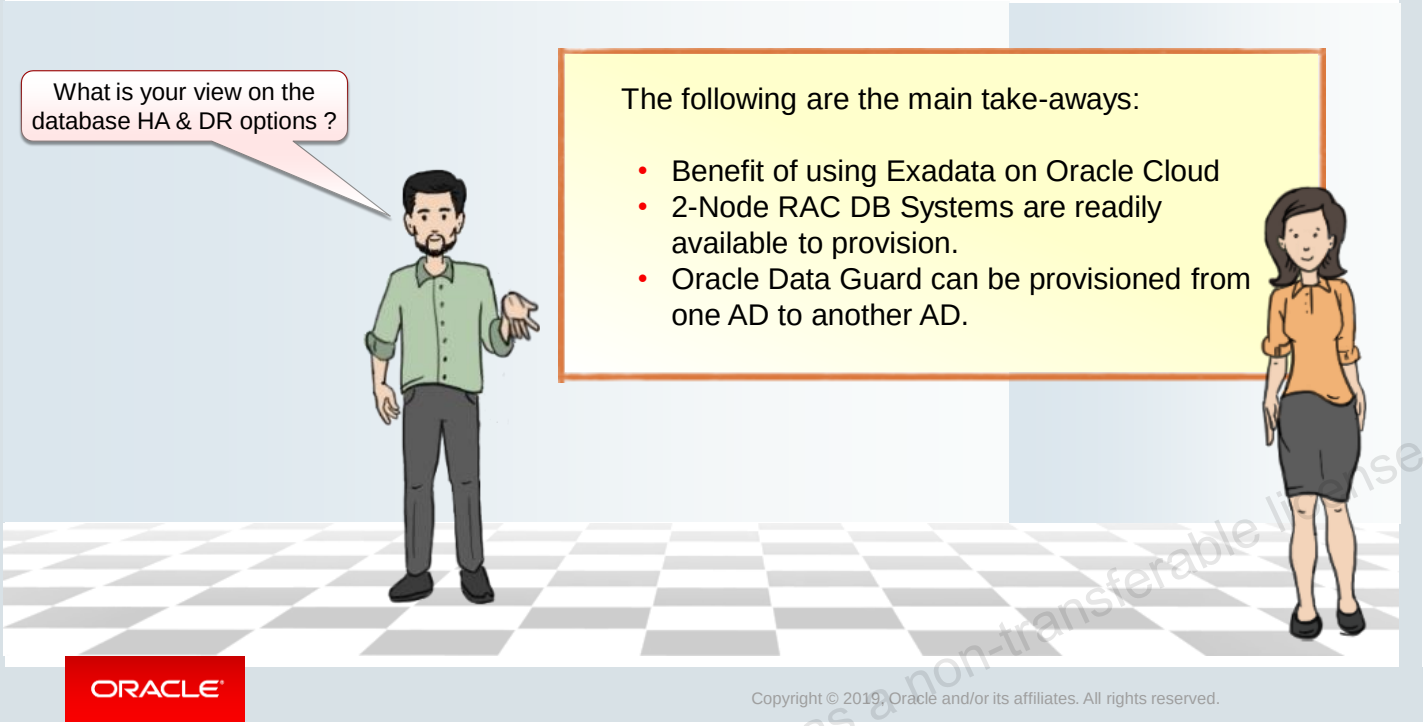
To improve availability and disaster recovery, we recommend placing the DB System of the standby database in a different availability domain from the DB System of the primary database. The high-performance network between Oracle Cloud Infrastructure availability domains enables this deployment.

Data Guard maintains the standby database by transmitting and applying redo data from the primary database. If the primary database becomes unavailable, you can use Data Guard to switch the standby database to the primary role.

You can perform following actions with Data Guard configuration to support high availability:

- **Switchover:** Reverses the primary and standby database roles. Each database continues to participate in the Data Guard association in its new role. A switchover ensures no data loss. You can use a switchover before you perform planned maintenance on the primary database.
- **Failover:** Transitions the standby database into the primary role after the existing primary database fails or becomes unreachable. A failover might result in some data loss when you use Maximum Performance protection mode.
- **Reinstate:** Reinstates a database into the standby role in a Data Guard association. You can use the reinstate command to return a failed database to service after correcting the cause of the failure.

Design Database High Availability



The following are the main take-aways:

- Benefit of using Exadata on Oracle Cloud
- 2-Node RAC DB Systems are readily available to provision.
- Oracle Data Guard can be provisioned from one AD to another AD.

Oracle Cloud Infrastructure for MAA

- Oracle's most advanced cloud infrastructure with all of the building blocks for database MAA:
  - Bare Metal Single Instance database systems
  - Virtual Machine single instance database systems
  - Virtual Machine 2-node Real Application Clusters Systems
  - Exadata systems
  - Regions, Availability Domains (ADs), and Fault Domains (FDs)
  - World class scalable networks
  - Scalable backup infrastructure with object storage

World class scalable networks:

- Secure, high bandwidth, and low latency within ADs and across ADs with Virtual Cloud (VCN) Peering with Public and fully Private subnets
- Secure, high bandwidth across Regions with VCN Peering

OCI is Oracle's most advanced cloud infrastructure with all of the building blocks for database MAA:

- Bare Metal Single Instance database systems with restart capabilities and redundant local storage
- Virtual Machine single instance database systems with restart capabilities and triple mirrored block storage
- Virtual Machine 2-node Real Application Clusters Systems
- Exadata systems (with various shapes, including quarter, half, and full racks) – best database platform
- Regions, Availability Domains (ADs), and Fault Domains (FDs) to provide outage isolation
- World class scalable networks
- Scalable backup infrastructure with object storage

OCI Database Infrastructure and Key MAA Components

Cloud Infrastructure	Backup/Restore Option	RAC	ADG	Replication across Ads/Regions
OCI (BM)	Backup to OCI Object Store (manual/automatic) Automatic backup copies across Availability Domains		✓	Across Ads Across Regions via VCN peering
OCI (VM)		✓*	✓	
Exa-OCI (X6/X7)		✓	✓	

* Oracle RAC VMs are placed in separate Fault Domains

High Availability Reference Architectures: Oracle Cloud Infrastructure - Database

Four High Availability (HA) reference architectures:

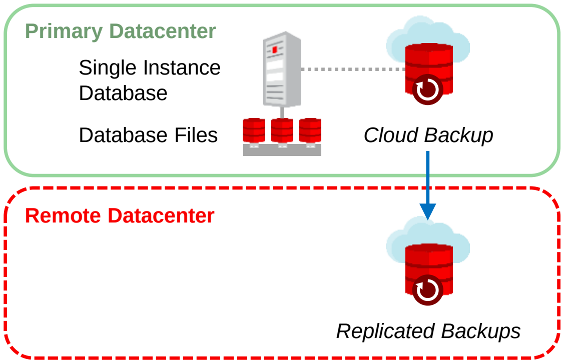
- Bronze
- Silver
- Gold
- Platinum

Oracle MAA best practices define four High Availability (HA) reference architectures that address the complete range of availability and data protection required by enterprises of all sizes and lines of business.

The reference architectures are designated:

- Bronze
- Silver
- Gold
- Platinum

Bronze Reference Architecture



Bronze Summary

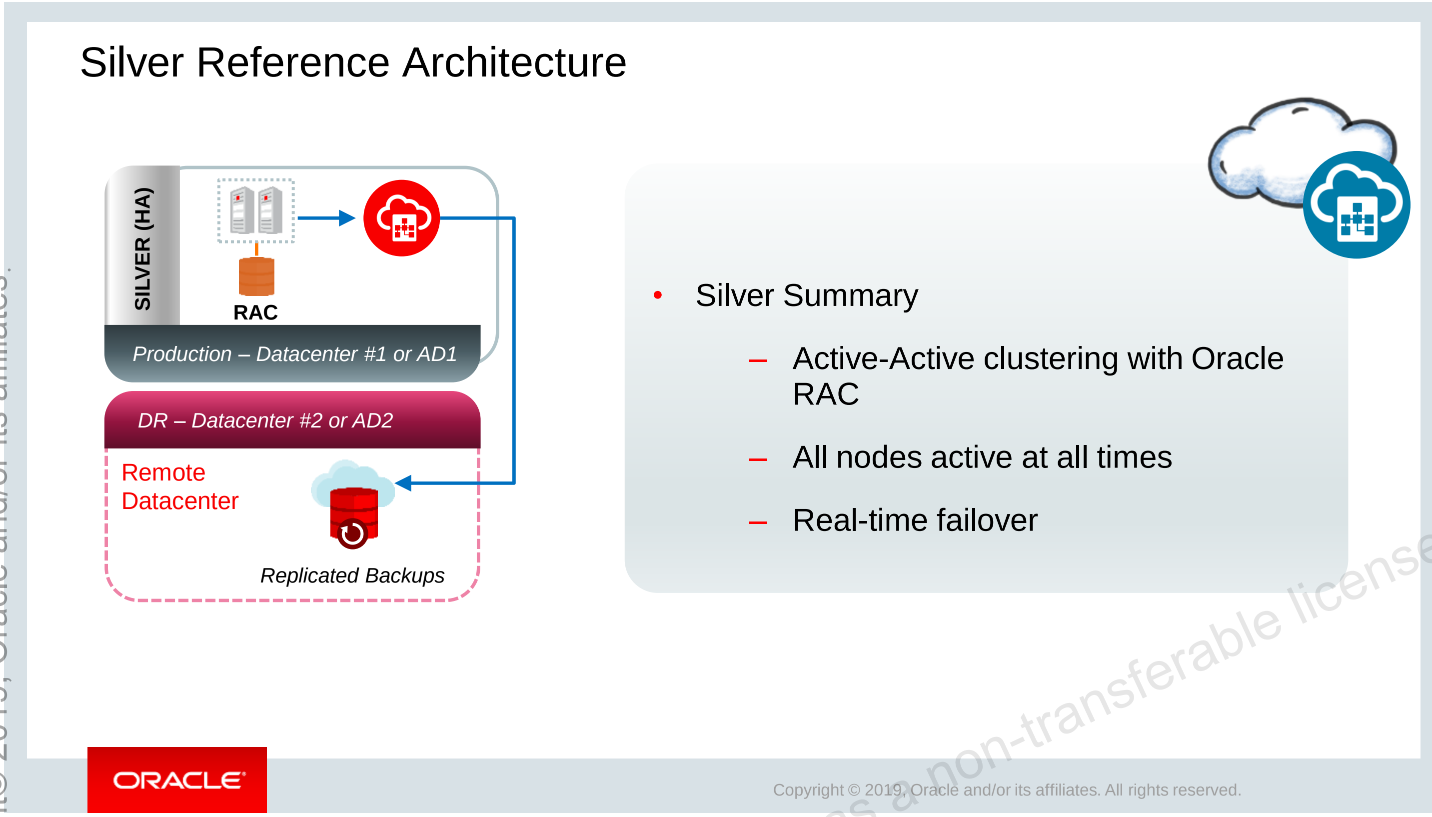
- Single instance database with backups & auto-restart capabilities with Oracle Clusterware
- Optional replication of backups (OCI replicates backups across another data center or Availability Domain)
- Restore from backup to resume service following unrecoverable outages

ORACLE

Bronze Reference Architecture is appropriate for databases where a simple restart of the database instance, node, or VM and restore from backup is 'HA and DR enough'. Bronze uses HA capabilities such as server and Oracle Clusterware monitoring and restart capabilities included with OCI and Oracle Standard and Enterprise Edition. Bronze is a single instance Oracle 11*g* database or single instance Oracle 12*c* or higher Multitenant database for additional consolidation, simplicity, and pluggable database agility. With Multitenant and pluggable databases, customers can relocate a PDB with PDB Relocate or refresh a PDB with PDB Hot Cloning. Oracle Multitenant is an option for database consolidation (multiple pluggable databases in a single container to reduce operational expenses by managing many databases as one, and to reduce capital costs by increasing consolidation density). Bronze relies upon Oracle-optimized backups to OCI object storage using Oracle Recovery Manager (RMAN) to provide data protection within the same region Backups are automatically replicated to another AD for additional isolation and protection.

RTO and RPO Service-Level Requirements for the Bronze Reference Architecture

Event	Downtime - RTO	Potential Data Loss - RPO
Disk failure	Zero	Zero
Recoverable Database Instance Failure	Minutes	Zero
Recoverable Database Server Failure	Minutes to Hour	Zero
Data corruption, unrecoverable instance, server, database or site failure	Hours to Day	Since last backup
Online File Move, Database reorganization or redefinition, Online Patching for eligible one-off patches	Zero	Zero
Hardware and software maintenance and patching	Minutes to Hour	Zero
Database upgrades (patch-sets and full releases)	Minutes to Hour	Zero
Platform migrations	Hours to a day	Zero
Application upgrades that modify back-end database objects	Hours to a day	Zero

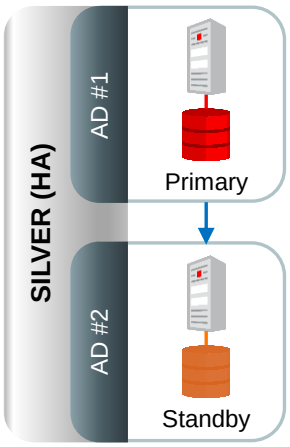


The Silver reference architecture is designed for databases that can't afford to wait for a cold restart or a restore from backup should there be an unrecoverable database outage. Silver begins with the same functionality of Bronze and adds capabilities that provide a choice of two different patterns for additional HA. The MAA recommended silver pattern uses Oracle RAC to enable automatic failover to a second active Oracle instance for HA, and provides a potential zero downtime for the most common set of software updates. Oracle RAC is available on OCI with Oracle RAC VMs and with Exadata. The alternative pattern uses Data Guard database replication with automatic failover to a completely synchronized copy of the production database in a different availability domain for HA. Similar to Bronze, backups will be sent to the local OCI object storage and replicated to another AD object storage automatically.

RTO and RPO Service-Level Requirements for the Silver Reference Architecture

Event	Downtime - RTO	Potential Data Loss - RPO
Disk failure	Zero	Zero
Recoverable Database Instance Failure	Seconds	Zero
Recoverable Database Server Failure	Seconds	Zero
Data corruption, unrecoverable instance, server, database or site failure	Hours to Day	Since last backup
Fault Domain failure (RAC nodes can be configured on separate fault domains within an AD)	Seconds	Zero
Online File Move, Database reorganization or redefinition, Online Patching for eligible one-off patches	Zero	Zero
Hardware and software maintenance and patching	Zero	Zero
Database upgrades (patch-sets and full releases)	Minutes to Hour	Zero
Platform migrations	Hours to a day	Zero

Alternative Silver Requirements (Data Guard Fast Start Failover)



An alternative Silver MAA:

- Single instance with Data Guard
- Fast Start Failover protection across ADs

An alternative Silver MAA pattern uses Data Guard Fast-Start failover to maintain a local but separate synchronized copy of the production database for HA across availability domains, or across Fault Domains when only AD exists.

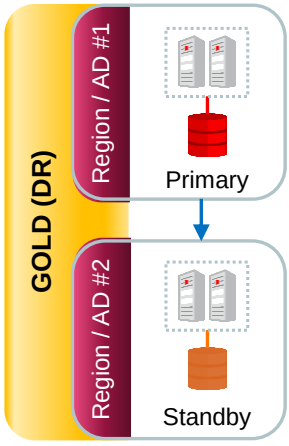
- Single instance with Data Guard
- Fast Start Failover protection across ADs

RTO and RPO Service-Level Requirements for the Alternative Silver with ADG FSFO Reference Architecture

Event	Downtime - RTO	Potential Data Loss - RPO
Disk failure	Zero	Zero
Recoverable Database Instance Failure	Seconds to minute	Zero with SYNC
Recoverable Database Server Failure	Seconds to minute	Zero with SYNC
Data corruption, unrecoverable instance, server, database or site failure	Seconds to minute	Zero with SYNC
Online File Move, Database reorganization or redefinition, Online Patching for eligible one-off patches	Zero	Zero
Hardware and software maintenance and patching	Minutes to Hour	Zero
Database upgrades (patch-sets and full releases)	Seconds to minute	Zero
Platform migrations	Seconds to minute	Zero
Application upgrades that modify back-end database objects	Hours to a day	Zero

Silver Active Data Guard Fast-Start Failover Summary Table summarizes RTO and RPO service level requirements for the Silver reference architecture. Highlighted are additional benefits when compared to the Bronze table. MAA recommends setting up Data Guard Fast-Start failover with Max Availability protection mode. Using a SYNC transport across ADs has minimal performance impact due to high bandwidth network and very low latency between ADs. Refer to MAA Observations later in the paper. From Table, Data Guard may provide additional protection for more outages because it is a separate database; however, hardware and software maintenance, which can be quarterly, is not zero or near zero.

Gold Reference Architecture



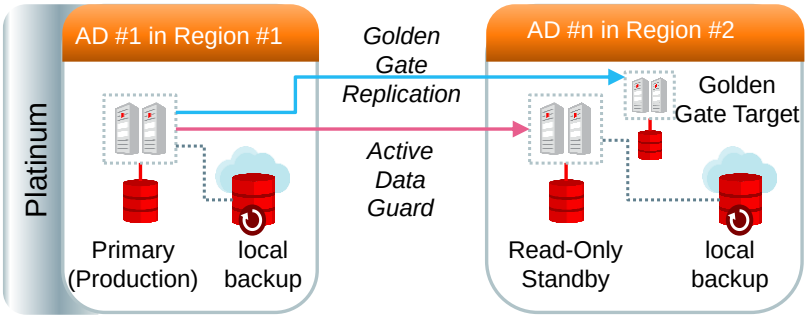
- Gold Summary
  - Active-Active clustering with Oracle RAC
  - All nodes active in each Availability Domain(AD)
  - Real-time failover
  - Real time data protection, HA & DR using Active Data Guard
  - Best corruption protection
  - Zero or near-zero data loss
  - Offload read-only and backups

The Gold reference architecture is ideal for service level requirements that cannot tolerate data center failures or possibly even regional site failures. It builds upon Silver with Oracle RAC but requires an Oracle Active Data Guard standby database that provides better data protection by enabling auto-block repair for physical data corruptions, and a remote standby to address complete database, cluster, or data center outage.

RTO and RPO Service-Level Requirements for the Gold Reference Architecture

Event	Downtime - RTO	Potential Data Loss - RPO
Disk failure	Zero	Zero
Recoverable Database Instance Failure	Seconds	Zero
Recoverable Database Server Failure	Seconds	Zero
Data corruption, unrecoverable instance, server, database or site failure	Seconds to Minutes	Zero with SYNC
Online File Move, Database reorganization or redefinition, Online Patching for eligible one-off patches	Zero	Zero
Hardware and software maintenance and patching	Zero	Zero
Database upgrades (patch-sets and full releases)	Seconds	Zero
Platform migrations	Seconds to Minutes	Zero
Application upgrades that modify back-end database objects	Hours to day	Zero

Platinum Reference Architecture

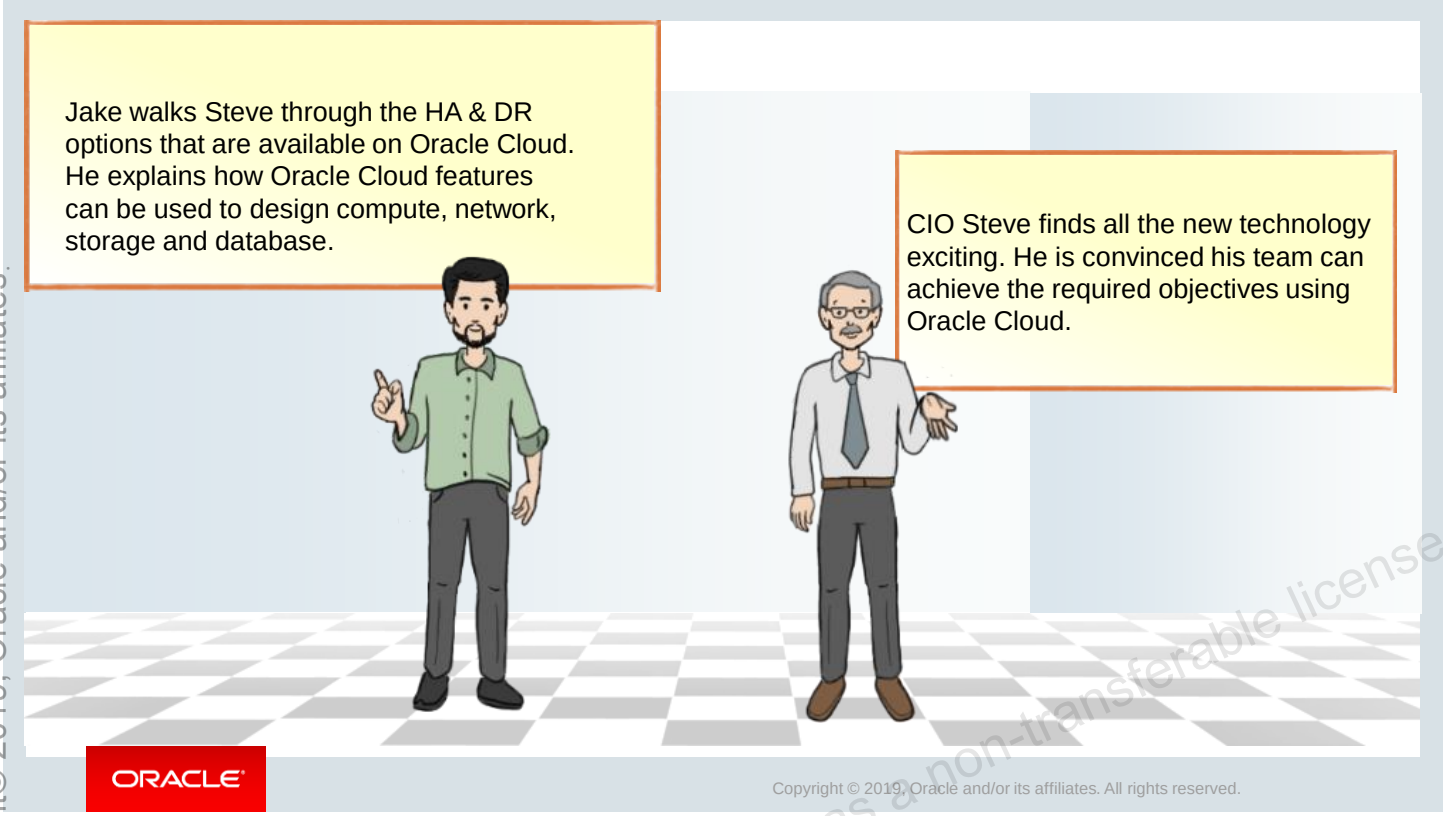


- Platinum Summary
  - Platinum uses Oracle Golden Gate and Edition-Based Redefinition to enable zero downtime maintenance, migrations, and application upgrades.

The Platinum reference architecture builds upon the Gold architecture by deploying an extra level of redundancy and several advanced HA capabilities. Platinum is ideal for applications that have extremely low, if any, tolerance for downtime or data loss.

RTO and RPO Service-Level Requirements for the Platinum Reference Architecture

Event	Downtime - RTO	Potential Data Loss - RPO
Disk failure	Zero	Zero
Recoverable Database Instance Failure	Zero or Seconds	Zero
Recoverable Database Server Failure	Zero or Seconds	Zero
Data corruption, unrecoverable instance, server, database or site failure	Zero or Seconds	Zero with SYNC
Online File Move, Database reorganization or redefinition, Online Patching for eligible one-off patches	Zero	Zero
Hardware and software maintenance and patching	Zero	Zero
Database upgrades (patch-sets and full releases)	Zero or Seconds	Zero
Platform migrations	Zero	Zero
Application upgrades that modify back-end database objects	Zero	Zero



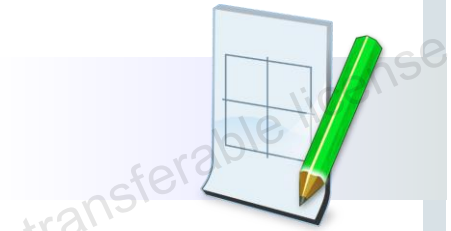
Summary

In this lesson, you should have learned how to describe:

- The High Availability Building Blocks
- Oracle Maximum Availability Architecture on Oracle Cloud
- Database High Availability Reference Architectures on Oracle Cloud

Practice 2: Overview

There are no practices for this lesson.



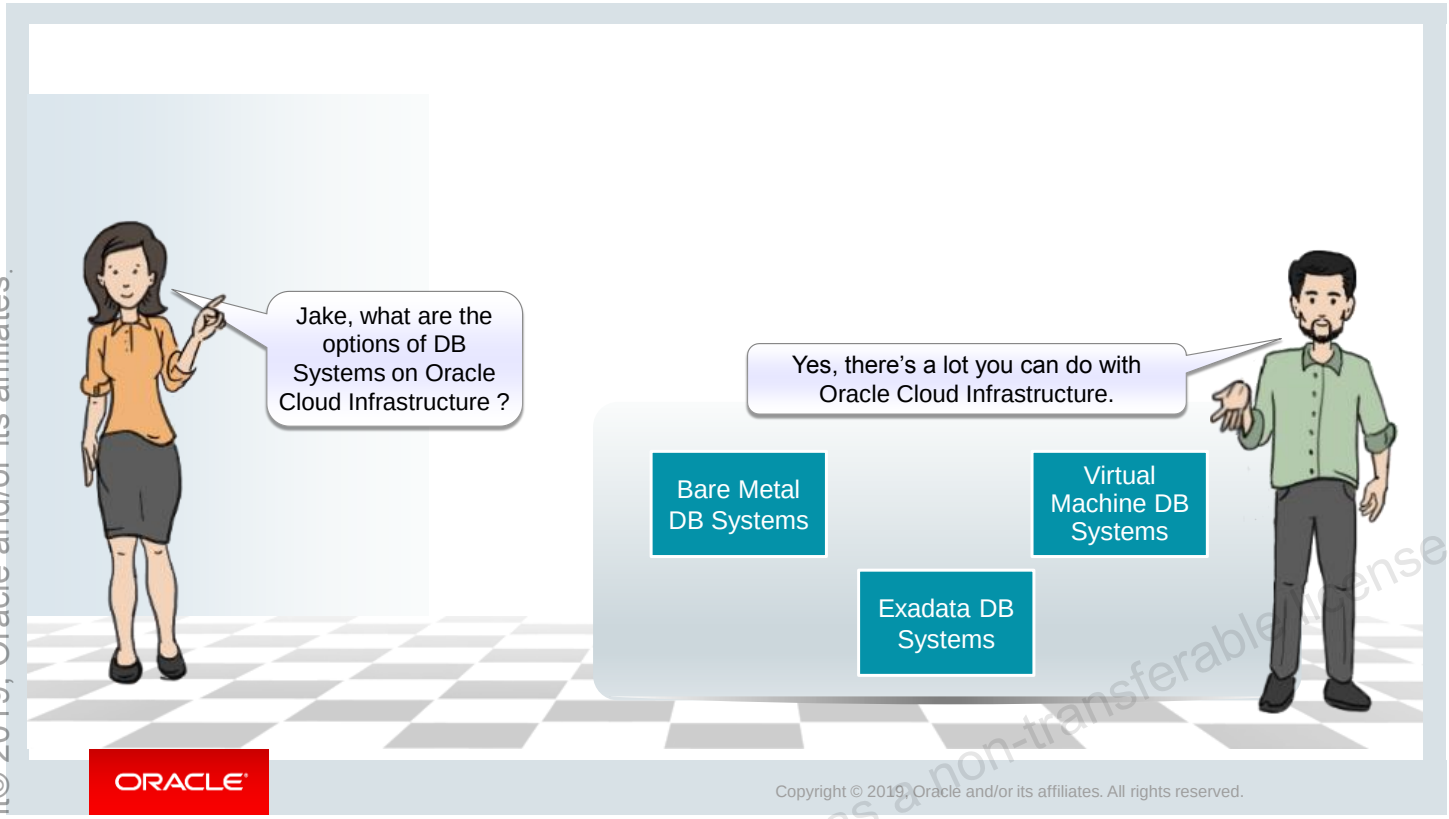
Objectives

After completing this lesson, you should be able to describe:

- The options of database systems available with Oracle Cloud Infrastructure
- The features of Database Service
- Database High Availability and scalability with Oracle Cloud Infrastructure

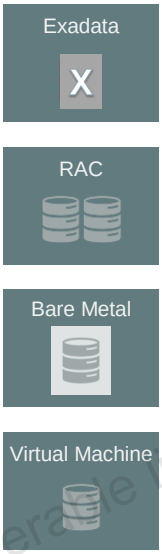
For this lesson we will look into fundamentals of the OCI Database System instances on Oracle Cloud Infrastructure.

We will go over the various types of DB Systems, some of the characteristics of the various OCI Database Systems, and finally go over how to launch an instance.



Oracle Cloud Infrastructure: Database Service

- Mission critical, enterprise grade cloud database service
- Complete Lifecycle Automation
- High Availability and Scalability
- Security
- OCI Platform Integration
- Bring Your Own License (BYOL)



At a very high level there are three types of DATABASE systems offered by Oracle Cloud Infrastructure - first the bare metal database systems comes in a single node shape. The second type of system is the VM based shapes which support single and two node cluster operations. The third type of Oracle Database System on Oracle Cloud Infrastructure is Exadata which comes in quarter, half, and full rack shapes.

Oracle Database Service is backed by a robust infrastructure and is capable of handling mission critical production workloads.

This includes three Availability Domains and multiple regions. Currently active redundancy can be implemented with features such as dataguard configured to operate across Availability Domains.

The networking that backs these database systems, along with every other system on OCI, is a fully non-blocking fully contextualized (multi-tenant with full isolation between networks). Speeds go from a minimum of 10 gigabit up to dual 25 gigabit per host along with dedicated InfiniBand for cluster and storage networking for RAC and Exadata shapes.

Isolation is accomplished through off-box networking which allows bare metal hosts along with database systems like Exadata to participate in virtual networks without needing vswitch software installed on host.

For multi-node shapes, the cluster networking is dedicated InfiniBand.

Database Systems are protected by 2 or 3-way mirroring.

The Database Systems can be brought up stand along or in a RAC cluster which is entirely configured and managed by the Database Service. In addition to RAC, Exadata Systems are also available.

Because the systems are fully managed they are MAA (maximum availability architecture) compliant.

Dynamic CPU and Storage Scaling features are available as well as the ability to upsize Exadata deployments across shapes. CPU core usage can be changed hourly to right-size the Database System.

For security there are a number of features and capabilities.

There are as part of the identity service users, groups, compartments, and policies which can share or isolate the database system with fine grained roles based controls.

There is also networking security, implicit isolation, off box network virtualization as well as security lists and on-host firewalls in place.

Along with the policies and network security there is a complete auditing service which tracks all actions of the users whether through the API or Console.

At the Database level there is encryption on by default. Data at rest is transparently encrypted. Backups done to the object store are encrypted and communications with the Database service are encrypted by default.

Licensing flexibility is also available with BYOL - either use the database service with included licenses or bring existing Oracle licenses to the host for use on the cloud.

All of the Database Systems on OCI can be managed by tools such as Enterprise Manager, SQL Developer, etc., just as a regular on premise database.

==========

Robust Infrastructure

- 3 Availability Domain – Region architecture
- Fully redundant and non blocking Clos Networking Fabric
- 3 way mirrored storage (optional 2 way mirroring) for Database
- Redundant Infiniband Fabric (Exadata, 2 Node RAC) for Cluster networking

Robust Database Options

- Database RAC Option
- Automated Data Guard
  - Within the AD and across AD
- MAA Certified Deployment

Automated CPU and Storage Scaling

Infrastructure

- Comprehensive IAM Resource Security Model
  - Users, Group, Policy and Resource Compartments
- Security List – IP Firewall
- Audit logs for IaaS/DBaaS API

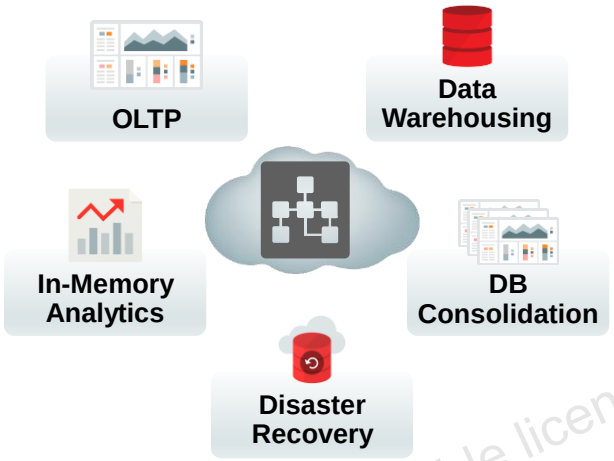
Database

- Default TDE encryption for at rest data
- Encrypted backup in Object Store
- Secure Client communication thru SQLNet

Mention - bring your own license.

Database Service: Use Cases

- Mission Critical Production Databases
- Test, Development, Certification, Try Before You Buy
- Disaster Recovery
- Migration of Database to the Cloud



The database service is suitable for a wide range of workloads and use cases.

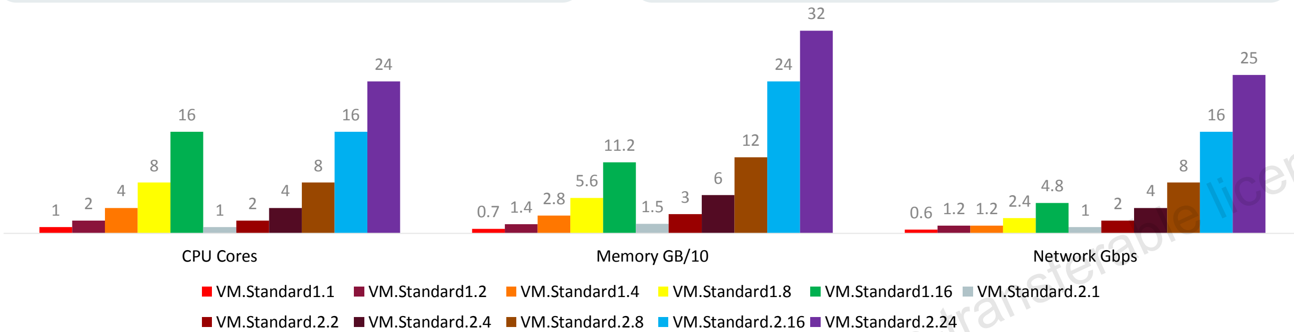
- Anything mission critical can be brought to an Oracle Cloud Infrastructure Database System.
- Very large databases, with scaling in Exadata currently going to 8 nodes/336 cores, 12 storage servers, 5.7TB of RAM, 150 TB of flash, 1.1 PB of raw disk and 330TB of usable storage with 3-way mirroring.
- Database consolidation, with containerized DBs - CDBs and PDBs; the database has been written with database consolidation in mind.
- OLTP, Date warehouse, analytics, and reporting
- The Database service is ideal to bring Applications Unlimited to the cloud - E-business Suite, JD Edwards, PeopleSoft and Siebel. These applications all have a growing set of tools to assist customers to Lift and Shift and Move and Improve on-premises applications to OCI.
- Smaller shapes are ideal for Test, development and certification efforts. In addition, it's possible to test out very large Database Systems shapes without having to deal with procurement to see how performance would be on an Exadata.
- Database Systems on OCI can be managed with existing tools such as enterprise manager / cloud control - same as on-premises systems. DB Systems can be configured with Dataguard, Data Pump, GoldenGate, work with RMAN, backup to object storage, etc.
- There's flexibility.

Virtual Machine DB Systems

Platform	CPU Core	Memory	Storage	Network	RAC Interconnect	Nodes
VM (X5)	1 -16	7-112 GB	256GB -40 TB	0.6- 4.8 Gbps	0.6-4.8 Gbps	1-2
VM (X7)	1-24	15-320 GB	256GB -40 TB	1- 24.6 Gbps	1-24.6 Gbps	1-2

- Single Instance or 2 Node RAC
- Multiple replicated copies of Block Storage
- VM.Standard2 shapes more performant than VM.Standard1 shapes at the same price

- Very high performance SR-IOV based network interface
- Scale storage from 256 GB to 40 TB with no down time
- VM.Standard2 shapes have ~100% more IOPS than VM.Standard1 shapes



ORACLE

First we can look at the Database Service on VMs.

Database on VMs offers a wide range of flexibility for the Database Service.

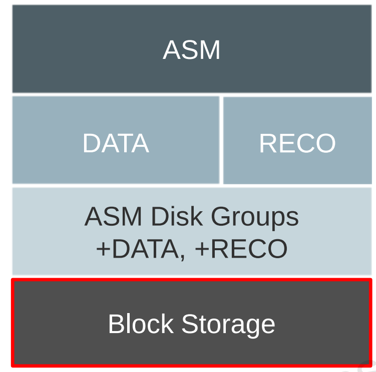
Not all workloads need dedicated baremetal servers. Customers asked for a cost effective, easy to get started, and durable database option well-suited for a variety of workloads ranging from proof of concept, dev/test environments to production applications.

VM based Database Shapes can accommodate these workloads.

The Database Service on VMs is fully featured - while these instances are run on VMs, the software can be configured with Standard, Enterprise, High and Extreme Editions. Database service on VMs is built on the same high performance, enterprise secure grade, highly durable, and available Cloud infrastructure used by all Oracle Cloud Infrastructure Services.

VM DB Systems Storage Architecture

- Tracks the layout, configuration, and status of storage
- Monitors the disks for hard and soft failures
- ASM relies on Block Storage for mirroring data.
- Different Block Storage volumes are used for DATA and RECO.
- Block volumes are mounted using iSCSI.
- ASM uses external redundancy by relying on the triple mirroring of the Block Storage.
- These actions ensure the highest level availability and performance at all times.



ORACLE

Storage on OCI Database Systems

ASM directly interfaces with the disks.

Disks are not mounted on ACFS or another file system providing maximum IO. Some resources such as wallets are mounted in a common store along with database homes (binaries) but the DATA and RECOVERY areas are within ASM.

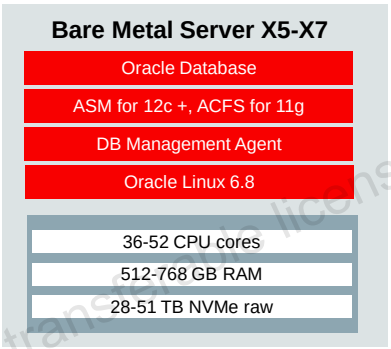
Storage is continuously monitored for any failures with the disks. These disks refer to NVME and SSDs. In the case of VM shapes, block volume is used, which is NVME based, and multiple block volumes are brought in and managed in the same way as these disks.

Any disks that fail will be managed. Space is reserved for rebalancing so the amount of free space is actually calculated based on that reservation. Whenever the shapes list a maximum amount of usable space in DATA and RECO, these reservations for rebalancing are already taken into account.

The root user has complete control over the Storage subsystem so customization and tuning is possible, but the service sets these up by default in an optimal way.

Bare Metal DB Systems

- Bare Metal DB Systems rely on Bare Metal servers running Oracle Linux.
- One-node database system:
  - Single Bare Metal server
  - Locally attached 28 or 51 TB NVMe storage (raw)
  - Scale up/down OCPUs based on requirement
  - Data Guard within and across ADs
  - Restore databases from current backups



The Bare Metal Database System comprises a 1-node DB System.

This is a single bare metal server running Oracle Linux 6.8, with locally attached NVMe storage. This is the least expensive type of system and is recommended for test and development environments. If the node fails, you can simply launch another system and restore databases from current backups.

You can manage these systems by using the Console, API, Enterprise Manager, Enterprise Manager Express, SQL Developer, and the dbcli CLI.

Shapes for Bare Metal Database Systems

Platform	CPU Core	Memory	Storage	Network	Nodes
Bare Metal	2-52	512-768 GB	28.8-51.2 TB	10-25 Gbps	1

- Dense IO X7
  - 1 x x86 Server
  - 52 Cores
  - 768 GB Memory
  - 51.2 TB SSD (8 x 6.5 NVMe)
  - Single Instance
  - Capacity On Demand, 2-52 Cores
  - 25 Gbps Networking
- Dense IO X5
  - 1 x x86 Server
  - 36 Cores
  - 512 GB Memory
  - 28.8 TB SSD (9 x 3.2 NVMe)
  - Single Instance
  - Capacity On Demand, 2-36 Cores
  - 10 Gbps Networking

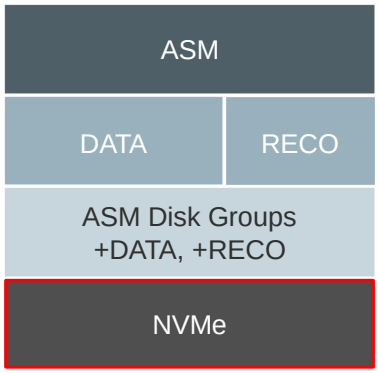
Shapes for Bare Metal DB Systems

When you launch a DB System, you choose a shape, which determines the resources allocated to the DB System. The available shapes are:

- **BM.DenseIO1.36:** Provides a 1-node DB System (one bare metal server), with up to 36 CPU cores, 512 GB memory, and nine 3.2 TB locally attached NVMe drives (28.8 TB total) to the DB System.
- **BM.DenseIO2.52:** Provides a 1-node DB System (one bare metal server), with up to 52 CPU cores, 768 GB memory, and sixteen 3.2 TB locally attached NVMe drives (51.2 TB total) to the DB System.

BM DB Systems Storage Architecture

- Tracks the layout, configuration, and status of storage
- Monitors disks for hard and soft failures
- Proactively offlines and corrects disks
- Automatic incident creation on disk failure
- ASM manages mirroring of NVMe disks
- Disks are partitioned: one for DATA and one for RECO



Salient features of the BM DB Systems Storage Architecture and its benefits:

- Tracks the layout, configuration, and status of storage
- Monitors disks for hard and soft failures
- Proactively offlines and corrects disks that fail/are predicted to fail/perform poorly
- On disk failure, automatically creates an internal ticket and notifies the internal team
- ASM manages mirroring of NVMe disks
- Disks are partitioned: one for DATA and one for RECO

Exadata DB Systems

- Full Oracle Database with all advanced options
- Fastest and most available database cloud platform
  - Scale-Out Compute, Scale-Out Storage, InfiniBand, PCIe flash
  - Complete isolation of tenants with no overprovisioning
- All benefits of public cloud
  - Fast, elastic, web-driven provisioning
  - Oracle experts deploy and manage infrastructure

In addition to VMs, Bare Metal hosts, and Bare Metal RAC and VM, Exadata is available on OCI.

The Exadata systems are provided in 3 shapes and all of them have all the advanced options that Exadata provides turned on.

These are physical Exadata engineered systems - complete with Infiniband networking and scalable compute and storage nodes - that can be run on OCI without modification.

Complete isolation of tenants is facilitated - whenever partial shapes of Exadata are used tenants are completely isolated.

Exadata on OCI gives all of the features, performance and capabilities of on-premise Exadata but with the flexibility of cloud.

All the installation, from systems, to firmware, to OS install and maintenance to patching are all managed by oracle and presented as a public cloud service.

Exadata DB X7 Systems

- Oracle manages Exadata infrastructure
- You can specify zero cores when you launch Exadata
- Billed for the Exadata infrastructure for the first month, and then by the hour after that
- Scaling from ¼ to a ½ rack, or from ½ to a full rack

- Oracle manages Exadata infrastructure: servers, storage, networking, firmware, hypervisor, etc.
- You can specify zero cores when you launch Exadata. This provisions and immediately stops Exadata.
- You are billed for the Exadata infrastructure for the first month, and then by the hour after that.
- Scaling from ¼ to a ½ rack, or from ½ to a full rack requires that the data associated with database deployment is backed up and restored on a different Exadata DB system.

Exadata DB X7 Systems

Resource	Quarter Rack		Half Rack		Full Rack	
	X6	X7	X6	X7	X6	X7
Number of Compute Nodes	2		4		8	
Total Minimum (Default) Number of Enabled CPU Cores	22	0	44	0	88	0
Total Maximum Number of Enabled CPU Cores	84	92	168	184	336	368
Total RAM Capacity	1440 GB		2880 GB		5760 GB	
Number of Exadata Storage Servers	3		6		12	
Total Raw Flash Storage Capacity	38.4 TB	76.8 TB	76.8 TB	153.6 TB	153.6 TB	307.2 TB
Total Raw Disk Storage Capacity	288 TB	360 TB	576 TB	720 TB	1152 TB	1440 TB
Total Usable Storage Capacity	84 TB	106 TB	168 TB	212 TB	336 TB	424 TB

ORACLE

Exadata DB Systems are offered in quarter rack, half rack, or full rack configurations, and each configuration consists of compute nodes and storage servers.

You can see on this table the usable storage capacity and ram for each of the configurations.

It is very nice to be able to try out Exadata for your database needs on the cloud without having to deal with procuring a physical Exadata. Customers are starting to be able with Oracle Cloud infrastructure try Exadata out and they like what they see.

Each compute nodes are each configured so that users have root access to a virtual context running on the compute hosts.

You have root privilege to these compute nodes so you can load and run additional software on them.

However, users do not have administrative access to the Exadata infrastructure components, such as the physical compute node hardware, network switches, power distribution units (PDUs), integrated lights-out management (ILOM) interfaces, or the Exadata Storage Servers, which are all administered by Oracle.

You have full administrative privileges for your databases, and you can connect to your databases via public or private IPs or both.

Users are responsible for database administration tasks such as creating tablespaces and managing database users.

You can also customize the default automated maintenance set up, and you control the recovery process in the event of a database failure.

Exadata DB Systems on Oracle Cloud Infrastructure benefit from having the IAM service which helps create policies on which users and groups can perform actions on the Exadata and DB Systems.

You can have compartments and VCNs for these database services and either isolate or share them.

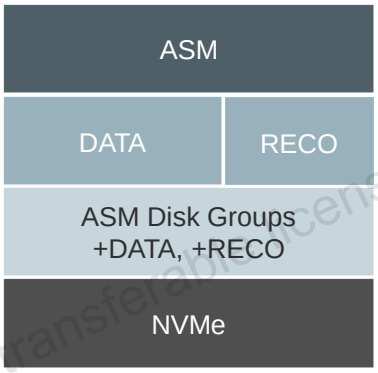
All of the virtual cloud network capabilities and advantages are afforded to the DB and Exadata DBAAS system. You do not have to use a public IP for any of the instances if you do not want to.

You can use VPN and fastconnect to connect to your on-prem environments.

Because of the capabilities of Oracle Cloud Infrastructure we can have the application tier seamlessly running on VMs while the database is running on bare metal.

Exadata DB Systems Storage Architecture

- Backups provisioned on Exadata storage: ~ 40% to DATA and ~ 60% to RECO
- Backups not provisioned on Exadata storage: ~ 80% to DATA and ~ 20% to RECO
- Submit a service request to adjust allocation without reconfiguring



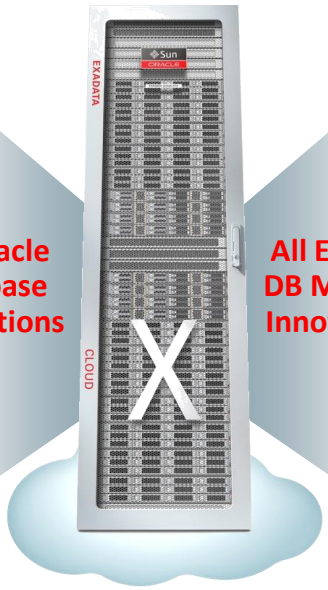
Salient features of the Exadata DB Systems Storage Architecture and its benefits

- Backups provisioned on Exadata storage: ~ 40% allocated to the DATA disk group and ~ 60% allocated to the RECO disk group
- Backups not provisioned on Exadata storage: ~ 80% allocated to the DATA disk group and ~ 20% allocated to the RECO disk group
- After storage is configured, the only way to adjust the allocation without reconfiguring the whole environment is by submitting a service request to Oracle.

Exadata Cloud Enterprise Edition Extreme Performance
Most Powerful Database + Platform

Multitenant	
In-Memory DB	
Real Application Clusters	
Active Data Guard	
Partitioning	
Advanced Compression	
Advanced Security, Label Security, DB Vault	
Real Application Testing	
Advanced Analytics, Spatial and Graph	
Management Packs for Oracle Database	

All Oracle Database Innovations



All Exadata DB Machine Innovations

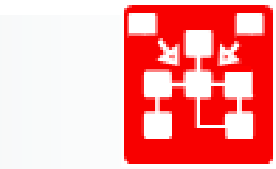
Offload SQL to Storage	
InfiniBand Fabric	
Smart Flash Cache, Log	PCI Flash
Storage Indexes	
Columnar Flash Cache	
Hybrid Columnar Compression	10:1
I/O Resource Management	I/O I/O I/O
Network Resource Management	PRIORITY LANE
In-Memory Fault Tolerance	
Exafusion Direct-to-Wire Protocol	

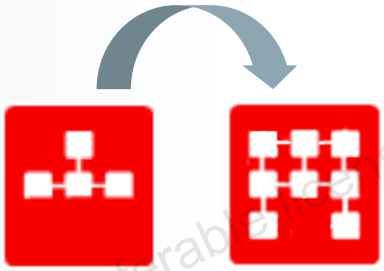
ORACLE

Scaling Exadata DB Systems

Two ways of scaling Exadata DB Systems:

- Scaling within an Exadata DB System
- Scaling across Exadata DB System configurations





There are a few options for scaling the Exadata DB Systems on Oracle Cloud Infrastructure

Scaling within: You can scale up the number of enabled CPU cores in the system if an Exadata DB System requires more compute node processing power.

Just modify the number of enabled CPU cores.

Scaling across: Exadata DB System configurations enables you to move to a different system configuration. This is useful when a database deployment requires:

- Processing power that is beyond the capacity of the current system configuration
- Storage capacity that is beyond the capacity of the current system configuration
- A performance boost that can be delivered by increasing the number of available compute nodes
- A performance boost that can be delivered by increasing the number of available Exadata storage servers

Scaling from a quarter rack to a half rack, or from a half rack to a full rack, requires that the data associated with your database deployment is backed up and restored on a different Exadata DB System, which requires planning and a maintenance window, but can happen very quickly due to the speed of the underlying infrastructure and networking.

OCI DB Systems: VM, BM, Exadata

	Virtual Machine (VM)	Bare Metal (BM)	Exadata
Scaling	Storage (number of CPU cores on VM DB cannot be changed)	CPU (amount of available storage cannot be changed)	CPU can be scaled within a ¼ , ½, and full rack. Storage cannot be scaled
Multiple Homes/Databases	No, single DB and Home only	Yes (one edition, but different versions possible)	Yes
Storage	Block Storage	Local NVMe disks	Local spinning disks and NVMe flash cards
Real Application Clusters (RAC)	Available (2-node)	Not Available	Available
Data Guard	Available	Available	Available*

*You can manually configure Data Guard on Exadata DB Systems using native Oracle Database utilities and commands. dbcli is not available on Exadata DB Systems.

ORACLE

First we can look at the Database Service on VMs.

Database on VMs offers a wide range of flexibility for the Database Service.

Not all workloads need dedicated baremetal servers. Customers asked for a cost effective, easy to get started, and durable database option well-suited for a variety of workloads ranging from proof of concept, dev/test environments to production applications.

VM based Database Shapes can accommodate these workloads.

The Database Service on VMs is fully featured - while these instances are run on VMs, the software can be configured with Standard, Enterprise, High and Extreme Editions. Database service on VMs is built on the same high performance, enterprise secure grade, highly durable, and available Cloud infrastructure used by all Oracle Cloud Infrastructure Services.

In virtualization, single root input/output virtualization or **SR-IOV** is a specification that allows the isolation of the PCI Express resources for manageability and performance reasons. A single physical PCI Express can be shared on a virtual environment using the **SR-IOV** specification.

Database Editions and Versions

	VM DB Systems	BM DB Systems	Exadata DB Systems	DB Versions
Standard Edition	Yes	Yes	No	11.2.0.4 12.1.0.2 12.2.0.1 18.1.0.0
Enterprise Edition	Yes	Yes	No	
High Performance	Yes	Yes	No	
Extreme Performance	Yes	Yes	Yes	
BYOL	Yes			

With OCI Database Service there are four main versions of the Database available , 11.2, 12.1, 12.2 and 18.1

Depending on the shape and clustering configuration, certain shapes are restricted to Extreme Performance.

All shapes have the ability for the user to BYOL.

All of the shapes can use multiple instances of the database and mix and match.

Database Editions and Options

Database Edition	Database Options
Database Standard Edition	Includes the Oracle Database Standard Edition Package
Database Enterprise Edition	Includes the Oracle Database Enterprise Edition Package, Data Masking and Subsetting Pack, Diagnostics and Tuning Packs, and Real Application Testing

Note that all packages include Oracle Database Transparent Data Encryption (TDE).

Database Editions and Options

Database Edition	Database Options
Database Enterprise Edition High Performance	Extends the Enterprise package with the following options: Multitenant, Partitioning, Advanced Compression, Advanced Security, Label Security, Database Vault, OLAP, Advanced Analytics, Spatial and Graph, Database Lifecycle Management Pack, and Cloud Management Pack for Oracle Database
Database Enterprise Edition Extreme Performance	Extends the High Performance package with the following options: Real Application Clusters (RAC), In-Memory Database, and Active Data Guard

Note that all packages include Oracle Database Transparent Data Encryption (TDE).

High Availability and Scalability

- Robust Infrastructure
  - Region with 3 Availability Domains architecture
  - Fully redundant and non-blocking networking fabric
  - 2-way or 3-way mirrored storage for database
  - Redundant InfiniBand fabric (Exadata) for cluster networking
- Database Options to enable HA
  - Database RAC option
  - Automated Data Guard within and across ADs
- Dynamic CPU and Storage Scaling

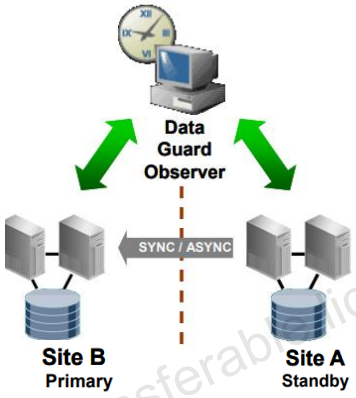
- The database service is built for availability and scalability.
- Backups are hosted on regional services like object storage which span across availability domains.
- Dataguard can be implemented across availability domains so that linked systems and backups can survive AD level disruptions.
- Networking fabric is fully non-blocking with bare metal servers having 10 and 25 gigabit networking to the host. The generation2/x7 shapes have dual 25gbe networking to the bare metal hosts.
- Storage is setup to be highly available and has two options, NORMAL/2-way mirroring and HIGH/3-way mirroring which guarantees that there are two or three copies of every extent.
- For RAC and Exadata shapes there is a dedicated Infiniband fabric for cluster networking.
- With RAC shapes the ability to create highly available database instances - from VMs, to Exadata. With dataguard the ability to stretch the availability of the database pair across availability domains.
- The Database Systems are fully managed by Oracle and follow MAA/Maximum Availability Architecture - the supported and best practices are built in.
- It is also possible to scale database shapes from minimum to maximum CPU usage on the fly on a hourly basis. Within Exadata shapes there are options for users to grow out of smaller shapes to larger ones.
- Dynamic storage
- Scaling for VMs only
- Bare metal dynamic CPU storage

Data Guard

- Supported on Bare Metal and Virtual Machine DB Systems only
- Limited to one Standby database per Primary database
- Standby database used for queries, reports, test, or backups (only for Active Data Guard)
- Switchover
  - Planned role reversal, never any data loss
  - No database re-instantiation required
  - Used for database upgrades, tech refresh, data center moves, etc.
  - Manually invoked via Enterprise Manager, DGMGRL, SQL*Plus, or GUI
- Failover
  - Unplanned failure of Primary
  - Flashback Database used to reinstate original Primary
  - Manually invoked via Enterprise Manager, DGMGRL, SQL*Plus, or GUI
  - May also be done automatically: Fast-Start Failover

Data Guard

- Run Primary, Standby, and Observer in separate ADs. Observer determines whether or not to fail over to a specific target standby database.
- Automatic database failover upon:
  - Database down
  - Designated health-check conditions
  - Request of an application
- Supported with:
  - Maximum Availability
  - Maximum Performance
  - Maximum Protection
- Default mode is set to Maximum Performance when you configure Data Guard using the OCI console.



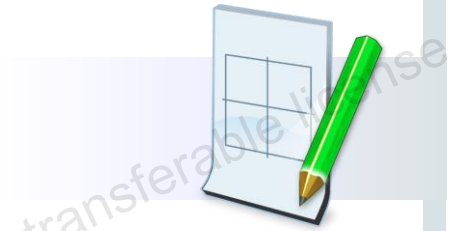
Summary

In the lesson, you should have learned how to describe:

- The options of database systems available with Oracle Cloud Infrastructure
- The features of Database Service
- Database High Availability and scalability with Oracle Cloud Infrastructure

Practice 3: Overview

There are no practices for this lesson.

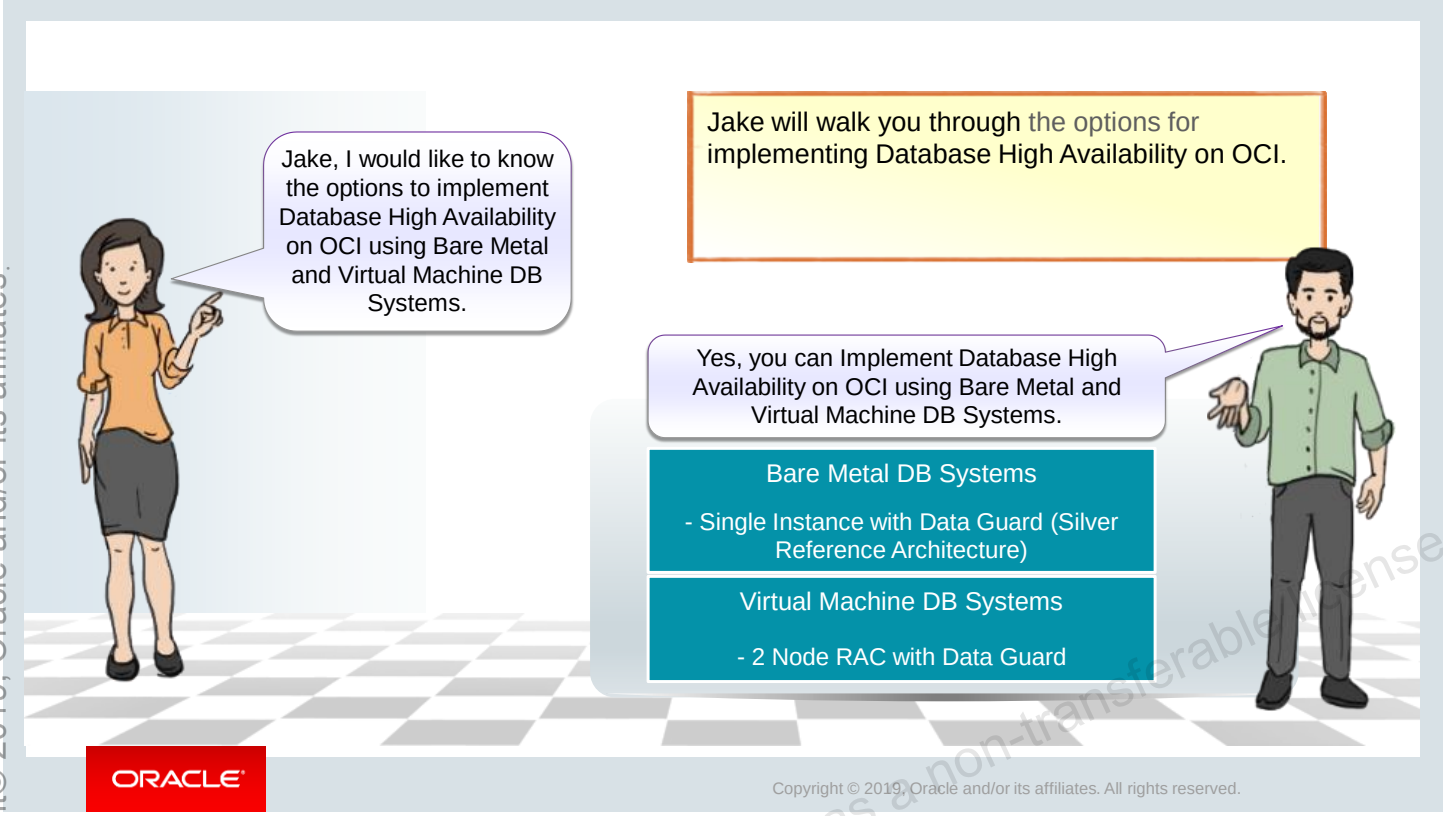


Available DB Systems for Implementing Database High Availability on OCI

Objectives

After completing this lesson, you should be able to describe:

- Bare Metal and Virtual Machine DB Systems
- Supported Database Editions and Versions
- Shapes for Bare Metal DB Systems
- Bare Metal Database Storage Options
- Shapes for Virtual Machine DB Systems
- Storage Options for Virtual Machine DB Systems
- Database System: Storage Architecture



Bare Metal DB Systems doesn't have RAC.

Database High Availability can be implemented by following the Silver Reference Architecture that has been explained in the lesson **'Building Blocks for High Availability in Oracle Cloud Infrastructure"**

RAC – Real Application Cluster

Compute: Bare Metal and Virtual Machines

Bare Metal (BM)

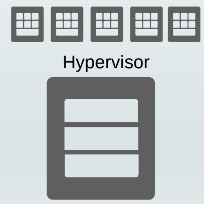
Direct Hardware Access: Customers get the full Bare Metal server.

(Single-tenant model)

Virtual Machine (VM)

A hypervisor to virtualize the underlying Bare Metal server into smaller VMs.

(Multi-tenant model)



VM compute instances run on the same hardware as Bare Metal instances, leveraging the same cloud-optimized hardware, firmware, software stack, and networking infrastructure.

ORACLE

OCI is the only public cloud that supports bare metal and VMs using the same set of APIs, hardware, firmware, software stack, and networking infrastructure. You can see the two models in the slide. Bare Metal instances are instances where customers get the full server. This is also referred to as a single-tenant model. The advantage here is that there is no performance overhead, no shared agents, and no noisy neighbors. On the other spectrum are VMs, where the underlying host is virtualized to provide smaller VMs – also referred to as the multi-tenant model. The advantage here is flexibility with regard to choice of instance shapes.

Bare Metal

Direct hardware access with all the security, capabilities, elasticity, and scalability of Oracle Cloud Infrastructure

Workloads that are performance-intensive

Workloads that are not virtualized

Workloads that require BYOL licensing

Database Editions and Versions

	VM DB Systems	BM DB Systems	Exadata DB Systems	DB Versions
Standard Edition	Yes	Yes	No	11.2.0.4 12.1.0.2 12.2.0.1 18.1.0.0
Enterprise Edition	Yes	Yes	No	
High Performance	Yes	Yes	No	
Extreme Performance	Yes	Yes	Yes	
BYOL	Yes			

With OCI Database Service there are four main versions of the Database available, 11.2, 12.1, 12.2 and 18.1

Depending on the shape and clustering configuration, certain shapes are restricted to Extreme Performance.

All shapes have the ability for the user to BYOL.

All of the shapes can use multiple instances of the database and mix and match.

Database Editions and Options

Database Edition	Database Options
Database Standard Edition	Includes the Oracle Database Standard Edition Package
Database Enterprise Edition	Includes the Oracle Database Enterprise Edition Package, Data Masking and Subsetting Pack, Diagnostics and Tuning Packs, and Real Application Testing

Note that all packages include Oracle Database Transparent Data Encryption (TDE).

Database Editions and Options

Database Edition	Database Options
Database Enterprise Edition High Performance	Extends the Enterprise package with the following options: Multitenant, Partitioning, Advanced Compression, Advanced Security, Label Security, Database Vault, OLAP, Advanced Analytics, Spatial and Graph, Database Lifecycle Management Pack, and Cloud Management Pack for Oracle Database
Database Enterprise Edition Extreme Performance	Extends the High Performance package with the following options: Real Application Clusters (RAC), In-Memory Database, and Active Data Guard

Note that all packages include Oracle Database Transparent Data Encryption (TDE).

Shapes for Bare Metal Database Systems

Platform	CPU Core	Memory	Storage	Network	Nodes
Bare Metal	2-52	512-768 GB	28.8-51.2 TB	10-25 Gbps	1

- Dense IO X7
  - 1 x x86 Server
  - 52 Cores
  - 768 GB Memory
  - 51.2 TB SSD (8 x 6.5 NVMe)
  - Single Instance
  - Capacity On Demand, 2-52 Cores
  - 25 Gbps Networking

- Dense IO X5
  - 1 x x86 Server
  - 36 Cores
  - 512 GB Memory
  - 28.8 TB SSD (9 x 3.2 NVMe)
  - Single Instance
  - Capacity On Demand, 2-36 Cores
  - 10 Gbps Networking

Shapes for Bare Metal DB Systems

When you launch a DB System, you choose a shape, which determines the resources allocated to the DB System. The available shapes are:

- **BM.DenseIO1.36:** Provides a 1-node DB System (one bare metal server), with up to 36 CPU cores, 512 GB memory, and nine 3.2 TB locally attached NVMe drives (28.8 TB total) to the DB System.
- **BM.DenseIO2.52:** Provides a 1-node DB System (one bare metal server), with up to 52 CPU cores, 768 GB memory, and sixteen 3.2 TB locally attached NVMe drives (51.2 TB total) to the DB System.

For latest list of available OCI Shapes refer this link:

https://docs.cloud.oracle.com/iaas/Content/Compute/References/computeshapes.htm

Bare Metal Database Storage Options

The following table outlines the storage used based on the shape and options of the Bare Metal Database System:

Shape	Raw Storage	Usable Storage with Normal Redundancy (2-way Mirroring)	Usable Storage with High Redundancy (3-way Mirroring)
BM.HighIO1.36	12.8 TB NVMe	DATA 3.5 TB RECO 740 GB	DATA 2.3 TB RECO 440 GB
BM.DenseIO1.36	28.8 TB NVMe	DATA 9.4 TB RECO 1.7 TB	DATA 5.4 TB RECO 1 TB
BM.RACLocalStorage1.72 (IAD)	24 TB SSD	DATA 8.6 TB RECO 1.6 TB	DATA 5.4 TB RECO 1 TB
BM.RACLocalStorage.72 (PHX, FRA)	64 TB SSD	DATA 23 TB RECOR 4.2 TB	DATA 14.4 TB RECO 2.6 TB

The shape you choose for a DB System determines its total raw storage. Options, like the percentage of the DISK use for RECOVERY (FRA, RECO, REDO) (either 20% or 60%), 2- or 3-way mirroring, and the space allocated for data files, affect the amount of usable storage on the system.

Since users have full control over Database Systems, you can log in and see exactly how all the disks are partitioned, allocated, and used.

Utilities like ASMCMD are available to the grid user to see the state of the DISK groups. You can also run SQL against any database instance and get the ASM information that lets you know how much space is left.

Disk Required Mirror Free MB: Space needed to rebalance after loss of single or double disk failure (for normal or high redundancy)

Disk Usable File MB: Usable space available after reserving space for disk failure and accounting for mirroring

PCT Util: Percent of Total Diskgroup Space Utilized

Shapes for Virtual Machine Database Systems

Platform	CPU Core	Memory	Storage	Network	RAC Interconnect	Nodes
VM	1 -16	7-112 GB	256GB -48 TB	0.6- 4.8 Gbps	0.6-4.8 Gbps (Shared)	1-2

- A shape for a DB System determines the resources allocated to the DB System.
- For example, the following table shows the available shapes for a virtual machine DB System on X7:

Shape	CPU Cores	Memory
VM.Standard2.1	1	15 GB
VM.Standard2.2	2	30 GB
VM.Standard2.4	4	60 GB
VM.Standard2.8	8	120 GB
VM.Standard2.16	16	240 GB
VM.Standard2.24	24	320 GB

For latest list of available OCI Shares refer this link:

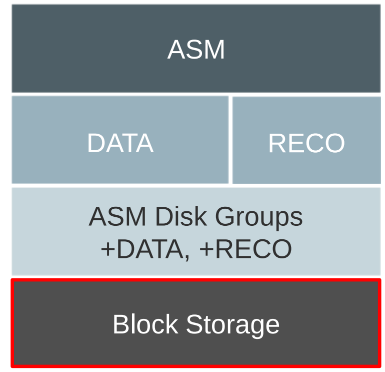
https://docs.cloud.oracle.com/iaas/Content/Compute/References/computeshapes.htm

Storage Options for Virtual Machine DB Systems

- Virtual machine DB Systems use Oracle Cloud Infrastructure block storage.
- Total storage includes available storage plus recovery logs.
- Remote storage starts at 256GB and goes up to 40TB.
- There is dynamic storage scaling.
- For 2 Node RAC virtual machine DB Systems, storage capacity is shared between the nodes.

VM DB Systems: Storage Architecture

- Tracks the layout, configuration, and status of storage
- Monitors the disks for hard and soft failures
- ASM relies on Block Storage for mirroring data.
- Different Block Storage volumes are used for DATA and RECO.
- Block volumes are mounted using iSCSI.
- ASM uses external redundancy relying on the triple mirroring of the Block Storage.
- These actions ensure highest level availability and performance at all times.



ORACLE

Storage on OCI Database Systems

ASM directly interfaces with the disks.

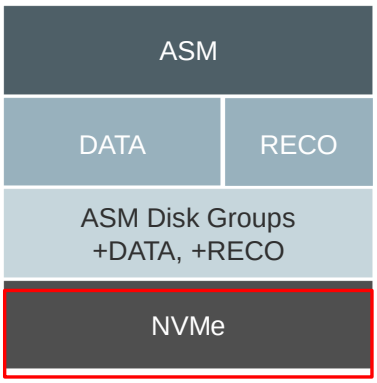
Storage is continuously monitored for any failures with the disks. These disks refer to NVME and SSDs. In the case of VM shapes, block volume is used, which is NVME based, and multiple block volumes are brought in and managed the same way as these disks.

Any disks that fail will be managed. Space is reserved for rebalancing so the amount of free space is actually calculated based on that reservation. Whenever the shapes list a maximum amount of usable space in DATA and RECO, these reservations for rebalancing are already taken into account.

The root user has complete control over the Storage subsystem so customization and tuning is possible but the service sets these up by default in an optimal way.

BM DB Systems: Storage Architecture

- Tracks the layout, configuration, and status of storage
- Monitors disks for hard and soft failures
- Offlines and corrects disks that fail/are predicted to fail/perform poorly
- On disk failure, creates an internal ticket and notifies internal team
- ASM manages mirroring of NVMe disks.



Summary

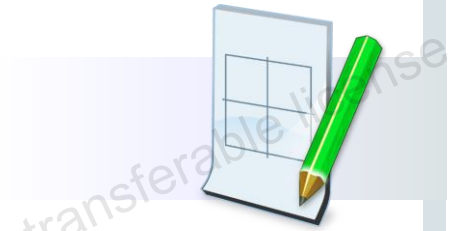
In this lesson, you should have learned how to describe:

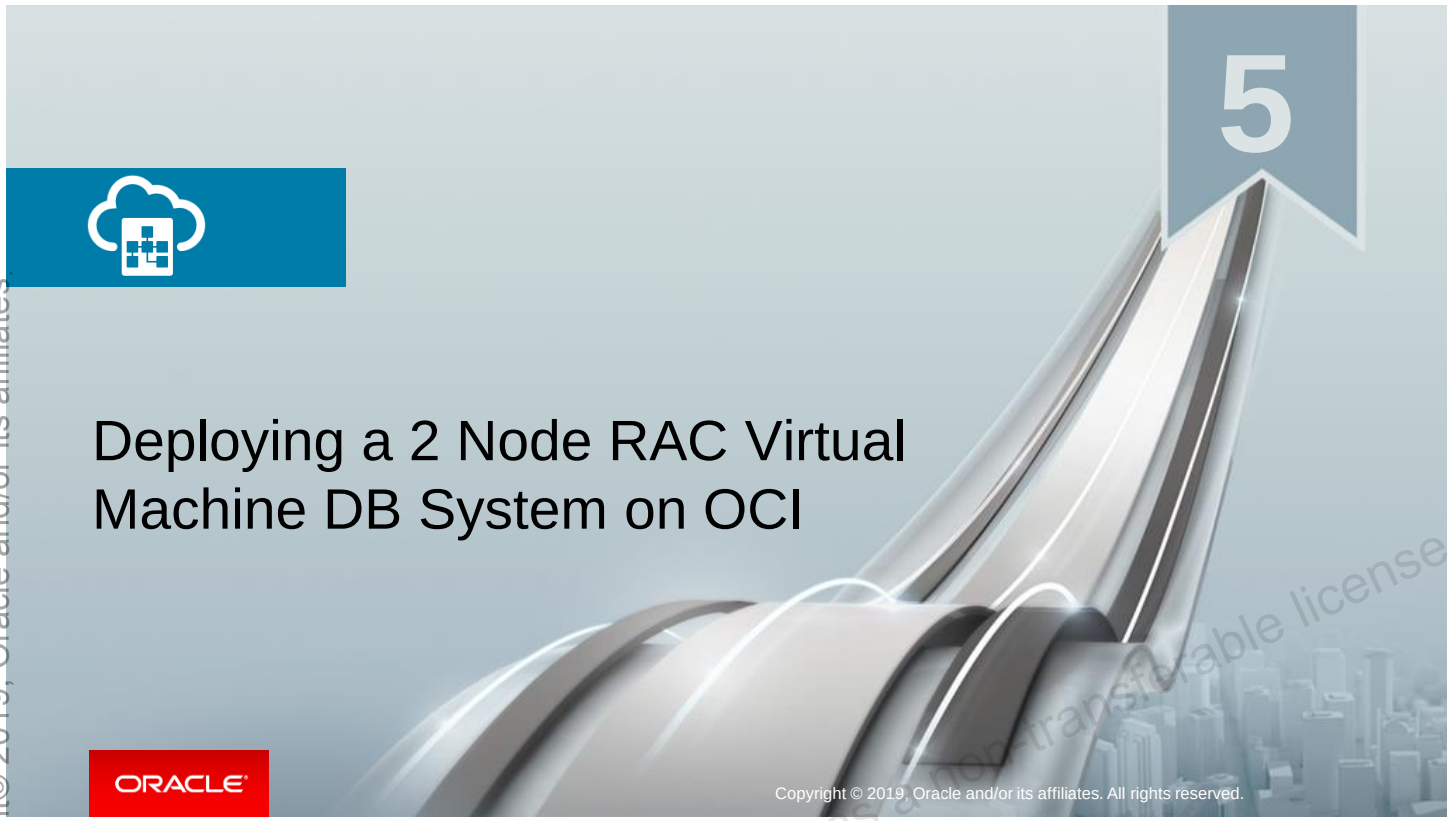
- Bare Metal and Virtual Machine DB Systems
- Supported Database Editions and Versions
- Shapes for Bare Metal DB Systems
- Bare Metal Database Storage Options
- Shapes for Virtual Machine DB Systems
- Storage Options for Virtual Machine DB Systems
- Database System: Storage Architecture

Practice 4: Overview

This practice covers the following topics:

- Practice 4-1: Setting Up PuTTY on Your Local Windows System
- Practice 4-2: Installing Oracle SQL Developer on Your Local Windows System
- Practice 4-3: Exploring the Oracle Cloud Infrastructure Console





Objectives

After completing this lesson, you should be able to:

- Identify the prerequisites to launch a 2 Node RAC Virtual Machine DB System
- Create a Virtual Cloud Network (VCN) for a DB System
- Use the Console to launch a DB System
- Set up DNS for a DB System
- List the special considerations for creating DB Systems

For this lesson we will look into fundamentals of the OCI Database System instances on Oracle Cloud Infrastructure.

We will go over the various types of DB Systems, some of the characteristics of the various OCI Database Systems, and finally go over how to launch an instance.

Prerequisites to Launch a 2 Node Virtual Machine DB System

- You need a public key in OpenSSH format.
- You need the name of a virtual cloud network (VCN).
- Do not use a subnet that overlaps with 192.168.16.16/28.
- For a 2 Node RAC DB System, the subnet must have at least six available IP addresses.

You need the following items to launch any DB System.

- The public key, in OpenSSH format, from the key pair that you plan to use for connecting to the DB System via SSH. A sample public key, abbreviated for readability, is shown below.

  ssh-rsa AAAAB3NzaC1yc2EAAAABJQAA....lo/gKMLVM2xzc1xJr/Hc26biw3TXWGEakrK1OQ== rsa-key-20160304
- The name of a virtual cloud network (VCN) to launch the DB System in.
- Do not use a subnet that overlaps with 192.168.16.16/28, which is used by the Oracle Clusterware private interconnect on the database instance. Specifying an overlapping subnet will cause the private interconnect to malfunction.
- For a 2-node RAC DB System, the subnet must have at least six available IP addresses. Three of each subnet's IP addresses are reserved, so the minimum allowed subnet size is /28.
- If you plan to back up your DB System to Object Storage or to use the managed patching feature, you can use a service gateway with a private subnet or an internet gateway with a public subnet. With an internet gateway, network traffic between the system and Object Storage does not leave the cloud and never reaches the public internet.
- Each VCN subnet has a default security list that contains a rule to allow TCP traffic on destination port 22 (SSH) from source 0.0.0.0/0 and any source port. You can update the default security list or create new lists to allow other types of access, but this can be done before or after you launch the DB System.
- For a 2-node RAC DB System, ensure that port 22 is open for both ingress and egress on the subnet, and that the security rules you create are stateful (the default), otherwise, the DB System might fail to provision successfully.
- If you need DNS name resolution for the system, decide whether to use a *Custom Resolver* (your choice of DNS server) or the *Internet and VCN Resolver* (the DNS capability built in to the VCN).

Prerequisites to Launch a 2 Node Virtual Machine DB System

- You need a service gateway with a private subnet or an Internet gateway with a public subnet in case you are backing up your DB System to Object Storage or using the managed patching feature.
- Each VCN subnet has a default security list.
- For a 2 Node RAC DB System, ensure that port 22 is open for both ingress and egress on the subnet.
- Use a Custom Resolver or the Internet and VCN Resolver for DNS name resolution.

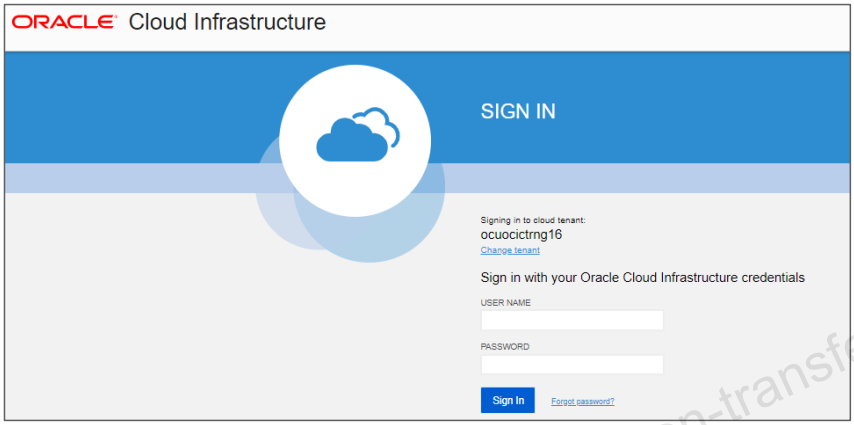
You need the following items to launch any DB System.

- The public key, in OpenSSH format, from the key pair that you plan to use for connecting to the DB System via SSH. A sample public key, abbreviated for readability, is shown below.

  ssh-rsa AAAAB3NzaC1yc2EAAAABJQAA....lo/gKMLVM2xzc1xJr/Hc26biw3TXWGEakrK1OQ== rsa-key-20160304
- The name of a virtual cloud network (VCN) to launch the DB System in.
- Do not use a subnet that overlaps with 192.168.16.16/28, which is used by the Oracle Clusterware private interconnect on the database instance. Specifying an overlapping subnet will cause the private interconnect to malfunction.
- For a 2-node RAC DB System, the subnet must have at least six available IP addresses. Three of each subnet's IP addresses are reserved, so the minimum allowed subnet size is /28.
- If you plan to back up your DB System to Object Storage or to use the managed patching feature, you can use a service gateway with a private subnet or an internet gateway with a public subnet. With an internet gateway, network traffic between the system and Object Storage does not leave the cloud and never reaches the public internet.
- Each VCN subnet has a default security list that contains a rule to allow TCP traffic on destination port 22 (SSH) from source 0.0.0.0/0 and any source port. You can update the default security list or create new lists to allow other types of access, but this can be done before or after you launch the DB System.
- For a 2-node RAC DB system, ensure that port 22 is open for both ingress and egress on the subnet, and that the security rules you create are stateful (the default), otherwise, the DB System might fail to provision successfully.
- If you need DNS name resolution for the system, decide whether to use a *Custom Resolver* (your choice of DNS server) or the *Internet and VCN Resolver* (the DNS capability built in to the VCN).

Creating a Virtual Cloud Network for a DB System

1. Log in to Oracle Cloud Infrastructure:
   - Enter Cloud Tenant.
   - Enter OCI User Name.
   - Enter OCI Password.



Open a supported browser and go to the Console URL given to you either in an email or by your administrator.

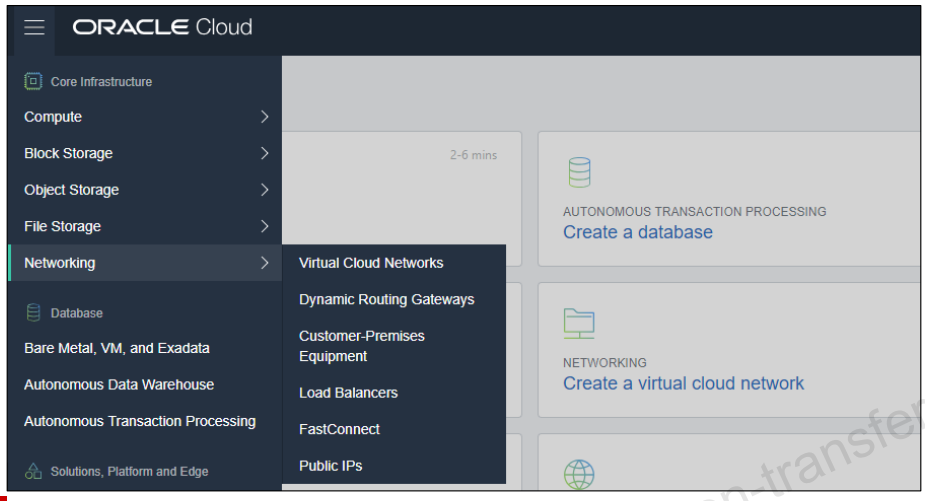
Enter your **Cloud Tenant** and click **Continue**.

Enter your Oracle Cloud Infrastructure user name and password. If this is the first time you are signing in, you will be prompted to change your temporary password.

Note: Credentials that you have set up for other Oracle Cloud products will not work with Oracle Cloud Infrastructure.

Creating a Virtual Cloud Network for a DB System

2. Choose Networking from the menu ☰.
3. Choose Virtual Cloud Networks.

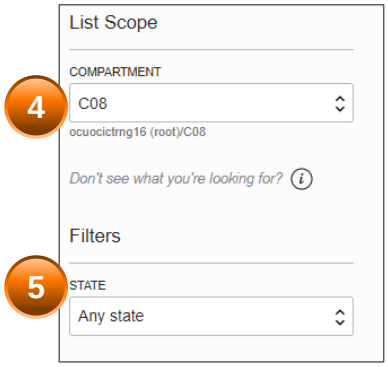


Before you can launch DB System, you need to have a virtual cloud network (VCN) and subnet to launch it into. A subnet is a subdivision of your VCN that you define in a single.

Open the navigation menu. Under **Core Infrastructure**, go to **Networking** and click **Virtual Cloud Networks**.

Creating a Virtual Cloud Network for a DB System

4. Select a Compartment.
5. Select a State.



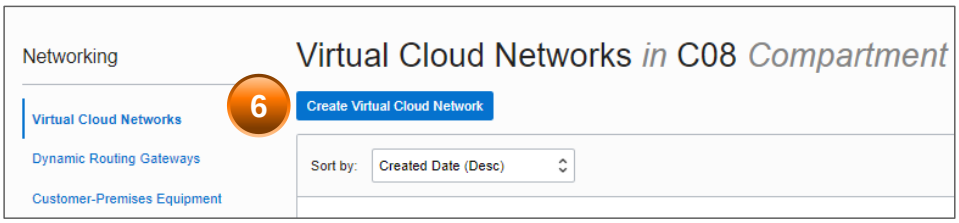
Compartments help you organize and control access to your resources. A compartment is a collection of related resources (such as cloud networks, compute instances, or block volumes) that can be accessed only by those groups that have been given permission by an administrator in your organization.

Ensure that the Sandbox compartment (or the compartment designated for you) is selected on the left.

You or an administrator has created a compartment for your network.

Creating a Virtual Cloud Network for a DB System

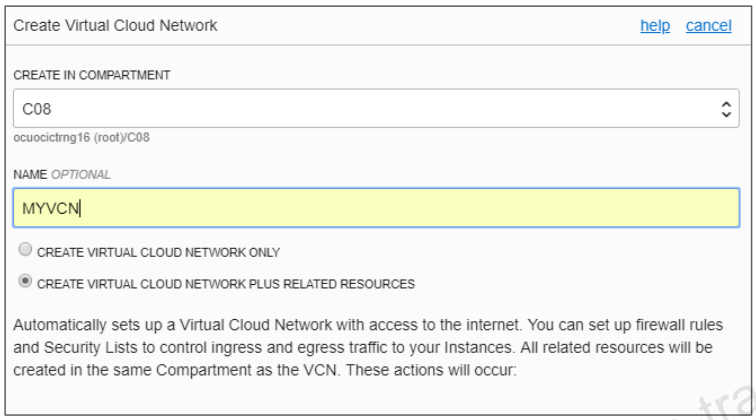
6. Click Create Virtual Cloud Network.



Click **Create Virtual Cloud Network**.

Creating a Virtual Cloud Network for a DB System

7. Enter a Name.
8. Select Create Virtual Cloud Network Plus Related Resources.
9. Click the Create Virtual Cloud Network button.



Enter the following:

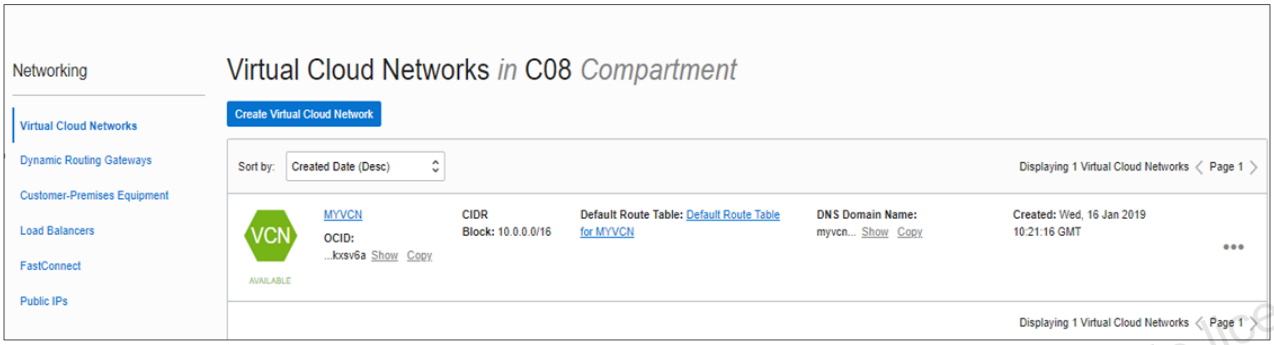
- **Create in Compartment:** This field defaults to your current compartment. Select the compartment you want to create the VCN in, if not already selected.
- **Name:** Enter a name for your cloud network, for example, <your_initials>_Network.
- Select: **Create Virtual Cloud Network Plus Related Resources**. The dialog expands to list the items that will be created with your cloud network.
- Accept the defaults for any other fields.

Scroll to the bottom of the dialog and click **Create Virtual Cloud Network**.

A confirmation page displays the details of the cloud network that you just created. The cloud network has the following resources and characteristics (some of which are not listed in the confirmation dialog):

- CIDR block range of 10.0.0.0/16
- An internet gateway
- A route table with a default route rule to enable traffic to and from the internet gateway
- A default security list. (https://docs.cloud.oracle.com/iaas/Content/Network/Concepts/securitylists.htm#Default). You will edit this default security list later in the tutorial.
- A public subnet in each availability domain.
- The VCN will automatically use the Internet and VCN Resolver (https://docs.cloud.oracle.com/iaas/Content/Network/Concepts/dns.htm) for DNS.

VCN Details

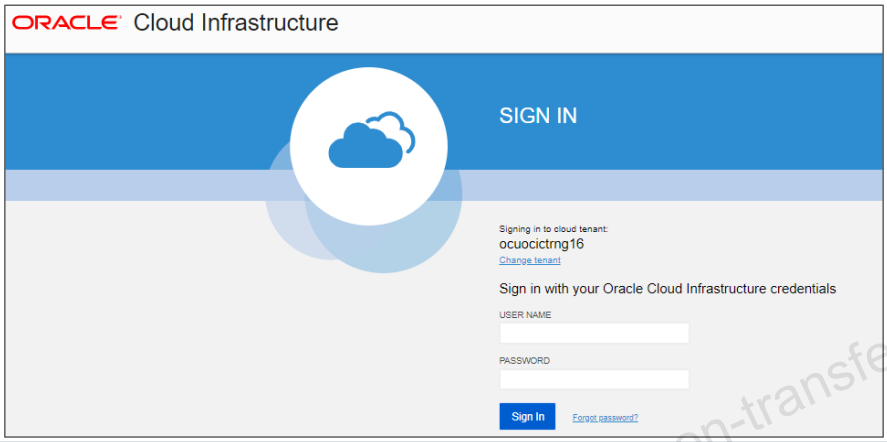


A virtual, private network that you set up in Oracle data centers. It closely resembles a traditional network, with firewall rules and specific types of communication gateways that you can choose to use. A VCN covers a single, contiguous IPv4 CIDR block of your choice.

Subdivisions you define in a VCN (for example, 10.0.0.0/24 and 10.0.1.0/24). Subnets contain virtual network interface cards (VNICs), which attach to instances. Each subnet exists in a single availability domain and consists of a contiguous range of IP addresses that do not overlap with other subnets in the VCN. Subnets act as a unit of configuration within the VCN.

Using the Console to Launch a 2 Node RAC Virtual Machine DB System

1. Log in to Oracle Cloud Infrastructure:
   - Enter Cloud Tenant.
   - Enter OCI User Name.
   - Enter OCI Password.



Open a supported browser and go to the Console URL given to you either in an email or by your administrator.

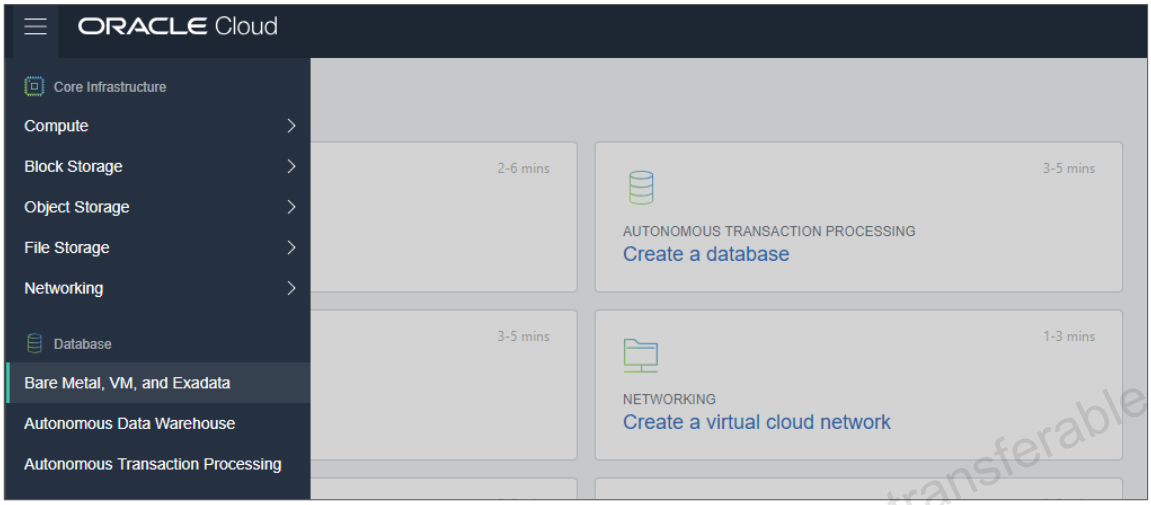
Enter your **Cloud Tenant** and click **Continue**.

Enter your Oracle Cloud Infrastructure user name and password. If this is the first time you are signing in, you will be prompted to change your temporary password.

Note: Credentials that you have set up for other Oracle Cloud products will not work with Oracle Cloud Infrastructure.

Using the Console to Launch a DB System

2. Select the “Bare Metal, VM, and Exadata” option from the OCI menu.

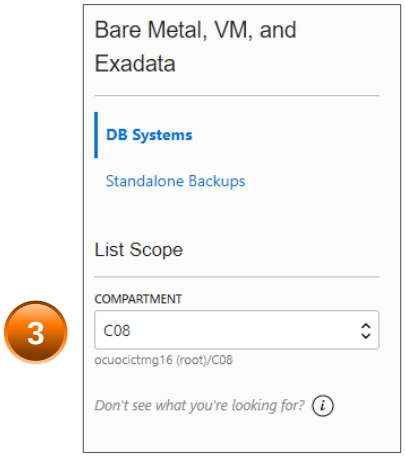


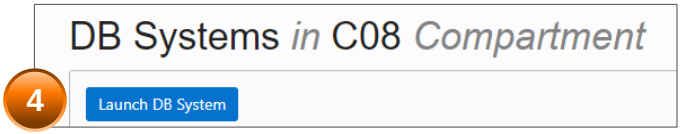
Oracle Cloud Infrastructure offers 1-node DB Systems on either bare metal or virtual machines, and 2-node RAC DB Systems on virtual machines.

You can manage these systems by using the Console, the API, the Oracle Cloud Infrastructure CLI, the Database CLI (DBCLI), Enterprise Manager, Enterprise Manager Express, or SQL Developer.

Using the Console to Launch a DB System

3. Select a Compartment.
4. Click Launch DB System.



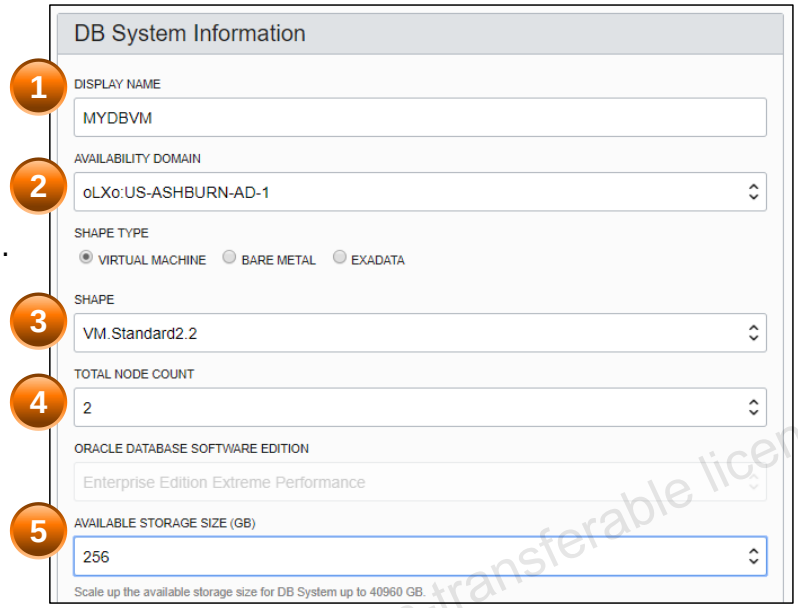


Select the compartment in which to create the Virtual Machine or Bare Metal instance from the Compartment section.

Click “Launch DB System” button.

Steps to Fill In DB System Information

1. Enter a Display Name.
2. Select an Availability Domain.
3. Select a Shape.
4. Select a Node Count.
5. Select an Available Storage Size.



Display Name: A friendly, display name for the DB System. The name doesn't need to be unique. An Oracle Cloud Identifier (OCID) will uniquely identify the DB System.

Availability Domain: The availability domain in which the DB System resides.

Shape Type: The type of shape to use to launch the DB System. The shape type filters the list of available shapes to select from.

Available types are:

- Virtual Machine (VM)
- Bare Metal (BM)
- Exadata

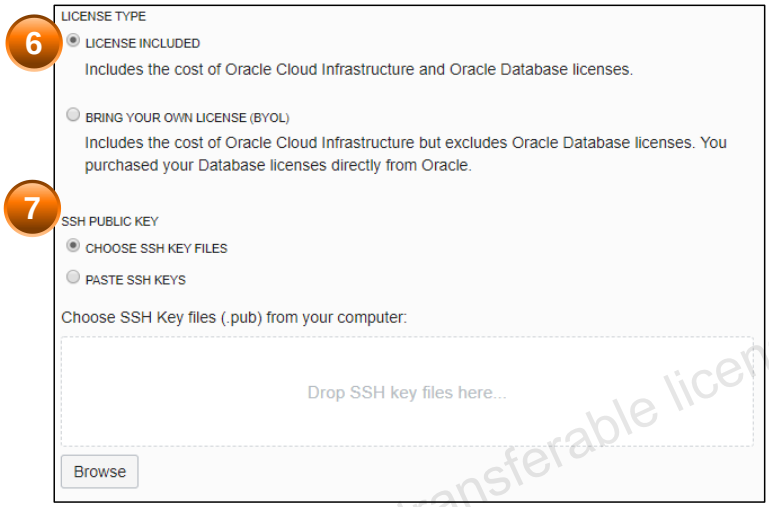
Shape: The shape to use to launch the DB System. The shape determines the type of DB System and the resources allocated to the system.

Total Node Count: Select 2 to provision a 2 Node RAC Virtual Machine DB System on OCI

Oracle Database Software Edition: This will be set to “Enterprise Edition Extreme Performance’ by default when total node count is set to 2.

Steps to Fill In DB System Information

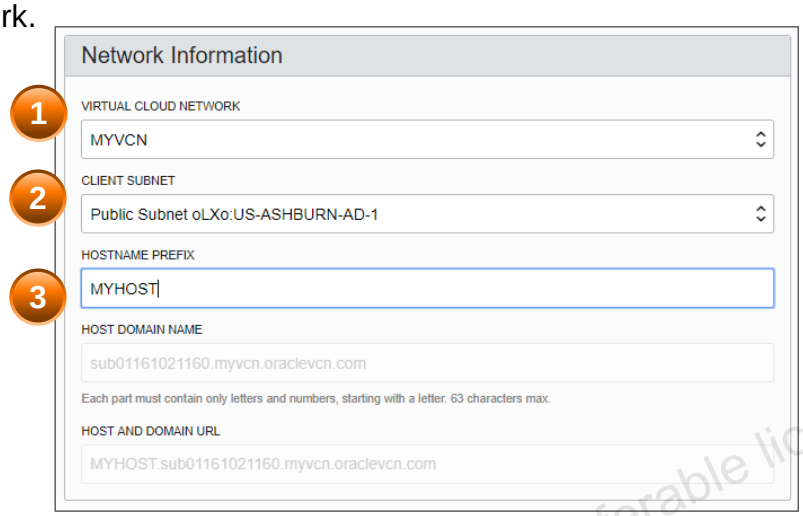
6. Select a type of license.
7. Provide a public key for SSH access.



- **License Type:** The type of license you want to use for the DB System. Your choice affects metering for billing.
  - **License included** means the cost of the cloud service includes a license for the Database service.
  - **Bring Your Own License (BYOL)** means you are an Oracle Database customer with an Unlimited License Agreement or Non-Unlimited License Agreement and want to use your license with Oracle Cloud Infrastructure. This removes the need for separate on-premises licenses and cloud licenses.
- **SSH Public Key:** The public key portion of the key pair you want to use for SSH access to the DB System. To provide multiple keys, paste each key on a new line. Make sure each key is on a single, continuous line. The length of the combined keys cannot exceed 10,000 characters.

Steps to Fill in Network Information

1. Select a Virtual Cloud Network.
2. Select a Client Subnet.
3. Enter a Hostname Prefix.



On Launch DB System in the **Network Information** section, complete these fields:

VIRTUAL CLOUD NETWORK

Use the pulldown to select the VCN in which to launch the DB System.

CLIENT SUBNET

Use the pulldown to select the subnet to which the DB System should attach.

HOSTNAME PREFIX

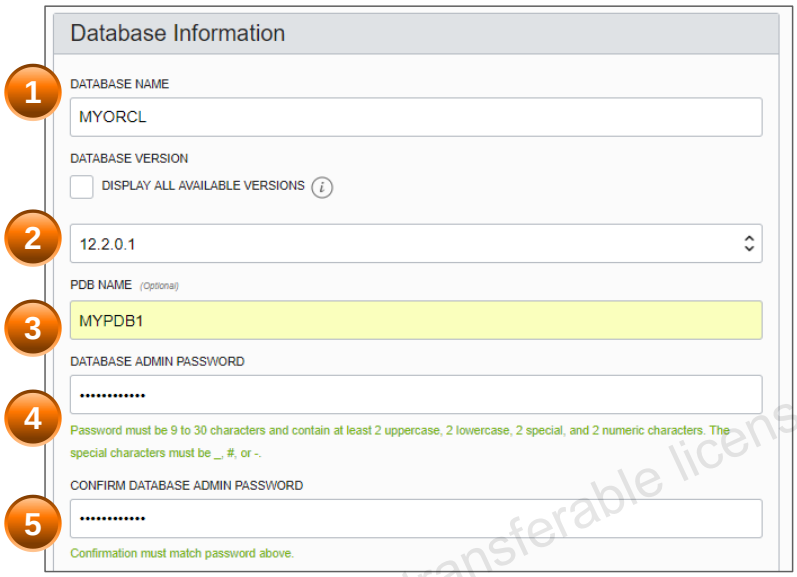
The domain name for the DB System. If the selected subnet uses the Oracle-provided Internet and VCN Resolver for DNS name resolution, this field displays the domain name for the subnet and it can't be changed. Otherwise, you can provide your choice of a domain name. For example, **testdnsvcn**.

HOST DOMAIN NAME

The domain name for the DB System. This value is displayed as the **DNS Domain Name** on the Subnet for the selected Availability Domain Name. For example, a valid value might be: **sub06220506332.jde_vcn.oraclevcn.com**

Steps to Fill in Database Information

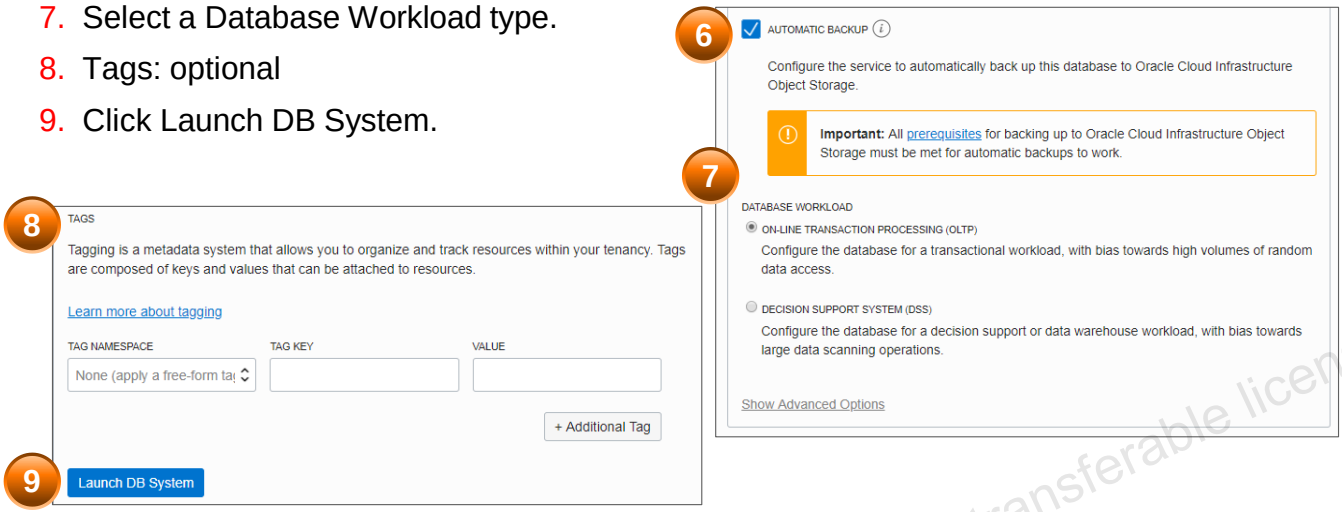
1. Enter a Database Name.
2. Select a Database Version.
3. Enter a PDB Name.
4. Provide a Database Admin Password.
5. Confirm the Database Admin Password.



- **Database Name:** The name for the database. The database name must begin with an alphabetic character and can contain a maximum of eight alphanumeric characters. Special characters are not permitted.
- **Database Version:** The version of the initial database created on the DB System when it is launched. After the DB System is active, you can create additional databases on it. You can mix database versions on the DB System, but not editions.
- **PDB Name:** *Not applicable to version 11.2.0.4.* The name of the pluggable database. The PDB name must begin with an alphabetic character, and can contain a maximum of 8 alphanumeric characters. The only special character permitted is the underscore (_).
- **Database Admin Password:** A strong password for SYS, SYSTEM, TDE wallet, and PDB Admin. The password must be 9 to 30 characters and contain at least 2 uppercase, 2 lowercase, 2 numeric, and 2 special characters. The special characters must be _, #, or -. The password must not contain the username (SYS, SYSTEM, and so on) or the word "oracle" either in forward or reversed order and regardless of casing.
- **Confirm Database Admin Password:** Re-enter the Database Admin Password you specified.

Steps to Fill in Database Information

6. Enable Automatic Incremental Backup (optional).
7. Select a Database Workload type.
8. Tags: optional
9. Click Launch DB System.

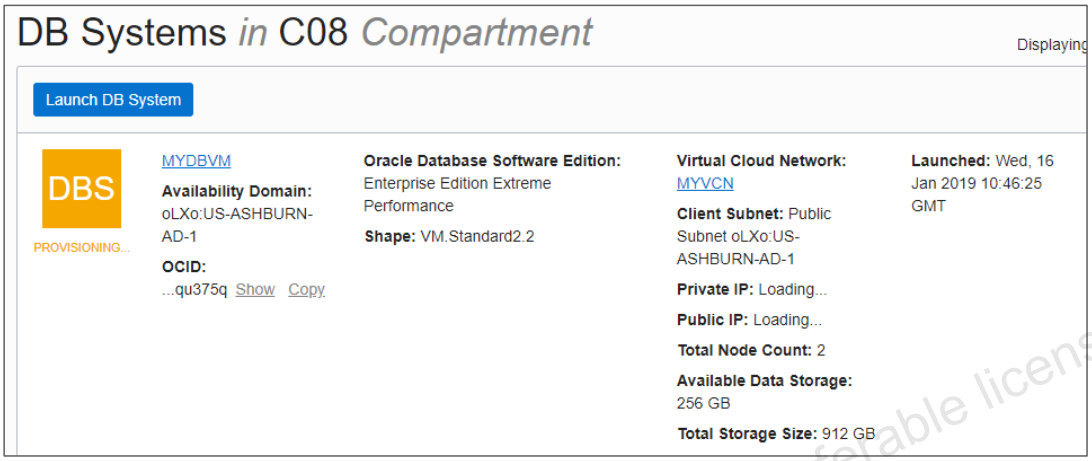


- **Automatic Backup:** Check the check box to enable automatic incremental backups for this database.
- **Database Workload:** Select the workload type that best suits your application.
  - **Online Transactional Processing (OLTP)** configures the database for a transactional workload, with a bias towards high volumes of random data access.
  - **Decision Support System (DSS)** configures the database for a decision support or data warehouse workload, with a bias towards large data scanning operations.
- **Character Set:** The character set for the database. The default is AL32UTF8.
- **National Character Set:** The national character set for the database. The default is AL16UTF16.
- **Tags:** Optionally, you can apply tags. If you have permissions to create a resource, you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags (https://docs.cloud.oracle.com/iaas/Content/General/Concepts/resourcetags.htm). If you are not sure if you should apply tags, skip this option (you can apply tags later) or ask your administrator.

Using the Console to Check the Status of a DB System

The different statuses of a DB System:

- Provisioning
- Available
- Starting
- Stopping
- Stopped
- Terminating
- Terminated
- Failed



Open the navigation menu. Under **Database**, click **Bare Metal**, **VM**, and **Exadata**.

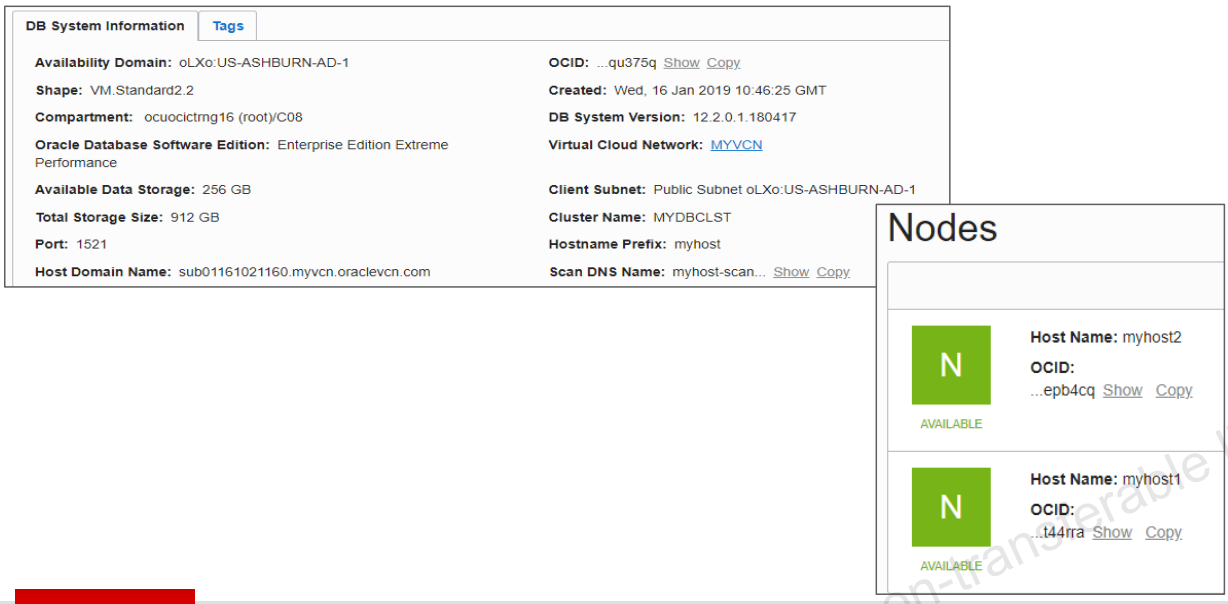
Choose your **Compartment**.

A list of DB Systems is displayed.

In the list of DB Systems, find the system you're interested in and check its icon. The color of the icon and the text below it indicates the status of the system.

- **Provisioning:** Yellow icon. Resources are being reserved for the DB system, the system is booting, and the initial database is being created. Provisioning can take several minutes. The system is not ready to use yet.
- **Available:** Green icon. The DB System was successfully provisioned. A few minutes after the system enters this state, you can SSH to it and begin using it.
- **Starting:** Yellow icon. The DB System is being powered on by the start or reboot action in the Console or API.
- **Stopping:** Yellow icon. The DB System is being powered off by the stop or reboot action in the Console or API.
- **Stopped:** Yellow icon. The DB System was powered off by the stop action in the Console or API.
- **Terminating:** Gray icon. The DB System is being deleted by the terminate action in the Console or API.
- **Terminated:** Gray icon. The DB System has been deleted and is no longer available.
- **Failed:** Red icon. An error condition prevented the provisioning or continued operation of the DB System.

2 Node RAC Virtual Machine DB System



Details of a 2 Node RAC Virtual Machine DB System

Setting Up DNS for a DB System

- DNS lets you use host names instead of IP addresses
- These are the choices for DNS name resolution for DB Systems:
  - Internet and VCN Resolver
  - DNS Server
- Oracle recommends using a VCN Resolver for DNS name resolution for the client subnet.

DNS lets you use host names instead of IP addresses to communicate with a DB System. You can use the *Internet and VCN Resolver* (the DNS capability built into the VCN).

Alternatively, you can use your choice of DNS server. You associate the host name and domain name to the public or private IP address of the DB System. You can find the host and domain names and IP addresses for the DB System in the Oracle Cloud Infrastructure Console on the **Database** page.

Special Considerations for Creating DB Systems

- Storage for the Virtual Machine DB System can be scaled up
- Storage for the Bare Metal DB System cannot be scaled up
- CPU cores for the Bare Metal DB can be scaled up
- CPU cores for the Virtual Machine DB System cannot be scaled up

- Storage for the Virtual Machine DB System can be scaled up but not for the Bare Metal DB System.
- CPU cores for the Bare Metal DB can be scaled up but not for a Virtual Machine DB. So during the creation, this should be taken into consideration.
- Some time during the creation of a Bare Metal DB System, due to limited resources for Bare Metal, we may get an error for service limits. This can be resolved by checking the service limits if we have administrator privileges or we can contact the administrator.

Summary

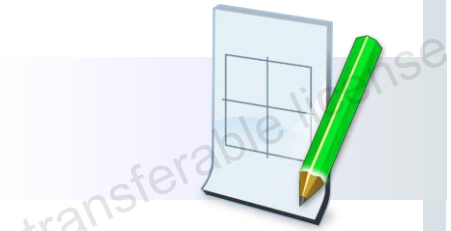
In this lesson, you should have learned how to:

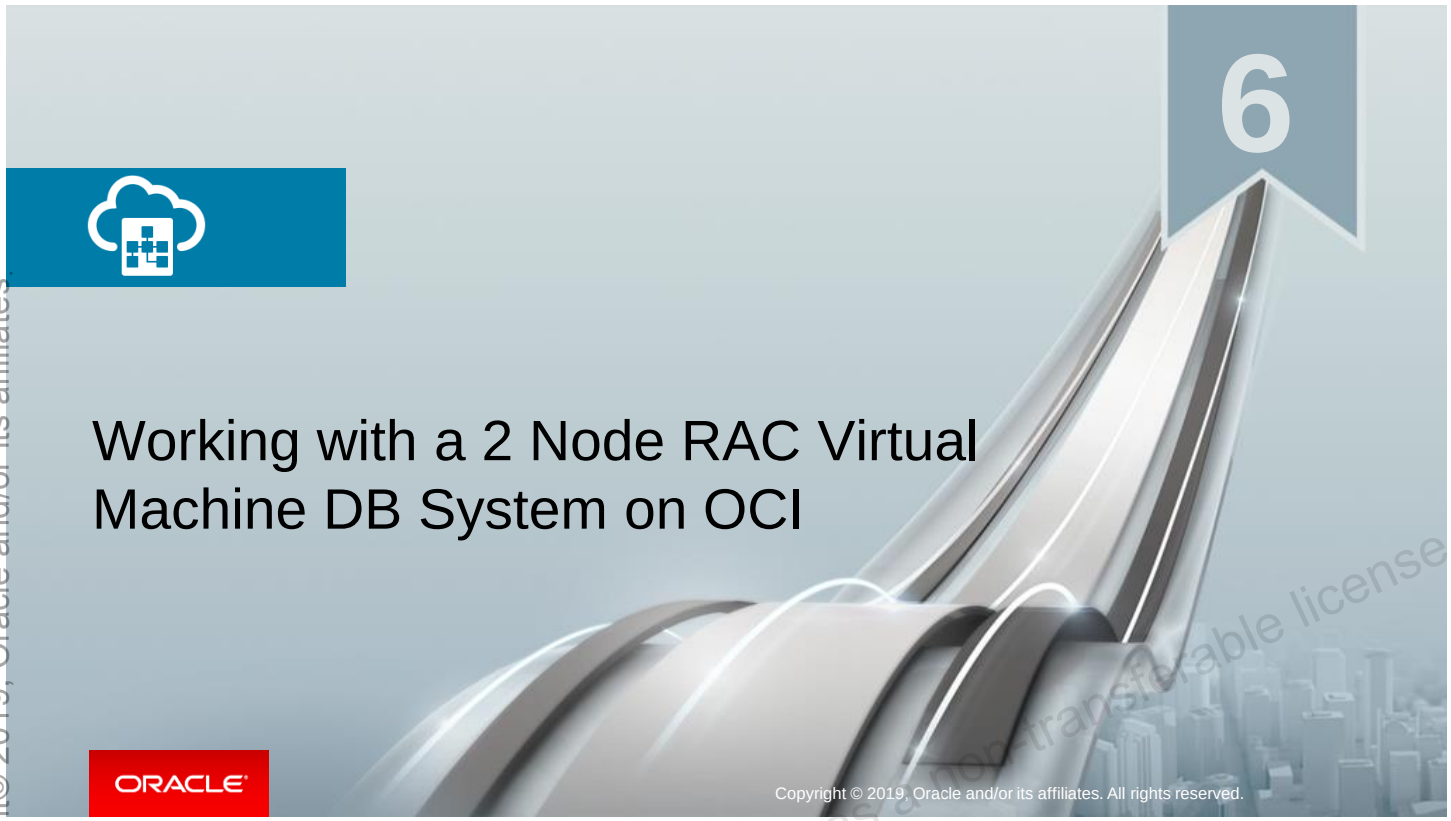
- Identify the prerequisites to launch a 2 Node RAC Virtual Machine DB System
- Create a Virtual Cloud Network (VCN) for a DB System
- Use the Console to launch a DB System
- Set up DNS for a DB System
- List the special considerations for creating DB Systems

Practice 5: Overview

This practice covers the following topics:

- Practice 5-1: Generating SSH Keys
- Practice 5-2: Creating a Virtual Cloud Network (VCN)
- Practice 5-3: Creating a 2 Node RAC Virtual Machine DB System





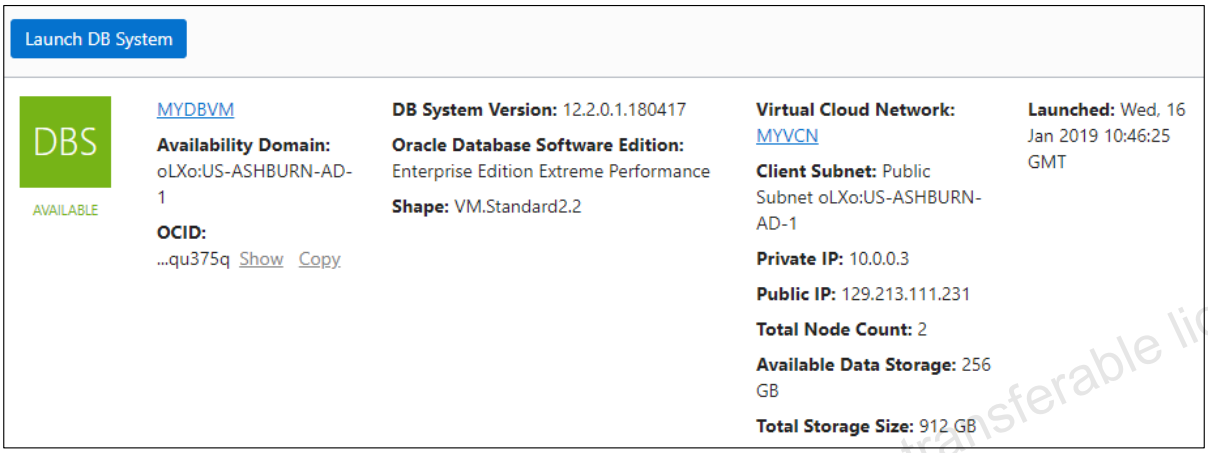
Objectives

After completing this lesson, you should be able to:

- Connect to a database on a multi-node DB System
- Set environment variables
- Connect to a RAC DB System with SSH
- Connect to a RAC database with Oracle SQL Developer
- Troubleshoot connection issues

Connecting to a Database on a Multi-Node DB System

- You can find the IP addresses in the console on the **Database** details page.



After you've created an SSH tunnel or opened port 1521, you can connect to a multi-node DB System using SCAN IP addresses or public IP addresses, depending on how your network is set up and where you are connecting from. You can find the IP addresses in the console on the **Database** details page.

Connecting Using SCAN IP Addresses

- On-Premises client
- FastConnect or VPN connection

```
testdb=
  (DESCRIPTION =
    (ADDRESS_LIST=
      (ADDRESS = (PROTOCOL = TCP)(HOST = <scanIP1>)(PORT = 1521))
      (ADDRESS = (PROTOCOL = TCP)(HOST = <scanIP2>)(PORT = 1521)))
    (CONNECT_DATA =
      (SERVER = DEDICATED)
      (SERVICE_NAME = <dbservice.subnetname.dbvcn.oraclevcn.com>)
    )
  )
```


You can connect to the database using the SCAN IP addresses if your client is on-premises and you are connecting using a FastConnect or VPN connection. You have the options shown on the slide.

Use the SCAN IP addresses, as shown in the tnsnames.ora example on this slide.

Connecting Using SCAN IP Addresses

- Define an external SCAN name in your on-premises DNS server.

```
testdb =
         (DESCRIPTION =
           (ADDRESS = (PROTOCOL = TCP)(HOST = <extscanname.example.com>)(PORT = 1521))
              (CONNECT_DATA =
              (SERVER = DEDICATED)
              (SERVICE_NAME = <dbservice.subnetname.dbvcn.oraclevcn.com>)
          )
        )
```


Define an external SCAN name in your on-premises DNS server. Your application can resolve this external SCAN name to the DB System's private SCAN IP addresses, and then the application can use a connection string that includes the external SCAN name. In the following tnsnames.ora example, extscanname.example.com is defined in the on-premises DNS server.

Connecting Using Public IP Addresses

- When to use node's public IP address?
- When the client uses the public IP address:
  - Client bypasses the SCAN listener
  - It cannot take advantage of the VIP failover feature

Remember:

- When the client uses the public IP address, the client bypasses the SCAN listener and reaches the node listener, so server side load balancing is not available.
- When the client uses the public IP address, it cannot take advantage of the VIP failover feature. If a node becomes unavailable, new connection attempts to the node will hang until a TCP/IP timeout occurs. You can set client side sqlnet parameters to limit the TCP/IP timeout.

Creating a TNS Entry for PDBs

- The `tnsnames.ora` file is located in `$ORACLEHOME/network/admin` on the DB System.
- By default, only the CDB will have the `tnsnames.ora` entry.
- Review the `tnsnames.ora` entries and add additional entries for PDBs, if necessary.
- The following `tnsnames.ora` example shows a connection string that includes the `CONNECT_TIMEOUT` parameter to avoid TCP/IP timeouts:

```
PDB_TEST=
  (DESCRIPTION =
    (CONNECT_TIMEOUT=60)
    (ADDRESS_LIST=
      (ADDRESS = (PROTOCOL = TCP)(HOST = <publicIP1>)(PORT = 1521))
      (ADDRESS = (PROTOCOL = TCP)(HOST = <publicIP2>)(PORT = 1521))
    )
    (CONNECT_DATA =
      (SERVER = DEDICATED)
      (SERVICE_NAME = <PDB_TEST.subnetname.dbvcn.oraclevcn.com>)
    )
  )
```


You can use the node's public IP address to connect to the database if the client and database are in different VCNs, or if the database is on a VCN that has an internet gateway. When the client uses the public IP address, the client bypasses the SCAN listener and reaches the node listener, so server side load balancing is not available. When the client uses the public IP address, it cannot take advantage of the VIP failover feature. If a node becomes unavailable, new connection attempts to the node will hang until a TCP/IP timeout occurs. You can set client side sqlnet parameters to limit the TCP/IP timeout.

To add additional entries for PDBs you just need to copy the existing entry for the CDB and replace the name of the CDB with the name of the PDB. Remember to replace the service name in the entry as well.

Setting Environment Variables

Set the following environment variables for a session before connecting to the database:

- **ORACLE_HOME**=<path of Oracle Home where the database is to be restored>
- **ORACLE_SID**=<database instance name>
- **ORACLE_UNQNAME**=<db_unique_name in lowercase>

The **oraenv** or **coraenv** script is usually called from the user's shell startup file (for example, .profile or .login) can be called using the command **. oraenv**. It sets the **ORACLE_SID** and **ORACLE_HOME** environment variables and includes the **$ORACLE_HOME/bin** directory in the **PATH** environment variable setting.

You can use **oraenv** to set the first two environment variable listed on this slide.

Prerequisites for SSH Access to the 2 Node RAC DB System

For SSH access to the DB System, you need:

- Virtual Cloud Network (VCN)
- Private and public key of the DB System
- Public or private IP address of the DB System

You need the following for SSH access to the DB System:

- Details of the Virtual Cloud Network (VCN) that is used to create the DB System.
- The full path to the file that contains the private key associated with the public key used when the DB System was launched.
- The public or private IP address of the DB System.
- Use the private IP address to connect to the DB System from your on-premises VPN, or from within the virtual cloud network (VCN). This includes connecting from a host located on-premises connecting through a VPN to your VCN, or from another host in the same VCN. Use the DB System's public IP address to connect to the system from outside the cloud (with no VPN). You can find the IP addresses in the Oracle Cloud Infrastructure Console on the **Database** page.

Connecting to a DB System with SSH

- To connect from a Linux system:

  $ ssh –i <private key> opc@<DB System IP address of Node>

- To connect from a Windows system:
  1. Open `putty.exe`.
  2. In the Category pane, select Session and enter the following fields:
     - Host Name (or IP address): *opc@<DB System IP address of Node>*
     - Connection Type: SSH
     - Port: 22
  3. In the Category pane, expand Connection, expand SSH, click Auth, and then browse to select your private key.
  4. Optionally, return to the Session category screen and save this session information for later.
  5. Click Open to start the session.

You can connect to a DB System by using a Secure Shell (SSH) connection. Most UNIX-style systems (including Linux, Solaris, BSD, and OS X) include an SSH client by default. For Windows, you can download a free SSH client called PuTTY from http://www.putty.org.

Connecting to a Database with Oracle SQL Developer

- From a Linux system, create a temporary SSH tunnel from your computer to the DB System.

```
$ ssh -i <private key> -L 1521:<DB System IP address>:1521 oracle@<DB System IP address>
```

- From a Windows system, create a temporary SSH tunnel from your computer to the DB System by using the PuTTY tunneling feature.
- For more durable access to the database, open port 1521 for the Oracle default listener by updating the security list used for the DB System.

You can connect to a DB System database with SQL Developer by using one of the following methods from Linux and Windows systems:

- Create a temporary SSH tunnel from your computer to the database. This method provides access only for the duration of the tunnel. (When you are done using the database, be sure to close the SSH tunnel by exiting the SSH session.)
- Open port 1521 for the Oracle default listener by updating the security list used for the DB System. This method provides more durable access to the database. For more information, see Updating the Security List for the DB System (https://docs.cloud.oracle.com/iaas/Content/Database/Tasks/monitoringDB.htm#Seclist).

Troubleshooting Connection Issues

The following issues might occur when connecting to a DB System or database.

- ORA-28365: Wallet is Not Open Error
- SSH Access Stops Working

The following issues might occur when connecting to a DB System or database.

ORA-28365: Wallet is Not Open Error

For a 1-node DB System or 2-node RAC DB System, regardless of how you connect to the DB System, *before* you use OS authentication to connect to a database (for example, sqlplus / as sysdba) be sure to set the ORACLE_UNQNAME variable. Otherwise, commands that require the TDE wallet will result in the error ORA-28365: wallet is not open.

Note that this is not an issue when using a TNS connection because ORACLE_UNQNAME is automatically set in the database CRS resource.

SSH Access Stops Working

If the DB System's root volume becomes full, you might lose the ability to SSH to the system (the SSH command will fail with permission denied errors). Before you copy a large amount of data to the root volume, for example, to migrate a database, use the dbcli create-dbstorage command to set up storage on the system's NVMe drives and then copy the database files to that storage. For more information, see Setting Up Storage on the DB System (https://docs.cloud.oracle.com/iaas/Content/Database/Tasks/mig-rman-duplicate-active-database.htm#Setting)

Summary

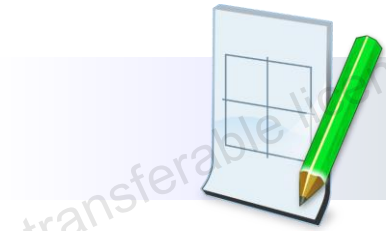
In this lesson, you should have learned how to:

- Connect to a database on a multi-node DB System
- Set environment variables
- Connect to a RAC DB System with SSH
- Connect to a RAC database with Oracle SQL Developer
- Troubleshoot connection issues

Practice 6: Overview

This practice covers the following topics:

- Practice 6-1: Connecting to a 2 Node RAC Virtual Machine DB System Using SSH
- Practice 6-2: Exploring High Availability Features
- Practice 6-3: Connecting to a RAC Database Using SQL Developer
- Practice 6-4: Configuring Transparent Application Failover on a 2 Node RAC

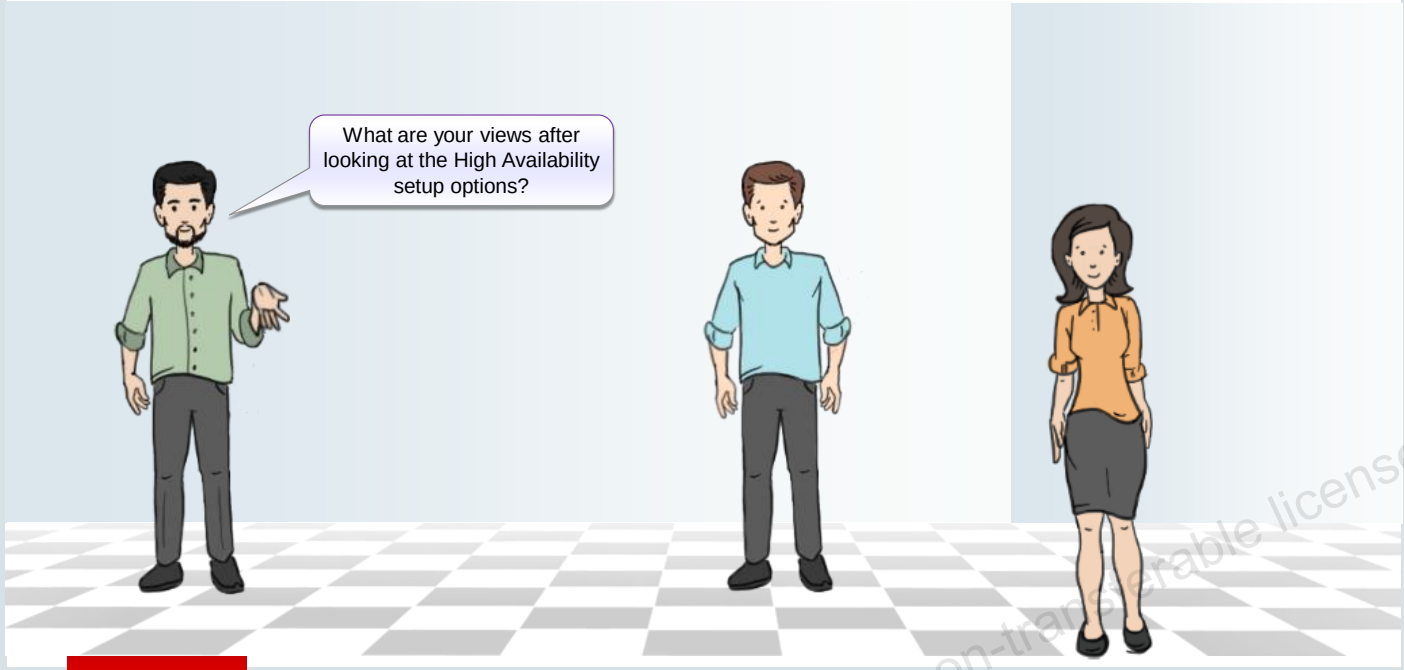


Objectives

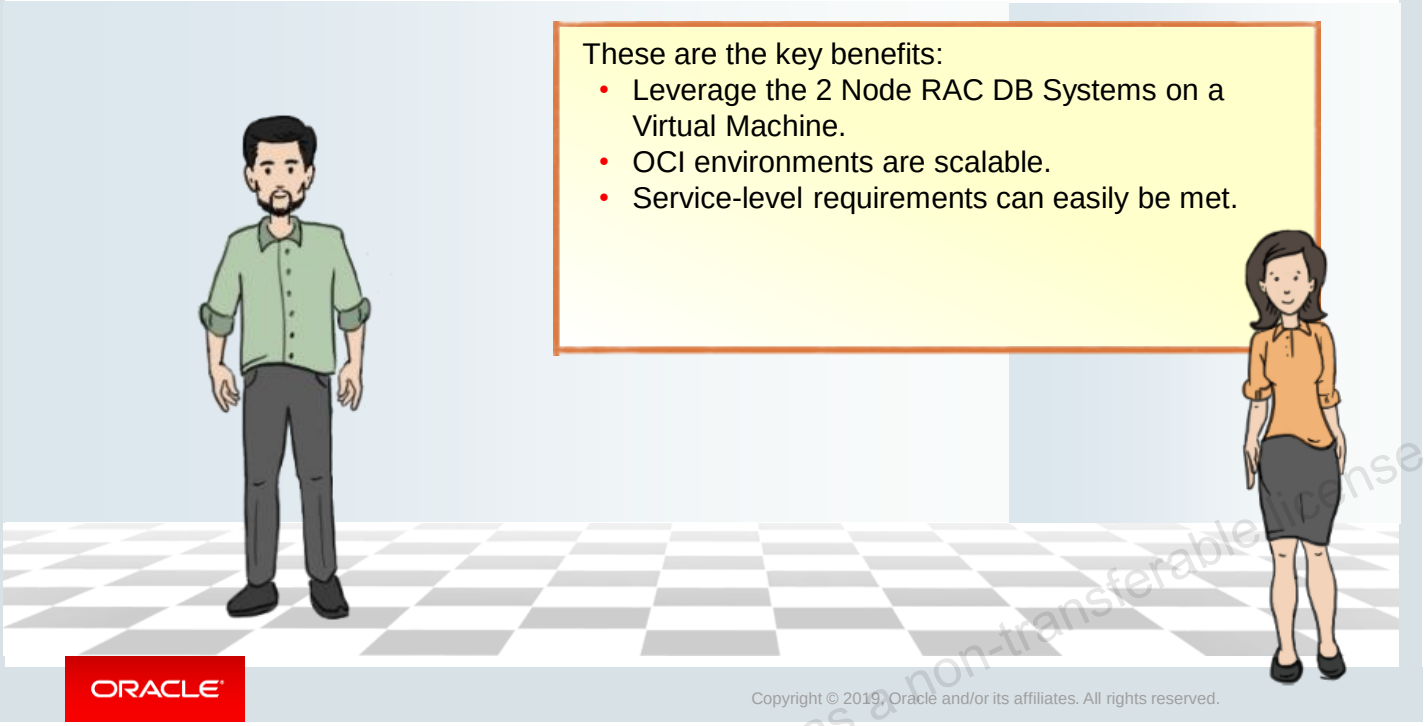
- Describe key benefits of implementing Database High Availability on OCI

After completing this lesson, you should be able to describe the key benefits of implementing Database High Availability on OCI.

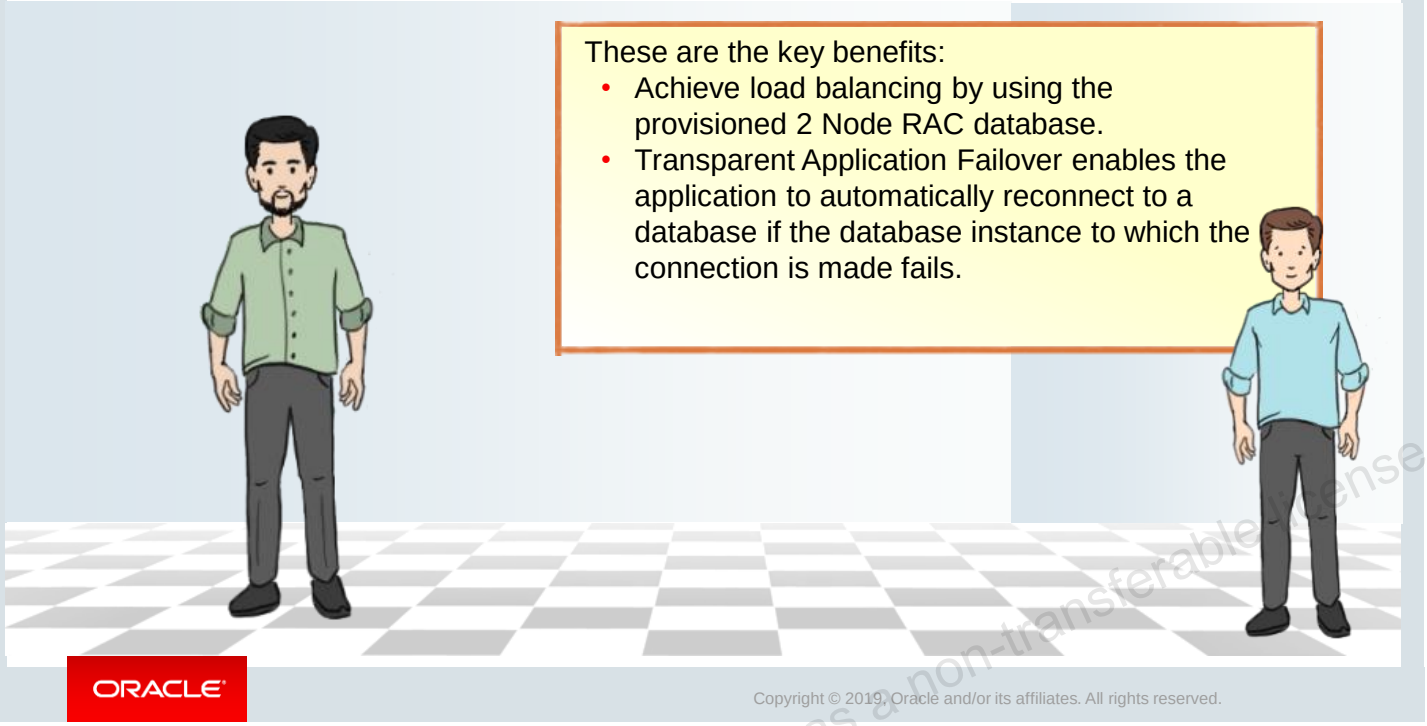
Database High Availability: Review



Database High Availability: Key Benefits

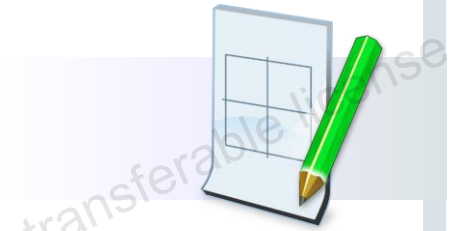


Database High Availability: Key Benefits



Practice 7: Overview

There are no practices for this lesson.



8

Introduction to Database Disaster Recovery on OCI

Objectives

After completing this lesson, you should be able to:

- Explain Disaster Recovery on Oracle Cloud Infrastructure
- Compare Disaster Recovery on-premises versus the cloud
- Identify where to use Oracle Cloud Disaster Recovery

Why You Need a Disaster Recovery Plan

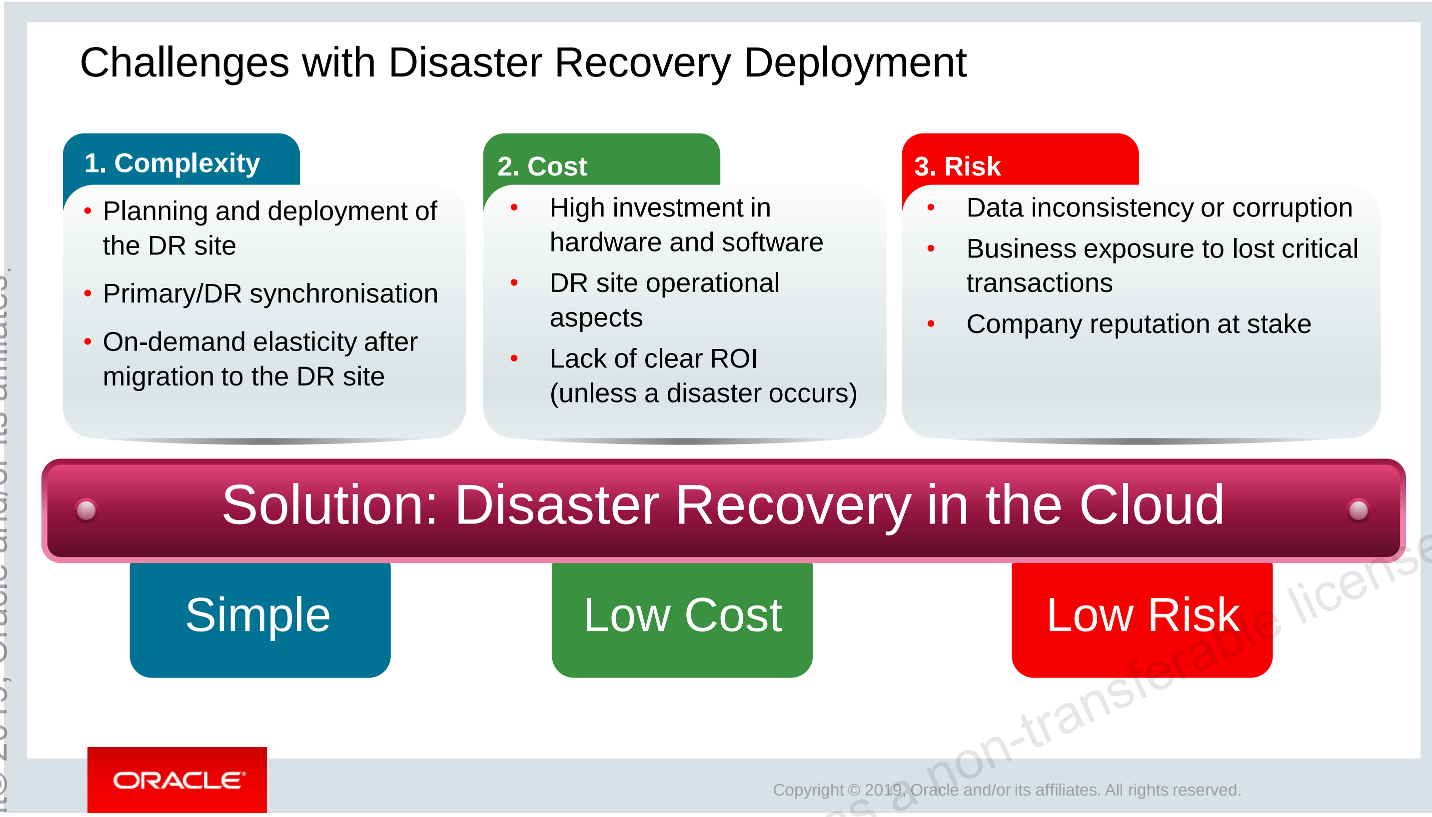
- Avoid a single point of failure
- Prevent data loss
- Reduce down time cost and revenue impact on planned and unplanned outages
- Manage disaster and data protection for compliance and regulatory purposes

ORACLE

Single points of failure in an I.T. environment can result in serious consequences business critical applications. They are analogous to walking a tight rope with no safety net, one mistake and you are out of business.

The purpose of a high availability architecture is to eliminate vulnerability to single points of failure so that applications and data remain available when an outage occurs, whether due to human error, software bugs, hardware faults, or even catastrophic events that can cause an entire data center to fail.

There are a number of challenges when implementing High Availability(HA). It can't be done in a vacuum – it needs to be cost effective, practical to manage, and provide high return on investment. It also needs to be comprehensive, addressing both unexpected outages and planned downtime to the extent required to meet service level expectations.



Although it is very true that every organisation would like to have 100% Disaster Recovery, there are a number of challenges that can prevent proper DR.

The first obstacle is complexity. Planning & Deployment of DR is not by any means a trivial task . It requires lots of time and effort.

A DR site needs to have a consistent copy of the production data and has to be able to guarantee enough CPU capacity and data storage after transitioning the business operations to the DR

The second obstacle is Cost. DR requires High investments in new Hardware, Software licenses and additional staff to operate the site. Not all customers can afford this and more often than not it is hard to justify the ROI(Return On Investments) unless a real disaster occurs.

Even if the DR infrastructure is in place, there is a substantial risk of not meeting the business SLAs after a disaster; specially if the Oracle MAA best practises haven't been implemented.

Customers can find themselves in the unfortunate situation where their mission critical applications cannot operate after a failover operation, for instance, due to data corruption .

Data corruption can happen if remote storage mirroring solutions are used to replicate database files instead of using Oracle Data Guard of Golden Gate.

The solution proposed in using Oracle Hybrid Cloud for Disaster Recovery, can mitigate these three challenges (complexity, cost and risk) and can help customers to deploy a Disaster Recovery infrastructure to meet their business SLAs.

Who Needs It? Disaster Recovery to the Cloud

Enterprises that do not have a DR site

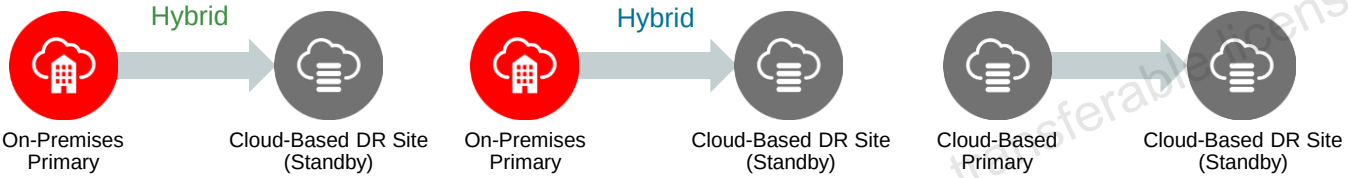
- Cannot afford CAPEX for deploying an on-premises DR site
- Want a low OPEX DR site with no active management
- Offsite copy for regulatory and compliance reasons
- Want a lower RTO/RPO

Enterprises that already have a DR site

- Want to reduce cost by migrating DR site to the cloud
- Want to have a sandbox environment in the cloud
- Want an additional offsite copy in the cloud
- Want on-demand commission and decommission of DR site

Enterprises who already have their production in the cloud or are planning to migrate to the cloud

- Low OPEX model
- All-in-the-cloud DR



RTO – Recovery Time Objective

RPO – Recovery Point Objective

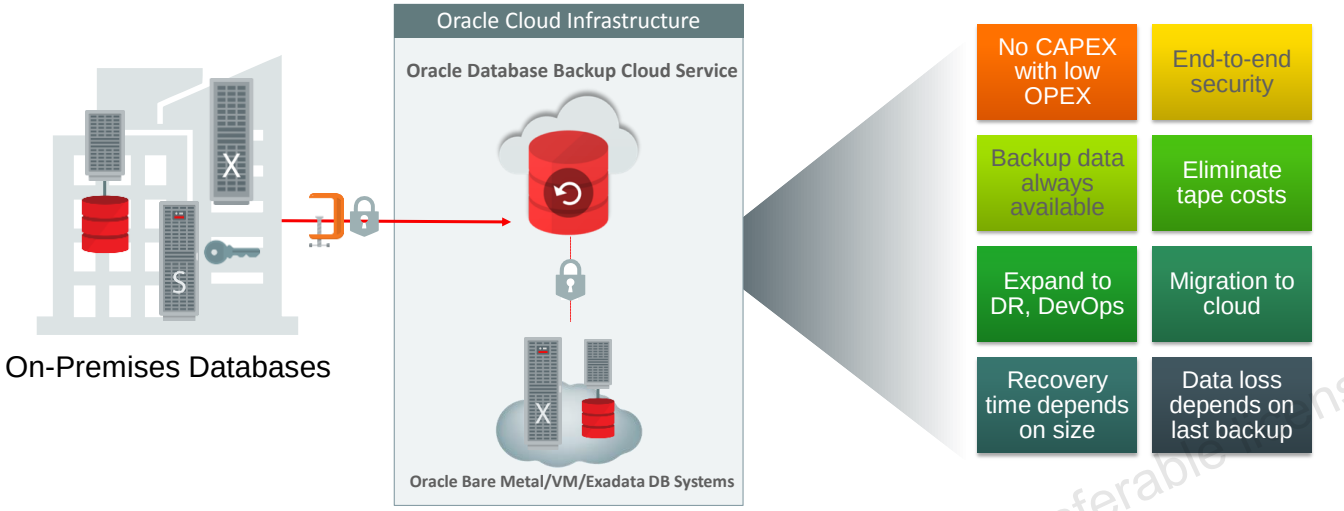
OPEX –Operating expense

DR-Disaster Recovery

Disaster Recovery to Oracle Cloud Infrastructure: Strategies

Using Backups	Using Data Guard	Using Active Data Guard
• RMAN backups to OCI • Restore to OCI • Use a cloud-based instance for Disaster Recovery	• Remote disaster recovery site in the cloud • Use cloud-based standby for temporary testing by converting to read/write • Offload regular backups from production, run them on standby • Use cloud-based standby for standby-first patching, rolling upgrades	• All Data Guard benefits • Use cloud-based standby for real-time read-only workloads • Repair on-premises primary corrupted blocks from standby • Offload fast backups to standby • Create multiple standby databases with real-time cascading (12c) • Application continuity (12c) • Advanced database rolling upgrade features (12c)

Hybrid: Disaster Recovery to Cloud Using Backups



This is termed as “COLD DR”

A public cloud solution for storing Oracle Database backups

Store database backups in Oracle Storage Cloud

Use familiar RMAN interface for backup and recovery operations

Oracle’s Database Backup Cloud Service provides a secure cost-effective solution for database backup and recovery, and enables companies to achieve lower costs, meet compliance requirements for data protection, and simplify the management of backups and restores

Cost effective, scalable cloud storage for database backups (10.2 and above)

End-to-end data encryption, compression and protection

- **Clients:** Data is always encrypted with keys kept locally at client, optionally compressed, and securely transmitted
- **Cloud:** Encrypted data is protected with 3-way mirroring on every write

Value Proposition

Fast Provisioning & Scalable

Offsite storage provisioned on-demand with on-demand capacity expansion capability

Low Cost

No capital expenditure, low operating expenses.

Secure and Reliable

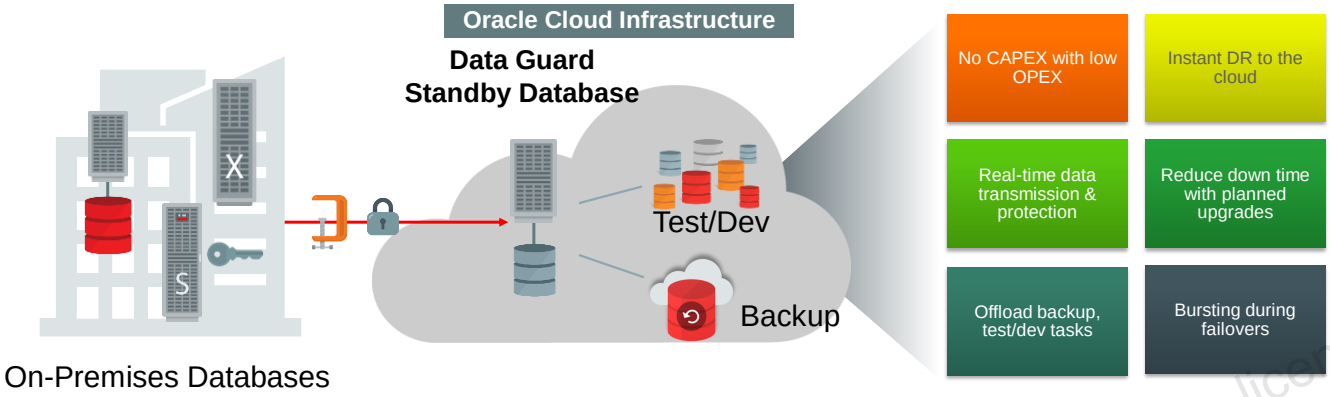
Data is secured with client-side encryption and transmitted securely to the cloud

24x7 Accessibility to Offsite Storage

Data accessible securely via internet from anywhere

Hybrid: Disaster Recovery to Cloud Using Standby

Data Guard Replication

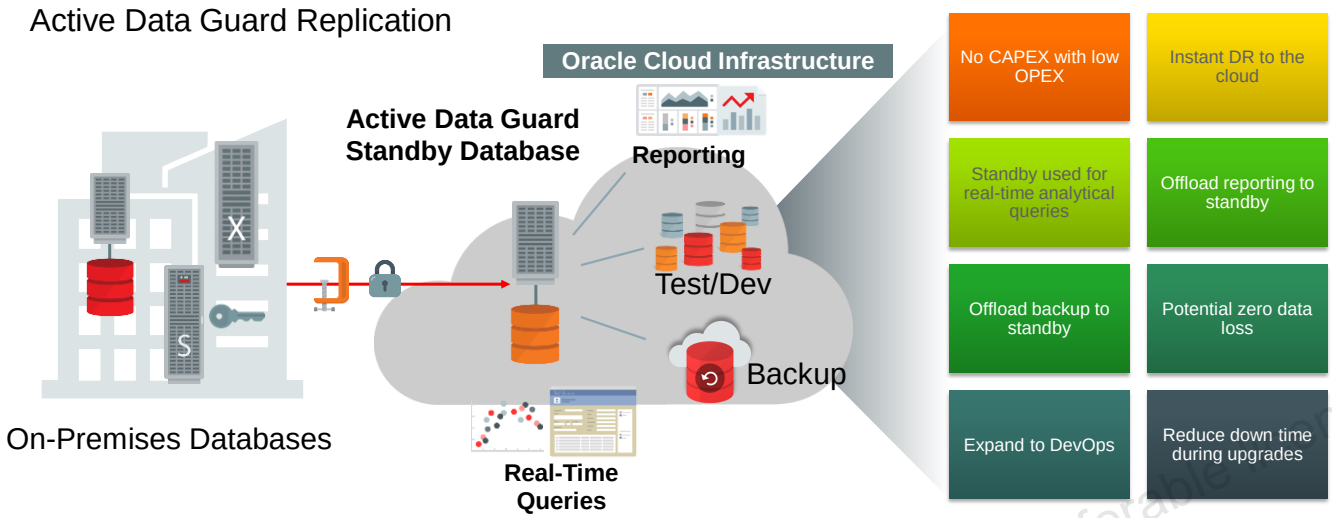


www.oracle.com/technetwork/database/availability/dr-to-oracle-cloud-2615770.pdf

This is termed as “WARM DR”

Supported for On-Premises Databases Oracle 11.2.0.4 and above.

Hybrid: Disaster Recovery to Cloud Using Active Standby



This is termed as “HOT DR”

Supported for On-Premises Databases Oracle 11.2.0.4 and above.

Benefits of Using Oracle Active Data Guard

Fully leverage the cloud standby database for better TCO and more

Benefit	Challenge Addressed	Product Feature
Cloud-based standby for read-only workloads (e.g. reporting)	Lower TCO by fully leveraging OCI	Active Data Guard
Repair on-premises databases automatically from Oracle Cloud	Risk avoidance	Automatic Block Repair
Offload fast backups to the Cloud	Lower TCO by fully leveraging OCI	Change Block Tracking
Use Cloud standby for planned maintenance	Minimize risk and complexity	Advanced Database Rolling Upgrade for Planned Maintenance (12c)
Zero data loss to the Cloud	Minimize risk	ADG Far Sync (12c)

ORACLE

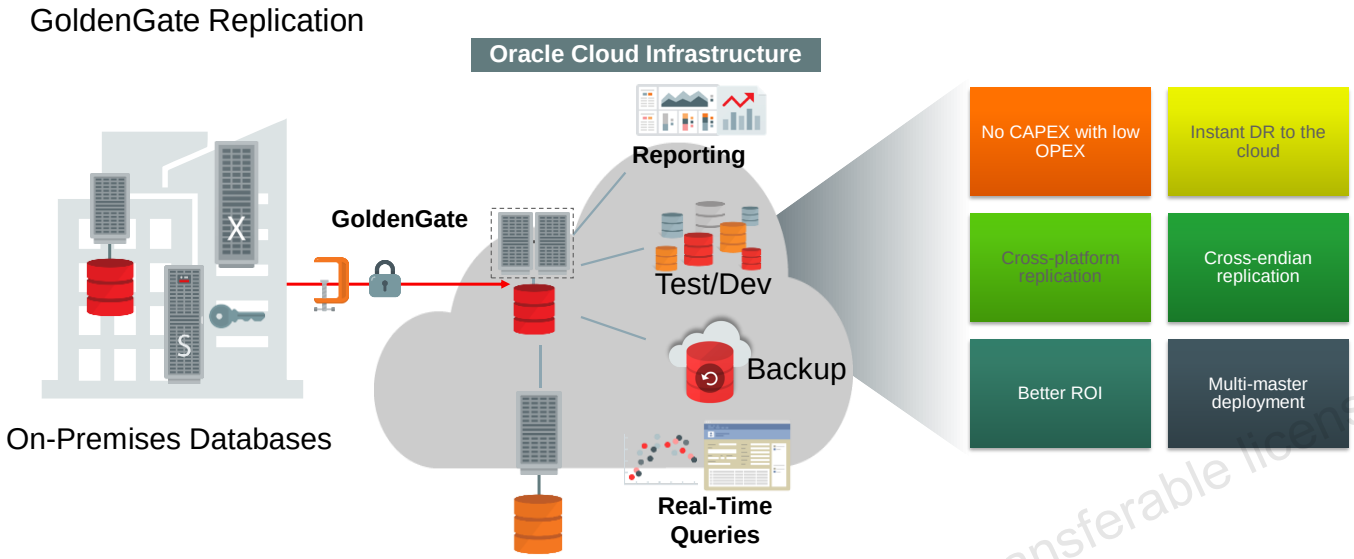
TCO – Total Cost of ownership.

Oracle Cloud Infrastructure (OCI)

The Benefits shown on this slide can be summarised:

1. Read only workloads, product feature is Active Data Guard(ADG)
2. Repair on premise databases (this refers to corrupted database blocks) using the automatic Block repair feature, part of ADG
3. Off load fast backups to the cloud, by enabling change block tracking on the standby.
   - Its termed as “fast backups” because RMAN reads the changed database blocks from the Change Block Tracking list as opposed to read all database files to find which blocks that have changed since the last incremental backup.
   - Change Block Tracking on the Standby requires Active Data Guard whereas Change Block Tracking on the primary is part of Enterprise Edition.
4. Cloud Standby for planned maintenance using advanced rolling upgrades in ADG 12*c*
5. Zero Data Loss(ZDL) to the cloud. This functionality differentiates ORACLE from competition . By using an intermediate ADG Far sync instance we can guarantee ZDL.

Hybrid: Disaster Recovery to Cloud with Read/Write in the Cloud



Golden gate can also be used as a mechanism to create a Disaster Recovery site on Oracle Cloud.

Supported for On-Premises Databases Oracle 11.2 and above.

Benefits of Using GoldenGate

Fully leverage a cloud standby database for better TCO and more

Benefit	Challenge Addressed
Cloud-based target for read-only workloads	Lower TCO by fully leveraging OCI
Cloud-based target for read-write (multi-master)	Load balancing
Offload backup operations to the Cloud	Lower TCO by fully leveraging OCI
Use Cloud Standby for planned maintenance/migration	Minimise risk and complexity
Logical replication with selected objects	Flexibility

Disaster Recovery to Cloud: Networking Considerations

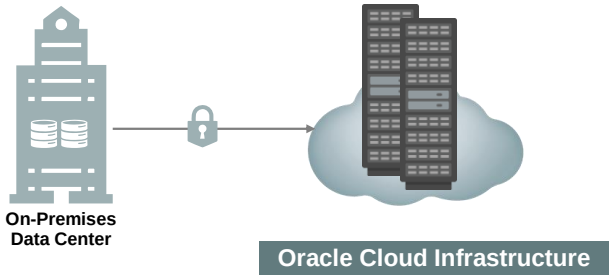
Hybrid Cloud Disaster Recovery

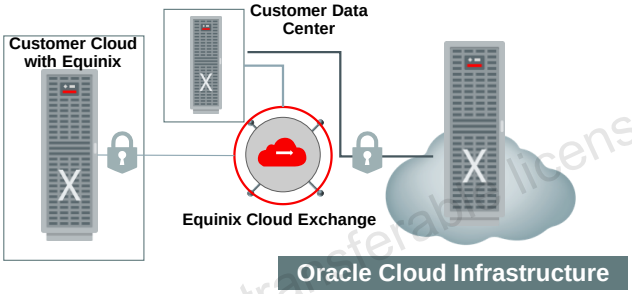
Option #1: Over Public Internet

- Unpredictable latency/low bandwidth
- Free of cost
- Suitable for low transactions

Option #2: Oracle FastConnect

- High bandwidth connectivity options
- Oracle FastConnect high bandwidth 1Gbps to 10Gbps capabilities
- Predictable latency/high bandwidth





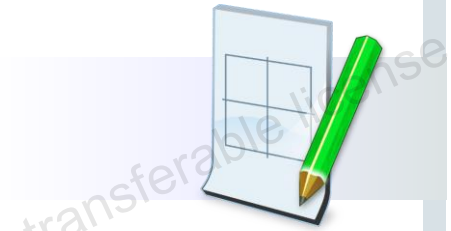
Summary

In this lesson, you should have learned how to:

- Explain Disaster Recovery on Oracle Cloud Infrastructure
- Compare Disaster Recovery on-premises versus the cloud
- Identify where to use Oracle Cloud Disaster Recovery

Practice 8: Overview

There are no practices for this lesson.

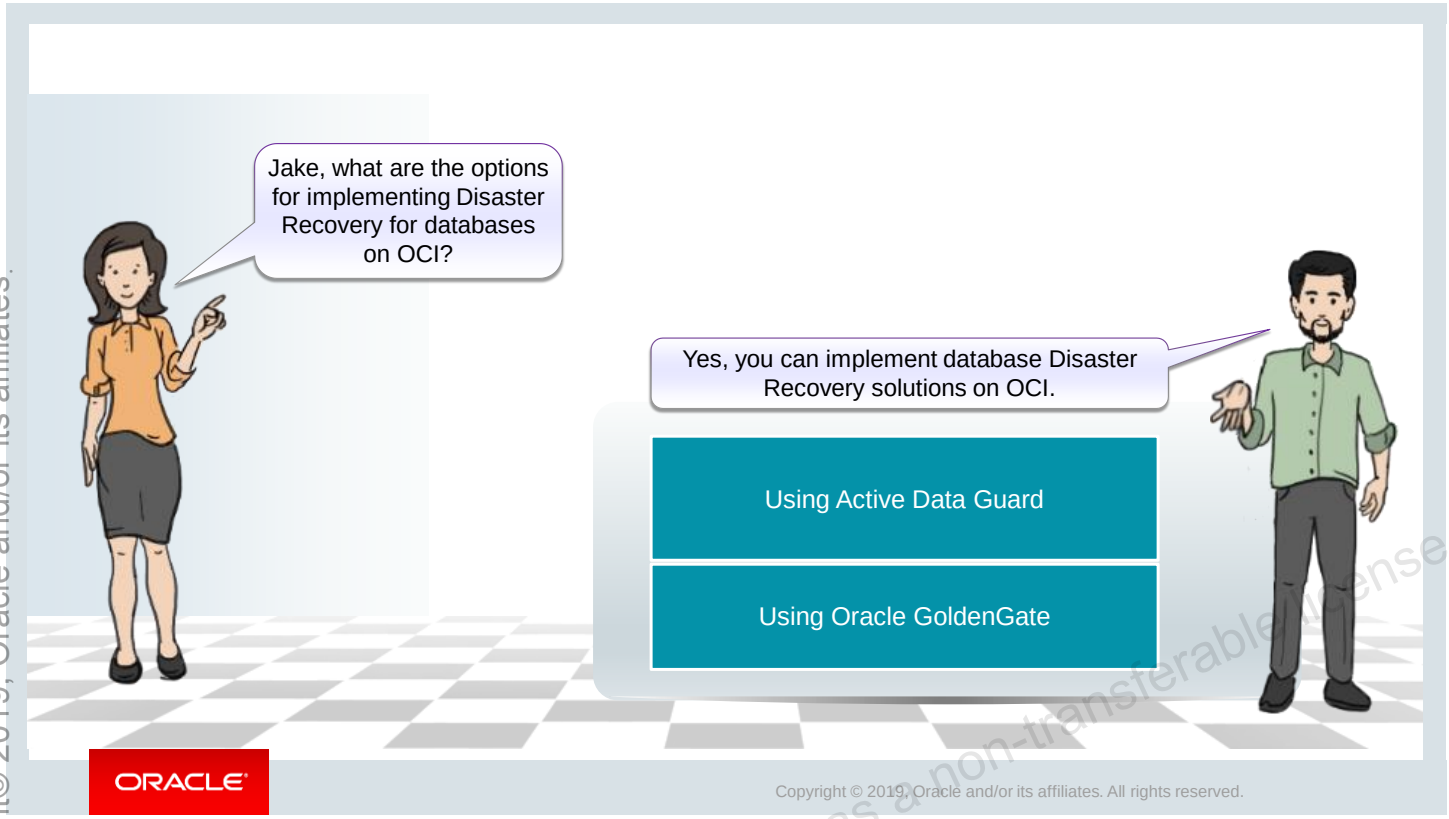


Database Disaster Recovery Solutions on OCI

Objectives

After completing this lesson, you should be able to:

- Explain the database strategies for Disaster Recovery: Active Data Guard and GoldenGate
- Identify the Oracle Cloud Infrastructure best practices for Data Guard configuration
- Identify the Oracle Cloud Infrastructure best practices for GoldenGate configuration
- Use both Active Data Guard and GoldenGate for DR on OCI



Database Strategies for Disaster Recovery

Two strategic capabilities in Oracle's software portfolio:

- Active Data Guard
- GoldenGate

Oracle Active Data Guard and Oracle GoldenGate are two strategic capabilities in Oracle's software portfolio.

- Active Data Guard provides data protection and availability for Oracle Database in a simple and economical manner by maintaining an exact physical replica of the production copy at a remote location that is open read-only while replication is active.
- GoldenGate is an advanced logical replication product that supports multi-master replication, hub and spoke deployment, and data transformation. GoldenGate provides customers flexible options to address the complete range of replication requirements, including heterogeneous hardware platforms.

Benefits of Using Oracle Active Data Guard on OCI

Benefit	Challenge Addressed
Secure physical replication	Data consistency is guaranteed
Simple, fast, one-way replication	Little administrative overhead
Oracle Data Guard Redo Apply supports all Oracle features	No restrictions
Isolates the standby database from I/O corruption	Best data protection
Zero data loss to the cloud	Minimal risk

Active Data Guard offers the following benefits:

- Secure physical replication. The standby database is open read-only so your data consistency is guaranteed.
- Simple, fast, one-way replication of a complete Oracle Database. The default configuration handles most workloads so there's little administrative overhead.
- No restrictions. Oracle Data Guard Redo Apply supports all Oracle features and transparently replicates all data and storage types, PL/SQL packages, and DDL without special considerations.
- Best data protection. Replication direct from memory isolates the standby database from I/O corruption that can occur at the primary database. Detects silent lost-write corruption that can occur independently on the primary or standby database. Automatically detects and repair physical block corruption that can occur independently on the primary or standby database.
- Choice of synchronous with zero data loss, or asynchronous with near-zero data loss protection.
- Simple to improve ROI by offloading read-only workloads or backups to a synchronized physical standby.
- Transparency of backups. An Oracle Data Guard primary database and standby database are physically exact copies of each other. RMAN backups are interchangeable.
- A single command converts a physical standby database as a test system open readwrite. A second command converts it back to a physical standby database and resynchronizes it with the primary database. Primary data is always protected.
- Integrated management of a complete configuration with Oracle Data Guard Broker command line or Oracle Enterprise Manager Cloud Control, integrated automatic database, and client failover.
- Supported for single-node database or multiple-node database (Real Application Cluster) configuration

Benefits of Using Oracle Active Data Guard on OCI

Benefit	Challenge Addressed
Synchronized physical standby	Improve ROI
RMAN backups are interchangeable	Transparency of backups
Supports Data Guard Broker command line & EM Cloud Control	Integrated management
Supports single-node & RAC database configuration	High Availability

- Offload read-only workloads or backups to a synchronized physical standby.
- An Oracle Data Guard primary database and standby database are exact physical copies of each other. RMAN backups are interchangeable.
- Complete configuration with Oracle Data Guard Broker command line or Oracle Enterprise Manager Cloud Control.
- Supports single-node database or multiple-node database (Real Application Cluster) configuration.

Data Guard Configuration Modes

Data Guard supports the following protection modes:

- Maximum Protection
- Maximum Availability
- Maximum Performance

Maximum Protection: This protection mode provides zero data loss if the primary database fails. To ensure that data loss can't occur, the primary database shuts down if a fault prevents it from writing its redo stream to the standby redo log of at least one standby database.

Maximum Availability: This protection mode provides the highest level of data protection that is possible without compromising the availability of the primary database. Like the Maximum Protection mode, a transaction doesn't commit until the redo needed to recover that transaction is written to the local online redo log and to the standby redo log of at least one transactionally consistent standby database. Unlike the Maximum Protection mode, the primary database doesn't shut down if a fault prevents it from writing its redo stream to a remote standby redo log. Instead, the primary database operates in maximum performance mode until the fault is corrected, and all gaps in redo log files are resolved. When all gaps are resolved, the primary database automatically resumes operating in Maximum Availability mode.

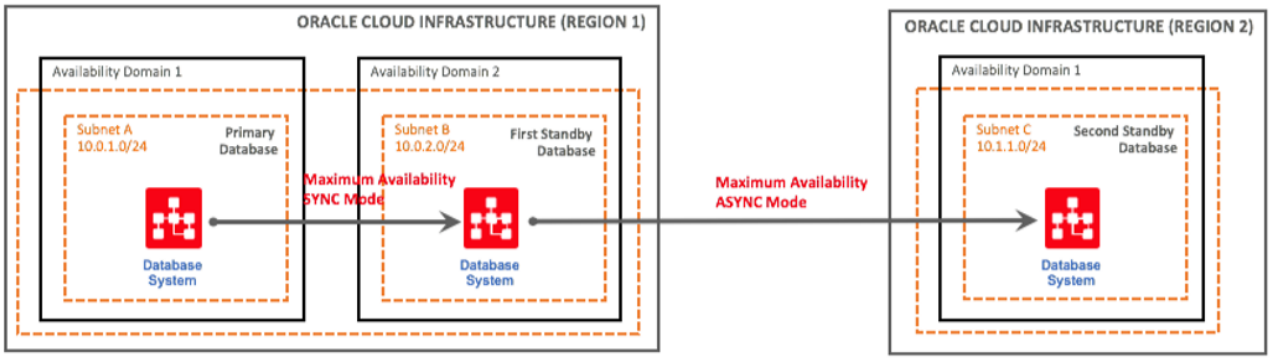
Maximum Performance: This protection mode (the default) provides the highest level of data protection that is possible without affecting the performance of the primary database. This is accomplished by allowing a transaction to commit when the redo data needed to recover that transaction is written asynchronously to the local online redo log. When network links with sufficient bandwidth are used, this mode provides a level of data protection that approaches that of Maximum Availability mode with minimal impact on primary database performance.

OCI Best Practices for Data Guard Configuration

- OCI supports all three Data Guard configurations
- Between two ADs within same region OCI recommends using Maximum Availability in SYNC mode
- Between two regions OCI recommends using Maximum Availability in ASYNC mode
- OCI recommends building this architecture in daisy-chain mode

- All three Data Guard configurations are fully supported on Oracle Cloud Infrastructure. However, because of a high risk of production outage, we don't recommend using the Maximum Protection mode for your Data Guard configuration.
- Oracle Cloud Infrastructure recommends using the Maximum Availability mode in SYNC mode between two availability domains (same region), and using the Maximum Availability mode in ASYNC mode between two regions. This architecture provides you the best RTO and RPO without causing any data loss.
- Oracle Cloud Infrastructure recommends building this architecture in daisy-chain mode, in which the primary database ships redo logs to the first standby database in another availability domain in SYNC mode, and then the first standby database ships the redo logs to another region in ASYNC mode. This method ensures that your primary database is not doing the double work of shipping redo logs, which can cause performance impact on a production workload.

Architecture for Data Guard on Oracle Cloud Infrastructure



This figure shows the recommended architecture for Data Guard on Oracle Cloud Infrastructure.

This configuration offers the following benefits:

- No data loss within a region.
- No overhead on the production database to maintain standbys in another region.
- Option to configure lagging on the DR site if needed for business reasons.
- Option to configure multiple standbys in different regions without any additional overhead on the production database. A typical use case is a CDN application. the recommended architecture for Data Guard on Oracle Cloud Infrastructure:

Oracle GoldenGate

- Real-time data integration and replication in heterogeneous IT environments
- Enables High Availability solutions

- Oracle GoldenGate is a comprehensive software package for real-time data integration and replication in heterogeneous IT environments.
- The product set enables high availability solutions, real-time data integration, transactional change data capture, data replication, transformations, and verification between operational and analytical enterprise systems.

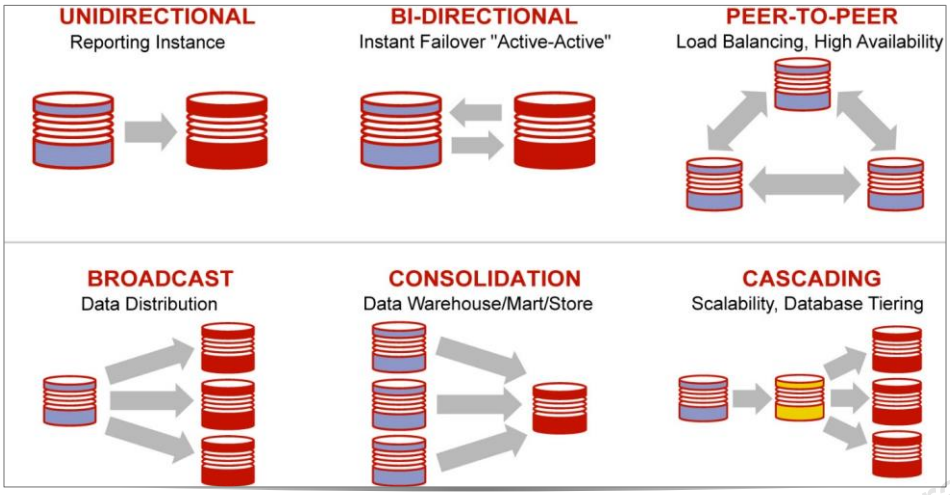
Benefits of Using Oracle GoldenGate on OCI

- It has advanced replication requirements
- Maintenance and migrations require zero down time
- Cross-platform migration is not supported by Data Guard
- The primary database and the live standby database can be on different operating systems or be of different types
- Replicate from a recent version of Oracle Database to an earlier version

Use Oracle GoldenGate when a replica database must be open read-write while replication is active, including in the following scenarios:

- Advanced replication requirements, such as multi-master and bidirectional replication, subset replication, many-to-one replication, cross-endian replication, and data transformations. • Maintenance and migrations that require zero downtime using bi-directional replication.
- Cross-platform migration that is not supported by Data Guard (for example, cross-endian platform migration).
- When the primary database and the live standby database are on different operating systems or are different types (for example, DB2/MySQL to Oracle and vice versa).
- When you replicate from a more recent version of Oracle Database to an earlier version of Oracle Database (for example, from Oracle Database 11*g* to Oracle Database 10*g*).

GoldenGate-Supported Topologies on OCI



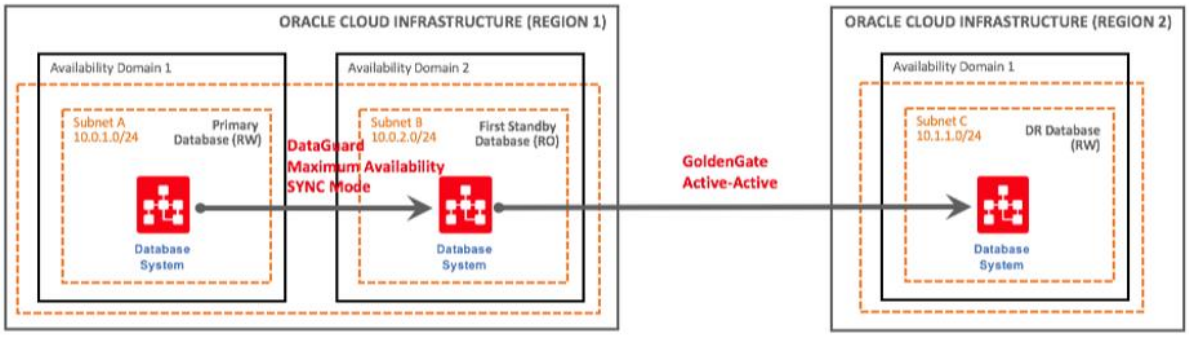
- **Unidirectional:** A unidirectional topology replicates data in one direction to a single target database.
- **Bi-Directional and Peer-to-Peer:** Bi-directional and peer-to-peer topologies replicate data among two or more peer databases to support high availability and load balancing.
- **Broadcast and Cascading:** Broadcast and cascading topologies support direct or phased data distribution from one source to many targets.
- **Consolidation:** A consolidation topology supports data centralization in a central database from many remote databases, such as to maintain a data warehouse.

OCI Best Practices for GoldenGate Configuration

- Replicates data on the transactional level
- Enables zero-data-loss solution with strong data consistency when used with Data Guard

- GoldenGate replicates data on the transactional level. Oracle Cloud Infrastructure recommends implementing Conflict Detection and Resolution (CDR) for data consistency between two sites.
- If you are using GoldenGate primarily for DR purposes and replication is only one way, we recommend adding Data Guard between two regions to provide a zero-data-loss solution with strong data consistency between the primary and Data Guard instance.

Architecture for GoldenGate on Oracle Cloud Infrastructure



Using Both Active Data Guard and GoldenGate on OCI

When can you use Active Data Guard and GoldenGate together?

Active Data Guard and GoldenGate are not mutually exclusive. You can use the solutions together in the following scenarios:

- Use an Active Data Guard standby for disaster protection and database rolling upgrades for a mission-critical OLTP database.
- Use GoldenGate to extract data from the Data Guard primary database (or from the standby database using GoldenGate ALO mode) for ETL update of an enterprise data warehouse.

Using Both Active Data Guard and GoldenGate on OCI

- Supports mission-critical application systems
- Provides optimal data protection and availability
- Enables zero-data-loss failover

ORACLE

- Use GoldenGate subset replication to extract, transform, and aggregate data from numerous data sources into a central operational data store (ODS). The ODS supports mission-critical application systems that generate significant revenue for the company. Use an Active Data Guard standby database to protect the ODS, providing optimal data protection and availability.

- Use GoldenGate multi-master replication to synchronize several databases, each located in different geographies. Each GoldenGate copy has its own local synchronous Data Guard standby database that enables zero-data-loss failover should an outage occur.

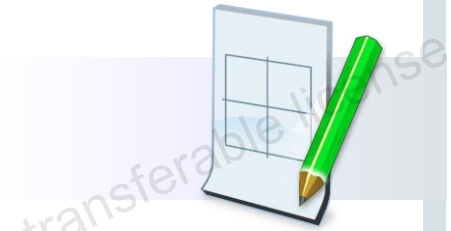
Summary

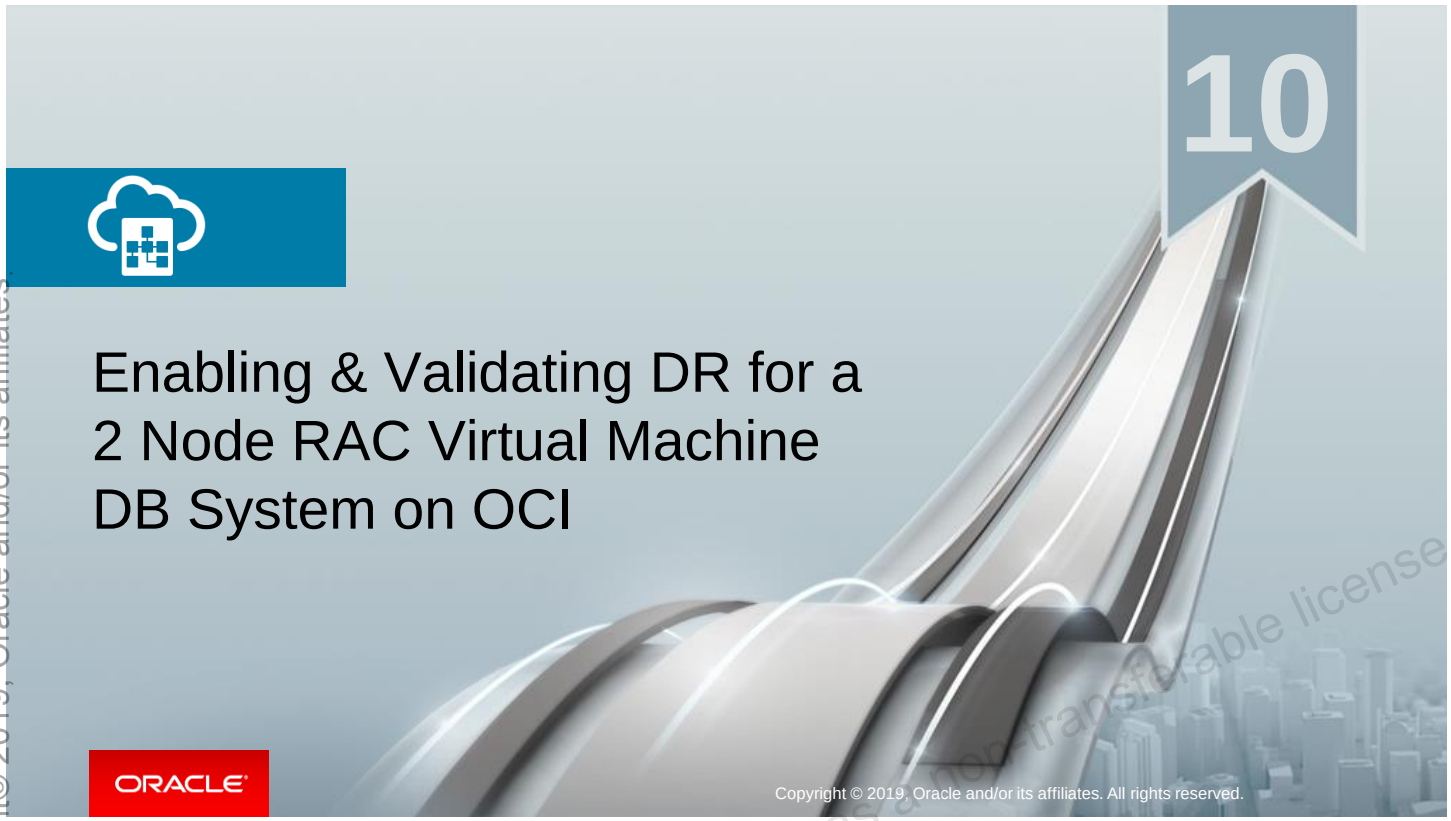
In this lesson, you should have learned how to:

- Explain the database strategies for Disaster Recovery: Active Data Guard and GoldenGate
- Identify the Oracle Cloud Infrastructure best practices for Data Guard configuration
- Identify the Oracle Cloud Infrastructure best practices for GoldenGate configuration
- Use both Active Data Guard and GoldenGate for DR on OCI

Practice 9: Overview

There are no practices for this lesson.

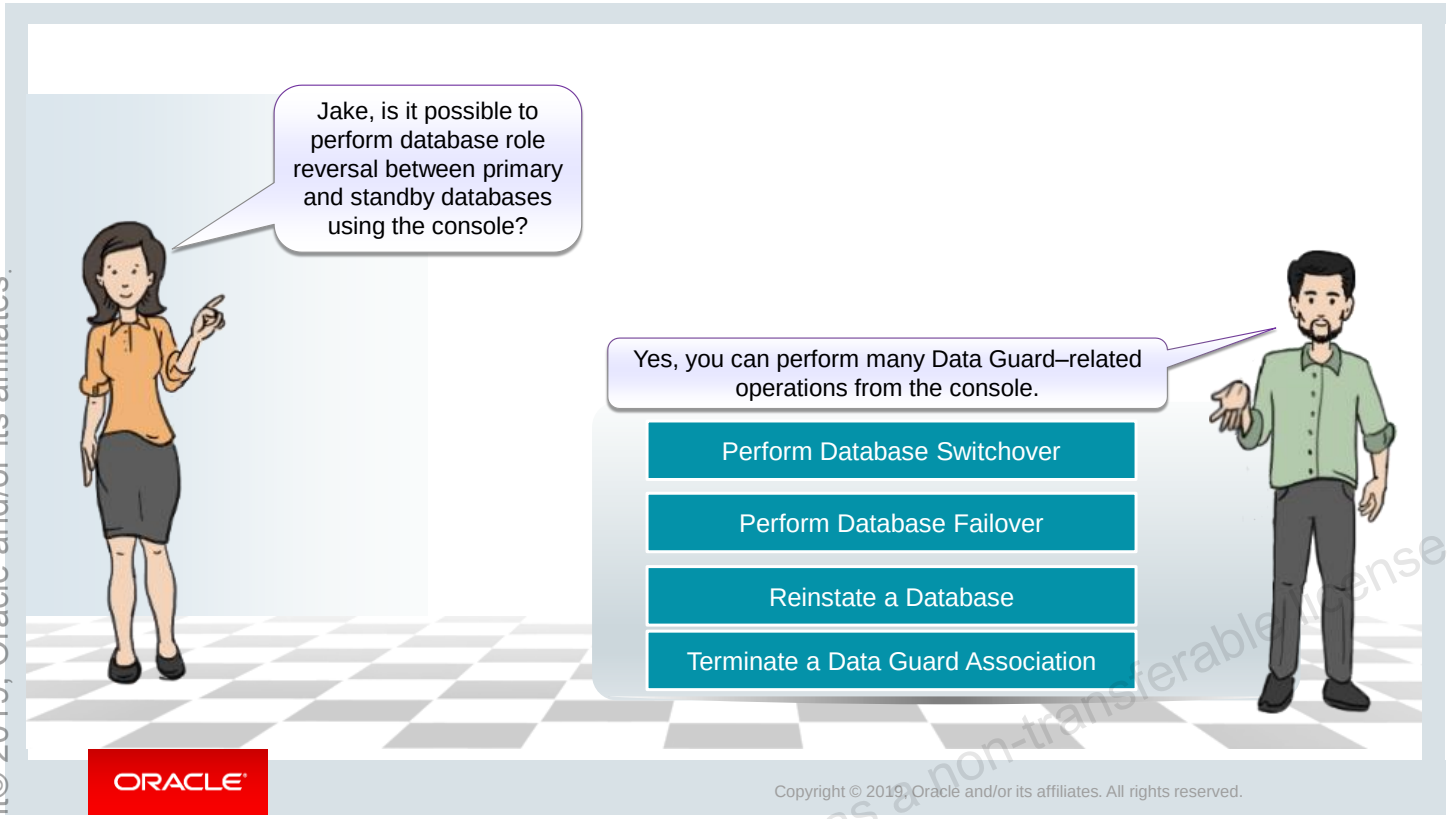




Objectives

After completing this lesson, you should be able to:

- Use Oracle Data Guard on OCI
- Configure security lists for primary and standby DB Systems
- Work with Oracle Data Guard on OCI
- Enable Data Guard on a Bare Metal DB System
- Enable Data Guard on a Virtual Machine DB System



Using Oracle Data Guard on OCI: Prerequisites

- Limited to one standby database per primary database
- Requires two DB Systems

A Data Guard configuration on the Oracle Cloud Infrastructure is limited to one standby database per primary database.

- A Data Guard implementation requires two DB systems, one containing the primary database and one containing the standby database.
- When you enable Data Guard for a Virtual Machine DB System database, a new DB system with the standby database is created and associated with the primary database.
- For a Bare Metal DB system, the DB system with the database to be used as the standby must already exist before you enable Data Guard.

Using Oracle Data Guard on OCI: Requirements

Mandatory requirements:

- Same compartment
- Same shape
- Database versions and editions must be identical
- Must use same VCN
- Port 1521 must be open

Mandatory requirements for using Oracle Data Guard on OCI:

- Both DB Systems must be in the same compartment, and they must be the same shape.
- The database versions and editions must be identical.
- Both DB Systems must use the same VCN, and port 1521 must be open.
- The database version determines whether Active Data Guard is enabled.

Note: Properly configure the security list ingress and egress rules for the subnets of both DB Systems in the Data Guard association to allow TCP traffic to flow between the applicable ports. Ensure that the rules you create are stateful (the default).

For example, if the subnet of the primary DB System uses the source CIDR 10.0.0.0/24 and the subnet of the standby DB System uses the source CIDR 10.0.1.0/24, create rules as shown in the following example.

Security List for the Primary DB System's Subnet

Ingress Rules:

Stateless: No
Source: 10.0.1.0/24
IP Protocol: TCP
Source Port Range: All
Destination Port Range: 1521
Allows: TCP traffic for ports: 1521

Egress Rules:

Stateless: No
Destination: 10.0.1.0/24
IP Protocol: TCP
Source Port Range: All
Destination Port Range: 1521
Allows: TCP traffic for ports: 1521

Note: Oracle recommends that the DB System of the standby database be in a different availability domain from the DB System of the primary database to improve availability and disaster recovery. If you enable Data Guard for a virtual machine DB System database and if you launch the DB System for the standby in the same availability domain as the primary, Oracle tries to ensure that the standby DB System is located in a different fault domain from that of the primary.

Security List for the Standby DB System's Subnet

Ingress Rules:

Stateless: No
Source: 10.0.0.0/24
IP Protocol: TCP
Source Port Range: All
Destination Port Range: 1521
Allows: TCP traffic for ports: 1521

Egress Rules:

Stateless: No
Destination: 10.0.0.0/24
IP Protocol: TCP
Source Port Range: All
Destination Port Range: 1521
Allows: TCP traffic for ports: 1521

Working with Oracle Data Guard on OCI

Switchover

- Reverses the primary and standby database roles

Failover

- Transitions the standby database into the primary role

Reinstate

- Reinstates a database into the standby role in a Data Guard association

Switchover

Reverses the primary and standby database roles. Each database continues to participate in the Data Guard association in its new role. A switchover ensures no data loss. You can use a switchover before you perform planned maintenance on the primary database.

Failover

A failover transitions the standby database into the primary role after the existing primary database fails or becomes unreachable. A failover might result in some data loss when you use **Maximum Performance** protection mode.

The Reinstate

It reinstates a database into the standby role in a Data Guard association.

Note: Oracle Data Guard ensures high availability, data protection, and disaster recovery for enterprise data. The Oracle Cloud Infrastructure Database Data Guard implementation requires two databases, one in a primary role and one in a standby role. The two databases compose a Data Guard association. Most of your applications access the primary database. The standby database is a transactionally consistent copy of the primary database.

Data Guard maintains the standby database by transmitting and applying redo data from the primary database. If the primary database becomes unavailable, you can use Data Guard to switch or fail over the standby database to the primary role.

Enabling Data Guard on a Bare Metal DB System

1. Open the navigation menu. Under Database, click Bare Metal, VM, and Exadata.
2. Select the compartment that contains the DB System with the database for which you want to enable Data Guard.
3. Under Resources, click Data Guard Associations.
4. Click Enable Data Guard.
5. In the Enable Data Guard dialog box, configure your Data Guard association.
6. Click Enable.

Note: In the **Enable Data Guard** dialog box, configure your Data Guard association.

Peer DB System: Select the DB System that will contain the peer (standby) database.

Protection Mode: The protection mode used for this Data Guard association. The Console supports only **Maximum Performance**.

Transport Type: The redo transport type used for this Data Guard association. The Console supports only **Async**.

Database Admin Password: Enter the primary database admin password.

The same password is used for the standby database.

Confirm Database Admin Password: Re-enter the Database Admin Password you specified.

When the association is created, a shield icon appears next to the name of this database and its peer, and their respective roles (primary or standby) are displayed.

Enabling Data Guard on a Virtual Machine DB System

1. Open the navigation menu. Under Database, click Bare Metal, VM, and Exadata.
2. Select the compartment that contains the DB System with the database for which you want to enable Data Guard.
3. Click the name of the DB System that contains the database you want to assume the primary role, and then click the name of that database.
4. Under Resources, click Data Guard Associations.
5. Click Enable Data Guard.
6. In the Enable Data Guard dialog box, configure your Data Guard association.
7. Click Enable.

Note: In the Enable Data Guard dialog box, configure your Data Guard association.

Display Name: A friendly, display name for the DB System. The name doesn't need to be unique. An Oracle Cloud Identifier (OCID) will uniquely identify the DB System.

Availability Domain: The availability domain in which the DB System resides.

Virtual Cloud Network: (Informational) Shows the VCN in which the DB System will be launched. The VCN of the primary database and the standby database must be the same.

Client Subnet: The subnet to which the DB System should attach.

Do not use a subnet that overlaps with 192.168.16.16/28, which is used by the Oracle Clusterware private interconnect on the database instance. Specifying an overlapping subnet will cause the private interconnect to malfunction.

Hostname Prefix: Your choice of host name for the DB System. The host name must begin with an alphabetic character, and can contain only alphanumeric characters and hyphens (-). The maximum number of characters allowed for a virtual machine DB System is 30.

Important

The host name must be unique within the subnet. If it is not unique, the DB System will fail to provision.

Host Domain Name: The domain name for the DB System. If the selected subnet uses the Oracle-provided Internet and VCN Resolver for DNS name resolution, this field displays the domain name for the subnet and it can't be changed. Otherwise, you can provide your choice of a domain name. Hyphens (-) are not permitted.

Host and Domain URL: Combines the host and domain names to display the fully qualified domain name (FQDN) for the database. The maximum length is 64 characters.

Protection Mode: The protection mode used for this Data Guard association. The Console supports only Maximum Performance.

Transport Type: The redo transport type used for this Data Guard association. The Console supports only Async.

Database Admin Password: Enter the primary database admin password.

The same password is used for the standby database.

Confirm Database Admin Password: Re-enter the Database Admin Password you specified.

When the association is created, a shield icon appears next to the name of this database and its peer, and their respective roles (primary or standby) are displayed.

Summary

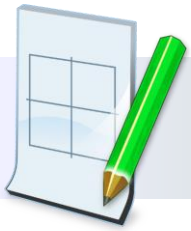
In this lesson, you should have learned how to:

- Use Oracle Data Guard on OCI
- Configure security lists for primary and standby DB Systems
- Work with Oracle Data Guard on OCI
- Enable Data Guard on a Bare Metal DB System
- Enable Data Guard on a Virtual Machine DB System

Practice 10: Overview

This practice covers the following topics:

- Practice 10-1: Enabling Data Guard for a 2 Node RAC Virtual Machine DB System
- Practice 10-2: Connecting to the DR DB System with SSH
- Practice 10-3: Performing a Database Switchover
- Practice 10-4: Performing a Database Switchback
- Practice 10-5: Performing a Database Failover
- Practice 10-6: Reinstating a Database
- Practice 10-7: Performing a Database Switchover
- Practice 10-8: Terminating a Data Guard Association on a Virtual Machine DB System
- Practice 10-9: Terminating a 2 Node RAC Virtual Machine DB System

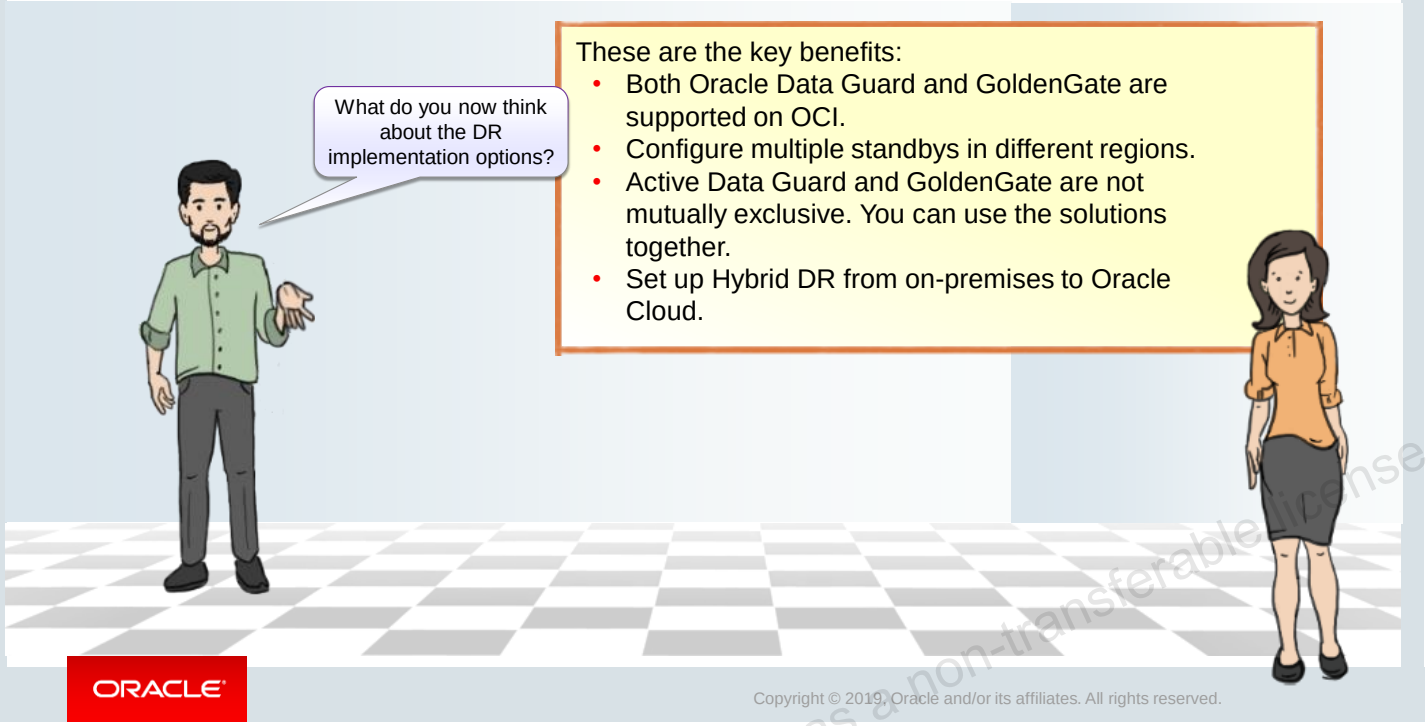


Objectives

- Describe key benefits of implementing database Disaster Recovery on OCI

After completing this lesson, you should be able to describe the key benefits of implementing the database Disaster Recovery system on OCI.

Database Disaster Recovery: Key Benefits



Conclusion

Practice 11: Overview

There are no practices for this lesson.