



Oracle Database Cloud for DBAs on Oracle Cloud Infrastructure

Student Guide

D105581GC10

Learn more from Oracle University at education.oracle.com

O

For Instructor Use Only.

This document should not be distributed.

Copyright © 2021, Oracle and/or its affiliates.

Disclaimer

This document contains proprietary information and is protected by copyright and other intellectual property laws. You may copy and print this document solely for your own use in an Oracle training course. The document may not be modified or altered in any way. Except where your use constitutes "fair use" under copyright law, you may not use, share, download, upload, copy, print, display, perform, reproduce, publish, license, post, transmit, or distribute this document in whole or in part without the express authorization of Oracle.

The information contained in this document is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

Restricted Rights Notice

If this documentation is delivered to the United States Government or anyone using the documentation on behalf of the United States Government, the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software" or "commercial computer software documentation" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

Trademark Notice

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

Third-Party Content, Products, and Services Disclaimer

This documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

1005272021

For Instructor Use Only.
This document should not be distributed.

Contents

1 Course Overview

Course Objectives 1-2
Objectives 1-3
Target Audience 1-4
Prerequisites 1-5
Course Roadmap 1-6
Course Practices 1-7
Summary 1-8
Practice 1: Overview 1-9

2 Oracle Cloud Platform for Database in the Cloud

Objectives 2-2
Oracle Database Cloud Services 2-3
Oracle Cloud Infrastructure (OCI) 2-4
Oracle Cloud Infrastructure: Database Service 2-5
OCI Security Features: Overview of Database Service 2-6
Journey to Autonomous Database 2-7
Automatic or Autonomous? 2-9
Autonomous Completes the Journey 2-10
One Autonomous Database | Optimized by Workload 2-11
Autonomous Optimizations | Specialized by Workload 2-12
Autonomous or User Managed? 2-13
Subscribing to an Oracle Cloud Service 2-14
Universal Credits 2-15
Bring Your Own License 2-16
Converged Database 2-17
Summary 2-18
Practice 2: Overview 2-19

3 Getting Started with Oracle Cloud Infrastructure

Objectives 3-2
Regions, Availability Domains, and Backbone Network 3-3
Inside a Region: High Availability Building Blocks 3-4
Inside an AD: High-Scale, High-Performance Network 3-5
Comprehensive Virtual Network with Off-Box Virtualization 3-6
Oracle Cloud Infrastructure: Innovation at Its Core 3-7
Oracle Cloud Infrastructure Services 3-9

Oracle Cloud Infrastructure Core Themes 3-10
Key Differentiators 3-11
Summary 3-12
Practice 3: Overview 3-13

4 Oracle Cloud Infrastructure Essentials

Objectives 4-2
Virtual Cloud Network (VCN) 4-4
Default VCN Components 4-5
OCI VPN: Overview 4-6
Compute: Bare Metal and Virtual Machines 4-8
Shape: Processor and Memory Resources 4-9
Available Shapes: Bare Metal 4-10
Available Shapes: VMs (Current Gen) 4-11
Available Shapes: VMs (Previous Gen) 4-12
Local NVMe SSD Devices 4-13
Object Storage Service 4-15
Common Object Storage Scenarios 4-16
Object Storage Resources 4-17
Object Storage Service Features 4-18
Object Storage Tiers 4-19
Block Volume Service Components 4-23
Boot Volumes: Manageable Boot Disks for Compute Instances 4-24
OCI Load Balancing Service 4-26
Public Load Balancer 4-28
Private Load Balancer 4-29
Concepts 4-30
Load Balancing Service: Shapes 4-31
Oracle Cloud Infrastructure: DNS 4-33
Capabilities of OCI DNS 4-34
Summary 4-35
Practice 4: Overview 4-36

5 Oracle Cloud Infrastructure: Database Service

Objectives 5-2
Oracle Cloud Infrastructure: Database Service 5-3
Database Service: Use Cases 5-5
Virtual Machine DB Systems 5-6
VM DB Systems Storage Architecture 5-7
Bare Metal DB Systems 5-8
Shapes for Bare Metal Database Systems 5-9

BM DB Systems Storage Architecture	5-10
Exadata DB Systems	5-11
Exadata DB X7 Systems	5-12
Exadata DB Systems Storage Architecture	5-14
Exadata Cloud Enterprise Edition Extreme Performance Most Powerful Database + Platform	5-15
Scaling Exadata DB Systems	5-16
OCI DB Systems: VM, BM, Exadata	5-17
Database Editions and Versions	5-18
Database Editions and Options	5-19
Managing DB Systems	5-20
Patching DB Systems	5-22
Backup/Restore	5-23
Automatic Backups	5-25
High Availability and Scalability	5-26
Data Guard	5-27
OCI Security Features Overview for Database Service	5-29
Summary	5-30
Practice 5: Overview	5-31

6 Bare Metal and Virtual Machine DB Systems

Objectives	6-2
Compute: Bare Metal and Virtual Machines	6-3
Bare Metal	6-4
Database Editions and Versions	6-5
Database Editions and Options	6-6
Shapes for Bare Metal Database Systems	6-7
Bare Metal Database Storage Options	6-8
Shapes for Virtual Machine Database Systems	6-9
Storage Options for Virtual Machine DB Systems	6-10
VM DB Systems Storage Architecture	6-11
BM DB Systems Storage Architecture	6-12
Oracle Database Software Images	6-13
Oracle Database Software Images: Example	6-14
Summary	6-15
Practice 6: Overview	6-16

7 Creating and Managing Bare Metal and Virtual Machine DB Systems

Objectives	7-2
Managing the Database Systems Overview	7-3
Required IAM Policy	7-4

Prerequisites to Launch a DB System	7-5
Default Options for the Initial Database	7-7
Creating a VCN for a DB System	7-8
VCN creates along with resources	7-14
VCN Details	7-15
Using the Console to Launch a DB System	7-16
Steps to Fill in DB System Information	7-19
Steps to Fill in Network Information	7-21
Steps to Fill in Database Information	7-22
Using the Console to Check the Status of a DB System	7-24
Using the Console to Manage a DB System	7-25
Using Console to Start, Stop, and Reboot a DB System	7-26
Using the Console to Scale Up Storage	7-27
Using the Console to Terminate a DB System	7-28
Using the Console to Manage BYOL Database Licenses	7-29
Using the Console to Manage Tags	7-30
Using the API Operations to Launch a DB System	7-31
Using the API Operations to Manage a DB System	7-32
Setting Up DNS for a DB System	7-33
Special Considerations for Creating DB Systems	7-34
Summary	7-35
Practice 7: Overview	7-36

8 Connecting to a DB System on OCI

Objectives	8-2
Connecting to a Pluggable Database	8-3
Setting Environment Variables	8-4
Prerequisites for SSH Access to the DB System	8-5
Connecting to a DB System with SSH	8-6
Connecting to a Database with Oracle SQL Developer	8-7
Connecting to a Database on a 1-Node DB System	8-8
Connecting to a Database on a Multi-Node DB System	8-9
Troubleshooting Connection Issues	8-10
Summary	8-11
Practice 8: Overview	8-12

9 Updating and Configuring a DB System on OCI

Objectives	9-2
Updating a DB System	9-3
Bash Profile Updates	9-4
Essential Firewall Rules	9-5

Important Guidelines for OS Updates	9-6
Configuring a DB System	9-7
Network Time Protocol (NTP)	9-8
Transparent Data Encryption	9-9
Scaling a DB System	9-10
Scaling a CPU	9-11
Scaling Storage	9-12
Cloning a Virtual Machine DB System	9-13
Summary	9-15
Practice 9: Overview	9-16

10 Patching a DB System on OCI

Objectives	10-2
Patching DB Systems	10-3
Patching Prerequisites	10-4
Performing Patch Operations on DB System Using Console	10-5
Viewing the Patch History of a DB System	10-6
Performing Patching Using CLI	10-8
Checking the Installed Patches	10-10
Patch Server Components	10-11
Patching Database Home Components	10-12
Applying Interim Patches	10-13
Patching Failures	10-15
Determining the Problem	10-16
Identifying the Root Cause of the Patching Operation Failure	10-17
Summary	10-18
Practice 10: Overview	10-19

11 Configuring and Monitoring a Database on OCI

Objectives	11-2
Monitoring a Database	11-3
Enabling EM Express Console	11-4
Connecting to EM Express Console	11-5
Enabling Enterprise Manager Database Control	11-6
Connecting to EM Database Control Console	11-7
Opening Ports on the DB System	11-8
Opening a Port on the DB System	11-9
Updating the Security List for the DB System	11-10
Updating an Existing Security List	11-11
Special Considerations to Create and Configure a New PDB	11-12
Creating and Activating a Master Encryption Key for a New PDB	11-13

Summary 11-14

Practice 11: Overview 11-15

12 Backing Up and Recovering a Database on OCI

Objectives 12-2

Backing Up a Database 12-3

Object Storage 12-4

Local Storage 12-5

Swift Object Storage 12-6

Backing Up to Oracle Cloud Infrastructure Object Storage 12-7

Backing Up Using the Console 12-8

Enabling or Disabling Automatic Backups for a DB 12-9

Creating an On-Demand Full Backup of a Database 12-10

Deleting a Full Backup from Object Storage 12-11

Backing Up to Object Storage Using RMAN 12-12

Installing the Backup Module on the DB System 12-13

Configuring RMAN 12-14

Backing Up the Database Using RMAN 12-15

Backing Up to Local Storage Using the Database CLI 12-16

Recovering a Database from Object Storage 12-17

Restoring an Existing Database Using the Console 12-18

Restoring a Database Using a Specific Backup from Object Storage 12-19

Creating a New Database from a Backup 12-20

Launching a New DB System from a Backup 12-21

Recovering a Database from a CLI Backup 12-22

Recovering the Database Using CLI 12-23

Recovering a Database from the Oracle Cloud Infrastructure Classic
Object Store 12-24

Steps to Recover a Database from OCIC Object Store 12-25

Troubleshooting Backup Failures 12-26

Identifying the Root Cause of a Backup Failure 12-27

Object Store Connectivity Issues 12-28

Known Challenges for Database Backup Failure 12-29

Improper Database State Affecting Backups 12-30

TDE Wallet and Backup Failures 12-32

Summary 12-33

Practice 12: Overview 12-34

13 Oracle Cloud Infrastructure Security

Objectives 13-2

OCI Security Features: Overview of Database Service 13-3

Identity and Access Management Service	13-4
Principals	13-5
Authentication	13-6
Authorization	13-7
User Authentication: OCI Security Credentials	13-8
Instance Isolation: OCI Database Bare Metal (BM) Instance	13-9
Network Security: Virtual Cloud Network (VCN)	13-10
User Authorization: OCI IAM	13-11
Data Encryption: OCI Storage Encryption	13-12
Data Encryption: OCI Database Service TDE	13-13
In the Cloud, Security Is a Shared Responsibility	13-14
Security What Can I Do to Prepare?	13-15
Oracle Data Safe: Overview	13-17
Features of Oracle Data Safe	13-18
Summary	13-19
Practice 13: Overview	13-20

14 Migrating Oracle Databases to OCI: Overview

Objectives	14-2
Why Migrate to Oracle Cloud Infrastructure?	14-3
Managing Oracle Database: On Premises Versus Oracle Cloud Infrastructure	14-4
Managing Oracle Database: On Premises Versus Cloud	14-5
What Can You Migrate to Oracle Database Cloud?	14-7
Considerations for Choosing a Migration Method	14-8
Migration: Information Gathering	14-9
Migration: Analysis and Planning	14-11
Migration: Data Transfer Options (Online and Sync)	14-13
Migration: Data Transfer Options (Offline)	14-14
Migration: Security Considerations	14-15
Migration Options	14-16
Zero Downtime Migration (ZDM)	14-17
Data Transfer Service	14-18
Summary	14-19
Practice 14: Overview	14-20

For Instructor Use Only.
This document should not be distributed.



Course Overview

1

0

For Instructor Use Only.

This document should not be distributed.

Course Objectives

After completing this course, you should be able to:

- Identify Oracle Database Cloud Services offerings
- Identify the differences between and benefits of User-Managed and Autonomous Database Services on Oracle Cloud
- Describe the essentials of Oracle Cloud Infrastructure
- Identify the deployment options available in virtual machine and bare metal DB systems
- Create and configure virtual machine DB systems
- Manage and monitor virtual machine DB systems
- Identify available database migration methods and techniques

2
O



For Instructor Use Only.

This document should not be distributed.

Objectives

After completing this lesson, you should be able to:

- Provide an overview of the topics covered
- List the prerequisites for this course

3



For Instructor Use Only.

This document should not be distributed.

Target Audience

This course is mainly intended for:

- Database administrators
- System administrators
- Database architects
- Cloud architects



0

For Instructor Use Only.

This document should not be distributed.

Prerequisites

To successfully complete this course you should have:

- General understanding of cloud technology
- Working knowledge of Oracle Database 11g, 12c, 18c, or 19c Administration
- Basic understanding of Oracle Cloud Infrastructure

Suggested prerequisites:

- Working knowledge of managing Oracle Multitenant Database
- *Oracle Cloud Infrastructure Fundamentals* (OU course)



0

For Instructor Use Only.

This document should not be distributed.

Course Roadmap

1. Course Overview
2. Oracle Cloud Platform for Database in the Cloud
3. Getting Started with Oracle Cloud Infrastructure
4. Oracle Cloud Infrastructure Essentials
5. Oracle Cloud Infrastructure: Database Service
6. Bare Metal and Virtual Machine DB Systems
7. Creating and Managing Bare Metal and Virtual Machine DB Systems
8. Connecting to a DB System on OCI
9. Updating and Configuring a DB System on OCI
10. Patching a DB System on OCI
11. Configuring and Monitoring a Database on OCI
12. Backing Up and Recovering a Database on OCI
13. Oracle Cloud Infrastructure Security
- 6 14. Migrating Oracle Databases to OCI: Overview



O

This course is organized into 14 lessons. Some lessons have an associated activity guide that allows the students to put their learnings into practice.

For Instructor Use Only.
This document should not be distributed.

Course Practices

- Lessons are reinforced with hands-on practices.
- Your practice environment consists of:
 - Your local system, i.e. laptop or desktop with Windows 64-bit operating system
 - Oracle Cloud account assigned to you as part of the course environment using which you will create the required Oracle Cloud service instance

Note: You should be on an open internet connection, i.e. not connected to any VPN or working in a restricted network that blocks connection from your local system to cloud service instances.

0

For Instructor Use Only.

This document should not be distributed.

Summary

In this lesson, you should have learned to:

- Provide an overview of the topics covered
- List the prerequisites for this course

0



For Instructor Use Only.

This document should not be distributed.



Practice 1: Overview

—
There are no practices for this lesson.



0

For Instructor Use Only.
This document should not be distributed.

For Instructor Use Only.
This document should not be distributed.

ORACLE



Oracle Cloud Platform for Database in the Cloud

2

0

For Instructor Use Only.

This document should not be distributed.

Objectives

After completing this lesson, you should be able to:

- Describe the offerings of Oracle Database Cloud Services
- Describe Oracle Cloud Platform for Database in the Cloud
- Describe Oracle Autonomous Cloud Platform
- Explain the difference between User-Managed and Autonomous Database Services
- Describe Oracle Cloud Subscription Models
- Describe a Converged Database



0

For Instructor Use Only.

This document should not be distributed.

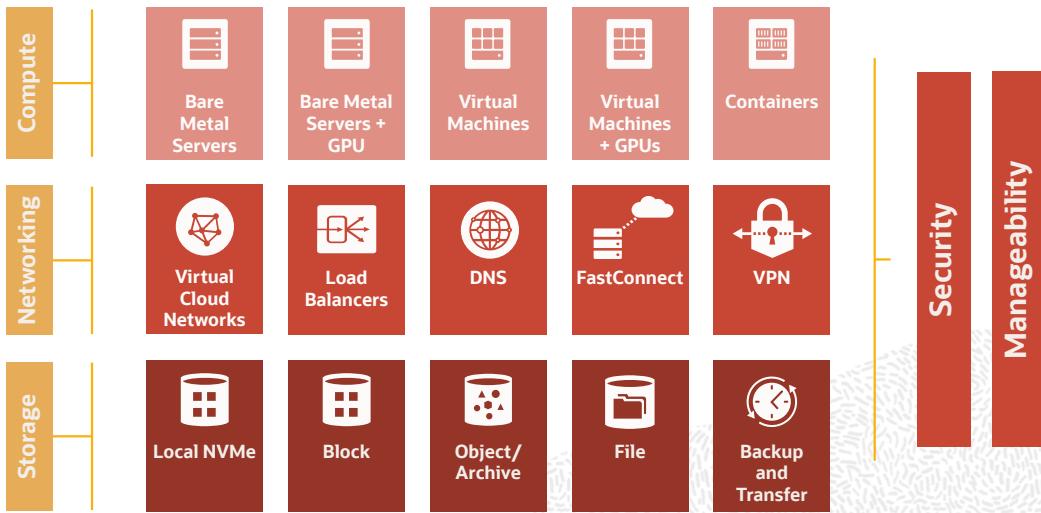
Oracle Database Cloud Services

- Oracle offers database cloud services in a range of public cloud deployment choices:
 - Fully managed pluggable databases with Exadata Express Cloud Service
 - Virtualized and bare metal databases with Database Cloud Service
 - Databases running on world-class engineered infrastructure with Exadata Cloud Service
- Oracle also offers Cloud at Customer for customers who want Exadata database cloud services behind their firewalls, on their own premises.

0

For Instructor Use Only.
This document should not be distributed.

Oracle Cloud Infrastructure (OCI)



4

0

For Instructor Use Only.
This document should not be distributed.

Oracle Cloud Infrastructure: Database Service

- Mission-critical enterprise-grade cloud database service with comprehensive offerings to cover all enterprise database needs
 - Virtual machine (VM), bare metal (BM), Exadata
- Complete life cycle automation
 - Provisioning, patching, backup, restore, clone, replicate (complete flexibility)
- High availability and scalability
 - Robust infrastructure
 - Robust database options
 - Dynamic CPU and storage scaling
- Security
 - Infrastructure (IAM, security lists, audit logs)
 - Database (Transparent Data Encryption)

5



O

OCI and OCI Database Service

OCI Database Service runs on top of OCI, which specializes in bare metal servers, off-box networking (which accommodates any workload, engineered system, VM, or bare metal host all on the same network) and high-speed storage.

OCI has a robust infrastructure.

Three Availability Domains (ADs). Multi-region architecture, currently three with a fourth region being brought up

Fully redundant and nonblocking networking fabric accommodating up to 2 * 25 Gbe networking to the hosts

Three-way mirrored storage (optional two-way mirroring) for database systems. Disk management set up by OCI Database Service is according to best practices, so ASM comes preconfigured for each of the shapes.

Redundant InfiniBand fabric for cluster networking (Exadata, 2 node, bare metal, RAC)

Robust database options

Database RAC option for VM DB system

Automatic backups to object storage are set up for users when the database is started. Automated Data Guard configuration for both primary and standby system (available within the AD and across AD).

All the systems are created so that they follow the Maximum Availability Architecture (MAA). This is considered a certified deployment.

For Instructor Use Only.
This document should not be distributed.

OCI Security Features: Overview of Database Service

No.	Security capability	OCI DBCA security feature
1	Instance security isolation	OCI bare metal instance
2	Network security and access control	VCN, VCN security lists, VCN public and private subnets, VCN route table
3	Secure and highly available connectivity	VPN DRGs
4	User authentication and authorization	IAM tenancy, compartments and security policies, console password, API signing key, SSH keys
5	Data encryption	DBaaS TDE, RMAN encrypted backups, storage and object encryption at rest
6	End-to-end TLS	LBaaS with TLS1.2, customer-provided certificates
7	Auditing	OCI API audit logs

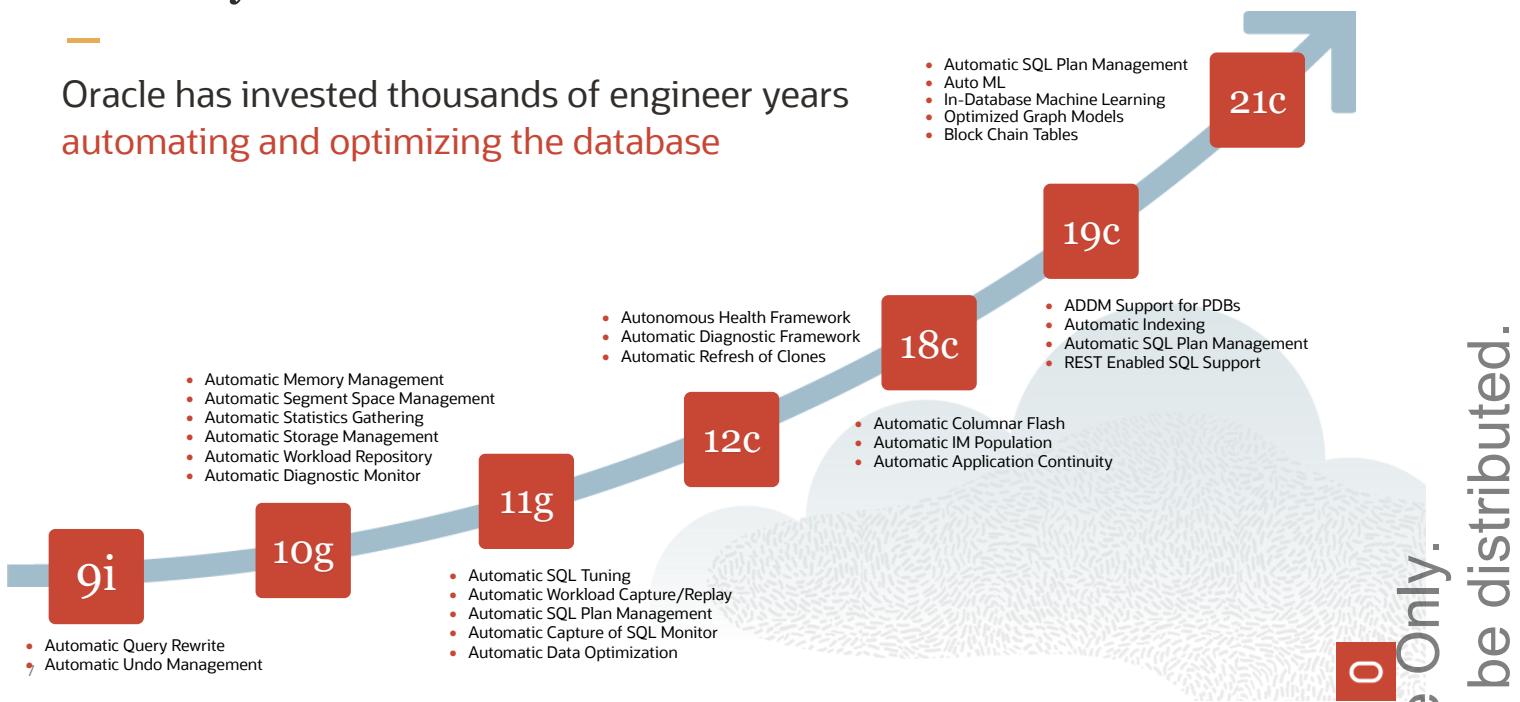
6

0

For Instructor Use Only.
This document should not be distributed.

Journey to Autonomous Database

Oracle has invested thousands of engineer years automating and optimizing the database



That's quite a tall order for a new product until you realized that we have been on this journey for over 20 years.

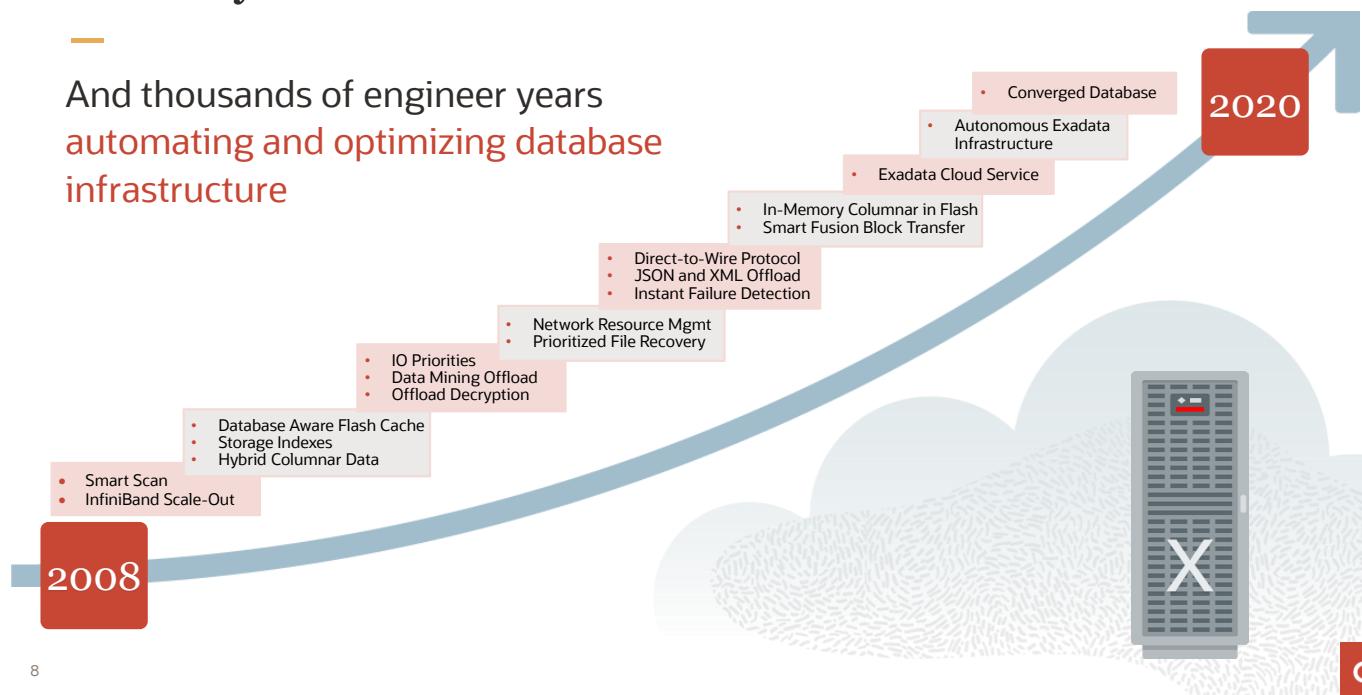
Starting with Oracle Database 9i we began to introduce and mature many sophisticated automation capabilities from memory management to workload monitoring and tuning, all of which are used in the Autonomous Database.

For Instructor Use Only.

This document should not be distributed.

Journey to Autonomous Database

And thousands of engineer years
automating and optimizing database
infrastructure



8

But it's not just database management that Oracle has been automating. We have also spent the last decade working on database infrastructure with our engineered systems, which provide the best platform for Oracle Database as they are the only preconfigured, pre-tested, and optimized platforms for the database.

For Instructor Use Only.

This document should not be distributed.

Automatic or Autonomous?

	Automatic	Autonomous
Autonomous Car 	<ul style="list-style-type: none">• Cruise control• Emergency stopping• Warnings for lane changes	<ul style="list-style-type: none">• No need to use the steering wheel or brake• Simply tell the car where you are going.
Autonomous Database 	<ul style="list-style-type: none">• Automatic storage management• Automatic workload repository• SQL Plan Management	<ul style="list-style-type: none">• All features automatically implemented• Simply tell the database your goals.

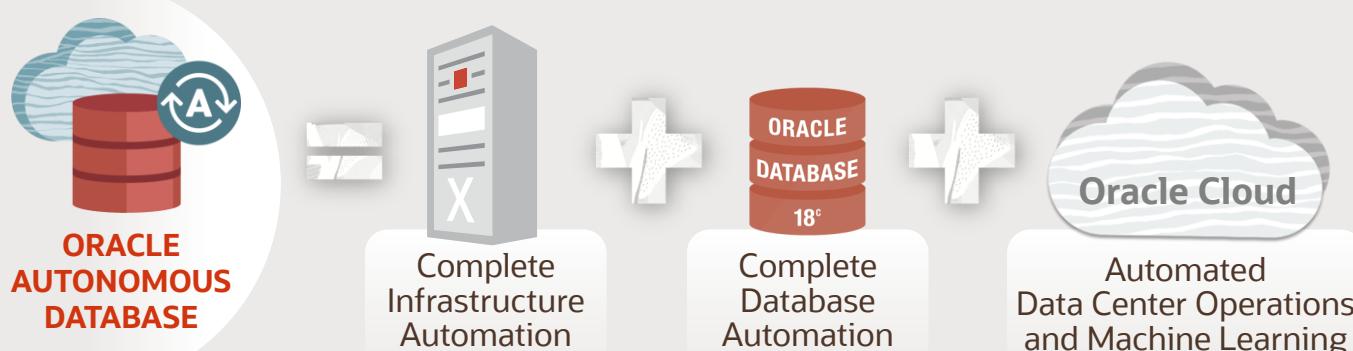
9

0

For Instructor Use Only.
This document should not be distributed.

Autonomous Completes the Journey

Brings Full Automation to Entire Database Lifecycle



World's First Autonomous Database

10

0

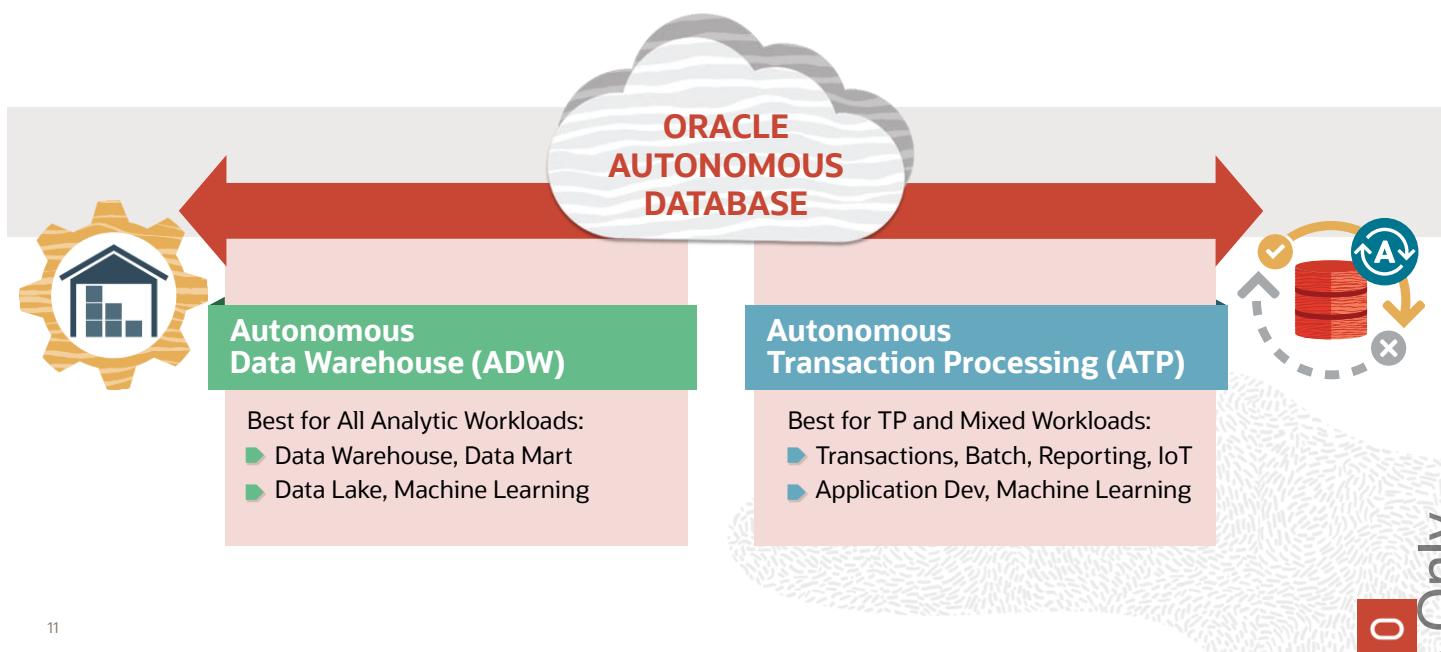
Oracle Cloud allows us to complete the journey to Autonomous Database as it is the integration of our complete infrastructure automation with Oracle Database 19c, and our fully automated data center operations.

Automated data center operations include:

- Provisioning, patching, upgrading, and online backups
- Monitoring, scaling, diagnosing performance, tuning, optimizing
- Testing and change management of complex applications and workloads
- Automatic handling of failures and errors

For Instructor Use Only.
This document should not be distributed.

One Autonomous Database | Optimized by Workload



11

O

Oracle Autonomous Database is actually a family of cloud services with each member of the family optimized by workload. The first member of the family to become available was the Autonomous Data Warehouse (ADW), which has been optimized for analytic workloads, such as data warehouse, data marts, or as part of a data lake.

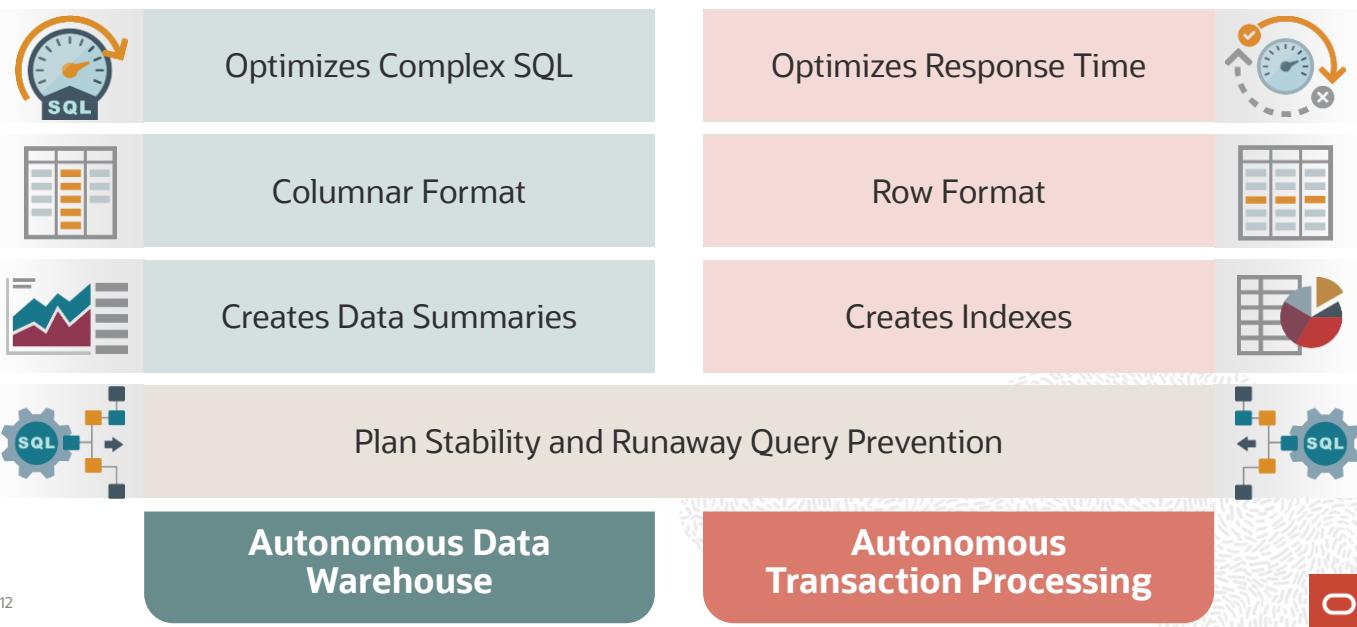
The second member of the family that's just become available is Autonomous Transaction Processing (ATP).

ATP is optimized for transaction processing or mixed workload environments and makes an excellent platform for new application development.

For Instructor Use Only.

This document should not be distributed.

Autonomous Optimizations | Specialized by Workload



12

Both ADW and ATP share the Autonomous Database platform of Oracle Database 19c on our Exadata Cloud infrastructure.

The difference is how the services have been optimized within the database. When you start loading data into the Autonomous Database, we store the data in the appropriate format for the workload.

If it is ADW, then we store data in columnar format as that's the best format for analytics processing.

If it is ATP, then we will store the data in a row format as that's the best format for fast single-row lookups.

Query Optimization

For analytics workload, we automatically parallelize the query execution to access large volumes of data in a short amount of time to answer business questions. If it is a transaction processing system, then we will automatically detect missing indexes and create them for you.

Regardless of the workload, we need to keep optimizer statistics current to ensure we get optimal execution plans. With ADW we are able to achieve this by gathering statistics as part of all bulk load activities. With ATP, where data is added using more traditional insert statements, statistics are automatically gathered periodically.

As the data volumes change, or new access structures are created, there is the potential for an execution plan to change. Any change could result in a performance regression so we use Oracle SQL Plan Management to ensure that plans only change for the better.

Autonomous or User Managed?



User Managed

- Automated with human intervention to take control in a customized environment for tuning to meet very specific business requirements
- Need to have complete operational control, including OS access, full DBA privileges



Autonomous

- Decision making, performing one or more tasks automatically

Example: Race Car Track

0

For Instructor Use Only.

This document should not be distributed.

Subscribing to an Oracle Cloud Service

To subscribe to an Oracle Cloud Service, perform the following steps:

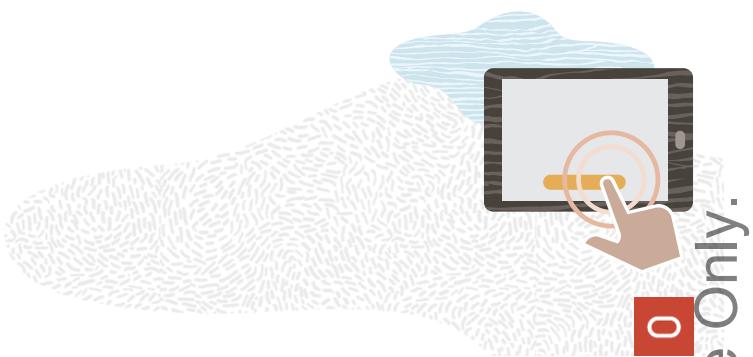
1. Order an Oracle Cloud account in one of the following ways:

- Sign up for an Always Free tier. See [Oracle Cloud Free Tier](#).
- Order a paid subscription to an Oracle Cloud Service. Estimate your monthly cost and choose the Pay As You Go and/or Monthly Flex subscription plans.

2. Activate the service.

3. Verify that the service is running.

4. Upgrade to a paid Oracle Cloud account.



14

Detailed information about subscribing to an Oracle Cloud Service trial and purchasing a subscription to an Oracle Cloud Service can be found in the *Getting Started with Oracle Cloud* guide.

For Instructor Use Only.
This document should not be distributed.

Universal Credits

- Universal access to all current and future IaaS and PaaS services
- Flexibility to upgrade, expand, or move services across data centers

Consumption Choices	
Pay As You Go <ul style="list-style-type: none">• No upfront commitment• Pay only for what you use• Pay in arrears based on usage	Universal Credits Monthly Flex <ul style="list-style-type: none">• One-year minimum term• Based on the results of your monthly cost estimate
<ul style="list-style-type: none">• List Price• Built for land and expand• Best when usage is uncertain• Elastic payments based on usage	<ul style="list-style-type: none">• PaaS savings vs Pay As You Go• Additional discounts based on size of deal and term of deal• Predictable spending• Spend more, save more

15

0

For Instructor Use Only.

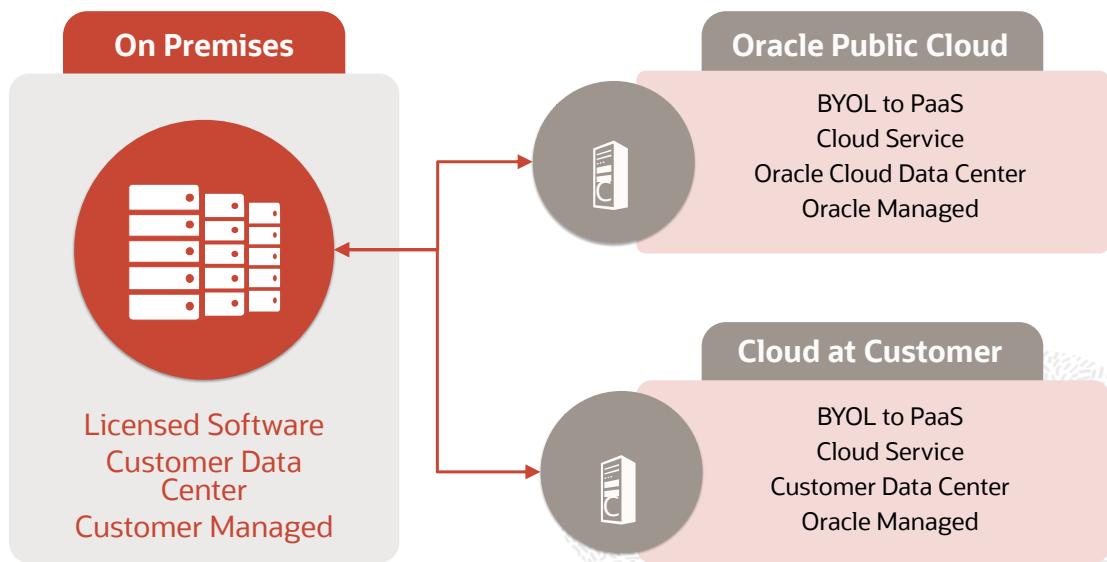
This document should not be distributed.

Universal Credits: Universal Cloud Credits make it easy for customers to take advantage of Oracle Cloud Services. Universal Cloud Credits can be applied to all Oracle IaaS and PaaS services in the public cloud, and allow customers to pay for services as they use them.

When you sign up for an Oracle Cloud account, you have unlimited access to all eligible services, and have the flexibility to sign up for a Pay As You Go subscription or the Monthly Flex plan. The Monthly Flex plan allows customers to pay in advance for a year with estimates based on monthly usage, which can help reduce cost.

Both of these payment plans can be applied to any new eligible cloud service as soon as it becomes available.

Bring Your Own License



16

O

For Instructor Use Only.
This document should not be distributed.

Converged Database

- A converged database is a database that has native support for all modern data types and the latest development paradigms built into one product.
- It supports spatial data for
 - Location awareness
 - JSON for document stores
 - IoT for device integration
 - In-memory technologies for real-time analytics
 - Traditional relational data
- Oracle Database is an excellent example of a converged database.
- It provides support for machine learning, blockchain, graph, spatial, JSON, REST, events, editions, and IoT streaming as part of the core database at no additional cost.



17

0

Converged databases support spatial data for location awareness, JSON for document stores, IoT for device integration, in-memory technologies for real-time analytics, and of course, traditional relational data. By providing support for all of these data types, a converged database can run all sorts of workloads from IoT to blockchain to analytics and machine learning. It can also handle any development paradigm, including microservices, events, REST, SaaS, and CI/CD, to name a few.

Traditionally when new data management technologies first come out, they are implemented as separate products. For example, when blockchain first came out, it was a separate stand-alone system that required you to use an entirely different, proprietary way to store and access data.

By integrating new data types, workloads, and paradigms as features within a converged database, you can support mixed workloads and data types in a much simpler way. You don't need to manage and maintain multiple systems or worry about having to provide unified security across them.

For more information, refer to: <https://blogs.oracle.com/database/what-is-a-converged-database>

<https://www.oracle.com/cloud/solutions/converged-database/>

For Instructor Use Only.

This document should not be distributed.



Summary

In this lesson, you should have learned how to:

- Describe the offerings of Oracle Database Cloud Services
- Describe Oracle Cloud Platform for Database in the Cloud
- Describe Oracle Autonomous Cloud Platform
- Explain the differences between User-Managed and Autonomous Database Services
- Describe Oracle Cloud Subscription Models
- Describe a Converged Database

0

For Instructor Use Only.

This document should not be distributed.



Practice 2: Overview

—
There are no practices for this lesson.



0

For Instructor Use Only.
This document should not be distributed.

For Instructor Use Only.
This document should not be distributed.



Getting Started with Oracle Cloud Infrastructure

3

0

For Instructor Use Only.

This document should not be distributed.

Objectives

After completing this lesson, you should be able to:

- Describe Oracle Cloud Infrastructure strategy
- Define key concepts and terminology
- Identify Oracle Cloud Infrastructure Services

2



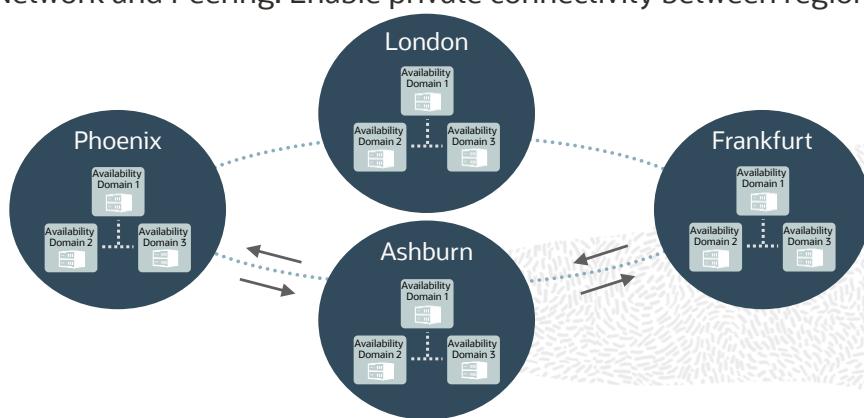
In this lecture, we'll describe the key concepts and terms used in the Oracle Cloud Infrastructure IAM service.

For Instructor Use Only.

This document should not be distributed.

Regions, Availability Domains, and Backbone Network

- Regions serve different geographies: Provide disaster recovery capability
- Availability Domains and Fault Domains: Provide an HA foundation within a region and an AD
- Backbone Network and Peering: Enable private connectivity between regions and direct peering



3

O

For Instructor Use Only.

This document should not be distributed.

Let me start with a quick recap of our core concepts. We operate in regions. A region is a metropolitan area. Inside regions, we have multiple data centers that are called Availability Domains (ADs). Each region consists of three ADs. These are isolated from each other and all your resources like compute and database go inside an AD. ADs are wired together over private dark fiber and there is very little latency between ADs making it a perfect fit for a high availability (HA) primitive replication of data. We have a dedicated backbone connecting these ADs. The backbone plugs into edge or peering points of presence where customers can get direct connections to our network.

Inside a Region: High Availability Building Blocks

- Multiple fault-decorrelated, completely independent data centers: ADs
- Predictable low latency and high speed, encrypted interconnect between ADs
 - < 500 µs expected one-way latency
- Enables zero-data-loss architectures (for example, Oracle MAA) and high availability scale-out architectures (for example, Cassandra)



4

0

Again, regions are constructed of isolated fault domains. You can see some latency numbers here: < 500 micro seconds one latency.

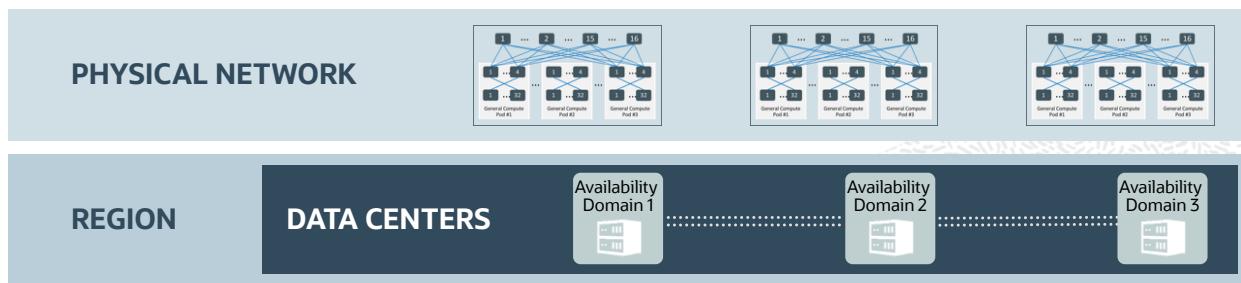
For Instructor Use Only.
This document should not be distributed.

Inside an AD: High-Scale, High-Performance Network

Non-oversubscribed network: Flat, fast, predictable

Very high scale: ~1 million network ports in an AD

- Predictable low latency and high-speed interconnect between hosts in an AD
 - ~100 µs expected one-way latency, 2 x 25 GB/s bandwidth



5

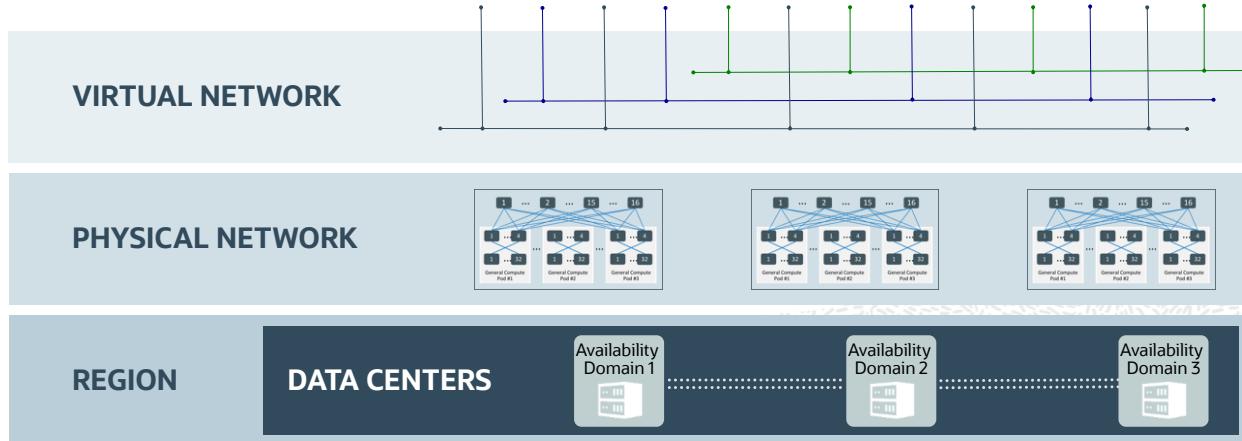
O

Inside these ADs, we have built one of the best public cloud networks. It is big, flat, and fast. It runs on a high scale to the tune of 1 million network works per AD. Flat means that it is not oversubscribed, so we get extremely good latency. Fast means we support 25 Gbps network bandwidth between hosts.

For Instructor Use Only.
This document should not be distributed.

Comprehensive Virtual Network with Off-Box Virtualization

Highly configurable private overlay networks: Moves management and I/O out of the hypervisor and enables lower overhead and bare metal instances



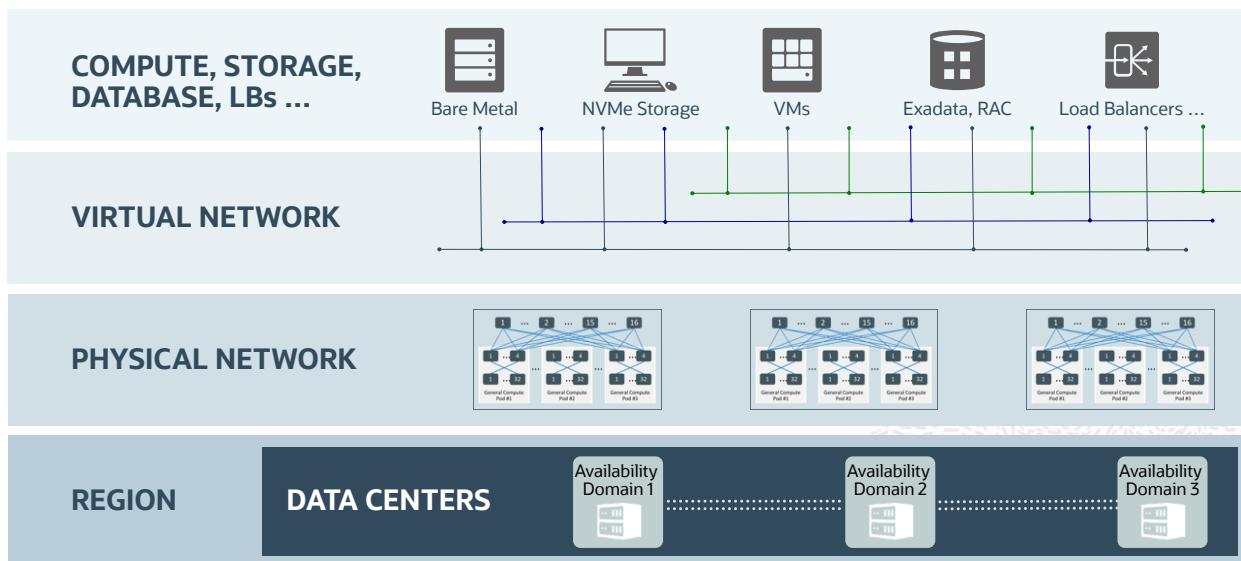
6

O

For Instructor Use Only.
This document should not be distributed.

We have made some drastic changes to how virtual networking is done. We call it off-box virtualization. As the name implies, we pulled all the virtualization out into the network, including storage and network I/O virtualization. Generally, this enables the next layer up; so we can take any physical form factor and plug that into our virtual network. This is the basis that lets us use bare metal and engineered systems like Exadata and plug it into this environment without making any changes. It is a massive enabler for us to deliver the classes of services and meet our goals around performance and security.

Oracle Cloud Infrastructure: Innovation at Its Core

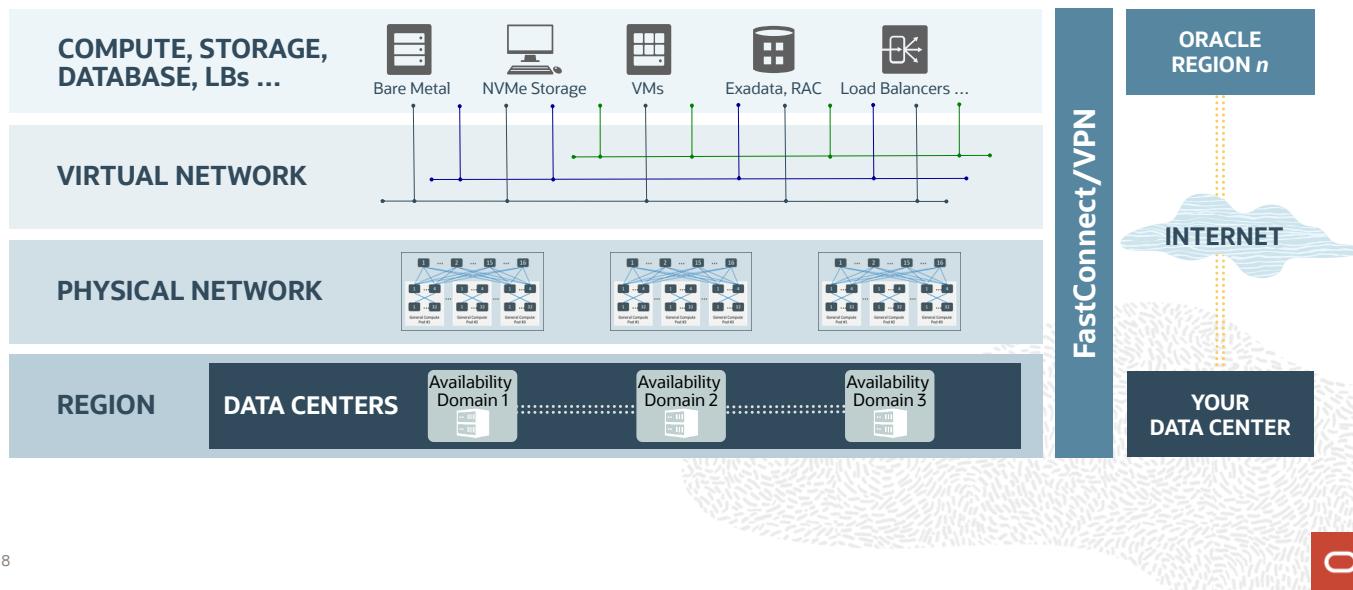


7

O

For Instructor Use Only.
This document should not be distributed.

Oracle Cloud Infrastructure: Innovation at Its Core



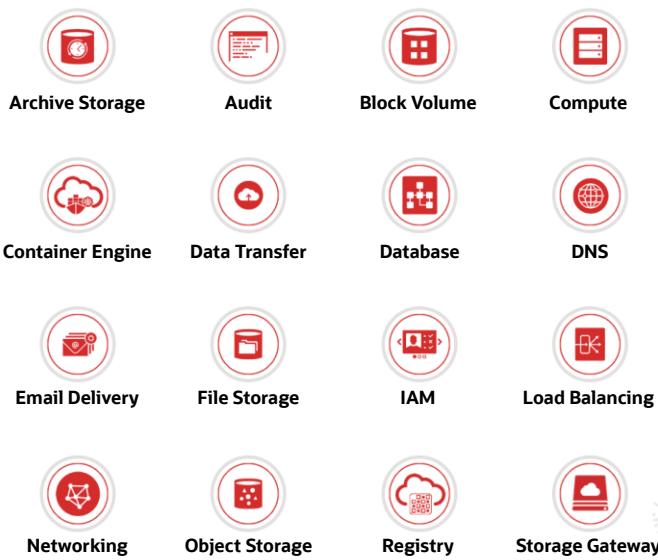
8

0

And if we bundle that with the backbone network, this is what the picture looks like.

For Instructor Use Only.
This document should not be distributed.

Oracle Cloud Infrastructure Services



PaaS Services

Analytics Cloud
Autonomous API Platform Cloud Service
Autonomous Data Warehouse Cloud
Autonomous Integration Cloud
Autonomous Mobile Cloud Enterprise
Autonomous Visual Builder Cloud Service
Big Data Cloud
Content and Experience Cloud
Data Integration Platform Cloud
Database Cloud Service
Developer Cloud Service
NoSQL Cloud Service
Java Cloud Service
MySQL Cloud Service
Oracle SOA Cloud Service

9

O

Now let's talk about the various services we have on our platform today. IAM service helps you set up administrators, users, and groups and specify their permissions. Audit service helps you track activity in your environment. Networking service helps you set up software-defined versions of traditional physical networks. Compute service helps you provision and manage compute instances.

Block Storage service helps you dynamically provision and manage block storage volumes. Object Storage service helps you manage data as objects that are accessed over the internet. Load Balancing service helps you create a load balancer within your virtual network. Database service helps you provision and manage Oracle databases.

For Instructor Use Only.

This document should not be distributed.

Oracle Cloud Infrastructure Core Themes

- **Lift and Shift:** Enable enterprise workload migration to the cloud without re-architecting
 - Unmatched Oracle on Oracle
 - Extend to non-Oracle workloads (VMware, SAP, custom apps)
- **Infrastructure-Heavy Workloads:** Demand high scale/high performance
 - Best hardware, best performance, best price
 - Big data, HPC, machine learning
- **Cloud Native Workloads:** Provide programmable infrastructure for cloud-first development
 - Self-service, cost, flexibility, agility
 - Modern apps and DevOps

10

O

For Instructor Use Only.

This document should not be distributed.

Key Differentiators

Oracle apps and support for Enterprise IaaS architecture:

- Best cloud to run Oracle Database and key enterprise Oracle apps
- Industry's first bare metal cloud service
- Flexibility and control (bare metal and VMs share the same set of APIs)
- Off-box network virtualization (with support for plugging Exadata appliances)
- Non-oversubscribed network, predictable performance with low latency and high throughput
- Robust security and governance capabilities

Industry-leading price performance:

- Simple pricing; best performance
- Lower compute costs than AWS EC2 compute
- Fast, predictable block storage with no additional cost for IOPS; multiple times cheaper than AWS
- Bandwidth costs less than AWS bandwidth by 85%

¹¹

0

There are two main areas of differentiation. First is the support for Oracle apps and enterprise IaaS architecture. OCI is the best platform for running Oracle Database and key enterprise Oracle apps. We are the only cloud that supports bare metal services and where VMs and bare metal servers have the same set of APIs. Also, our network is highly differentiated; we have a fundamentally different approach to networking through off-box network virtualization and our network is big, flat, and fast. As a result, you can get tremendous throughput and low latency. We also have a unique approach to security and governance through the use of compartments, which we'll talk about in later modules.

Second, we are the price performance leader: our compute, storage, and network costs are all lower than those of AWS.

For Instructor Use Only.

This document should not be distributed.

Summary

In this lesson, you should have learned how to:

- Describe Oracle Cloud Infrastructure strategy
- Define key concepts and terminology
- Identify Oracle Cloud Infrastructure Services

O



12

In this lecture, we described the key concepts and terms used in the IAM service.

For Instructor Use Only.

This document should not be distributed.



Practice 3: Overview

—
There are no practices for this lesson.



0

For Instructor Use Only.
This document should not be distributed.

For Instructor Use Only.
This document should not be distributed.

ORACLE



Oracle Cloud Infrastructure Essentials

4

0

For Instructor Use Only.

This document should not be distributed.

Objectives

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

- Key Virtual Cloud Network (VCN) concepts
- OCI Compute service
- Object Storage service
- Block Volume service
- Oracle Cloud Infrastructure Load Balancing service concepts
- OCI DNS services available with Oracle Cloud Infrastructure

0



For Instructor Use Only.
This document should not be distributed.



Virtual Cloud Network Service

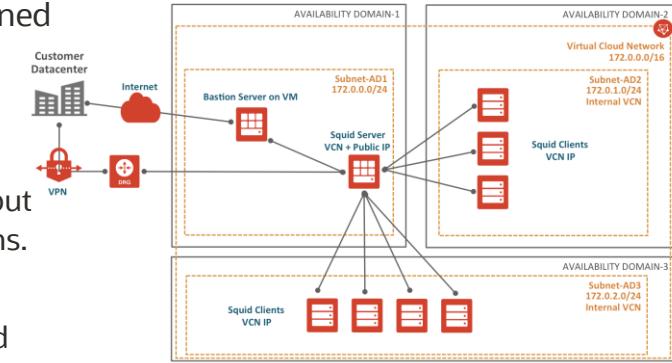


For Instructor Use Only.

This document should not be distributed.

Virtual Cloud Network (VCN)

- A Virtual Cloud Network is a software-defined version of a traditional physical network including subnets, route tables, and gateways on which your instances run.
 - 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 provides a single point of entry for remote network paths coming into your VCN.
 - You can use a DRG to establish a connection with your on-premises network via IPSec VPN or FastConnect.



4

O

A VCN within Oracle Cloud Infrastructure is a software-defined version of a traditional physical network. VCN is a regional service and you can create a VCN by specifying a CIDR range. Each VCN network is subdivided into subnets, and subnets can be either AD-specific or regional.

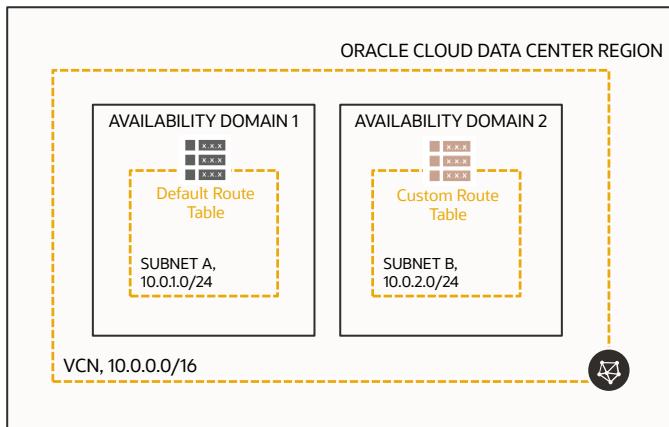
Internet gateway provides a path for network traffic between your VCN and the Internet.

DNS enables lookup using host names. Remember this isn't a public DNS service, but DNS for VCN and subnets. The default choice is Internet and VCN Resolver which lets the instances use hostnames to communicate. The way it works is that you enable the Internet and VCN Resolver across your entire VCN. This means all instances in the VCN can communicate with each other without knowing their IP addresses.

With FastConnect, you can establish a connection in one of these ways:

- **Colocation:** By colocating with Oracle in a FastConnect location
- **Provider:** By connecting to a FastConnect provider

Default VCN Components

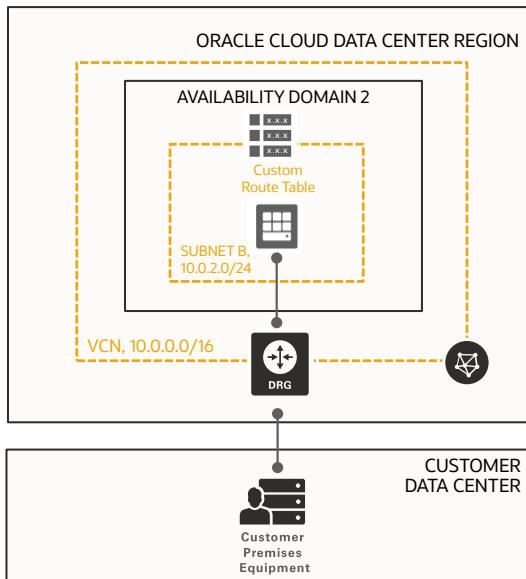


Your VCN automatically comes with some default components:

- Default Route Table
- Default Security List
- Default set of DHCP options

You can't delete these default components; however, you can change their contents (for example, individual route rules). Also, you can create more of each kind of component in your cloud network (for example, additional route tables).

OCI VPN: Overview



- OCI VPN securely connects an on-premises network to OCI VCN through an IPSec VPN connection.
- VPN can help a business ensure that its networks provide secure remote connectivity.
- Bandwidth is dependent on the customer's access to the internet and general internal congestion (typically, less than 250 Mbps, but your mileage may vary).
- **VPN service is offered for free.**
- Customer Proofs of Concept usually start as a VPN and then morph into FastConnect designs.
- OCI provisions redundant VPN tunnels located on physically and logically isolate tunnel endpoints.

0

For Instructor Use Only.

This document should not be distributed.

One of the options to securely connect your on-premises network to OCI VCN is to use the IPSec VPN service.

When you create an IPSec VPN connection with your on-premises network, multiple redundant IPSec tunnels are created, which are logically and physically isolated providing complete high availability from the OCI side. We use asymmetric routing across the multiple tunnels that make up the IPSec VPN connection.

Currently, to route the traffic over the IPSec tunnels, we use static routing; BGP is not supported.

As part of creating the IPSec VPN, several components are created. We have already learned about some of them, such as route tables, SL, subnets, and so on, in the foundation module of VCN.

CPE Object: At the customer end of the IPSec VPN is the actual router in its on-premises network, which can be hardware or software. The term customer premises equipment (CPE) is used to refer to this type of on-premises equipment. When setting up the IPSec VPN, you must create a virtual representation of this router. The CPE object contains basic information about your on-premises network that is required.

DRG: We have already talked about this.

IPSec Connection: After creating the CPE object and DRG, you connect them by creating an IPSec connection, which results in multiple redundant IPSec tunnels.



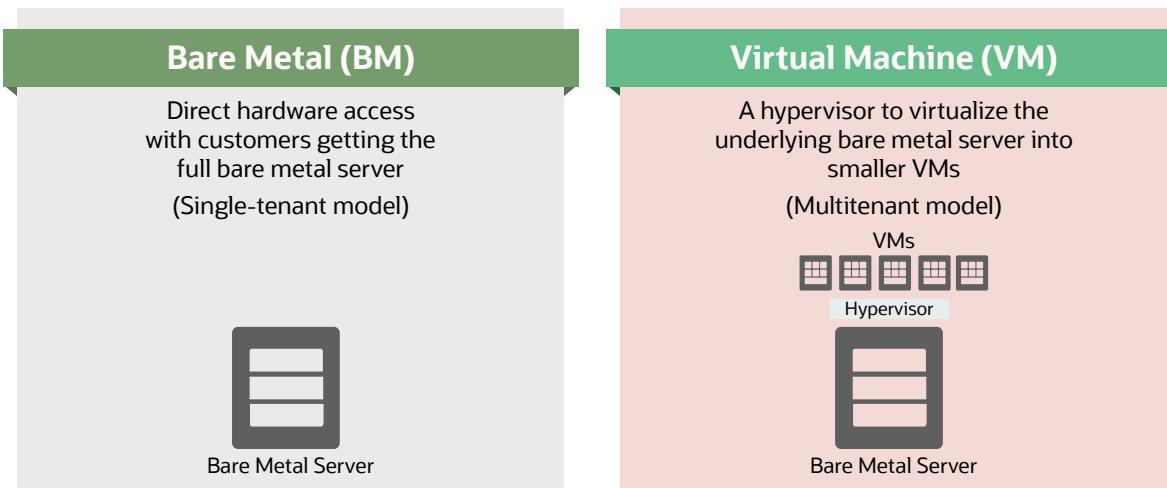
For Instructor Use Only.

This document should not be distributed.

0

Compute Service

Compute: Bare Metal and Virtual Machines



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

8

O

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. At the other end of the spectrum are VMs, where the underlying host is virtualized to provide smaller VMs; this is also referred to as the multitenant model. The advantage here is flexibility with regard to choice of instance shapes.

For Instructor Use Only.
This document should not be distributed.

Shape: Processor and Memory Resources

- Oracle Compute Cloud Service enables you to select from a range of predefined shapes that determine the number of CPUs, amount of RAM, and local storage available in an instance.
- Several predefined shapes are available for both BM and VM instances.

0

9

When creating compute instances, you can assign CPU and memory resources by selecting from a wide range of resource profiles (called shapes), each of which is a carefully designed combination of processor and memory limits.

For information on compute shapes refer to this page:

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

For Instructor Use Only.

This document should not be distributed.

Available Shapes: Bare Metal

Shape	Instance Type	OCPUs	RAM (GB)	Local Disk (TB)	Network Bandwidth	Max vNICs
BM.Standard2.52	X7-based Standard compute	52	768	Block Storage only	2 X 25 Gbps	24
BM.DenseIO2.52	X7-based Dense I/O compute	52	768	51.2 TB NVMe SSD	2 X 25 Gbps	24
BM.Standard1.36	X5-based Standard compute	36	256	Block Storage only	10 Gbps	16
BM.HighIO1.36	X5-based High I/O compute	36	512	12.8 TB NVMe SSD	10 Gbps	16
BM.DenseIO1.36	X5-based Dense I/O compute	36	512	28.8 TB NVMe SSD	10 Gbps	16

- Pricing info: <https://www.oracle.com/in/cloud/compute/pricing.html>
- 2 x 25 Gbps implies two NIC cards with 25 Gbps bandwidth.

Network bandwidth is based on expected bandwidth for traffic within a VCN.

X7-based shapes are available only in IAD.

X7 shapes have two in them and X5 shapes have one.

X5-based shapes' availability is limited to monthly universal credit customers in the us-phoenix-1, us-ashburn-1, and eu-frankfurt-1 regions.

In case of standard VM instances, NVMe storage is not available. For all the shapes, Block Volume storage is offered.

The Dense I/O instances are configured with 28.8 TB of local NVMe storage. They are ideal for extreme transactional workloads that work on large datasets and require low latency and high throughput, such as big data and High Performance Compute (HPC) applications.

Available Shapes: VMs (Current Gen)

Shape	Instance Type	OCPUs	RAM (GB)	Local Disk (TB)	Network Bandwidth	Max vNIC
VM.Standard2.1	Standard	1	15	Block Storage only	1 Gbps	2
VM.Standard2.2	Standard	2	30	Block Storage only	2 Gbps	2
VM.Standard2.4	Standard	4	60	Block Storage only	4.1 Gbps	4
VM.Standard2.8	Standard	8	120	Block Storage only	8.2 Gbps	8
VM.Standard2.16	Standard	16	240	Block Storage only	16.4 Gbps	16
VM.Standard2.24	Standard	24	320	Block Storage only	24.6 Gbps	24
VM.DenseIO2.8	Dense I/O	8	60	6.4 TB NVMe SSD	8.2 Gbps	8
VM.DenseIO2.16	Dense I/O	16	240	12.8 TB NVMe SSD	16.4 Gbps	16
VM.DenseIO2.24	Dense I/O	24	320	25.6 NVMe SSD	24.6 Gbps	24

11

0

For Instructor Use Only.
This document should not be distributed.

Available Shapes: VMs (Previous Gen)

Shape	Instance Type	OCPUs	RAM (GB)	Local Disk (TB)	Network Bandwidth	Max vNIC
VM.Standard1.1	Standard	1	7	Block Storage only	Up to 600 Mbps	2
VM.Standard1.2	Standard	2	14	Block Storage only	Up to 1.2 Gbps	2
VM.Standard1.4	Standard	4	28	Block Storage only	1.2 Gbps	2
VM.Standard1.8	Standard	8	56	Block Storage only	2.4 Gbps	4
VM.Standard1.16	Standard	16	112	Block Storage only	4.8 Gbps	8
VM.DenseIO1.4	Dense I/O	4	60	3.2 TB NVMe SSD	1.2 Gbps	2
VM.DenseIO1.8	Dense I/O	8	120	6.4 TB NVMe SSD	2.4 Gbps	4
VM.DenseIO1.16	Dense I/O	16	240	12.8 TB NVMe SSD	4.8 Gbps	8

Local NVMe SSD Devices

- Some instance shapes in OCI include locally attached NVMe devices.
- Local NVMe SSD can be used for workloads that have high storage performance requirements.
- Locally attached SSDs are not protected and OCI provides no RAID, snapshots, or backup capabilities for these devices.
- Customers are responsible for the durability of data on the local SSDs.

Instance Type	NVMe SSD Devices
BM.DenseIO2.52	8 drives = 51.2 TB raw
VM.DenseIO2.8	2 drives = 6.4 TB raw
VM.DenseIO2.16	4 drives = 12.8 TB raw
VM.DenseIO2.24	8 drives = 25.6 TB raw

```
ubuntu@nvme:~$ lsblk
NAME   MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
sda    8:0    0 46.6G 0 disk
└─sda1  8:1    0 46.5G 0 part /
└─sda14 8:14   0   4M 0 part
└─sda15 8:15   0 106M 0 part /boot/efi
nvme0n1 259:4 0 2.9T 0 disk
nvme1n1 259:5 0 2.9T 0 disk
nvme2n1 259:3 0 2.9T 0 disk
nvme3n1 259:6 0 2.9T 0 disk
nvme4n1 259:7 0 2.9T 0 disk
nvme5n1 259:8 0 2.9T 0 disk
nvme6n1 259:1 0 2.9T 0 disk
nvme7n1 259:0 0 2.9T 0 disk
nvme8n1 259:2 0 2.9T 0 disk
```

13

O

Some instance shapes in Oracle Cloud Infrastructure include locally attached NVMe devices. These devices provide extremely low-latency, high-performance storage that is ideal for big data, OLTP, and any other workload that can benefit from high-performance storage. Note that these devices are not protected in any way; they are individual devices locally installed on your instance. Oracle Cloud Infrastructure does not take images or backup, or use RAID or any other methods to protect the data on NVMe devices. It is your responsibility to protect and manage the durability of data on these devices.

For Instructor Use Only.

This document should not be distributed.



Object Storage Service

0

For Instructor Use Only.

This document should not be distributed.

Object Storage Service

- An internet-scale, high-performance storage platform
- Ideal for storing unlimited amount of unstructured data (images, media files, logs, backups)
- Data managed as objects using an API built on standard HTTP verbs
- Data safely and securely stored or retrieved
- A regional service that is not tied to any specific compute instance



O

15

The Oracle Cloud Infrastructure Object Storage Service is an internet-scale, high-performance durable storage platform that offers reliable and cost-efficient data durability.

The Object Storage Service can store an unlimited amount of unstructured data of any content type, including analytic data and rich content, like images and videos.

Data is managed as objects and not as files or blocks. It is not managed via any storage protocol but rather uses standard HTTP methods, such as HTTP GET, HTTP PUT methods.

Moreover, with Object Storage, you can safely and securely store or retrieve data directly from the internet or you can do it from within the cloud platform using multiple management interfaces that let you easily manage storage at scale.

One last thing to mention about Object Storage is that it is completely independent of the compute server and is a regional service. So, as long as you have the Object Storage endpoints and relative authorization, you can access the data from anywhere.

Common Object Storage Scenarios

- Content Repository
 - Highly available and durable content repository for data, images, logs, videos, etc.
- Archive/Backup
 - Use of Object Storage for preserving data for longer periods of time
- Log Data
 - Application log data for analysis and debugs/troubleshooting
- Large Data Sets
 - Large data, such as pharmaceutical trials data, genome data, and Internet of Things (IoT)
- Big Data/Hadoop Support
 - Use as a primary data repository for big data giving ~50% improvement
 - HDFS connector provides connectivity to various big data analytic engines like Apache Spark and MapReduce

16

HDFS Connector

HDFS: A distributed file system used in Hadoop. HDFS provides high throughput access to application data and is suitable for applications that have large data sets.

The HDFS connector lets your Apache Hadoop application read and write data to and from the Oracle Cloud Infrastructure Object Storage service.

<https://docs.us-phoenix-1.oraclecloud.com/Content/API/SDKDocs/hdfsconnector.htm>

Let's talk about common use cases for Object Storage.

The Object Storage service offers a scalable storage platform which enables you to not only store large data sets but also operate seamlessly, making it an ideal storage solution for big data applications. We also have a Hadoop Distributed File System (HDFS) Connector which lets your Apache Hadoop application read and write data to and from the Object Storage service.

Another common use case is backup or archive, where data is typically written once and read many times. Or the data is to be archived for longer periods of time. The durability and low-cost characteristics of Object Storage tiers make it a perfect platform to store long-living data.

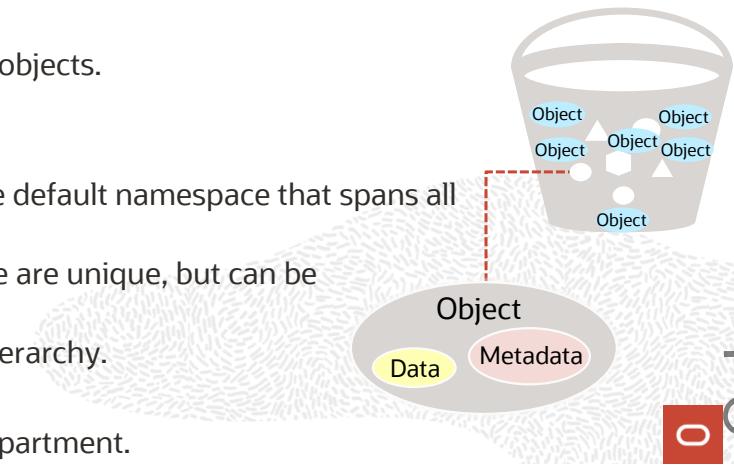
Object Storage can also be used as a content repository for storing different kinds of data and scaling it seamlessly as the data grows.

Additional use cases include log data analysis and storing large data sets.

Object Storage Resources

- Object
 - All data, regardless of content type, is managed as objects (for example, logs and videos).
 - Each object is composed of the object itself and metadata of the object.
- Bucket
 - It is a logical container for storing objects.
 - Each object is stored in a bucket.
- Namespace
 - Each tenant is associated with one default namespace that spans all compartments.
 - Bucket names within a namespace are unique, but can be repeated across namespaces.
 - Buckets and objects exist in flat hierarchy.
- Compartment
 - Buckets can only exist in one compartment.

17



O

Within the Object Storage service, there are some key resources.

As we discussed earlier, all individual data elements are stored as an object, regardless of the content type. Each object is stored in a bucket and is a combination of the object itself and its metadata. The metadata is a list of key value pairs of data (for example, name, size, content type, last modified date, etc.).

A bucket is a logical container created by the user and can contain an unlimited number of objects. A bucket is associated with a single compartment, which in turn defines policies that indicate what actions a user can perform on a bucket.

A namespace is a logical entity that gets created with a tenant and spans all compartments in that tenant. Within a single namespace, the bucket names are unique. Buckets and objects in a namespace are in flat hierarchy, but you can create directory structures for your ease.

For Instructor Use Only.

This document should not be distributed.

Object Storage Service Features

- Strong Consistency
 - Object Storage service always serves the most recent copy of the data when retrieved.
- Durability
 - Data is stored redundantly across multiple storage servers across multiple ADs.
 - Data integrity is actively monitored and corrupt data detected and auto-repaired.
- Performance
 - Compute and Object Storage services are colocated on the same fast network.
- Custom Metadata
 - Define your own extensive metadata as key-value pairs.
- Encryption
 - 256-bit Advanced Encryption Standard (AES-256) is employed to encrypt object data.

18

O

For Instructor Use Only.

This document should not be distributed.

So what are the top Object Storage features?

Object Storage has a strong consistency mode, which means when a read request is made, you are guaranteed a consistent most recent copy of the data that has been completely written in the system. We have a high-performance network where lookups for data are fast and consistent.

To provide durability, the Object Storage service copies object data throughout a region across multiple availability domains. Data integrity is maintained with active scrubbing functions. Typically there are three to six copies of a given object in the service.

The data on the object store is always encrypted. Each object has its own key and then object keys are encrypted with a master key that is frequently rotated so that the encryption scheme is robust.

Object Storage Tiers

- Standard Storage Tier (Hot)
 - Fast, immediate, and frequent access is possible.
 - Object Storage service always serves the most recent copy of the data when retrieved.
 - Data retrieval is instantaneous.
 - Standard buckets can't be downgraded to archive storage.
- Archive Storage Tier (Cold)
 - This is for rarely accessed data that must be retained and preserved for long periods of time.
 - Minimum retention requirement for Archive Storage is 90 days.
 - Objects need to be restored before download.
 - Archive Bucket can't be upgraded to Standard Storage tier.
 - Time To First Byte (TTFB) after Archive Storage restore request is made is 1 hour.

The screenshot shows a 'Create Bucket' dialog box. At the top right are 'help' and 'cancel' buttons. Below them is a note: 'Specify the storage tier for this bucket. Storage tier for a bucket can only be specified during creation.' There are two sections: 'BUCKET NAME' containing the value 'ObjectStorageBucketName' and 'STORAGE TIER' with two options: 'STANDARD' (which is checked) and 'ARCHIVE'. At the bottom is a blue 'Create Bucket' button.

19

o

Currently Object Storage provides two different storage tiers options when creating a bucket.

Standard Storage tiers are for frequently accessed data. Any data stored in this tier is retrieved immediately and instantly. Data accessibility and performance justifies a higher price point to store data in the Standard tier. Once a Standard Storage bucket is created, it can't be downgraded to an Archive Storage tier.

The other option is an Archive Storage tier. This is for data that is not frequently accessed, but must be preserved for longer periods of time.

While storing data in Archive Storage, a minimum 90-day retention period is required. Removal of the data before that results in a penalty fee.

Once the data is uploaded in Archive Storage, it first needs to be restored before it can be accessed. The TTFB is four hours, and total time for full restoration depends on the size of the data stored.



Block Volume Service

0

For Instructor Use Only.

This document should not be distributed.

Block Volume Service

- Block Volume service lets you store data on block volumes independently and beyond the lifespan of compute instances.
- Block volumes operate at the raw storage device level and manage data as a set of numbered, fixed-size blocks using a protocol such as iSCSI.
- You can create, attach, connect, and move volumes, as needed, to meet your storage and application requirements.
- Typical Scenarios
 - Persistent and durable storage
 - Expand an instance's storage
 - Instance scaling

O

To understand the service, let's begin by understanding what block volume is. Block volume is a type of data storage that is more expansive than file storage. It uses the iSCSI Ethernet protocol to deliver features and performance similar to on-premises storage area networks or SANS and are designed for the security and durability of the data life cycle. Using this service, you can create block volumes and attach them to your compute instance.

The Oracle Cloud Infrastructure Block Volume service delivers a simple, scalable service that fulfills all your workload performance needs. The service lets you dynamically provision and manage block storage volumes. You can create, attach, create backups, and move volumes, as needed, to meet your storage and application requirements.

Once attached and connected to an instance, you can use the volume like a regular hard drive. The service also lets you store data on blocked volumes, manage block volumes, control your data, and achieve the storage configuration your application requires.

Block Volume service utilizes industry-leading highest performance NVMe drives and is offered over the network using standard iSCSI protocol.

Some of the typical scenarios for block volume service include:

Expanding an instance storage: Typically block volumes are used to increase an instance storage. Once any compute instance is launched, you can attach block volumes to the instance, increasing the instance's storage capacity.

Persistent and durable storage: Block volumes can be detached from one instance and reattached to another without any loss of data. This data persistence allows the user to safely migrate the data between the instances, and also store it safely even when it is not attached to an instance.

Additionally, block volumes offer a high level of data durability compared to locally attached drives. All volumes are automatically replicated for you, helping to protect against data loss.

Instance scaling: With new features like boot volume, the service allows scaling of the instance CPUs keeping the data secure in the process. We will talk about this later in the lesson.

One important thing to remember is that block volume is always associated with an instance; therefore, it is always created within an availability domain. That is why it is an AD construct.

For Instructor Use Only.

This document should not be distributed.

Block Volume Service Components

The components required to create a volume and attach it to an instance are as follows:

- Instance:
 - An Oracle Cloud Infrastructure compute host
- iSCSI:
 - A TCP/IP-based standard used for communication between the instance and the attached volume
- Volume:
 - Block Volume: A detachable block storage device that allows you to dynamically expand the storage capacity of an instance
 - Boot Volume: A detachable boot volume device that contains the image used to boot a compute instance

23

O

Let's talk about the Block Volume service components.

An instance is a compute resource in OCI (VM or bare metal).

As discussed earlier, block volumes use the standard iSCSI protocol for communication between the host and the block volumes.

There are two types of volumes.

Block volume is a detachable block storage device that you attach to an instance once the instance is launched.

Boot volume is a recently announced feature of the Block Volume service. Whenever you launch a bare metal or virtual instance with an Oracle-provided image or custom image, a new boot volume is automatically launched in the same compartment containing the image used to boot that instance. This boot volume is associated with the instance that is launched.

We will talk more about boot volume later in the deck.

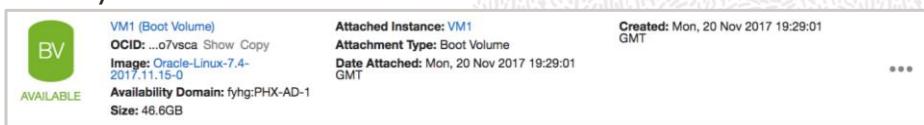
For Instructor Use Only.

This document should not be distributed.

Boot Volumes: Manageable Boot Disks for Compute Instances

All Oracle Cloud Infrastructure compute instances are now launched with manageable boot volumes, provided by the Block Volume service, as their system boot disks. Boot volumes offer the following features:

- Ability to preserve your boot disk content by keeping it when you terminate a compute instance
- High durable boot disks by creating multiple replicas across the AD
- Compute instance scaling via boot volumes
- Faster launch times for Linux and Windows VMs
- All boot volumes encrypted by default
- Ability to troubleshoot and repair your boot disks and OS images by using Block Volume detach/attach features



24

O

We briefly discussed boot volumes earlier.

When any instance is launched (virtual machine or a bare metal) on an Oracle-provided image or a custom image, a new boot volume for the instance is created in the same compartment. That boot volume is associated with that instance until you terminate the instance. When you terminate the instance, you have the option of preserving the boot volume and its data. This feature gives you more control over the boot volumes of your compute instance. For instance, it gives you the ability to preserve your boot disk content by keeping it when you terminate a compute instance. You can use the preserved boot volume for new instance creation.

Just as block volumes are replicated across ADs, the boot volumes are also highly durable as they are automatically replicated across ADs.

Boot volumes can also help in instance scaling. Since you can preserve the boot volume when terminating an instance, the preserved boot volume can be used with a new instance of different shape, which can have more OCPUs.

The launch times are much faster than earlier.

All boot volumes are encrypted at rest like block volumes.

They also help us in troubleshooting or repairing boot disks.

To use boot volumes, there is nothing special that one needs to do. Moving forward, all instances that are launched will be done using boot volumes with all the features we have talked about.



Load Balancing Service

0

For Instructor Use Only.

This document should not be distributed.

OCI Load Balancing Service

- Provides automated traffic distribution from one entry point to multiple servers in a VCN
- Improves resource utilization, facilitates scaling, and helps ensure high availability
- Supports public and private load balancers
- Public load balancer service regional in scope and requires two ADs
- Protocols supported: TCP, HTTP/1.0, HTTP/1.1, HTTP/2, WebSocket
- Supports SSL termination, end-to-end SSL, and SSL tunneling
- Supports session persistence and content-based routing
- Key differentiators:
 - Private or public load balancer (with public IP address)
 - Provisioned bandwidth: 100 Mbps, 400 Mbps, 8 Gbps
 - Single load balancer for TCP (layer 4) and HTTP (layer 7) traffic

26

Oracle Cloud Infrastructure Load Balancing service provides an automated traffic distribution from one entry point into multiple back-end servers in your Virtual Cloud Network.

This helps to load balance large amounts of traffic that could overwhelm a single server. It gives a mechanism to scale out an application tier by adding more servers, and also provides the application higher availability so even if one availability domain has an issue, you can still be up and running in other ADs.

Load balancer is a regional service. Load balancers come in pairs, active and passive, and public load balancers live in two separate availability domains providing HA, with no single point of failure.

The OCI Load Balancing service supports TCP and the usual http protocols, as well as HTTP/2 and WebSocket, supporting features like data compression, server push, and multiplexing of requests.

For security purposes, it supports SSL offloading, SSL termination, end-to-end SSL, and SSL tunneling.

Let's talk about the key differentiators of the Load Balancing service.

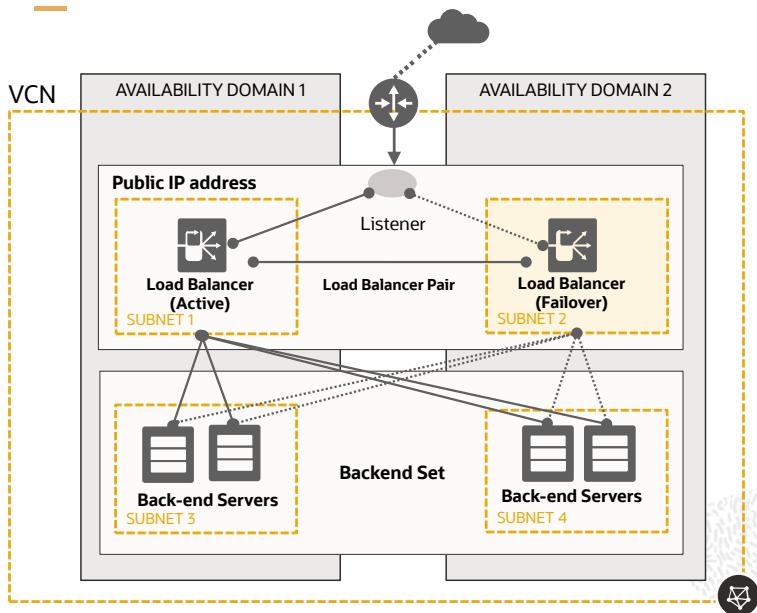
1. We can deploy the service either as public facing where a listener is running on the public IP and back-end servers are on the inside.

We can also use the same service to load balance within OCI between tiers keeping it entirely private.

2. The other nice feature of the OCI Load Balancing service is that you get a public or a dedicated IP address. You don't have to worry about getting a CNAME and dealing with that to use this service. The listener listens on the service port on this IP address and it is mapped to the user's OCI tenancy.
3. Load balancers come in three sizes: 100 Mbps, 400 Mbits, and 8 Gbits. These sizes are for aggregate throughput. The good thing about having this much capacity provisioned is that it is always available to the user. There is no warm-up period required when using these shapes; this aggregate throughput performance is always available.
4. There is a single load balancer for HTTP and TCP. This makes the service easier to use in general.

For Instructor Use Only.
This document should not be distributed.

Public Load Balancer



28

- Public load balancer accepts traffic from the internet using a public IP address that serves as the entry point for incoming traffic.
- Regional load balancer
- Requires two subnets, each in a separate AD: Subnet 1—primary load balancer; Subnet 2—standby load balancer for high availability in case of an AD outage
- Public IP is attached to Subnet 1; load balancer and IP switch to Subnet 2 in case of an outage.
- The service treats the two load balancer subnets as equivalent; you cannot denote one as “primary.”

O

Let's move forward and discuss how the Load Balancing service works.

There are two kinds of LBs: public LB and private LB. Let's talk first about the public LB.

When you create a public LB, you select two ADs for the LB to reside in. In this case this LB lives in AD1 and AD2. Because OCI is going to create two copies of the LB to make the service highly available, you need to have two subnets (Subnet 1 and Subnet 2). After creation, the public load balancer sits at the edge of a VCN.

What happens next is that a primary load balancer is selected automatically to hold the public IP and a secondary load balancer in an active/standby configuration. This is completely invisible to the user; there is no requirement or capability to designate primary or secondary LB. Next we have a listener. This is the public IP address and the service ports that are opened up to sit between the internet and your back-end servers.

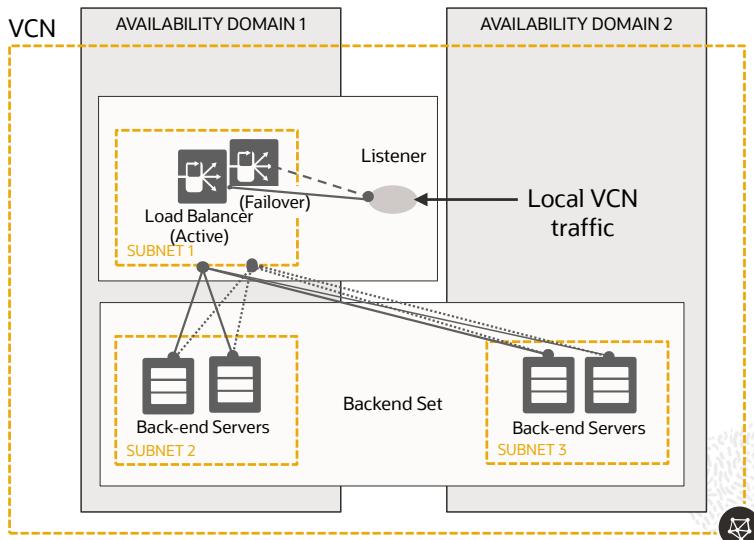
In case one of the ADs goes down, the listener will failover to the other AD automatically; where we see a dotted line up at the top will be the new path for the traffic.

This HA is built in; the user doesn't have to manage the HA. Remember there is no way or reason to change which LB is acting as the primary load balancer. It is all managed by the service itself.

The second type of LB is a private LB.

For a private load balancer the implementation is a bit different. Two copies of the LB go into a single subnet into a single AD. So it doesn't give you HA in case of AD outage. However, apart from this, all other capabilities are the same.

Private Load Balancer



29

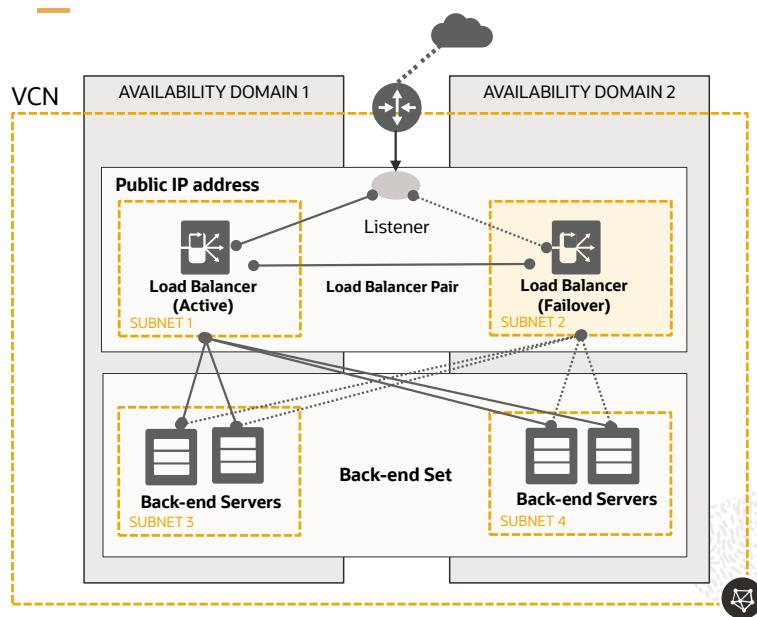
- Assigned a private IP address from the subnet hosting the load balancer
- Highly available within an AD
- The primary and standby load balancers each require a private IP address from that subnet.
- The load balancer is accessible only from within the VCN that contains the associated subnet, or as further restricted by your security list rules.

0

For Instructor Use Only.

This document should not be distributed.

Concepts



30

- **Back-end Server:** Application server responsible for generating content in reply to the incoming TCP or HTTP traffic
- **Backend Set:** Logical entity defined by a list of back-end servers, a load balancing policy, and a health check policy
- **Load Balancing Policy:** Tells the load balancer how to distribute incoming traffic to the back-end servers
 - round-robin
 - IP hash
 - least connection
- **Health Checks:** A test to confirm the availability of back-end servers
 - TCP-level health checks
 - HTTP-level health checks
- **Listener:** Entity that checks for incoming traffic on the load balancer's IP address

O

For Instructor Use Only.

This document should not be distributed.

Let's move forward and discuss how the Load Balancing service works.

There are two kinds of LBs, a public LB and a private LB. Let's first talk about the public LB.

When you create a public LB you select two ADs for the LB to reside in; in this case this LB lives in AD1 and AD2. Because OCI is going to create two copies of the LB to make the service highly available, you need to have two subnets (subnet 1 and subnet 2). After creation, the public load balancer sits at the edge of a VCN.

What happens next is that a primary load balancer is selected automatically to hold the public IP and a secondary load balancer is in an active/standby configuration. This is completely invisible to the user; there is no requirement or capability to designate primary or secondary LB. Next we have a listener. This is the public IP address and the service ports that are opened up to sit between the internet and your back-end servers.

In case one of the ADs goes down, the listener will automatically failover to the other AD; where we see a dotted line at the top will be the new path for the traffic.

This HA is built in; the user doesn't have to manage this HA. Remember there is no way or reason to change which LB is acting as the primary LB. It is all managed by the service itself.

The second type of load balancer is a private LB.

For a private load balancer the implementation is a bit different. Two copies of the load balancer go into a single subnet into a single AD. So it doesn't give you HA in case of AD outage. However, apart from this, all other capabilities are the same.

Load Balancing Service: Shapes

A template that determines the load balancer's total pre-provisioned maximum capacity (bandwidth) for ingress plus egress traffic. Available shapes are:

100 Mbps	400 Mbps	8000 Mbps
Process 100 Mbps total bandwidth when multiple clients connected	Process 400 Mbps total bandwidth when multiple clients connected	Process 8000 Mbps total bandwidth when multiple clients connected
Key characteristics: Up to 1K SSL handshakes per sec with cipher (ECDHE-RSA2K)	Key characteristics: Up to 4K SSL handshakes per sec with cipher (ECDHE-RSA2K)	Key characteristics: Up to 40K SSL handshakes per sec with cipher (ECDHE-RSA2K)

31

0

As we discussed before, these are the three shapes available for the Load Balancing service. The sizes are for aggregate capacity, and you can also see the scaling SSL handshakes.

ECDHE is Elliptic Curve Diffie–Hellman Exchange, an encrypted key exchange standard.



For Instructor Use Only.

This document should not be distributed.

0

OCI DNS Service

Oracle Cloud Infrastructure: DNS

- Highly scalable, global anycast Domain Name System (DNS) network that ensures high site availability and low latency
- Customers can manage DNS records; domain names can be either cloud or non-cloud resources
- OCI DNS service is used when:
 - Domains and zones need to be exposed via the internet for DNS resolution
 - Domains and zones can reside in both Enterprise on premises and OCI environments
 - DNS traffic needs to be intelligently handled across multiple resources

33

The Dyn network (Managed DNS, Email Delivery, Internet Guide) is deployed on top of a global IP network, consisting of 20 existing facilities and connectivity from a mix of Tier 1 Internet Service Providers (ISPs).

The network has been split into two diverse constellations to provide active/active failover between constellations in the event of catastrophic failure.

Within each constellation, we distribute traffic to multiple data centers, providing global active-active load balancing using the anycast routing technique. Queries via the anycast technique allow the fastest of the entire network to answer the query.

This network allows OCI DNS/Dyn DNS to offer its customers an industry-leading level of service and reliability.

The network continues to grow and add more points of presence.

This results in a superior end-user experience connecting to OCI.

By configuring OCI DNS, enterprise and business customers can connect their DNS queries to various kinds of assets such as OCI Compute, as well as to third-party and private assets.

Operators can manage their own DNS records for both cloud and non-cloud resources.

OCI DNS is used when zones need to be exposed to the internet for resolution.

Domains and zones can be both on OCI environment and in the enterprise.

DNS needs to be handled across multiple resources.

DYN can also act either as a primary or secondary DNS and follow DNS specifications carefully and by the appropriate RFC whenever possible.

Capabilities of OCI DNS

The following functions are available:

- Creating and managing zones
- Creating and managing records
- Importing/uploading zone files
- Zone transfer
- Saving and publishing changes
- Viewing all zones
- Query counts: total and per zone

Domain	TTL	Type	RDATA
ocitraining.net	300	SOA	ns1.p68.dns.oraclecloud.net hostmaster.ocitraining.net. 2 3600 600 604800 1800
ocitraining.net	86400	NS	ns4.p68.dns.oraclecloud.net
ocitraining.net	86400	NS	ns1.p68.dns.oraclecloud.net
ocitraining.net	86400	NS	ns2.p68.dns.oraclecloud.net

34

O

OCI DNS service offers a complete set of functions for zone management within the user interface.

It is possible to create zones within the tenancy. Zones are tenancy-wide and along with IAM OCI DNS crosses all regions.

Users can also manage records from the consoles.

It is also possible to import complete zones via the OCI DNS console.

It is possible to set up OCI DNS as a secondary server and facilitate zone transfers from the primary DNS server.

OCI DNS supports zone transfers via AXFR (full) or IXFR (incremental) zone transfer.

OCI DNS keeps track of all queries against the service, both at the zone level and total.

Summary

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

- Key Virtual Cloud Network (VCN) concepts
- OCI Compute service
- Object Storage service
- Block Volume service
- Oracle Cloud Infrastructure Load Balancing service concepts
- OCI DNS services available with Oracle Cloud Infrastructure

O



For Instructor Use Only.

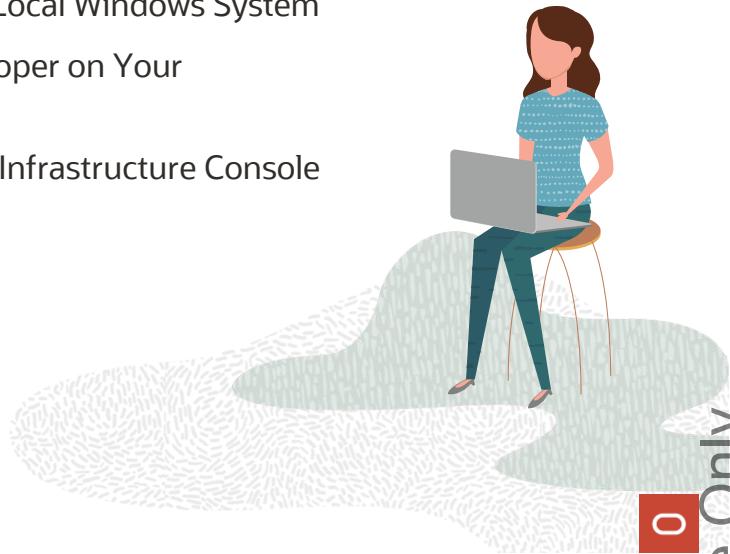
This document should not be distributed.



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



0

For Instructor Use Only.

This document should not be distributed.



Oracle Cloud Infrastructure: Database Service

5

0

For Instructor Use Only.

This document should not be distributed.

Objectives

After completing this lesson, you should be able to:

- Describe the options for database systems available with Oracle Cloud Infrastructure
- Describe the features of the Database Service
- Launch a one-node database system



0

2

In this lesson we will look into the 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 DB systems, and, finally, how to launch an instance.

For Instructor Use Only.
This document should not be distributed.

Oracle Cloud Infrastructure: Database Service

- Mission-critical, enterprise-grade cloud database service with comprehensive offerings to cover all enterprise database needs
 - Exadata, RAC, bare metal, VM
- Complete Life Cycle Automation
 - Provisioning, patching, backup, and restore
- High Availability and Scalability
 - RAC and Data Guard
 - Dynamic CPU and storage scaling
- Security
 - Infrastructure (IAM, security lists, audit logs)
 - Database (TDE, RMAN backup/block volume encryption)
- OCI Platform Integration
 - Tagging, limits, and usage integration
- Bring Your Own License (BYOL)



0

3

At a very high level there are three types of DB systems offered by Oracle Cloud Infrastructure. The first type, the bare metal database system, comes in a single-node shape. The second type of system is the VM-based shape that supports 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 (ADs) and multiple regions. Currently active redundancy can be implemented with features such as Data Guard configured to operate across ADs.

The networking that backs these database systems, along with every other system in OCI, is a fully non-blocking, fully contextualized (multitenant 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 two- or three-way mirroring.

For Instructor Use Only.

This document should not be distributed.

The DB systems can be brought up stand alone 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 role-based controls.

There are 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 the Console.

At the database level encryption is 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 in OCI can be managed by tools such as Enterprise Manager, SQL Developer, etc., just as a regular on-premises database.

=====

Robust Infrastructure

Three Availability Domains: Region architecture

Fully redundant and non-blocking Clos networking fabric

three-way mirrored storage (optional two-way mirroring) for the 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

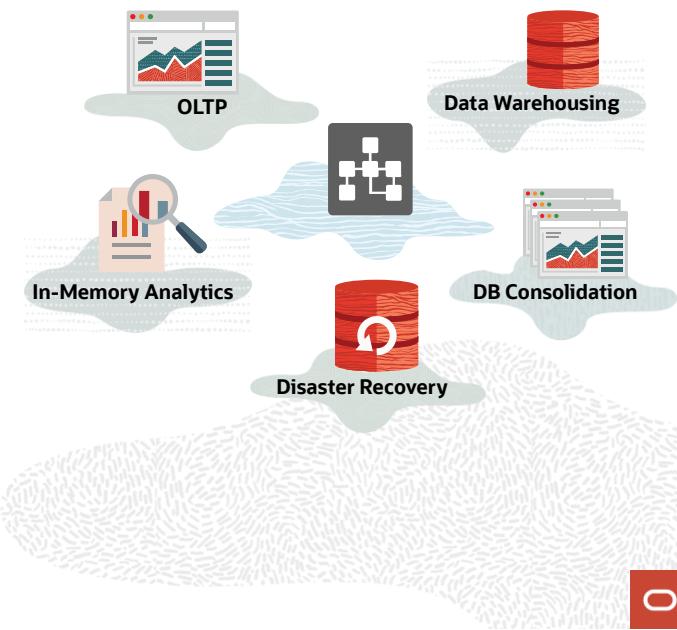
Encrypted backup in Object Store

Secure client communication thru SQLNet

Mention: bring your own license.

Database Service: Use Cases

- Mission-Critical Production Databases
 - Very large databases (VLDB)
 - Database consolidation
 - OLTP, data warehousing, analytics, reporting
 - Apps Unlimited (EBS, test, development, certification, try before you buy)
- Disaster Recovery
- Migration of Database to Cloud



5

O

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, 5.7 TB of RAM, 150 TB of flash, 1.1 PB of raw disk, and 330 TB of usable storage with three-way mirroring.

Database consolidation, with containerized DBs (CDBs and PDBs); the database has been written with database consolidation in mind.

OLTP, data warehousing, analytics, and reporting

The Database service is ideal to bring Applications Unlimited to the cloud: E-business Suite, JD Edwards, PeopleSoft, and Siebel. All these applications 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 system shapes without having to deal with procurement to see how performance would be on an Exadata.

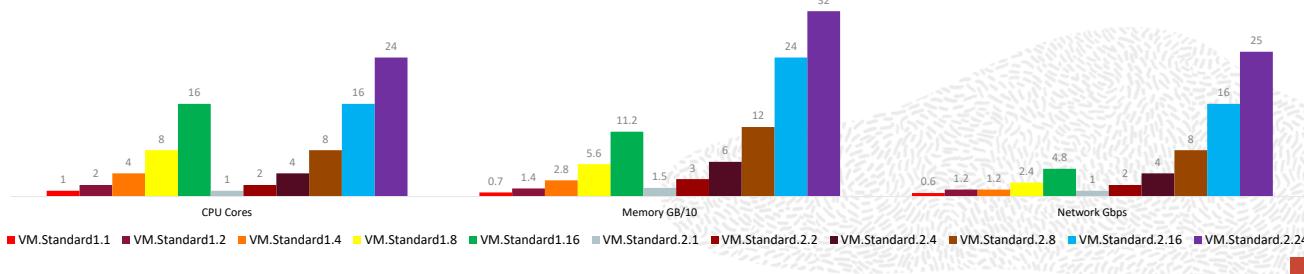
Database systems on OCI can be managed with existing tools such as enterprise manager/cloud control, same as on-premises systems. DB systems can be configured with Data Guard, Data Pump, and GoldenGate, work with RMAN, back up to Object Storage, etc. There is flexibility.

Virtual Machine DB Systems

Platform	CPU Core	Memory	Storage	Network	RAC Interconnect	Nodes
VM (X5)	1-16	7-112 GB	256 GB-40 TB	0.6-4.8 Gbps	0.6-4.8 Gbps	1-2
VM (X7)	1-24	15-320 GB	256 GB-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 downtime
- VM.Standard2 shapes have ~100% more IOPS than VM.Standard1 shapes



6

O

First, we can look at the Database service on VMs.

Database on VMs offers a wide range of flexibility.

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

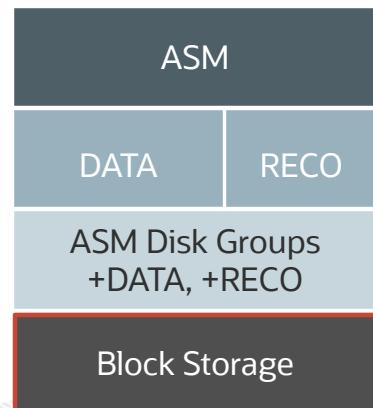
VM-based Database shapes can accommodate these workloads.

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.

<https://docs.cloud.oracle.com/en-us/iaas/Content/Database/Concepts/overview.htm#vmShapes>

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 Block Storage.
- These actions ensure the highest level availability and performance at all times.



7

0

Storage in 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 the same way as these disks.

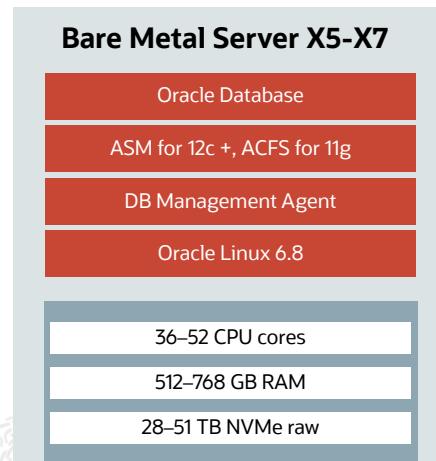
Any disks that fail will be managed. Space is reserved for rebalancing so the amount of free space is actually calculated based on that reservation. Whenever the shapes list a maximum amount of usable space in DATA and RECO, these reservations for rebalancing are already taken into account.

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

For Instructor Use Only.
This document should not be distributed.

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)
 - Start with two cores and scale up/down OCPUs based on requirement.
 - Data Guard within and across ADs
 - If single node fails, launch another system and restore the databases from current backups.



8

0

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 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

BM.DenseIO2.52

- 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

BM.DenseIO1.36

- 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

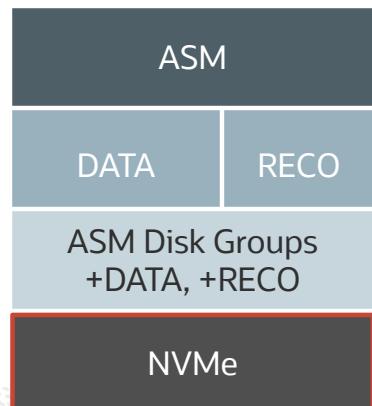
Shapes for 1- and 2-Node RAC DB Systems

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 16 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 the disks for hard and soft failures
- Proactively off-lines disks that failed, predicted to fail, or are performing poorly and performs corrective actions, if possible
- On disk failure, the DB system automatically creates an internal ticket and notifies the internal team to contact the customer.
- ASM manages mirroring of NVMe disks.
- Disks are partitioned: one for DATA and one for RECO.
- These actions ensure the highest level availability and performance at all times.



10

0

Storage in 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 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 are possible but the service sets these up by default in an optimal way.

For Instructor Use Only.
This document should not be distributed.

Exadata DB Systems

- Full Oracle Database with all advanced options
- On the 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



11

0

In addition to VMs, bare metal hosts, and bare metal RAC and VM, Exadata is available on OCI.

The Exadata systems are provided in three 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-premises Exadata but with the flexibility of the cloud.

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

Exadata DB X7 Systems

- Oracle manages Exadata infrastructure: servers, storage, networking, firmware, hypervisor, etc.
- You can specify zero cores when you launch Exadata; this provisions and instantly stops Exadata.
- You are billed for the Exadata infrastructure for the first month, and then by the hour after that. Each OCPU you add to the system is billed by the hour from the time you add it.
- Scaling from $\frac{1}{4}$ to a $\frac{1}{2}$ rack, or from $\frac{1}{2}$ to a full rack requires that the data associated with database deployment is backed up and restored on a different Exadata DB system.

Resource	Quarter Rack			Half Rack			Full Rack		
	X6	X7	X8	X6	X7	X8	X6	X7	X8
Number of Compute Nodes	2			4			8		
Total Minimum (Default) Number of Enabled CPU Cores	22	0	0	44	0	0	88	0	0
Total Maximum Number of Enabled CPU Cores	84	92	100	168	184	200	336	368	400
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	76.8 TB	153.6 TB	179.2 TB	153.6 TB	307.2 TB	358.5TB
Total Usable Storage Capacity	84 TB	106 TB	149 TB	168 TB	212 TB	299 TB	336 TB	424 TB	598 TB

12

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

In this table you can see the usable storage capacity and RAM for each of the configurations.

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

Each compute node is 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 setup, and you control the recovery process in the event of a database failure.

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

<https://docs.cloud.oracle.com/en-us/iaas/Content/Database/Concepts/exaoverview.htm#SystemConfiguration>

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

All of the VCN 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.

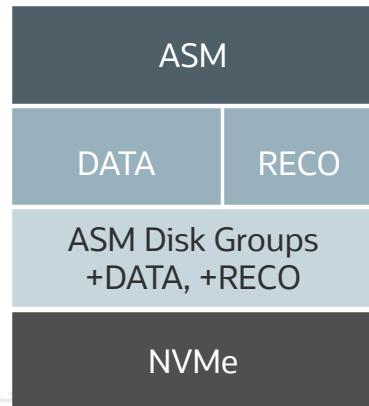
You can use VPN and FastConnect to connect to your on-premises environments.

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.

For Instructor Use Only.
This document should not be distributed.

Exadata DB Systems Storage Architecture

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



14

0

Storage in 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.

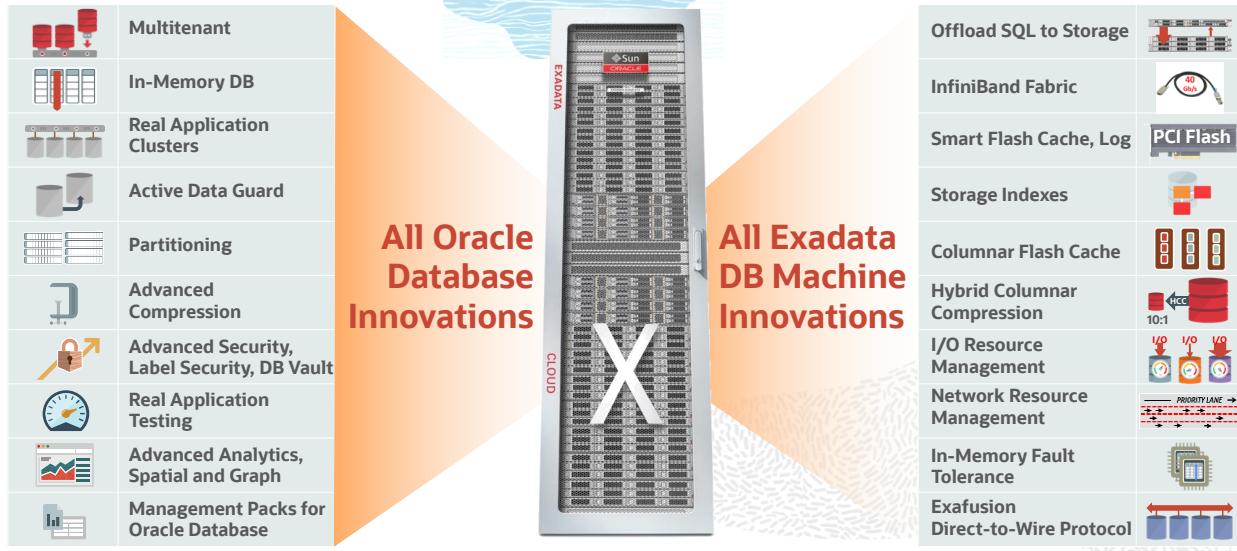
Storage is continuously monitored for any failures with the disks; these disks refer to NVMe and SSDs. In the case of VM shapes block volume is used—which is NVMe based—and multiple block volumes are brought in and managed the same way as these disks.

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 are possible but the service sets these up by default in an optimal way.

Exadata Cloud Enterprise Edition Extreme Performance Most Powerful Database + Platform

15



O

For Instructor Use Only.

This document should not be distributed.

Scaling Exadata DB Systems

Two ways of scaling Exadata DB systems

- Scaling across Exadata DB system configurations:

Lets you move to a different configuration (for example, from a quarter rack to a half rack)

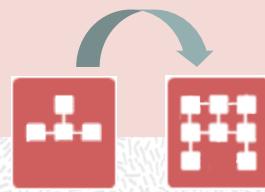
- Requires movement of database deployment
- Planned and executed in coordination with Oracle



- Scaling within an Exadata DB system:

Lets you modify the compute node processing power within the system

- Can be done without disruption
- Can be accomplished by the customer



16

0

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 enable 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 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.

17

0

First, we can look at the Database service on VMs.

Database on VMs offers a wide range of flexibility.

Not all workloads need dedicated bare metal servers. Customers ask for a cost-effective, easy-to-get-started, and durable database option well suited for a variety of workloads ranging from proof of concept, development and 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	
Enterprise Edition	Yes	Yes	No	11.2.0.4 12.1.0.2 12.2.0.1
High Performance	Yes	Yes	No	18.9.0.0 19.6.0.0 21.0.0.0
Extreme Performance	Yes	Yes	Yes	
BYOL			Yes	

With OCI Database Service there are six main latest versions of the Database available: 11.2, 12.1, 12.2, 18.9, 19.6, and 21.0.

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
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).

Managing DB Systems

You can use the Console to perform the following tasks:

- Launch a DB system: You can create a database system.
 - Status check: You can view the status of your database creation, and after that, you can view the runtime status of the database.
- Start, stop, or reboot DB systems.
 - Billing continues in stop state for BM DB systems (but not for VM DB).
- Scale CPU cores: Scale up the number of enabled CPU cores in the system (BM DB systems only).
- Scale up storage: Increase the amount of Block Storage with no impact (VM DB systems only).
- Terminate: Terminating a DB system permanently deletes it and any databases running on it.

Now that we have an overview of the Database service on OCI, we can move on to the hands-on lab.

Launching a database system is done through the Console.

Open the Console, click Database tab under DB Systems, make sure your compartment is set correctly, and then start the Launch DB System process.

In the Launch DB System dialog box, enter or select the appropriate values:

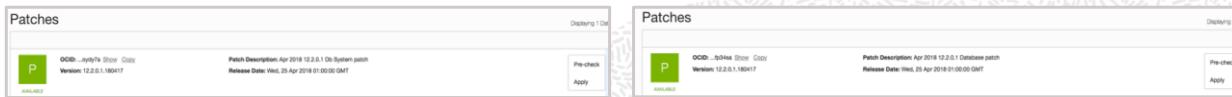
- DB System Information
- DISPLAY NAME
- AVAILABILITY DOMAIN
- SHAPE
- VM, BM, RAC, Exadata
- ORACLE DATABASE SOFTWARE EDITION
- CPU CORE COUNT
- LICENSE TYPE (Included, BYOL)
- SSH PUBLIC KEY
- DATA STORAGE PERCENTAGE (DATA:RECO Split) (40/80)

- DISK REDUNDANCY (Normal (2-way mirror)|HIGH (3-way mirror))
- VIRTUAL CLOUD NETWORK
- CLIENT SUBNET
- HOSTNAME PREFIX
- DATABASE NAME (CDB)
- DATABASE VERSION
- PDB NAME
- DATABASE ADMIN PASSWORD
- AUTOMATIC BACKUP ON|OFF
- DATABASE WORKLOAD
- ON-LINE TRANSACTION PROCESSING (OLTP)/ DECISION SUPPORT SYSTEM (DSS)
- CHARACTER SET
- NATIONAL CHARACTER SET

While the task of launching a database is quite simple, you should plan your database implementations with your database architects.

Patching DB Systems

- **Automated Applicable Patch Discovery:** Automatic patch discovery and pre-flight checks/tests
- **On-Demand Patching:** N-1 patching (previous patch is available if it hasn't been applied), pre-check, and patching at the click of a button
- **Availability during Patching:** For Exadata and RAC shapes, patches are rolling. For single-node systems if Active Data Guard is configured this can be leveraged by the patch service.
- **Two-Step Process:** Patching is a two-step process, one for the DB system and one for the database. The DB system needs to be patched first before the database is patched.
- **Identity and Access Controls:** Granular permissions – it's possible to control who can list patches, apply them, etc.

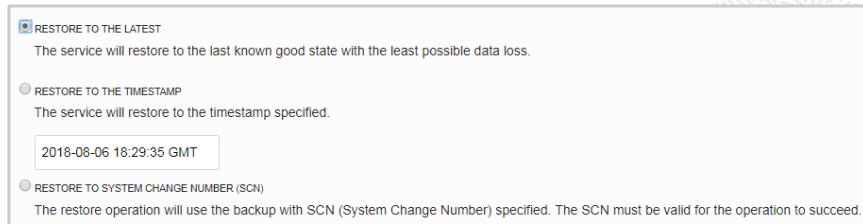


22

For Instructor Use Only.
This document should not be distributed.

Backup/Restore

- Managed backup and restore feature for VM/BM DB systems; Exadata backup process requires creating a backup config file.
- Backups stored in Object or Local Storage (recommended: Object Storage for high durability)
- DB system in private subnets can leverage Service Gateway.
- Backup options
 - Automatic incremental: runs once/day, repeats the cycle every week; retained for 30 days
 - On-demand, standalone/full backups
- Restore a DB.



23

Database Service: Backup/Restore

OCI Database service is a critical service for Oracle Cloud Infrastructure.

OCI's ability to provide a simple and seamless experience in managing the backup/restore policies for their databases make it easy, simple, and safe to move to the cloud while being fully supported.

Migration: There are many options to migrate from on-premises to the cloud.

Oracle certification: Database backup management adhering to Oracle's standard best practices while not compromising on the patterns and the flexibility that Oracle DBAs follow on premises today

Reduce DBA overhead: Offers a completely managed database backup/restore experience: configuring the backup policy, requesting on-demand backups for databases, restoring databases, or moving data.

IAM Integrated: Operators can also grant granular access for these actions for their DBAs using IAM.

Migrate On-Premises Database and Restore in OCI

OCI operators should be able to easily back up their databases from on premises and restore them in the cloud.

In addition to offering a complete Console and API experience OCI is also developing scripts to be executed on the on-premises Database instance set which has the database that needs to be transferred to OCI. These scripts will ask for credentials to log into the OCI tenancy and then invoke RMAN to back up the database.

After this operation is complete, the user will be able to log into OCI Database backup as a “restorable” entity.

At this point, OCI users can follow the “restore database from backup” workflow to recreate the database.

List backups

Customers need the ability to list all the backups for a given database with metadata (timestamp, tag, name, Database OCID, DB System OCID) that allows them to easily identify the source of the backups.

How does the Backup/Restore functionality work?

The Database service completely manages the backups on the customer’s behalf and places the backups in a DBaaS Control Plane managed tenancy. The following points illustrate the design decisions that have been taken around how DBaaS Control Plane managed backups will work.

DBaaS Managed Backup Tenancy: One DBaaS-owned tenancy would be created per region for managing the backups. This tenancy will host all the database backup resources including users, groups, policies, and buckets for all customer tenancies in that region.

Object Storage Backup User Credentials: For every database, one user will be created in the DBaaS tenancy. The database backup operation is performed on the DB system via the database software (RMAN). Current version of RMAN uses Swift-based authentication to authenticate/authorize with Casper. Hence, we use the “swift based” backup user to be allowed in the IAM policy to LIST, READ, WRITE, and DELETE objects in the Casper bucket to be used for database backup. We will not create any IAM resources (users, groups, policies, and buckets) in the customer’s tenancy.

Note: This step will go away with the availability of Instance Principals and RMAN support for token-based authentication.

Customer Tenancy–Compartment mapping: Every customer tenancy that has DB systems will be mapped to a compartment in DBaaS Backup tenancy. This will be a 1:1 relationship between CustomerTenancy:DbaaSSTenancyCompartment.

Database–Object Storage Bucket mapping: One Object Storage bucket will be created in the relevant compartment for every database. To leverage a simple policy language experience, the bucket name and the user name will be the same.

IAM policy for access control: A single policy statement at the tenancy level will be added to allow the corresponding user access to the bucket.

Allow any-user to use object-family in tenancy where target.bucket.name = request.user.name

DB System Backup Configuration: Once the above is complete, the backup user credentials will be configured on the DBaaS Host for performing backup for the database.

Automatic Backups

- By default, automatic backups are written to Oracle-owned Object Storage (customers will not be able to view the object store backups).
- Default policy cannot be changed at this time.
- The backup window is defined by Oracle.
- Backup jobs are designed to be automatically retried.
- Oracle automatically gets notified if a backup job is stuck.
- All backups to cloud Object Storage are encrypted.
- Link to troubleshooting backup issues:
<https://docs.us-phoenix-1.oraclecloud.com/Content/Database/Troubleshooting/Backup/backupfail.htm>

25

0

For Instructor Use Only.

This document should not be distributed.

High Availability and Scalability

- Robust Infrastructure
 - Region with three Availability Domains architecture
 - Fully redundant and non-blocking networking fabric
 - two-way or three-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

26

O

Oracle Database Service is built for availability and scalability.

Backups are hosted on regional services like Object Storage, which span ADs.

Data Guard can be implemented across ADs 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 set up 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 there is the ability to create highly available database instances - from VMs to Exadata.

With Data Guard there is the ability to stretch the availability of the database pair across availability domains.

The Database systems are fully managed by Oracle and follow Maximum Availability Architecture (MAA); 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 virtual machine and bare metal DB systems
- Limited to one Standby database per Primary database on OCI
- 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, or SQL*Plus
- Failover
 - Unplanned failure of Primary
 - Flashback database used to reinstate original Primary
 - Manually invoked via Enterprise Manager, DGMGRL, or SQL*Plus
 - May also be done automatically: Fast-Start Failover

27

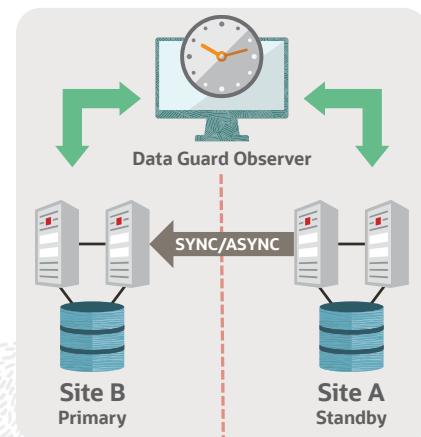
0

For Instructor Use Only.

This document should not be distributed.

Data Guard

- Run Primary, Standby, and Observer in separate ADs. Observer determines whether or not to failover 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.



0

For Instructor Use Only.
This document should not be distributed.

OCI Security Features Overview for Database Service

Security Capability	Features
Instance security isolation	BM DB systems
Network security and access control	VCN, security lists, VCN public and private subnets, route table, service gateway
Secure and highly available connectivity	VPN DRGs, VPc, FastConnect
User authentication and authorization	IAM tenancy, compartments and security policies, Console password, API signing key, SSH keys
Data encryption	DBaaS TDE, RMAN encrypted backups, local storage, Object Storage encryption at rest
End-to-end TLS	LBaaS with TLS1.2, customer-provided certificates
Auditing	OCI API audit logs

29

0

In subsequent lessons we will look at key features of Oracle Cloud Infrastructure Security.

For Instructor Use Only.
This document should not be distributed.

Summary

In the lesson, you should have learned how to:

- Describe the options for database systems available with Oracle Cloud Infrastructure
- Describe the features of Database service
- Launch a one-node database system

 A red square containing a white checkmark icon.

0

For Instructor Use Only.

This document should not be distributed.



Practice 5: Overview

—
There are no practices for this lesson.



0

For Instructor Use Only.
This document should not be distributed.

For Instructor Use Only.
This document should not be distributed.



Bare Metal and Virtual Machine DB Systems

6

0

For Instructor Use Only.

This document should not be distributed.

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 DB storage options
- Shapes for virtual machine DB systems
- Storage options for virtual machine DB systems
- Storage architecture of the DB system
- Oracle Database software images

2

O



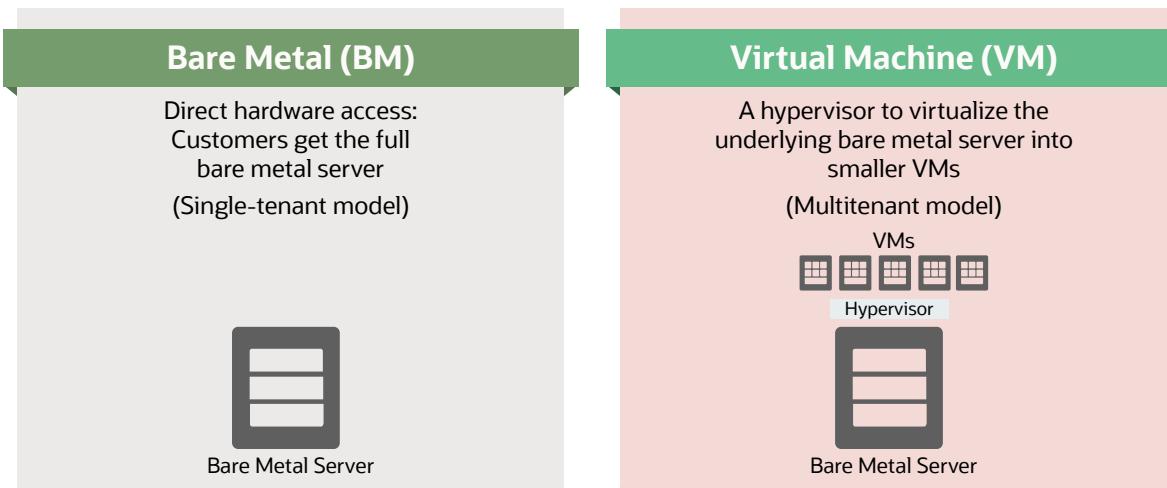
In this lesson we will look into the fundamentals of the OCI Database system instances on Oracle Cloud Infrastructure.

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

For Instructor Use Only.

This document should not be distributed.

Compute: Bare Metal and Virtual Machines



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

3

0

OCI is the only public cloud that supports BM 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 are no performance overheads, 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 multitenant model. The advantage here is flexibility with regard to choice of instance shapes.

For Instructor Use Only.

This document should not be distributed.

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 BYO
licensing

0

For Instructor Use Only.
This document should not be distributed.

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
Enterprise Edition	Yes	Yes	No	18.8.0.0 19.5.0.0 21.1.0.0.0
High Performance	Yes	Yes	No	
Extreme Performance	Yes	Yes	Yes	
BYOL			Yes	

5

With OCI Database Service there are six main latest versions of the Database available: 11.2, 12.1, 12.2, 18.8, 19.5, and 20.0.

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 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
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

0

Shapes for 1-Node RAC DB Systems

When you launch a DB system, you choose a shape that 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 the latest list of available OCI shapes refer to 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 (Two-Way Mirroring)	Usable Storage with High Redundancy (Three-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 1TB
BM.RACLocalStorage1.72 (IAD)	24 TB SSD	DATA 8.6 TB RECO 1.6 TB	DATA 5.4 TB RECO 1TB
BM.RACLocalStorage.72 (PHX, FRA)	64 TB SSD	DATA 23 TB RECOR 4.2 TB	DATA 14.4 TB RECO 2.6 TB

8

O

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 DB 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 disk group space utilized

Shapes for Virtual Machine Database Systems

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

- A shape for the DB system determines the resources allocated to the DB system.
- For example, the table below 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

9

0

For latest list of available OCI shapes, refer to this link:

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

For Instructor Use Only.

This document should not be distributed.

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 starting 256 GB up to 40 TB
- Dynamic storage scaling
- For 2-node RAC virtual machine DB systems, storage capacity is shared between the nodes.

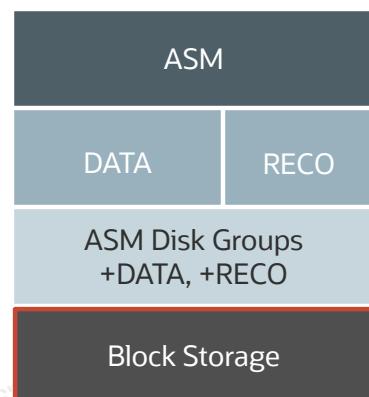
10

0

For Instructor Use Only.
This document should not be distributed.

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.



11

0

Storage in 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 the same way as these disks.

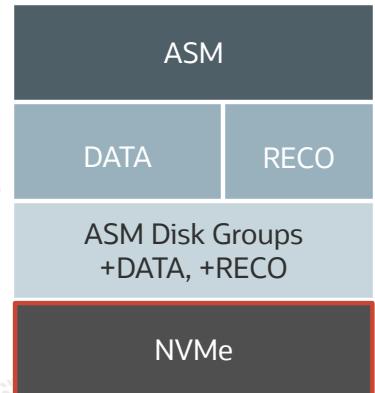
Any disks that fail will be managed. Space is reserved for rebalancing so the amount of free space is actually calculated based on that reservation. Whenever the shapes list a maximum amount of usable space in DATA and RECO, these reservations for rebalancing are already taken into account.

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

For Instructor Use Only.
This document should not be distributed.

BM DB Systems Storage Architecture

- Tracks the layout, configuration and status of storage.
- Monitors the disks for hard and soft failures.
- Proactively off-lines disks that failed, predicted to fail, or are performing poorly, and performs corrective actions, if possible.
- On disk failure, the DB system automatically creates an internal ticket and notifies the internal team to contact the customer.
- ASM manages mirroring of NVMe disks.
- Disks are partitioned: one for DATA and one for RECO.
- These actions ensure the highest level availability and performance at all times.



12

0

Storage in 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 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 are possible but the service sets these up by default in an optimal way.

Oracle Database Software Images

Database software images are resources within your tenancy before provisioning or patching a DB system, Exadata Cloud Service instance, Database Home, or database.

Steps to create a database software image

1. Open the navigation menu. Under **Oracle Database**, click **Bare Metal, VM, and Exadata**.
2. Under Resources, click **Database Software Images**.
3. Click **Create Database Software Image**.
4. In the Display name field, provide a display name for your image.
5. Choose your **Compartment**.
6. Choose a Shape family: **Bare metal and virtual machine DB systems or Exadata Cloud Service instances**
7. Choose the Database version for your image.
8. Click **Create Database Software Image**.

13

O

Database software images are automatically stored in Oracle-managed Object Storage, and viewed and managed in the Oracle Cloud Infrastructure Console.

Using a Database Software Image with a Bare Metal or Virtual Machine DB System

Provisioning: After you create a database software image, you can use it to provision the initial database in a new BM or VM DB system, or to provision a new database in an existing BM DB system.

Patching: You can use a database software image to update the database software of an existing VM or BM database in Oracle Cloud Infrastructure.

For Oracle Data Guard associations, you can use a custom database software image for in-place patching on both the primary and standby database instances to ensure that both databases have the same patches.

Oracle Database Software Images: Example

The screenshot shows the Oracle Cloud Infrastructure console. On the left, there's a sidebar with categories like Bare Metal, VM, and Exadata; DB Systems; Exadata at Oracle Cloud; Exadata VM Clusters; Exadata Infrastructure; Resources; and Database Software Images (which is highlighted with a red box). The main area is titled "Database Software Images in C11 Compartment". It has a "Create Database Software Image" button. Below it is a table with columns: Display name, State, Shape Family, and Database Version. A message says "No items found." To the right, a modal window titled "Create Database Software Image" is open. It asks for a "Display name" (MYDBIMAGE) and "Select a compartment" (C11). Under "Shape Family", "Virtual Machine and Bare Metal Shapes" is selected (highlighted with a red box). In the "Configure the database software image" section, "Database version" is set to "21c" (highlighted with a red box). At the bottom of the modal are "Create Database Software Image" and "Cancel" buttons.

14

0

For Instructor Use Only.

This document should not be distributed.

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 DB storage options
- Shapes for virtual machine DB systems
- Storage options for virtual machine DB systems
- Storage architecture of the DB system
- Oracle Database software images

15

0

For Instructor Use Only.

This document should not be distributed.



Practice 6: Overview

—
There are no practices for this lesson.



0

For Instructor Use Only.
This document should not be distributed.



Creating and Managing Bare Metal and Virtual Machine DB Systems

7

0

For Instructor Use Only.

This document should not be distributed.

Objectives

After completing this lesson, you should be able to:

- Manage the Database Systems Overview
- Identify the prerequisites to launch a DB system
- Identify the default options for the initial database
- Create a Virtual Cloud Network (VCN) for a DB system
- Use the Console to launch and manage a DB system
- Use the Console to scale up storage in and terminate a DB system
- Use the API Operations to launch and manage a DB system
- Set up DNS for a DB system
- List special considerations for creating DB systems

2

O



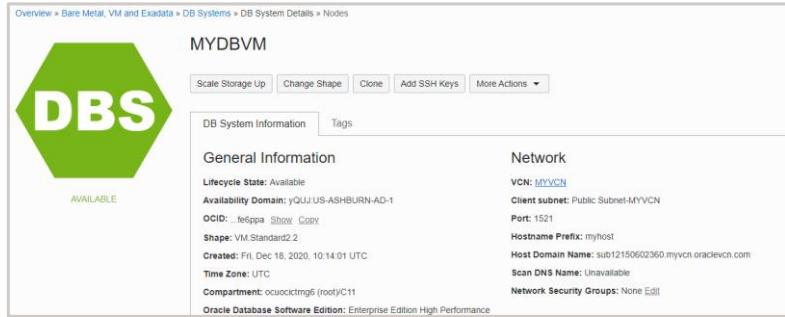
In this lesson we will look into the fundamentals of the OCI Database System instances on Oracle Cloud Infrastructure.

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

Managing the Database Systems Overview

You can use the Console to perform the following tasks:

- Launch a DB system: You can create a database system.
- Check the status: You can view the status of your database creation, and after that, you can view the runtime status of the database.
- Start, stop, or reboot.
- Scale: You can scale up the number of enabled CPU cores in the system.
- Terminate: Terminating a DB system permanently deletes it and any databases running on it.



3

0

For Instructor Use Only.

This document should not be distributed.

Required IAM Policy

- Which of the services within Oracle Cloud Infrastructure can I control access to through policies?
- All, including IAM itself.
- Can users do anything without an administrator writing a policy for them?
- Yes. All users can automatically do these things without an explicit policy:
 - Change or reset their own Console password.
 - Manage their own API signing keys and other credentials.

The default setup for a new tenancy:	
CompanyA Tenancy	
Policies attached to the tenancy:	
Users	Wenpei
Groups	
Administrators	Wenpei

0

4

An IAM document specifies who has what type of access to your resources.

It is used in different ways:

An individual statement written in the policy languageAa collection of statements in a single, named “policy” document (which has an Oracle Cloud ID [OCID] assigned to it)

The overall body of policies your organization uses to control access to resources.

To use Oracle Cloud Infrastructure, you must be given the required type of access in a policy written by an administrator, whether you're using the Console or the REST API with an SDK, CLI, or any other tool. If you try to perform an action and get a message that you don't have permission or are unauthorized, confirm with your administrator the type of access you've been granted and which compartment you should work in.

For IAM policy reference:

<https://docs.cloud.oracle.com/iaas/Content/Identity/Reference/iampolicyreference.htm>

Prerequisites to Launch a DB System

You need the following items to launch any DB system:

- Public key in OpenSSH format
- 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.
- Service gateway with a private subnet or an internet gateway with a public subnet in case of back up your DB system to Object Storage or 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.

5

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).

For Instructor Use Only.

This document should not be distributed.

Default Options for the Initial Database

The following default options are used for the initial database:

- **Console Enabled:** **False**
- **Create Container Database:** **False** for version 11.2.0.4 databases, otherwise True
- **Create Instance Only (for standby and migration):** **False**
- **Database Home ID:** Creates a new database home
- **Database Language:** **AMERICAN**
- **Database Sizing Template:** **odb2**
- **Database Storage:** **ACFS** for version 11.2.0.4 databases, otherwise **ASM**
- **Database Territory:** **AMERICA**
- **Database Unique Name:** The user-specified database name and a system-generated suffix (for example, `dbtst_phx1cs`)
- **PDB Admin Name:** `pdbuser` (not applicable for version 11.2.0.4 databases)

7

0

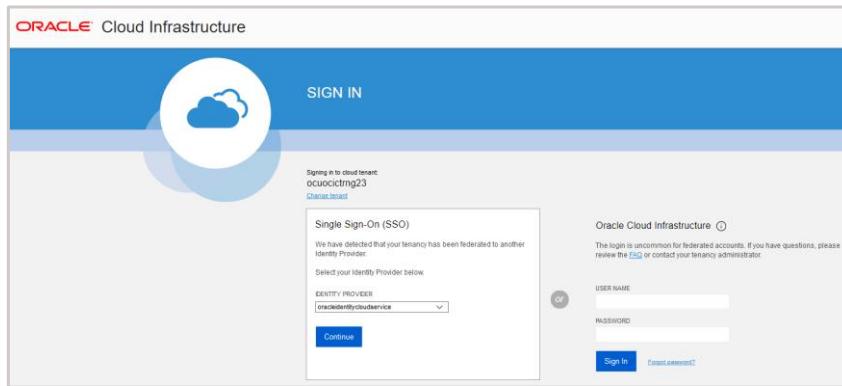
For Instructor Use Only.

This document should not be distributed.

Creating a VCN for a DB System

1. Log in to Oracle Cloud Infrastructure using:

- Enter Cloud Tenant.
- Enter OCI User Name.
- Enter OCI Password.



8

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

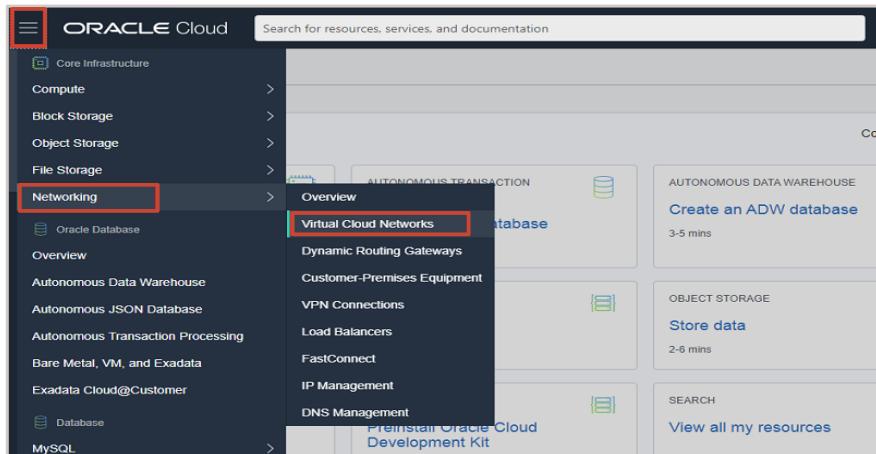
Enter your **Cloud Tenant** and click **Continue**.

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 OCI.

Creating a VCN for a DB System

2. Select **Networking** from the menu.
3. Select **Virtual Cloud Networks**.



9

Before you can launch a 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**.

For Instructor Use Only.
This document should not be distributed.

Creating a VCN for a DB System

- 4. Choose a Compartment.
- 5. Choose a State.

The screenshot shows the 'IP Management' section of the Oracle Cloud Infrastructure console. At the top, there are two buttons: 'IP Management' and 'DNS Management'. Below them is a 'List Scope' section with a dropdown menu labeled 'COMPARTMENT' containing 'C11'. Underneath it, a tooltip shows the full path: 'ocuocictrng6 (root)/C11'. Below this is a 'Filters' section with a dropdown menu labeled 'STATE' containing 'Available'.

10

0

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

For Instructor Use Only.

This document should not be distributed.

Creating a VCN for a DB System

6. Click Start VCN Wizard.



The screenshot shows the Oracle Cloud Infrastructure Networking Virtual Cloud Networks page. On the left, there's a sidebar with options like Overview, Virtual Cloud Networks (which is selected and highlighted in blue), Dynamic Routing Gateways, Customer-Premises Equipment, VPN Connections, and Load Balancers. The main content area has a title "Virtual Cloud Networks in C11 Compartment". Below it is a brief description of what Virtual Cloud Networks are. At the top right of the main area, there are two buttons: "Create VCN" (blue) and "Start VCN Wizard" (red, with a red box around it). Below these buttons is a table header with columns: Name, State, CIDR Block, Default Route Table, DNS Domain Name, and Created. The table body below the header shows "No items found." and "Showing 0 Items < 1 of 1 >".

11

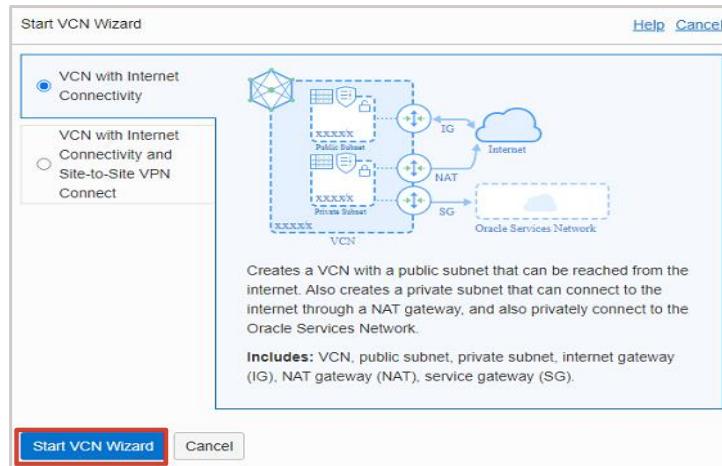
0

For Instructor Use Only.
This document should not be distributed.

Create a Virtual Cloud Network using “Networking Quickstart” option. This option is the quickest way to get a working cloud network in the least number of steps.

Creating a VCN for a DB System

7. In the dialog box, choose VCN with Internet Connectivity and click **Start VCN Wizard**.



12

VCN with Internet Connectivity

Creates a [VCN](#).

Creates an [internet gateway](#), [NAT gateway](#), and [service gateway](#) for the VCN.

Creates a regional public subnet with routing to the internet gateway. Instances in a public subnet may optionally have public IP addresses.

Creates a regional private subnet with routing to the NAT gateway and service gateway (and therefore the Oracle Services Network). Instances in a private subnet cannot have public IP addresses.

Sets up basic security list rules for the two subnets, including SSH access.

Creating a VCN for a DB System

8. Provide configuration information:

- VCN Name
- Confirm Compartment
- VCN CIDR Block
- Public Subnet CIDR Block
- Private Subnet CIDR Block

The screenshot shows the 'Basic Information' and 'Configure VCN and Subnets' sections of the VCN creation interface. In the 'Basic Information' section, 'VCN NAME' is set to a redacted value and 'COMPARTMENT' is set to 'C1T'. In the 'Configure VCN and Subnets' section, 'VCN CIDR BLOCK' is set to a redacted value, 'PUBLIC SUBNET CIDR BLOCK' is set to a redacted value, and 'PRIVATE SUBNET CIDR BLOCK' is set to a redacted value. A 'DNS RESOLUTION' checkbox is checked, with the label 'USE DNS HOSTNAMES IN THIS VCN' and a note about it being required for instance hostname assignment.

13

Enter the following:

VNC Name: A friendly name for the subnet. It doesn't have to be unique, and it cannot be changed later in the Console (but you can change it with the API). Avoid entering confidential information.

Compartment: If you've enabled compartment selection, specify the compartment where you want to put the subnet.

CIDR Block: A single, contiguous CIDR block for the subnet (for example, 10.0.0.0/16). Make sure it's within the cloud network's CIDR block and doesn't overlap with any other subnets. You cannot change this value later.

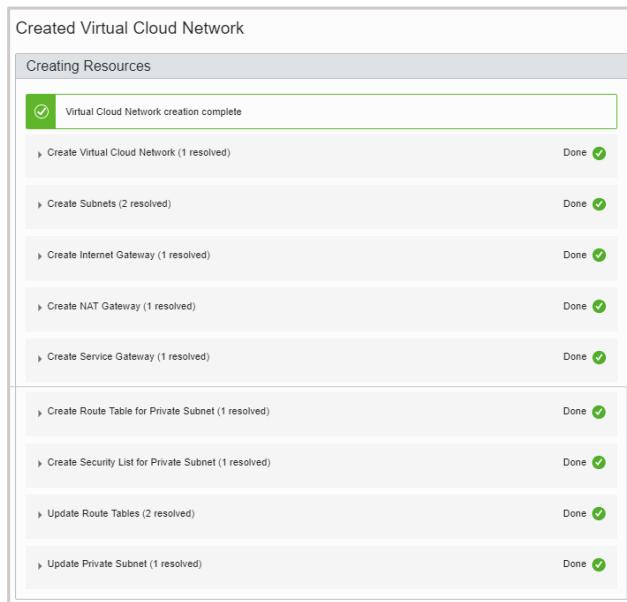
Public Subnet: This controls whether VNICs in the subnet can have public IP addresses (for example, 10.0.0.0/24).

Private Subnet: This controls whether VNICs in the subnet can have private IP addresses (for example, 10.0.1.0/24).

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.

VCN creates along with resources



14

VCN creates along with resources like subnets, internet gateway, route table, and security lists.

0

VCN Details

Name	State	CIDR Block	Subnet Access	Created
Private Subnet-MYVCN	Available	10.0.1.0/24	Private (Regional)	Tue, Dec 15, 2020, 06:09:39 UTC
Public Subnet-MYVCN	Available	10.0.0.0/24	Public (Regional)	Tue, Dec 15, 2020, 06:09:36 UTC

15

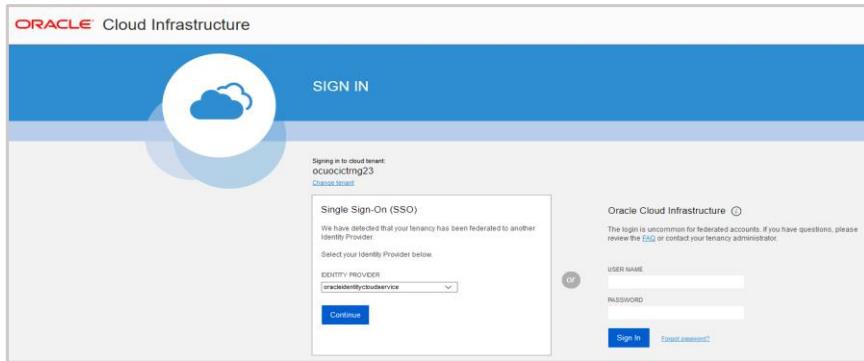
The Console has an easy option to verify the Public Subnet and Private Subnet created for a VCN.

Also, the Console has an easy “Terminate” process that deletes a VCN and its related networking resources (subnets, route tables, security lists, sets of DHCP options, internet gateway, and so on). The “Terminate” process deletes one resource at a time and takes a minute or two. A progress report is displayed to show you what's been deleted so far.

Using the Console to Launch a DB System

1. Log in to Oracle Cloud Infrastructure using:

- Enter Cloud Tenant.
- Enter OCI User Name.
- Enter OCI Password.



16

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

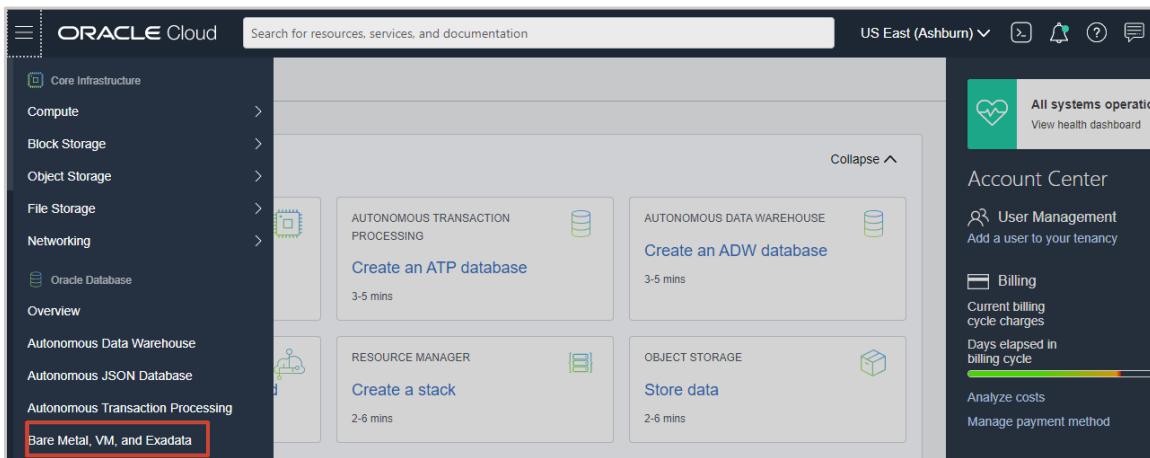
Enter your **Cloud Tenant** and click **Continue**.

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 OCI.

Using the Console to Launch a DB System

2. Click **Bare Metal, VM, and Exadata** from the OCI menu.



17

O

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.

For Instructor Use Only.
This document should not be distributed.

Using the Console to Launch a DB System

3. Choose a Compartment.
4. Click **Create DB System**.

The screenshot shows the Oracle Cloud console interface. The left sidebar has sections for Bare Metal, VM, and Exadata; DB Systems (which is selected and highlighted in blue); Exadata at Oracle Cloud; Exadata VM Clusters; Exadata Infrastructure; Resources; Database Software Images; Standalone Backups; and List Scope. Under List Scope, there is a Compartments dropdown set to C11. The main area is titled "DB Systems in C11 Compartment". It features a "Create DB System" button in a red box. Below it is a table with columns: Display Name, State, Availability Domain, Shape, CPU Core Count, and Created. A message "No items found." is displayed. At the bottom right of the table, it says "Showing 0 items < 1 of 1 >". In the bottom right corner of the page, there is a watermark that says "Activate Windows Go to PC settings to activate Windows".

18

0

Select the compartment in which to create the virtual machine or bare metal instance from the Compartment section.

Click “Create DB System” button.

For Instructor Use Only.

This document should not be distributed.

Steps to Fill in DB System Information

1. Enter Display Name.
2. Select an Availability Domain.
3. Select a Shape.
4. Select a Database Edition.
5. Select a Storage Management Software.

The screenshot shows the 'Choose Storage Management Software' section of the Oracle Cloud Infrastructure interface. It displays two options: 'Oracle Grid Infrastructure' and 'Logical Volume Manager'. The 'Logical Volume Manager' option is selected, indicated by a blue border around its checkbox and a checked checkmark icon. A small explanatory text below it states: 'Recommended for quick deployments using Logical Volume Manager.'

19

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 AD 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.

Oracle Database Software Edition: The database edition supported by the DB system. You can mix supported database versions on the DB system, but not editions. (The database edition cannot be changed and applies to all the databases in this DB system.)

As part of the practice session in this course you will learn to launch a VM DB system and manage it.

Storage Management Software: ACFS for version 11.2.0.4 databases. Otherwise, ASM for all bare metal and multi-node virtual machine DB systems. Single-node VM systems can optionally be provisioned using Logical Volume Manager for faster provisioning.

Steps to Fill in DB System Information

6. Select Available Storage Size.
7. Upload SSH Public Key.
8. Select License Type.

The screenshot shows three sequential steps in the configuration process:

- Step 6:** Configure storage. It shows an available storage of 256 GB and a total storage of 712 GB. A note states: "The maximum storage amount is 2560 GB."
- Step 7:** Add public SSH keys. It includes fields for "Upload SSH key files" and "Paste SSH keys". A note says: "Drop files here or [browse](#) SSH Public Keys (.pub) only."
- Step 8:** Choose a license type. It offers two options: "License Included" (selected) and "Bring Your Own License (BYOL)". A note for BYOL says: "Bring my existing Oracle Database software licenses to the Database service."

20

o

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.

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.

Steps to Fill in Network Information

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

The screenshot shows a dialog box titled "Specify the network information".
1. Under "Virtual cloud network in C17 (Change Compartment)", the dropdown is set to "MYVCN".
2. Under "Client Subnet in C17 (Change Compartment)", the dropdown is set to "Public Subnet-MYVCN(regional)".
3. Under "Hostname prefix", the input field contains "MYHOST".
Other fields shown include "Host domain name" and "Host and domain URL".

21

0

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 Database name.
2. Select Database version.
3. Enter PDB name.
4. Provide Database administration password.
5. Confirm admin password.

The screenshot shows the 'Create DB System' interface. It has two tabs: 'DB System Information' (selected) and 'Database Information'. Under 'Database Information', there are fields for 'Database name' (containing 'MYORCL'), 'Database image' (containing 'Oracle Database 21c'), 'PDB name (OPTIONAL)' (containing 'MYPDB1'), 'Create administrator credentials' (with 'Username (READ-ONLY)' set to 'SYS' and 'Password (1)' masked as '*****'), and a 'Confirm password' field below it.

22

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.

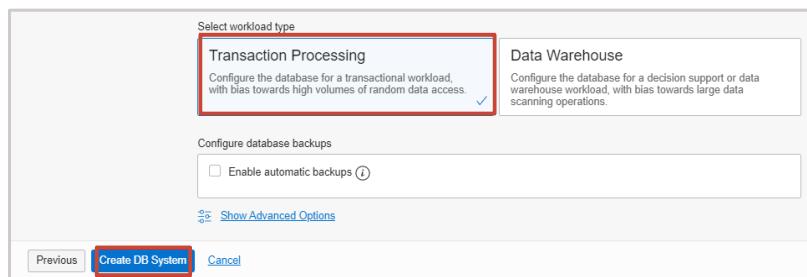
PDB Name: *Not applicable to version 11.2.0.4.* The name of the pluggable database. The PDB name must begin with an alphabetic character, and can contain a maximum of eight alphanumeric characters. The only special character permitted is the underscore (_).

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. Select workload type.
7. Enable automatic backup.
8. Click **Create DB System**.



23

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.

Automatic Backup: Check the check box to enable automatic incremental backups for this database.

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) (<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

Different statuses of a DB system:

- Provisioning
- Available
- Updating
- Stopped
- Terminating
- Terminated
- Failed

Display Name	State	Availability Domain	Shape	CPU Core Count	Created
MYDBVM	Available	yQUU.US-ASHBURN-AD-1	VM.Standard2.2	2	Fri, Dec 18, 2020, 10:14:01 UTC

24

o

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.

Using the Console to Manage a DB System

- Database Status
- Start, Stop, and Reboot
- Scale CPU Cores
- Scale Up Storage
- Terminate DB System
- BYOL Database Licenses
- Tags for DB Systems and Database Resources

The screenshot shows the Oracle Cloud Infrastructure (OCI) console interface for managing a Database System. At the top, there's a green hexagonal icon with 'DBS' and the word 'AVAILABLE'. Below it, the DB System name 'MYDBVM' is displayed. A toolbar at the top right includes buttons for 'Scale Storage Up', 'Change Shape', 'Clone', 'Add SSH Keys', and 'More Actions'. The main area is divided into sections: 'General Information' and 'Network'. Under General Information, details include: Lifecycle State: Available; Availability Domain: yGUL.US-ASHBURN-AD-1; OCID: oducocidr9gj (root)C11; Shape: VM Standard-2; Created: Fri, Dec 18, 2020, 10:14:01 UTC; Time Zone: UTC; Compartment: oducocidr9gj (root)C11; Oracle Database Software Edition: Enterprise Edition High Performance; Storage Management Software: Logical Volume Manager; Available Data Storage: 512 GB; Total Storage Size: 968 GB. The Network section shows: VCN: MYVNCN; Client subnet: Public Subnet MYVNCN; Port: 1521; Hostname Prefix: myhost; Host Domain Name: sub12150602360.myvncn.oraclevcn.com; Scan DNS Name: Unavailable; Network Security Groups: None. Below this, a 'Databases' section lists one entry: MYORCL (Available, MYORCL_1ad16q, Transaction Processing, 21.1.0.0, Fri, Dec 18, 2020, 10:14:01 UTC). A message at the bottom says 'Showing 1 Item < 1 of 1'.

25

0

You can launch the Console to start, stop, terminate, scale, manage licenses for, and check the status of a bare metal and virtual machine DB system, and set up DNS for a 1-node or 2-node RAC DB system.

For Instructor Use Only.
This document should not be distributed.

Using Console to Start, Stop, and Reboot a DB System

Different actions of DB system:

- Start
- Reboot
- Copy OCID

Resources		Nodes					
		Name	State	Public IP Address	Floating IP Address	Private IP Address & DNS Name	Fault Domain
Databases (1)		myhost	Available	193.122.143.137	-	10.0.0.7 (myhost... <a>Show <a>Copy)	FAULT-DOMAIN-3
Nodes (1)		Displaying 1 Node < 1 of 1 >					
Patches (0)							
Patch History (0)							
Console Connections (0)							
Work Requests (0)							

26

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 DB system you want to stop or start and then click its name to display details about it.

In the list of nodes, click the Actions icon (three dots) for a node and then click one of the following actions:

Start: Restarts a stopped node. After the node is restarted, the **Stop** action is enabled.

Stop: Shuts down the node. After the node is powered off, the **Start** action is enabled.

Reboot: Shuts down the node and then restarts it.

Using the Console to Scale Up Storage

You can increase the block storage at any time without impacting the virtual machine DB system.

The screenshot shows two pages from the Oracle Cloud Infrastructure console:

- DB System Details Page:** Shows details for a DB system named "MYDBVM". The "Scale Storage Up" button is highlighted with a red box.
- Scale Storage Up Dialog:** A modal window titled "Scale Storage Up" with the following fields:
 - Available Data Storage (GB):** Set to 512.
 - Total Storage Size (GB):** Set to 968.
 - Update** and **Cancel** buttons.

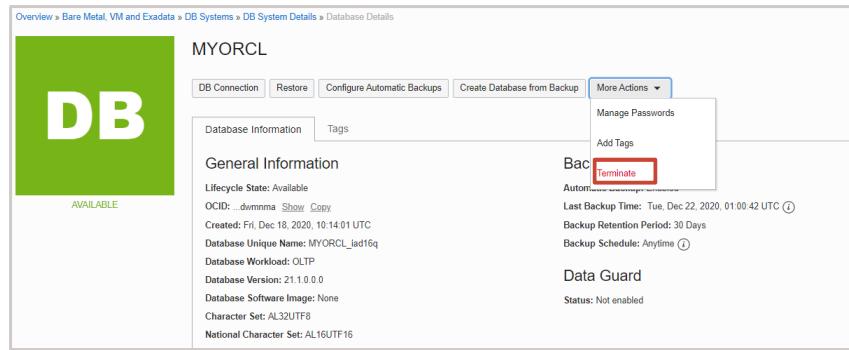
27

1. Open the navigation menu. Under **Database**, click **Bare Metal, VM, and Exadata**.
2. Choose your **Compartment**. A list of DB systems is displayed.
3. In the list of DB systems, find the system you want to scale up and click its highlighted name. The system details are displayed.
4. Click **Scale Storage Up** and then select the new storage size from the dropdown list.
5. Click **Scale Storage Up**.

Note: This procedure does not apply to bare metal DB systems.

Using the Console to Terminate a DB System

- Terminating a DB system permanently deletes it.
- Full backups remain in Object Storage.
- This removes all automatic incremental backups of all databases from Object Storage.



28

O

Note: The database data is local to the DB system and will be lost when the system is terminated. Oracle recommends that you back up any data in the DB system prior to terminating it.

- Open the navigation menu. Under **Database**, click **Bare Metal, VM, and Exadata**.
- Choose your **Compartment**. A list of DB systems is displayed.
- For the DB system you want to terminate, click the Actions icon (three dots) and then click **Terminate**.
- Confirm when prompted. The DB system's icon indicates **Terminating**.

At this point, you cannot connect to the system and any open connections will be terminated.

Using the Console to Manage BYOL Database Licenses

- You can control the number of database licenses that you run at any given time.
- You can scale up or down the number of OCPUs on the instance.
- These additional licenses are metered separately.
- You cannot change the number of CPU cores for a virtual machine DB system directly.
- You can change the shape of the DB system to change the CPU cores.

29

0

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.

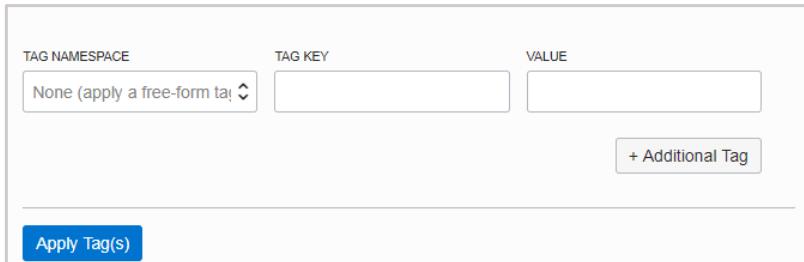
Bring Your Own License (BYOL) means you are an Oracle Database customer with an Unlimited License Agreement or Non-Unlimited License Agreement and want to use your license with Oracle Cloud Infrastructure. This removes the need for separate on-premises licenses and cloud licenses.

If you want to control the number of database licenses that you run at any given time, you can scale up or down the number of OCPUs on the instance. These additional licenses are metered separately.

1. Open the navigation menu. Under **Database**, click **Bare Metal**, **VM**, and **Exadata**.
2. Choose your **Compartment**.
3. A list of DB systems is displayed.
4. In the list of DB systems, find the system you want to scale and click its highlighted name.
5. The system details are displayed.
6. Click **Scale Up/Down OCPU** and then change the number.

Using the Console to Manage Tags

- Tags for DB Systems
- Tags for Database Resources



30

When you have many resources (for example, instances, VCNs, load balancers, and block volumes) across multiple compartments in your tenancy, it can become difficult to track resources used for specific purposes, or to aggregate them, report on them, or take bulk actions on them. Tagging allows you to define keys and values and associate them with resources. You can then use the tags to help you organize and list resources based on your business needs. There are two types of tags:

Defined tags are set up in your tenancy by an administrator. Only users granted permission to work with the defined tags can apply them to resources.

Free-form tags can be applied by any user with permissions on the resource.

To manage tags for your DB systems and database resources:

1. Open the navigation menu. Under **Database**, click **Bare Metal**, **VM**, and **Exadata**.
2. Choose your **Compartment**.
3. Find the DB system or database resource you're interested in and click the name.
4. Click the **Add Tags** from **More Actions** tab to view or edit the existing tags. Or click **Apply Tag(s)** to add new ones.

For more details about tags:

<https://docs.cloud.oracle.com/iaas/Content/Identity/Concepts/taggingoverview.htm#Introduc>

Using the API Operations to Launch a DB System

The following requirements are needed on the host:

- python >= 2.6
- Python SDK for Oracle Cloud Infrastructure
- oci uses a simple dict to build clients and other components.
- You can build these manually or oci can parse and validate a config file from default location `~/.oci/config`

```
# Example
- name: Create DB System
oci_db_system:
  compartment_id: "ocid1.compartment.aaaa"
  availability_domain: "AD-2"
  cluster_name: "db-cluster"
  cpu_core_count: 2
  data_storage_percentage: 80
  database_edition: "STANDARD_EDITION"
  db_home:
    database:
      admin_password: 'BEstr0ng_#1'
      character_set: 'AL32UTF8'
      db_backup_config:
        auto_backup_enabled: False
      db_name: 'db15'
      db_workload: 'OLTP'
      ncharacter_set: 'AL16UTF16'
      pdb_name: 'db15'
      freeform_tags:
        deployment: 'production'
```

31

0

The following requirements are needed on the host to work with API.

`python >= 2.6`

Python SDK for Oracle Cloud Infrastructure <https://oracle-cloud-infrastructure-python-sdk.readthedocs.io>

oci uses a simple dict to build clients and other components. You can build these manually, or oci can parse and validate a config file.

Using the default configuration location `~/.oci/config` you can use `config.from_file()` to load any profile. By default, the DEFAULT profile is used:

```
>>> from oci.config import from_file
>>> config = from_file()
# Using a different profile from the default location
>>> config = from_file(profile_name="integ-beta")
# Using the default profile from a different file
>>> config = from_file(file_location="~/.oci/config.prod")
```

Since config is a dict, you can also build it manually and check it with `config.validate_config()`.

Using the API Operations to Manage a DB System

To list all DB systems

```
- name: List all DB System in a
compartment  oci_db_system_facts:
compartment_id:
'ocid1.compartment..xcds'
```

To update a DB system's CPU core

```
- name: Update DB System CPU core
count  oci_db_system:
db_system_id: "ocid1.dbsystem.aaaa"
cpu_core_count: 4      state: 'present'
```

To fetch a specific DB system

```
- name: List a specific DB System
oci_db_system_facts:
db_system_id: 'ocid1.dbsystem..xcds'
```

To terminate a DB system

```
- name: Terminate DB System
oci_db_system:    db_system_id:
"ocid1.dbsystem.aaaa"
state: 'absent'
```

0

For Instructor Use Only.
This document should not be distributed.

Setting Up DNS for a DB System

- DNS lets you use host names instead of IP addresses to communicate with a DB system.
- Following 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.

33

0

For Instructor Use Only.

This document should not be distributed.

Special Considerations for Creating DB Systems

- 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 the virtual machine DB; the shape can be changed for the DB system to scale up the CPU cores.
- Sometimes during the creation of the bare metal DB system, due to limited resources for bare metal we may get an error for service limits that 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:

- Manage the Database Systems Overview
- Identify the prerequisites to launch a DB system
- Identify the default options for the initial database
- Create a Virtual Cloud Network (VCN) for a DB system
- Use the Console to launch and manage a DB system
- Use the Console to scale up storage in and terminate a DB system
- Use the API Operations to launch and manage a DB system
- Set up DNS for a DB system
- List special considerations for creating DB Systems

35



0

For Instructor Use Only.

This document should not be distributed.

Practice 7: Overview

This practice covers the following topics:

- Practice 7-1: Generating SSH Keys
- Practice 7-2: Creating a Virtual Cloud Network (VCN)
- Practice 7-3: Creating a Virtual Machine DB System



0

For Instructor Use Only.
This document should not be distributed.



Connecting to a DB System on OCI

0

For Instructor Use Only.

This document should not be distributed.

Objectives

After completing this lesson, you should be able to:

- Connect to a pluggable database
- Set environment variables
- Connect to a DB system with SSH
- Connect to a database with Oracle SQL Developer
- Connect to a database on a 1-node DB system
- Connect to a database on a multi-node DB system
- Troubleshoot connection issues

2

In this lesson we will look into the 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, how to launch an instance.



For Instructor Use Only.

This document should not be distributed.

Connecting to a Pluggable Database

- Connect to a pluggable database using the following syntax.

Syntax: sqlplus

```
sys/<password>@<hostname>.<DB_domain>:1521/<DB_unique_name>.<DB_domain> as sysdba
```

Example:

```
sqlplus  
sys/**********@myhost.sub12150602360.myvcn.oraclevcn.com:  
1521/MYPDB1.sub12150602360.myvcn.oraclevcn.com as sysdba
```

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 lower case>

4

O

The `oraenv` or `coraenv` script is usually called from the user's shell startup file (for example, `.profile` or `.login`) and 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 variables listed on this slide.

For Instructor Use Only.

This document should not be distributed.

Prerequisites for SSH Access to the DB System

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

- Name of a Virtual Cloud Network (VCN)
- Private and public keys of the DB system
- Public or private IP address of the DB system



5

O

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 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>
```

- 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>*

- Connection type: SSH

- Port: 22

3. In the Category pane, expand **Connection**, expand **SSH**, and then click **Auth**, and browse to select your private key.

4. Optionally, return to the **Session** category screen and save this session information for reuse later.

5. Click **Open** to start the session.

6

0

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>.

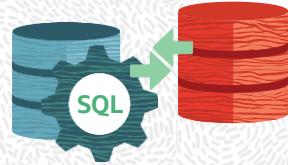
Connecting to a Database with Oracle SQL Developer

You can connect to a database with SQL Developer by using one of the following methods:

- 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 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.



0

7

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>).

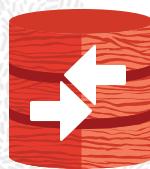
Connecting to a Database on a 1-Node DB System

After creating an SSH tunnel or opening port 1521, start your SQL Developer client and create a connection using the following connection details:

- **Username:** sys as sysdba
- **Password:** The Database Admin Password that was specified in the Launch DB System dialog box in the Console.
- **Hostname:** localhost if using an SSH tunnel, or the public IP address of the DB system if not using a tunnel.
- **Port:** 9999 (or the port of your choice) if using an SSH tunnel, or 1521 if not using a tunnel.
- **Service name:** The concatenated Database Unique Name and Host Domain Name (for example, db1_phx1tv.mycompany.com). You can find both these names in the Console by clicking Database and then clicking the DB System name for details.

Connecting to a Database on a Multi-Node DB System

- 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, in the **Database** details page.
- 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.



0

For Instructor Use Only.

This document should not be distributed.

9

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 following options:

Use the private SCAN IP addresses, as shown in the following tnsnames.ora example:

```
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>) ) )
```

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, extscancode.example.com is defined in the on-premises DNS server.

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

Troubleshooting Connection Issues

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

- **ORA-28365: Wallet is Not Open Error**
 - Before you use OS authentication to connect to a database (for example, sqlplus / as sysdba) be sure to set the ORACLE_UNQNAME variable.
 - 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**
 - 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.

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 pluggable database
- Set environment variables
- Connect to a DB system with SSH
- Connect to a database with Oracle SQL Developer
- Connect to a database on a 1-node DB system
- Connect to a database on a multi-node DB system
- Troubleshoot connection issues



0

For Instructor Use Only.

This document should not be distributed.

Practice 8: Overview

This practice covers the following topics:

- Practice 8-1: Connecting to a DB System Using SSH
- Practice 8-2: Connecting to a Database Using SQL Developer
- Practice 8-3: Creating TNS Entry for a PDB



0

For Instructor Use Only.
This document should not be distributed.



Updating and Configuring a DB System on OCI

9

0

For Instructor Use Only.

This document should not be distributed.

Objectives

After completing this lesson, you should be able to:

- Update a DB system
- Configure a DB system
- Scale a DB system
- Clone a DB system



0

For Instructor Use Only.
This document should not be distributed.

Updating a DB System

Considerations for updating the OS of a bare metal or virtual machine DB system:

- Bash Profile Updates
- Essential Firewall Rules
- Important Guidelines for OS Updates



0

3

This topic includes information on how to update the OS of a bare metal or virtual machine DB system.

Note: This is not applicable for Exadata DB systems.

For Instructor Use Only.
This document should not be distributed.

Bash Profile Updates

- Do not add interactive commands such as `.oraenv`.
- Do not add commands which might return an error or warning.

4

0

Considerations for Bash Profile Updates

Do not add interactive commands such as `oraenv`, or commands that might return an error or warning message, to the `.bash_profile` file for the grid or oracle users. Adding such commands can prevent database service operations from functioning properly.

For Instructor Use Only.

This document should not be distributed.

Essential Firewall Rules

- Rules for ports 1521, 7070, and 7060 that allow the Database service to manage the DB system
- Rules for 169.254.0.2:3260 and 169.254.0.3:80 that prevent non-root users from escalating privileges and tampering with the system's boot volume and boot process

Removing or modifying these rules can allow non-root users to modify the system's boot volume.

5

0

For a 1-node DB system or 2-node RAC DB system, do not remove or modify the following firewall rules in /etc/sysconfig/iptables:

The firewall rules for ports 1521, 7070, and 7060 allow the Database service to manage the DB system. Removing or modifying them can result in the Database service no longer operating properly.

The firewall rules for 169.254.0.2:3260 and 169.254.0.3:80 prevent non-root users from escalating privileges and tampering with the system's boot volume and boot process. Removing or modifying these rules can allow non-root users to modify the system's boot volume.

Important Guidelines for OS Updates

- Do not remove packages from a DB system.
- Test the updates thoroughly before updating a production system.
- Apply the required OS security updates published regularly.
- Configure the DB system's VCN to allow access to the YUM repository.

Note: Do not install NetworkManager on the DB system; it may cause severe loss of access to the system.



6

Before you update the OS, review the following important guidelines and information:

Do not remove packages from a DB system. However, you might have to remove custom RPMs (packages that were installed after the system was provisioned) for the update to complete successfully.

Oracle recommends that you test any updates thoroughly before updating a production system.

The image used to launch a DB system is updated regularly with the necessary patches. After you launch a DB system, you are responsible for applying the required OS security updates published through the Oracle public YUM server.

To apply OS updates, the DB system's VCN must be configured to allow access to the YUM repository.

Configuring a DB System

Considerations to configure a DB system:

- Network time protocol
- Transparent data encryption



0

7

This topic provides information to help you configure your DB system.

For Instructor Use Only.
This document should not be distributed.

Network Time Protocol (NTP)

- Oracle recommends running an NTP daemon on the DB system to keep system clocks stable during rebooting.
- Oracle recommends configuring NTP on both the nodes of the 2-node RAC DB system to synchronize time on both nodes.

8

0

Oracle recommends that you run a Network Time Protocol (NTP) daemon on your 1-node DB System to keep system clocks stable during rebooting.

Oracle recommends that you configure NTP on both nodes in a 2-node RAC DB System to synchronize time across the nodes. If you do not configure NTP, then Oracle Clusterware configures and uses the Cluster Time Synchronization Service (CTSS), and the cluster time might be out of sync with applications that use NTP for time synchronization.

Transparent Data Encryption

- All user-created tablespaces in a DB system are encrypted by default.
- Set the ENCRYPT_NEW_TABLESPACES parameter to DDL if you don't want tablespaces to be encrypted.
- Use the `dbcli update-tdekey` command to update the master encryption key for a database.
- Create and activate a master encryption key for any newly created PDBs.
- Use the `dbcli update-tdekey` command to create and update the master encryption key for a PDB.
- Each PDB has its own master encryption key that is stored in a single keystore used by all containers.

9

O

All user-created tablespaces in a DB system database are encrypted by default, using Transparent Data Encryption (TDE).

For version 12c databases, if you don't want your tablespaces encrypted, you can set the ENCRYPT_NEW_TABLESPACES database initialization parameter to DDL.

On a 1- or 2-node RAC DB system, you can use the `dbcli_update-tdekey` command to update the master encryption key for a database.

You must create and activate a master encryption key for any PDBs that you create. After creating or plugging in a new PDB on a 1- or 2-node RAC DB system, use the `dbcli update-tdekey` command to create and activate a master encryption key for the PDB. Otherwise, you might encounter the error “ORA-28374: typed master key not found in wallet” when attempting to create tablespaces in the PDB. In a multitenant environment, each PDB has its own master encryption key that is stored in a single keystore used by all containers.

For Instructor Use Only.

This document should not be distributed.

Scaling a DB System

- Scaling CPU
- Scaling Storage



0

For Instructor Use Only.
This document should not be distributed.

Scaling a CPU

- Bare Metal Compute Node processing power can be scaled up by increasing the number of CPU cores.
- Virtual Machine DB system CPU cores cannot be changed directly.
- The shape of a VM DB system can be changed due to which CPU cores can be increased.



11

O

Scale a CPU for Bare Metal DB System:

If a multi-node DB system requires more compute node processing power, you can scale up (burst) the number of enabled CPU cores in the system.

To scale a CPU for a bare metal DB system:

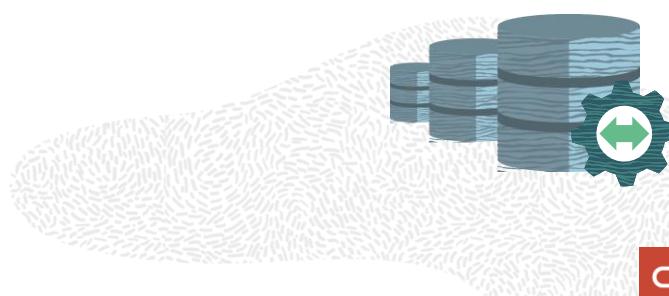
1. Open the navigation menu. Under Database, click Bare Metal, VM, and Exadata.
2. Choose your Compartment. A list of DB systems is displayed.
3. In the list of DB systems, find the system you want to scale up and click its highlighted name. The system details are displayed.
4. Click Scale Storage Up and then select the new storage size from the dropdown list.
5. Click Scale Storage Up.

Change shape of a VM DB system:

1. Open the navigation menu. Under Database, click Bare Metal, VM, and Exadata.
2. Choose your Compartment. A list of database systems is displayed.
3. Click the system you want to scale; the system details are displayed.
4. Click Change Shape.
5. Select the new shape from the list of compatible shapes and click Change.

Scaling Storage

- The storage of a VM DB System can be scaled up any time without impacting the system.
- The storage of bare metal DB systems cannot be scaled up.



12

0

If a VM DB system requires more block storage, you can increase the storage at any time without impacting the system.

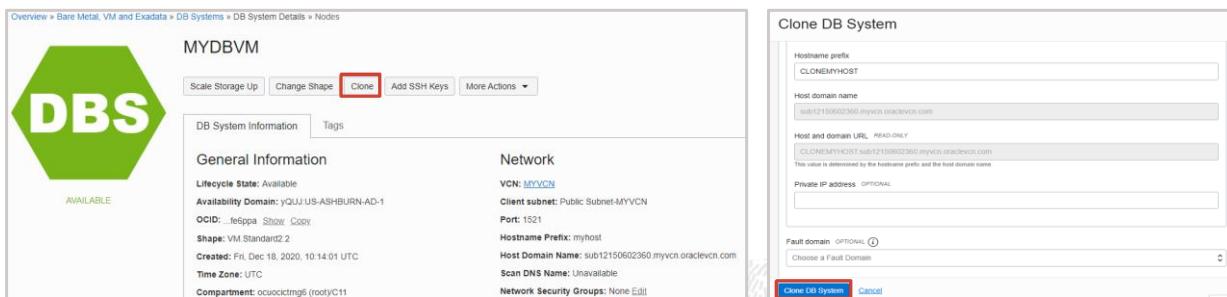
To scale storage for the VM DB system:

1. Open the navigation menu. Under Database, click Bare Metal, VM, and Exadata.
2. Choose your Compartment. A list of DB systems is displayed.
3. In the list of DB systems, find the system you want to scale and click its highlighted name. The system details are displayed.
4. Click Scale Up/Down and then change the number in CPU Core Count. The text below the field indicates the acceptable values, based on the shape used when the DB system was launched.
5. Click Scale Up/Down DB System.

For Instructor Use Only.
This document should not be distributed.

Cloning a Virtual Machine DB System

- Cloning creates a copy of a source DB system as it exists at the time of the cloning operation, including the storage configuration software and database volumes.
- When creating a clone, specify a new SSH key and admin password.



13

0

Steps to Clone a Virtual Machine DB System:

1. Open the navigation menu. Under Oracle Database, click Bare Metal, VM, and Exadata.
2. Choose the compartment where the source DB system is located.
3. In the list of DB systems, find the virtual machine DB system you want to clone and click its highlighted name.
4. On the DB System Details page of your source DB system, click Clone. This opens the Clone DB System dialog box.
5. Select a compartment. By default, the DB system is created in your current compartment and you can use the network resources in that compartment.
6. **Display name:** A non-unique, display name for the DB system. An Oracle Cloud Identifier (OCID) uniquely identifies the DB system.
7. **Add public SSH keys:** The public key portion of each key pair you want to use for SSH access to the DB system. You can browse or drag and drop .pub files, or paste in individual public keys. To paste multiple keys, click + Another SSH Key and supply a single key for each entry.
8. The clone will use the SSH keys specified during the cloning operation, and the source DB system will continue to use the SSH keys that were in place prior to the cloning operation.
9. **Choose a license type:** The type of license you want to use for the DB system. Your choice affects metering for billing.

This document should not be distributed.
For Instructor Use Only.

- 10. Virtual Cloud Network:** The VCN in which to create the DB system. Click Change Compartment to select a VCN in a different compartment. Note that the clone can use a different VCN and subnet from the source DB system.
- 11. Client Subnet:** The subnet to which the DB system should attach.
12. Click **Change Compartment** to select a subnet in a different compartment.
- 13. Network Security Groups:** Optionally, you can specify one or more network security groups (NSGs) for your DB system. NSGs function as virtual firewalls, allowing you to apply a set of ingress and egress security rules to your DB system.
- 14. Hostname prefix:** Your choice of host name for the bare metal or virtual machine DB system.
- 15. 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, then 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.
- 16. 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.
- 17. Private IP address:** Optionally, you can define the IP address of the clone.
- 18. Fault domain:** The fault domain in which the DB system resides.
- 19. 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. You can use the same database name that is used in the source DB system.
- 20. Password:** A strong password for the SYS user.
- 21. Confirm password:** Re-enter the password you specified.
22. Clicking **Show Advanced Options** allows you to configure the following:
 23. Tags: If you have permissions to create a resource, then 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. If you are not sure if you should apply tags, skip this option (you can apply tags later) or ask your administrator.
24. Click **Clone DB System**.

Summary

In this lesson, you should have learned how to:

- Update a DB system
- Configure a DB system
- Scale a DB system
- Clone a DB system

 A red square containing a white checkmark icon.

0

For Instructor Use Only.

This document should not be distributed.

Practice 9: Overview

- Practice 9-1: Scaling Up Storage for a Virtual Machine DB System
- Practice 9-2: Changing Shape of a Virtual Machine DB System



0

For Instructor Use Only.
This document should not be distributed.



Patching a DB System on OCI

0

For Instructor Use Only.

This document should not be distributed.

Objectives

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

- Patching of DB systems
- Patching prerequisites
- Performing of patch operations using the Console
- Performing of patch operations using CLI
- Applying interim patches
- Troubleshooting patching failures

0

2

Note: This topic is not applicable to Exadata DB systems.



For Instructor Use Only.

This document should not be distributed.

Patching DB Systems

- Use the Console or CLI to patch a DB system.
- Patching requires a reboot; plan to run it when the users have minimal impact.
- Implement a high availability strategy to reduce the downtime.
- Test the patch on the test system before applying to the production system.
- Back up your database before applying the patch.
- Patch the DB system first and then patch the databases within the system.



0

3

To perform any administrative task in Oracle Cloud Infrastructure such as patching, you must be given the required type of access in a policy written by an administrator. Ensure you have the required access before performing these tasks.

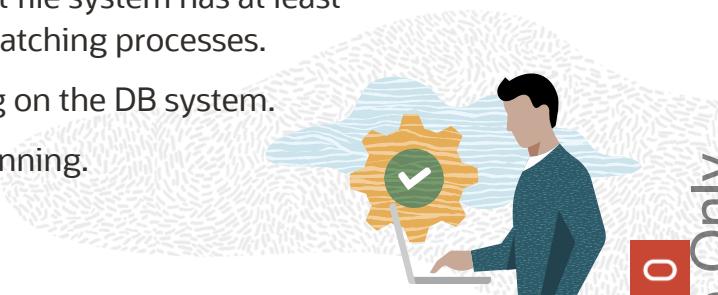
Policy: This is an Identity and Access Management Service (IAM) document that specifies who has what type of access to your resources.

IAM service is covered in the subsequent lessons. For more details on administering OCI resources refer to the Oracle University training *Oracle Cloud Infrastructure Fundamentals*.

Patching Prerequisites

- VCN must be configured with either a service gateway or internet gateway for the DB system.
- Add a route rule with internet gateway as the target and destination CIDR block IP range.
- The DB system must have connectivity to the applicable Swift endpoint for Object Storage.
- The /u01 directory on the database host file system has at least 15 GB of free space for the execution of patching processes.
- The Oracle Clusterware is up and running on the DB system.
- All nodes of the DB system are up and running.

4



O

Prerequisites

The DB system's cloud network (VCN) must be configured with either a service gateway or an internet gateway.

If you use an internet gateway instead of a service gateway, add a route rule with the internet gateway as the target and the destination CIDR block as the IP range listed under Object Storage IP Allocations.

Oracle recommends that you update the backup subnet's security list to disallow any access from outside the subnet and allow egress traffic for TCP port 443 (https) on the IP ranges listed under Object Storage IP Allocations.

In addition to the prerequisites listed, ensure that the following conditions are met to avoid patching failures:

The /u01 directory on the database host file system has at least 15 GB of free space for the execution of patching processes.

The Oracle Clusterware is up and running on the DB system.

All nodes of the DB system are up and running.

Performing Patch Operations on DB System Using Console

1. Open the navigation menu. Under **Database**, click **Bare Metal**, **VM**, and **Exadata**.
2. Select your **Compartment**. A list of DB systems is displayed.
3. Select the DB system you want to patch.
4. Under **Resources**, click **Patches**.
5. Review the list of **patches**.
6. Click the Actions icon (three dots) for the patch and then click one of the actions:
 - **Pre-check:** Check for any prerequisites to make sure that the patch can be successfully applied.
 - **Apply:** This performs the pre-check, and then applies the patch.
7. Confirm when prompted.
8. In the list of patches, click the patch name to display its patch request and monitor the progress of the patch operation.

5

0

For Instructor Use Only.

This document should not be distributed.

Viewing the Patch History of a DB System

To view the patch history of a DB system:

1. Open the navigation menu. Under Database, click **Bare Metal**, **VM**, and **Exadata**.
2. Select your **Compartment**. A list of DB systems is displayed.
3. Select the **DB system** and click the system name to display details about it.
4. Under **Resources**, click Patch History.
 - The history of patch operations for that DB system is displayed.

Viewing Patch History of a Database

To view patch history of a database:

1. Open the navigation menu. Under **Database**, click **Bare Metal**, **VM**, and **Exadata**.
2. Choose your **Compartment**. A list of DB systems is displayed.
3. Select the **DB system** where the database is located and click the system name to display details about it. A list of databases is displayed
4. Select the database you are interested in and click the name to display details.
5. Under **Resources**, click **Patch History**.
 - The history of patch operations for that database is displayed.

0

For Instructor Use Only.

This document should not be distributed.

Performing Patching Using CLI

- Use the command line interface on the DB system to patch a DB system.
- Patches are available from the Oracle Cloud Infrastructure Object Storage service.
- Use the `dbcli` commands to download and apply patches to some or all of the components in your system.

8



0

For Instructor Use Only.
This document should not be distributed.

Updating the CLI with the Latest Commands

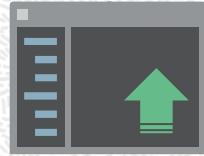
To update the CLI, ensure you have the latest patching commands:

1. Log in to DB system with `opc` user.
2. Switch to `root` user using: `sudo su -`.
3. Update the CLI using:

```
[root@dbsys ~]# cliadm update-dbcli
```

4. Wait for the update job to complete successfully. Check the status of the job using:

```
[root@dbsys ~]# dbcli list-jobs
```



0

For Instructor Use Only.
This document should not be distributed.

Checking the Installed Patches

1. Log in to DB system with `opc` user.

2. Switch to `root` user using `sudo su -`.

3. Display the installed patch versions using:

```
[root@dbsys ~]# dbcli describe-component
```

4. Display the latest patch versions available in Object Storage using:

```
[root@dbsys ~]# dbcli describe-latestpatch
```



O

For Instructor Use Only.
This document should not be distributed.

Patch Server Components

1. Log in to the DB system with `opc` user.
2. Switch to `root` user using `sudo su -`.
3. Update the server components using:

```
[root@dbsys ~]# dbcli update-server
```

4. Note the job ID from the output of the command.
5. Check the job output by using the `dbcli describe-job` command with the job ID:

```
[root@dbsys ~]# dbcli describe-job -i 9a02d111-e902-4e94-bc6b-9b820ddf6ed8
```

6. Verify that the server components were updated successfully by using the `dbcli describe-component` command. The Available Version column should indicate update-to-date.

Patching Database Home Components

1. Log in to the DB system with `opc` user.

2. Switch to root user using `sudo su -`.

3. Get the ID of the database home using:

```
[root@dbsys ~]# dbcli list-dbhomes
```

4. Update the database home components using:

```
[root@dbsys ~]# dbcli update-dbhome -i <Database ID>
```

5. Note the job ID from the output of previous command.

6. Check the job output using:

```
[root@dbsys ~]# dbcli describe-job -i <JOB_ID>
```

7. Verify that the database home components were updated successfully by using the `dbcli describe-component` command. The Available Version column should indicate update-to-date.

Applying Interim Patches

- Applies only to database homes
- Apply an interim patch:
 1. Obtain the applicable interim patch from My Oracle Support.
 2. Review the information in the patch README.txt file.
 3. Use SCP or SFTP to place the patch on your target database.
 4. Shut down each database that is running in the database home:
`srvctl stop database -db <db name> -stopoption immediate -verbose`
 5. Set the Oracle home environment variable to point to the target Oracle home:
`sudo su - oracle export ORACLE_HOME=u01/app/oracle/product/21.0.0/dbhome_1`Change to the directory where you placed the patch and unzip the patch:
`cd <work_dir_where_opatch_is_stored>`
`unzip p26543344_122010_Linux-x86-64.zip`

13

0

For Instructor Use Only.

This document should not be distributed.

Applying Interim Patches

6. Change to the directory with the unzipped patch and check for conflicts:

```
cd 26543344
```

```
$ORACLE_HOME/OPatch/opatch prereq CheckConflictAgainstOHWithDetail -ph ./
```

7. Apply the patch:

```
$ORACLE_HOME/OPatch/opatch apply
```

8. Verify the patch was applied successfully:

```
$ORACLE_HOME/OPatch/opatch lsinventory -detail -oh $ORACLE_HOME
```

9. If the database home contains databases, restart them:

```
$ORACLE_HOME/bin/srvctl start database -db <db_name>
```

Otherwise, run the following command as root user:

```
# /u01/app/<db_version>/grid/bin/setasmgidwrap  
o=/u01/app/oracle/product/<db_version>/dbhome_1/bin/oracle
```

10. If the readme indicates that the patch has a sqlpatch component, run the datapatch command against each database. Before you run datapatch, ensure that all pluggable databases (PDBs) are open.

```
$ORACLE_HOME/OPatch/datapatch
```

0

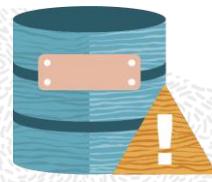
For Instructor Use Only.

This document should not be distributed.

Patching Failures

In addition to the prerequisites, ensure that the following conditions are met:

- The /u01 directory on the DB system file system has at least 15 GB of free space for the execution of patching processes.
- The Oracle Clusterware is up and running on the DB system.
- All nodes of the DB system are up and running.



0

For Instructor Use Only.
This document should not be distributed.

Determining the Problem

- Identify the failed patching operation from the patch history of the DB system or database using the Console.
- A patch that was not successfully applied displays a status of Failed.
- It includes a brief description that caused the failure.
- For more information about the solution you can use database CLI and log files to gather more data.



O

For Instructor Use Only.
This document should not be distributed.

Identifying the Root Cause of the Patching Operation Failure

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

```
dbcli list-jobs
```

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

3. Use the following command to check the details of that job:

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

4. For more information, review the /opt/oracle/dcs/log/dcs-agent.log file.
5. Find the job ID in this file by using the timestamp returned by the job report in step 2.

Summary

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

- Patching of DB systems
- Patching prerequisites
- Performing of patch operations using the Console
- Performing of patch operations using CLI
- Applying interim patches
- Troubleshooting patching failures

0





Practice 10: Overview

—
There are no practices for this lesson.



0

For Instructor Use Only.
This document should not be distributed.

For Instructor Use Only.
This document should not be distributed.



Configuring and Monitoring a Database on OCI

0

For Instructor Use Only.

This document should not be distributed.

Objectives

After completing this lesson, you should be able to:

- Monitor a database
- Monitor a database with Enterprise Manager Express
- Monitor a database with Enterprise Manager Database Control
- Open ports on the DB system
- Update the security list for the DB System
- Explain special considerations for creating and configuring a new PDB

0

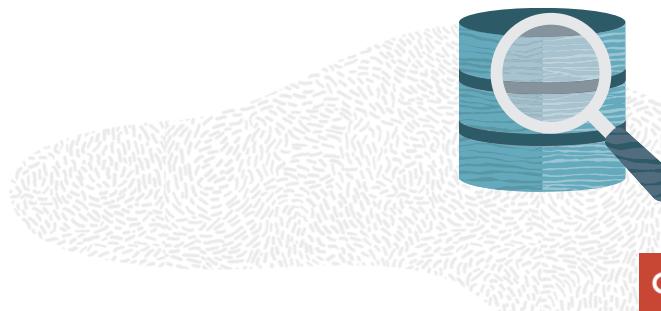


For Instructor Use Only.
This document should not be distributed.

Monitoring a Database

Set up an:

- Enterprise Manager Express console to monitor a version 12.1.0.2 or later database
- Enterprise Manager Database Control console to monitor a version 11.2.0.4 database



0

3

Monitoring a Database

As a DBA you need tools to monitor and manage the database after launching the DB system and creating a database.

In this lesson you will learn how to make use of the available monitoring tools and some special considerations to work with the DB system.

This topic explains how to set up an:

- Enterprise Manager Express console to monitor a version 12.1.0.2 or later database
- Enterprise Manager Database Control console to monitor a version 11.2.0.4 database

Each console is a web-based database management tool inside the Oracle Database. You can use the console to perform basic administrative tasks such as managing user security, memory, and storage, and to view performance information.

For Instructor Use Only.
This document should not be distributed.

Enabling EM Express Console

By default, EM Express console is not enabled on version 21c, 19c, 18c, and 12c databases.

To enable EM Express:

1. SSH to the DB system.
2. Log in as `opc` user, sudo to the `oracle` user, and log in to the database as `SYS`.
3. To enable the console and set its port, execute the command:

```
exec DBMS_XDB_CONFIG.SETHTTPSPORT(<port>);
```

4. To determine the port for a previously enabled console, use:

```
select dbms_xdb_config.getHttpsPort() from dual;
```

5. Open the console's port.
6. Update the security list for the console's port.

4

Enable EM Express console and determine its port number

On 1- and 2-node RAC DB systems, by default, EM Express console is not enabled on version 21c, 19c, 18c, and 12c databases. You can enable it for an existing database as described below, or you can enable it when you create a database by using the `dbcli create-database` command with the `-co` parameter.

You must also update the security list and iptables for the DB system as described later in this topic.

When you enable the console, you'll set the port for the console. The procedure below uses port 5500, but each additional console enabled on the same DB system will have a different port.

Connecting to EM Express Console

- From a web browser, connect to the console using:
`https://<ip_address:<port>/em`
- A login page is displayed. Enter the valid database credentials.

5

0

After you've enabled the console and opened its port, you can connect to EM Express console as shown in the slide.

For Instructor Use Only.
This document should not be distributed.

Enabling Enterprise Manager Database Control

By default, EM Database Control console is not enabled on the 12c database.

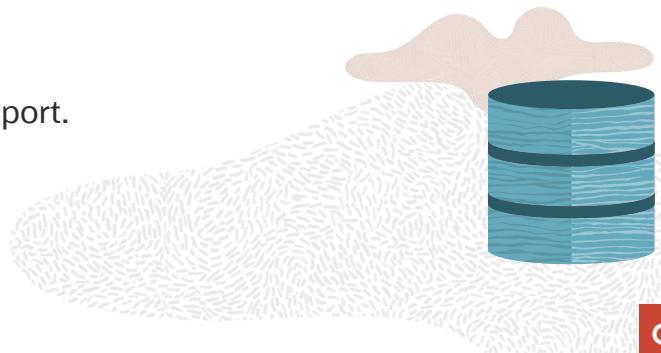
To enable EM Database Control:

1. SSH to the DB system, log in as `opc`, and sudo to the `oracle` user.
2. Use the following command to get the port number:

```
$ emctl status dbconsole
```

3. Open the console's port.
4. Update the security list for the console's port.

0



6

Enable Enterprise Manager Database Control

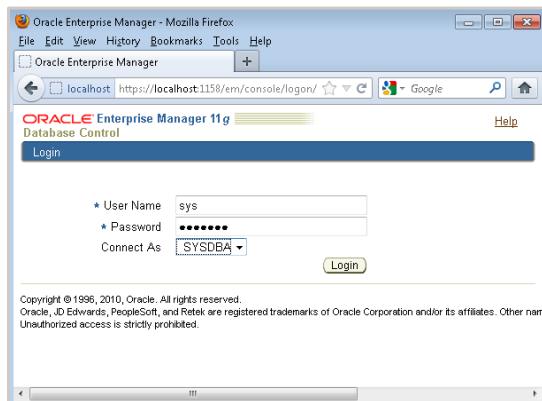
By default, the Enterprise Manager Database Control console is not enabled on the version 12c database. You can enable the console when you create a database by using the `dbcli create-database` with the `-co` parameter.

Port 1158 is the default port used for the first console enabled on the DB system, but each additional console enabled on the DB system will have a different port.

For Instructor Use Only.
This document should not be distributed.

Connecting to EM Database Control Console

- From a web browser, connect to the console using:
`https://<ip_address:<port>/em`
- A login page is displayed. Enter the valid database credentials.



After you've enabled the console and opened its port in the security list, you can connect to EM Database Control console as shown in the slide.

Opening Ports on the DB System

Ports needed for the DB system:

- 6200: For Oracle Notification Service (ONS)
- 5500: For EM Express. 5500 is the default port. Additional EM Express console enabled will have a different port.
- 1158: For EM Database. 1158 Control is the default port. Additional DB console enabled will have a different port.

8

0

Opening Ports on the DB System

Open the following ports as needed on the DB system:

- **6200:** For Oracle Notification Service (ONS)
- **5500:** For EM Express. 5500 is the default port, but each additional EM Express console enabled on the DB system will have a different port.
- **1158:** For Enterprise Manager Database Control. 1158 is the default port, but each additional console enabled on the DB system will have a different port.

For Instructor Use Only.

This document should not be distributed.

Opening a Port on the DB System

1. SSH to the DB system. Log in as `opc` and then sudo to the `root` user.
2. Save a copy of iptables as a backup:

```
[root@dbsys ~]# iptables-save > /tmp/iptables.orig
```

3. Dynamically add a rule to iptables to allow inbound traffic on the console port:

```
[root@dbsys ~]# iptables -I INPUT 8 -p tcp -m state --state NEW -m tcp --dport 5500 -j ACCEPT -m comment --comment "---".
```

4. Make sure the rule was added:

```
[root@dbsys ~]# service iptables status
```

5. Save the updated file to `/etc/sysconfig/iptables`:

```
[root@dbsys ~]# /sbin/service iptables save
```

6. The change takes effect immediately.

7. Update the DB system's security list.

9

0

For Instructor Use Only.

This document should not be distributed.

Updating the Security List for the DB System

1. Review the list of ports.
2. For every port open in iptables, update the security list or create a new security list.
3. Port 1521 default port for Oracle listener is included in the iptables.

10



0

For Instructor Use Only.

This document should not be distributed.

Updating the Security List for the DB System

Review the list of ports and for every port you open in iptables, update the security list used for the DB system, or create a new security list.

Note that port 1521 for the Oracle default listener is included in iptables, but should also be added to the security list.

Updating an Existing Security List

1. Open the navigation menu. Under Database, click **Bare Metal, VM**, and **Exadata**.
2. Choose your **Compartment**. A list of DB systems is displayed.
3. Locate the DB system in the list.
4. Note the DB system's subnet name and click its Virtual Cloud Network.
5. Locate the subnet in the list and then click its security list under Security Lists.
6. Click **Edit All Rules** and add an ingress rule with source type = CIDR, source CIDR=<source CIDR>, protocol=TCP, and port=<port number or port range>.



0

For Instructor Use Only.

This document should not be distributed.

Special Considerations to Create and Configure a New PDB

To create a PDB:

1. SSH to the DB system. Log in as `opc` and then switch to the `oracle` user.
2. Log in to `CDB$ROOT` as `sysdba`.
3. Execute the command to create a PDB:

```
SQL> CREATE PLUGGABLE DATABASE MYPDB2 ADMIN USER pdbadmin  
IDENTIFIED BY QazWsx_123# CREATE_FILE_DEST='+DATA';  
Pluggable database created.
```

4. Execute the command to open the newly created PDB:

```
SQL> ALTER PLUGGABLE DATABASE MYPDB2 OPEN;  
Pluggable database altered.
```

12

O

As a DBA you may need to create a new PDB in addition to the default PDB that gets created at the time of launching a DB system. You can use the above instructions to create a new PDB.

In the next slide you will see some necessary configuration steps you need to perform for this new PDB.

Creating and Activating a Master Encryption Key for a New PDB

To use Oracle Transparent Data Encryption (TDE) in a pluggable database (PDB):

1. Invoke SQL*Plus and log in to the database as the SYS user with SYSDBA privileges.

2. Set the container to the new PDB created:

```
SQL> ALTER SESSION SET CONTAINER = pdb;
```

3. Query V\$ENCRYPTION_WALLET as follows:

```
SQL> SELECT wrl_parameter, status, wallet_type FROM v$encryption_wallet;
```

4. If the STATUS column has a value OPEN_NO_MASTER_KEY, then create and activate the master encryption key.

5. Create and activate a master encryption key in the PDB by executing the command:

```
SQL> ADMINISTER KEY MANAGEMENT SET KEY USING TAG 'tag' FORCE KEYSTORE  
IDENTIFIED BY keystore-password WITH BACKUP USING 'backup_identifier';
```

13

O

As a DBA you will need to perform some additional configuration tasks related to Oracle Transparent Data Encryption (TDE) when you create a new PDB in a DB system.

TDE is enabled by default for the PDB that gets created at the time of launching the DB system, but you need to take care of this when you create a new PDB. Without this you will encounter errors and will not be able to connect to the PDB.

Summary

In this lesson, you should have learned how to:

- Monitor a database
- Monitor a database with Enterprise Manager Express
- Monitor a database with Enterprise Manager Database Control
- Open ports on the DB system
- Update the security list for the DB system
- Explain special considerations for creating and configuring a new PDB

0

For Instructor Use Only.
This document should not be distributed.



Practice 11: Overview

Practice 11-1: Create and Activate a Master Encryption Key for a New PDB



0

For Instructor Use Only.
This document should not be distributed.

For Instructor Use Only.
This document should not be distributed.



Backing Up and Recovering a Database on OCI

0

For Instructor Use Only.

This document should not be distributed.

Objectives

After completing this lesson, you should be able to:

- Back up a database
- Describe Object Storage
- Describe Swift storage-based Object Storage
- Describe local storage
- Recover a database from Object Storage
- Recover a database from a CLI backup
- Recover a database from the Oracle Cloud Infrastructure Classic Object Store
- Troubleshoot backup failures

2



For Instructor Use Only.

This document should not be distributed.

Backing Up a Database

The purpose of a backup is to protect the database against data loss and reconstruct the database after data loss.

Typically, backup administration tasks include the following:

- Planning and testing responses to different kinds of failures
- Configuring the database environment for backup and recovery
- Setting up a backup schedule
- Monitoring the backup and recovery environment
- Troubleshooting backup problems
- Recovering from data loss if the need arises



0

3

Backing up your DB system is a key aspect of any Oracle Database environment. You can store backups in the cloud or in local storage. Each backup destination has advantages and requirements that you should consider. This lesson will help you understand these aspects about database backup in the DB system.

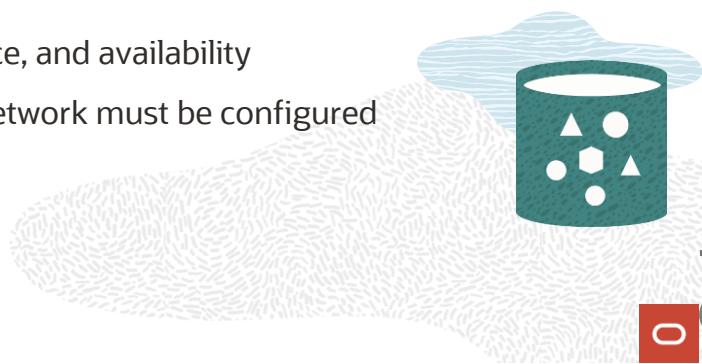
Object Storage

You can store database backups in the Oracle Cloud Infrastructure Object Storage.

Following are the backup considerations for Object Storage:

- Durability: High
- Availability: High
- Backup and Recovery Rate: Medium
- Advantages: High durability, performance, and availability
- Requirements: The DB system's cloud network must be configured with an internet gateway.

0



4

Object Storage (Recommended)

Backups are stored in the Oracle Cloud Infrastructure Object Storage.

Durability: High

Availability: High

Backup and Recovery Rate: Medium

Advantages: High durability, performance, and availability

Requirements: The DB system's cloud network must be configured with an internet gateway. Before deciding on this option, find out if your network administrator will allow an internet gateway.

Local Storage

You can store database backups locally in the Fast Recovery Area of the DB system.

Following are the backup considerations for local storage:

- Durability: Low
- Availability: Medium
- Backup and Recovery Rate: High
- Advantages: Optimized backup and fast point-in-time recovery
- An internet gateway is not required.
- Requirements: If the DB system becomes unavailable, the backup is also unavailable.

Note: Currently OCI does not provide the ability to attach block storage volumes to a DB system.

5

0

Backups are stored locally in the Fast Recovery Area of the DB System.

Durability: Low

Availability: Medium

Back Up and Recovery Rate: High

Advantages: Optimized backup and fast point-in-time recovery

An internet gateway is not required.

Requirements: If the DB system becomes unavailable, the backup is also unavailable.

Currently, Oracle Cloud Infrastructure does not provide the ability to attach block storage volumes to a DB system, so you cannot back up to network-attached volumes.

Swift Object Storage

Swift is the OpenStack object store.

- Offers cloud storage software to store and retrieve large data with a simple API
- Ideal for storing unstructured data that can grow without bounds
- Long-term storage system for large amounts of static data that can be retrieved and updated
- A distributed architecture with no central point of control, providing greater scalability, redundancy, and permanence
- Ideal for cost-effective, scale-out storage
- A fully distributed, API-accessible storage platform that can be integrated directly into applications or used for backup, archiving, and data retention.

6

0

For Instructor Use Only.

This document should not be distributed.

Backing Up to Oracle Cloud Infrastructure Object Storage

Prerequisites and conditions:

- The DB system's cloud network (VCN) must be configured with service gateway or internet gateway.
- DB system must have connectivity to the applicable Swift endpoint for Object Storage.
- The database's archiving mode is set to ARCHIVELOG.
- The `/u01` directory has sufficient free space for the execution of backup processes.
- The `.bash_profile` file for the oracle user does not include any interactive commands.
- No changes were made to the default `WALLET_LOCATION` entry in the `sqlnet.ora` file for automated backups.
- No changes were made to RMAN backup settings by using standard RMAN commands.

7

Prerequisites

The DB system's cloud network (VCN) must be configured with either a service gateway or an internet gateway.

If you use an internet gateway instead of a service gateway, add a route rule with the internet gateway as the target and the destination CIDR block as the IP range.

DB system must have connectivity to the applicable Swift endpoint for Object Storage.

In addition to the prerequisites listed, ensure that the following conditions are met to avoid backup failures:

The database's archiving mode is set to ARCHIVELOG (the default).

The `/u01` directory on the database host file system has sufficient free space for the execution of backup processes.

The `.bash_profile` file for the oracle user does not include any interactive commands (such as `oraenv` or one that could generate an error or warning message).

(For automatic backups) No changes were made to the default `WALLET_LOCATION` entry in the `sqlnet.ora` file.

No changes were made to RMAN backup settings by using standard RMAN commands.

Backing Up Using the Console

- Enable automatic incremental backups.
- Create full backups on demand.
- View the list of managed backups for a database.
- Delete full backups.



O

8

Using the Console

You can use the Console to enable automatic incremental backups, create full backups on demand, and view the list of managed backups for a database. The Console also allows you to delete full backups.

The database and DB system must be in an “Available” state for a backup operation to run successfully. Oracle recommends that you avoid performing actions that could interfere with availability (such as patching and Data Guard operations) while a backup operation is in progress. If an automatic backup operation fails, the Database service retries the operation during the next day’s backup window. If an on-demand full backup fails, you can try the operation again when the DB system and database availability are restored.

Enabling or Disabling Automatic Backups for a DB

1. Open the navigation menu. Under Database, click **Bare Metal**, **VM**, and **Exadata**.
2. Choose your **Compartment**. A list of DB systems is displayed.
3. Find the DB system where the database is located and click the system name to display details about it. A list of databases is displayed.
4. Find the database for which automatic backup needs to be enabled or disabled and click its name to display database details. The details indicate whether automatic backups are enabled.
5. Under **Resources**, click **Backups**.
6. A list of backups is displayed.
7. Click **Enable Automatic Backup** or **Disable Automatic Backup**, as applicable.
8. Confirm when prompted.

9

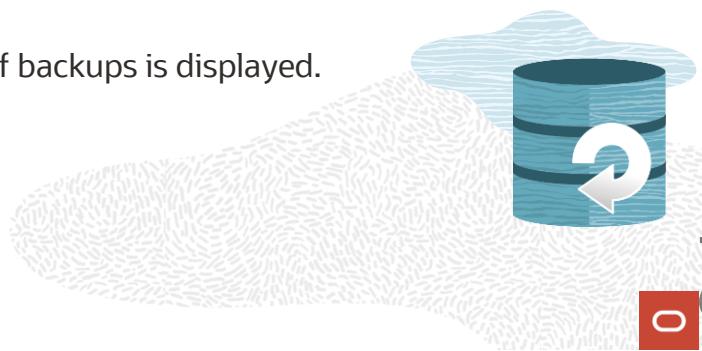
0

For Instructor Use Only.

This document should not be distributed.

Creating an On-Demand Full Backup of a Database

1. Open the navigation menu. Under Database, click **Bare Metal, VM**, and **Exadata**.
2. Choose your **Compartment**. A list of DB systems is displayed.
3. Find the DB system where the database is located and click the system name to display details about it. A list of databases is displayed.
4. Find the database for which an on-demand full backup needs to be created and click its name to display database details.
5. Under **Resources**, click **Backups**. A list of backups is displayed.
6. Click **Create Backup**.



0

For Instructor Use Only.
This document should not be distributed.

Deleting a Full Backup from Object Storage

1. Open the navigation menu. Under Database, click **Bare Metal**, **VM**, and **Exadata**.
2. Choose your **Compartment**. A list of DB systems is displayed.
3. Find the DB system where the database is located and click the DB system name to display details. A list of databases is displayed.
4. Find the database you are interested in and click its name to display database details.
5. Under **Resources**, click **Backups**. A list of backups is displayed.
6. Click the Actions icon (three dots) for the backup you are interested in and then click **Delete**.
7. Confirm when prompted.

Note: Backups cannot be deleted explicitly, unless the database is not terminated. Automatic backups will be deleted at the end of the selected preset retention period of 7, 15, 30, 45, or 60 days.

Backing Up to Object Storage Using RMAN

RMAN can be used to manage backups of both bare metal or virtual machine DB to Object Storage.

Prerequisites:

- A DB system and a database to back up
- The DB system's cloud network (VCN) must be configured with an internet gateway.
- An existing Object Storage bucket to use as the backup destination
- An auth token generated by Oracle Cloud Infrastructure
- Tenancy-level access to Object Storage for the user specified to use the backup module

Backing Up to Object Storage Using RMAN

Recovery Manager (RMAN) can be used to manage backups of your bare metal or virtual machine DB system database to your own Object Storage.

To back up to the service you'll need to create an Object Storage bucket for the backups, generate a password for the service, install the Oracle Database Cloud Backup Module, and then configure RMAN to send backups to the service. The backup module is a system backup to tape (SBT) interface that's tightly integrated with RMAN, so you can use familiar RMAN commands to perform backup and recovery operations.

Prerequisites

A DB system and a database to back up

The DB system's cloud network (VCN) must be configured with an internet gateway. Note that the network traffic between the DB system and Object Storage does not leave the cloud and never reaches the public internet.

An existing Object Storage bucket to use as the backup destination. You can use the Console or the Object Storage API to create the bucket.

An [auth token](https://docs.cloud.oracle.com/iaas/Content/General/Concepts/credentials.htm#Swift) (<https://docs.cloud.oracle.com/iaas/Content/General/Concepts/credentials.htm#Swift>) generated by Oracle Cloud Infrastructure. You can use the Console or the IAM API to generate the password.

The user name (specified when you install and use the backup module) must have tenancy-level access to Object Storage. An easy way to do this is to add the user name to the Administrators group. However, that allows access to all of the cloud services.

Installing the Backup Module on the DB System

1. SSH to the DB system, log in as `opc`, and sudo to the `oracle` user.
2. Change to the directory that contains the backup module `opc_install.jar` file:

```
cd /opt/oracle/oak/pkgrepos/oss/odbc5
```

3. Use the following command syntax to install the backup module:

```
java -jar opc_install.jar -opcId <user_id> -opcPass  
'<auth_token>' -container <bucket_name> -walletDir  
~/hsbtwallet/ -libDir ~/lib/ -configfile ~/config -host  
https://swiftobjectstorage.<region_name>.oraclecloud.com/v1/<  
tenant>
```

Configuring RMAN

1. On the DB system, ORACLE_SID environment variables using the oraenv utility.
2. Connect to the database using RMAN.
3. Configure RMAN to use the SBT device and point to the config file that was created while installing the backup module:

```
RMAN> CONFIGURE CHANNEL DEVICE TYPE 'SBT_TAPE' PARMs  
'SBT_LIBRARY=/home/oracle/lib/libopc.so,  
SBT_PARMs=(OPC_PFILE=/home/oracle/config)';
```

4. Configure RMAN to use SBT_TAPE by default:

```
RMAN> CONFIGURE DEFAULT DEVICE TYPE TO SBT_TAPE;  
RMAN> CONFIGURE CONTROLFILE AUTOBACKUP FORMAT FOR DEVICE TYPE SBT_TAPE  
TO '%F';  
RMAN> CONFIGURE ENCRYPTION FOR DATABASE ON;
```

Backing Up the Database Using RMAN

1. Set the database encryption:

```
RMAN> SET ENCRYPTION IDENTIFIED BY "password" ONLY;
```

Note that this setting is not permanent; it must be set for each new RMAN session.

2. Back up the database and archivelogs:

```
RMAN>BACKUP INCREMENTAL LEVEL 0 SECTION SIZE 512M DATABASE PLUS  
ARCHIVELOG;
```

3. Back up archivelogs frequently to minimize potential data loss and keep multiple backup copies as a precaution:

```
RMAN> BACKUP ARCHIVELOG ALL NOT BACKED UP 2 TIMES;
```

Backing Up to Local Storage Using the Database CLI

1. SSH to the DB system. Log in as `opc` and then sudo to the `root` user.

2. Create a backup configuration using:

```
[root@dbsys~]# dbcli create-backupconfig -n probackup -d disk -w 5
```

3. Get the ID of the database using: [root@dbsys~]# dbcli list-databases

4. Get the ID of the backup configuration using:

```
[root@dbbackup backup]#/opt/oracle/dcs/bin/dbcli list-backupconfigs
```

5. Associate the backup configuration ID with the database ID using:

```
[root@dbsys ~]# dbcli update-database -bi 78a2a5f0-72b1-448f-bd86-cf41b30b64ee -i 71ec8335-113a-46e3-b81f-235f4d1b6fde
```

6. Initiate the database backup using:

```
[root@dbsys~]# dbcli create-backup -i 71ec8335-113a-46e3-b81f-235f4d1b6fde
```

Recovering a Database from Object Storage

Prerequisites:

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



0

For Instructor Use Only.
This document should not be distributed.

Restoring an Existing Database Using the Console

1. Open the navigation menu. Under Database, click **Bare Metal**, **VM**, and **Exadata**.
2. Choose your **Compartment**. A list of DB systems is displayed.
3. Select the DB system and click the system name to display details. A list of databases is displayed.
4. Find the database to be restored and click its name to display details about it. A list of backups is displayed in the default view of the database details. The list of backups for a database can be accessed by clicking **Backups** under **Resources**.
5. Click the Actions icon (three dots) for the backup to be used and then click **Restore**.
6. Select one of the following options, and click **Restore Database**:
 - **Restore to the latest:** Restores the database to the last known good state with the least possible data loss
 - **Restore to the timestamp:** Restores the database to the timestamp specified
 - **Restore to SCN:** Restores the database using the SCN specified. This SCN must be valid.
7. Confirm when prompted.

Restoring a Database Using a Specific Backup from Object Storage

1. Open the navigation menu. Under **Database**, click **Bare Metal**, **VM**, and **Exadata**.
2. Choose your **Compartment**. A list of DB systems is displayed.
3. Find the DB system where the database is located and click the system name to display details about it. A list of databases is displayed.
4. Find the database you want to restore and click its name to display details about it.
5. Under **Resources**, click **Backups**. A list of backups is displayed.
6. Click the Actions icon (three dots) for the backup you are interested in and then click **Restore**.
7. Confirm when prompted.

19

0

Note: You cannot delete an incremental backup nor restore from a specific incremental backup.

For Instructor Use Only.
This document should not be distributed.

Creating a New Database from a Backup

1. Open the navigation menu. Under **Database**, click **Bare Metal**, **VM**, and **Exadata**.
2. Click **Standalone Backups**.
3. In the Standalone Backups, find the backup you want to use to create the database.
4. Click the Actions icon (three dots) for the backup you are interested in and then click **Create Database**.
5. In the **Create Database from Backup** dialog box, select **Use Existing DB System**.
6. Enter the following:
 - **DB System:** The DB system in which you want to create the database
 - **Database Admin Password:** A strong password for SYS, SYSTEM, PDB Admin, and TDE wallet for the new database
7. Click **Create Database**.

20

0

Note: A standalone backup list is available only if you have taken on-demand backups.

For Instructor Use Only.

This document should not be distributed.

Launching a New DB System from a Backup

1. Open the navigation menu. Under **Database**, click **Bare Metal**, **VM**, and **Exadata**.
2. Click **Standalone Backups**.
3. In the list of standalone backups, find the backup you want to use to create the database.
4. Click the Actions icon (three dots) for the backup you are interested in and then click **Create Database**.
5. In the **Create Database from Backup** dialog box, select **Launch New DB System**.
6. Enter the required details.
7. Click **Create Database**.

Recovering a Database from a CLI Backup

- The backups must be created with `dbcli create-backup` command.
- Backups reside in the local Fast Recovery Area of the DB system.
- If the database is configured with Transparent Data Encryption (TDE), make sure the password-based and auto-login TDE wallets are present in the following location:

```
/opt/oracle/dcs/commonstore/wallets/tde/<db_unique_name>
```



Recovering the Database Using CLI

1. SSH to the DB system. Log in as `opc` and then sudo to the `root` user.
2. Find the ID of the database to recover using:

```
[root@dbsys ~]# dbcli list-databases
```

3. Initiate the recovery using:

```
[root@dbsys ~]# dbcli create-recovery --dbid 5a3e980b-e0fe-4909-9628-fcefe43b3326 --recoverytype Latest
```

Note the job ID in the command output.

4. Check the status of the recovery using:

```
[root@dbsys ~]# dbcli describe-job -i c9f81228-2ce9-43b4-88f6-b260d398cf06
```

Recovering a Database from the Oracle Cloud Infrastructure Classic Object Store

Prerequisites:

- The service name, identity name, container, user name, and password for Oracle Cloud Infrastructure Object Storage Classic
- The backup password if password-based encryption was used when backing up to Object Storage Classic
- The source database ID, database name, database unique name (for setting up storage)
- If the source database is configured with TDE, backup of the wallet and the wallet password
- Tnsnames to set up for any database links
- The output of `Opatch lsinventory` for the source database `Oracle_home`, for reference
- A copy of the `sqlpatch` directory from the source database home. This is required for rollback in case the target database does not include these patches.

24

0

Here the source database is the database backup in Object Storage Classic.

The target database is the new database on a DB system in Oracle Cloud Infrastructure.

For Instructor Use Only.

This document should not be distributed.

Steps to Recover a Database from OCIC Object Store

1. Set up storage on the DB system.
2. Choose an `ORACLE_HOME` or the database for restore and then switch to that home.
3. Copy the source database wallets.
4. Install the Oracle Database Backup Module.
5. Allocate an RMAN SBT channel.
6. Ensure decryption is turned on for RMAN restore sessions.
7. Restore `spfile` and update the database parameters.
8. Restore the control file.
9. Restore the database and reset the logs.
10. Register the database on the DB system.
11. Update `tnsnames.ora`.

25

0

For more details refer to this link:

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

For Instructor Use Only.

This document should not be distributed.

Troubleshooting Backup Failures

Database backup can fail for various reasons:

- The database cannot access the object store.
- There are problems on the host or with the database configuration.



0

26

For more details refer to this link:

<https://docs.cloud.oracle.com/iaas/Content/Database/Troubleshooting/Backup/backupfail.htm>

Swift API Endpoints:

US West: <https://swiftobjectstorage.us-phoenix-1.oraclecloud.com>

US East: <https://swiftobjectstorage.us-ashburn-1.oraclecloud.com>

EMEA UK: <https://swiftobjectstorage.uk-london-1.oraclecloud.com>

EMEA Germany: <https://swiftobjectstorage.eu-frankfurt-1.oraclecloud.com>

For Instructor Use Only.
This document should not be distributed.

Identifying the Root Cause of a Backup Failure

1. Log on to the host as the `root` user and navigate to the `/opt/oracle/dcs/bin/` directory.
2. Determine the sequence of operations performed on the database:
`dbcli list-jobs | grep -i <dbname>`
Note the last job ID listed with a status other than Success.
3. Use the following command to check the details of that job:
`dbcli describe-job -i <job_ID> -j`
4. If you require more information, review the `/opt/oracle/dcs/log/dcs-agent.log` file.
5. If the problem details suggest an RMAN issue, review the RMAN logs in the `/opt/oracle/dcs/log/<hostname>/rman/bkup/<db_unique_name>/rman_bakup/<yyyy-mm-dd>` directory.

27

0

For Instructor Use Only.

This document should not be distributed.

Object Store Connectivity Issues

Backing up your database to Oracle Cloud Infrastructure Object Storage requires that the host can connect to the applicable Swift endpoint. To test the connectivity:

1. Create a Swift user in your tenancy.
2. Execute the command with Swift user to check connectivity between host and object store:

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

3. If there is connectivity problem to the object store, check the Prerequisites for how to configure object store connectivity.

Known Challenges for Database Backup Failure

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

- Interactive commands in the Oracle profile
- Full file system
- Incorrect version of the Oracle Database Cloud backup module
- Changes to the site profile file (`glogin.sql`)



29

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

Interactive Commands in the Oracle Profile

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

Full File System

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

Incorrect Version of the Oracle Database Cloud Backup Module

Your system might not have the required version of the backup module (`opc_installer.jar`). Review the title “Unable to use Managed Backups in your DB System” for details about this known issue, in this link: <https://docs.cloud.oracle.com/iaas/Content/knownissues.htm#six>.

To fix the problem, you can follow the procedure in that section or simply update your DB system and database with the latest bundle patch.

Changes to the Site Profile File (`glogin.sql`)

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

Improper Database State Affecting Backups

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

- Database not running during backup
- Archiving mode set to NOARCHIVELOG
- Stuck database archiver process and backup failures
- Temporary tablespace errors
- RMAN configuration and backup failures
- RMAN retention policy and backup failures
- Loss of object store wallet file and backup failures

30

0

Database Issues

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

Database Not Running during Backup

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

Archiving Mode Set to NOARCHIVELOG

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

Stuck Database Archiver Process and Backup Failures

Backups can fail when the database instance has a stuck archiver process. For example, this can happen when the flash recovery area (FRA) is full. You can check for this condition using the `srvctl status database -db <db_unique_name> -v` command. If the command returns the following output, you must resolve the stuck archiver process issue before backups will succeed.

Temporary Tablespace Errors

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

RMAN Configuration and Backup Failures

Editing certain RMAN configuration parameters can lead to backup failures in Oracle Cloud Infrastructure. To check your RMAN configuration, use the show all command at the RMAN command-line prompt.

RMAN Retention Policy and Backup Failures

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

Loss of ObjectStore Wallet File and Backup Failures

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

For Instructor Use Only.
This document should not be distributed.

TDE Wallet and Backup Failures

- Incorrect TDE wallet location specification
- Incorrect state of the TDE wallet
- Incorrect configuration related to the TDE wallet
- Missing TDE wallet file
- Missing auto login wallet file



32

Incorrect TDE Wallet Location Specification

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

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

Incorrect State of the TDE Wallet

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

The ORACLE_UNQNAME environment variable was not set when the database was started using SQL*Plus.

A pluggable database was added with an incorrectly configured master encryption key.

Incorrect Configuration Related to the TDE Wallet

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

Missing TDE Wallet File

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

Missing Auto Login Wallet File

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

Summary

In this lesson, you should have learned how to:

- Back up a database
- Describe Object Storage
- Describe Swift storage-based object storage
- Describe local storage
- Recover a database from Object Storage
- Recover a database from a CLI backup
- Recover a database from the Oracle Cloud Infrastructure Classic Object Store
- Troubleshoot backup failures

33

O



For Instructor Use Only.

This document should not be distributed.

Practice 12: Overview

This practice covers the following topics:

- Practice 12-1: Create an Auth Token
- Practice 12-2: Enabling or Disabling Automatic Backups
- Practice 12-3: Creating On-Demand Backup Using the Console
- Practice 12-4: Backing Up to Object Storage Using RMAN
- Practice 12-5 Backing Up to Local Storage Using CLI
- Practice 12-6: Recovering a Database Using CLI
- Practice 12-7: Restoring an Existing Database Using the Console
- Practice 12-8: Performing Point-in-Time Recovery of a Database



0

For Instructor Use Only.
This document should not be distributed.



Oracle Cloud Infrastructure Security

0

For Instructor Use Only.

This document should not be distributed.

Objectives

After completing this lesson, you should be able to:

- Identify key features of the Identity and Access Management Service
- Identify security features of Oracle Database on Oracle Cloud Infrastructure
- Describe how Oracle Cloud Infrastructure resources are secured
- Explain why security is a shared responsibility
- Describe Data Safe



0

For Instructor Use Only.
This document should not be distributed.

OCI Security Features: Overview of Database Service

No.	Security capability	OCI DBCA security feature
1	Instance security isolation	OCI Bare Metal (BM) instance
2	Network security and access control	VCN, VCN security lists, VCN public and private subnets, VCN route table
3	Secure and highly available connectivity	VPN DRGs
4	User authentication and authorization	IAM tenancy, compartments and security policies, console password, API signing key, SSH keys
5	Data encryption	DBaaS TDE, RMAN encrypted backups, storage and object encryption at rest
6	End-to-end TLS	LBaaS with TLS1.2, customer-provided certificates
7	Auditing	OCI API audit logs

3

0

Security Features of the OCI Database Service

This includes instance security isolation, network security and total isolation, IPSec VPNs and FastConnect dedicated network circuits, and granular controls for users, in addition to secure methods for API and SSH access. We also have TDE on by default, with all backups and block and object storage encrypted by default. We will also look at the OCI load balancer, which supports encryption and auditing via the OCI audit logs.

For Instructor Use Only.

This document should not be distributed.

Identity and Access Management Service

- Identity and Access Management (IAM) service enables you to control who can do what in your OCI account:
 - Control who can access your OCI account
 - What services and resources they can use
 - How they can use these services and resources
- Resource is a cloud object that you create and use in OCI (for example, compute instances, block storage volumes, and Virtual Cloud Networks).
- IAM uses traditional identity concepts, such as principals, users, groups, and policies.
- OCI IAM introduces a new feature called compartments.

4

O

For Instructor Use Only.

This document should not be distributed.

Principals

- A principal is an IAM entity that is allowed to interact with OCI resources.
- There are two types of principals:
 - IAM users/groups
 - When customers sign up for an OCI account, the first IAM user is the default administrator.
 - The default administrator sets up other IAM users and groups.
 - Users are persistent identities set up through IAM service to represent individual people or applications.
 - Users enforce the security principle of least privilege.
 - A user has no permissions until placed in one (or more) group.
 - A group has at least one policy with permission to tenancy or a compartment.
 - Group is a collection of users who all need the same type of access to a particular set of resources.
 - A user can be a member of multiple groups.
 - Instance principals
 - Instance principals let instances (and applications) make API calls against other OCI services, removing the need to configure user credentials or a configuration file.

5

O

A principal is an IAM entity that is allowed to interact with OCI resources. The three principals that can authenticate and interact with OCI resources are root users, IAM users, and group and instance principals. The root user is associated with the actual OCI account and cannot be restricted in any way. IAM users and groups are persistent identities that can be controlled through the IAM service.

For Instructor Use Only.

This document should not be distributed.

Authentication

IAM service authenticates a principal by:

- User name, password
 - You use the password to sign in to the web console.
 - An administrator will provide you with a one-time password when setting up your account.
 - At your first login, you are prompted to reset the password.
- API signing key
 - The API signing key is required when using the OCI API in conjunction with the SDK/CLI.
 - The key is an RSA key pair in the PEM format (minimum 2048 bits required).
 - In the interfaces, you can copy and paste the PEM public key.

Add Public Key help cancel

Note: Public Keys must be in the PEM format.

PUBLIC KEY

```
-----BEGIN RSA PUBLIC KEY-----
MIIBCgKCAQEATxVsJ1rZiz/w07fwm3g+xnvdxDXTvG6oPw4f4D60d4q8YvUqy
K/nmmFL63Txx7ng53qut96rL4jra1Wtm6DvxBuyJR+c5z4kIcc6o/miqHvYLiuza
zsRwXpgjxV8pQc/ahsVP1ldvAqVbkeLXd9aEeHczg+Ak5ICmnI+SHlg/6Ph8jIH
Z9IKpxTdGPQkOn2HeRhT8cczq95KtTvdGMl6El9ADCoYzx955Xv8enkVs6SKnHj
KmdaJ1mo3zXy5GqcjpA1jBgJASx+LGJ0vMmDjTHfoAGw5601hTAX9LJ9Ud670ff
jEvn/jEQqcincf0dsfUGaelRb1L9G44ESuxQIDAQAB
-----END RSA PUBLIC KEY-----
```

Add

6

0

When you log in to the OCI console as a root user or IAM user, you use a username–password combination. A program that accesses the API with an IAM user or root user uses an API signing key.

For Instructor Use Only.
This document should not be distributed.

Authorization

- Authorization is the process of specifying what actions an authenticated principal can perform.
- Authorization in IAM service is done by defining specific privileges in policies and associating them with principals.
- Authorization supports the security principle of least privilege; by default, users are not allowed to perform any actions. (Policies can be attached only to groups, not to users.)
- Policies comprise one or more statements, which specify what groups can access what resources and what level of access users in that group have.
- Policies are written in human-readable format:
 - Allow group <group_name> to <verb> <resource-type> in tenancy
 - Allow group <group_name> to <verb> <resource-type> in compartment <compartment_name> [where <conditions>]
- Policies can be attached to a compartment or the tenancy. Where you attach it controls who can then modify it or delete it.

7

0

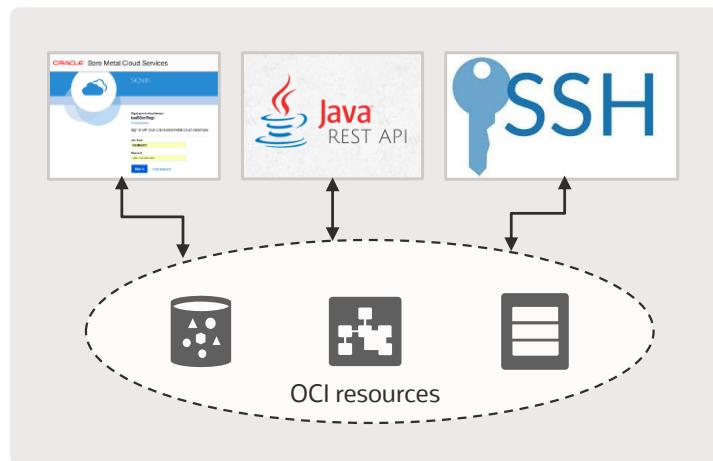
Note that in OCI, policies cannot be attached directly to IAM users; this can be done only to groups.

For Instructor Use Only.

This document should not be distributed.

User Authentication: OCI Security Credentials

- Console password
 - Access to the OCI Console
- API signing key
 - Access to OCI REST APIs
 - Signed API calls over TLS1.2
 - 2048-bit RSA key pair
- SSH key pair
 - Access to OCI instances
 - 2048-bit RSA or DSA, 128-bit ECC



8

0

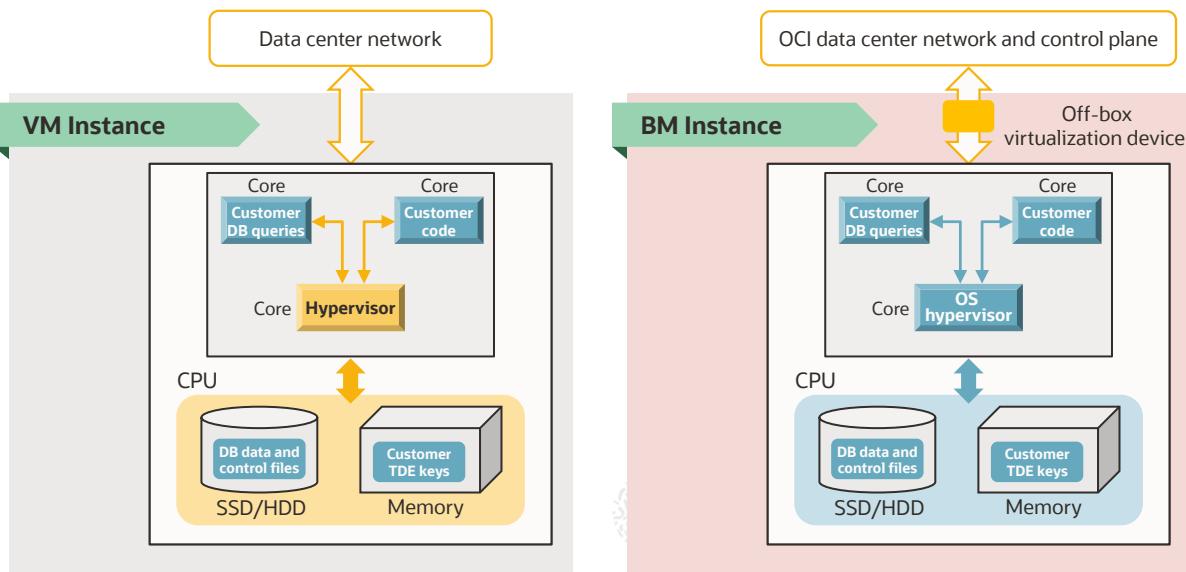
Console access is done by a password.

Multi-factor authentication can be enabled and disabled by users for their own accounts.

The access to the OCI API is done via a 2048-bit key pair. This is done on a per-user basis. These keys can be used to access OCI not only with the REST API, but also CLI, the SDKs, the chef knife plug-in, and terraform.

Instances by default only allow access to SSH over the network. The instances are configured for SSH access with key-based authentication only. Password login, root login, and weak keys are disabled by default. This includes Ubuntu, Centos, and Oracle Linux as well as the database nodes.

Instance Isolation: OCI Database Bare Metal (BM) Instance



9

O

For every instance we have isolation in place.

For VM shapes, the hypervisor separates instances from each other by default. Memory, CPUs, and storage data are never accessible by another tenant. For VMs, the network is virtualized off-box so there is no shared network or vSwitch isolation issues on the host.

On VMs the storage is done to block, which is highly secure—rotating encryption keys and data to the service is encrypted in flight over dedicated networks—and not shared with the VM networks. Block also stores the data at rest encrypted.

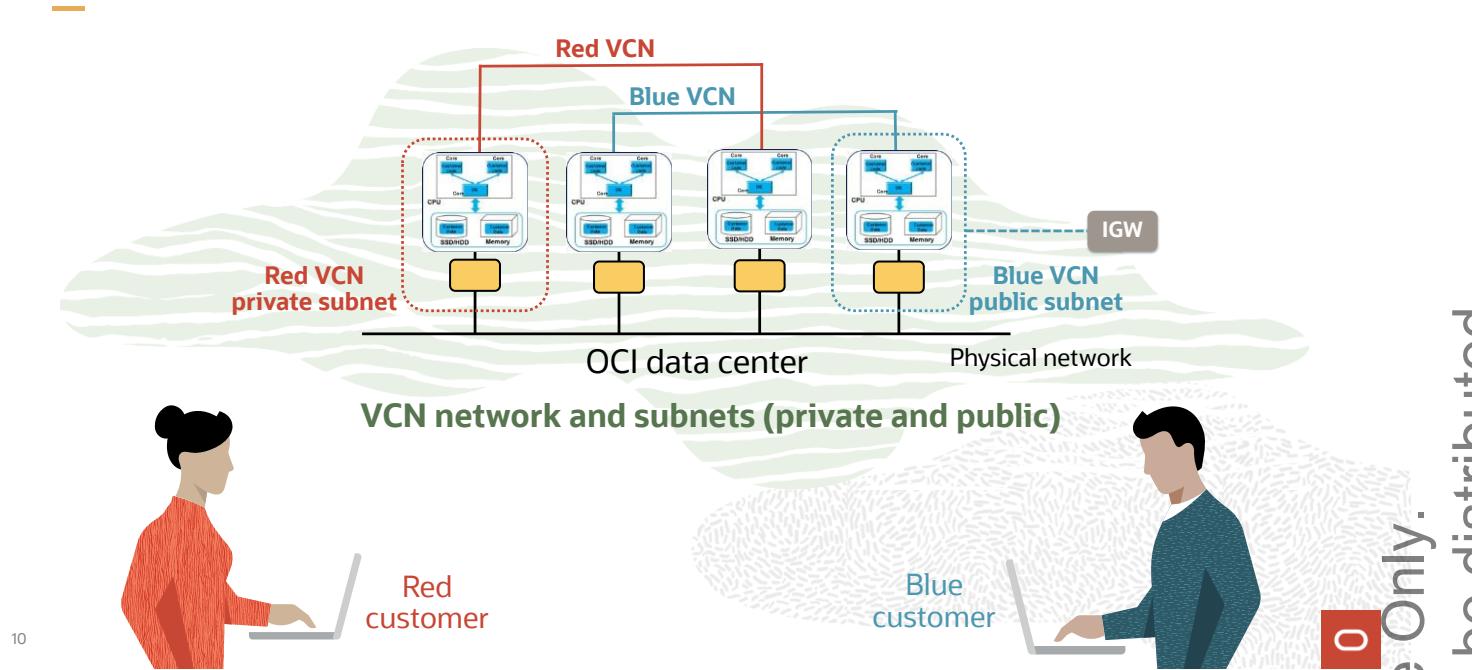
On bare metal database instances including RAC, there is no shared tenancy model at all. The machines and the network are fully dedicated to the tenant. There is nothing shared. The entire CPU and memory are dedicated to the tenant, the network is fully virtualized off-box, and storage is fully encrypted.

For Exadata, quarter- and half-rack shapes can be shared but never on the same physical storage or compute nodes. There is a virtual context in each of the compute nodes to isolate operators from common resources. Administrators still have full access to the context but cannot make system-wide changes—just changes that affect their own databases, compute, and storage nodes.

Networking and cluster networking are divided such that they are non-blocking and storage and compute nodes are dedicated to a user's shape. The cluster network is partitioned so that no inter-tenant data leakage or contention is possible.

For Instructor Use Only.
This document should not be distributed.

Network Security: Virtual Cloud Network (VCN)



10

O

Networking in OCI is completely virtualized. Access can be restricted between the tenancies and within the tenancy itself.

Tenancies are completely network isolated. Permissions can be used to isolate networking between compartments and between VCNs.

Within a given VCN, subnets can be created on different availability domains. Subnets can either be public (where instances can optionally receive a public IP address) or private (where it is not possible for instances to receive a public IP address and they will have to rely on networking from something other than the internet gateway).

Because the networking is done off-box, no amount of rooting or compromising the hypervisor on shared hosts or abuse on bare metal hosts will give access to other networks. It's not isolated at the vSwitch; it's done off host.

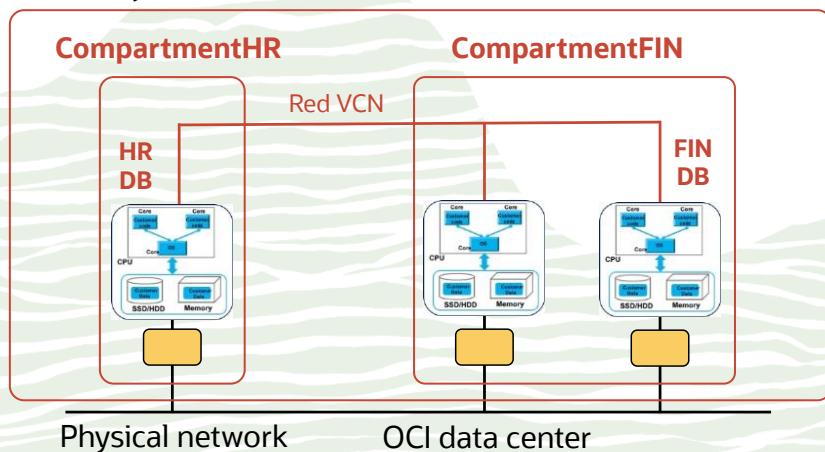
The networking in OCI provides a security environment to create tiers and provide security to keep public traffic away from the database as well as to keep the database service away from friendly-fire incidents within the tenancy with compartments and policy.

For Instructor Use Only.

This document should not be distributed.

User Authorization: OCI IAM

Tenancy of Red customer



IAM Security Policies:

Allow group DatabaseAdmins to manage databases in tenancy

Allow group HR to read databases in CompartmentHR

Allow group Finance (FIN) to read/write databases in CompartmentFIN

11

o

With IAM, policies can isolate who can interact with the database service.

We can give access across the entire tenancy for a group of database administrators to fully manage all databases. But groups that enabled networking or other permissions would not be able to make changes to the service.

In addition to that, we can create policies that isolate users of their own compartments from one another or keep users in their own compartments from managing their own database instances. A policy could be defined to allow users in the HR group to perform read-only operations on database service instances in their compartments, and another can be made to allow those database users in the finance compartment. Keep in mind these are restrictions to the OCI Database service itself, and each service has a definition of what inspect, read, user, and manage can do.

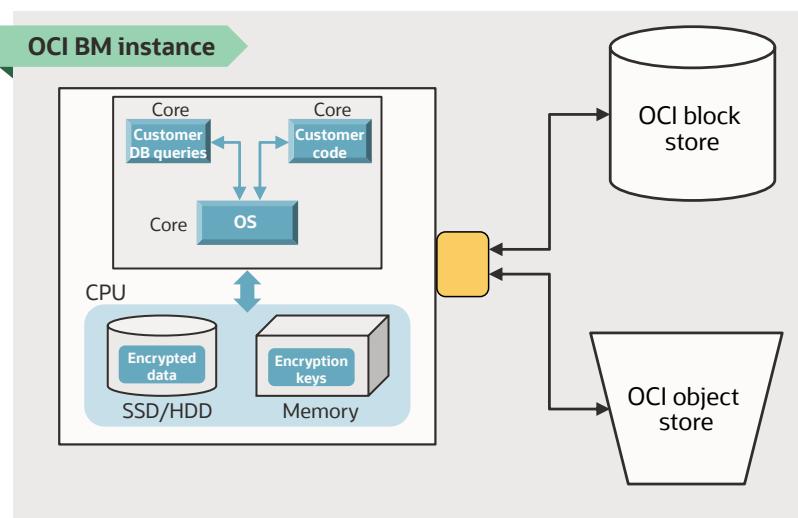
For the database, service policies can be implemented on:

- db-systems
- db-nodes
- db-homes
- Individual databases

Permissions are given as follows: inspect > read > use > manage. This model is done with least privilege. No statement for a group to a given resource means no access.

Permissions are as granular as to include individual database, database backup operations, database home management, db node management (for example, start, stop, restart), general backup operations including managing database backups, and Data Guard failover operations.

Data Encryption: OCI Storage Encryption



- Customer encryption
 - Client-side encryption
 - Customer-controlled keys
- OCI block storage
 - Encryption at rest
- OCI object store
 - Per-object encryption

12

O

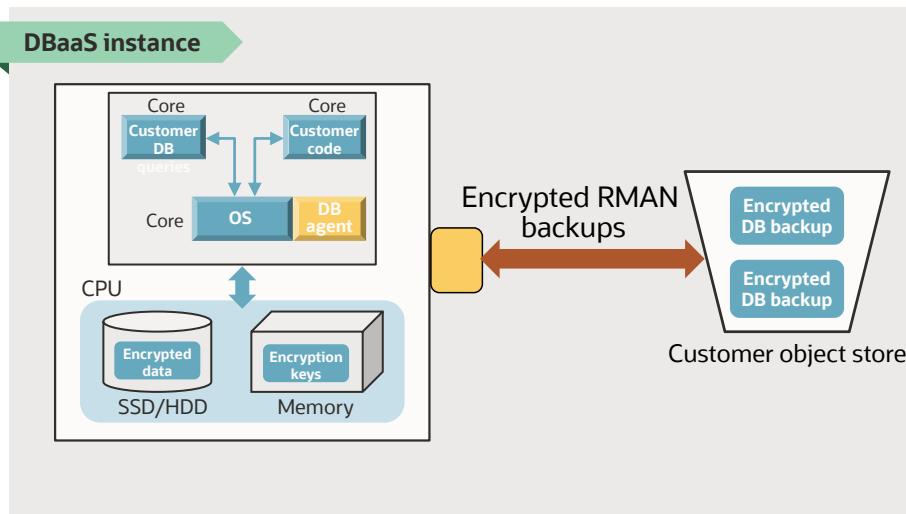
OCI block storage has in-flight data encryption as well as encryption at rest. Data is persisted to a minimum of three copies in an Availability Domain are durable and secure.

OCI object storage has a per-object security and encryption mechanism. Authentication requests to objects can be done at the bucket level or object level. The object store itself is a region and maintains a minimum of three copies of an object at all times (more is more common) and spreads them throughout the region. Access to the object is secure and encrypted and these objects are encrypted at rest as well.

For Instructor Use Only.

This document should not be distributed.

Data Encryption: OCI Database Service TDE



- Oracle TDE encryption (by default)
- TDE master key in Oracle Wallet on BM instance
- Encrypted RMAN backups (by default)

13

0

The OCI database service is set by default to enable TDE on all databases by default.

The keys are managed by the service as well, so if the system or databases are restarted, the keys are automatically used to reopen/restart the databases.

TDE can be disabled if more performance is needed, but TDE is on by default.

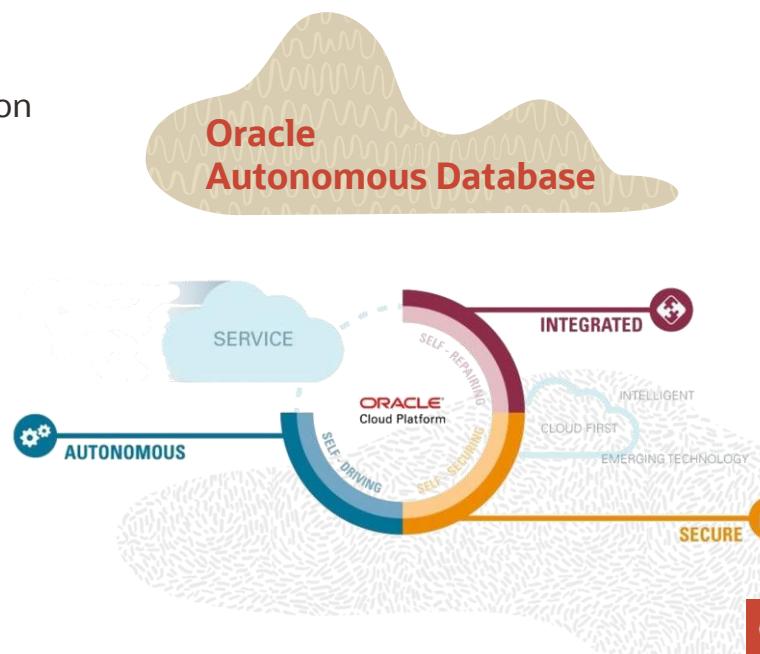
The administrator of the OCI database system can get to the mount point, which contains all the wallets for all the databases and uses tools like orapki and Wallet Manager to manage those keys.

By default all of the backups are also encrypted. If automatic backups are selected, the full backups to the object will be fully encrypted. Restore operations require the correct password or manual key management.

In the Cloud, Security Is a **Shared** Responsibility

Security **Managed by Oracle**

- Network security and threat detection
- Strong platform security
- Automatic database patches
- Strict administrative control
- Data encryption by default



14

Security

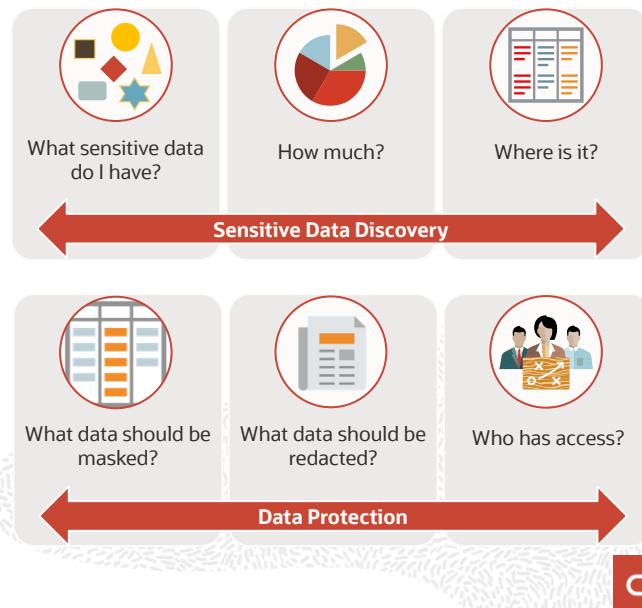
What Can I Do to Prepare?

Identify your assets

- Know what data you have and where.

Secure all databases

- Make sure there are no insecure settings, default passwords, and so on.
- Remove unnecessary privileges.
- Determine what data should be masked in dev and test environments.
- Determine what data should be redacted or dynamically masked in applications.



Security

What Can I Do to Prepare?

Encrypt your data

- All cloud services encrypt data.

Back up your data

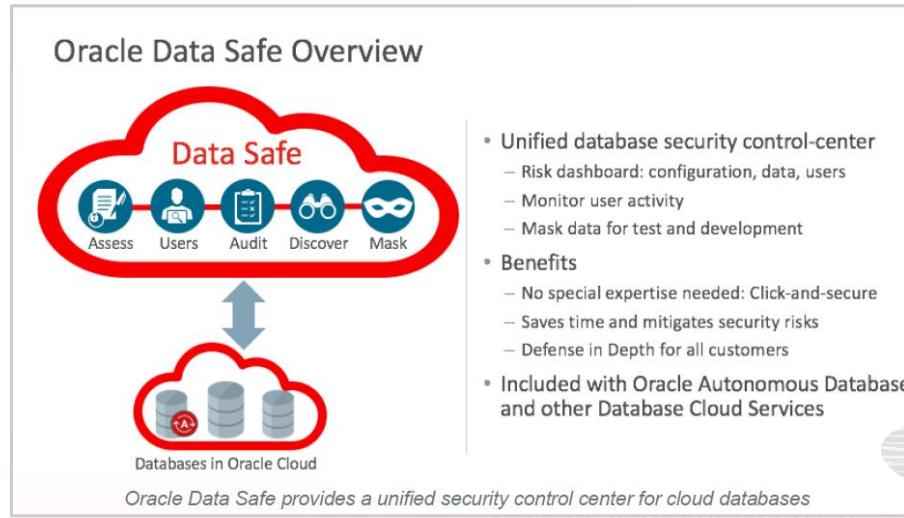
- Make sure you can recover from backups.

Work with application development

- See if redaction is applicable to current applications.



Oracle Data Safe: Overview



17



O

For Instructor Use Only.

This document should not be distributed.

Oracle Data Safe consists of a web application and an Oracle pluggable database (PDB) and resides in Oracle Cloud Infrastructure. The web application is the main user interface for Oracle Data Safe and is referred to as the Oracle Data Safe Console. The PDB is the repository for Oracle Data Safe and contains audit data and collected sensitive data for target databases. You can enable Oracle Data Safe in each region of your tenancy in Oracle Cloud Infrastructure.

Features of Oracle Data Safe

Oracle Data Safe provides the following set of features for protecting sensitive and regulated data in Oracle Cloud databases, all in a single, easy-to-use management console:

- Security Assessment
- User Assessment
- Data Discovery
- Data Masking
- Activity Auditing



18

Security Assessment helps you assess the security of your cloud database configurations. It analyzes database configurations, user accounts, and security controls, and then reports the findings with recommendations for remediation activities that follow best practices to reduce or mitigate risk.

User Assessment helps you assess the security of your database users and identify high-risk users. It reviews information about your users in the data dictionary on your target databases and calculates a risk score for each user. For example, it evaluates the user types, how users are authenticated, the password policies assigned to each user, and how long it has been since each user has changed their password. It also provides a direct link to audit records related to each user. With this information, you can then deploy appropriate security controls and policies.

Data Discovery helps you find sensitive data in your cloud databases. You tell Data Discovery what kind of sensitive data to search for, and it inspects the actual data in your database and its data dictionary, and then returns to you a list of sensitive columns. By default, Data Discovery can search for a wide variety of sensitive data pertaining to identification, biographic, IT, financial, health care, employment, and academic information.

Data Masking provides a way for you to mask sensitive data so that the data is safe for non-production purposes. For example, organizations often need to create copies of their production data to support development and test activities. Simply copying the production data exposes sensitive data to new users. To avoid a security risk, you can use Data Masking to replace the sensitive data with realistic but fictitious data.

Activity Auditing lets you audit user activity on your databases so you can monitor database usage and be alerted about unusual activities.

For Instructor Use Only.
This document should not be distributed.

Summary

In this lesson, you should have learned to:

- Identify key features of the Identity and Access Management Service
- Identify security features of Oracle Database on Oracle Cloud Infrastructure
- Describe how Oracle Cloud Infrastructure resources are secured
- Explain why security is a shared responsibility
- Describe Data Safe



0

For Instructor Use Only.

This document should not be distributed.



Practice 13: Overview

—
There are no practices for this lesson.



0

For Instructor Use Only.
This document should not be distributed.



Migrating Oracle Databases to OCI: Overview

0

For Instructor Use Only.

This document should not be distributed.

Objectives

After completing this lesson, you should be able to:

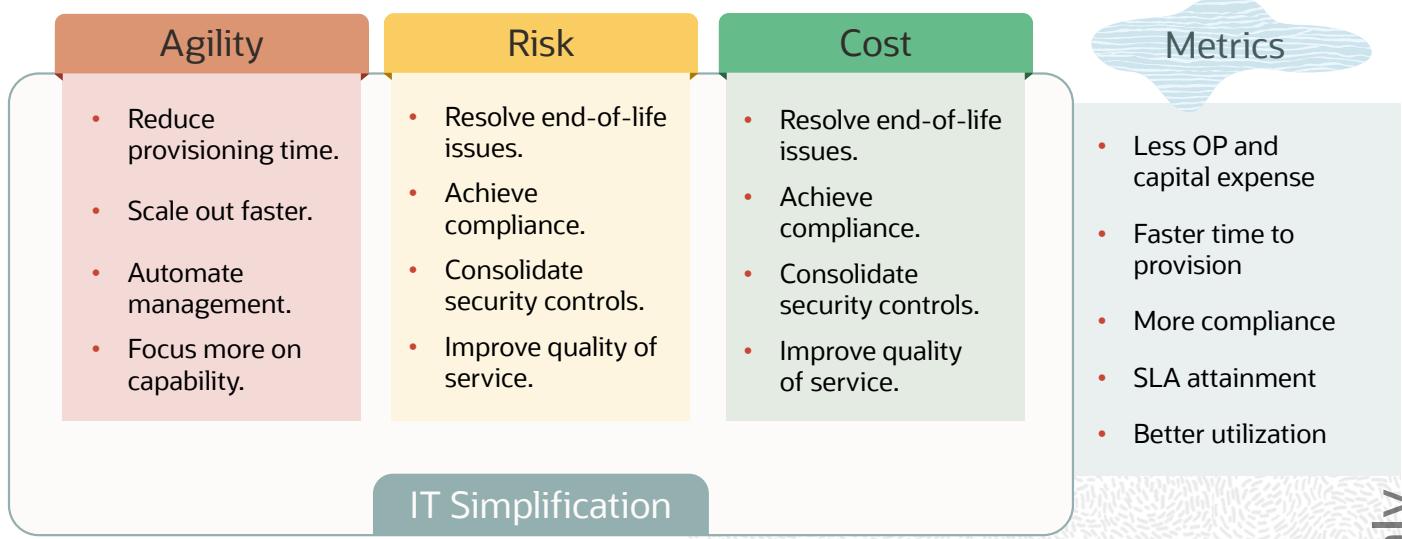
- Describe the benefits of migrating to Oracle Cloud
- Explain database management in the cloud as opposed to on premises
- Identify what can be migrated
- Get started with cloud database migration
- Identify the available migration methods
- Accomplish zero downtime migration
- Explain Data Transfer Service

0



For Instructor Use Only.
This document should not be distributed.

Why Migrate to Oracle Cloud Infrastructure?



3

0

This slide shows the benefits of using Oracle Cloud Services in terms of:

- Lowering operational costs
- Lowering capital expenditure
- Reducing time to provision

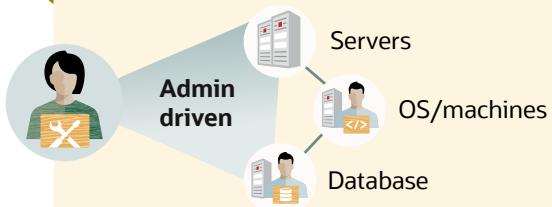
Maintaining service-level agreements by adhering to the **compliance** and **utilization** metrics

For Instructor Use Only.

This document should not be distributed.

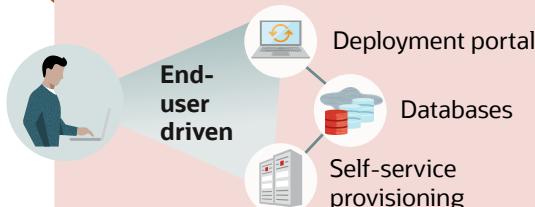
Managing Oracle Database: On Premises Versus Oracle Cloud Infrastructure

Traditional Database Deployment



- Specify and procure hardware.
- Configure hardware.
- Deploy hardware.
- Add hardware and reconfigure stack as demand grows.
- Deploy database.

OCI DB Systems



- Request database deployment via the cloud.
- Adjust capacity as demand changes.
- Retire database when not needed.

4

O

Traditional IT operations are very administration driven, customized for the application environment, and slow due to the transitions between different administrative teams such as hardware, storage, database, and so on.

For Instructor Use Only.

This document should not be distributed.

Managing Oracle Database: On Premises Versus Cloud

Operation type	On-premises database	Cloud database
Database backup	Local storage or cloud	<ul style="list-style-type: none"> • Local compute node storage • Oracle Storage Cloud Service container • Both Cloud Storage and Local Storage
Scheduling of database backups	Manual scheduling using RMAN> backup	Automatic or Manual Scheduling: <code>bkup_api</code>
Database installation	Manual <ul style="list-style-type: none"> • Oracle Database 11g, 12c, 18c, or 19c • Database creation 	Automatic <ul style="list-style-type: none"> • Oracle Database 11g, 12c, 18c, 19c, or 21c • Pre-created database
Location for database files and backups	Manual	Automatic
Housekeeping of database logs and diagnostics files	Manual	Automatic, using a configuration file or manual
Tools used for database monitoring	EM Express, EM Cloud Control, SQL Developer	EM Express, Oracle Management Cloud, EM Cloud Control, SQL Developer, SQL Developer Web
Oracle Database Architecture	Non-CDBs and CDBs	Only CDBs from 12c onwards
Patch compliance	<ul style="list-style-type: none"> • None • Oracle Support • EM Cloud Control 	<ul style="list-style-type: none"> • GUI tool: Oracle Database Cloud Service console • <code>dbcli</code>, <code>oci cli</code>

The table in the slide lists the main differences (based on type of DBA operations) between on-premises databases and cloud database deployments.

Managing Oracle Database: On Premises Versus Cloud

Operation type	On-premises database	Cloud database
Database recovery	Manual using RMAN> recover	Automated using Database Service console or dbcli, oci cli
Storage allocation	Manual: Using UNIX commands	GUI tool: Oracle Database Cloud Service console
Tablespace encryption	None by default	Default encryption for user-defined tablespaces: Initialization parameter <code>encrypt_new_tablespaces = cloud_only</code>
Types of server connection	All types (password, SSH ...)	SSH: Pair key based
Database user and group	<code>oracle user and oinstall group</code>	<code>oracle and opc users, and oinstall group</code>

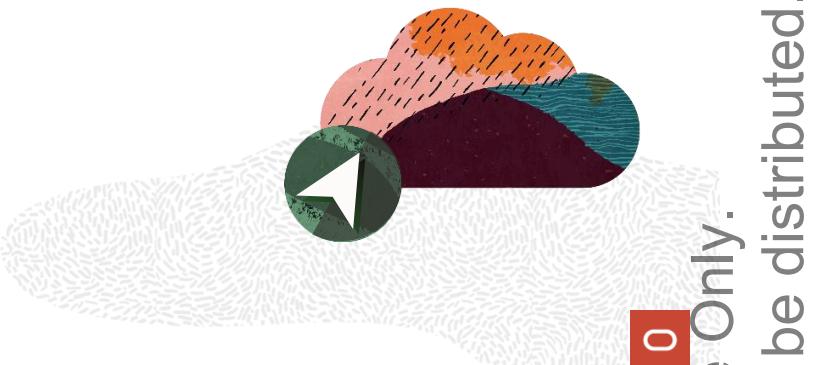
6

O

For Instructor Use Only.
This document should not be distributed.

What Can You Migrate to Oracle Database Cloud?

- Tables or partitioned tables
- Schemas
- PL/SQL objects
- Tablespaces
- Non-container databases
- Container database (CDB)
- Pluggable databases (PDBs)



7

O

Note: All the on-premises database objects listed in the slide (output of the query `select distinct object_type from dba_objects`) can be migrated to the cloud. A few commonly used ones will be discussed in detail in subsequent lessons.

For Instructor Use Only.

This document should not be distributed.

Considerations for Choosing a Migration Method

- On-premises database version
- Database service database version
- On-premises host operating system and version
- On-premises database character set
- Quantity of data, including indexes
- Data types used in the on-premises database
- Storage for data staging
- Acceptable length of system outage
- Network bandwidth



O

8

Various migration methods exist, and each migration method has different benefits, opportunities, requirements, and limitations.

For example, Oracle Cloud Service uses a little-endian platform, so if you are migrating from a big-endian platform, some physical migration approaches are not feasible or require extra processing to achieve. Also, the use of specific database features, such as materialized views or object data types, may impose restrictions on some migration methods.

For more details on migrating to OCI Database refer to Oracle University training Migrating Your Oracle Database to Oracle Cloud Infrastructure.



Migration: Information Gathering

- Database version of your on-premises database
- For on-premises Oracle Database 19c databases, the architecture of the database (multitenant or non-CDB)
- Endian format (byte ordering) of your on-premises database's host platform
- Database character set of your on-premises database and your Database Cloud Service database
- Database version of your Database Cloud Service database

9

Determining Applicable Methods

To determine which migration methods might be applicable to your migration scenario, gather the following information.

Database version of your source database:

- Oracle Database 11g Release 2 version lower than 11.2.0.3
- Oracle Database 11g Release 2 version 11.2.0.3 or higher
- Oracle Database 12c Release 1 version lower than 12.1.0.2
- Oracle Database 12c Release 1 version 12.1.0.2 or higher
- Oracle Database 12c Release 2 version 12.2.0.1
- Oracle Database 18c version 18.6.0.0.0 or higher
- Oracle Database 19c version 19.3.0.0.0 or higher

For Oracle Database 12c Release 1/Oracle Database 12c Release 2 source databases, the architecture of the database:

- Multitenant container database (CDB)
- Non-CDB

Your source database host platform and endian format:

- Query `V$DATABASE` to identify the platform name for your source database. Platforms are either little-endian or big-endian depending on the byte ordering that they use.
- Query `V$TRANSPORTABLE_PLATFORM` to view all platforms that support cross-platform tablespace transport, along with the endian format of each platform.
- Oracle Cloud Infrastructure Database uses the Linux platform, which is little-endian.

The database character set of your source database and the Oracle Cloud Infrastructure Database database:

By default, databases are configured to use the AL32UTF8 database character set on Oracle Cloud Service. You can select the required character set during provisioning.

The target database version to which you are migrating on Oracle Cloud Service:

- Oracle Database 11g Release 2
- Oracle Database 12c Release 1
- Oracle Database 12c Release 2
- Oracle Database 18c
- Oracle Database 19c
- Oracle Database 21c

For Instructor Use Only.
This document should not be distributed.

Migration: Analysis and Planning



11

Downtime: Determine from your business what the downtime service level agreements (SLAs) are and how much downtime, if any, the business can accommodate. You can also review Recovery Time Objective (RTO) and Recovery Point Objective (RPO) SLAs to see how much downtime is acceptable according to your disaster recovery (DR) and business continuity (BC) guidelines.

Database Size: Determine the data volume. Typically, the size of the database is based on two factors: whether the physical or logical migration method is considered, and whether all or part of the data will be migrated to the target database.

Network Bandwidth: Determine the available network bandwidth between the source and target databases. In addition to available bandwidth, network reliability is also important. Based on the data transfer method, network interruption might require you to restart the data transfer job.

Cross-Platform Migration: Determine the endianness of the source and target platforms. Oracle Cloud Infrastructure databases are little-endian. If your source database is big-endian, you can either select the logical migration method, which is typically slower, or use Oracle Data Guard or RMAN cross-platform features for the cross-platform migrations.

Database Character Set: Determine the database character set for the source and target databases. For most migration methods, the target database character set must be a superset of the source database character set. Some methods might need the exact same character set to avoid data loss.

Data Encryption: Determine whether the source database uses Transparent Data Encryption (TDE). TDE is mandatory for all Oracle Cloud Infrastructure databases. If TDE is not used at the source, enable it either at the source or at the target. Be sure to back up and restore the required TDE wallets from the source to the target.

Database Version, Edition, and Options: Determine the database version, edition, and options for the source and target databases. Based on the migration method, the target and source database version and edition must be compatible. For the Oracle Cloud Infrastructure 12c database target, the multitenant architecture is mandatory, so ensure that the selected migration method can accomplish the migration into the CDB/PDB, as needed.

Databases Patches: Determine the patch level for the source and target databases. Ensure that the source and target are at the same or compatible Patch Set and Release Upgrade level. Apply any required patches at the source to minimize any discrepancies during or after the migration. Also, as necessary, apply any one-off patches at the target.

DB Name: Determine the database name used at the source database. For full database restore methods, it is mandatory to create the target database by using the same database name as used at the source database. However, use the DB Unique Name of the target as created by the Oracle Cloud Infrastructure tooling.

DB Block Size: Determine the database block size used at the source database. For partial restore methods like transportable tablespaces, it might be necessary to adjust the cache size parameters based on the target database.

DB Time Zone: Determine the database time zone used at the source database. It might be necessary to adjust the database time zone at the target database.

DB Users, Privileges, and Objects: Determine the database users, privileges, and objects, like DB links, from the source database that might also need to be created at the target database.

Sizing: Determine the source database sizing and consider future growth to size the target database. In addition to CPU and memory, ensure the sizing meets your IOPS and network bandwidth requirements.

Target Database: To ensure the target database has all the required metadata for OCI tooling to work, create the target database using one of the supported methods like OCI Console, OCI CLI, or Terraform OCI provider. This target database will be cleaned to be used as a shell for the migration, as needed.

Migration: Data Transfer Options (Online and Sync)

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

13

0

For Instructor Use Only.

This document should not be distributed.

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

Public Internet: Online, OCI CLI, OCI API, OCI Console, rclone

IPSec VPN: Online, OCI CLI, OCI API, OCI Console, rclone

<https://docs.cloud.oracle.com/iaas/Content/Network/Tasks/managingIPsec.htm>

FastConnect: Online, OCI CLI, OCI API, OCI Console, rclone

<https://docs.cloud.oracle.com/iaas/Content/Network/Concepts/fastconnect.htm>

Storage Gateway: Sync, cp/scp to NFS mount points

<https://docs.cloud.oracle.com/iaas/Content/StorageGateway/Concepts/storagegatewayoverview.htm>

Migration: Data Transfer Options (Offline)

Data Transfer Disk



- Send your data to an Oracle Data Transfer site (US or Frankfurt).
- Oracle will upload the data for you over fast network connections.
- Data is wiped off the disks and shipped back after it is uploaded to Oracle Cloud.

Data Transfer Appliance



- Rent a Data Transfer Appliance from Oracle to migrate PB scale datasets to Oracle Cloud.
- Each transfer appliance can migrate up to 150 TBs.
- Use multiple appliances to migrate large datasets.
- Keep the transfer appliance onsite for up to 30 days.
- Available for use in US and European Union countries

14

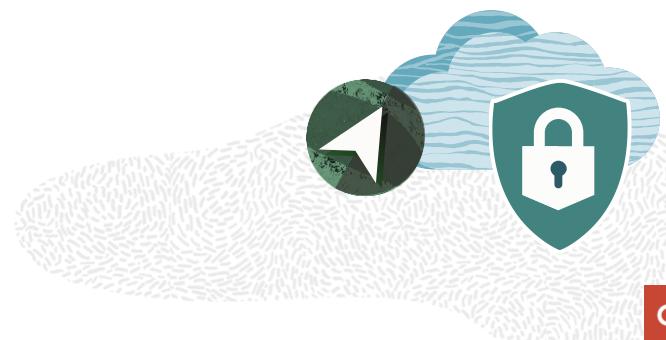
0

<https://docs.cloud.oracle.com/iaas/Content/DataTransfer/Concepts/overview.htm>

For Instructor Use Only.
This document should not be distributed.

Migration: Security Considerations

- Transparent Data Encryption (TDE) is **mandatory** for all OCI databases.
- Enable it on the source or target.
- Make sure you back up and restore your TDE wallets from the source to the target.



15

For Instructor Use Only.
This document should not be distributed.

Migration Options

Migration Option	Autonomous	BM/VM/Exadata	Database Versions	Benefits
Restore from Object Store (Online or sync data transfer)	Data Pump ✓	RMAN-based Restore ✓	All	Supports all database editions and platforms along with full and incremental backups
Restore from Object Store (Offline data transfer using Data Transfer Service)	✓	✓	All	Same as Restore from Object Store. Additionally, supports low-bandwidth/high-data volume scenarios
Golden Gate	✓	✓	All. Requires separate license	No downtime
Data Guard	NA	✓	Enterprise Edition and above	Minimal downtime
Oracle SQL Developer	✓	NA	All	Quick and simple, suitable for migrating database objects of small to medium size

16

0

Apart from the options listed above, there are a bunch of standard Oracle options available for migration, which are discussed in the Oracle University training *Migrating Your Oracle Database to Oracle Cloud Infrastructure*.

For Instructor Use Only.
This document should not be distributed.

Zero Downtime Migration (ZDM)

- Enables easy and efficient migration of on-premises database to Oracle Cloud
- Leverages Oracle MAA technologies such as Oracle Active Data Guard and Golden Gate
- Supports various migration methods, based on the chosen backup medium
- Provides a robust, flexible, and resumable migration process that is also easy to roll back
- Supports offline (backup and recovery) migration.



17

O

Zero Downtime Migration

Zero Downtime Migration gives you a quick and easy way to move on-premises databases and Oracle Cloud Infrastructure Classic instances to Oracle Cloud Infrastructure, Exadata Cloud at Customer, and Exadata Cloud Service without incurring any significant downtime, by leveraging technologies such as Oracle Active Data Guard.

Zero Downtime Migration uses mechanisms such as backing up the source database to Oracle Cloud Infrastructure Object Storage, creating a standby database (with Data Guard configuration, Oracle Data Guard Maximum Performance protection mode, and asynchronous [ASYNC] redo transport mode) in the target environment from the backup, synchronizing the source and target databases, and switching over to the target database as the primary database.

Data Transfer Service

- Provides offline data transfer solutions that let you migrate data to OCI
- Exports data from OCI to your data center offline
- Disk-based data transfer
 - Data sent on encrypted commodity disk to an Oracle transfer site
- Appliance-based data transfer
 - Data sent on secure, high-capacity, Oracle-supplied storage appliances to an Oracle transfer site
- Appliance-based data export
 - Data sent from OCI bucket to your data center using an Oracle-provided appliance



O

18

Data Transfer Service

Oracle offers offline data transfer solutions that let you migrate data to Oracle Cloud Infrastructure. You can also export data currently residing in OCI to your data center offline. Moving data over the public internet is not always feasible because of high network costs, unreliable network connectivity, long transfer times, and security concerns. Our transfer solutions address these pain points, are easy to use, and provide faster data upload compared to over-the-wire data transfer.

Disk-based Data Transfer

You send your data as files on encrypted commodity disk to an Oracle transfer site. Operators at the Oracle transfer site upload the files into your designated Object Storage bucket in your tenancy. This transfer solution requires you to source and purchase the disk used to transfer data to OCI. The disk is shipped back to you after the data is successfully uploaded.

Appliance-based Data Transfer

You send your data as files on secure, high-capacity, Oracle-supplied storage appliances to an Oracle transfer site. Operators at the Oracle transfer site upload the data into your designated Object Storage bucket in your tenancy. This solution supports data transfer when you are migrating a large volume of data and when using a transfer disk is not a practical alternative. You do not need to write any code or purchase any hardware. Oracle supplies the transfer appliance and software required to manage the transfer.

Appliance-based Data Export

You export your data from your OCI Object Storage bucket to your data center using an Oracle-provided appliance. This solution is useful if you have media content or processed datasets you need to share with a customer or business partner.

Summary

In this lesson, you should have learned how to:

- Describe the benefits of migrating to Oracle Cloud
- Explain database management in the cloud as opposed to on premises
- Identify what can be migrated
- Get started with cloud database migration
- Identify the available migration methods
- Accomplish zero downtime migration
- Explain Data Transfer Service



0

For Instructor Use Only.
This document should not be distributed.



Practice 14: Overview

—
There are no practices for this lesson.



0

For Instructor Use Only.
This document should not be distributed.