

Exam Domains

- Cloud Concepts
- OCI Infrastructure
- OCI Core Services
- Security
- Billing and Pricing

Passing Grade: 680/1000

Cloud Computing: the practice of using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or a personal computer.

Oracle: HQ in Redwood Shores, California; 2nd largest software company by revenue and market capitalization (2019)

OCI = Oracle Cloud Infrastructure

Advantages of Cloud Computing:

- On-Demand
- Going Global
- Share the Cost
- Stop Guessing
- Less Waste
- Fast to Market

Types of Cloud Computing:

- SaaS: for customers
- PaaS: for developers
- IaaS: for admins

Cloud Deployment Models

- Cloud-Native: Everything built on the cloud
- Hybrid-Architecture: Using both On-Premise and the Cloud
- Cross-Cloud (or multi-cloud, hybrid-cloud): Using multiple cloud providers

High Availability: Ability of a service to remain available by ensuring there is no single point of failure and/or ensuring a certain level of performance

Oracle Load Balancer: Allows to evenly distribute traffic to multiple servers in one or multiple datacenters. Traffic is routed only to healthy servers.

High Scalability: Ability to increase capacity based on the increasing demand of traffic, memory and computing power

High Elasticity: Ability to automatically increase or decrease capacity based on the current demand or traffic, memory and computing power

AutoScaling Configuration: Allows to configure scaling rules for your instances in OCI

Highly Fault Tolerant: Ability of a service to ensure there is no single point of failure. It prevents the chance of failure. Example: Standby Slave for a master database

Fail-overs is when you have a plan to shift traffic to a redundant system in case the primary system fails.

High Durability: Ability to recover from a disaster and to prevent the loss of data. Solutions that recover from a disaster is known as Disaster Recovery (DR)

Key questions:

- Do you have a backup?
- How fast can you restore that backup?
- Does your backup still work?
- How do you ensure current live data is not corrupt?

Capex (On-Premise, Software license fees) vs Opex (OCI, Subscription fees)

Opex focuses on implementation, configuration and training

Hypervisor is the software layer that lets you run the VMs.

Docker Deamon is the name of the software layer that lets you run multiple containers

OCI Infrastructure

A region is a geographically distinct location that has many datacenters (availability domains). May be referred to as “Localized Geographic Area”

Three kinds of regions:

- Commercial
- Government
- Azure Connected

A Fault Domain (FD) is a logical datacenter, or a virtual/abstract datacenter within a physical datacenter. Its primary purpose is to isolate groupings of hardware within a datacenter so that they do not share a single point of failure. Fault domains protect against failures within an availability domain.

A tenancy, or root compartment, is a secure and isolated partition within OCI where you can create, organize, and administer your cloud resources. One sign up, a tenancy is created by default.

A compartment is a logical collection of related resources (such as instances, VCNs, or Block Volumes) that can be accessed only by certain groups that have been given permission by an administrator.

Compartments can be nested 6 levels deep, and they are not region specific

Oracle Cloud IDs (OCIDS) are unique IDs assigned by Oracle to your cloud resources, that are used in policies and OCI API to reference specific cloud resources.

Cloud Shell: A web browser-based terminal accessible from the Oracle Cloud that can be used to access the CLI

OCI Core Services

Core Computing Services:

- Virtual Machines
- Container Engines - Docker as a Service
- Functions - Serverless compute
- Dedicated Virtual Hosts - Single-tenant server running a hypervisor with multiple instances owned by the same customer
- Bare Metal - Dedicated server that has no hypervisor layer

Instance types are: Standard, DenseIO, GPU and HPC shapes. Stopping a standard shape instance pauses billing.

Storage Services:

- Block Volume
- Local Non-Volatile-Memory Express (NVMe) - transfer protocol for SSD
- File Storage - uses NFSv3 file systems allowing multiple connections simultaneously
- Object Storage - Serverless storage - unlimited scale
- Archive Storage - long term cold storage

Block Volume Tiers:

- Basic
- Balanced
- Higher Performance

Block volumes sizes can be from 50GB to 32TB. You can attach up to 32 volumes per instance.

Local NVMe (Non-Volatile Memory Express) = Instance Storage in AWS

File storage supports multiple reads, though writing locks the file. Object storage also supports multiple reads and writes without locks. Block volume only supports a single write volume

Networking Services:

- Region
- Availability Domains
- Fault Domains
- VCN
- Internet Gateway - sits on the edge of OCI and enables access to the internet
- Subnets - logical partition of an IP network into smaller network segments
- Virtual Firewall
 - Security Rules - associated with VCINs within subnets
 - Network Security Groups (NSGs)
 - Security Lists - associated with subnets
- Service Gateways - secure tunnel that keeps traffic within the OCI network
- NAT Gateway - let resources in a private subnet reach the Internet
- IPSec VPN - secure connection between your on-prem and Oracle Cloud
- Fast Connect - dedicated secure connection to your on-prem to Oracle Cloud
- Dynamic Routing Gateway (DRG) - virtual router that provides a path for private traffic between your VCN and outside network
- VCN Peering - creates a network connection between VCNs (Local Peering Gateway: within a region; Remote Peering Connection: in different regions, uses DRG)

Virtual Cloud Networks (VCNs): a logically isolated section of the OCI Cloud where you can launch OCI resources. You choose a range of IPs using CIDR Range.

Virtual Network Interface Cards (VCINs): enables an instance to connect to a VCN and determines how the instance connects with endpoints inside and outside the VCN.

Network Security Groups (NSGs): designed for application components that have a different security posture. NSGs are supported only for specific services. NSGs are directly associated with VCINs regardless of what subnet they are in.

Database Services:

- VM DB Systems: A VM running a managed Oracle Database Instance - uses block storage [fast provisioning]
- VM BM Systems: A Bare Metal machine running a managed Oracle Database Instance - uses fast local storage [fast performance]

- Oracle RAC: Oracle databases running as a cluster - [highly available]
- Exadata DB Systems: Pre-configured combination of hardware and software that provides an infrastructure for running Oracle databases; it provides the best performance for running OLTP workloads [specialized infrastructure]
- Autonomous: highly available by default, secure by default, self-healing bad data; can be shared or dedicated [Fully Managed]

Workload types for autonomous databases:

- Data Warehouse (OLAP)
- Transaction Processing (OLTP)

Data guards modes (Bare Metal DB Systems only):

- Switchover: planned migration, no data loss
- Failover: unplanned migration, minimal data loss

FSFO: Fast-Start Fail Over - Automatic Failover option

Oracle NoSQL database is a key/value store

Use cases for Oracle NoSQL databases:

- Produce and consume data at high volume and velocity
- Require instantaneous response time to match user expectations
- Developed with continuously evolving data models
- Scale on-demand based on the dynamic workloads

Cloud Native Services

- Oracle API Gateway
- Oracle Streaming
- Oracle Kubernetes Container Engine (OKE)
- Oracle Registry (OCIR): A repository for your docker containers
- Oracle Notifications: A fully managed publish-subscribe service for reliable and scalable message delivery
- Oracle Integrations: connecting to on-prem

Billing and Pricing

Oracle UC = Universal Credit Pricing

Pricing Models:

- Pay As You Go (PAYG)
- Monthly Flex (minimum 12 months, \$1,000/month, 30-65% savings)
- Bring Your Own License (BYOL)

All regions have the same pricing

Data Transfer rules:

- Data-in (ingress) is free
- Data-out (egress) costs money
- Data transfer within the same availability domain is free
- Data transfer between availability domains in the same region is free
- Data transfer between regions will result in a charge for data leaving the region

Block volume pricing components:

- Storage cost: \$0.0225/GB/month
- Performance cost: based on Volume Performance Units (VPUs) per month

OCI Cost Analysis will help you visualize your ongoing costs. You can filter based on compartments, tagged resources, and start and end dates

Usage Reports: Provides a granular view of your spending and allows you to find ways to save. Can be downloaded as a CSV or you can use the OCI API to access detailed billing information.

Cost report is automatically generated daily and stored in an Object Storage bucket

Oracle Marketplace are managed VM images or stacks from third-party vendors that are free or paid that you can launch

OCI SLAs: <https://www.oracle.com/ca-en/cloud/iaas/sla.html>

Premier Support: Support service provided by Oracle Cloud

OCI Security

Identity and Access Management (IAM) components:

- Users
- Groups
- Dynamic Groups
- Policies

A single compute instance can belong to a maximum of 5 dynamic groups.

Principals: An IAM entity that is allowed to interact with OCI resources. The two types are IAM Users and Instance Principals

OCI Authorization = Policies

OCI Common Policies:

<https://docs.cloud.oracle.com/en-us/iaas/Content/Identity/Concepts/commonpolicies.htm>

Policy verbs in OCI: Inspect, Read, Use and Manage

Federation Identity is the ability to enable users from one domain to securely access data or systems of another domain without the need of a redundant user administrator

Security Services in OCI:

- Identity and Access Management: OCI IAM, MFA, Federation
- Data Protection: Data Safe, Key Management, Encryption
- OS and Workload management: Patch Management, Workload Isolation
- Infrastructure Protection: VCN NSG, SL, WAF, DDoS Protection

Single Sign On is the technology that enable users to authenticate without the need to log in or have separate pair of credentials to third party systems

An Identity Provider (IdP) is a trusted provider of your user identity that lets you authenticate to access other services. Examples are Microsoft AD, Facebook, Amazon, Google or Oracle Identity Cloud Service.

Encryption options for Database Service:

- Transparent Data Encryption (TDE)
- Oracle Data Safe
- Database Vault

Transparent Data Encryption(TDE) enables you to encrypt sensitive data, such as credit card numbers, stored in tables and tablespaces. Encrypted data is transparently decrypted for a database user or application that has access to data. TDE helps protect data stored on media in the event that the storage media or data file gets stolen

Bring Your Own Keys (BYOKs): Encryption option available for block volumes, file storages and object storages.

Encryption in Transit is available for block volume and file storage, but not for object storage.

Oracle Data Safe is a unified control center for your Oracle databases which helps you understand the sensitivity of your data, evaluate risks to data, mask sensitive data, implement

and monitor security controls, assess user security, monitor user activity, and address data security compliance requirements.

OCI Vault makes it easy for you to create, control and rotate encryption keys used to encrypt data on OCI (previously known as OCI Key Management). It is a multi-tenant CloudHSM.

OC Management is a service that allows you to manage updates and patches for the VMs operating systems running on OCI

OCI's Web Application Firewall (WAF) protects your web applications from common web exploits (CWEs)

OCI Audit (under Governance): provide details about historical actions by users

MAA = Maximum Availability Architecture

TDE = Transparent Data Encryption

OCI SLA coverage:

- Availability (Data Plane - Usage)
- Manageability (Control Plane - Administration)
- Performance (applicable for Compute and Block Volume services only)

Oracle RAC allows multiple computers to run Oracle RDBMS software simultaneously while accessing a single database, thus providing clustering. In a non-RAC Oracle database, a single instance accesses a single database. The database consists of a collection of data files, control files, and redo logs located on disk

Two key advantages of bare metal systems: Performance and Isolation