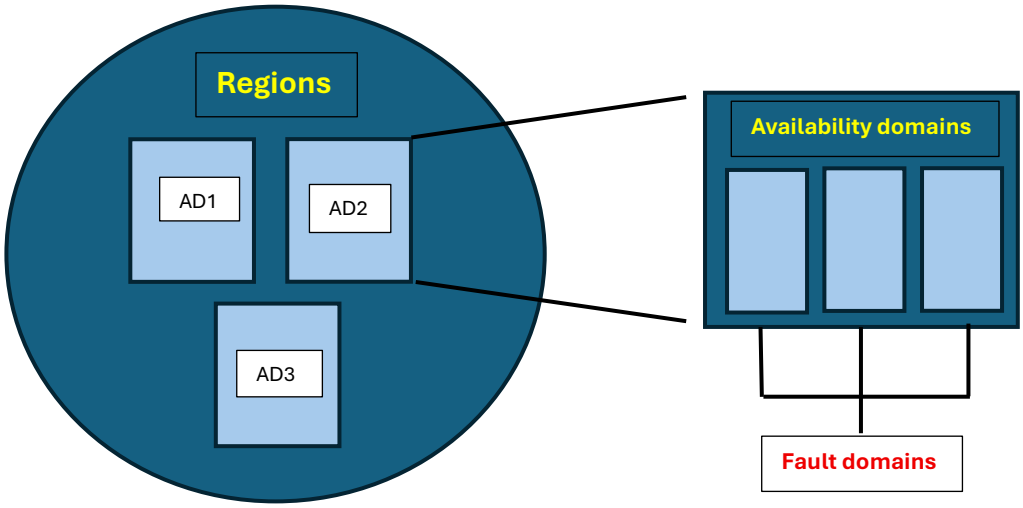
ORACLE Cloud Infrastructure

Oracle Cloud Infrastructure 2025 Foundations Associate (1Z0-1085-25)

OCI Introduction

1. **OCI Architecture:** OCI Architecture is built on a region-based design, where each region contains one or more availability domains (ADs). Each AD is further divided into fault domains (FDs) to ensure high availability, fault tolerance, and disaster recovery for cloud resources.



1. A Region is a geographic area where Oracle has its cloud services available.
   - Each region contains one or more Availability Domains (ADs) (data centers).
   - You choose a region based on where your users are or where data must be stored.

2. An Availability Domain (AD) is a physical data center in a region.
   - Each AD is further divided into Fault Domains (FDs), usually 3 per AD.
   - A Fault Domain is like a separate "rack or set of racks" with independent power, cooling, and hardware resources.

3. A Fault Domain is like a separate section inside a data center.
   - If you put all your servers in the same section and that section's power or cooling fails → all your servers go down.
   - But if you spread them across different fault domains → even if one section fails, the others keep running.

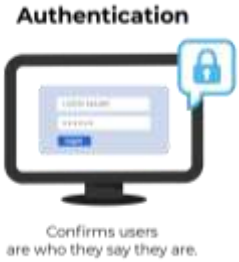
Identity and Access Management

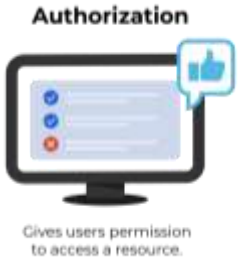
IAM in OCI is also referred to as fine-grained access control or role-based access control (RBAC). It ensures that the right individuals and resources have the right level of access to OCI services.

IAM primarily focuses on two key aspects:

1. Authentication (AuthN) – "Who are you?"
    - This step verifies your identity.
    - Example: Logging in with a username/password, API key, or federated login.
2. Authorization (AuthZ) – "What can you do?"
    - This step defines the permissions you have after your identity is confirmed.
    - Example: Once logged in, are you allowed to view, create, or delete compute instances?

AuthN





AuthZ

Authentication in OCI	Authorization in OCI
• Username / Password • API Signing keys • Authentication tokens	• Policies

Oracle Cloud Identifier (OCID):

- Every resource you create in OCI (like a compute instance, block volume, VCN, user, etc.) gets a unique identifier.
- This identifier is called an OCID.
- Think of it like a serial number or Aadhaar number for each resource.

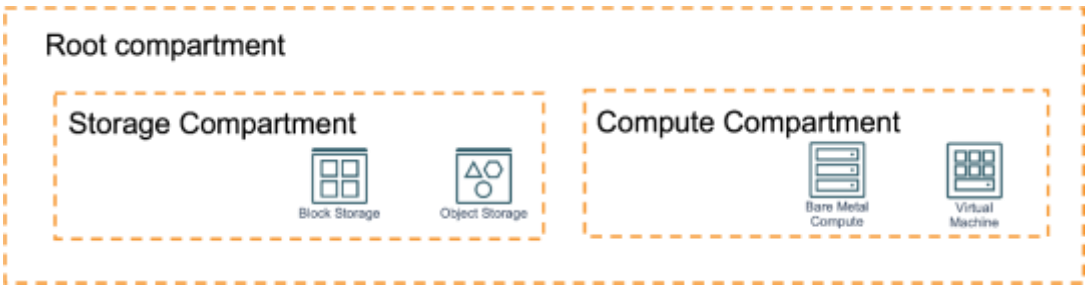
  Format of OCID:

  ```
  ocid1.<resource type>.<realm>.[region][.futureuse].<unique_ID>
  ```

Compartment in OCI:

A Compartment is a logical container used to organize and isolate your cloud resources in OCI.

- It helps you group related resources (compute, storage, networking, databases) together.
- Think of it as a folder on your computer, but for cloud resources.
- Compartment structure is hierarchical – you can have compartments inside compartments (sub-compartments).



- The Root Compartment is the top-level compartment created automatically when you set up your OCI tenancy.
- It has access to all resources in the tenancy by default.

Note: It is not a best practice to create all resources in the root compartment. Compartments are used to organize and isolate resources to provide a finer level of access control.

Compartment Nesting in OCI:

- You can create compartments within compartments (sub-compartments) to any depth.
- OCI currently allows up to 6 levels of nesting under the root compartment.
- This hierarchy helps in organizing resources by team, project, environment, or business unit.

Principals in OCI IAM:

- Principals are entities allowed to interact with OCI resources.
- Types of principals:

1. Users – Individual human users
2. Groups – Collection of users with similar access needs
3. Dynamic Groups – Resources (like compute instances) acting as principals

- Policies are written to give principals permissions on compartments or resources.

Groups in OCI IAM:

- A group is a collection of users who require the same type of access to resources.
- Instead of assigning policies to individual users, you assign policies to group, simpler and more scalable.
- Example:
    - Group: Developers
    - Policy: Allow group Developers to manage all resources in the Dev compartment
    - Effect: All users in the Developers group inherit the same permissions.

Tenancy Setup:

Image source: Oracle Cloud Infrastructure documentation

This diagram represents how user access and permissions flow in Oracle Cloud Infrastructure (OCI) using tenancy, admins, groups, and policies.

**Oracle strongly recommends not using the Tenancy Admin (root user) for daily operations.

- The Tenancy Admin/root user has unlimited power in OCI.
- If compromised, the entire tenancy is at risk.
- Best practice: Use it only for initial setup, then delegate responsibilities using groups + policies.

Tenancy Admin creates → Admin users → Groups → Policies → Scoped access to compartments.

Daily work happens using group-based access, not the Tenancy Admin itself.

Networking

Virtual Cloud Network (VCN): A Virtual Cloud Network (VCN) in OCI is a highly scalable, secure, and highly available private network in the cloud. It lets you control IP ranges, subnets, gateways, and traffic rules for your resources.

Highly Scalable:

- You can define large IP ranges (CIDR blocks).

- Add multiple subnets, gateways, and resources as your application grows

Secure:

- Security Lists and Network Security Groups (NSGs) let you control inbound/outbound traffic.
- You decide whether subnets are public (internet-facing) or private.

Highly Available:

- Regional subnets span the entire region (not tied to a single data center).
- OCI networking infrastructure is redundant and fault tolerant.

OCI Gateways:

1. Internet Gateway (IGW): Lets your resources talk to and from the internet. (Example: A public web server).
2. NAT Gateway: Lets your private resources go out to the internet, but the internet cannot reach them. (Example: Private server downloading updates).
3. Service Gateway: Lets your resources talk to Oracle Cloud services (like Object Storage) without using the internet.

A Dynamic Routing Gateway (DRG) in Oracle Cloud is like a router that connects your Virtual Cloud Network (VCN) with networks outside OCI.

1. Site-to-Site VPN Connect: lets you securely connect your on-premises network to your VCN over the internet using IPsec tunnels.
2. FastConnect: provides a private, high-speed, and more reliable connection from your on-premises network to OCI (not over the internet).

Route Tables:

A VCN (Virtual Cloud Network) uses route tables to control where network traffic goes that is, how packets leaving a subnet reach their destination.

Each subnet in a VCN is linked to one route table that route table tells the subnet where to send traffic that's not local (i.e., not inside the same VCN).

E.g.:

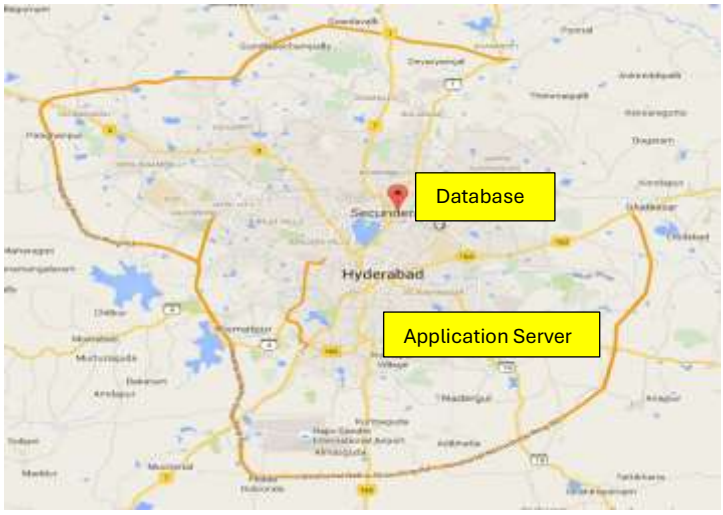
Dest. CIDR	Route Target
0.0.0.0/0	NAT Gateway
192.168.0.0/16	Dynamic Routing Gateway

This route table defines how network traffic from a subnet in your VCN (Virtual Cloud Network) is directed based on its destination address.

Local Peering & Remote Peering:

Local Peering: Connecting two VCNs (Virtual Cloud Networks) that are in the same OCI region but in different availability domains or compartments.

- Data never leaves the OCI region.
- Useful for inter-VCN communication within the same region.



Assume both are in same region

Remote Peering: Connecting two VCNs in different OCI regions that enables secure, private communication across regions.

- Slightly higher latency than local peering because data travels across regions.
- Useful for multi-region deployments, disaster recovery, or global applications.

Assume in this case two locations will be at different points

VCN Security:

Security Lists: Acts like a firewall at the subnet level.

- Purpose: Control ingress (incoming) and egress (outgoing) traffic.
- Example:
    - Allow HTTP (port 80) from the internet.
    - Block all other ports.

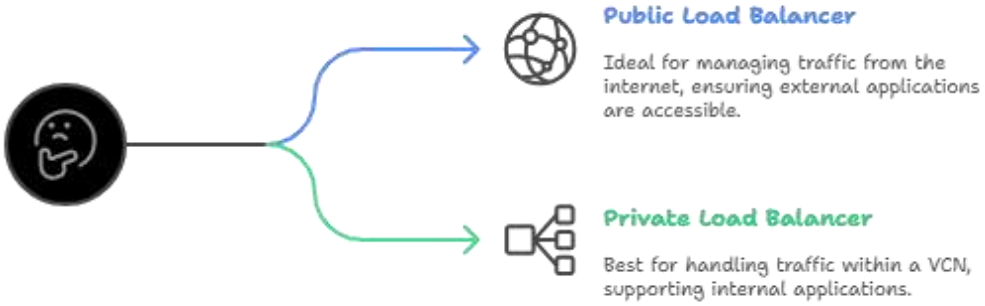
Network Security Groups (NSGs): Virtual firewall at the instance or group of instances level.

- Purpose: Fine-grained control of traffic to specific compute instances.
- Example:
    - Allow SSH only from your office IP.
    - Allow database access only from a certain app server.

Load Balancer: A Load Balancer is a service that distributes incoming traffic across multiple servers (compute instances) to ensure applications run smoothly.

Features:

- ✓ High Availability
- ✓ Scalability
- ✓ Improved Performance
- ✓ Security
- ✓ Simplified Performance



Compute

OCI (Oracle Cloud Infrastructure) Compute is a service that allows you to create and manage virtual machines (VMs) or bare metal servers in Oracle's cloud.
It's like AWS EC2 or Azure Virtual Machines — basically, you can run applications, host websites, or deploy workloads in the cloud.

Flexible Shapes:

In OCI, a shape defines the amount of CPU, memory, and other resources assigned to your instance.

- Flexible shapes let you customize the number of OCPUs (Oracle CPUs) and memory for your instance instead of being locked to fixed sizes.
- This helps you allocate just the right amount of resources you need — saving cost and increasing efficiency.

Example:
You can create an instance with 2 OCPUs and 8 GB memory — or adjust it later to 4 OCPUs and 16 GB without recreating the instance.

Choice of Processors:

OCI is one of the only two major cloud providers that allow you to choose between multiple processor architectures for your compute instances:

- AMD EPYC
- Intel Xeon
- Ampere Altra (ARM-based)

This flexibility lets you pick the processor that best fits your workload (for example, Ampere for high efficiency, AMD for price/performance, Intel for specific compatibility).

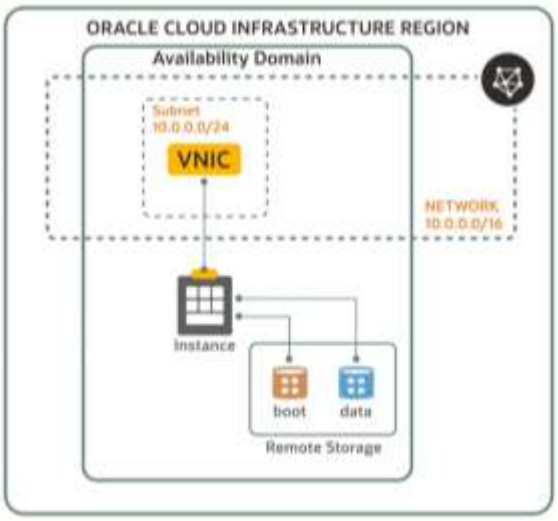
Basics of Instance: An instance in OCI is basically a virtual machine running in the cloud.

Pay-As-You-Go Pricing:

OCI uses a pay-as-you-go model — meaning:

- You only pay for what you use.
- There are no upfront costs or long-term commitments (unless you choose reserved capacity).
- Billing is based on the number of OCPUs, memory, storage, and network usage during your runtime.

This is ideal for startups, testing environments, or dynamic workloads.



- ✓ The outer box represents an OCI Region
- ✓ Inside a region, there are Availability Domains — isolated data centers.
- ✓ The network here represents your Virtual Cloud Network (VCN).
- ✓ The VNIC connects your instance to the network. It provides the IP address
- ✓ Boot Volume – Contains the OS (operating system).
- ✓ Data Volume – Optional; used for additional data, backups

Image source: Oracle Cloud Infrastructure documentation

(VNIC - Virtual Network Interface Card)

Scaling:

Scaling means increasing or decreasing compute resources (like CPU, memory, or number of instances) depending on the workload or demand.
It ensures:

- You have enough power when usage is high.
- You save cost when demand is low.

Vertical Scaling: Making a single server bigger or smaller.

Horizontal Scaling: Adding or removing multiple instances instead of changing the size of one.

Autoscaling: Automatic Horizontal Scaling.

Instead of manually adding or removing instances, OCI can monitor your instance load (like CPU usage, memory, or requests) and:

- Add instances when traffic is high (Scale Out)
- Remove instances when traffic drops (Scale In)

Normal Load: 

High Load: 

Low Load: 

(When there is no load, OCI will get back into normal mode with less instances)

Oracle Container Engine for Kubernetes (OKE):

Virtual Machines vs Containers

Aspect	Virtual Machines (VMs)	Containers
Architecture	Each VM runs its own OS, libraries, and app on top of a hypervisor	All containers share the same OS kernel, run isolated via a container runtime (e.g., Docker)
Size	Heavy (GBs)	Lightweight (MBs)
Boot Time	Slow (minutes)	Fast (seconds)
Resource Usage	High (each OS consumes resources)	Low (shared OS)
Portability	Limited	Highly portable (can run anywhere with container runtime)

So, Containers are faster, smaller, portable, and efficient compared to traditional virtual machines.

Once you have many containers:

- They need to communicate, scale, recover, and update automatically.
- This automation is called Container Orchestration.

Sol: Kubernetes is an open-source orchestration system for managing containers.

What is OKE?

- ✓ A fully managed Kubernetes service provided by Oracle Cloud Infrastructure (OCI).
- ✓ Built on open-source Kubernetes.
- ✓ Highly available, scalable, and managed by Oracle.

OKE Architecture Overview:

- Node → A machine where containers (pods) run.
- Pod → Smallest deployable unit containing one or more containers that share storage & network.
- Node Pool → Group of nodes.
- Cluster → Set of node pools + managed control plane.

Cluster Types in OKE:

Type	Description	SLA
Enhanced Cluster	Supports all features (auto-scaling, virtual nodes, etc.)	Financially backed SLA
Basic Cluster	Core features only	Service Level Objective (SLO) – no SLA guarantee

Node Pool types:

Node Type	Managed By	Features	Availability
Virtual Nodes	Oracle	Serverless, automatic upgrades, patches	Only in Enhanced Clusters
Managed Nodes	Customer	Full control, manual upgrades, flexible config	In Basic & Enhanced Clusters

➡️ Choose Virtual Nodes if you want a serverless, hands-off experience.
➡️ Choose Managed Nodes if you need control & customization.

Oracle Functions & Serverless:

Serverless computing means developers only write and upload code — they don't manage servers or infrastructure. The cloud provider handles execution, scaling, and availability.

Evolution Path:

- Bare Metal: Full hardware control.
- Virtual Machines (VMs): Split a large server into smaller independent units.
- Containers: Lightweight, portable, faster than VMs, share OS kernel.
- Functions: Only code runs; no server management. Fully event-driven and pay-per-execution.

Oracle Functions:

- A Function-as-a-Service (FaaS) offering by Oracle.
- Event-driven — triggers from APIs, CLI, or OCI events.
- Runs inside containers managed by Oracle.
- Powered by the open-source Fn Project engine.
- Consumption-based pricing: You pay only for the time code runs, not for idle time.
- Highly scalable and autonomous — can execute multiple functions in parallel.
- Integrates easily with other OCI services or external systems.

Although it's called Serverless, servers still exist — but the developer doesn't manage them. Oracle handles everything behind the scenes.

Storage

Oracle Cloud offers different types of storage depending on how you want to store and access your data.

- Persistence: Data remains even after you stop or restart your instance
- Durability: How safely your data is stored — i.e., how unlikely it is to be lost.

Local NVMe: • This storage is physically attached to your VM. • It's very fast but temporary. • When you stop or delete your instance, data is lost. Example: Like a pen drive connected directly to your computer - fast, but not permanent.	Block Volume: It's persistent storage that you can attach/detach to VMs. • Create a block volume. • Attach it to your VM. • Create a partition (divide space). • Create a file system (format it). • Mount it (make it usable). Example: Like adding an external hard drive to your computer.
File Storage: • Shared storage — multiple VMs can access the same files. • Good for applications or databases that need shared access. Example: Like a network drive shared among several computers in a lab.	Object Storage: • Used to store unstructured data - images, videos, backups, logs, etc. • You upload files as objects with a unique name. • It's highly durable and accessible over the internet (HTTP APIs). Example: Like Google Drive or Dropbox — you just upload and download files.

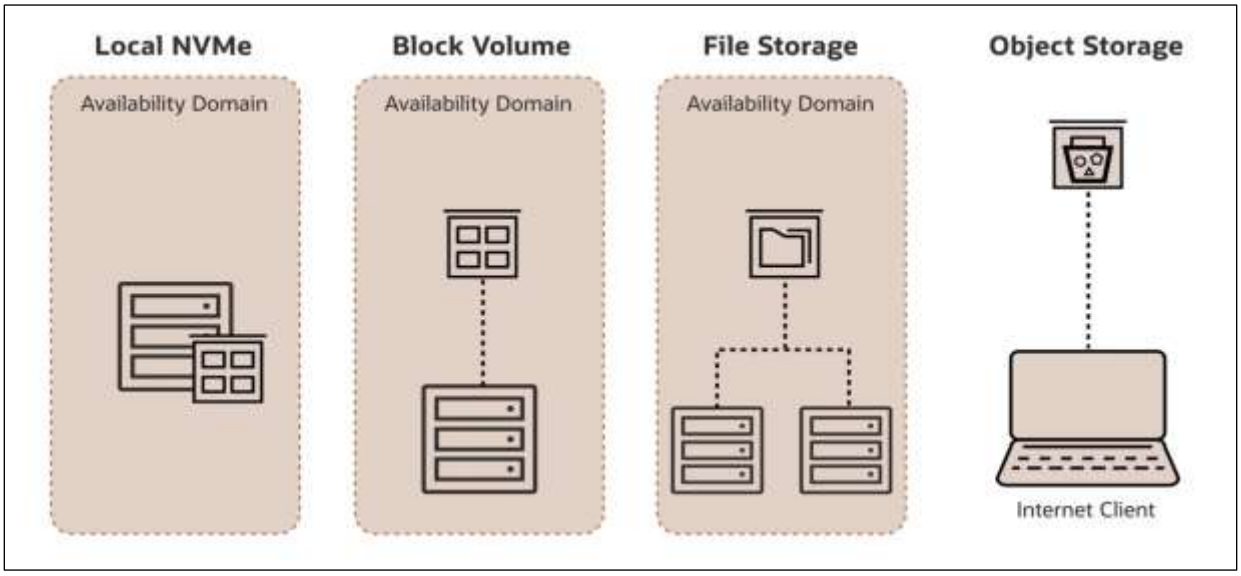


Image source: Oracle Cloud Infrastructure documentation

OCI Migration Services

1. Data Transfer Disk

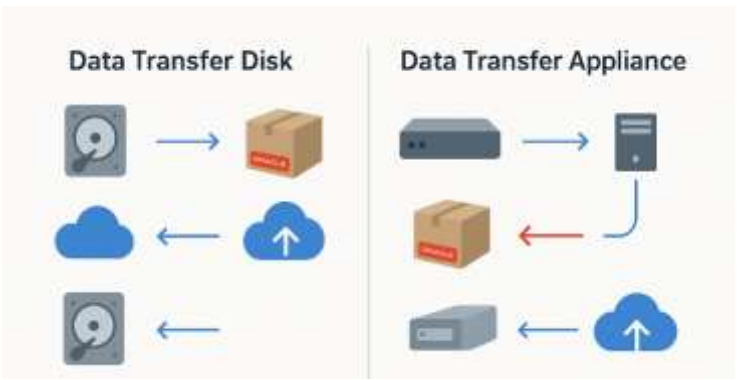
- You copy your data onto your own hard drives.
- Then, you ship those disks to Oracle.
- Oracle uploads the data to your Object Storage in the cloud.
- Finally, Oracle returns your disks to you.

Use case: If you have a few terabytes of data and want a low-cost method to move it.

2. Data Transfer Appliance

- Oracle sends you a special high-capacity, encrypted appliance (device).
- You load your data into it using a fast network connection.
- Then you ship the appliance back to Oracle.
- Oracle uploads everything securely into your OCI Object Storage.

Use case: When you have huge datasets (tens or hundreds of TBs or more) and want faster, more secure transfer.



Oracle Cloud Object Storage

Object Storage is used to store unstructured data (like photos, backups, logs, videos, etc.) in the cloud. It's highly durable, scalable, and accessible over the internet.

- Data is managed as objects.
- Each object has:
  - Name (key) → Identifier (like a file name)
  - Value (data) → Actual file/content
  - Metadata → Info about the file (date, type, size, etc.)
- Objects are stored inside buckets (like folders).

Storage tiers:

Tier Name	Usage	Minimum Storage Duration	Cost	Description
Standard Tier (Hot)	Frequently accessed data	No limit	Highest	For data you need often (daily use)
Infrequent Access Tier (Cool)	Infrequent Access	31 days	💰 💰 \~60% cheaper than Standard	For backups or monthly reports
Archive Tier (Cold)	Archive	90 days	💰 💰 💰 Cheapest	For long-term storage like old logs, records, etc.

Auto-Tiering

- Oracle automatically moves objects between tiers based on how often you use them.
- Example:
  - If a file hasn't been accessed for 30 days, it moves from Standard → Infrequent Access.
  - If accessed again, it can move back to Standard.
- This helps you save money automatically while keeping performance when needed.

Oracle Cloud Block Volume:

- It's persistent storage that works like a hard drive for your Oracle Cloud VM.
- You can attach, detach, resize, and move it easily.

- It supports read/write sharing - meaning multiple VMs can access the same block volume (useful for clustered apps).

Types of Block Volume Performance Levels

Oracle Cloud offers four performance options based on your speed and cost needs 👇

Characteristic	Lower Cost	Balanced	Higher Performance	Ultra-High Performance
Cost	Cheapest	Default	Higher	Maximum
Speed	Slower	Good Mix	Faster	Maximum
Use Case	Archival	General Workloads	Databases	High-End Databases

Read/Write Shareable

- A Block Volume can be attached to multiple compute instances at once in read/write mode.
- This allows shared access, useful in clustering, parallel processing, or HA systems (High Availability).

Example: Two VMs reading/writing to the same database volume.

Volume Groups:

A Volume Group is a collection of block volumes that you can manage together as a single unit. It makes it easier to handle multiple volumes at once.

Think of it like putting several files into one folder — you can manage them all together.

Features:

- Groups volume together for early management
- Time consistent backups

Oracle Cloud File Storage

- File Storage is a hierarchical collection of documents, organized into named directories and folders, just like in your computer.
- It provides shared file systems that can be accessed by multiple compute instances at the same time.

  Think of it like a shared network drive (like a college lab drive) that everyone can access together.

Security

Image source: Oracle Cloud Infrastructure documentation

- Security in the cloud is a shared responsibility between you (the customer) and Oracle.
- Who manages what depends on where your data and apps are running.

Oracle Cloud Guard:

1. Cloud Guard is a security monitoring and automation service in Oracle Cloud.
2. It helps you detect security problems and automatically respond to them.

Think of it like a security guard for your cloud - it keeps watch and fixes issues when found.

Component	Meaning	Simple Example
Target	The place Cloud Guard is watching (like a project, region, or tenancy).	"Monitor my whole project."
Detector	The one that looks for security risks or bad configurations.	Finds if a storage bucket is public.
Problem	What Cloud Guard reports when it finds something wrong.	"Public bucket detected."
Responder	The fixer — takes steps to solve or reduce the problem.	Makes the bucket private again automatically.

(Watch → Find → Report → Fix)

Security Zones

1. A Security Zone is a special compartment in Oracle Cloud that automatically enforces strong security rules on all resources inside it.
2. You can't create or configure anything inside a Security Zone that breaks Oracle's best security practices.

Max Security Zone:

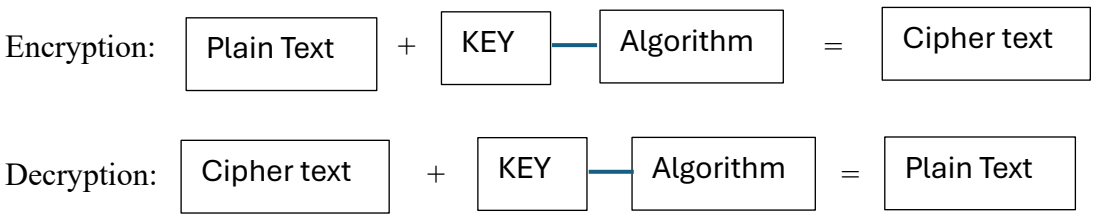
- It's the strictest type of security zone.
- Enforces maximum security policies by default (like encryption, no public buckets, etc.).
- Ensures your most critical workloads are fully protected.

Security Advisor:

- The Security Advisor is a recommendation tool in Oracle Cloud.
- It checks your tenancy (cloud setup) and gives suggestions to improve security.
- It can also guide you on creating security zones for better protection.

Basics of Encryption:

- Encryption: Process of converting plain text → cipher text to protect data from unauthorized access.
- Decryption: Process of converting cipher text → plain text using a key.
- Key: A piece of information (like a password or code) used to perform encryption and decryption.



Encryption at Rest

- Means data is encrypted while stored on disks, databases, or backups.
- Protects data if someone gains access to the physical storage.

Your files stored in Oracle Object Storage are encrypted on the server's disk, so even if someone steals the storage device, they can't read your data.

Encryption in Transit

- Means data is encrypted while moving between systems — for example, between your computer and the cloud.

- Protects data from hackers during transmission (like on a network).

When you upload a file to Oracle Cloud, it's sent using HTTPS (SSL/TLS) so no one can intercept or read it in between.

Symmetric Encryption:

- The same key is used for both encryption and decryption.
- Ex: You lock and unlock a box using the same key.

Asymmetric Encryption:

- Uses two different keys — a public key to encrypt and a private key to decrypt
- Ex: You lock the box with a public key, but only the person with the private key can open it.

AES (Advanced Encryption Standard)

- AES is a symmetric key encryption algorithm, meaning the same key is used for both encryption and decryption.
- Since the same key is shared between sender and receiver, key management is crucial for maintaining security.
- AES works on fixed block sizes (typically 128 bits) and supports key lengths of 128, 192, or 256 bits.
- However, it cannot be used for digital signatures, as that requires asymmetric encryption involving a public and private key pair.

RSA (Rivest–Shamir–Adleman)

- RSA is an asymmetric key encryption algorithm, meaning it uses two different keys a public key and a private key.
- The public key is used to encrypt data, while the private key is used to decrypt it.
- In digital signing, RSA works in reverse: the private key signs the message, and the public key verifies the signature.

ECDSA (Elliptic Curve Digital Signature Algorithm)

- ECDSA is an asymmetric cryptographic algorithm used mainly for digital signatures, not for encryption.
- It is based on elliptic curve mathematics, which makes it faster and more secure with smaller key sizes compared to RSA.
- It uses two keys — a private key to sign data and a public key to verify the signature.

Hardware Security Module (HSM)

A Hardware Security Module (HSM) is a physical device used to protect and manage digital keys and perform encryption/decryption in a highly secure way.

Ex: When a bank encrypts sensitive data (like transactions), the HSM stores the encryption keys and performs all cryptographic operations securely inside it — protecting the data even if the system is hacked.

OCI Vault: OCI Vault is a secure key management service in Oracle Cloud that helps you store, manage, and control encryption keys and secrets used to protect your cloud resources and data.

Governance and Administration

Pricing Models:

Pay-As-You-Go (PAYG):

- You pay only for what you use, when you use it — no long-term commitment required.
- Good when your usage is unpredictable or you're just starting out.
- Unit pricing tends to be at standard list rates (so potentially higher than if you commit).
- Flexible: you can scale up/down easily.

Annual Universal Credits:

- You commit to a pre-paid number of credits (for a 12-month term or more) to use across eligible OCI services.
- In return, you get discounted rates compared to PAYG.
- Flexibility: the credits can be used for many services across regions (within the contract's scope).
- Risk: If you don't use the credits, you may lose value (unused credits expire).
- Best when you have predictable workloads and can estimate needs for the year.

Bring Your Own License (BYOL):

- If you already own valid licenses for certain Oracle software (on-premises), you may reuse them in OCI to reduce costs.
- Especially relevant for customers migrating existing Oracle workloads to the cloud and wanting to "carry forward" investment in licenses.
- Helps with cost-optimization — less "license-included" cost when you supply your own license.

Factors Impacting OCI Prices

1. **Resource Size:** The larger your resource (like CPU cores, memory, or storage size), the higher the cost.
2. **Data Transfer:**

- Data movement between OCI and the internet affects cost.

- Incoming traffic (uploads) → Free
- Outgoing traffic (downloads) →Charged, but the cost is lower compared to many other clouds.

3. **Resource Type:**
- Different services have different pricing models.
- Example: Compute, Storage, Database, and AI services all have their own rate per hour or per GB.

4. **OCI Regions:**
- Oracle maintains consistent pricing across all OCI regions.
- No extra cost based on where your resource is located.

5. **Usage Duration:**
- The longer your resources are active, the more you pay (especially in Pay-As-You-Go).
- Stopping or terminating unused resources saves cost.

OCI Cost Management

1. **OCI Budgets:**
   - You can set a spending limit (budget) for a compartment or the entire tenancy.
   - OCI alerts you (via email or notification) when your spending approaches or exceeds that limit.

2. **Cost Analysis:**
   - Helps you visualize and analyse your cloud spending.
   - You can check past costs, identify trends, and manage current costs.

3. **Usage Reports:**
   - Provides detailed CSV reports with daily or hourly usage for each service.
   - Useful for tracking exact consumption and for financial auditing or forecasting.

4. **Service Limits and Usage:**
   - Every service has a quota or limit (like number of CPUs, storage size, etc.).
   - You can monitor current usage and request limit increases when needed.

5. **Compartment Quotas:**
   - Compartment quotas are rules that let you control and limit how much cloud resources can be used within a specific compartment.
   - They act as a fine-grained control mechanism for resource allocation inside your tenancy.
     Quota Statements in OCI

     - SET: Used to define the maximum number of resources a compartment can use.
     - UNSET: Used to remove or reset a quota rule, restoring it to the default service limits.
     - ZERO: Used to block access to a specific resource type for a compartment.

Tagging in OCI: Tagging helps you organize, track, and manage your cloud resources easily. You can assign metadata (tags) to resources like compute instances, storage, or databases for better visibility and cost tracking.

1. **Free-Form Tags**
    - Simple key-value pairs that you can add without predefined structure.
    - Easy to create, flexible, but no access control or validation.
2. **Defined Tags**
    - Tags created within a tag namespace by an administrator.
    - They are predefined, controlled, and validated, ensuring consistent tagging across the organization.