



ORACLE

OCI Foundations

Nestor Cayllahua

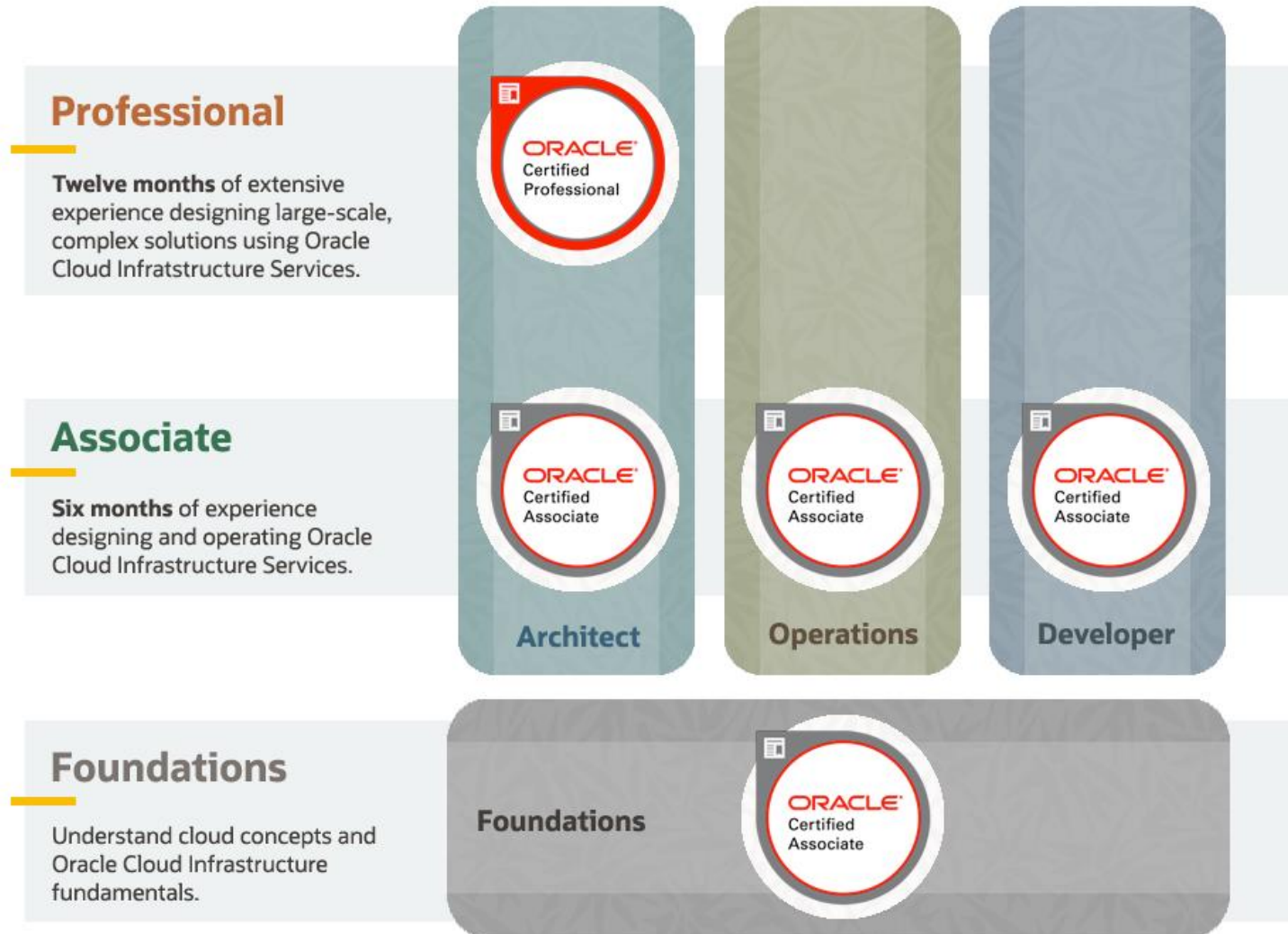
Senior Solution Engineer

Oracle Cloud Infrastructure Architect Certified

Safe Harbor Statement

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

Oracle Cloud Infrastructure Certifications



Course Content

Lesson 1 :
Cloud Concepts

Lesson 2 :
OCI Architecture

Lesson 3 :
Networking Services

Lesson 4 :
Compute Services

Lesson 5 :
Storage Services

Lesson 6 :
Database Services

Lesson 7 :
IAM Service

Lesson 8 :
Security

Lesson 9 :
Pricing and Billing



ORACLE

Cloud Concepts

Rohit Rahi

Oracle Cloud Infrastructure

Feb 2020

Agenda

Cloud Computing
Service Models
Cloud Terminology
CAPEX v/s OPEX

Cloud Computing

On-demand self-service

Provision computing capabilities as needed automatically without requiring human interaction with service provider

Broad network access

Capabilities are available over the network and accessed through standard mechanisms

Resource pooling

The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different resources dynamically assigned and reassigned according to demand

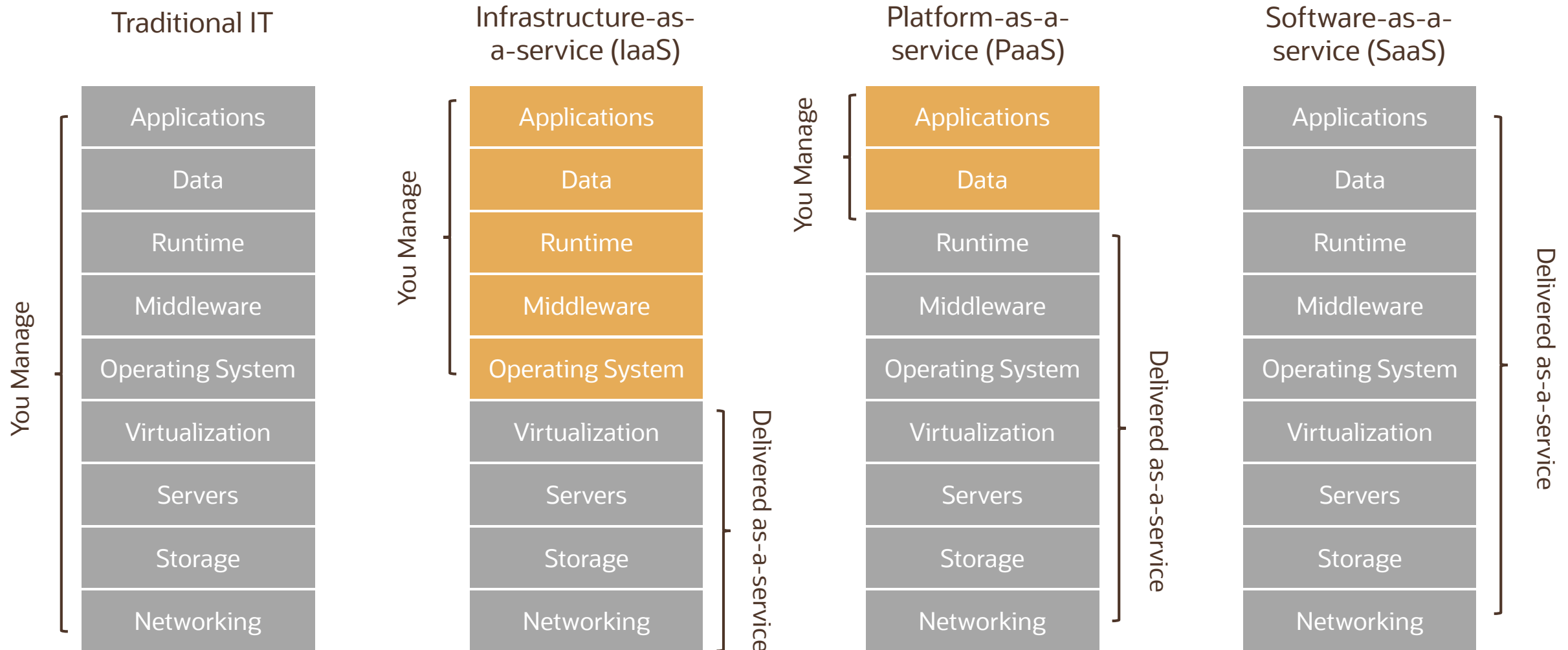
Rapid elasticity

Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward with demand

Measured service

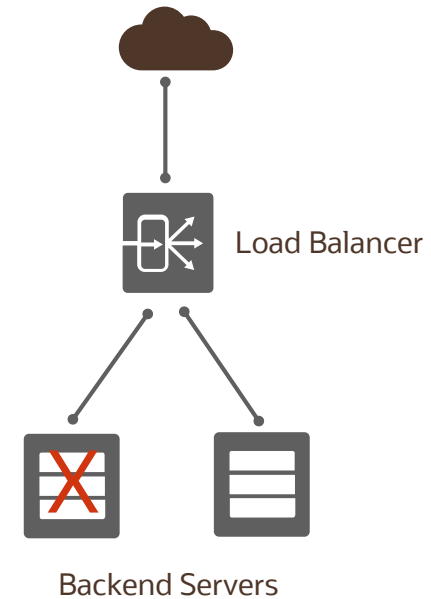
Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service

Service Models



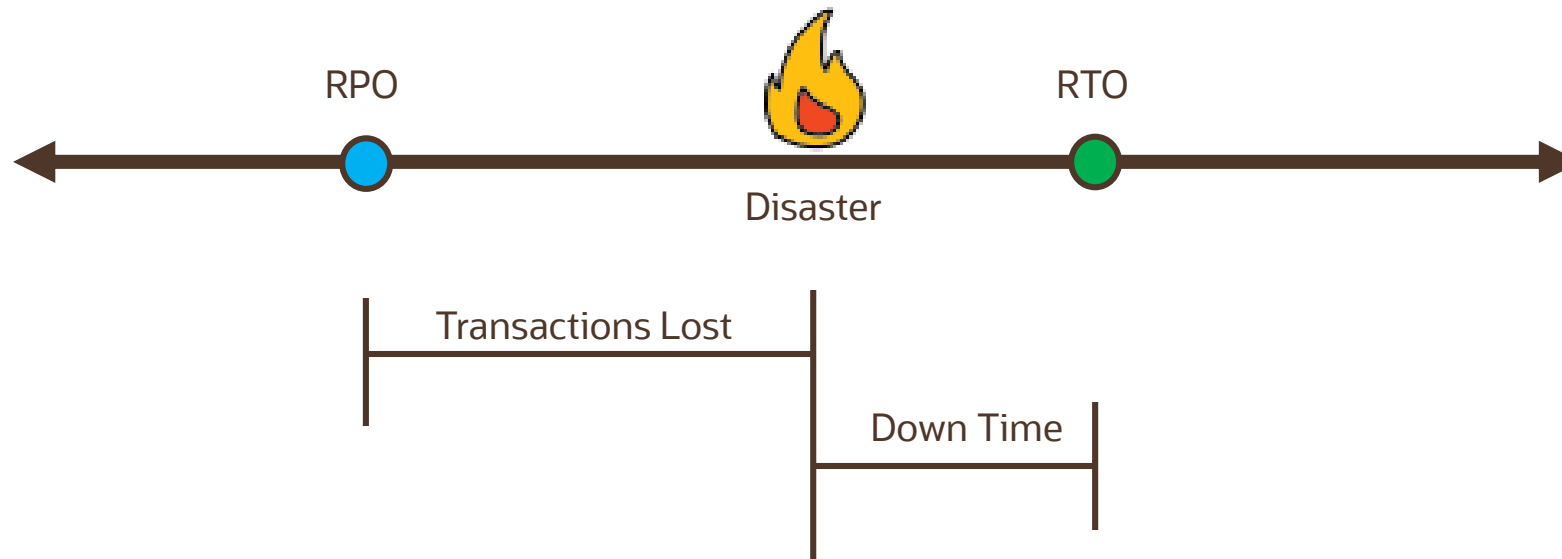
High Availability

- Computing environments configured to provide nearly full-time availability are known as high availability systems
- Such systems typically have redundant hardware and software that makes the system available despite failures
- Well-designed high availability systems avoid having single points-of-failure
- When failures occur, the failover process moves processing performed by the failed component to the backup component. The more transparent that failover is to users, the higher the availability of the system



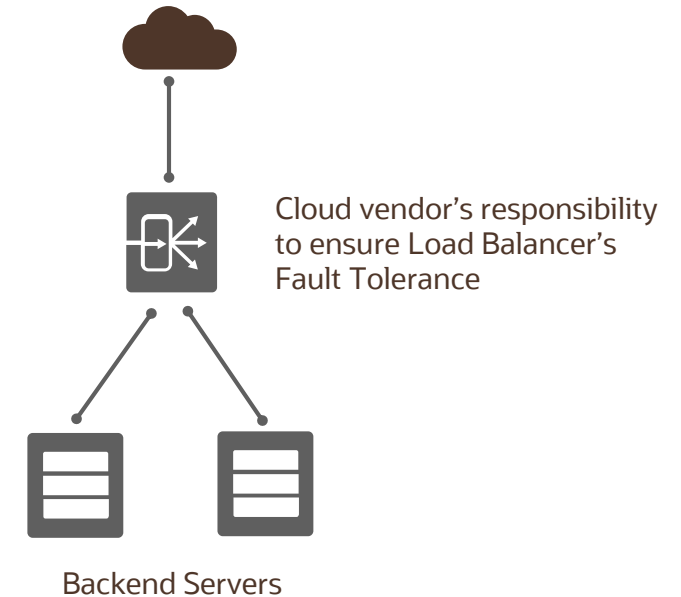
Disaster Recovery

- Disaster recovery (DR) involves a set of policies, tools and procedures to enable the recovery or continuation of vital technology infrastructure and systems
- Disaster recovery should indicate the key metrics of [recovery point objective](#) (RPO) and [recovery time objective](#) (RTO)



Cloud Terminology

- **Fault Tolerance** describes how a cloud vendor will ensure minimal downtime for services provided
- **Scalability** refers to scaling out (or in) or scaling up (or down).
 - Scaling out (or in) is called horizontal scaling
 - Scaling up (or down) is called vertical scaling
- **Elasticity** is the ability to quickly increase or decrease resources



CAPEX v/s OPEX



CAPEX

Capital expenditure or capital expense (CAPEX) is the money an organization or corporate entity spends to buy, maintain, or improve its fixed assets, such as buildings, vehicles, equipment, or land



OPEX

Operational expenditure or OPEX is an ongoing cost for running a product, business, or system

Cloud lets you trade CAPEX for OPEX

Instead of having to invest heavily in data centers and infrastructure, in the cloud, **you can pay only when you consume resources**, and **pay only for how much you consume**

ORACLE

OCI Architecture

Agenda

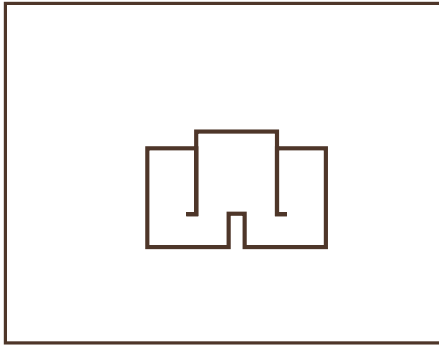
OCI Regions
Availability Domains
Fault Domains
High Availability Design
Compartments

Oracle Cloud Infrastructure Global Footprint

February 2020: 21 Regions Live, 15 Planned

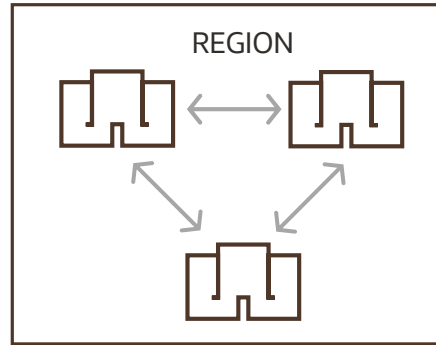


OCI Architecture



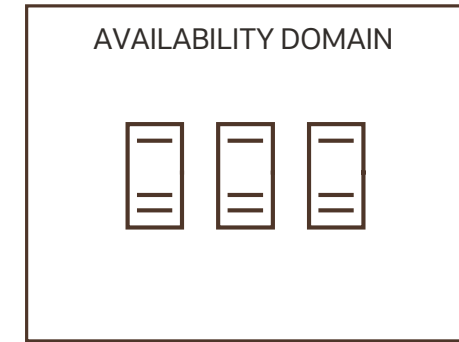
Regions

Localized geographic area, comprised of one or more Availability Domains (AD)



Availability Domains (AD)

One or more fault-tolerant, isolated data centers located within a region, but connected to each other by a low latency, high bandwidth network



Fault Domains (FD)

Grouping of hardware and infrastructure within an Availability Domain to provide anti-affinity (logical data center)

One AD Regions

- OCI has chosen to launch regions in new geographies with one AD (to increase our global reach quickly)
- For any region with one AD, a second AD or region in the same country or geo-political area will be made available within a year to enable further options for DR and data residency

OCI Region (current)	# ADs
US West (Phoenix)	3
US East (Ashburn)	3
UK South (London)	3
Germany Central (Frankfurt)	3
Australia East (Sydney)	1
Australia Southeast (Melbourne)	1
Canada Southeast (Toronto)	1
India West (Mumbai)	1
Japan East (Tokyo)	1
Japan Central (Osaka)	1

OCI Region (current)	# ADs
Brazil East (Sao Paulo)	1
Netherlands Northwest (Amsterdam)	1
Saudi Arabia West (Jeddah)	1
South Korea Central (Seoul)	1
Switzerland North (Zurich)	1

Choosing a region

Location

Choose a region closest to your users for lowest latency and highest performance!

Data Residency & Compliance

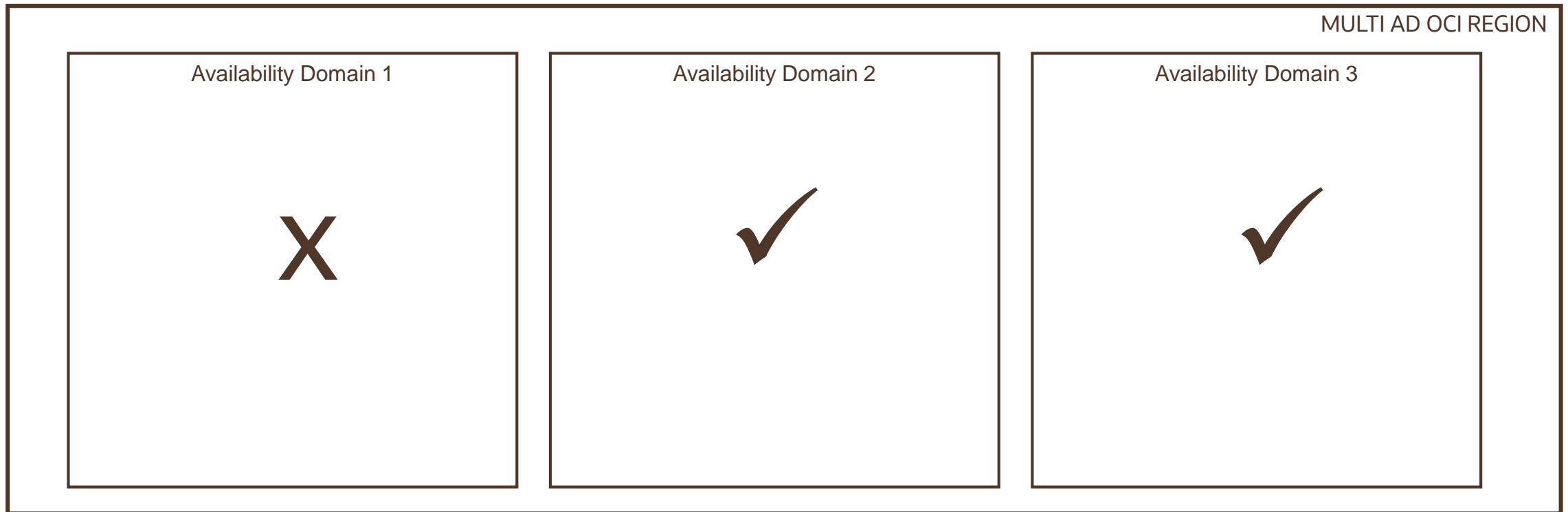
Many countries have strict data residency requirements

Service Availability

New cloud services are made available based on regional demand, regulatory compliance, resource availability, and other factors

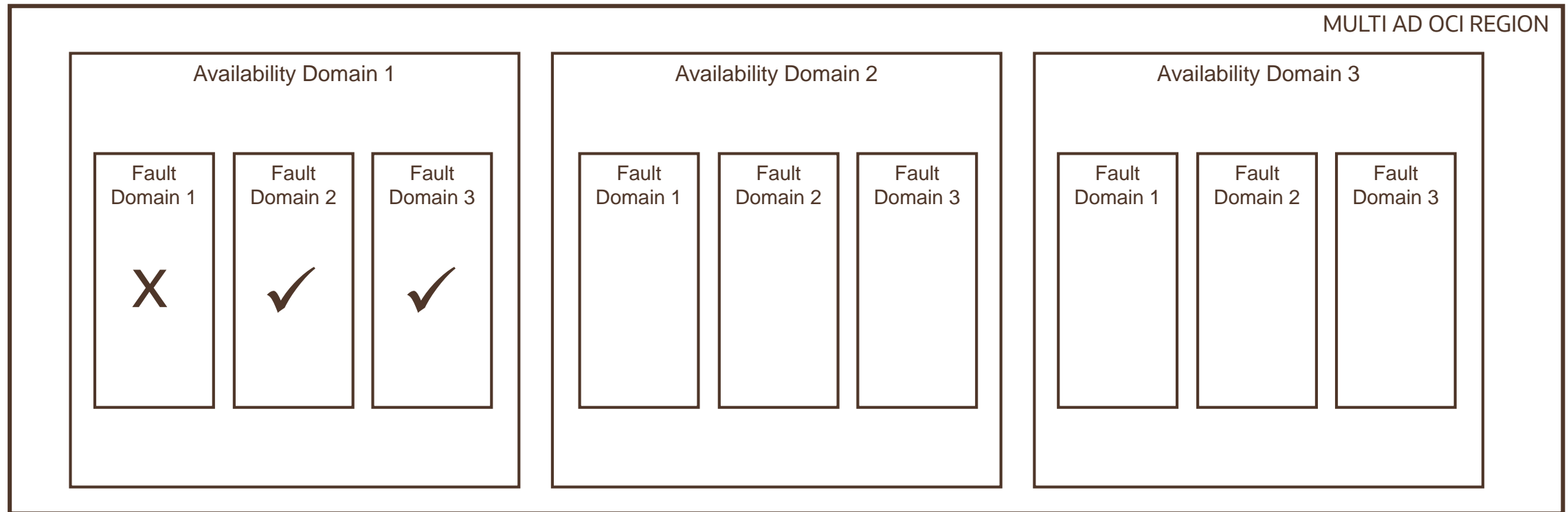
Availability Domains

- Availability domains are **isolated from each other**, fault tolerant, and very unlikely to fail simultaneously.
- Because availability domains **do not share physical infrastructure, such as power or cooling, or the internal availability domain network**, a failure that impacts one AD is unlikely to impact the availability of the others



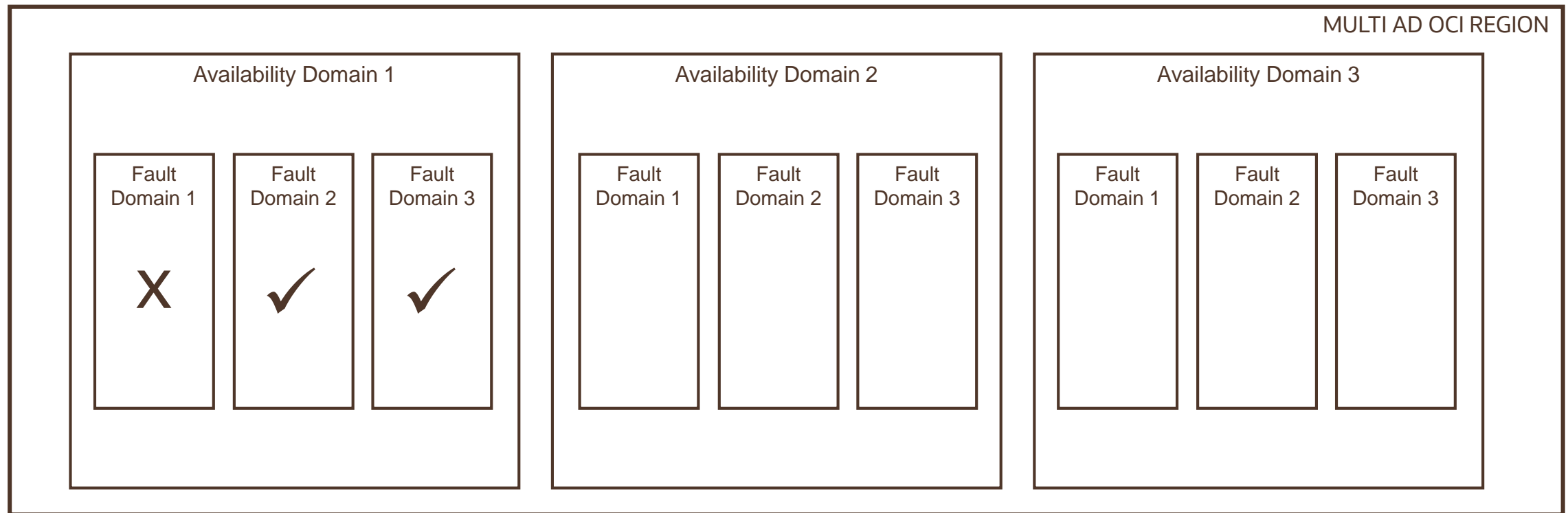
Fault Domains

- Each Availability Domain has three Fault Domains (FD)
- FDs act as a **logical data center** within an AD. Usage of multiple FDs reduces correlation of failures within an AD
- Resources placed in different FDs will not share single points of hardware failure (same physical server, physical rack, top of rack switch or power distribution unit)



Fault Domains

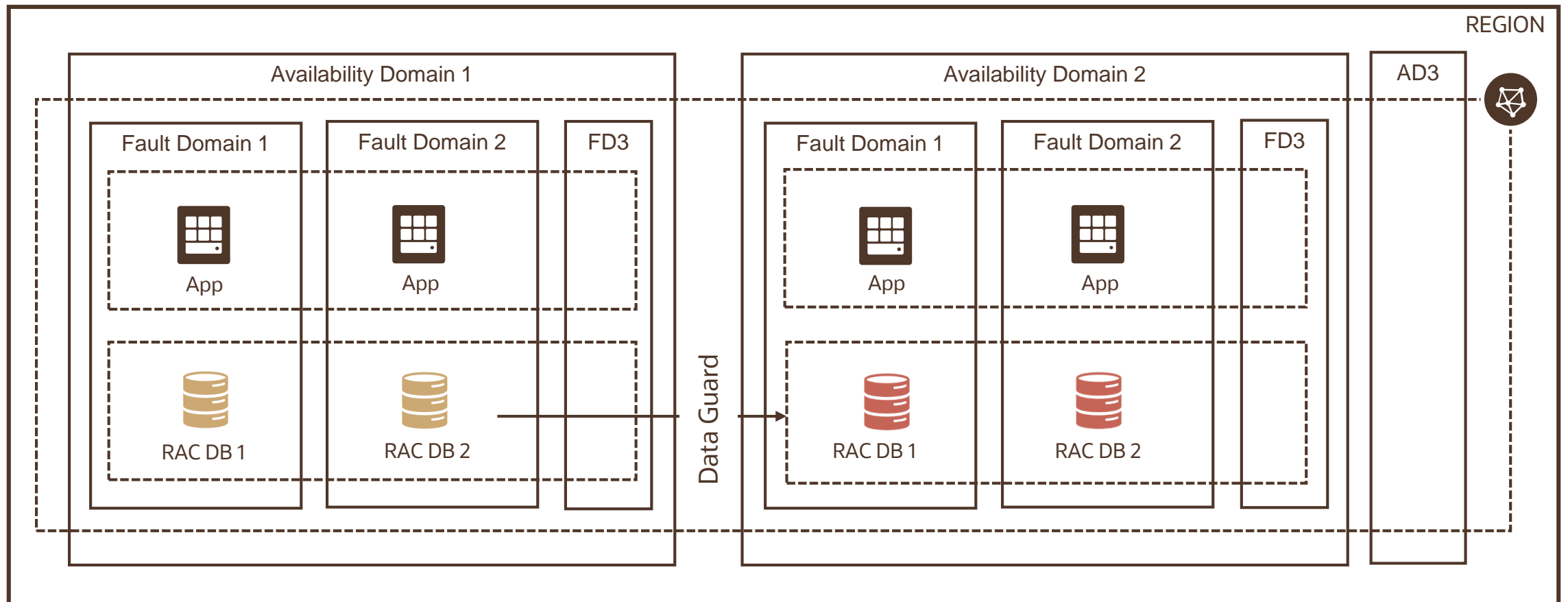
- In any region, resources in at most ONE fault domain are being actively changed at any point in time. This means that availability problems caused by change procedures are isolated at the fault domain level
- You can control the placement of your compute or database instances to fault domains at instance 'launch' time



Avoid single points of failure

Design your architecture to deploy instances that perform the same tasks

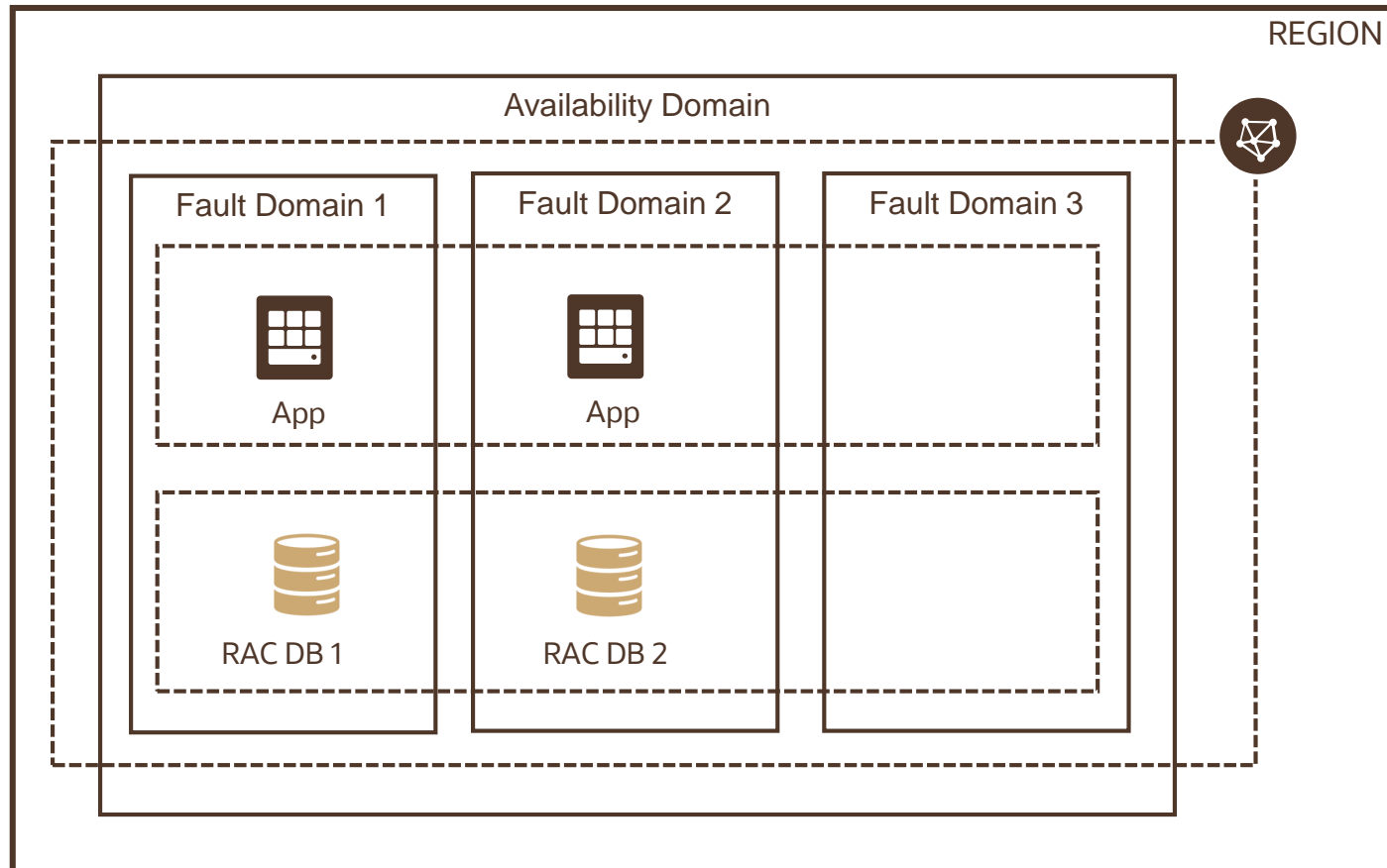
- In different Fault Domains (in one AD regions)
- In different Availability Domains for multiple AD regions



Avoid single points of failure

Design your architecture to deploy instances that perform the same tasks

- In different Fault Domains in one AD regions

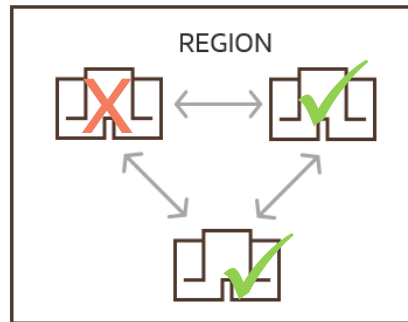


High Availability Design



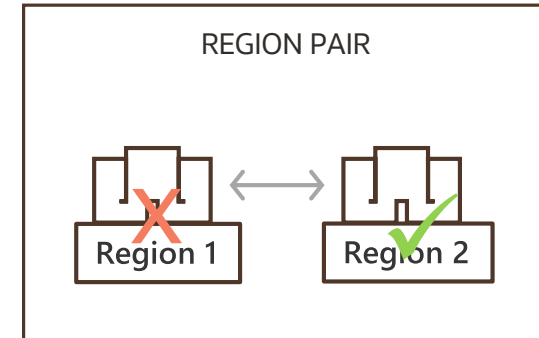
Fault Domains

Protection against failures within an Availability Domain



Availability Domains

Protection from entire Availability Domain failures (multi-AD region)



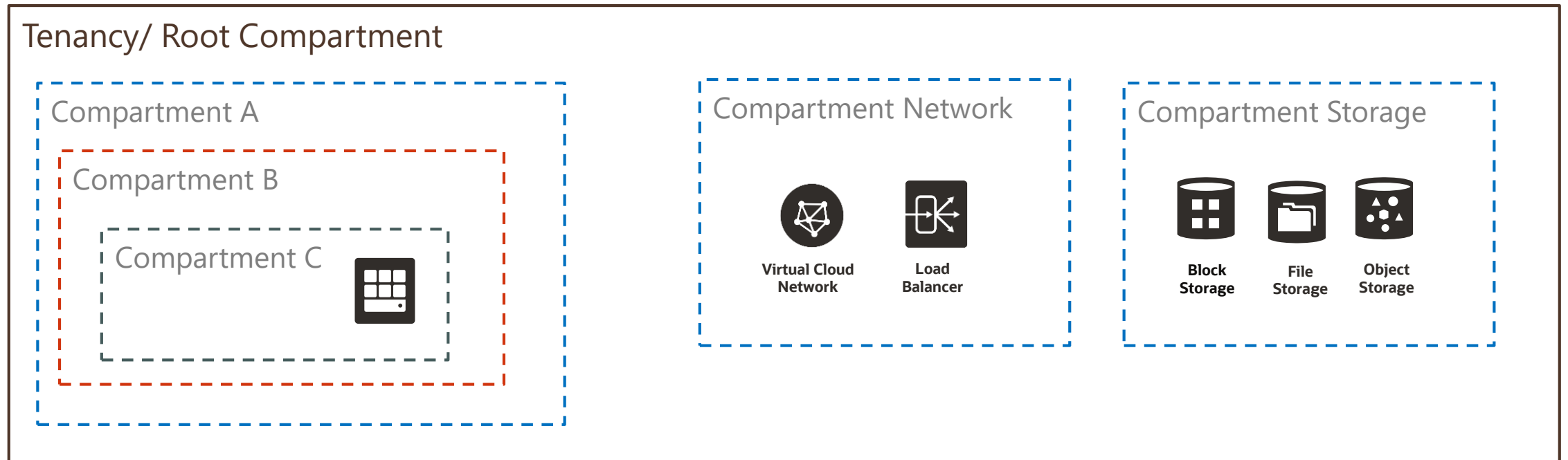
Region Pair

Protection from disaster with data residency & compliance

SLAs on Availability, Management and Performance

Compartment

A compartment is a collection of related resources. It helps you isolate and control access to your resources



Root Compartment can hold all the cloud resources. Best practice is to create dedicated compartments when you need to isolate resources

Compartment

Each resource belongs to a single compartment

Resources can interact with other resources in different compartments

Resources and compartments can be added and deleted anytime

Resources can be moved from one compartment to another

Resources from multiple regions can be in the same compartment

Compartments can be nested (six levels deep)

You can give group of users access to compartments by writing Policies

Analyze cost and assign budget for resources in compartments



ORACLE

The background features several abstract, organic shapes. On the left, a large, textured, brownish-grey shape resembles a cloud or a stylized mountain. On the right, there are two smaller, more fluid shapes: a light blue one and a red one, both with a fine, wavy texture. Scattered throughout the background are small, horizontal orange and yellow lines and dots, giving the impression of a digital or network environment.

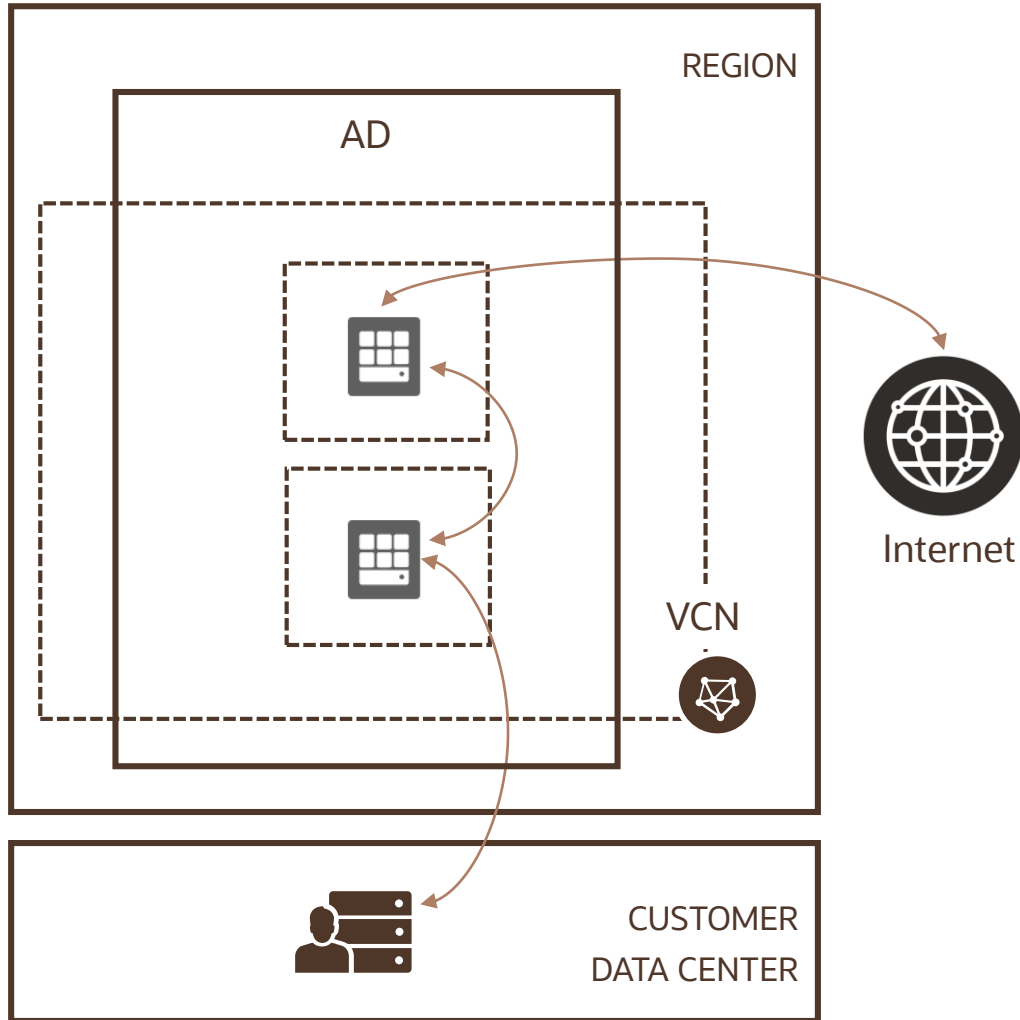
OCI Networking Services

Agenda



Virtual Cloud Network
Gateways
Peering
VCN Security
Load Balancer

Virtual Cloud Network (VCN)



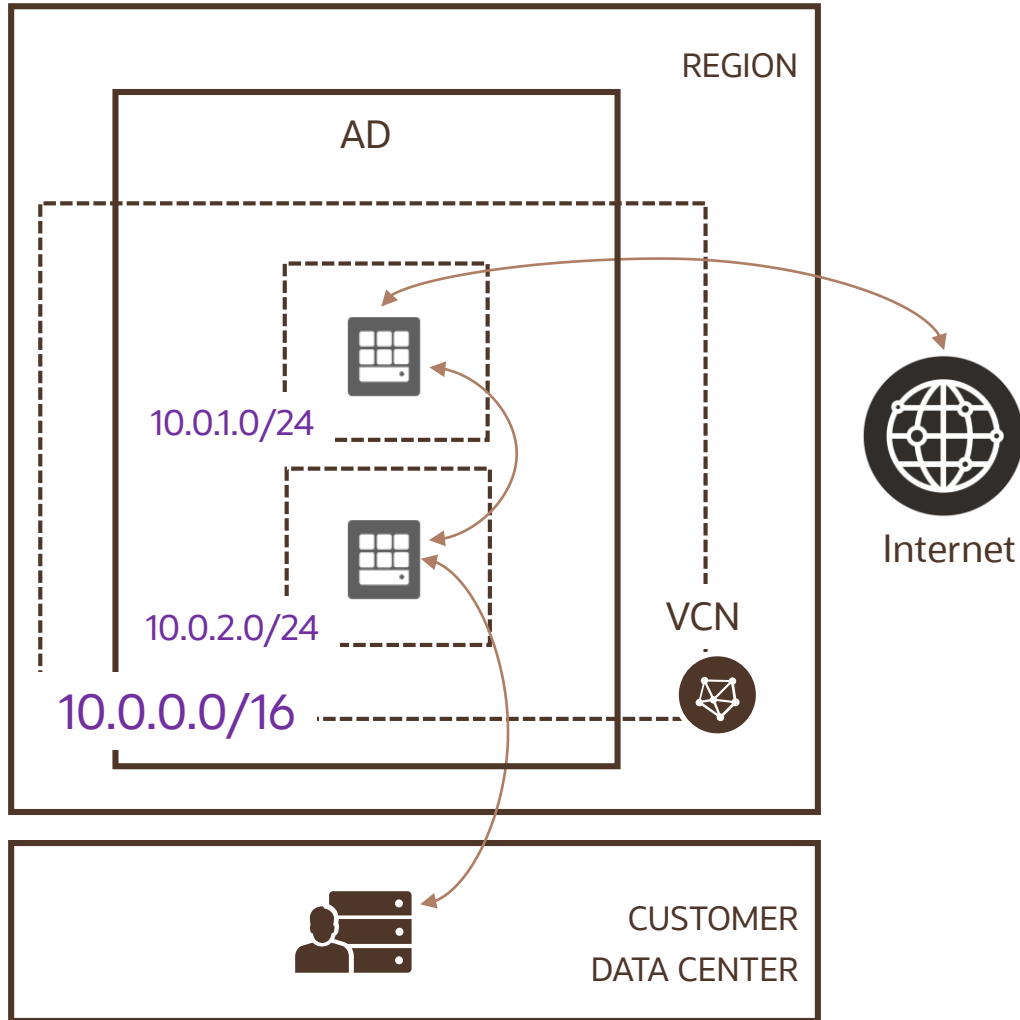
Software defined private network that you set up in OCI

Enables OCI resources such as compute instances to securely communicate with Internet, other instances or on-premises data centers

Lives in an OCI region

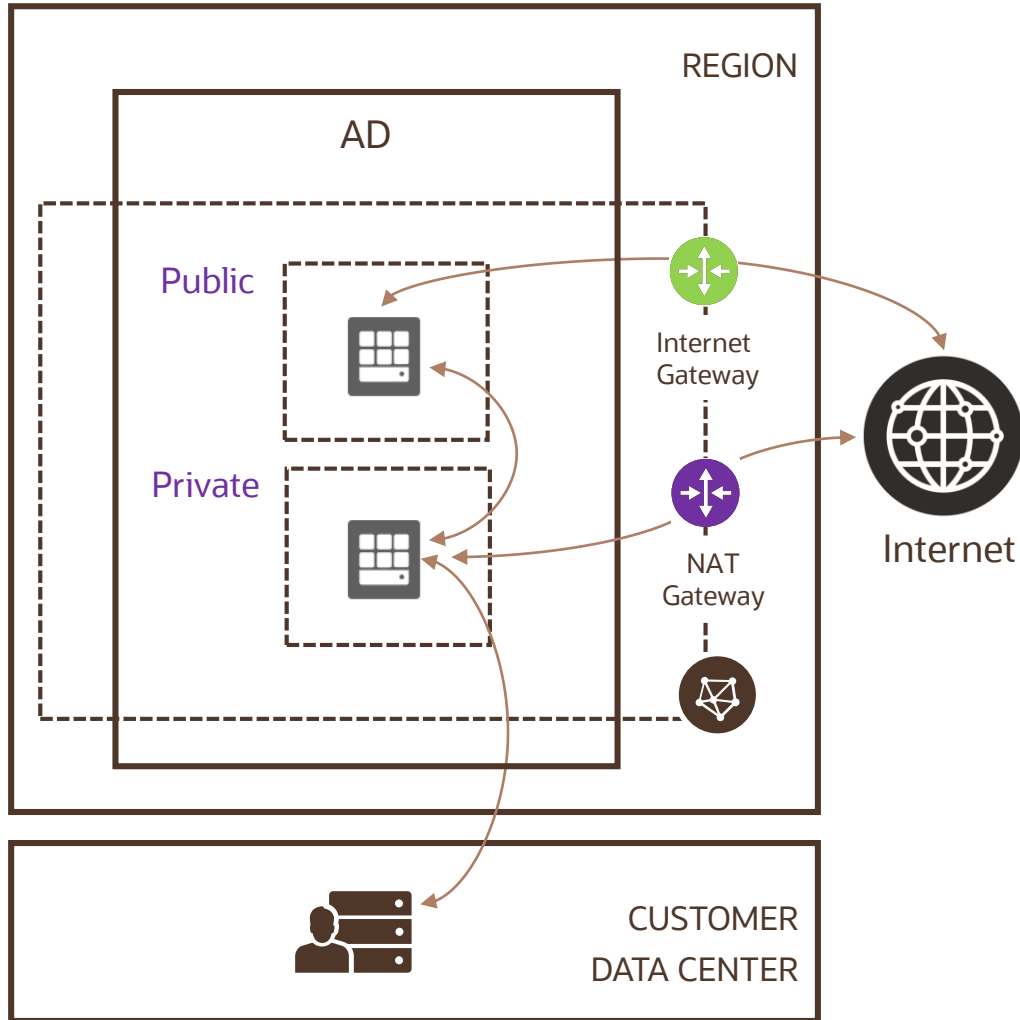
Highly Available, Scalable and Secure

VCN address space



- Address space is a range of IP address that you assign to a VCN E.g., 10.0.0.0/16
 - Range: 10.0.0.0 – 10.0.255.255
- Every resource that is connected to this VCN will get its own unique private IP address
 - Server 1 : 10.0.1.2
 - Server 2: 10.0.2.2
- Subnets let you divide the VCN into one or more sub networks
 - E.g., 10.0.0.0/16 – 10.0.1.0/24, 10.0.2.0/24..
 - Compute instances are placed in subnets
 - Subnets can be isolated and secured

Communication to Internet

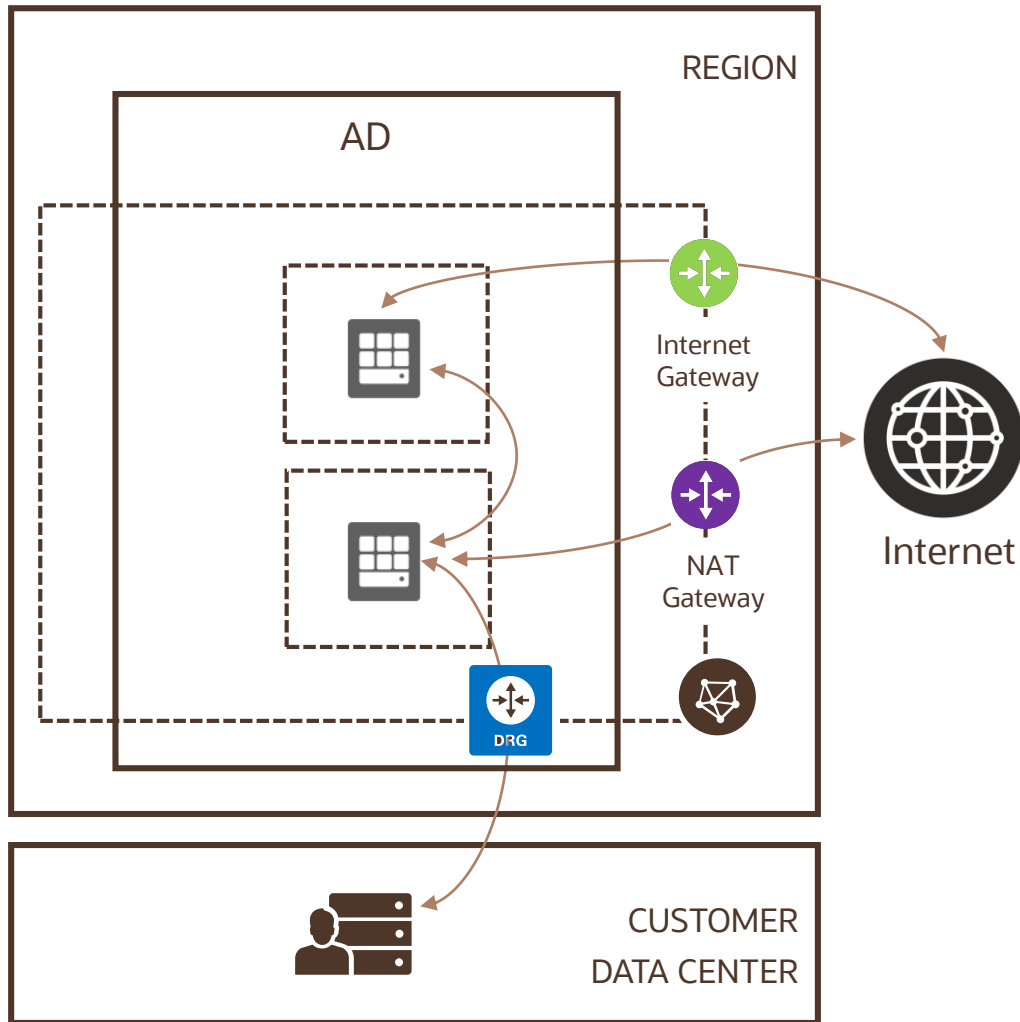


Internet gateway provides a path for network traffic between your VCN and the internet

NAT Gateway enables outbound connections to the internet, but blocks inbound connections initiated from the internet

Use case: updates, patches)

Communication to on-premises

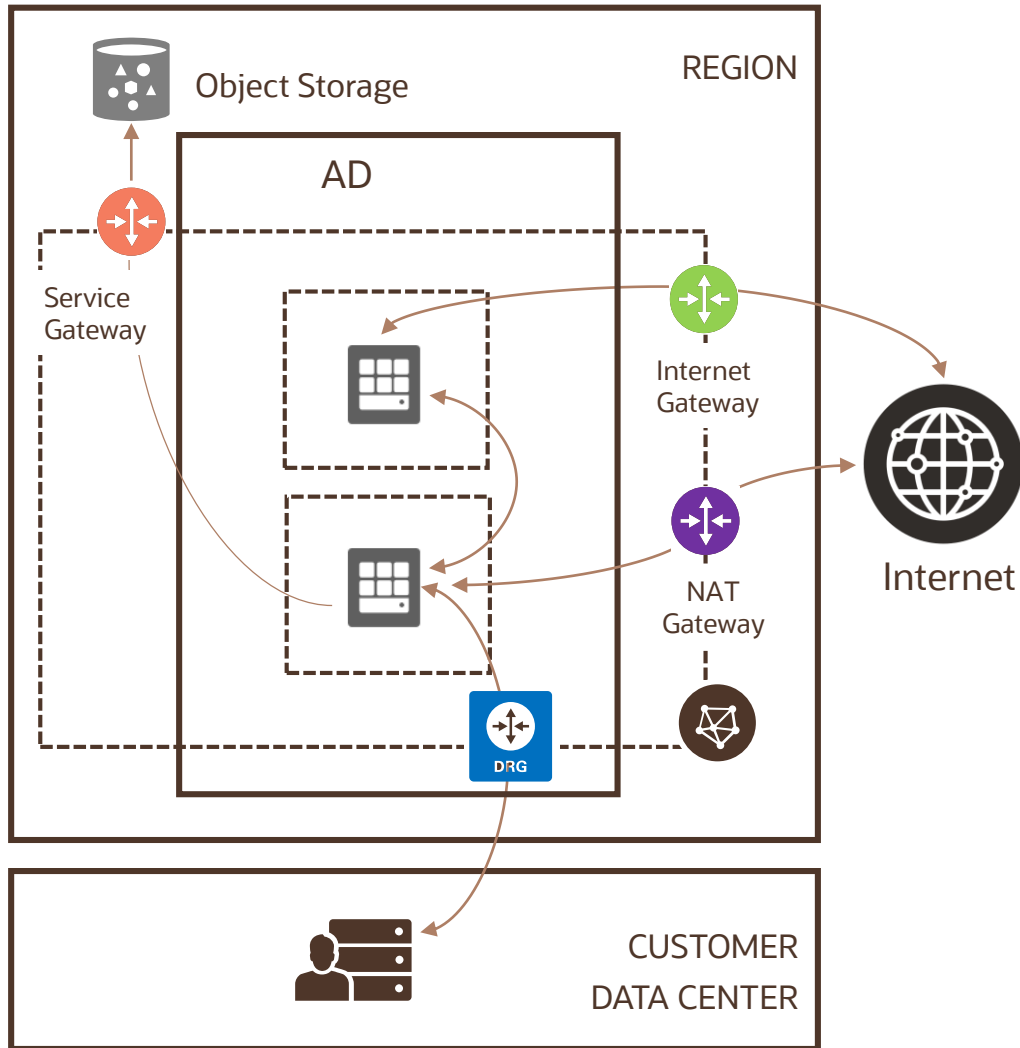


DRG is a virtual router that provides a path for private traffic between your VCN and destinations other than the internet

You can use it to establish a connection with your on-premises network via

- IPsec VPN
- FastConnect (private, dedicated connectivity)

Communication to public OCI services

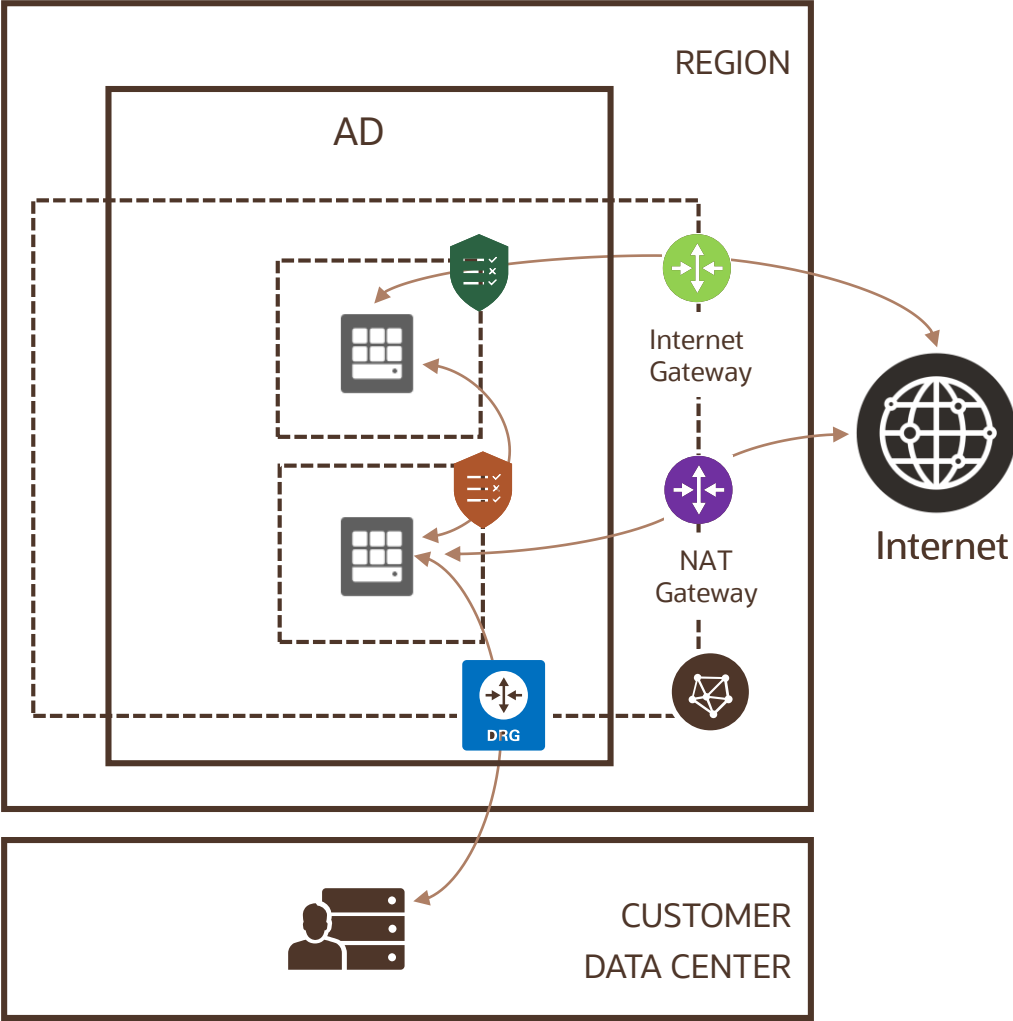


Service gateway lets resources in VCN access public OCI services such as Object Storage, but without using an internet or NAT gateway

Any traffic from VCN that is destined for one of the supported OCI public services uses the instance's private IP address for routing, travels over OCI network fabric, and never traverses the internet.

Use case: back up DB Systems in VCN to Object Storage)

VCN Security



A common set of firewall rules associated with a subnet and applied to all instances launched inside the subnet

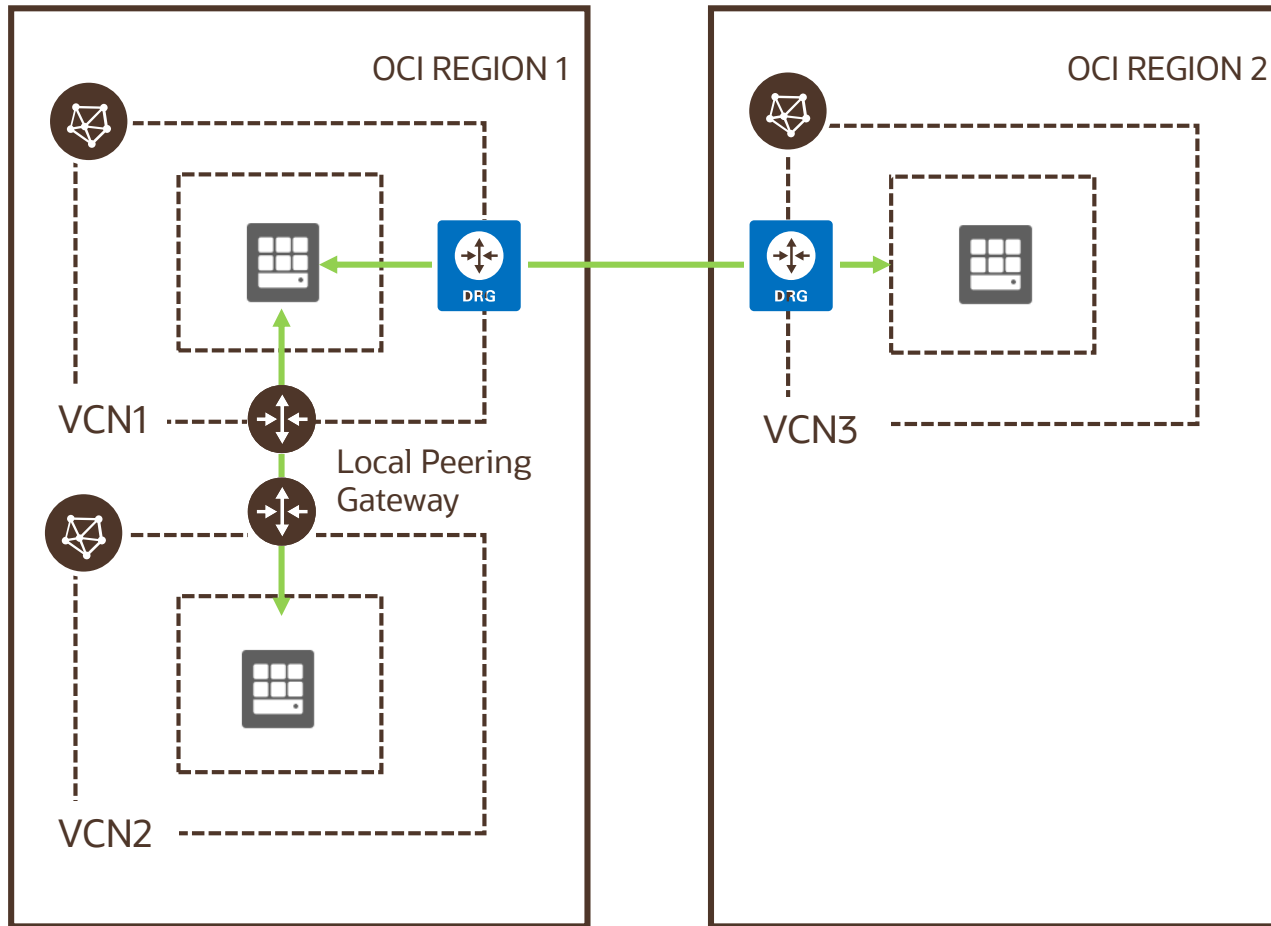
- Security list consists of rules that specify the types of traffic allowed in and out of the subnet
- Security list apply to a given instance whether it's talking with another instance in the VCN or a host outside the VCN
- Stateful or stateless



	Direction	CIDR	Protocol	Source Port	Dest Port
Stateful	Ingress	0.0.0.0/0	TCP	All	80
Stateful	Egress	10.0.2.0/24	TCP	All	1521

- Network Security Group consists of set of rules that apply only to a set of VNICs of your choice

Communication to other VCNs: Peering



VCN peering is the process of connecting multiple VCNs

Local VCN Peering is the process of connecting two VCNs in the same region so that their resources can communicate using private IP addresses

Remote VCN Peering is the process of connecting two VCNs in different regions so that their resources can communicate using private IP addresses

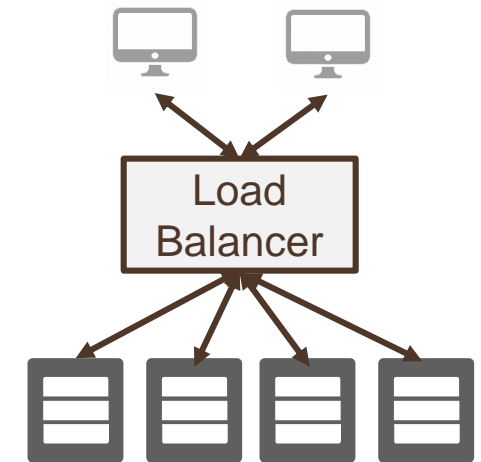
Load Balancer

A load balancer sits between the clients and the backends performs tasks such as:

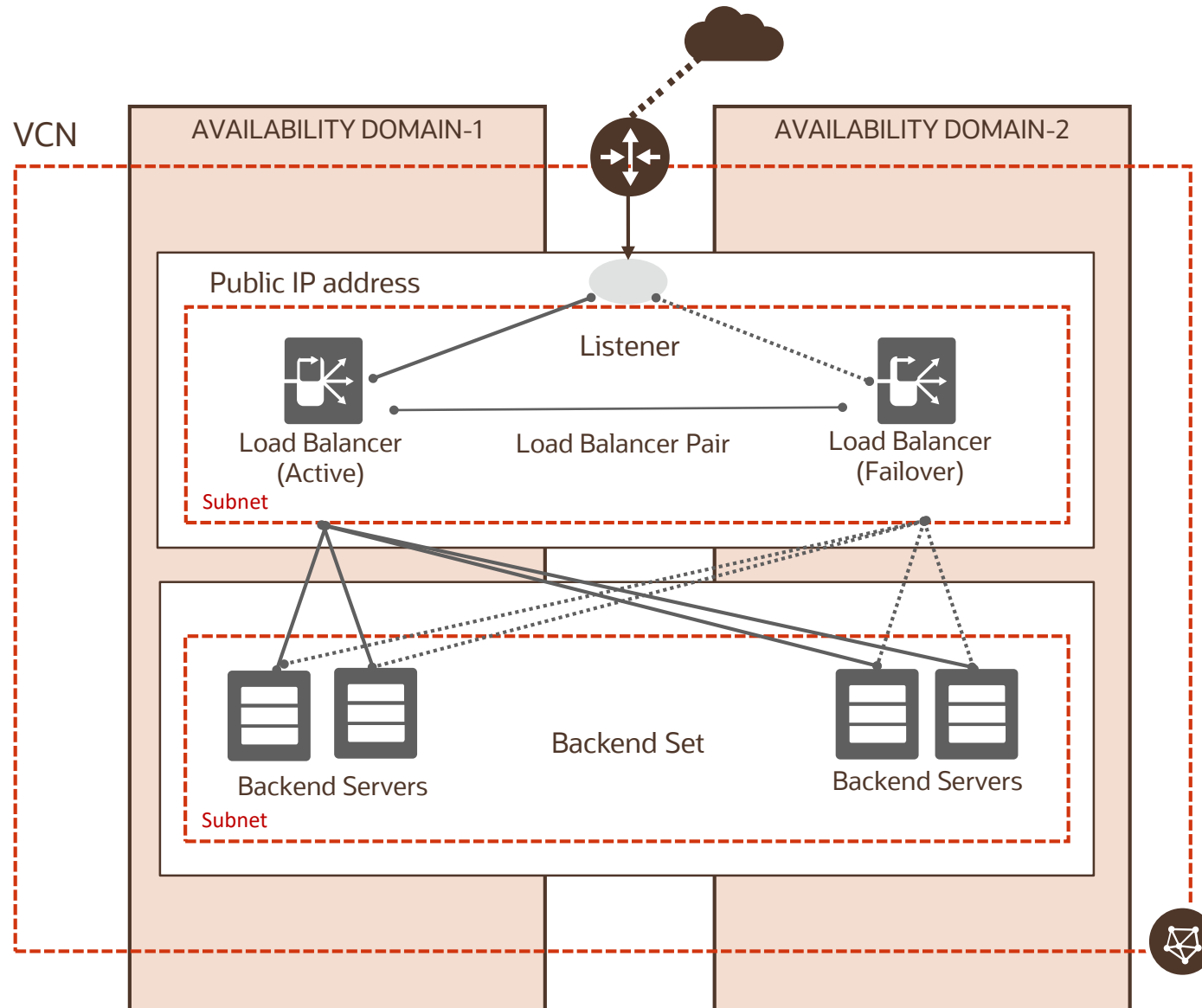
- **Service Discovery:** What backends are available? How should LB talk to them?
- **Health Check:** What backends are currently healthy to accept requests?
- **Algorithm:** What algorithm should be used to balance individual requests across the healthy backends?

Load Balancer benefits

- **Fault tolerance and HA:** using health check + LB algorithms, a LB can effectively route around a bad or overloaded backend
- **Scale:** LB maximizes throughput, minimizes response time, and avoids overload of any single resource
- **Naming abstraction:** name resolution can be delegated to the LB; backends don't need public IP addresses



Public Load Balancer



ORACLE

OCI Compute Services

Agenda



Bare Metal

VMs

Scaling

Container Engine

Functions

OCI Compute Services



Bare Metal

Code
App Container
Language Runtime
Operating System
Virtualization



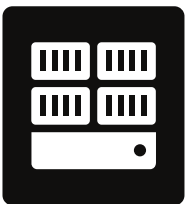
**Dedicated
Virtual Hosts**

Code
App Container
Language Runtime
Operating System



**Virtual
machines**

Code
App Container
Language Runtime
Operating System



**Container
Engine**

Code
App Container



Functions

Code

Bare Metal, VM and Dedicated Hosts

Bare Metal (BM)

Direct Hardware Access –
customers get the full bare
metal server
(single-tenant server)

No VMs

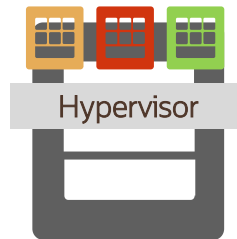


Bare Metal Server

Virtual Machine (VM)

A hypervisor to virtualize the
underlying bare metal server into
smaller VMs
(multi-tenant VMs)

VMs (multi-tenant)

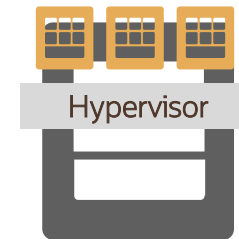


Bare Metal Server

Dedicated VM Hosts (DVH)

Run your VMs instances
on dedicated bare metal
servers (single-tenant VMs)

VMs (single-tenant)



Bare Metal Server

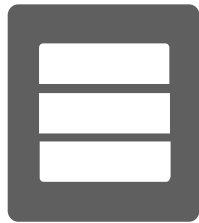
VM compute instances runs on the same hardware as a Bare Metal instances, leveraging the same cloud-optimized hardware, firmware, software stack, and networking infrastructure

Bare Metal use cases

Direct Hardware Access with all the Security, Capabilities, Elasticity and Scalability of OCI



Workloads that are
Performance-intensive



Workloads that are
not virtualized



Workloads that require
a specific hypervisor



Workloads that
require BYO Licensing

VM use cases



Use VMs when you want to control all aspects of an environment

Use VMs when you want to deploy a legacy app running on Windows or Linux

You can use VMs to move applications from on-premises to Oracle Cloud Infrastructure

VMs require work – OS patch management, security configuration, monitoring, application configuration and scaling to handle variable traffic

Instance basics

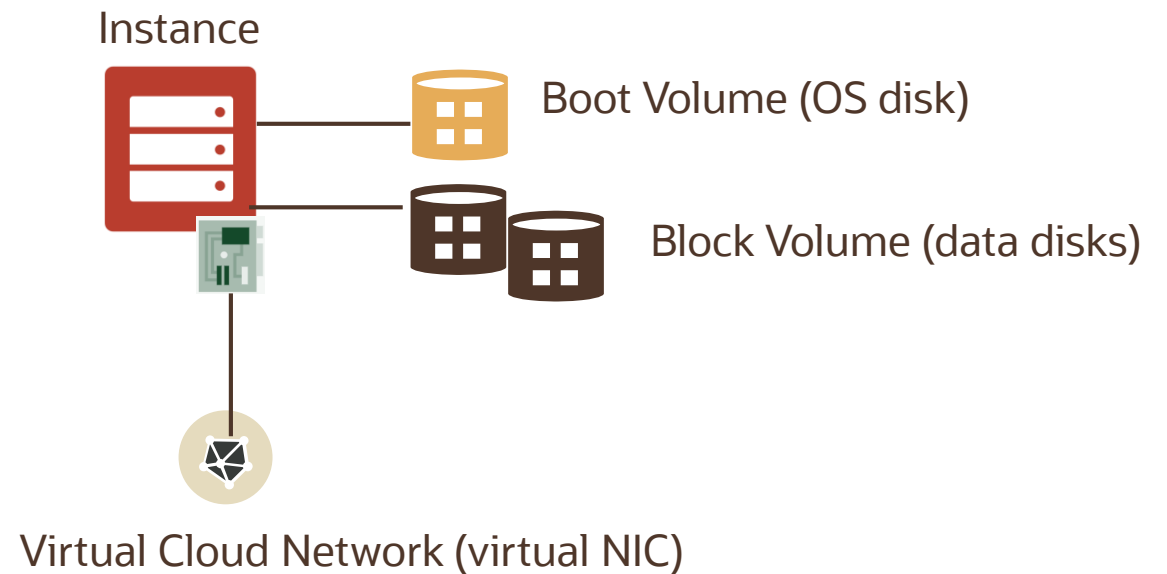
Various instance sizes for every workloads (CPU, RAM, Bandwidth)

Supports both Intel and AMD processors with industry leading price/performance

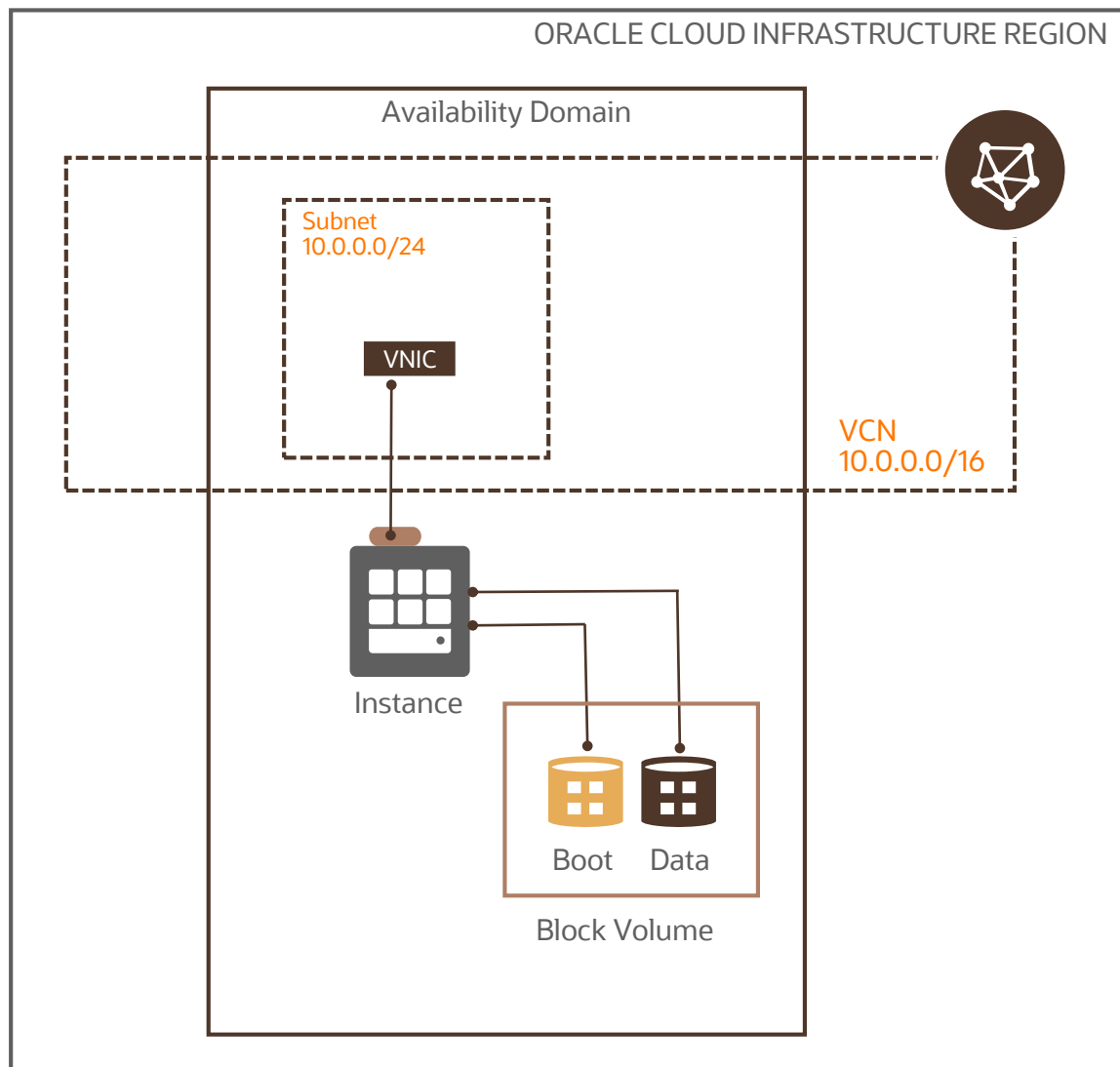
Provide GPU and HPC instance options

Instances are placed on virtual network with powerful connectivity options (incl. on-premises)

Compute instances depend on other OCI services such as Block Volume and VCN



Instance basics



Vertical Scaling

- Scale-up and Scale-down instance shape supported
- New shape must have the same hardware architecture.
- Downtime is required. The instance must be stopped before resize it

Resize Instance

[help](#) [cancel](#)

Change the size of your instance to support changes in application workload.

Current Shape: VM.Standard2.1

!

This instance is running. You must stop the instance before you resize it. [Learn more](#) about resizing instances.

	Shape Name	OCPU	Memory (GB)	Local Disk (TB)	Network Bandwidth	Max Total VNICs
<input checked="" type="checkbox"/>	VM.Standard2.1	1	15	Block Storage only	1 Gbps	2
<input type="checkbox"/>	VM.Standard2.2	2	30	Block Storage only	2 Gbps	2
<input type="checkbox"/>	VM.Standard2.4	4	60	Block Storage only	4.1 Gbps	2
<input type="checkbox"/>	VM.Standard2.8	8	120	Block Storage only	8.2 Gbps	4
<input type="checkbox"/>	VM.Standard2.16	16	240	Block Storage only	16.4 Gbps	8
<input type="checkbox"/>	VM.Standard2.24	24	320	Block Storage only	24.6 Gbps	12

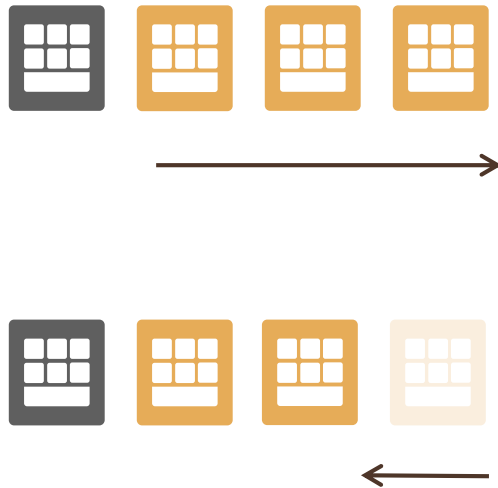
1 Selected

Showing 6 Item(s)

Resize

Cancel

Autoscaling



Enables large scale deployment of VMs from a single gold image with automatic configuration

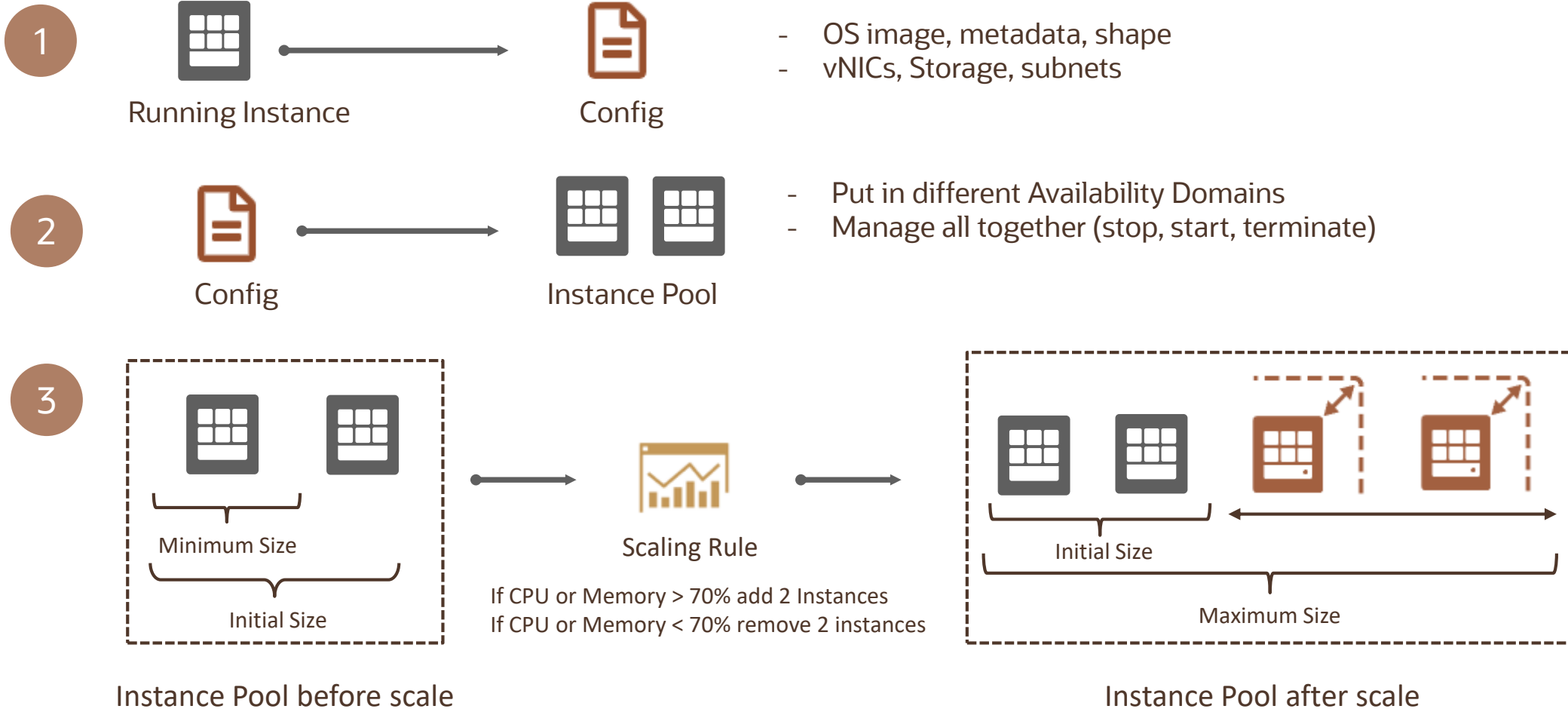
Referred to as scale-out or scale-in

If one VMs fails in the Autoscaling group, others will keep working

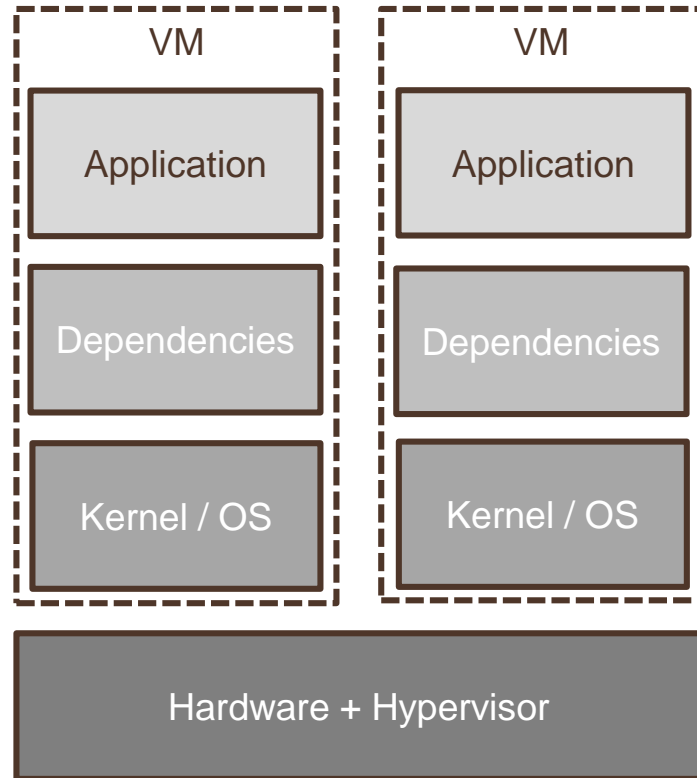
Match traffic demand by adding or removing VMs automatically (supports auto scaling based on metrics – CPU or Memory utilization)

No extra cost for using Autoscaling

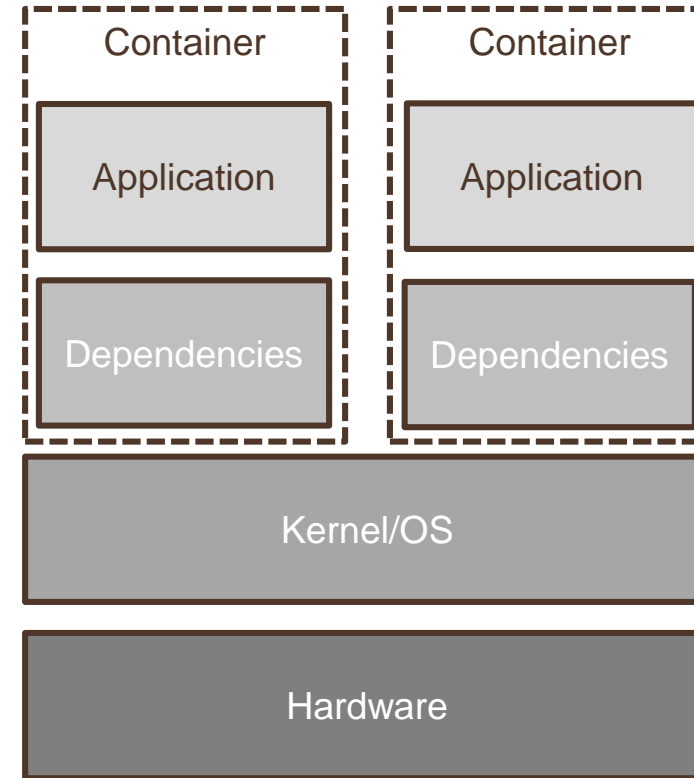
Autoscaling



Containers v/s VMs



Each virtual machine (VM) includes the app, the necessary binaries and libraries and an entire guest operating system



Containers include the app & all of its dependencies, but share the kernel/OS with other containers. Containers are not tied to any specific infrastructure and can run anywhere

How to deploy Containers?

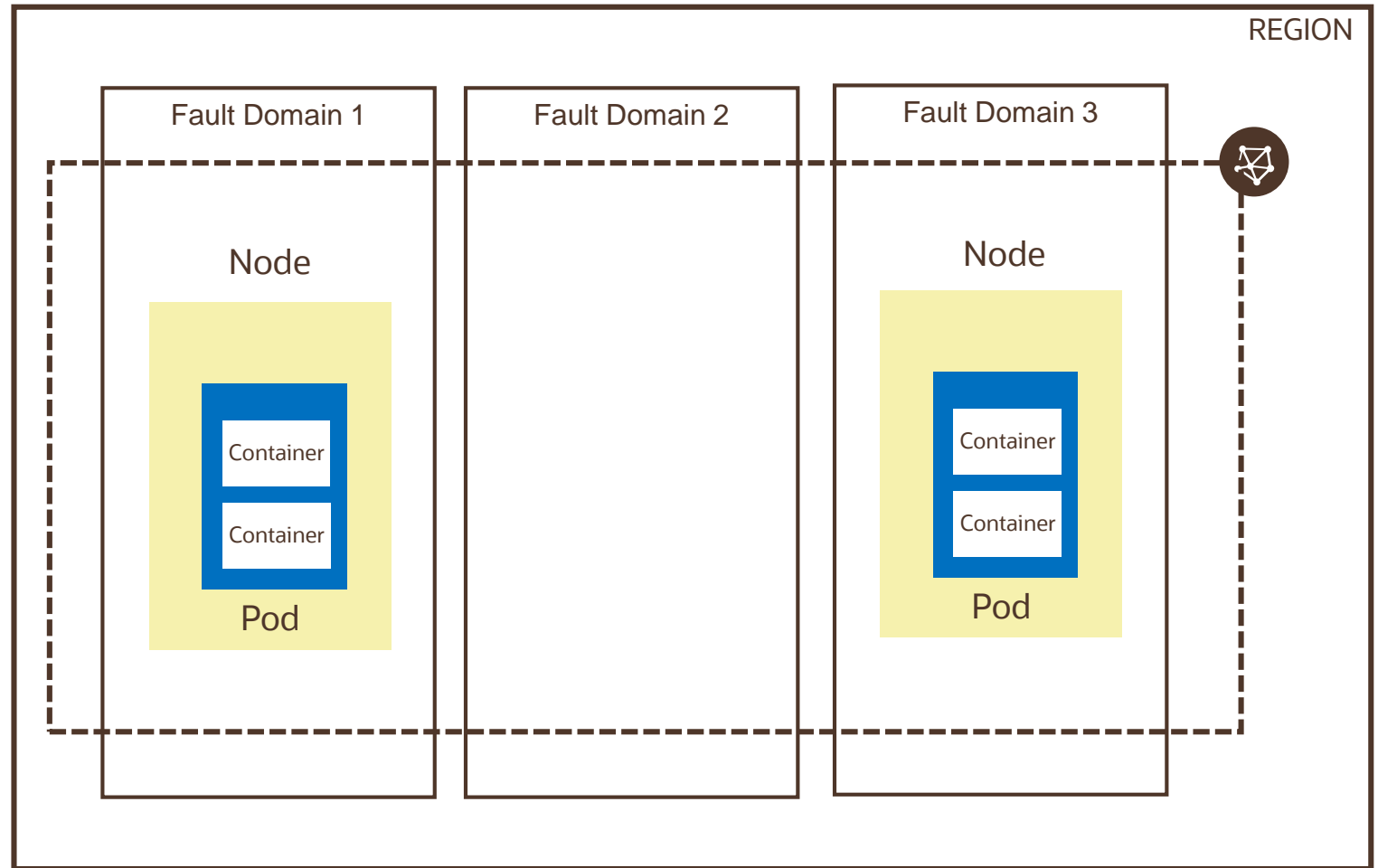
- Manually SSH into machines and run Docker
 - Pro: Simple and easily understood
 - Con: Not automated, no reproducible, doesn't scale, doesn't self heal
- Scripting or config management tools
 - Pro: Integrates with existing environments, easily understood
 - Con: Doesn't scale, doesn't self heal, no scheduling mechanism
- Orchestration Systems
 - Pro: Automated, reproducible, self healing, scalable
 - Con: additional tooling and training required, some overhead

Oracle Kubernetes Engine

Kubernetes is an open source system for automating deployment, scaling and management of containerized applications

OKE is a fully-managed, scalable, and highly available service that you can use to deploy your containerized applications in OCI

OCIR is a managed Docker container registry service and can be used to pull images for k8s deployments



Functions

In Oracle Functions, functions are:

- small but powerful blocks of code that generally do one simple thing
- stored as Docker images in a specified Docker registry
- invoked in response to a CLI command or signed HTTP request



Push container
to registry



Configure function
trigger



Code runs only
when triggered



Pay for code
execution time only



ORACLE

The background features several abstract, organic shapes. On the left, a large, dark brown, textured shape resembling a cloud or a stylized 'O' is positioned. On the right, there are two smaller, more fluid shapes: a light blue one and a red one, both with a fine, concentric-line texture. Scattered throughout the background are small, horizontal orange and yellow dashes and lines, some of which are grouped together.

OCI Storage Services

Agenda



Block Volume
Local NVMe
File Storage
Object Storage
Archive Storage

Storage Requirements

Persistent v/s non-persistent?

What type of data?

Database, videos, audio, photos, text

Performance?

Max capacity, IOPS, throughput

Durability?

of copies of data

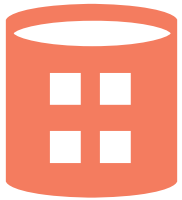
Connectivity?

Local v/s network, how does app access the data

Protocol

Block v/s File v/s HTTPs

OCI Storage Services



Block
Volume



Local
NVMe



File
Storage



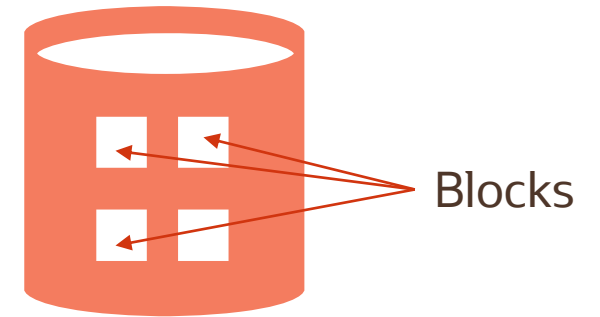
Object
Storage



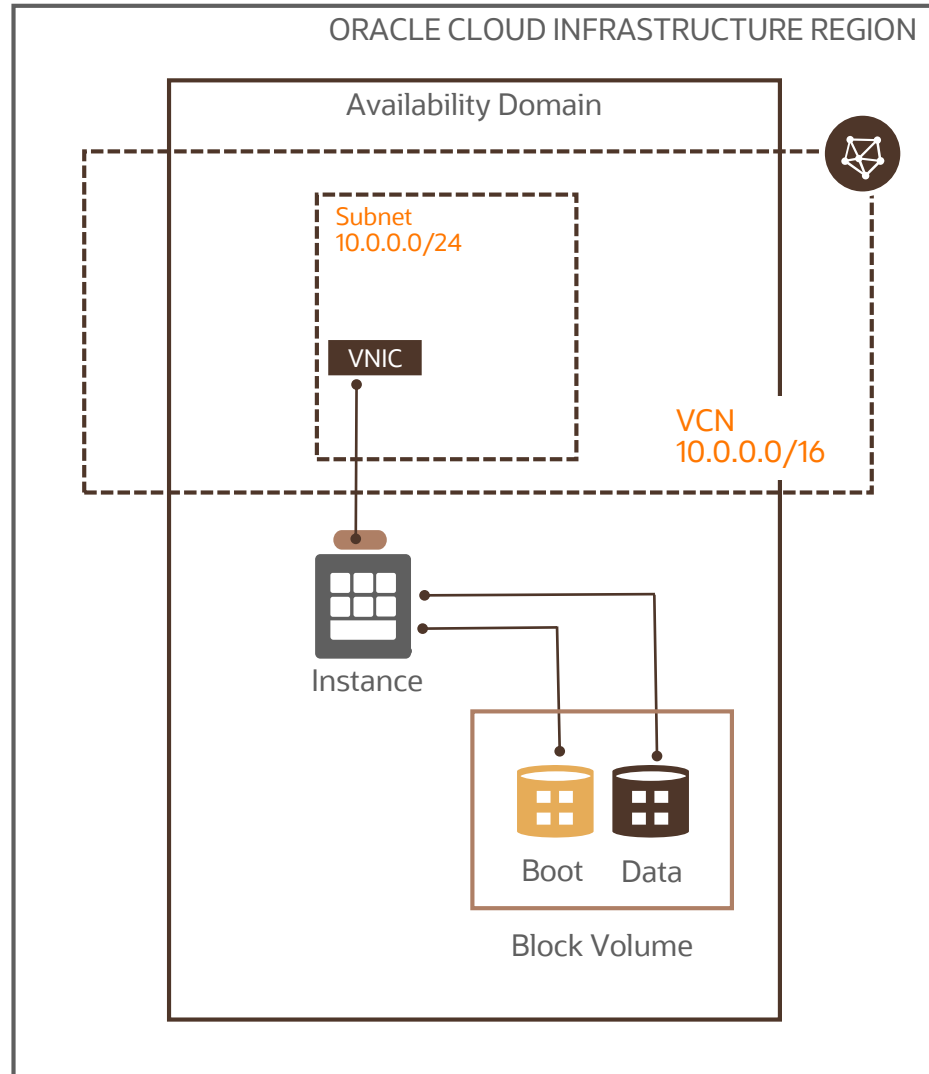
Archive
Storage

What is Block Storage?

- Hard drive in a server except the hard drive happens to be installed in a remote chassis
- Data is typically stored on device in fixed sized blocks (e.g. 512 Bytes)
- Accessed by operating system as mounted drive volume
- Applications/file systems decide how blocks are combined and accessed
- Data is stored without any higher-level metadata e.g. for data format, type or ownership
- You can place any kind of file system on block level storage. E.g., Windows uses NTFS; VMware uses VMFS
- Commonly deployed in Storage Area Network (SAN) storage



Block Volume Service

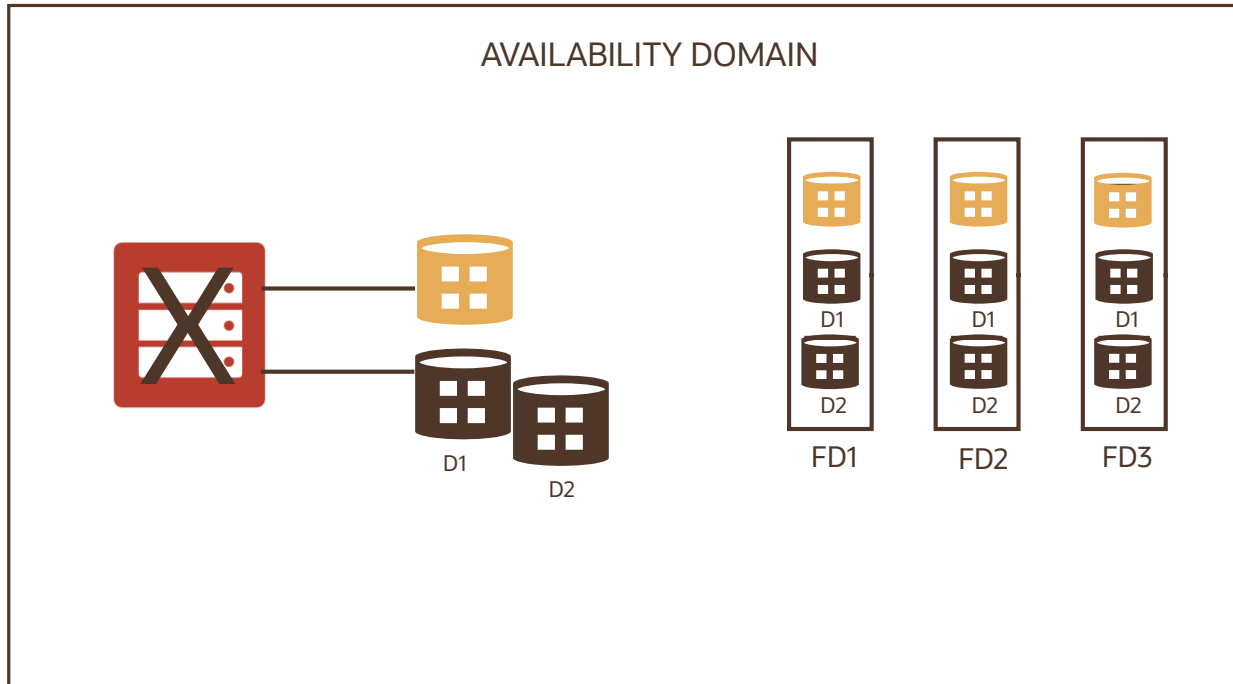


- Storage for compute instances
- 2 types: Boot Volume (OS disk), Block Volume (data disks)
- Service lets you store data independently and beyond the lifespan of compute instances

Use cases:

- Databases
- Exchange (supports block level storage only)
- VMware (common to deploy VMware servers that use shared VMFS volumes on block level storage)
- Server boot (in public clouds, instances are configured to boot from block level storage)

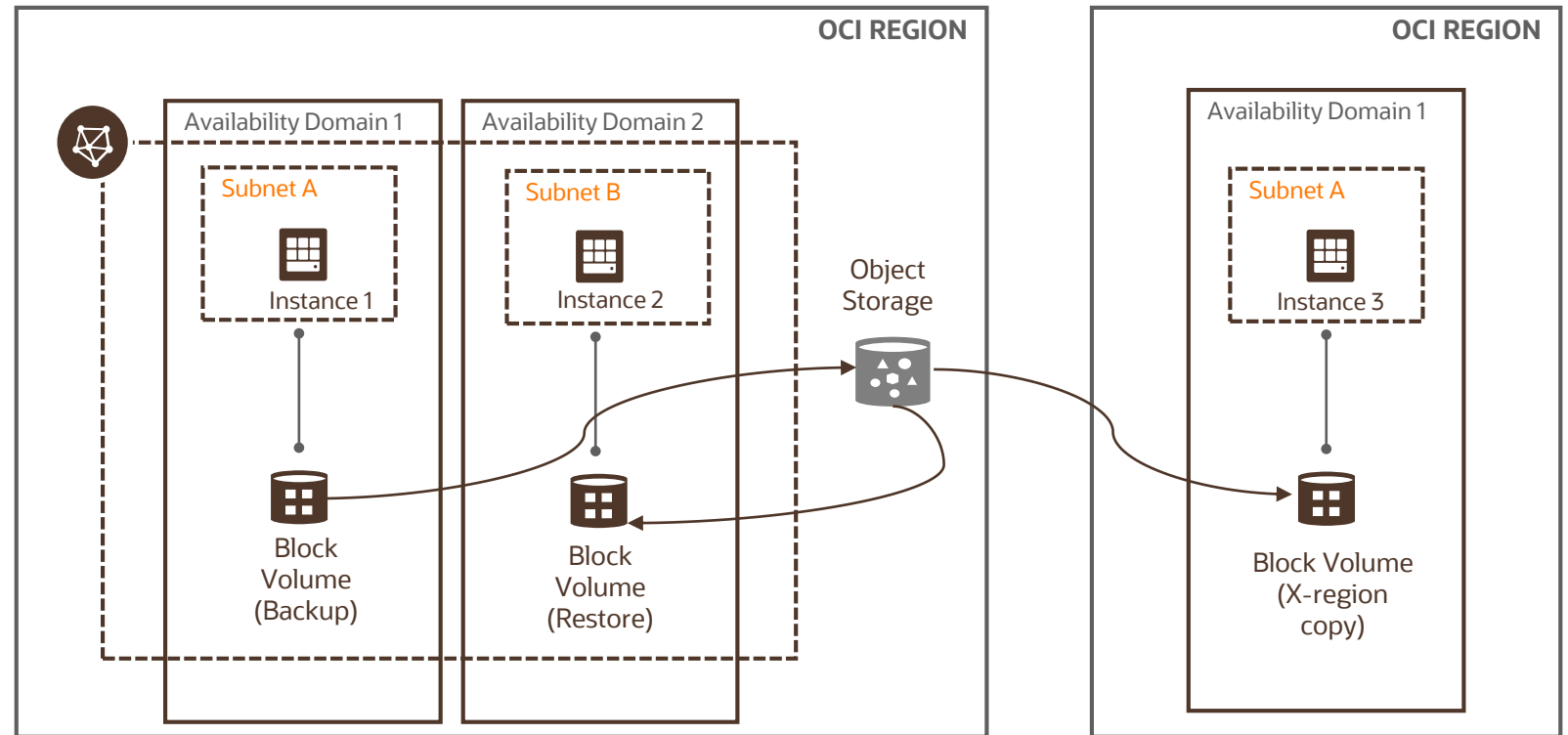
Block Volume – highly durable



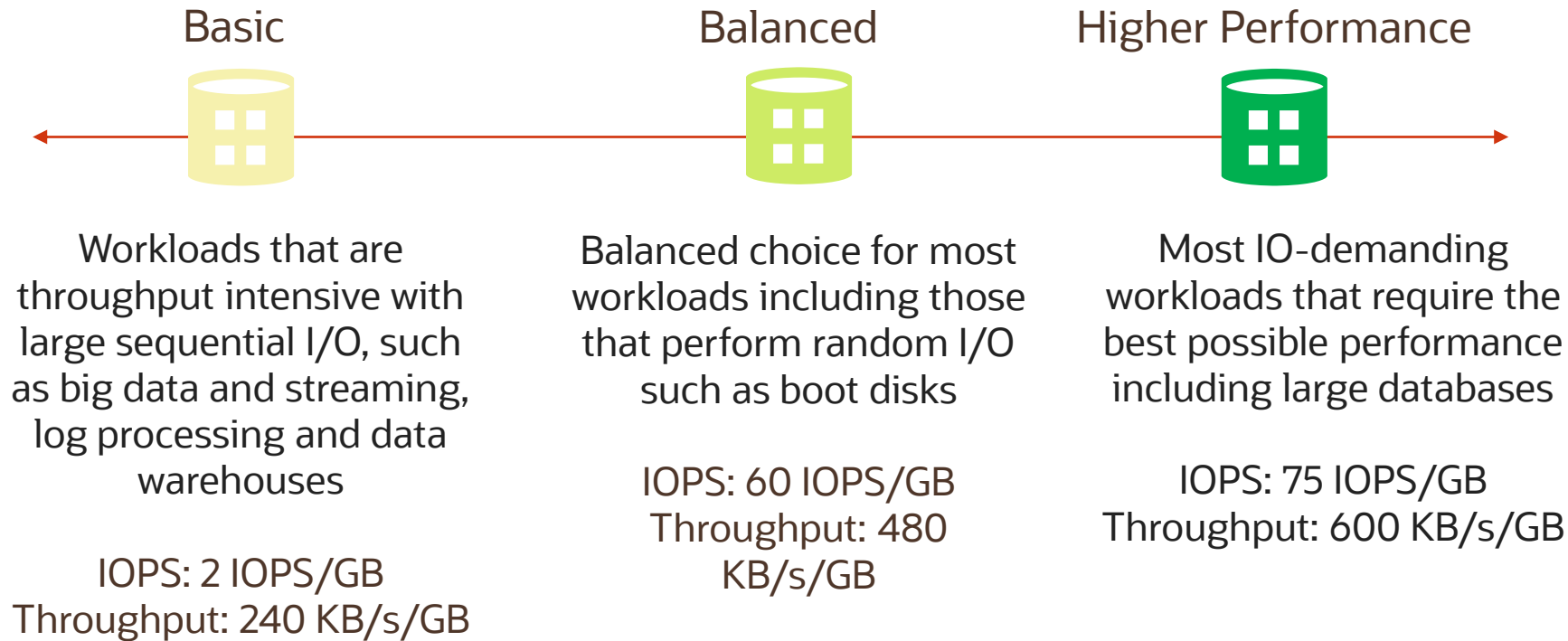
- Storage is highly durable and persistent
- Block Volume stores replica of data in 3 separate Fault Domains
- You don't need to configure any software based protection (RAID-10 etc.)
- To minimize loss of data due to deletes or corruption, we recommend to take periodic backups of block volumes. OCI allows automated scheduled backups

Block Volume Backup

- Complete point-in-time snapshot copy of your block volumes
- Encrypted and stored in the Object Storage, and can be restored as new volumes to any AD within the same region (for multi-AD regions)
- Can copy block volume backups from one-region to another
- Backups can be scheduled



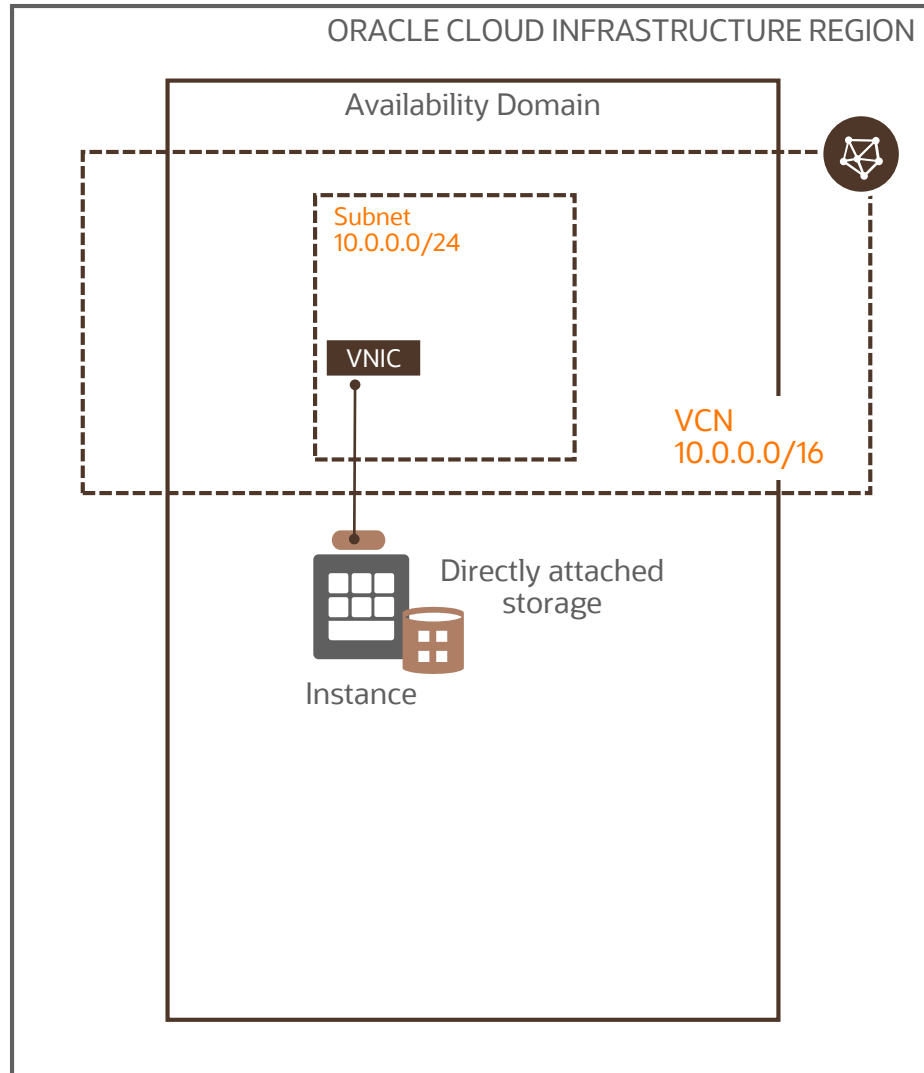
Block Volume Tiers



Volumes can be 50 GB - 32 TB in size; you can attach up to 32 volumes/instance.

Data encrypted at rest and in-transit (oracle managed) or customer managed keys

Local NVMe



- Temporary NVMe based storage locally attached to the compute instances
- Designed for applications that require high-performance local storage
- Use cases:
 - NoSQL databases (e.g. Cassandra, MongoDB, Redis),
 - in-memory databases,
 - Scale-out transactional databases,
 - Data warehousing
- Storage is non-persistent (survives reboot)



Local NVMe



OCI uses NVMe (Non-Volatile Memory Express) interface for very high performance

OCI provides no RAID, snapshots, backups capabilities for these devices and customers are responsible for data durability

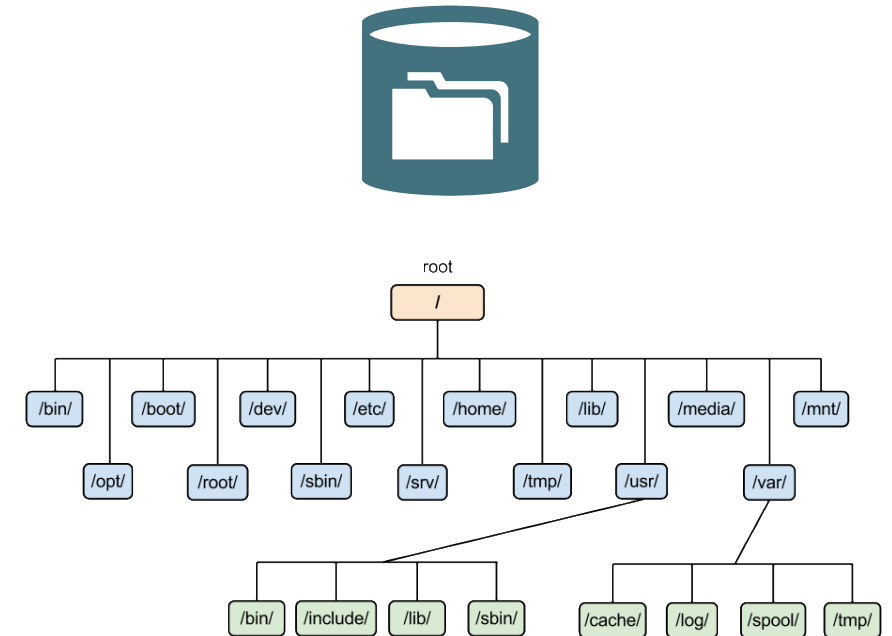
Block based Protocol (like Block Volume)

SLA around Performance

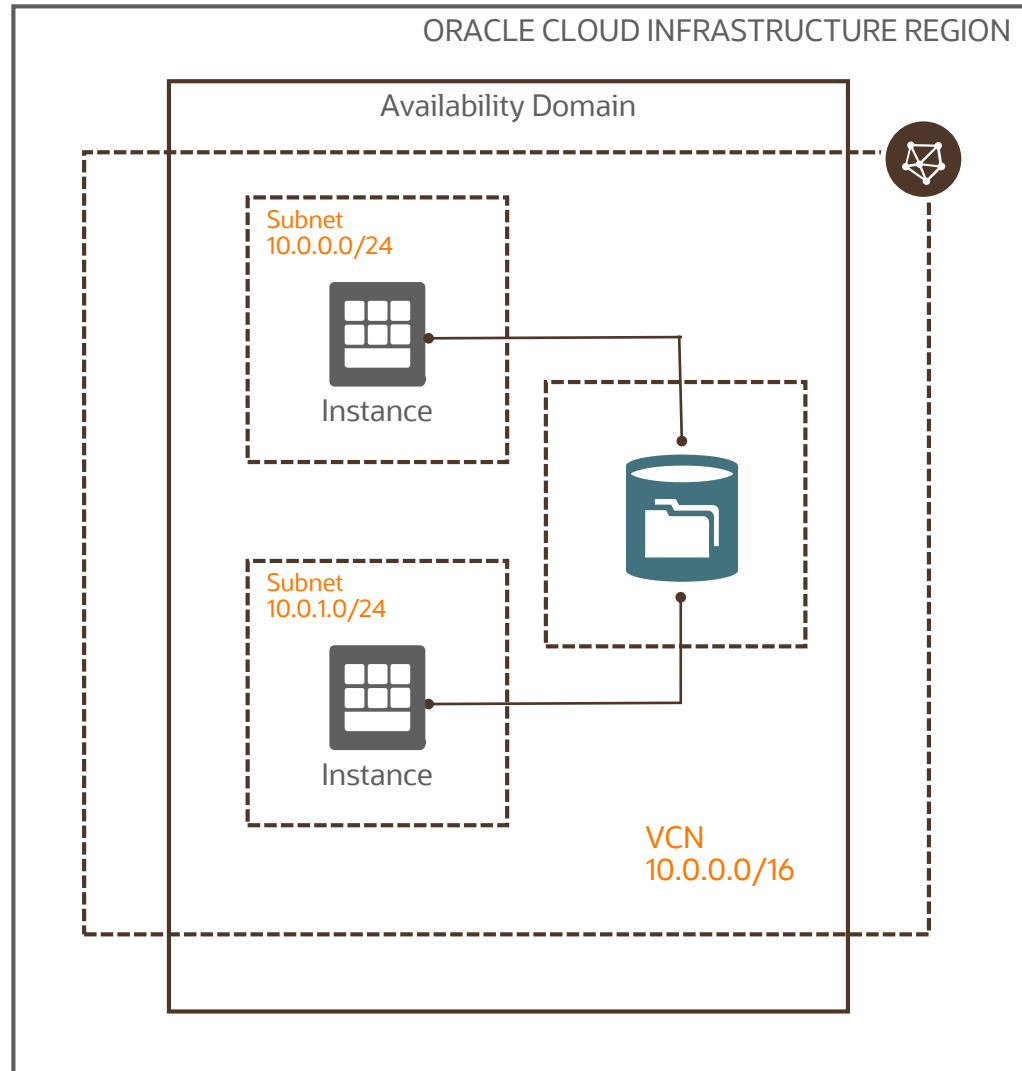
Instance type	NVMe SSD Devices	IOPS
BM.DenseIO2.52	8 drives = 51.2 TB raw	250k
VM.DenseIO2.8	2 drive = 6.4 TB raw	400k
VM.DenseIO2.16	4 drives = 12.8 TB raw	800k
VM.DenseIO2.24	8 drives = 25.6 TB raw	3.0MM

What is File Storage?

- Hierarchical collection of documents organized into named directories which are themselves structured files
- Distributed file systems make distributed look exactly like local file systems
- Distributed file standards – NFS and SMB
 - Supported by Unix and Windows
 - Allow creation, deletion, reading, writing, sharing and locking
 - Supported by all major OSes and hypervisors
 - (typically) no extra client software needed
 - Provide access over networks

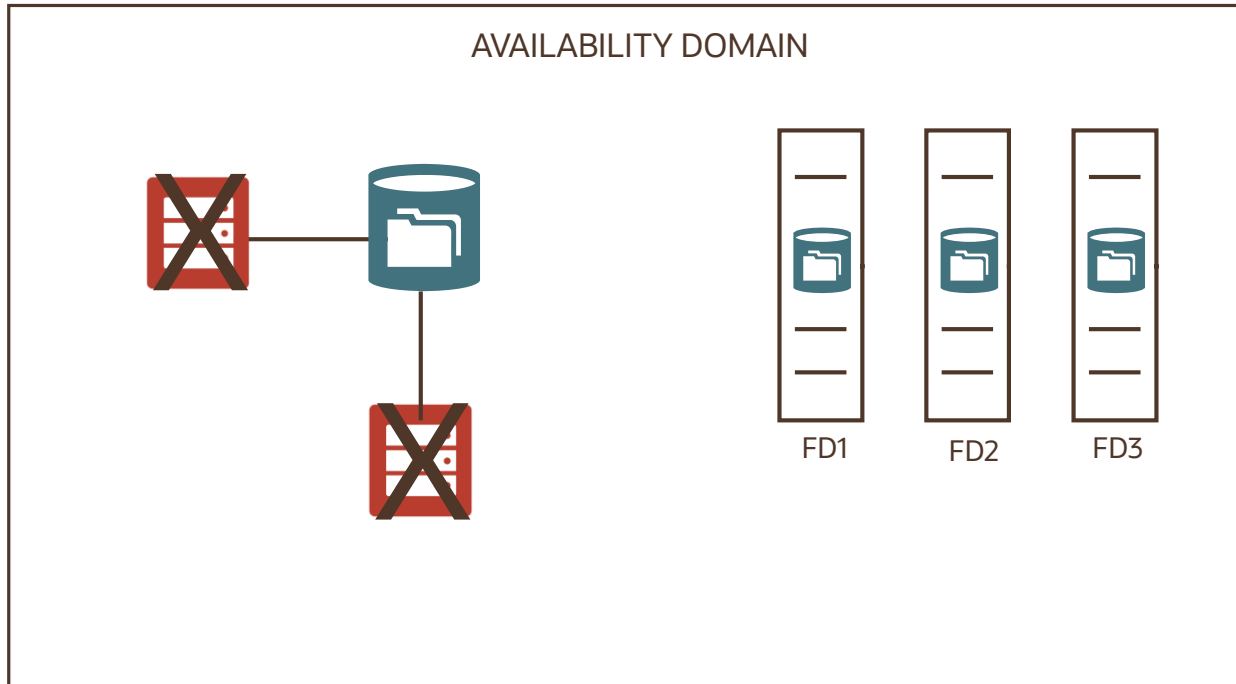


File Storage Service (FSS)



- Shared file system storage for compute instances
- Supports NFS v.3 distributed file system
- Data protection: Snapshots (10,000 snapshots per file system)
- Security: data-at-rest and in-transit encryption for all file systems & metadata
- Use cases:
 - Oracle Applications (e.g. EBS)
 - HPC
 - Big Data and Analytics
 - General purpose File systems

File Storage – highly durable



Storage is highly durable and persistent

File Storage stores replica of data in 3 separate Fault Domains

You can take snapshots of file systems that provide a read-only, space efficient, point-in-time backup of a file system

You can restore a file within the snapshot, or an entire snapshot using the `cp` or `rsync` command

What is Object Storage?

- All data, regardless of content type, is managed as objects
- Each object is stored in a bucket. A bucket is a logical container for storing objects
- Objects are stored in a single, flat structure without a folder hierarchy. This means that accessing individual objects is fast and easy
- Each Object is composed of object itself and metadata of the object. This makes it easier to index and access data
- Object storage is quite common in cloud-based storage scenarios with very high scalability and reliability
- While files and blocks are generally available to an operating system (by mount operation), object storage relies on standard HTTP verbs



Object Storage Service



An internet-scale, high-performance storage platform

Ideal for storing unlimited amount of unstructured data (images, media files, logs, backups)

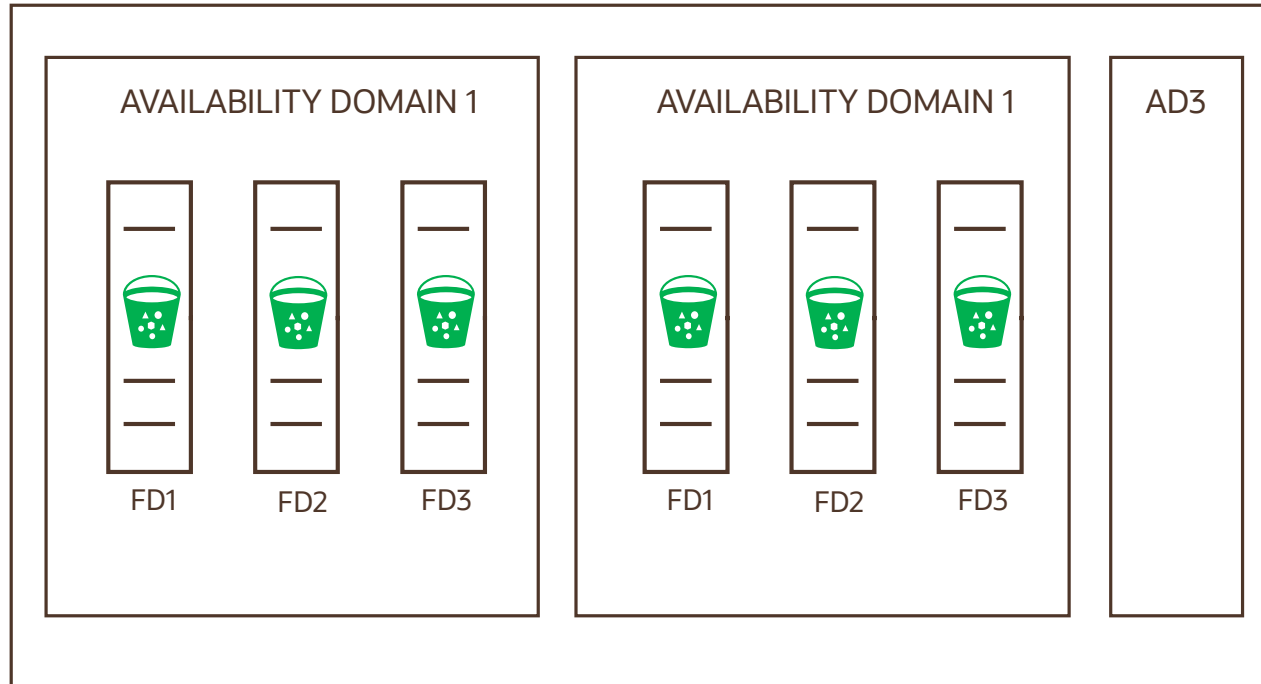
Regional service, not tied to any specific compute instance

Offers two distinct storage classes "hot" storage (standard), "cold" storage (Archive)

Use cases

- Content repository for data, images, logs, and video etc.
- Archive/Backup for longer periods of time
- Storing log data for analysis and debugs/troubleshooting
- Storing large data sets (genome data, IoT)
- Big Data/Hadoop storage

Object Storage – highly durable



Storage is highly durable and persistent

Object storage stores replica of data in 3 separate Fault Domains in an AD

In a multi-AD region, it stores replica of data in more than one AD

Data integrity is actively monitored and corrupt data detected and auto repaired

You can leverage cross-region copy for disaster recovery scenarios

Object Storage Tiers

Standard Storage Tier (Hot)

- Fast, immediate, and frequent access
- Data retrieval is instantaneous
- Always serves the most recent copy of the data when retrieved
- Standard buckets can't be downgraded to archive storage

Archive Storage Tier (Cold)

- Seldom or rarely accessed data but must be retained and preserved for long periods of time
- 10X cheaper than Standard Tier (\$0.0026 v/s \$0.0255 Gb/month)
- 90 days minimum retention requirement
- Objects need to be restored before download; Time To First Byte (TTFB) after restore request is made: 4 Hours
- Archive Bucket can't be upgraded to Standard storage tier

Create Bucket

[help](#) [cancel](#)

Specify the storage tier for this bucket. Storage tier for a bucket can only be specified during creation.

BUCKET NAME

ObjectStorageBucketName

STORAGE TIER

☒ STANDARD

☐ ARCHIVE

Create Bucket

OCI Storage Services

	Local NVMe	Block Volume	File Storage	Object Storage	Archive Storage
Type	NVMe SSD based temporary storage	NVMe SSD based block storage	NFSv3 compatible file system	Highly durable Object storage	Long-term archival & backup
Access	Block	Block	File	Object	Object
Structure	Block level structured	Block level structured	Hierarchical	Unstructured	Unstructured
Durability	Non-persistent; survives reboots	Durable (multiple copies in an AD)	Durable (multiple copies in an AD)	Multiple copies across ADs*	Multiple copies across ADs*
Capacity	Terabytes+	Petabytes+	Exabytes+	Petabytes+	Petabytes+
Unit Size	51.2 TB for BM, 6.4-25.6 TB for VM	50 GB to 32 TB/vol 32 vols/instance	Up to 8 Exabyte	10 TB/object	10 TB/object
Use cases	OLTP, NoSQL, Data warehousing	Database, VMFS, NTFS, boot and data disks for instances	Oracle apps (EBS), HPC, general purpose file systems	Unstructured data incl. logs, images, videos	Backups and long term archival (DB backups)

* in multi-AD regions

ORACLE

OCI Database Services

Agenda

OCI DB Options

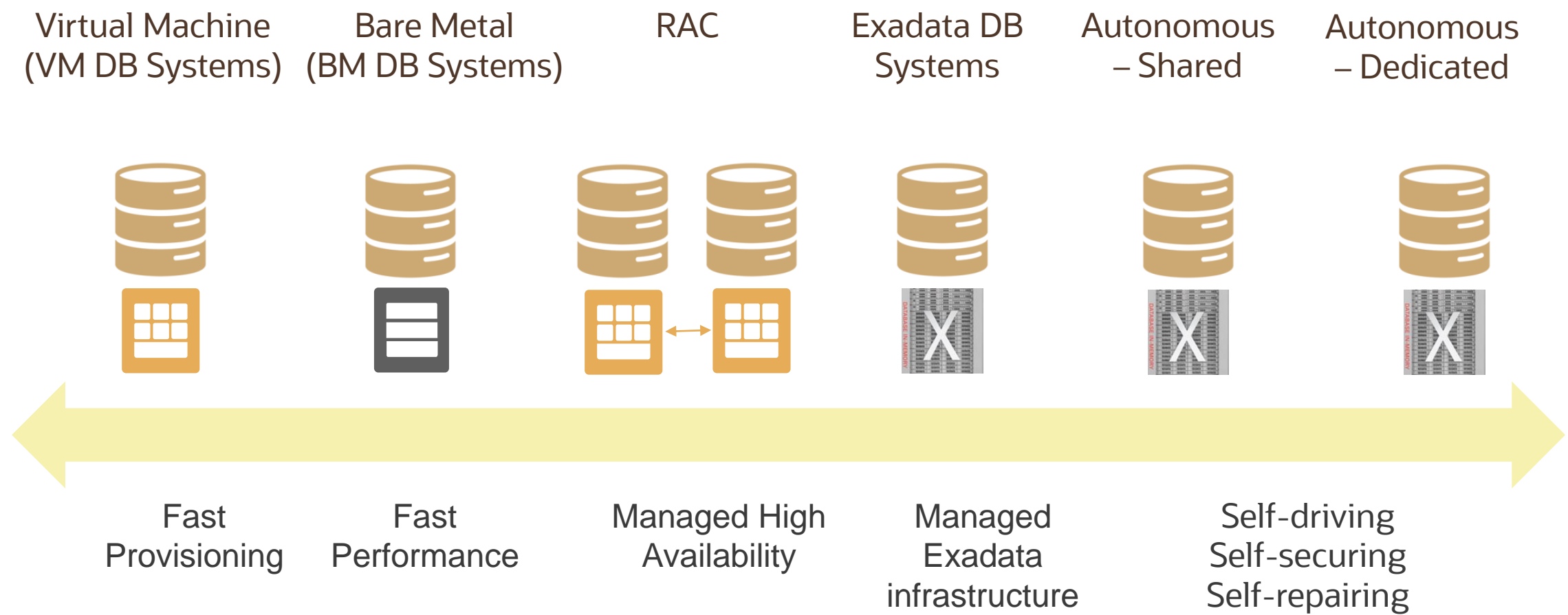
DB Systems

DB Systems Backup

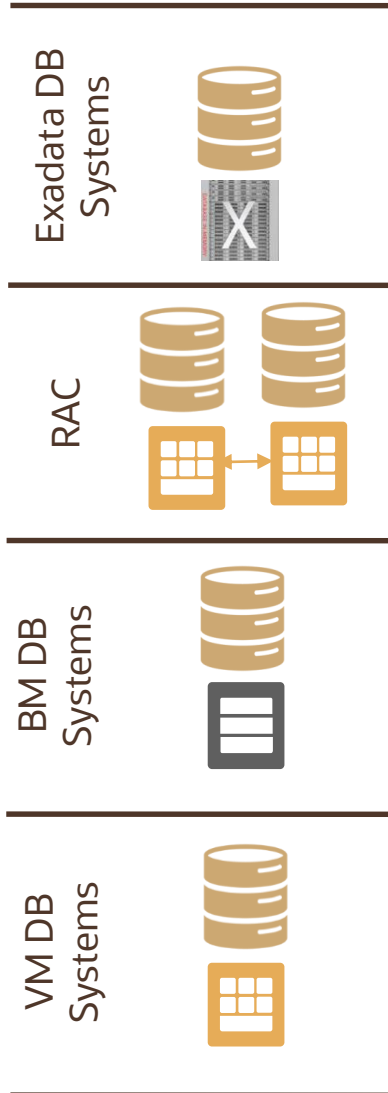
DB Systems HA and DR

Autonomous Databases

OCI Database options



DB Systems



Managed DB Systems – Exadata, RAC, Bare Metal, VM

Complete lifecycle automation – Provisioning, Patching, Backup & Restore

High Availability and DR – RAC & Data Guard

Scalability – Dynamic CPU and Storage scaling

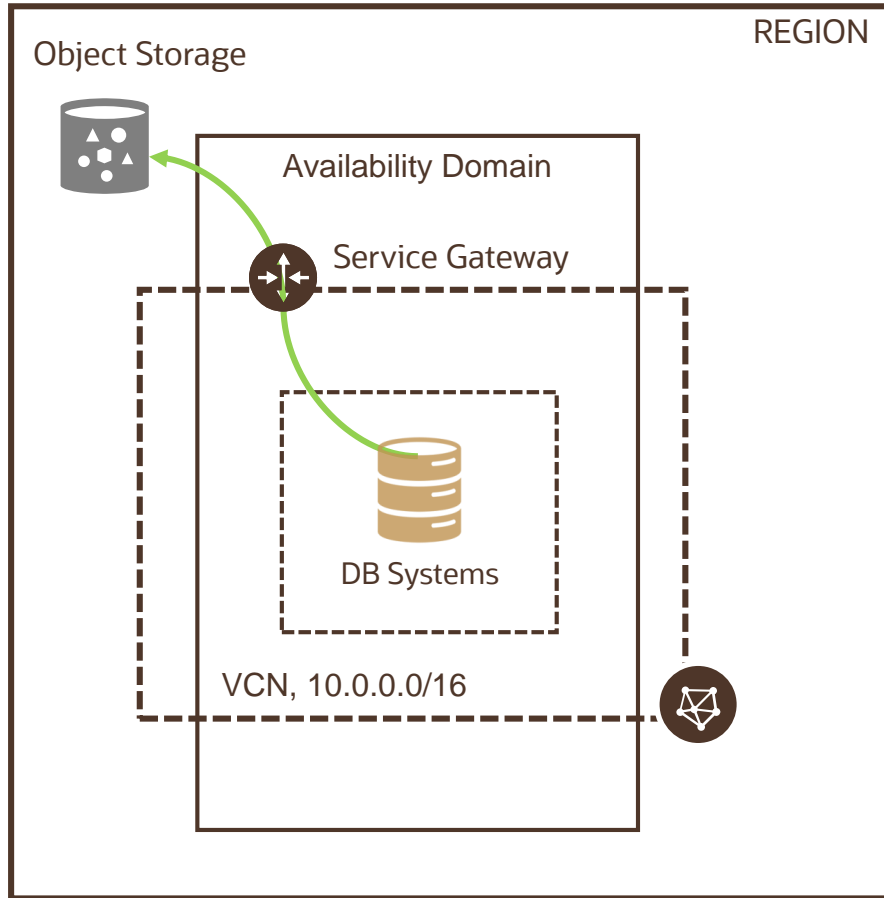
Security – Infrastructure (IAM, VCN, Audit), Database (TDE, Encrypted RMAN backup / Block volume encryption)

Bring Your Own License (BYOL)

DB Systems Operations

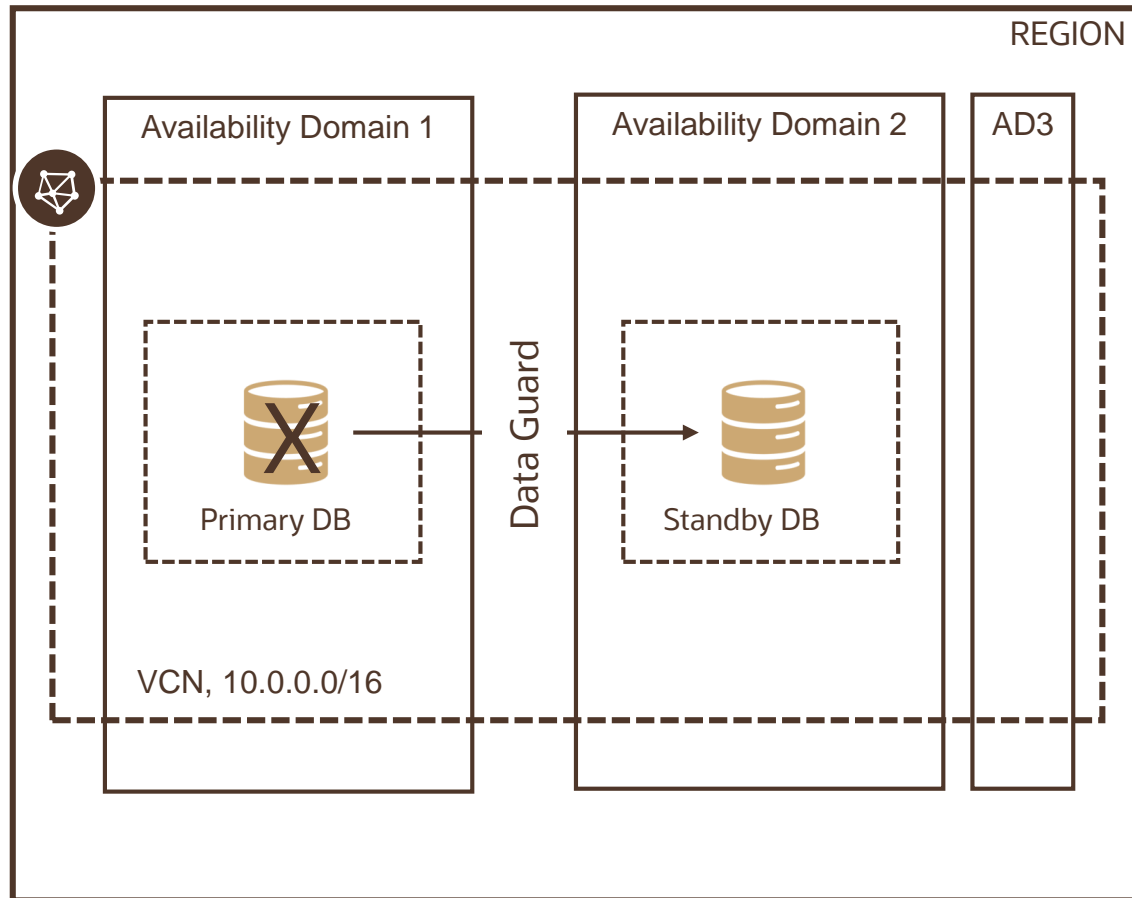
- Launch, start, stop, or reboot DB Systems
 - Billing continues in stop state for BM DB Systems (but not for VM DB)
- Scale
 - CPU cores – scale up the number CPU cores (BM DB systems only)
 - Storage – increase the amount of block storage with no impact (VM DB systems only)
- Patch
 - 2 step process – DB System patched first before the database is patched
 - For Exadata and RAC shapes, patches are rolling

DB Systems Backup/restore



- Manual or Automatic backups
- Automatic backups written to Oracle owned object storage buckets (customers cannot view the backups)
- Backups run between midnight – 6:00 AM in the DB system's time zone (optionally, specify a 2 hr. window)
- Preset retention periods : 7, 15, 30, 45 and 60 days
- Recover a database from a backup stored in Object Storage
 - To last known good state with least possible data loss
 - Using the timestamp specified
 - Using the SCN specified

DB Systems DR



Oracle Data Guard provides a set of services that create, maintain, manage, and monitor one or more standby databases to enable Oracle databases to survive disasters and data corruptions. It maintains synchronization between the primary and the standby db

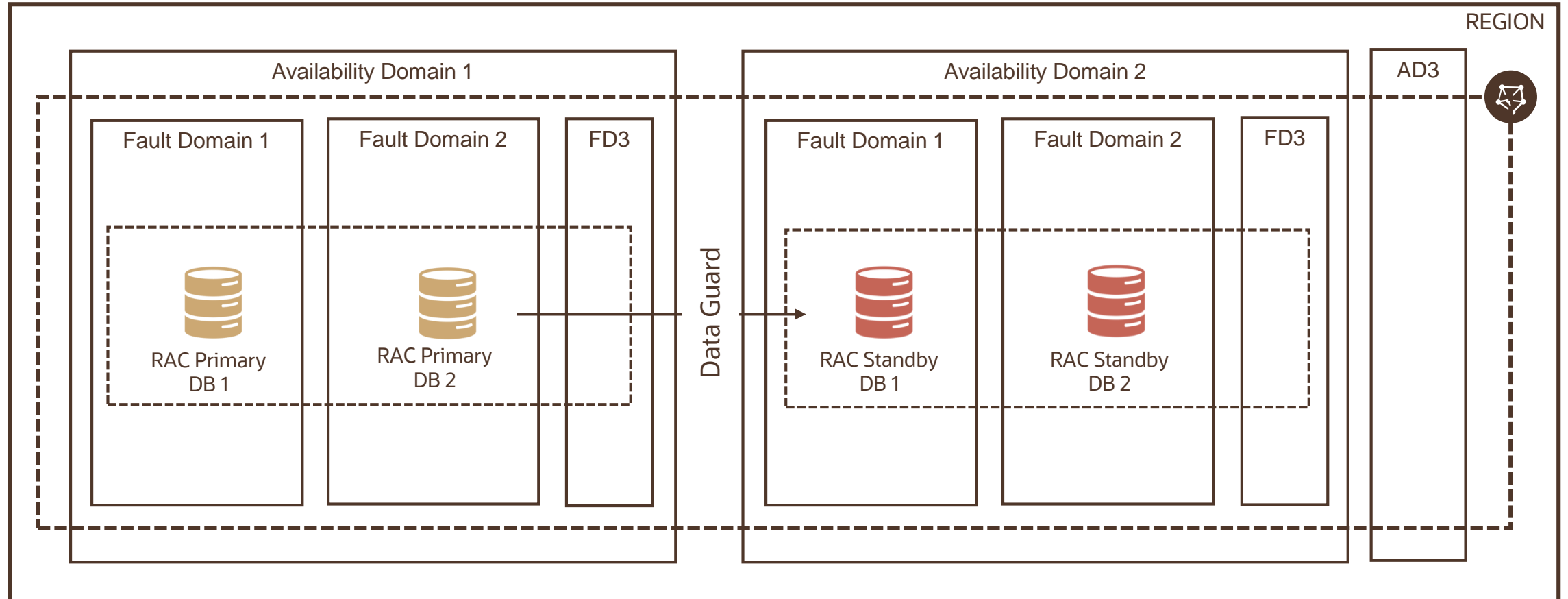
Active Data Guard extends Data Guard by providing advanced features for data protection and availability. It is included in the Extreme Performance Edition and Exadata Service.

Two modes – switchover and failover

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

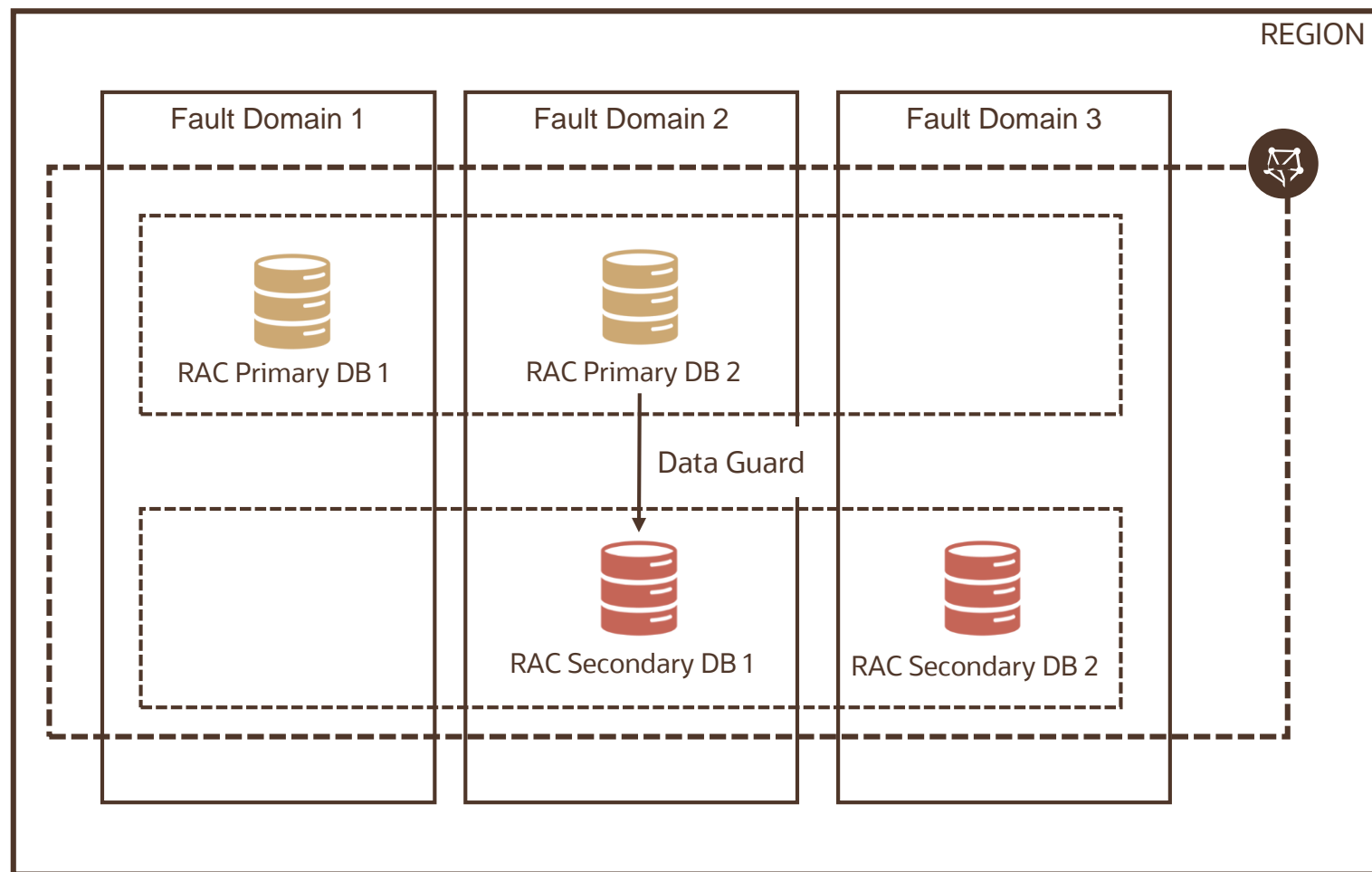
DB Systems HA and DR (Multi AD region)

Primary and standby databases can be either a single-instance Oracle database or a RAC database



DB Systems HA and DR (single AD region)

Primary and standby databases can be either a single-instance Oracle database or a RAC database



- If your primary and standby databases are 2-node RAC databases
- and both are in the same AD
- only one of the two nodes of the standby database can be in a fault domain that does not include any other nodes from either the primary or standby database.

Autonomous Database

Autonomous
- Shared



Autonomous
- Dedicated



Fully managed database with 2 workload types

- Autonomous Transaction Processing
- Autonomous Data Warehouse

Deployment options

- Dedicated: you have exclusive use of the Exadata hardware. Supported for both ATP and ADW.
- Shared: you provision and manage only the Autonomous DB, while Oracle handles Exadata infrastructure deployment and management. Supported for both ATP and ADW.

Automates the following tasks

- Backing up the database
- Patching the database (incl. maintenance w/o downtime)
- Upgrading the database
- Tuning the database

DB services

	VM DB Systems	BM DB Systems	Exadata DB Systems	Autonomous – Shared	Autonomous - Dedicated
Management	Customer	Customer	Customer	Oracle	Oracle
Updates	Customer initiated	Customer initiated	Customer initiated	Automatic	Customer policy control
Scaling	Storage (CPU cores cannot be changed)	CPU (storage cannot be changed)	Within Exa CPU, across Exa racks	Both CPU and Storage	Both CPU and Storage
Backups	Customer initiated	Customer initiated	Customer initiated	Automated	Automated
Storage	Block Storage	Local NVMe disks	Local disks and NVMe flash cards	Local disks and NVMe flash cards	Local disks and NVMe flash cards
RAC	Available (2-node)	Not Available	Available	Not Available	Not Available
Data Guard	Available	Available	Available*	Not Available	Not 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

**The database can be a container database with multiple pluggable databases, if the edition is High Performance or Extreme Performance.





Oracle Cloud always free tier:

oracle.com/cloud/free/

OCI training and certification:

cloud.oracle.com/en_US/iaas/training

cloud.oracle.com/en_US/iaas/training/certification

education.oracle.com/oracle-certification-path/pFamily_647

OCI hands-on labs:

ocitraining.cloudable.com/provider/oracle

Oracle learning library videos on YouTube:

youtube.com/user/OracleLearning



ORACLE

OCI Identity and Access Management

Agenda

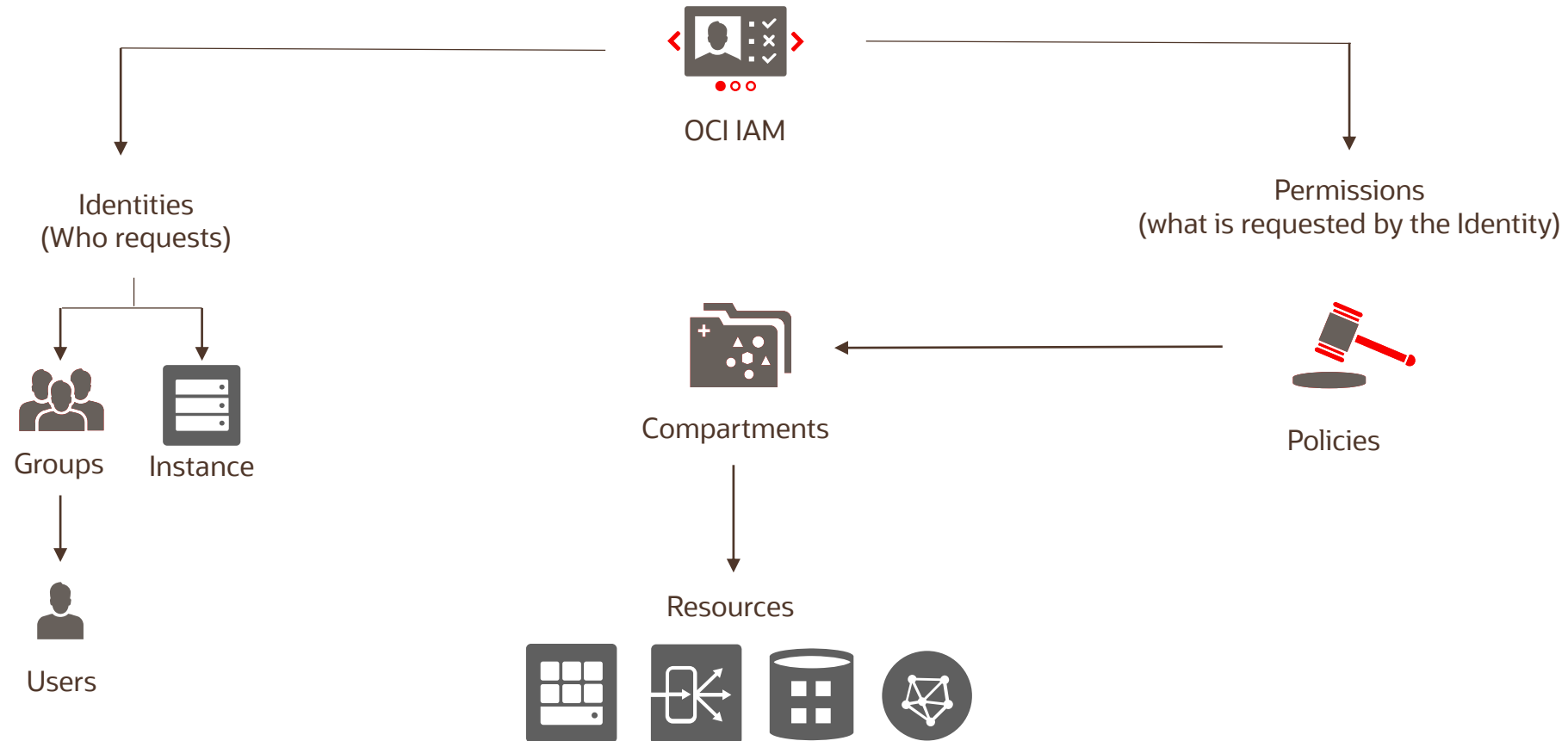
IAM

Authentication

Authorization

Policies

Identity and Access Management

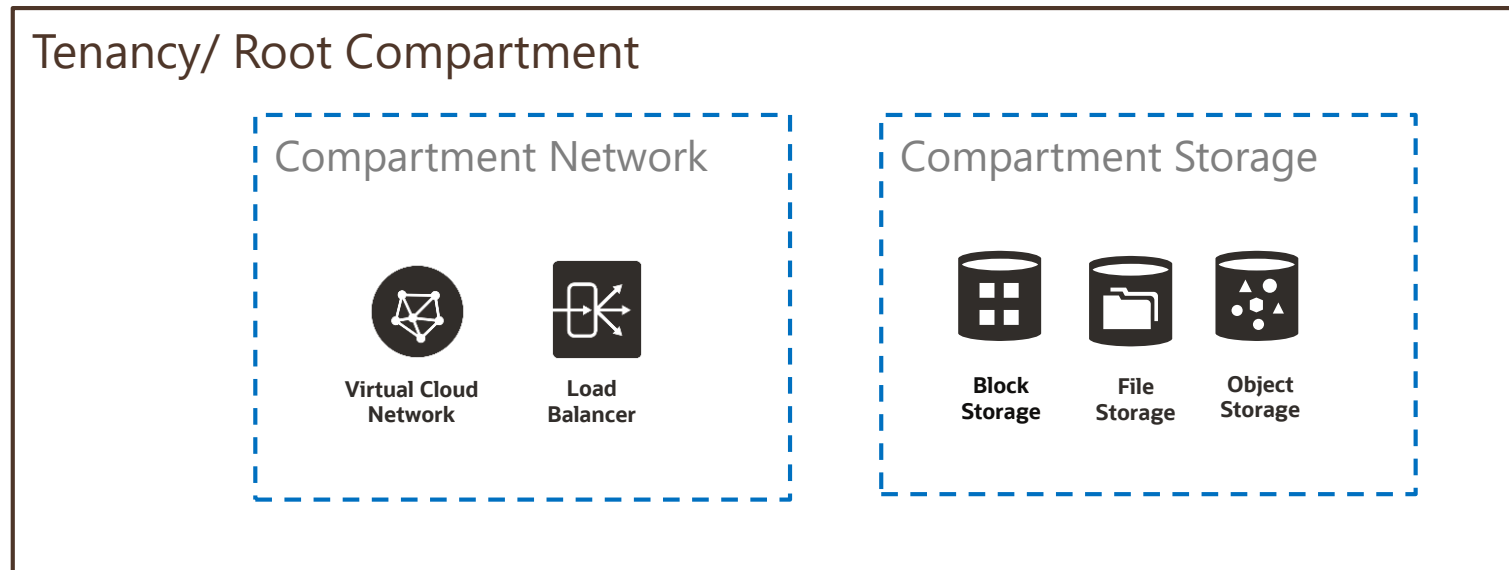


Principals

- A principal is an IAM entity that is allowed to interact with OCI resources
- Principals – IAM users and Instance Principals
- **IAM Users and Groups**
 - Users = individual people or applications
 - First IAM user = default administrator; admin sets up other IAM users and groups
 - Users enforce security principle of least privilege
 1. Users → Groups
 2. Group → at least one policy with permission to tenancy or a compartment
- **Instance Principals**
 - Instance Principals lets instances (and applications) to make API calls against other OCI services removing the need to configure user credentials or a configuration file

Compartment

A compartment is a collection of related resources. It helps you isolate and control access to your resources



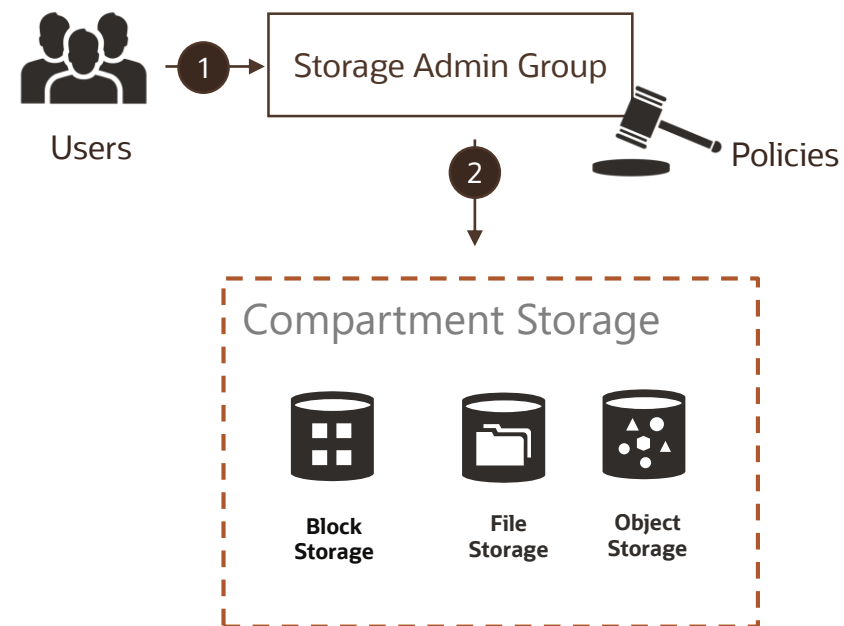
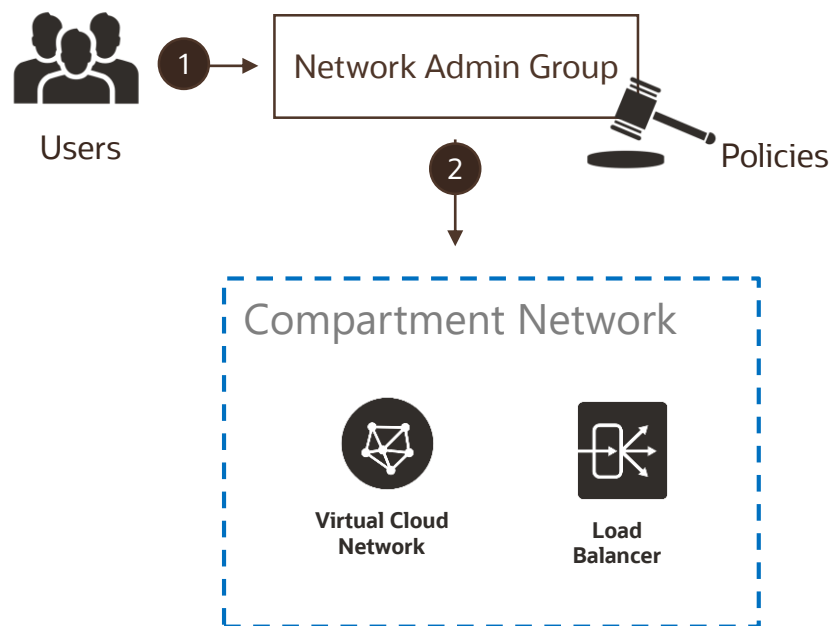
Root Compartment can hold all the cloud resources. Best practice is to create dedicated compartments when you need to isolate resources

Each resource belongs to a single compartment

Resources can interact with other resources in different compartments

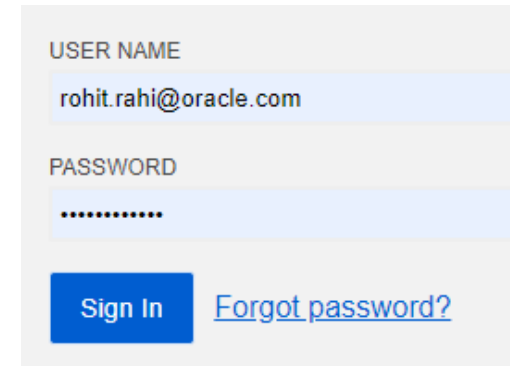
You can give group of users access to compartments by writing Policies

Tenancy/ Root Compartment



Authentication

- Authentication deals with user identity: who is this person? Is this who he says he is?
- OCI IAM service authenticates a Principal by –
 - User name, Password
 - API Signing Key
 - Required when using the OCI API in conjunction with the SDK/CLI
 - Auth Tokens
 - Oracle-generated token strings to authenticate with 3rd party APIs that do not support OCI signature-based authentication (e.g. ADW)



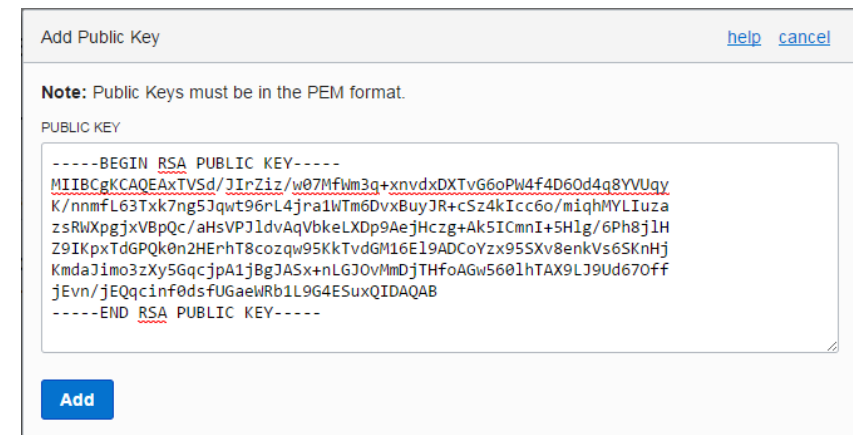
USER NAME

rohit.rahi@oracle.com

PASSWORD

.....

[Sign In](#) [Forgot password?](#)



Add Public Key [help](#) [cancel](#)

Note: Public Keys must be in the PEM format.

PUBLIC KEY

```
-----BEGIN RSA PUBLIC KEY-----
MIIBCAgKCAQEAxTV5d/JIrZiz/w07Mfwm3q+xnvdxDXTvG6oPW4f4D60d4g8YVUqy
K/nmfL63Txk7ng5Jqwt96rL4jra1wTm6DvxBuyJR+cS4kIcc6o/miqhMYLIuza
zsRWXpgjxVBpQc/aHsVPJldvAqVbkeLXDp9AejHczg+Ak5ICmnI+5Hlg/6Ph8j1H
Z9IKpxTdGPQk0n2HErhT8cozqw95KkTvdGM16E19ADCoYzx95SXv8enkVs6SKnHj
KmdaJimo3zXy5GqcjpA1jBgJASx+nLG30vMmDjTHfoAGw5601hTAX9LJ9Ud670ff
jEvn/jEQqcinf0dsfUGaewRb1L9G4ESuxQIDAQAB
-----END RSA PUBLIC KEY-----
```

[Add](#)

```
begin
  DBMS_CLOUD.create_credential (
    credential_name => 'OBJ_STORE_CRED',
    username => '<userXX>',
    password => '<your Auth Token>'
  );
end;
```

Authorization

- Authorization specifies various actions an authenticated Principal can perform
- OCI Authorization = Policies
- 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>`]
- Policy Attachment: Policies can be attached to a compartment or the tenancy. Where you attach it controls who can then modify it or delete it

Policy Syntax

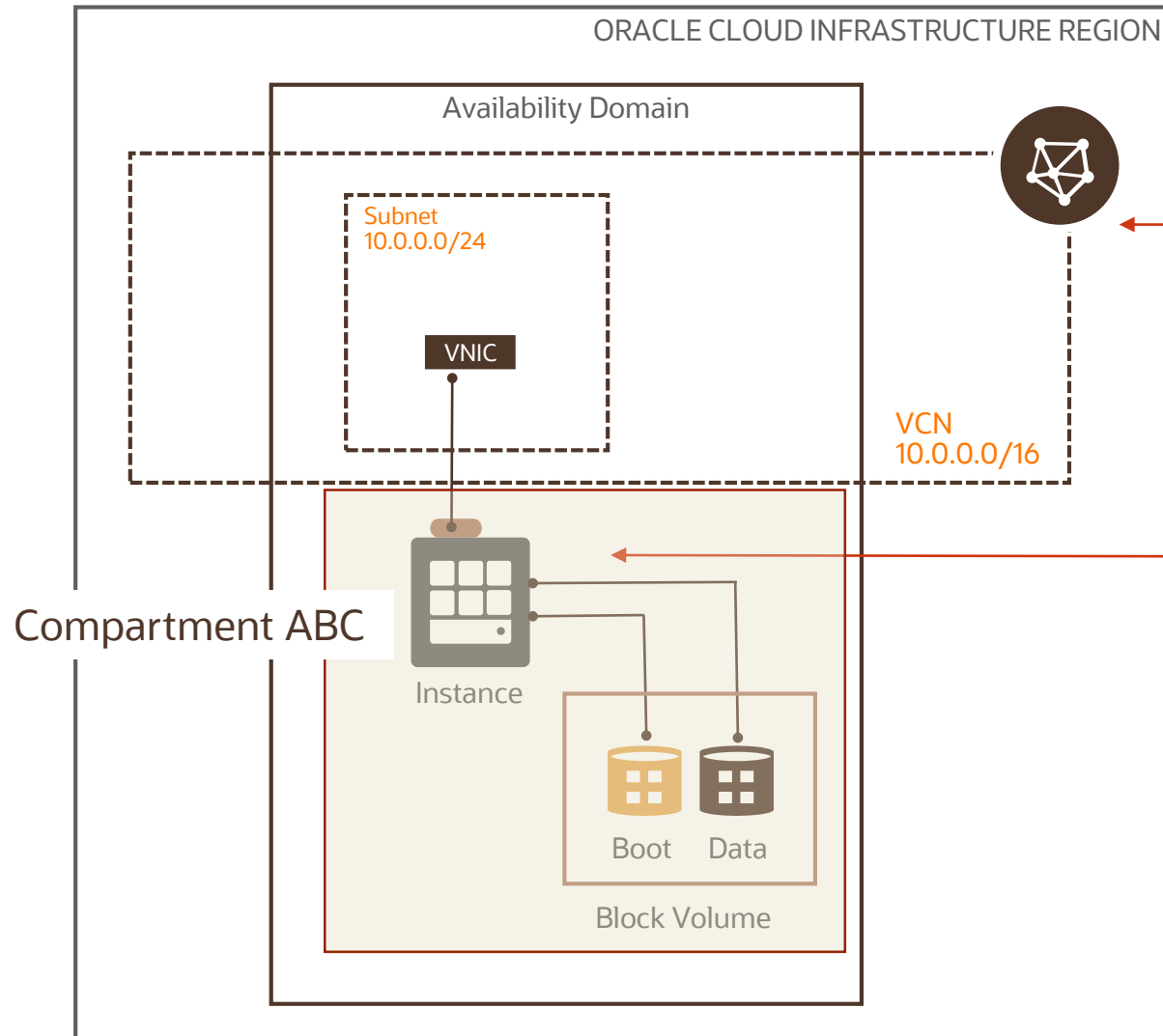
Allow <subject> to <verb> <resource-type> in <location> where <conditions>

Verb	Type of access
inspect	List resources
read	Inspect + user-specified metadata
use	Read + Update (the actions vary by resource type)*
manage	All permissions

* In general, this verb does not include the ability to create or delete that type of resource

Aggregate resource-type	Individual resource type
all-resources	
database-family	db-systems, db-nodes, db-homes, databases..
instance-family	instances, instance-images, volume-attachments..
object-family	buckets, objects..
virtual-network-family	vcn, subnet, route-tables, security-lists, ...
volume-family	volumes, volume-attachments, volume-backups
Cluster-family	clusters, cluster-node-pool, cluster-work-requests
File-family	file-systems, mount-targets, export-sets...
dns	dns-zones, dns-records, dns-traffic,...

Common Policies



Network Admins manage a cloud network

Allow group NetworkAdmins to **manage** **virtual-network-family** in tenancy

Users launch compute instances

Allow group InstanceLaunchers to **manage** **instance-family** in compartment ABC

Allow group InstanceLaunchers to **use** **volume-family** in compartment ABC

Allow group InstanceLaunchers to **use** **virtual-network-family** in compartment XYZ

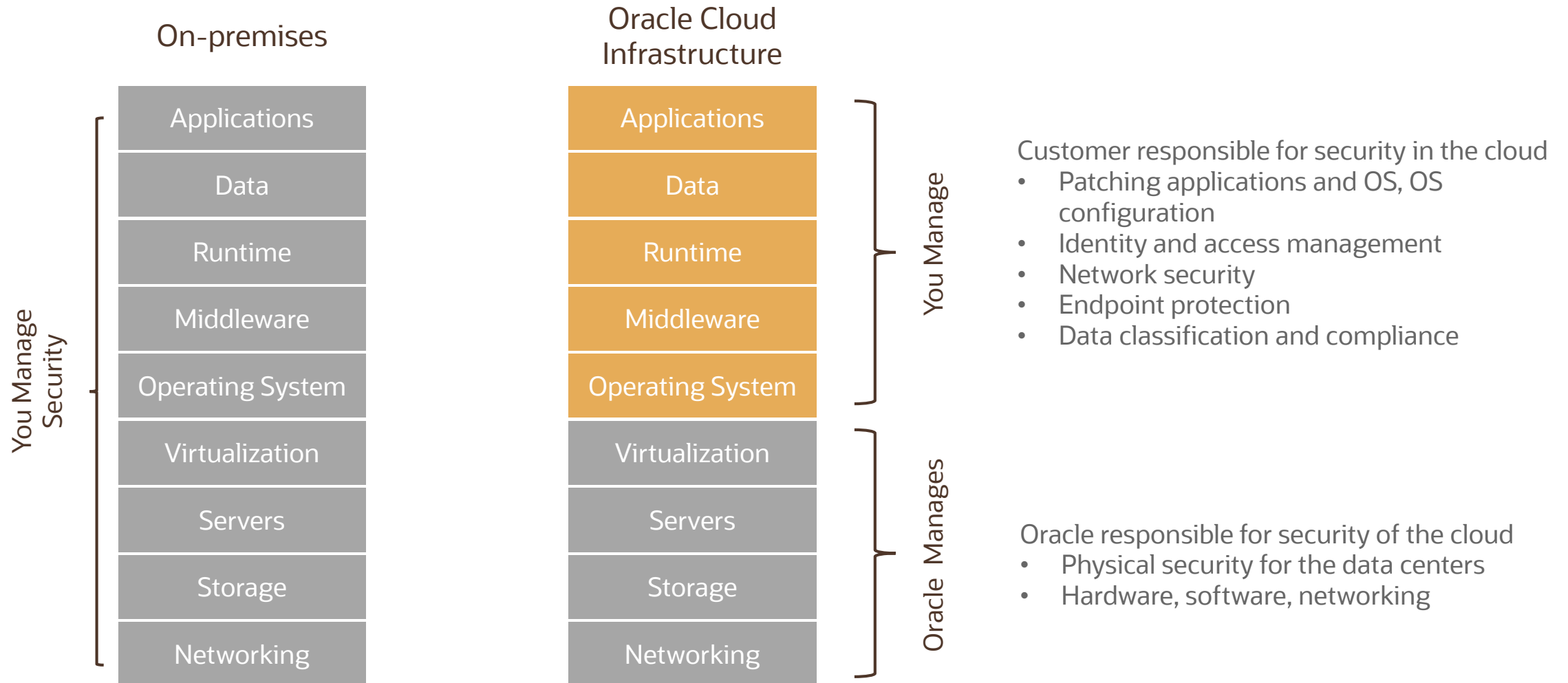
ORACLE

OCI Security

Agenda

Shared Security Model
Security services
Identity and Access Management
Data protection
OS and workload isolation
Infrastructure protection

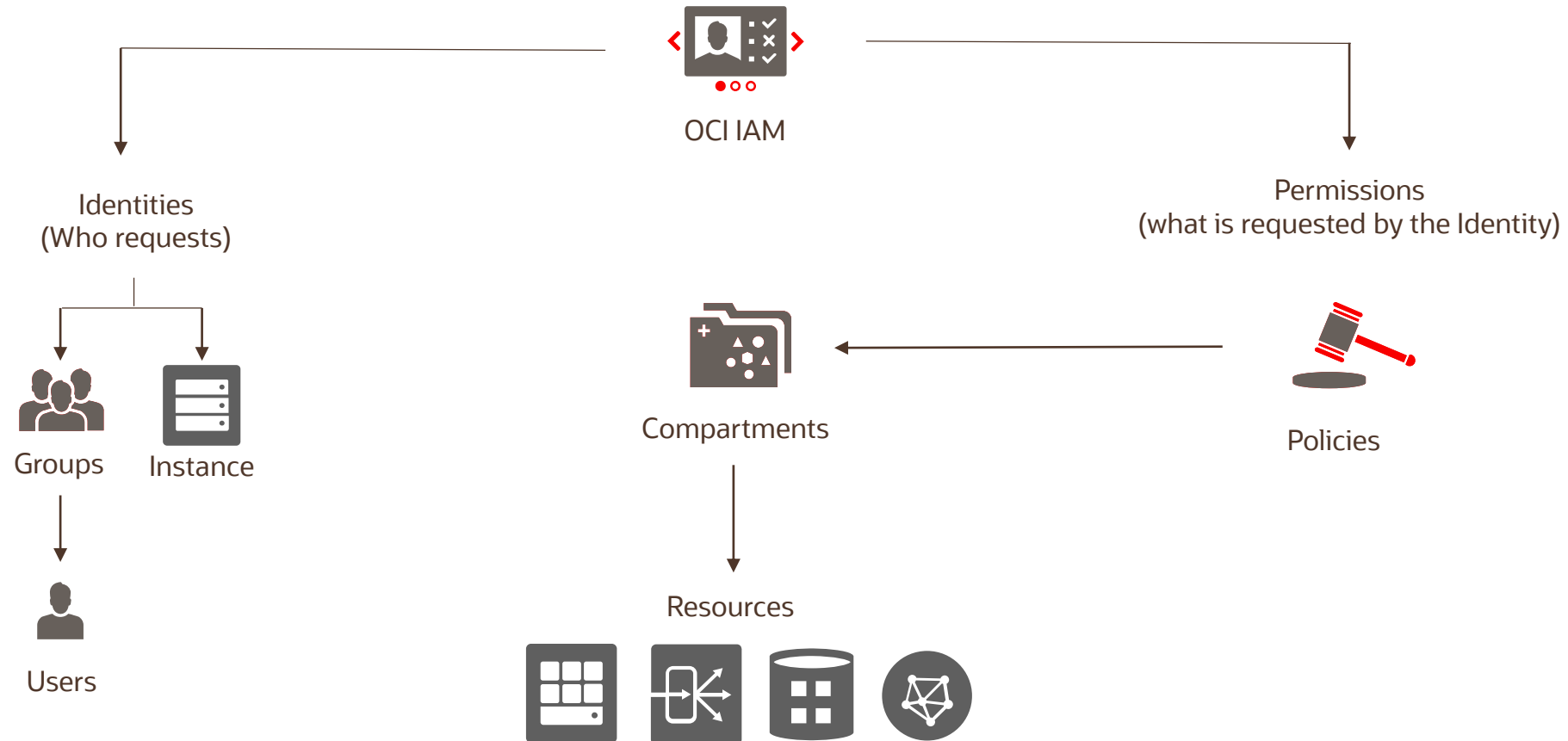
Shared Security Model



Security Services

	Use case	Service
Identity and Access Management	Manage user access and policies	OCI IAM
	Manage multi-factor authentication	MFA
	Single sign-on to identity providers	Federation
Data Protection	Encryption for data at rest, in-transit	Storage and DB services
	Discover, classify and protect your data	Data Safe
	Hardware based key storage	Key Management
	Centralized key management	Key Management
OS and workload management	Patch Management	OS Management service
	Workload isolation	Bare Metal, Dedicated VM Hosts
Infrastructure Protection	Network security controls	VCN NSG, SL
	Filter Malicious web traffic	Web Application Firewall
	DDoS Protection	In-built

Identity and Access Management



Multi-factor Authentication (MFA)



Multi-factor authentication (MFA) is a method of authentication that requires the use of more than one factor to verify a user's identity. Examples of authentication factors are a password (something you know) and a device (something you have)

Federation

- Enterprises use an identity provider (IdP) to manage user login/passwords and to authentications
- When someone in your company wants to use OCI Console, they must sign in with a user login and password.
- Your administrators can federate with a supported IdP so that each employee can use an existing login and password (and not create a new set to use OCI)
- Federated users choose which IdP to use for sign-in, and then they're redirected to that IdP's sign-in experience for authentication
- After entering their login and password, they are authenticated by the IdP and redirected to the OCI Console

Signing in to cloud tenant:
ociobenablement

[Change tenant](#)

Single Sign-On (SSO)

We have detected that your tenancy has been federated to another Identity Provider.

Select your Identity Provider below.

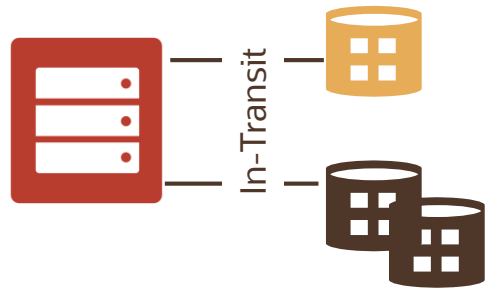
IDENTITY PROVIDER

identitycloudservice ▼

Continue

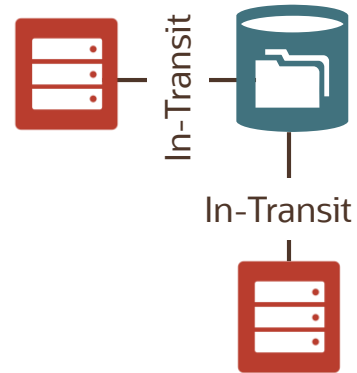
Data Protection

Block Volume



- Data encrypted at-rest
- Data encrypted in-transit
- Bring Your Own Keys

File Storage



- Data encrypted at-rest
- Data encrypted in-transit
- Bring Your Own Keys

Object Storage



- Data encrypted at-rest
- Bring Your Own Keys
- Private Buckets, Pre-authenticated Requests

Database



- Transparent Data Encryption
- Data Safe
- Data Vault

Key Management

- Managed service that enables you to encrypt your data using keys that you control
- Key Management provides you with
 - Centralized key management capabilities
 - Highly available, durable, and secure key storage in hardware security modules (HSMs)*
 - Integration with select Oracle Cloud Infrastructure services
- Uses HSMs that meet Federal Information Processing Standards (FIPS) 140-2 Security Level 3 security certification
- HSM hardware is tamper-evident, has physical safeguards for tamper-resistance, requires identity-based authentication, and deletes keys from the device when it detects tampering

* A HSM is a physical computing device that safeguards digital keys and provides crypto processing

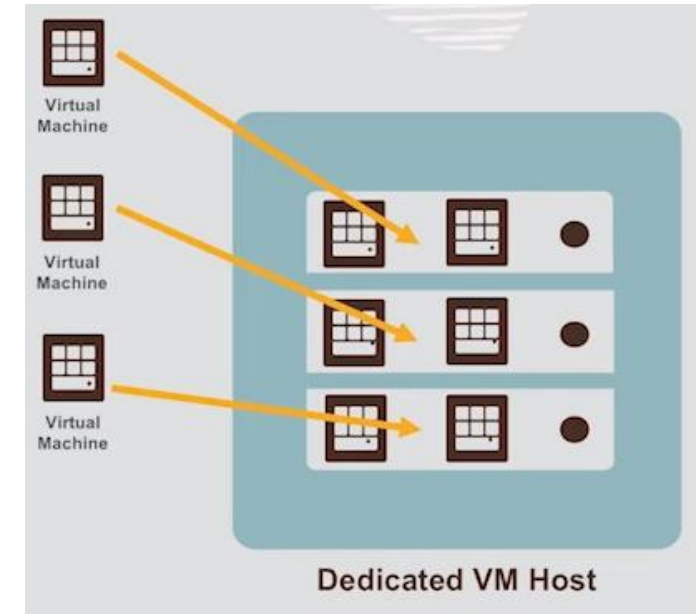
Data Safe

- Managed service that provides a complete and integrated set of features for protecting sensitive and regulated data in Oracle Cloud databases
- Features include Security Assessment, User Assessment, Data Discovery, Data Masking, and Activity Auditing
- Supports ATP (shared), ADW (shared), VM/BM DB Systems
- Saves time and mitigates security risks
- Defense in Depth for all customers
- No special security expertise needed
- No extra costs to use



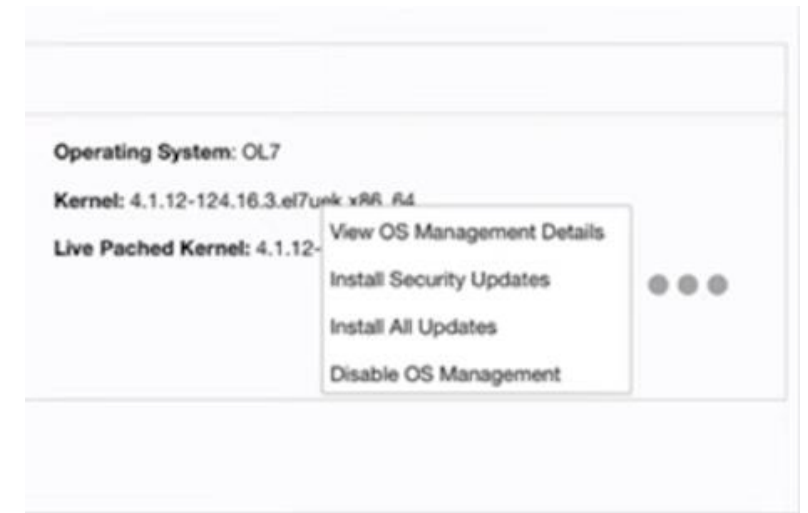
Dedicated VM Host

- Security of Bare Metal combined with ease and flexibility of VMs
- Single-tenant: never share HW with another customer's VMs
- Pay only for dedicated VM Host – no additional charge for the VMs running on it
- Control and convenience
 - Control over placement across Dedicated VM Hosts, or let Oracle optimize it automatically
 - Oracle manages and monitors the hypervisor and hardware

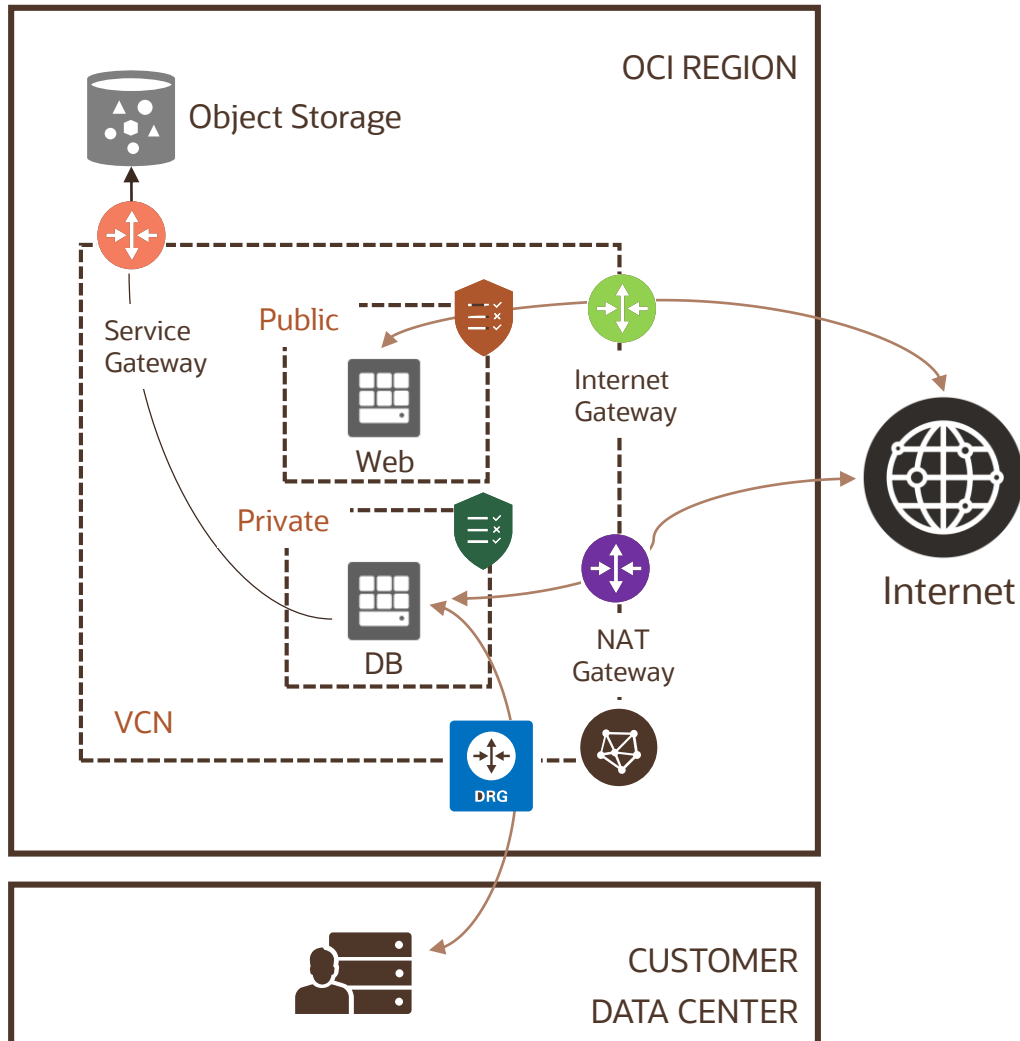


OS Management Service

- Executes and automates common and complex management tasks
- Package management, configuration management
- Security/compliance reporting
- Enables live patching of critical components and Linux kernel w/o downtime
- Configured by default for Oracle Linux instances in OCI



Network protection



Tiered subnet strategy for the VCN

- DMZ subnet for load balancers
- Public subnet for web servers
- Private subnet for internal hosts such as databases

Gateways

- NAT Gateway – for connectivity to internet for patching
- Service Gateway – for connectivity to public OCI services
- Dynamic Routing Gateway – for connectivity to on-premises

Security Lists, NSG

- SL determines the types of traffic allowed in and out of the subnet
- NSG the types of traffic allowed in and out of a VNIC

OCI Web Application Firewall

What is a WAF?

- WAF refers to a device, server-side plugin, or filter that applies a set of rules to HTTP/S traffic
- By intercepting HTTP/S traffic and passing them through a set of filters and rules, WAF is able to uncover and protect against attack streams hitting a web application
- Rules cover common attacks (Cross-site Scripting (XSS), SQL Injection) and ability to filter specific source IPs or bad bots
- Typical responses from WAF will either be allowing the request to pass through, audit logging the request, or blocking the request by responding with an error page.

OCI Web Application Firewall (WAF) is a cloud-based, PCI-compliant, global security service that protects applications from malicious and unwanted internet traffic.

Use cases:

- Protect any internet-facing endpoint from cyberattacks and malicious actors
- Protect against cross-site scripting (XSS) and SQL injection
- Bot management – dynamically blocking bad bots
- Protection against layer 7 DDoS attacks

Compliance certifications

Global	 SOC 1 : SOC 2 : SOC 3	 27001 : 27017 : 27018	 Level 1	 US Privacy Shield			
Government	 DoD DISA SRG IL2	 DoD DISA SRG IL5	 Moderate – Agency ATO	 VPAT – Section 508	 G-Cloud 11 - UK	 Model Clauses - EU	
Industry	 HIPAA	 PCI DSS	 FISC - Japan	 IG Toolkit - UK	 FINMA - Switzerland		
Regional	 GDPR - EU	 BSI C5 - Germany	 TISAX - Germany	 PIPEDA - Canada	 Cyber Essentials Plus - UK	 My Number - Japan	 Cloud Security Principles - UK



ORACLE

OCI Pricing and Billing

Rohit Rahi

Oracle Cloud Infrastructure

Feb 2020

Agenda

Pricing Models

Pricing Example

Billing

Cost Management

Free Tier

Pricing Models

Pay as you go (PAYG)

- Charged only for the resource consumed
- No upfront commitment
- No minimum service period
- Usage metered hourly
- Consumption based model for services like Oracle Functions

Monthly Flex (Universal Credits)

- A minimum of \$1000 monthly charge and a minimum 12 month fixed commitment
- Observed 33%-60% savings vs PAYG
- Discounts based on size of deal and term of deal
- Usage is consumed from monthly prepaid commitment

Bring Your Own License (BYOL)

- Apply your current on-premises Oracle licenses to equivalent, highly automated Oracle IaaS & PaaS services in the cloud
- Complete license mobility with on-premises

UC Price list, <https://www.oracle.com/cloud/ucpricing.html>

BYOL FAQs, <https://www.oracle.com/cloud/bring-your-own-license/faq/>

Factors that impact Pricing

Resource Size

Bigger resources cost more!

Data Transfer

No Ingress cost
Careful with Egress cost

Resource Type

VMs v/s BMs
VMs v/s Functions
BYOL v/s managed DBs..

All OCI regions have the
same pricing!

Resource Size

Bigger resources
cost more!

Resource Type

VMs v/s BMs
Intel v/s AMD
GPU, HPC

Product	Pay As You Go	Monthly Flex	Part Number	Metric
Windows OS	\$0.0204	\$0.0204	B88318	OCPU Per Hour
Virtual Machine Standard - X5	\$0.0638	\$0.0638	B88317	OCPU Per Hour
Compute - Virtual Machine Dense I/O - X7	\$0.1275	\$0.1275	B88516	OCPU Per Hour
Compute - Virtual Machine Standard - X7	\$0.0638	\$0.0638	B88514	OCPU Per Hour
Compute - Virtual Machine GPU Standard - X7	\$1.275	\$1.275	B88518	GPU Per Hour
Compute - Virtual Machine Standard - E2 Micro - Free			B91444	OCPU Per Hour
Compute - Standard - E2	\$0.03	\$0.03	B90425	OCPU Per Hour
Compute - HPC - X7	\$0.075	\$0.075	B90398	OCPU Per Hour
Compute - BM Standard - B1	\$0.0638	\$0.0638	B91119	OCPU Per Hour
Compute - VM Standard - B1	\$0.0638	\$0.0638	B91120	OCPU Per Hour
Compute - Microsoft SQL Enterprise - OCPU Per Hour	\$1.47	\$1.47	B91372	OCPU Per Hour
Compute - Microsoft SQL Standard - OCPU Per Hour	\$0.37	\$0.37	B91373	OCPU Per Hour

Block Volume Pricing

Block Volume Pricing

1. Storage cost (GB/month): \$0.0255

+

2. Performance cost (VPU/GB):

- NA for Basic
- 10 VPUs at \$0.0017 for Balanced
- 20 VPUs at \$0.034 for Higher Performance

	VPUs/GB	IOPS/GB
Basic	NA	2
Balanced	10	60
Higher Performance	20	75

100 GB of BV

Basic



200 IOPS

Storage (S) : \$0.0255 x100

Performance (P) : \$0

Total (S) + (P) : \$2.55

Balanced



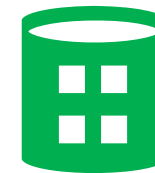
6000 IOPS

Storage (S) : \$0.0255 x100

Performance (P) : \$0.17

Total (S) + (P) : \$2.72

Higher Performance



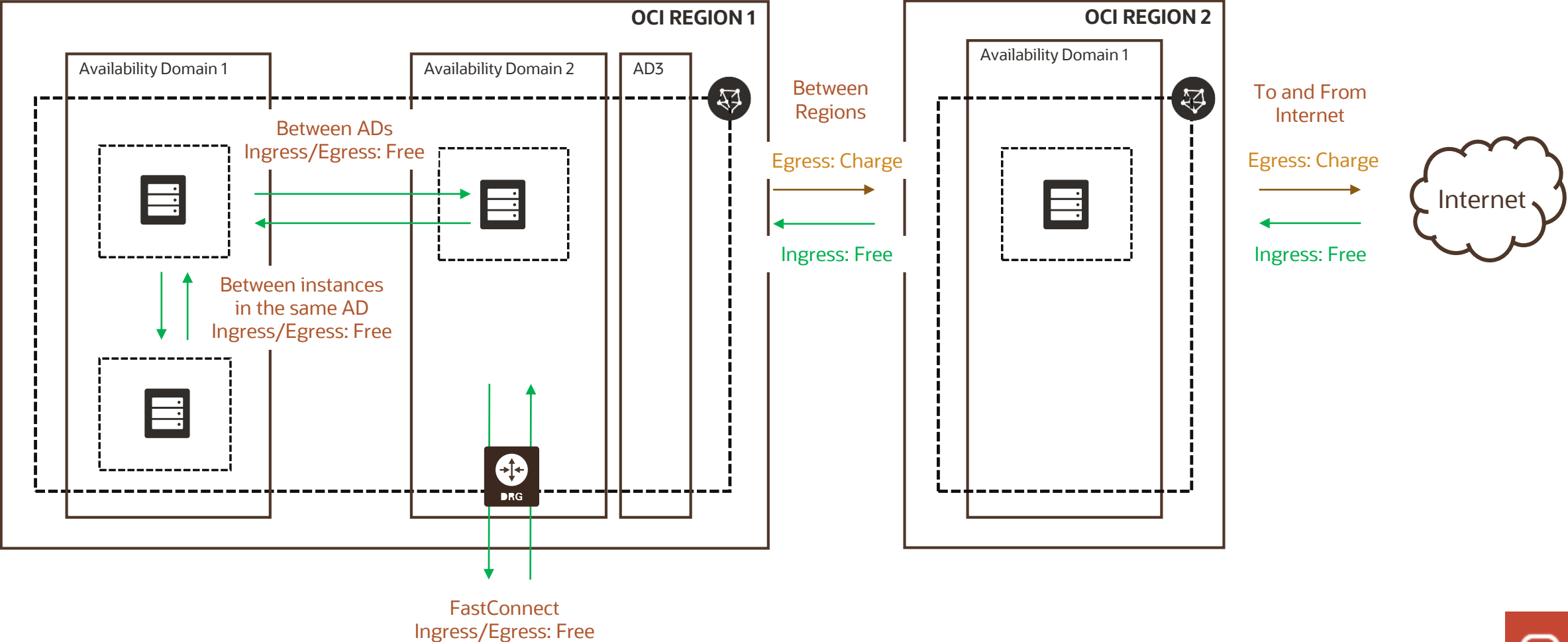
7500 IOPS

Storage (S) : \$0.0255 x100

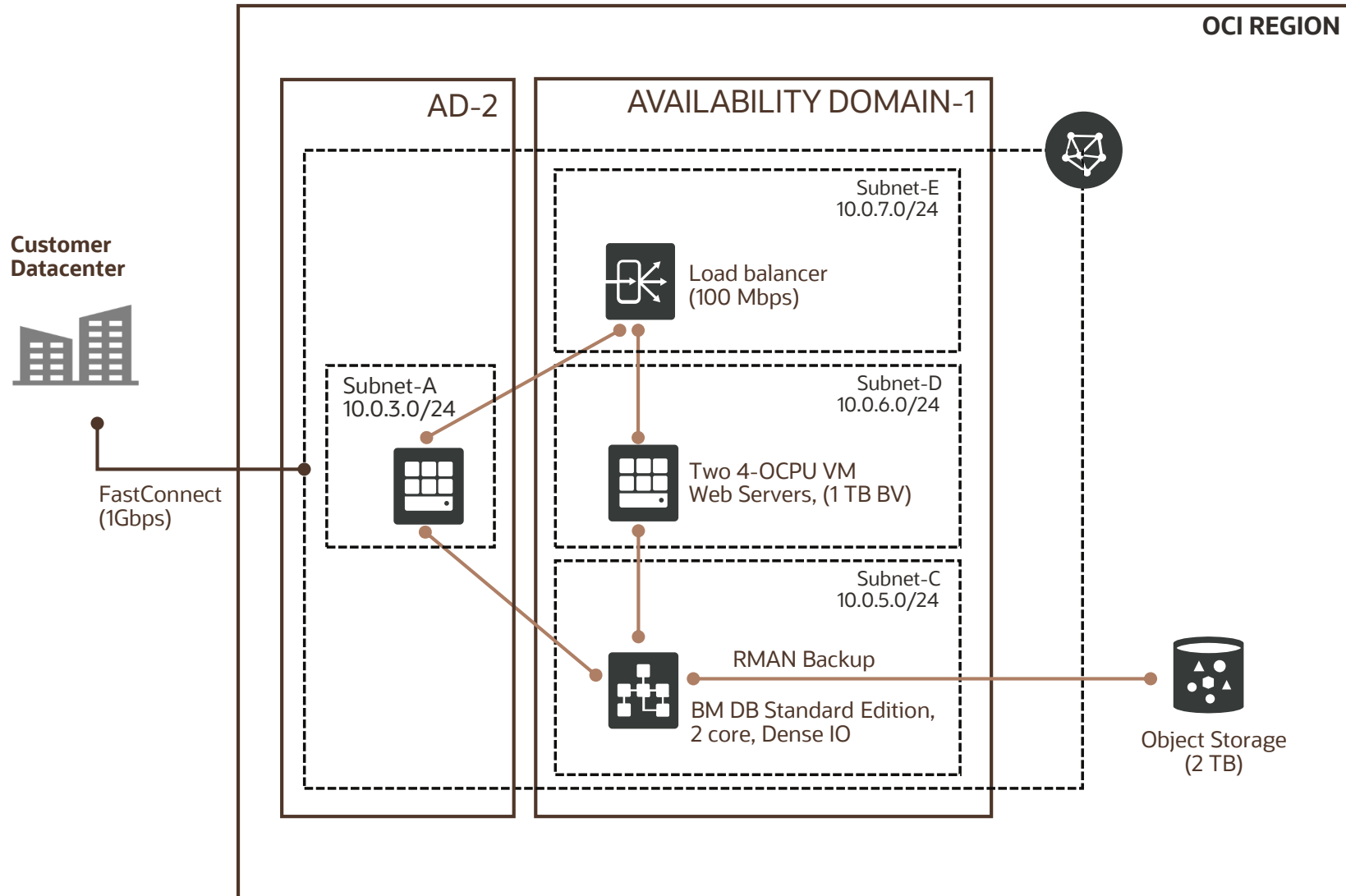
Performance (P) : \$3.4

Total (S) + (P) : \$5.95

Data Transfer costs



Pricing Example



- Two 4-OCPU Virtual Machine instances
- Total Block Volume Storage: 2 TB
- Object Storage Service: 2 TB
- Database Cloud Service: Standard Edition - Dense I/O
- Virtual Cloud Network: 10TB Outbound Data Transfer
- FastConnect: 1 Gbps*
- Load Balancer Service: 100 Mbps

Pricing Example

SKU Name	Part #	PAYG (USD)	Monthly Flex (USD)	Metric	Qty	PAYG Annual cost (USD)	Flex Annual cost (USD)
Oracle Cloud Infrastructure – Block Volume	B91961	\$0.0255	\$0.0255	GB/month	2000	\$612.00	\$612.00
Oracle Cloud Infrastructure – Block Volume Performance Units (High Performance)	B91962	\$0.034	\$0.0017	VPUs/GB/month	2000	\$816.00	\$816.00
Oracle Cloud Infrastructure – Object Storage - Storage	B88324	\$0.0255	\$0.0255	GB/month	2000	\$612.00	\$612.00
Oracle Cloud Infrastructure – Object Storage - Requests	B88323	\$0.0034	\$0.0034	10K req/month	100	\$0.34	\$0.34
Oracle Cloud Infrastructure – Compute - Virtual Machine Standard - X7	B88514	\$0.0638	\$0.0638	OCPU/hour	8	\$4,556.80	\$4,556.80
Oracle Cloud Infrastructure – Outbound Data Transfer	B88327	\$0.0085	\$0.0085	GB/month	10	0	0
Oracle Cloud Infrastructure – Database Standard Edition - Dense I/O - X7	B89621	\$10.746	\$7.164	Hosted/Hr.	1	\$95,940.24	\$63,960.19
Oracle Cloud Infrastructure – FastConnect 1 Gbps	B88325	\$0.2125	\$0.2125	Port Hour	1	\$1897.20	\$1897.20
Oracle Cloud Infrastructure – 100 Mbps Load Balancer	B88319	\$0.0213	\$0.0213	Load Balancer Hour	1	\$190.16	\$190.16
Total						\$104,624	\$72,644



ORACLE

Billing and Cost Management

Cost Tracking Tags

Governance » Tag Namespaces » Tag Namespace Details

Finance

NS ACTIVE

Add Tags Move Tag Namespace Retire Namespace Delete Tag Namespace

Tag Namespace Information Tags

Description: CostCenter
OCID: ...5frc3q Show Copy
Number of Cost-tracking Tags: 0

Tag Key Definitions in this Namespace in Tr

Create Tag Key Definition

This Tag Key Definition will be created in the "Finance" Namespace

TAG KEY

CostCenter

Spaces and periods are not allowed.

DESCRIPTION

Cost center tags

☒ COST-TRACKING ⓘ

TAG VALUE TYPE

☐ STATIC VALUE
User can enter a string to set the value for this key

☒ A LIST OF VALUES
User selects from a list to set the value for this key

VALUES

Marketing
Operations

Separate multiple values with new lines

Create Tag Key Definition

Compute » Instances » Instance Details

web server AD2

Start Stop Reboot Move Resource Apply Tag(s) Actions

Instance Information Tags

No Tags

There are no tags associated with this resource.

Apply Tag(s)

What is tagging?

Tagging is a metadata system that allows you to organize and track resources within your tenancy. Tags are composed of keys and values that can be attached to resources.

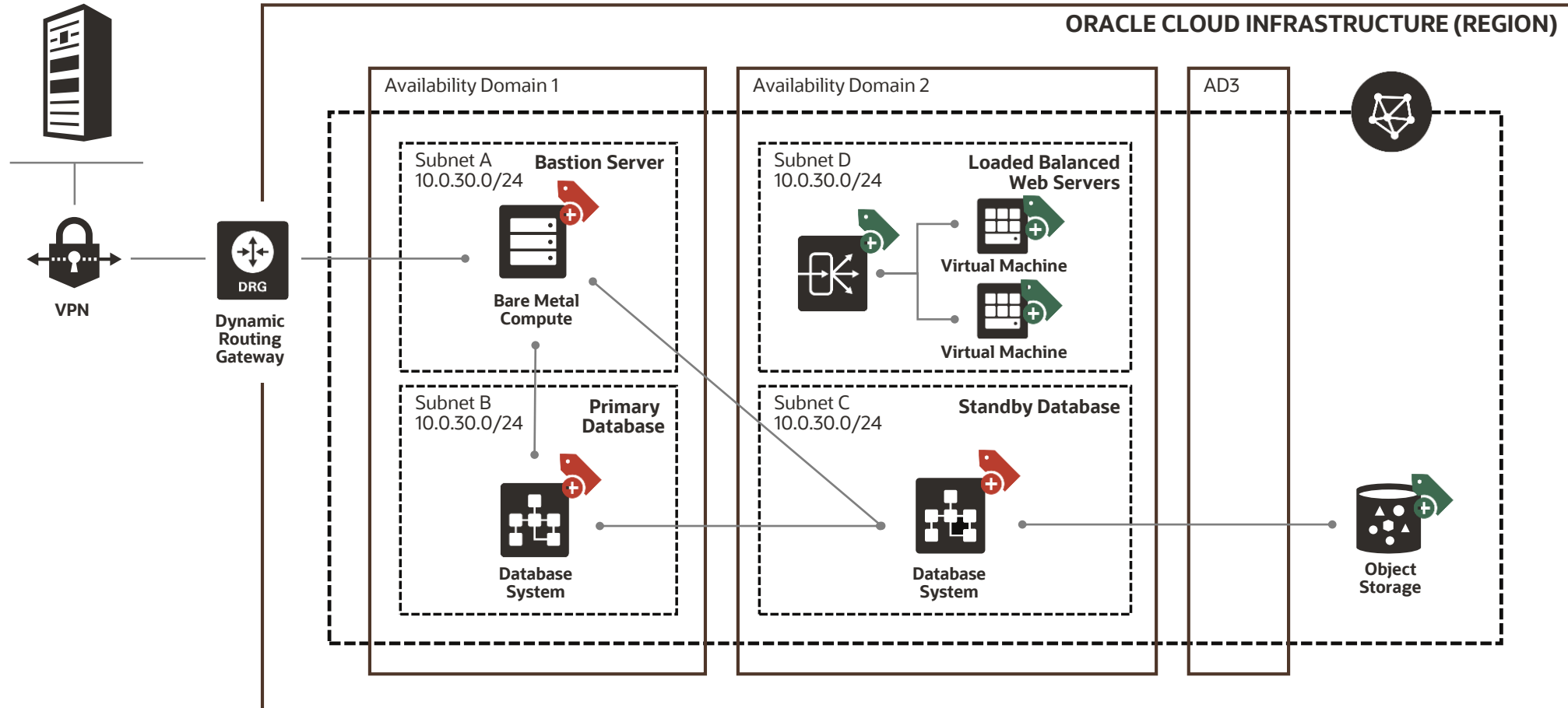
[Learn more about tagging](#)

TAG NAMESPACE TAG KEY VALUE

Finance CostCenter Marketing

Apply Tag(s)

Tag all resources



Cost Analysis

- Visualization tools Help understand spending patterns at a glance
- Filter costs by Date, Tags and Compartments
- To use Cost Analysis you must be a member of the Administrators group

Filtering the usage by tags will show you only the costs generated by the resources tagged with "Finance.CostCenter=Marketing"

Budgets

- A monthly threshold you define for your OCI spend
- Can be set on cost-tracking tags or compartments and track all spending in the cost-tracking tag or compartment and any child compartments
- Can define email alerts that get sent out for your budget
- Alerts are evaluated every 15 minutes, and can be triggered when your actual or forecasted spending hits either a budget % or a specified amount

Create Budget

BUDGET SCOPE

☒ COMPARTMENT ☐ COST-TRACKING TAG

NAME

Name can only contain alphanumeric characters, dashes, periods, and underscores.

DESCRIPTION

TARGET COMPARTMENT ⓘ

intoraclerohit (root)

MONTHLY BUDGET AMOUNT

The minimum allowed value is 1; the maximum allowed value is 999,999,999,999.

Budget Alert Rule (optional)

You can set up a budget alert rule now, or add it later. You can set up multiple alerts for the same budget.

THRESHOLD METRIC ⓘ

☒ ACTUAL SPEND ☐ FORECAST SPEND

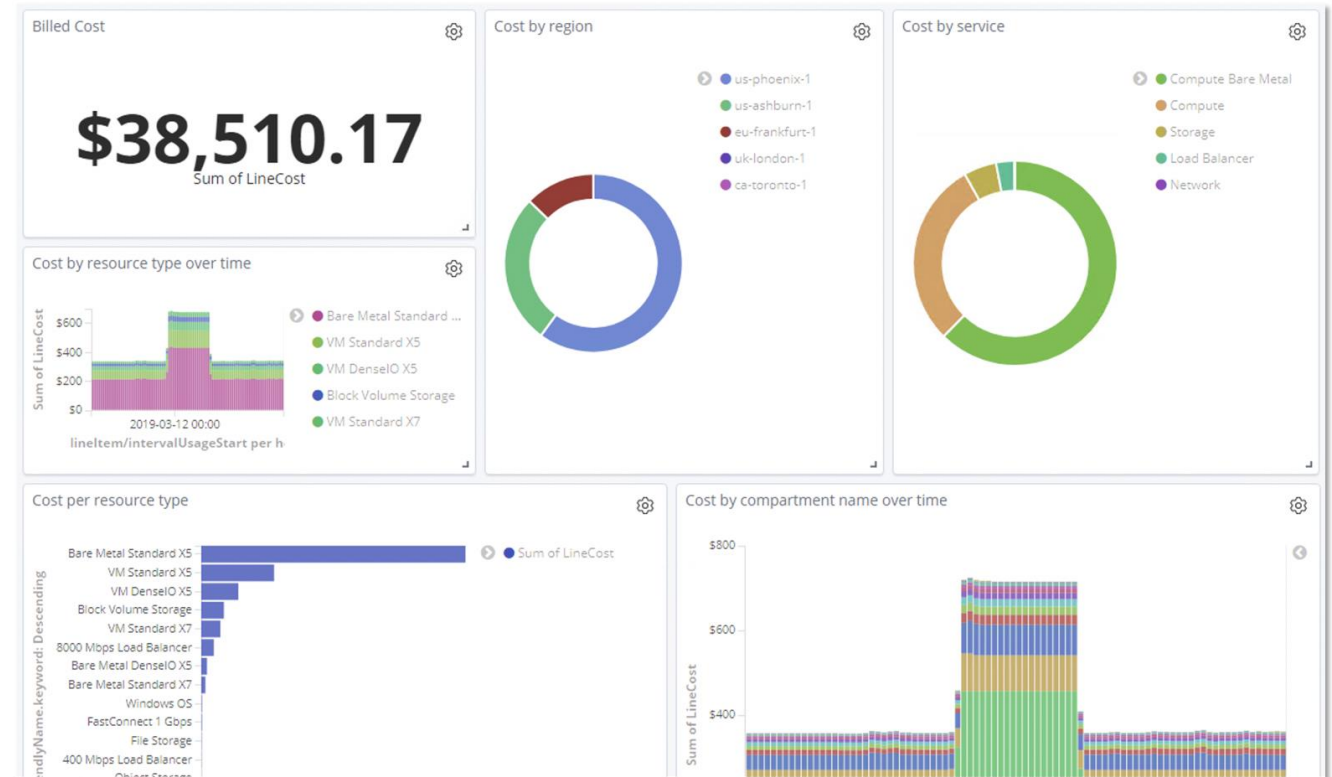
THRESHOLD TYPE ⓘ

☒ PERCENTAGE OF BUDGET ☐ ABSOLUTE AMOUNT

THRESHOLD %

Usage Reports

- Detailed information about your OCI consumption
- CSV file with one record per resource per hour with metadata and tags
- Automatically generated daily, and stored in an Oracle-owned object storage bucket
- Contain 24 hours of usage data
- Retained for one year



ORACLE

Free Tier

OCI Free Tier + Always Free

Free Tier

- \$300 free credits valid for 30 days
- Access to a wide range of OCI services
- May be used until your US\$300 of free credits are consumed or the 30 days has expired, whichever comes first.
- Up to eight instances across all available services
- Up to 5 TB of storage

Always Free

- Services you can use for an unlimited time.
- Two Oracle Autonomous Databases
- Two OCI Compute VMs; Block, Object, and Archive Storage; Load Balancer and data egress; Monitoring and Notifications

<https://www.oracle.com/cloud/free/#free-cloud-trial>

Summary

Pricing Models

Pricing Example

Billing

Cost Management

Free Tier



Oracle Cloud always free tier:

oracle.com/cloud/free/

OCI training and certification:

cloud.oracle.com/en_US/iaas/training

cloud.oracle.com/en_US/iaas/training/certification

education.oracle.com/oracle-certification-path/pFamily_647

OCI hands-on labs:

ocitraining.qcloudable.com/provider/oracle

Oracle learning library videos on YouTube:

youtube.com/user/OracleLearning

Thank you

