



# Prod-DR Strategy Guidelines

# Agenda

- **High Availability & Disaster Recovery**
  - OCI & Oracle PaaS Cloud High Availability or Maximum Availability Architecture Concepts.
  - OCI Disaster Recovery (DR)
    - DR Concepts
    - RTO & RPO
    - DR for OCI in Region
    - DR for OCI across Region
    - DR Using Backup & Recovery
    - DR from On-Premise To Cloud
  - High Availability or Maximum Availability Architecture & Disaster Recovery - Building Blocks.
    - Region
    - Availability Domain
    - Fault Domain
    - Floating IP

# Agenda

- High Availability Compute, Storage & Network.
  - Compute Active/Active & Active/Passive.
  - Object, Block, File Storage High Availability.
  - Volume Group Backup
  - VCN peering (Remote).
- High Availability for Database and Applications
  - Real Application Cluster (RAC)
  - Data-guard (Standby)
  - Active Data Guard
  - Recommended Data Guard options
  - Golden Gate for Mission Critical Databases
  - Topology for Single Region
  - Topology for Multiple Region

# HA / MAA & DR

## Benefits

- Business Continuity
- Scaling Hardware on demand / redundant on secondary site/s.
- DR can setup across region(Geographical) and as well on same region.
- Failure can move over to Available service (HA and or DR).

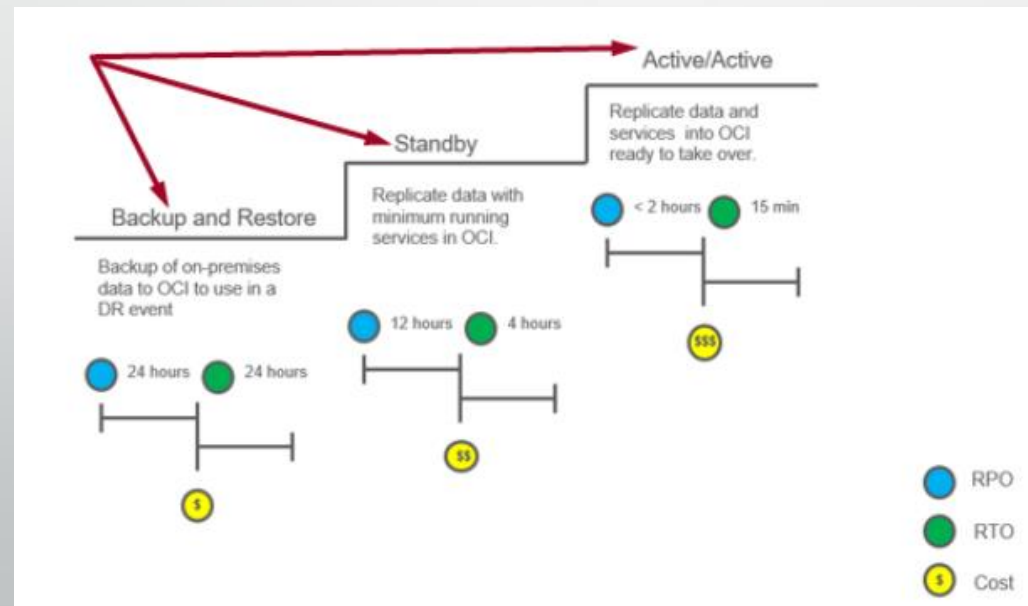
## Overview:

Disaster recovery (DR) is the process of protecting your applications from a disaster. A disaster can be anything that puts applications at risk, from network outages to equipment failures to natural disasters. When an unforeseen disaster happens, a well-architected DR plan enables applications to recover as quickly as possible and to continue to provide services to users. Oracle Cloud Infrastructure provides highly available and scalable cloud infrastructure and services that enable the DR for applications to be reliable, secure, and fast.

# DR Concepts

Disaster Recovery Concepts To understand DR planning, it's important to understand two commonly used terms: recovery time objective (RTO) and recovery point objective (RPO).

- The RTO is the target time that is required to restore application functionality after a disaster happens. The goal is to measure how quickly application/service recover from a disaster. Typically, the more critical the applications, the lower the RTO.
- The RPO is the acceptable timeframe of lost data that applications can tolerate. RPO is about how much data the applications can afford to lose in a disaster scenario. To build a DR plan that guarantees the survival of applications after a disaster and is also cost effective, must consider both RTO and RPO. Ensure that both RTO and RPO goals can be achieved to recover your applications effectively from a disaster.



# Geographical Locations - Regions

Geographical locations Hosting oracle Cloud Datacentre's / Regions.

Regions: Ashburn → us-ashburn-1 Phoenix → us-phoenix-1

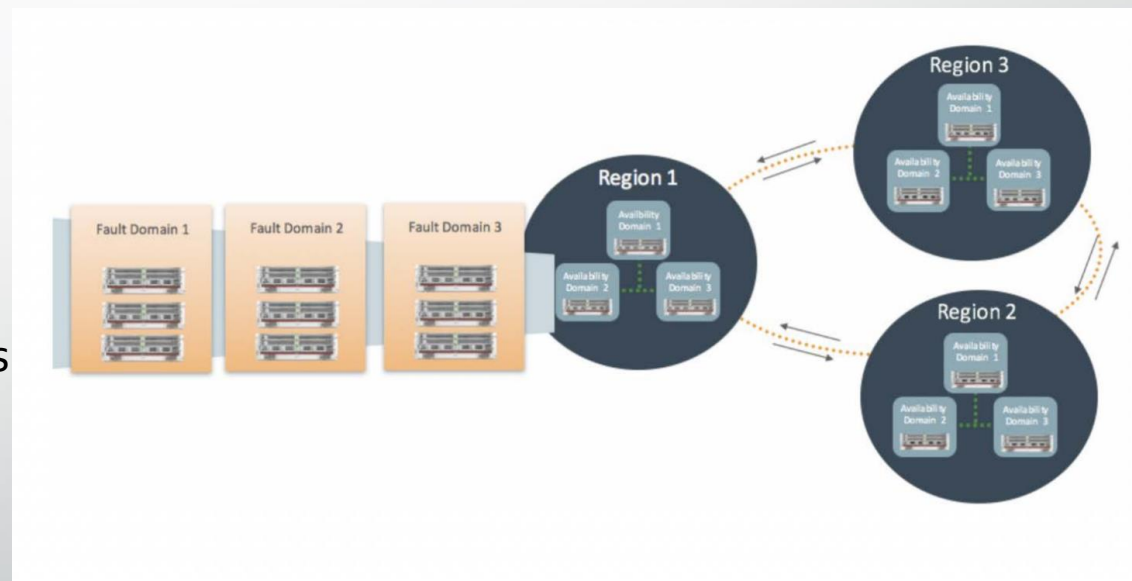
**Regions** are independent of other regions and can be separated by vast distances— across countries or even continents. Applications can be deployed in different regions to mitigate the risk of region-wide events, such as large weather systems or earthquakes.



# HA MAA & DR- Building Blocks

**Availability domain** is one or more data centres located within a region. Availability domains are isolated from each other, fault tolerant, and unlikely to fail simultaneously. Because availability domains don't share physical infrastructure, such as power or cooling, or the internal availability domain network, a failure that impacts one availability domain is unlikely to impact others. Availability domains in a region are connected to each other by a low-latency, high-bandwidth network. This predictable, encrypted interconnection between availability domains provides the building blocks for both high availability (HA) and DR.

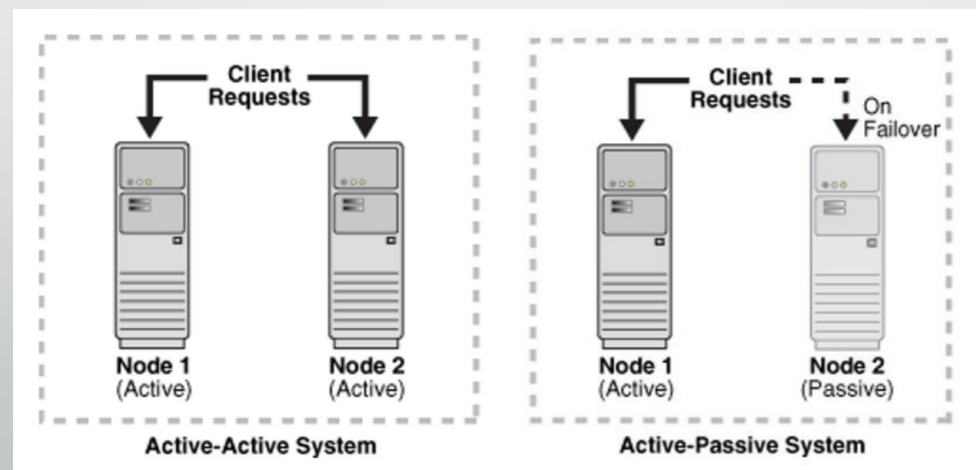
**Fault domain** is a grouping of hardware and infrastructure within an availability domain. Each availability domain contains three fault domains. Fault domains let you distribute your instances so that they are not on the same physical hardware within a single availability domain. As a result, hardware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



## High Availability Principle

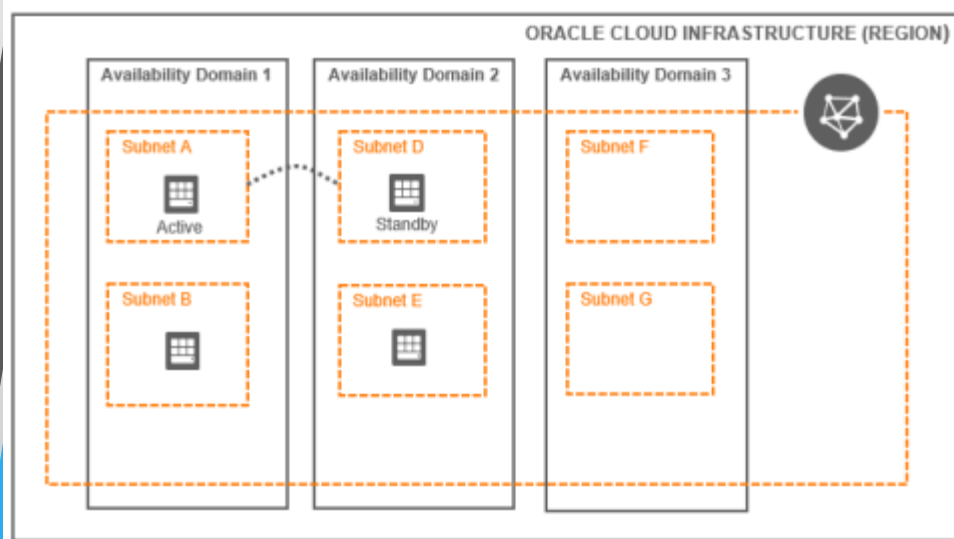
- Redundancy
  - Multiple components performing same tasks so there is no single point of failure
  - If one component fails then other component will take care of task
- Failover
  - Not all components run in A/A, some components are A/P
  - Process by which secondary component becomes primary
- Monitoring
  - Checks whether or not component is working properly or not

HA – Types: A/A A/P





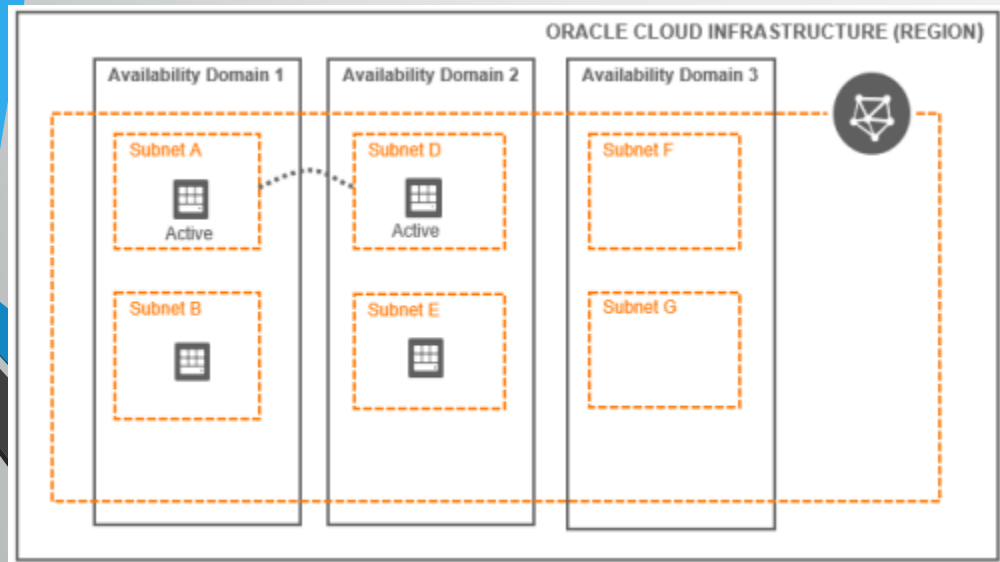
## OCI / Oracle PaaS Application HA (A/P)



Standby mode is typically used for applications that need to maintain their states.

For Stateful Applications

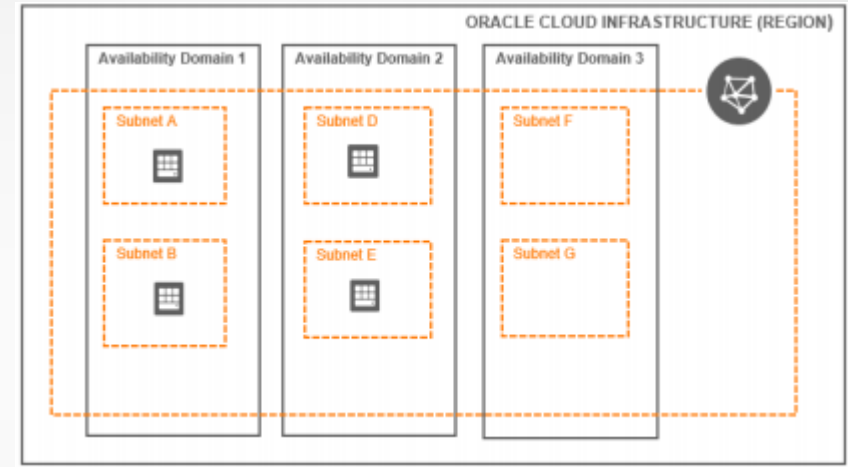
## OCI / Oracle PaaS Application HA (A/A)



For Stateless Applications

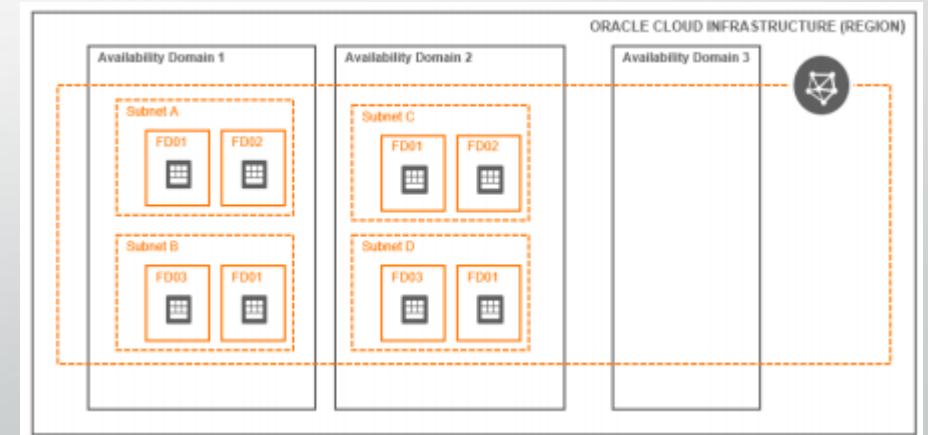
## OCI / Oracle PaaS Application HA - AD (Hardware Isolation)

- AD: physically isolated, fault tolerant, and unlikely to fail simultaneously
- No sharing of power, cooling, or internal AD network, failure in one AD will highly unlikely to impact servers/block volume in other AD
- Keep Compute & Block Volume in multiple Availability Domain (AD)



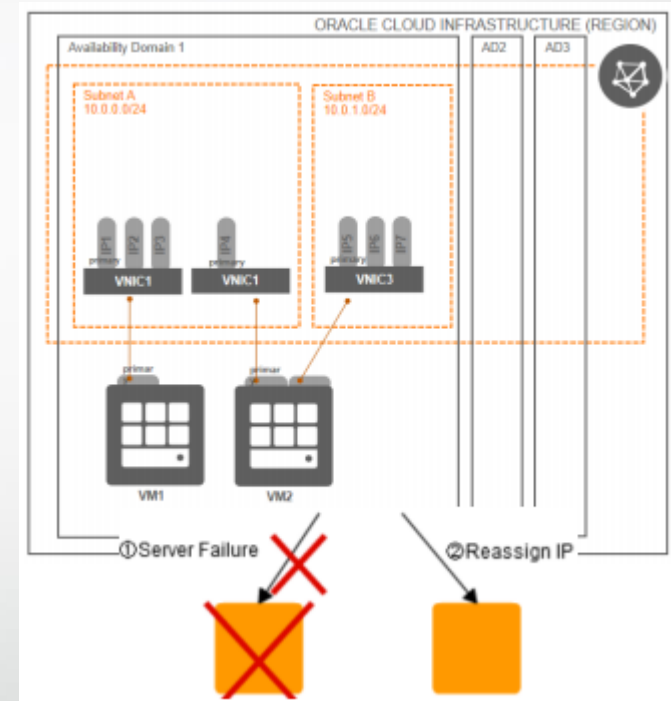
## OCI / Oracle PaaS Application HA - FD (Hardware Isolation)

- Fault Domain (FD): enables to distribute instances so that they are not on same physical hardware within a single AD
- If Oracle apply software update, only single FD is impacted at one time to ensure availability of instances in other Fault Domains
- Within AD, Deployed multiple servers in different FD



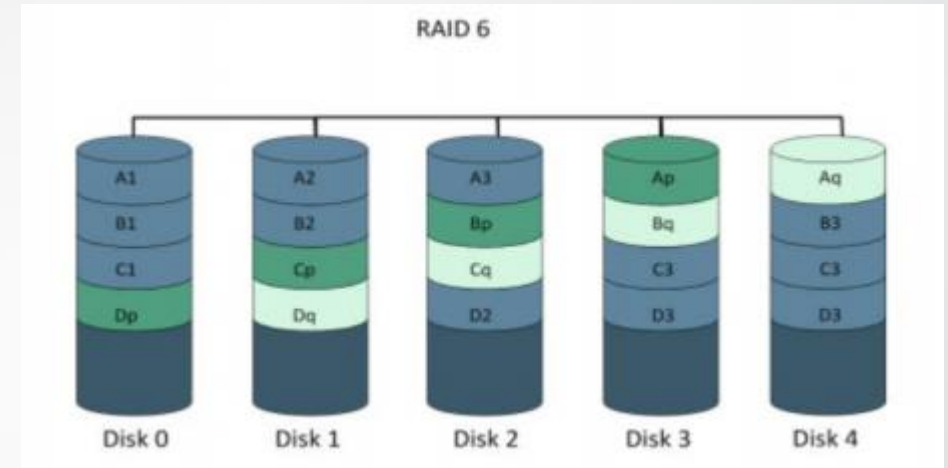
## Floating IP Address

- Floating IP can be Secondary IP or Reserved IP of Compute instances
- When compute instance fail secondary IP can be assigned to standby instance
- Failover will be achieved in the same subnet
- Reserved IP you can unassign from Primary and reassign to Standby
- Automation via Coro sync or Pacemaker



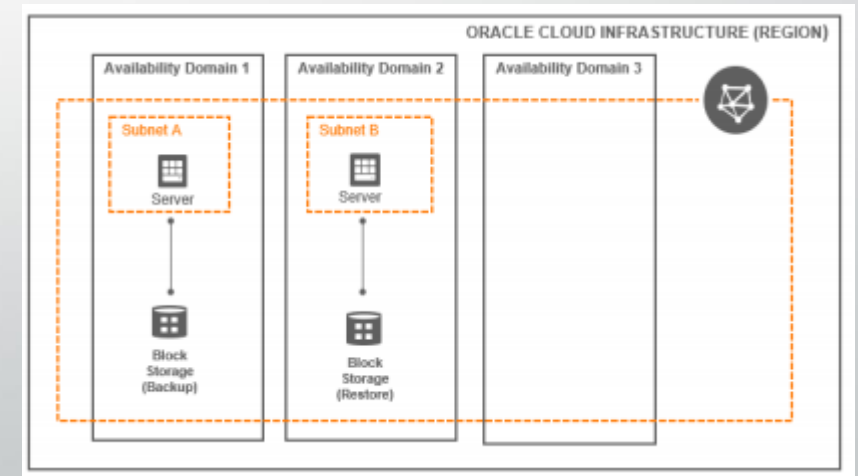
## HA: Local NVMe

- No Maintenance Operation performed from Oracle
- Customer need to plan High Availability on its own.
- Oracle Recommends RAID



## HA: Block Volume

- Policy-based backups to perform automatic, scheduled backups and retain them on Object Storage.
- Restore backups across Availability Domain.
- Cross Region Backups
- Group Volume Backup and Clone



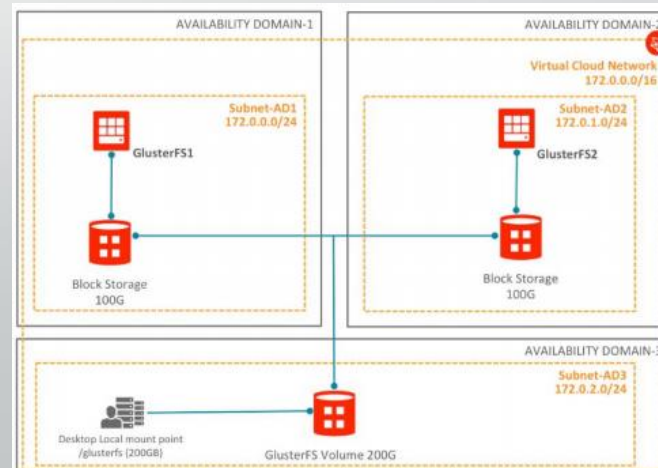
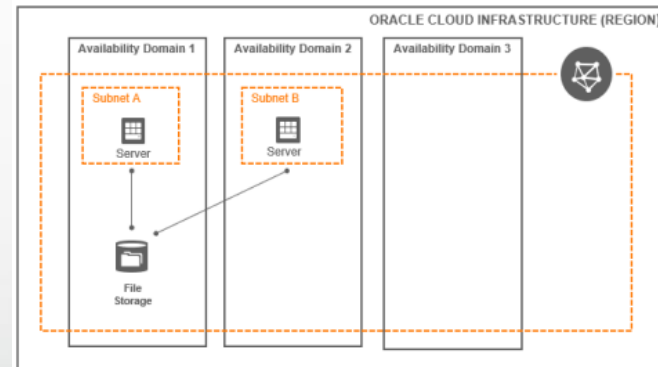
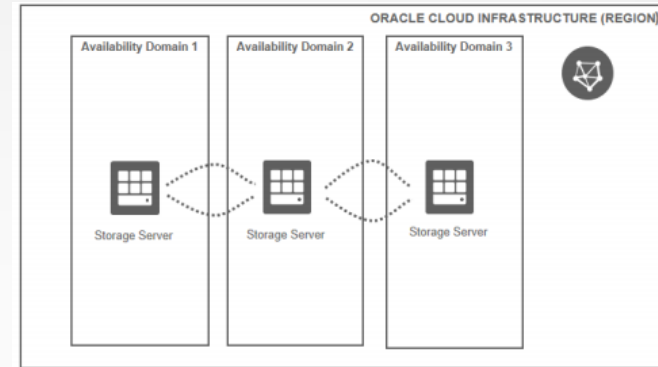
## HA: Local NVMe

Multiple copies of data are stored across three ADs. Data Integrity is actively maintained using checksums. Corrupt data is auto detected and auto healed

## HA: File Storage

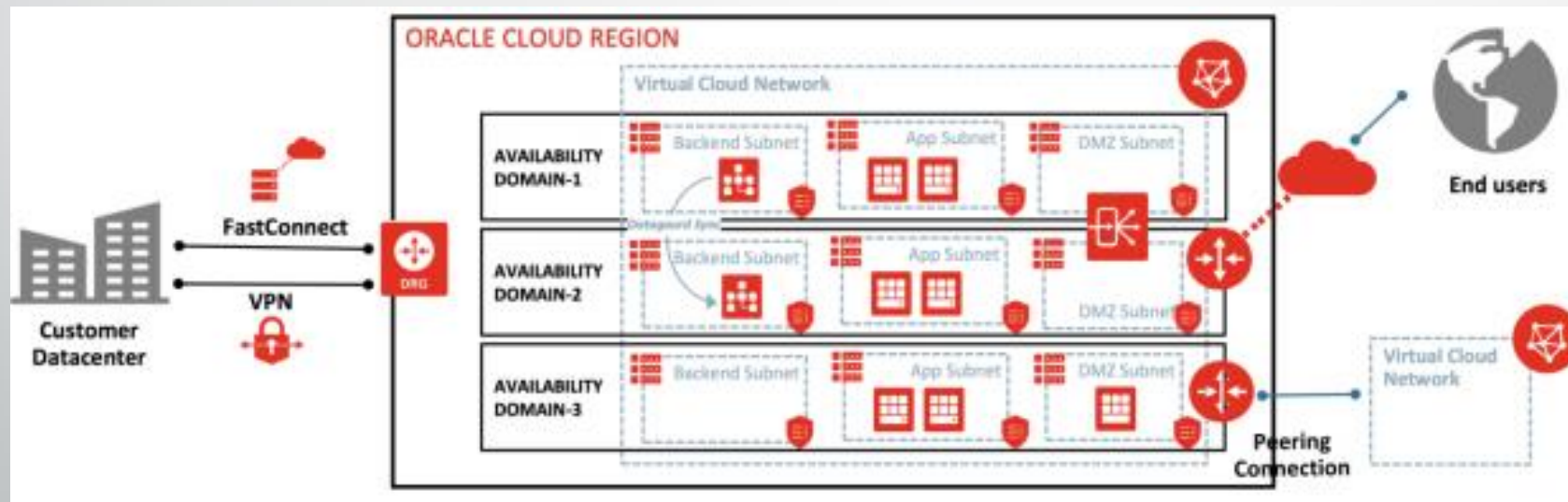
➤ Manually copy (rsync) asynchronously to another file system in a different AD

## Distribute File System: GlusterFS

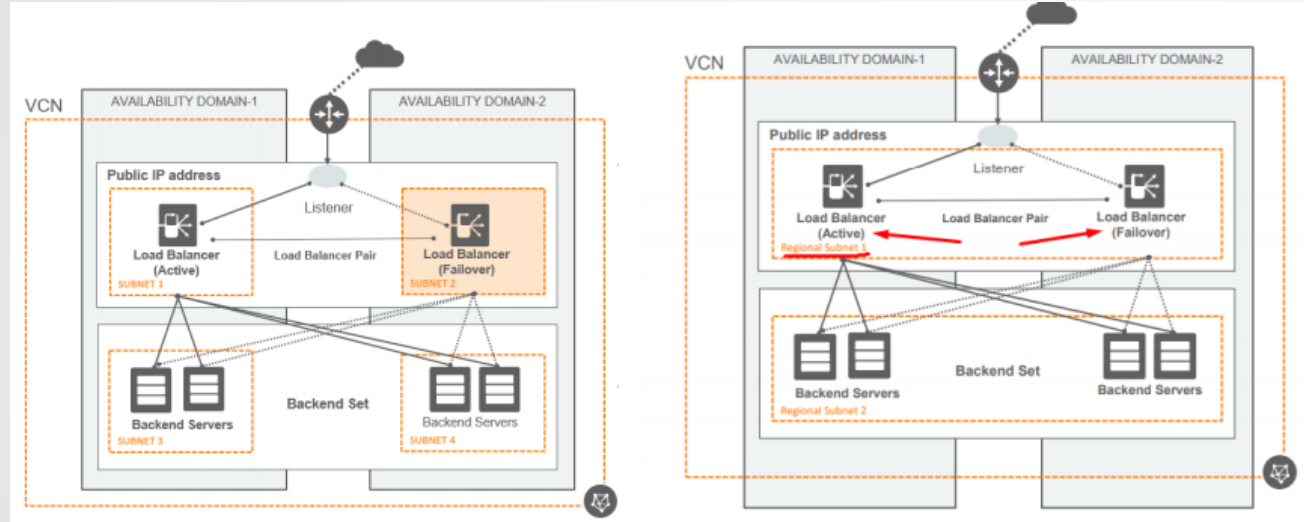


## HA: VCN

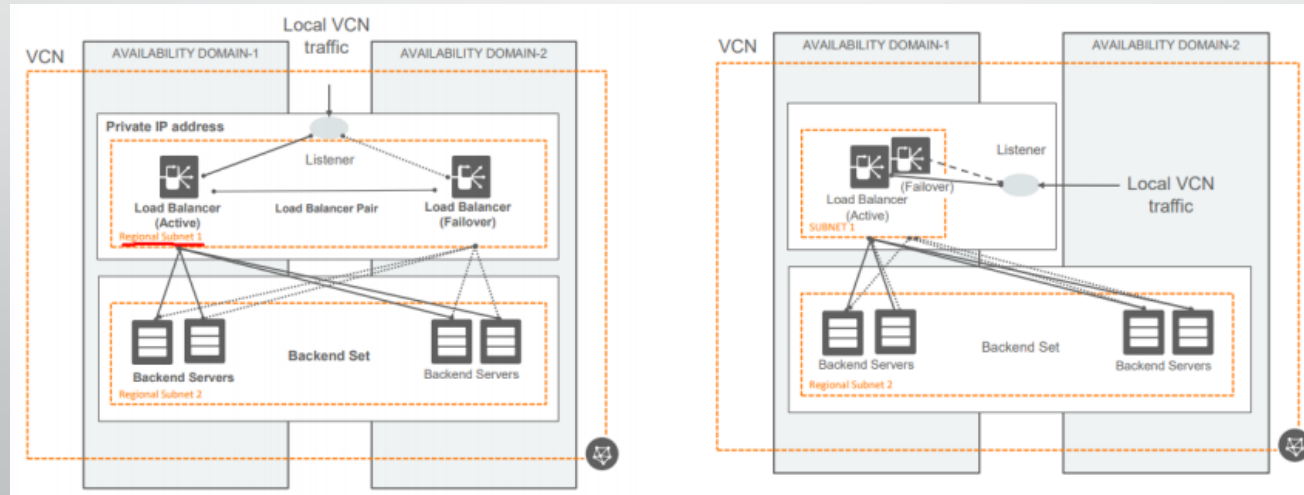
- VCN Resides within a single Region but can cross multiple Availability Domain (AD)
- Subnets in Different AD for Applications
- Regional Subnets Recommended by Oracle.
- Scope of Various Network Services



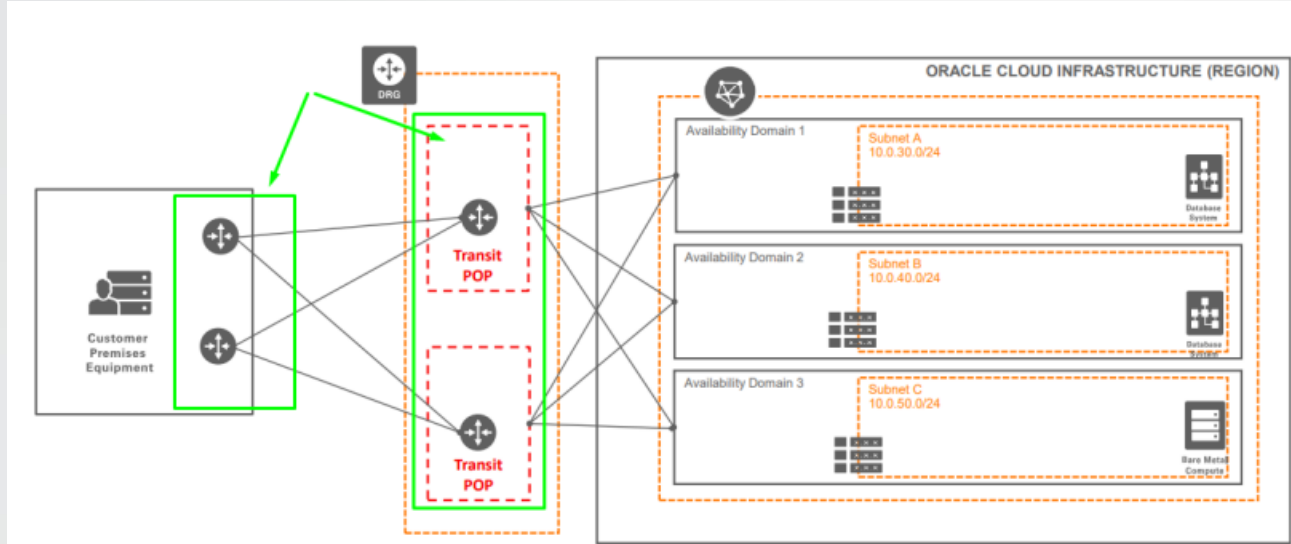
## HA: Public Load Balancer



## HA: Private Load Balancer

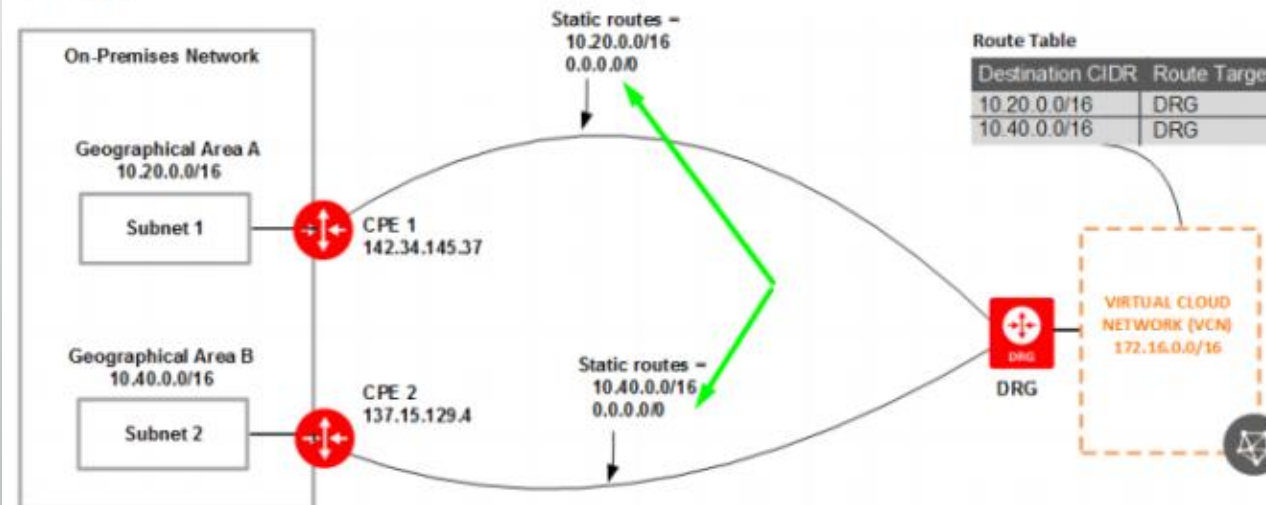


## HA: IPSec VPN Tunnel



## HA: IPSec VPN Tunnel (Routes)

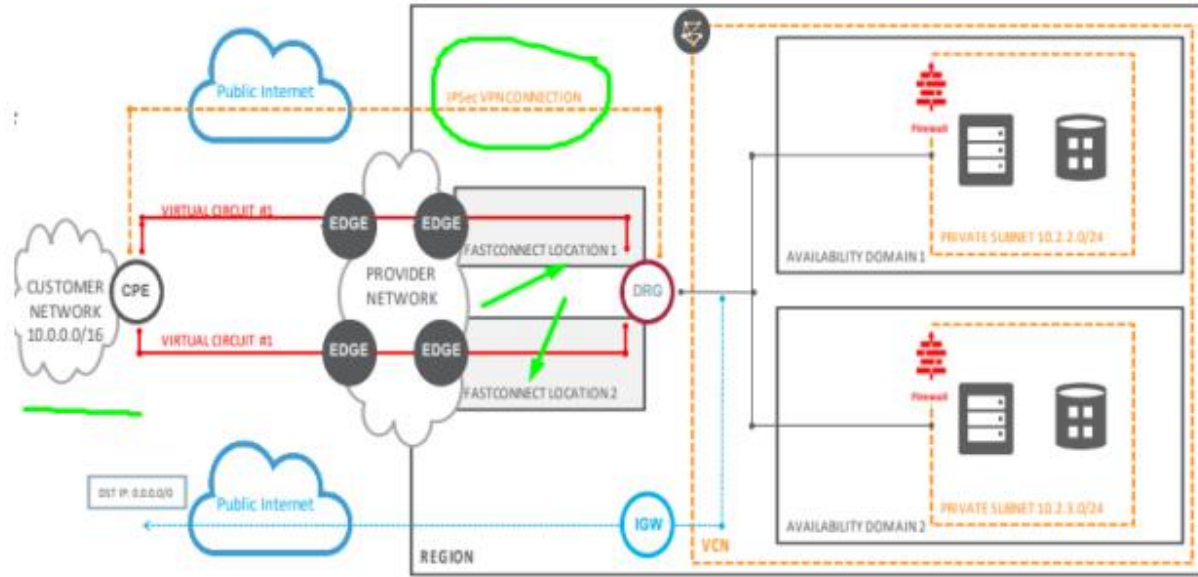
Broad CIDR for high availability and flexibility to your network design



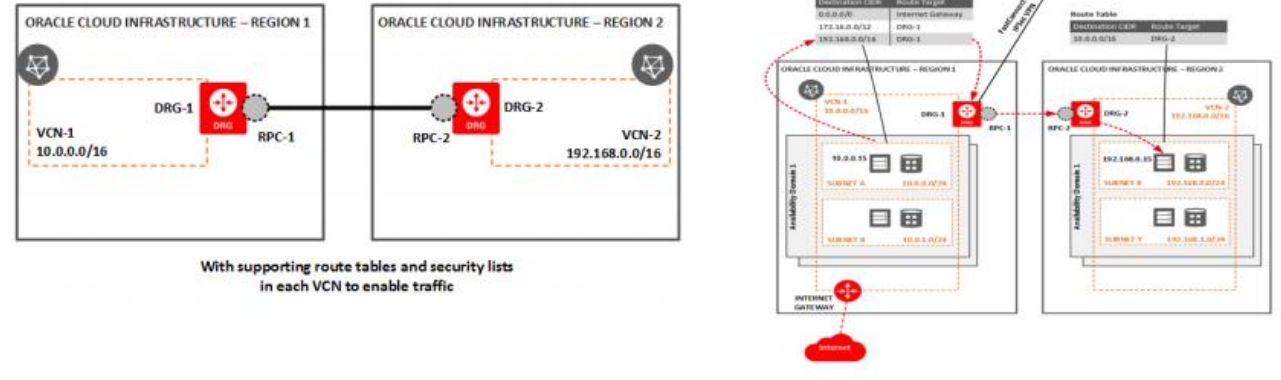


# HA: Fastconnect

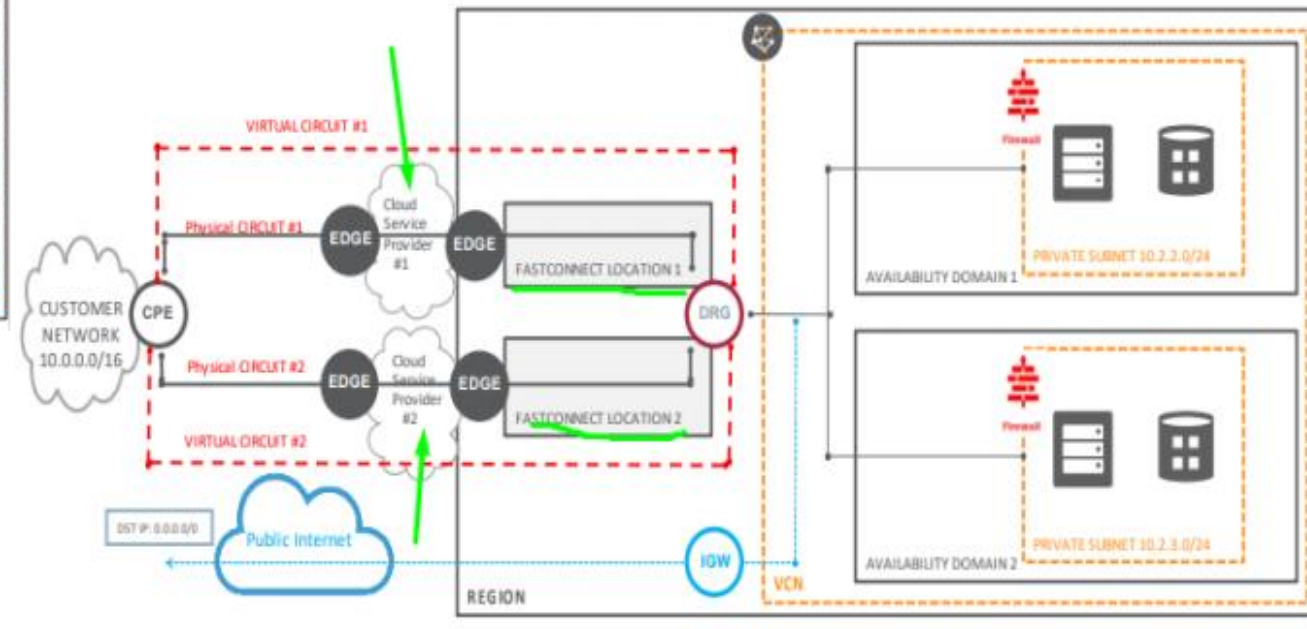
## Service Redundancy



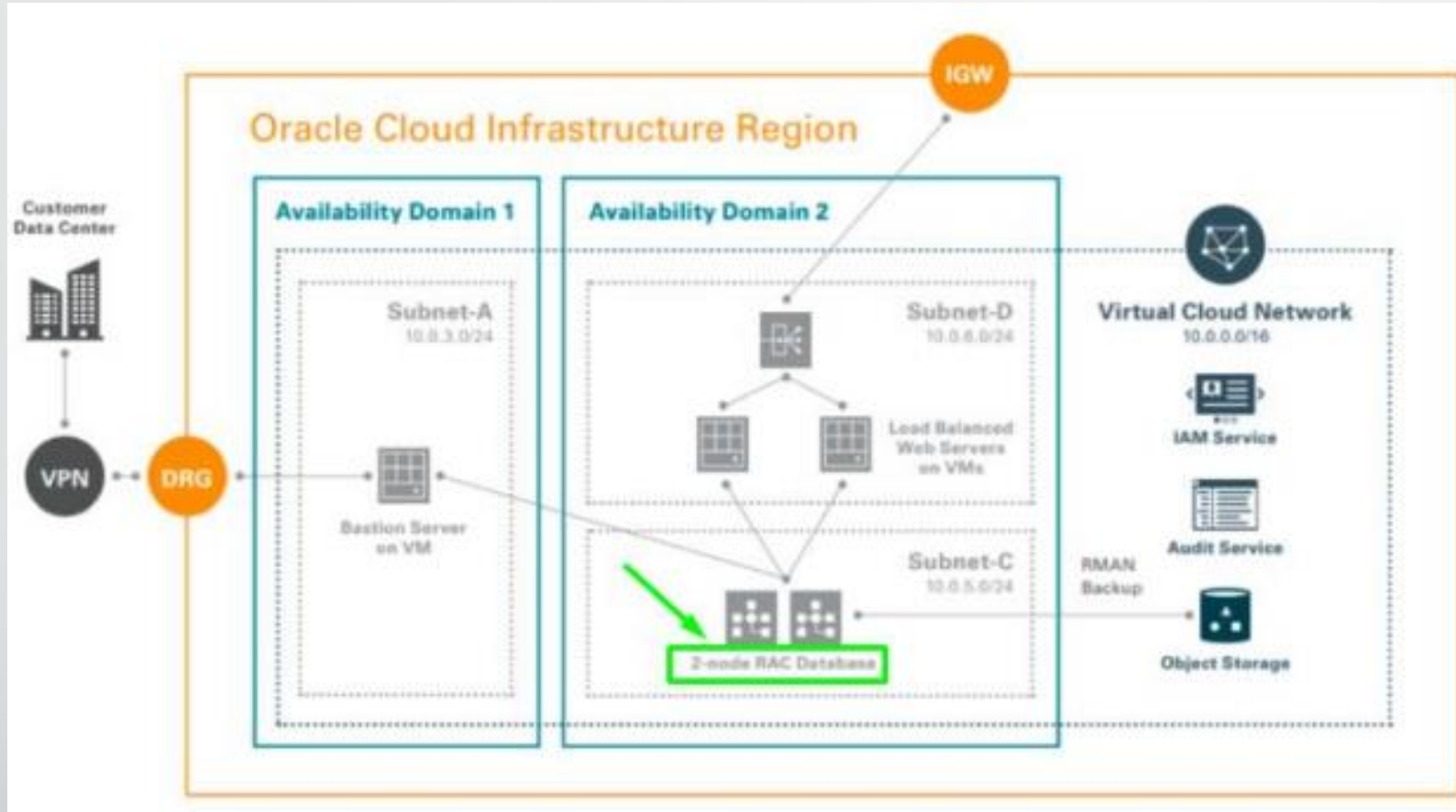
## Remote VCN Peering for DR



## Partner or provider redundancy

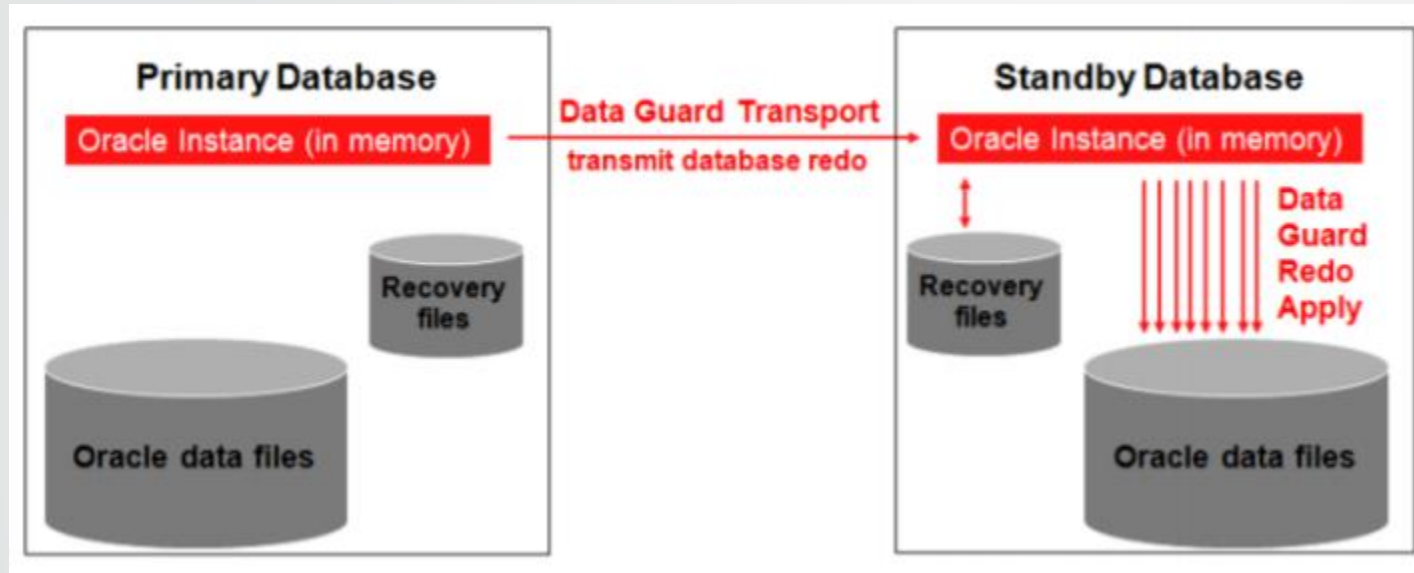


# Real Application Cluster (RAC) Active-Active HA & ADG options

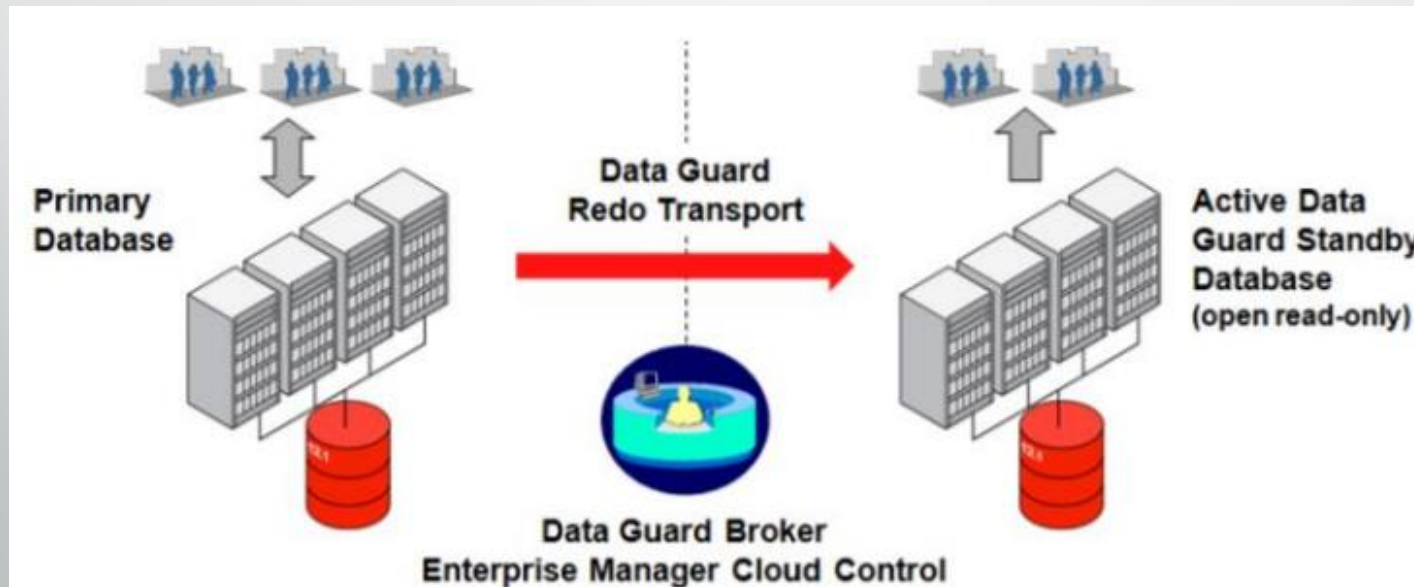


Cloud Infrastructure	Backup/Restore Options	RAC	ADG	Replication across ADs/Regions
OCI (BM)	Backup to OCI Object Storage (manual/automatic)		✓	Across ADs Across Regions via VCN peering
OCI (VM) (with SI or RAC)		✓*	✓	
Exa-OCI (x6/x7)	Automatic backup copies across Availability Domains (ADs)	✓	✓	

## Oracle Data Guard: Standby



## Active Data Guard



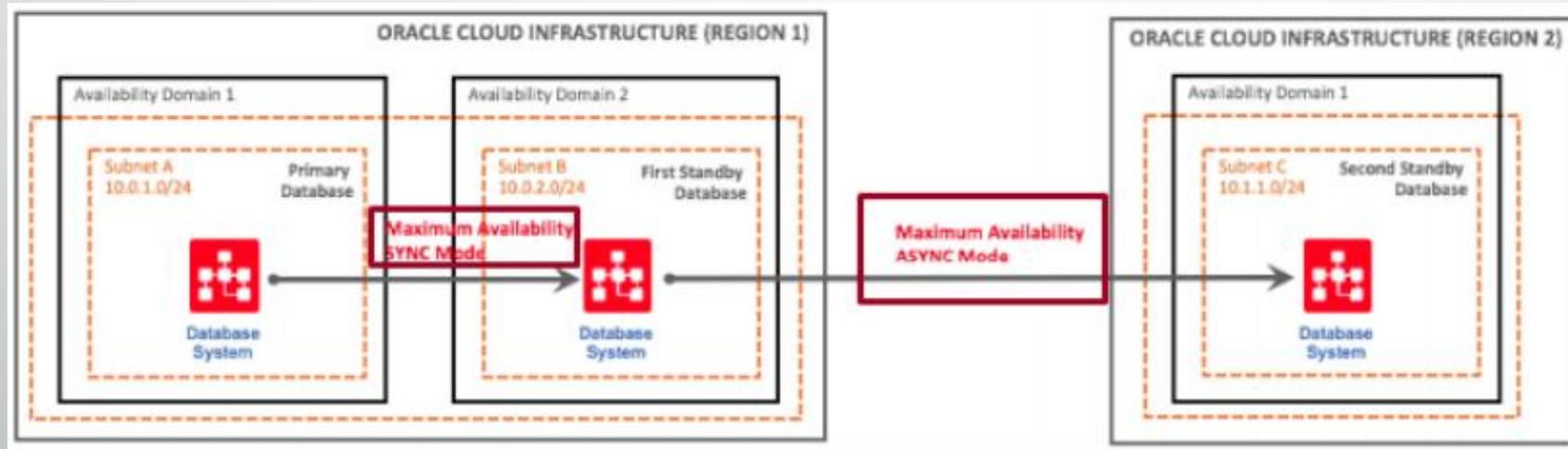
➤ Use the Maximum Availability mode in SYNC mode between AD (same region)

➤ Maximum Availability mode in ASYNC mode between two regions.

➤ Follow daisy-chain mode

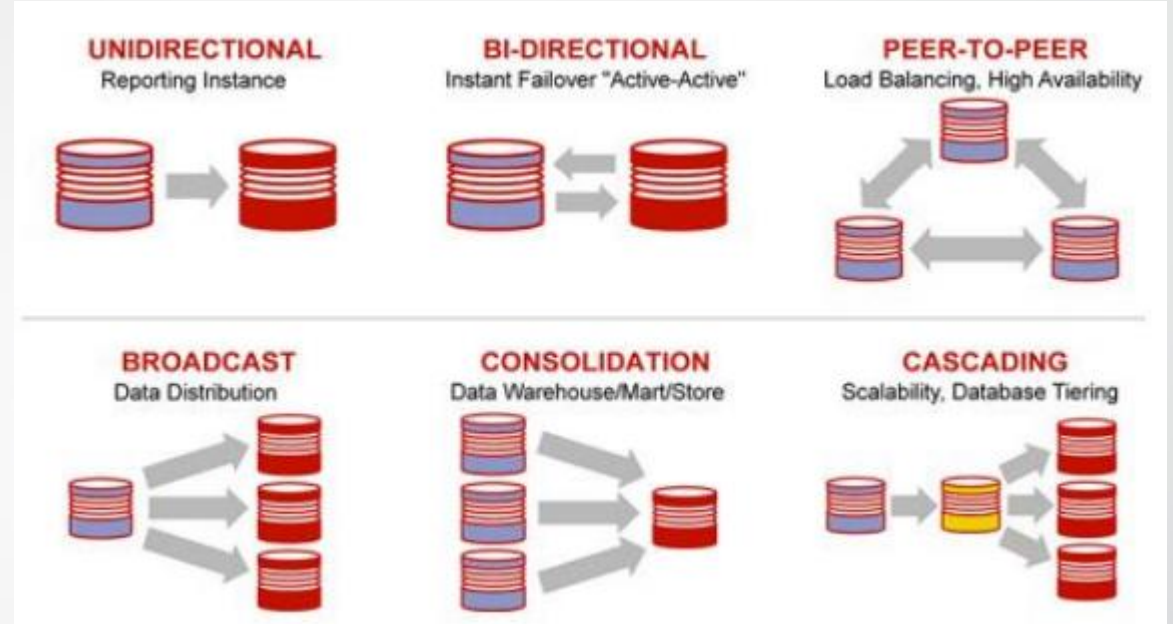
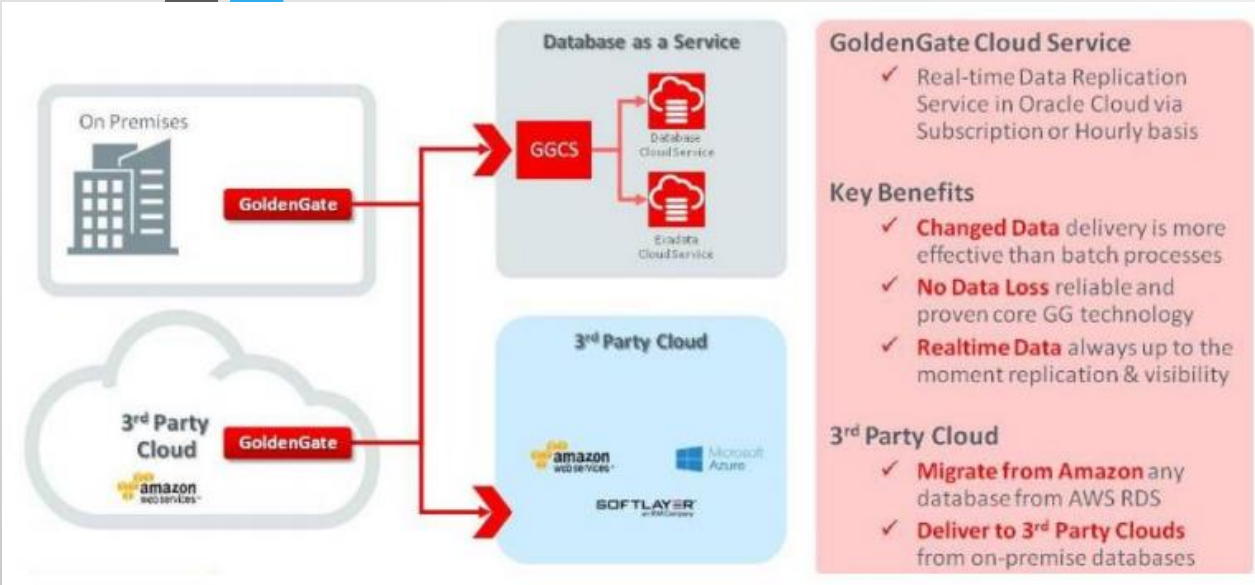
## Oracle Data Guard: Standby

- No data loss within a region.
- No overhead on the production database to maintain standbys in another region.
- Option to configure lagging on the DR site
- Option to configure multiple standbys in different regions



# Oracle Golden Gate: Replication

## Modes



Data Guard between two regions to provide a zero-data-loss solution

