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, timing, and pricing of any features or functionality described for Oracle's products may change and remains at the sole discretion of Oracle Corporation.

High Availability and Disaster Recovery

Level 300

Flavio Pereira

Changbin Gong
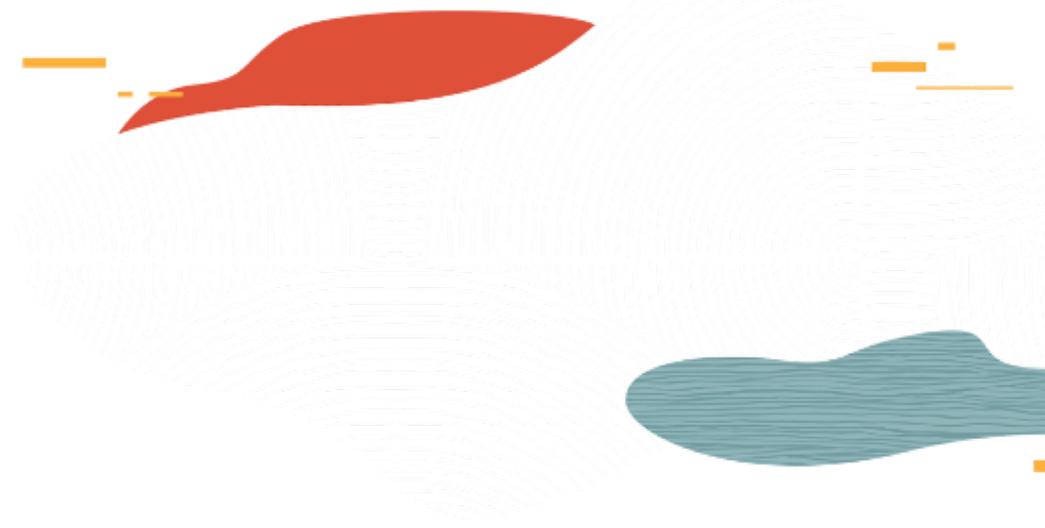
Oracle Cloud Infrastructure

October 2019

Objectives

After completing this lesson, you should be able to:

- Describe High Availability and Disaster Recovery

- How to Leverage OCI for HA and DR

- HA and DR features for OCI

- High Availability and disaster Recover scenarios
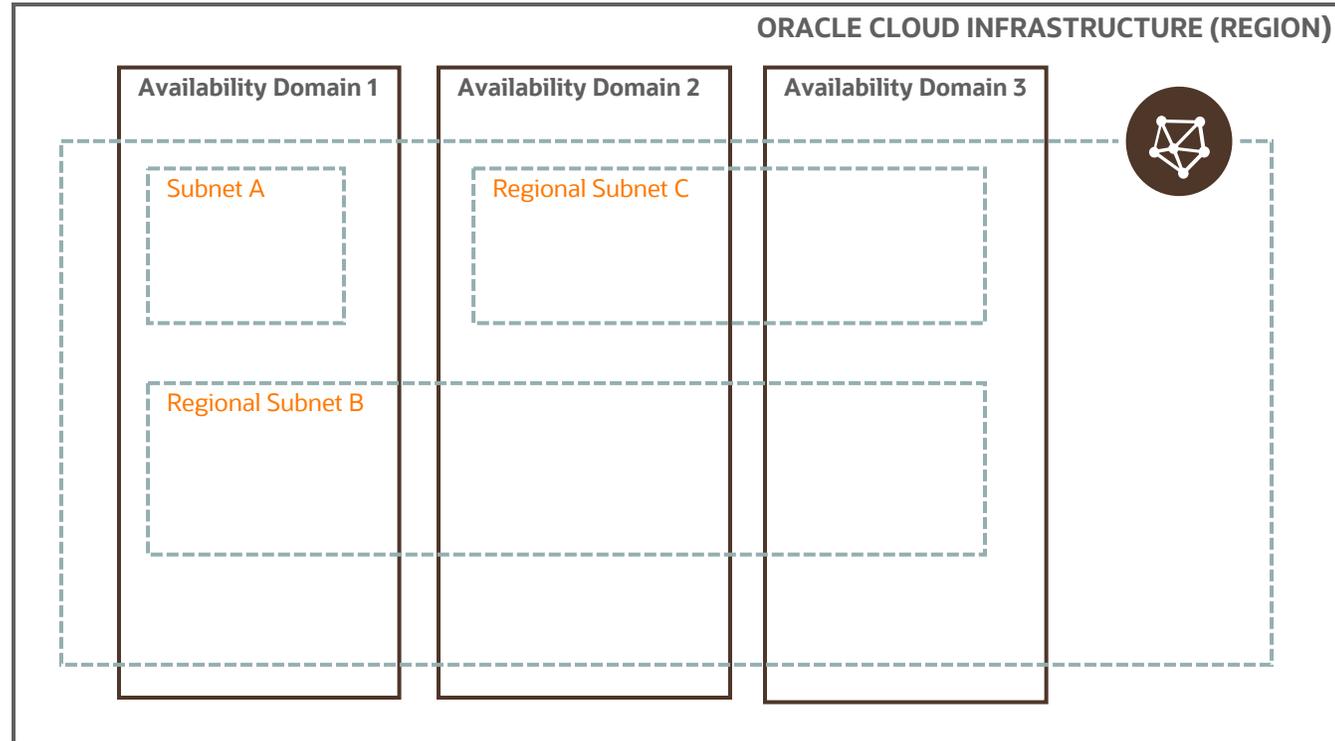
High Availability

High Availability Concepts

- 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.
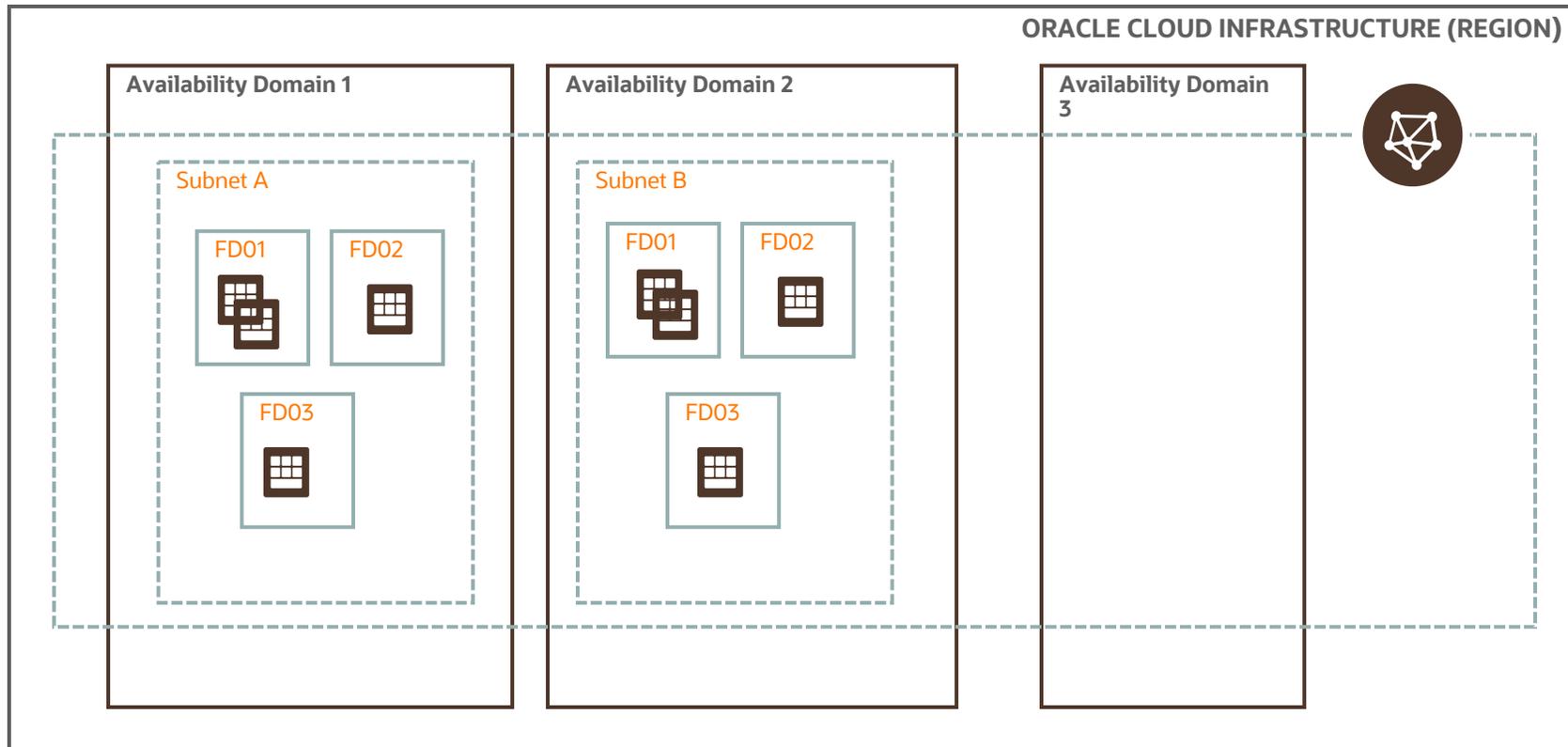
Availability Domains

- 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 availability domain is unlikely to impact the availability of the others.

ORACLE CLOUD INFRASTRUCTURE (REGION)

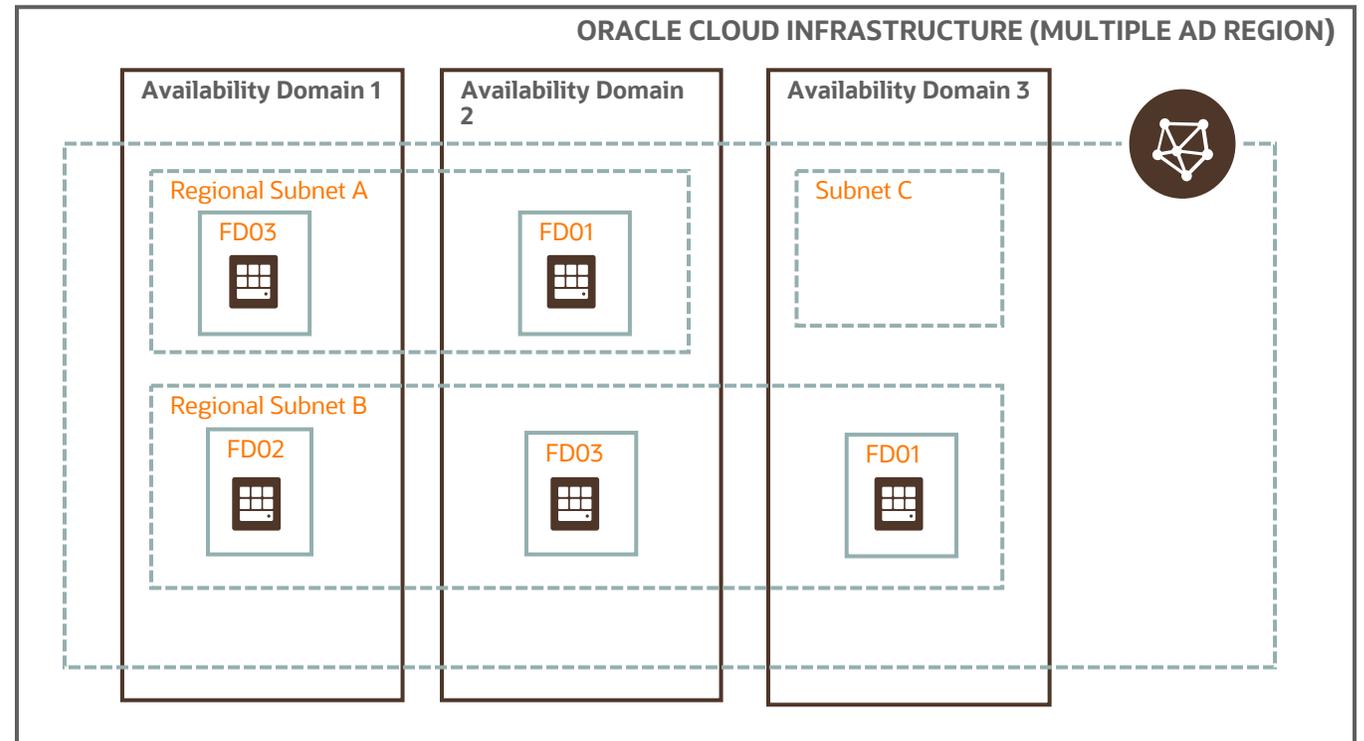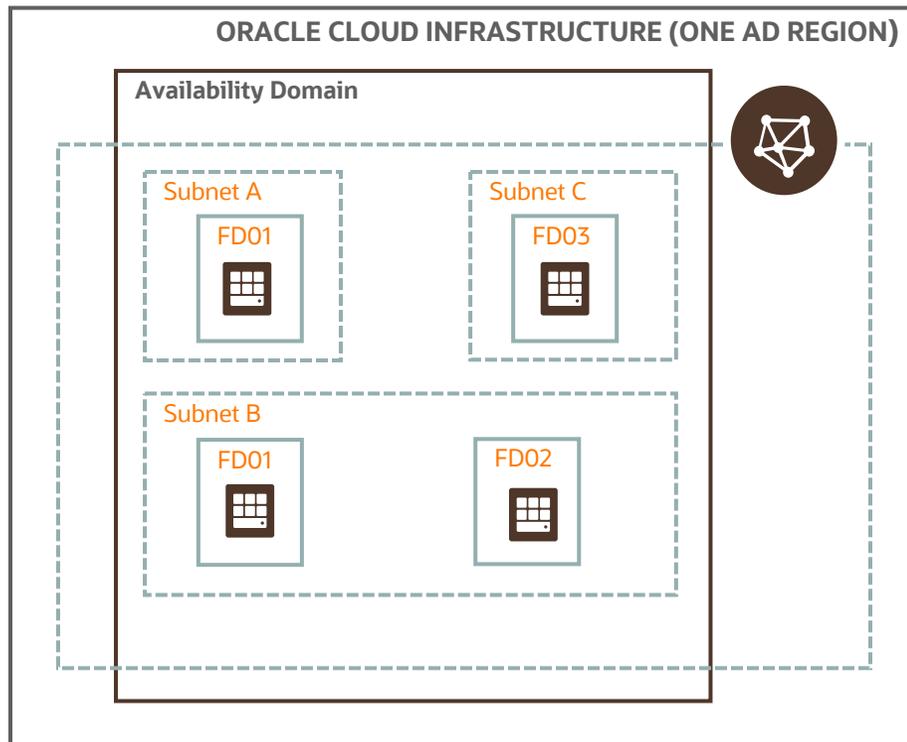| Availability Domain 1	Availability Domain 2	Availability Domain 3
Subnet A	Regional Subnet C	
Regional Subnet B		

Fault Domains

- Fault Domains (FD) enable you to distribute your instances so that they **are not on the same physical hardware** within a single AD. Each AD will have 3 FDs.
- Fault domains provide high availability for application resources within an availability domain by protecting against unexpected hardware failures and maintenance updates on the compute hardware.

ORACLE CLOUD INFRASTRUCTURE (REGION)

Availability Domain 1

Subnet A

FD01 FD02

FD03

Availability Domain 2

Subnet B

FD01 FD02

FD03

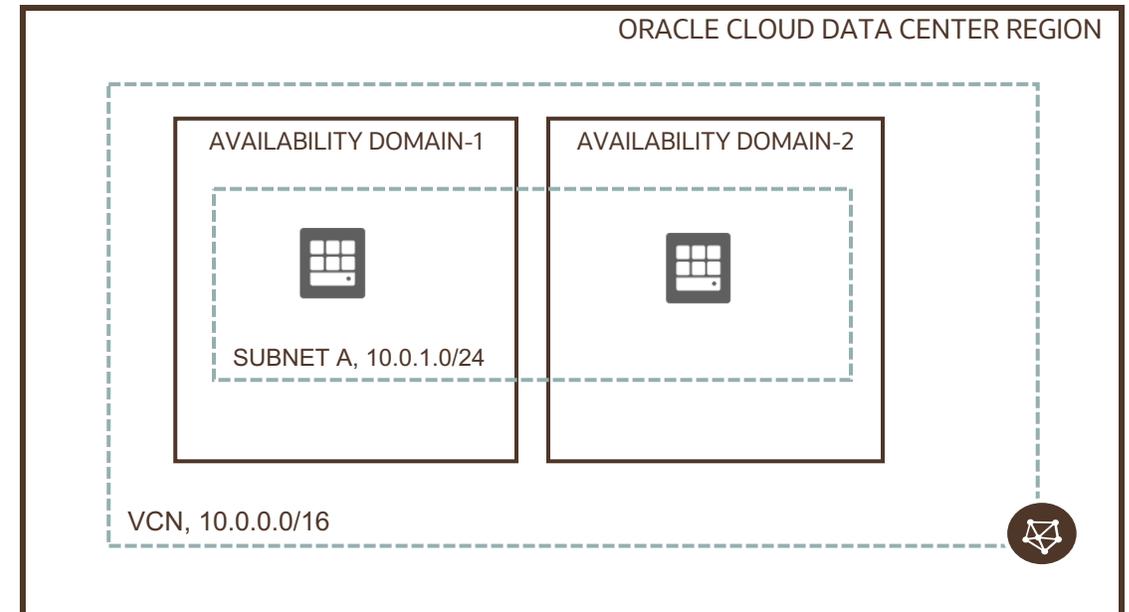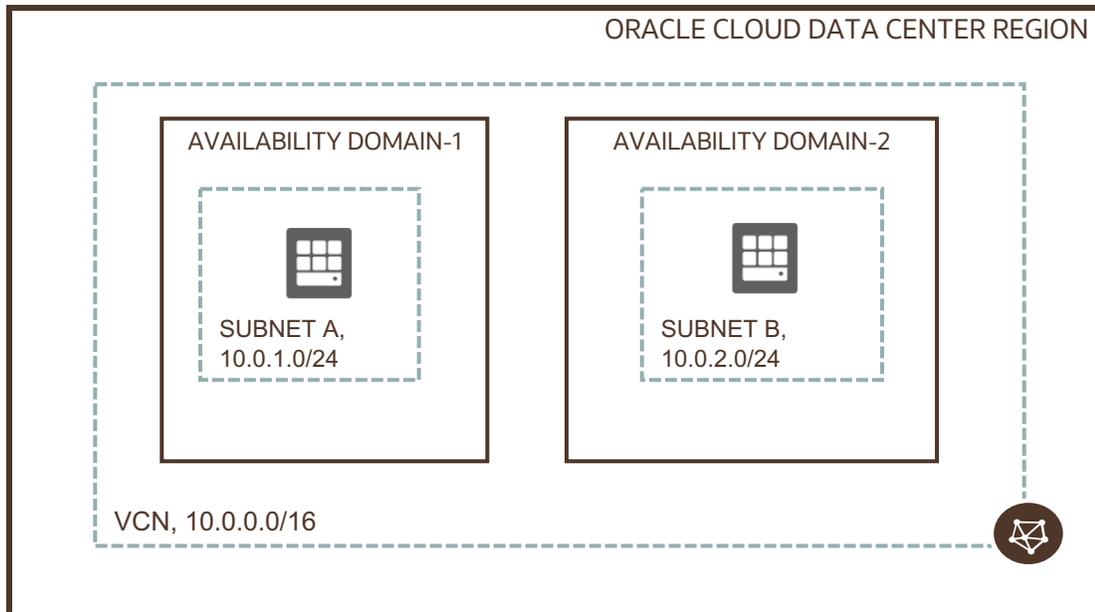**Availability Domain 3**

Avoid single points-of-failure

One of the key principles of designing high availability solutions is to **avoid single point of failure**. We recommend designing your architecture to deploy instances that perform the same tasks **in different fault domains for one AD regions and if possible**, in different availability domains for multiple AD regions. This design removes a single point of failure by introducing redundancy.
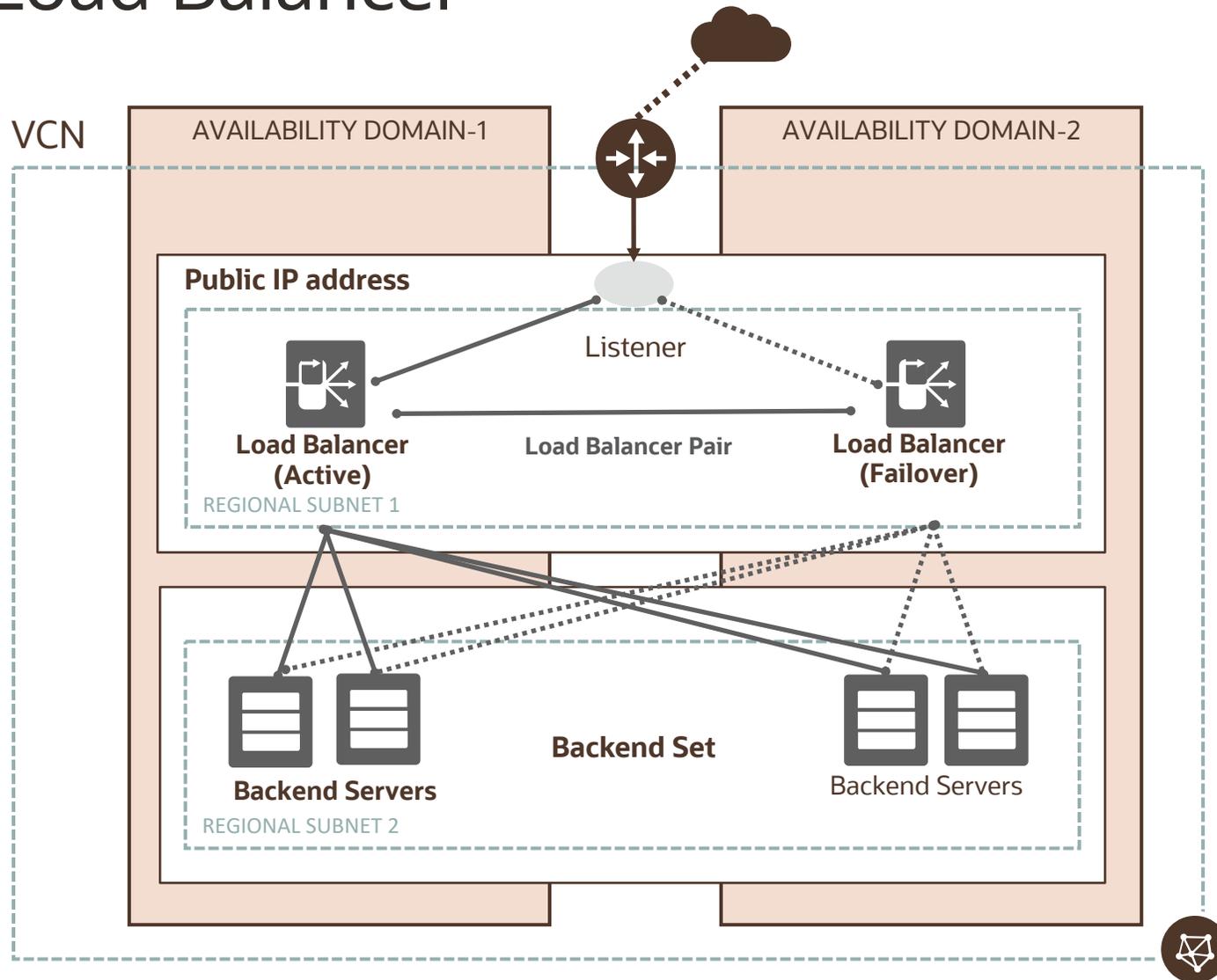
Regional and AD Specific Subnets

- Each subnet in a VCN exists in a single availability domain (**AD Specific Subnets**) or in multiple availability domains (**Regional Subnets**) and consists of a contiguous range of IP addresses that do not overlap with other subnets in the cloud network.
- You can not change the size of the subnet after it is created, so it's important to think about the size you need before creating subnets

ORACLE CLOUD DATA CENTER REGION

AVAILABILITY DOMAIN-1

SUBNET A, 10.0.1.0/24

AVAILABILITY DOMAIN-2

SUBNET B, 10.0.2.0/24

VCN, 10.0.0.0/16

ORACLE CLOUD DATA CENTER REGION

AVAILABILITY DOMAIN-1

SUBNET A, 10.0.1.0/24

AVAILABILITY DOMAIN-2

VCN, 10.0.0.0/16

Load Balancer

- **Load Balancer:** Load Balancing service improves resource utilization, facilitates scaling, and helps ensure high availability. It supports routing incoming requests to various backend sets based on virtual hostname, path route rules, or combination of both. (Public and Private LB)

- **NOTE:** Private and Public Load Balancer is only Highly-available within an AD for single AD regions.

Virtual IP
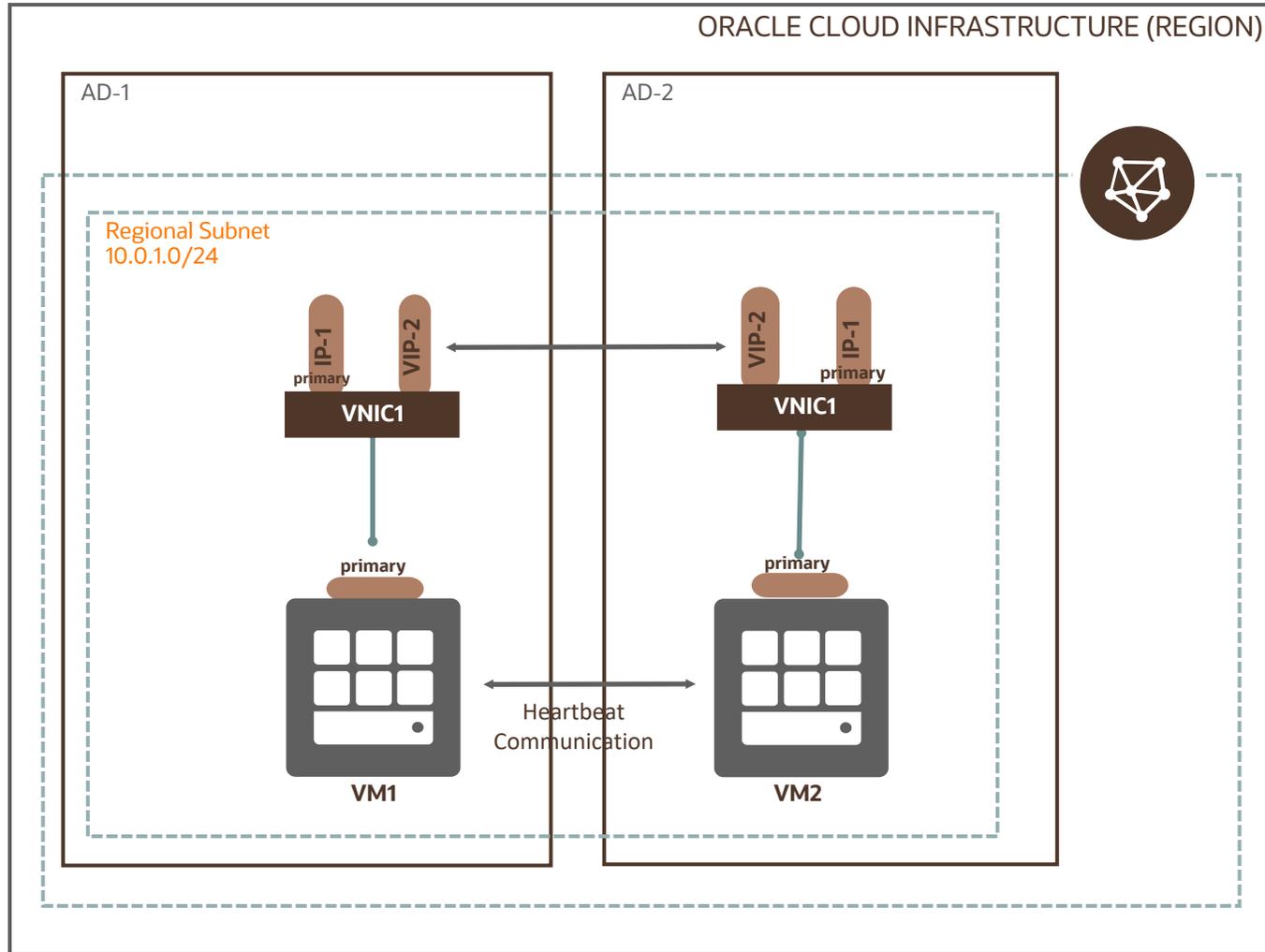
- **Virtual IP:** A Compute instance can be assigned a secondary private IP address. If the VM1 has problems, the Virtual IP (VIP-2) will be reassign to VM2 instance in the same subnet to achieve instance failover.
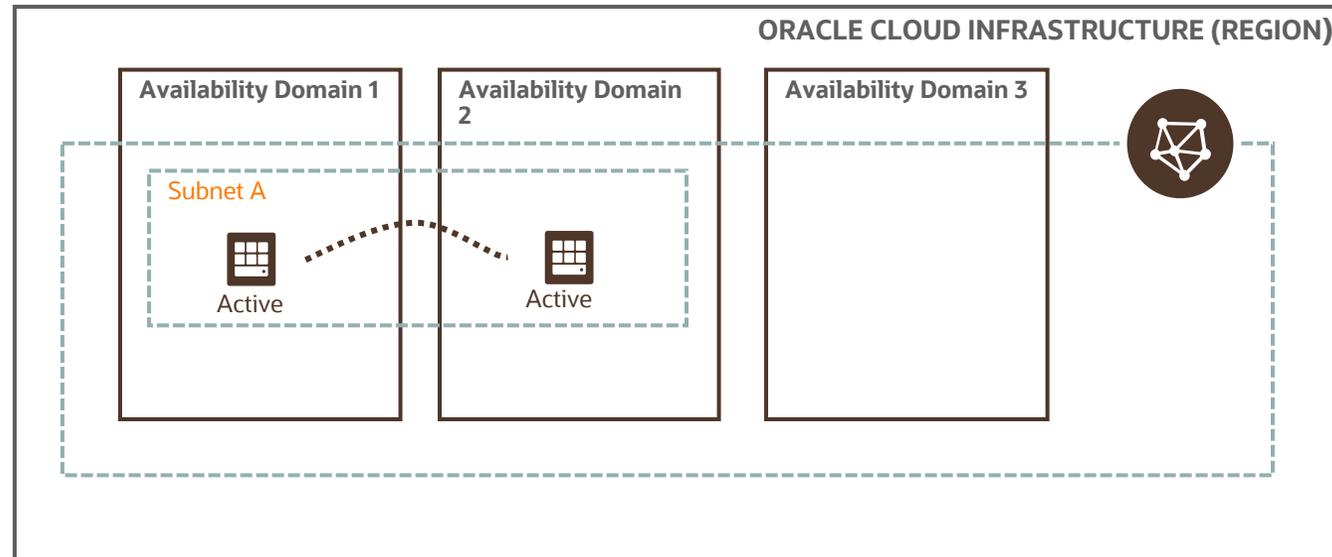
Compute

Depending on your system or application requirements, you can implement this architecture redundancy in either standby or active mode:

- **Standby mode**: a secondary or standby component runs side-by-side with the primary component. When the primary component fails, the standby component takes over. Standby mode is typically used for applications that need to maintain their states.
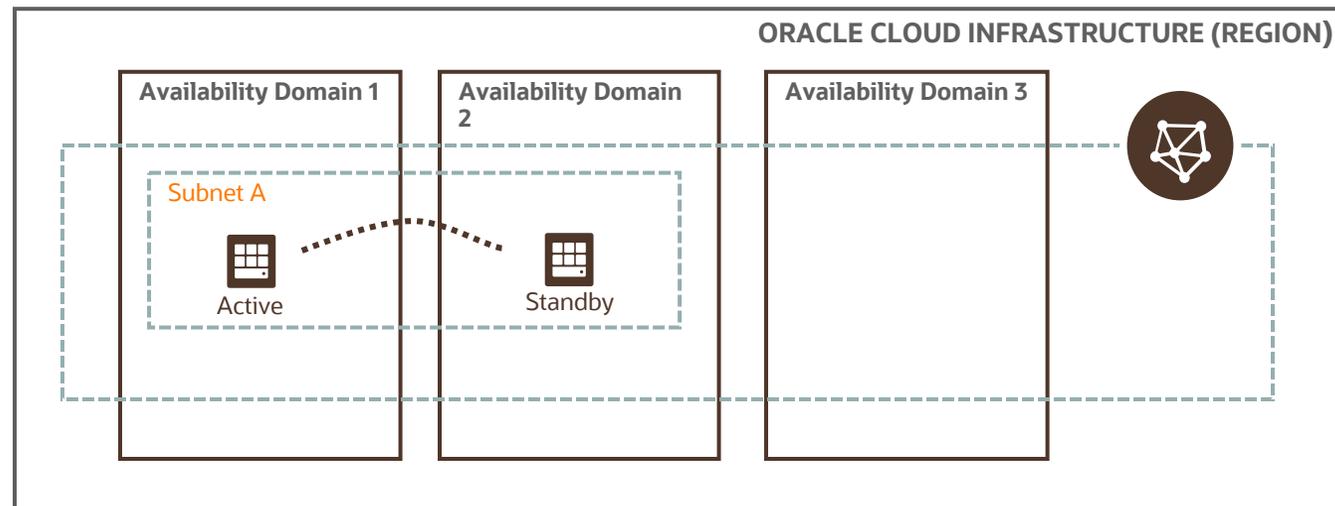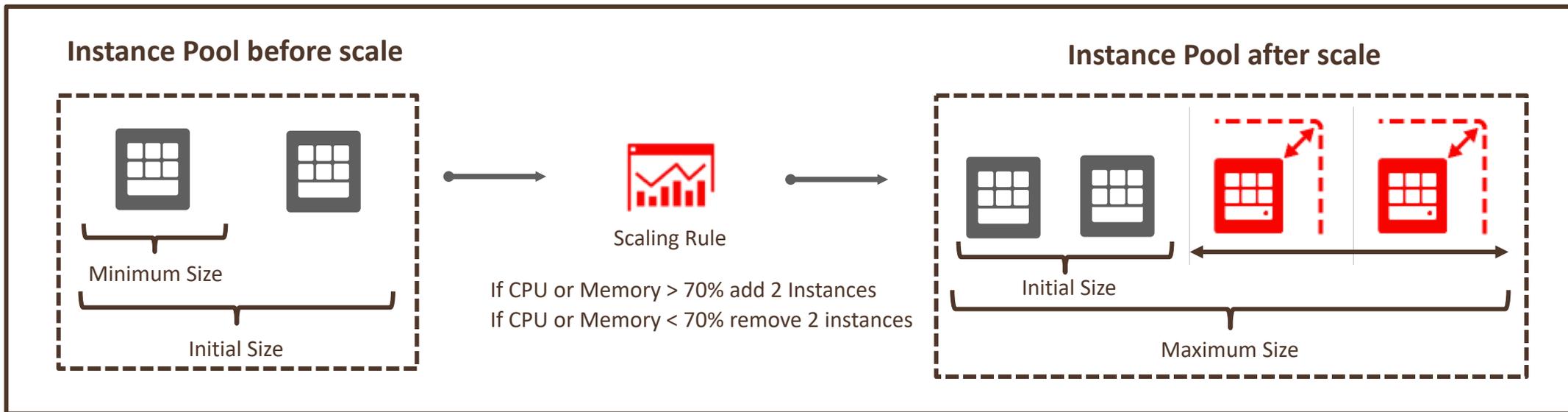
Compute

- **Active/Active mode**: all components are actively participating in performing the same tasks. When one of the components fails, the related tasks are simply distributed to another component. Active mode is typically used for stateless applications.

ORACLE CLOUD INFRASTRUCTURE (REGION)

Availability Domain 1	Availability Domain 2	Availability Domain 3

Subnet A

Active   Active

Compute – Auto Scaling

- Avoid single point of failure
- Enables automatic adjustments for the number of Compute instances in an instance pool based on performance metrics. For instance,
  - CPU utilization
  - Memory utilization
- Recommend to attaching a load balancer to the instance pool which has autoscaling configured

Instance Pool before scale

Instance Pool after scale

Minimum Size

Initial Size

Scaling Rule

If CPU or Memory > 70% add 2 Instances
If CPU or Memory < 70% remove 2 instances

Initial Size

Maximum Size

High Availability for OCI – Connectivity

Highly available, fault-tolerant network connections are key to a well-architected system. You can choose to implement IPSec VPN connections to connect your data center to OCI or FastConnect which provides higher-bandwidth options and a more reliable and consistent networking experience compared to internet-based connections:

- **IPSec VPN:** DRG has multiple VPN endpoints so that each IPSec VPN connection consists of multiple redundant IPSec tunnels that use static routes to route traffic. To ensure high availability, you must set up VPN connection availability within your internal network to use either path when needed.

- **FastConnect:** You can either connect directly to OCI routers in provider points-of-presence (POPs) or use one of Oracle's many partners to connect from POPs around the world to their OCI Networking resources. Oracle provides features that allow you to build fault-tolerant connections, including multiple POPs per region and multiple FastConnect routers per POP.
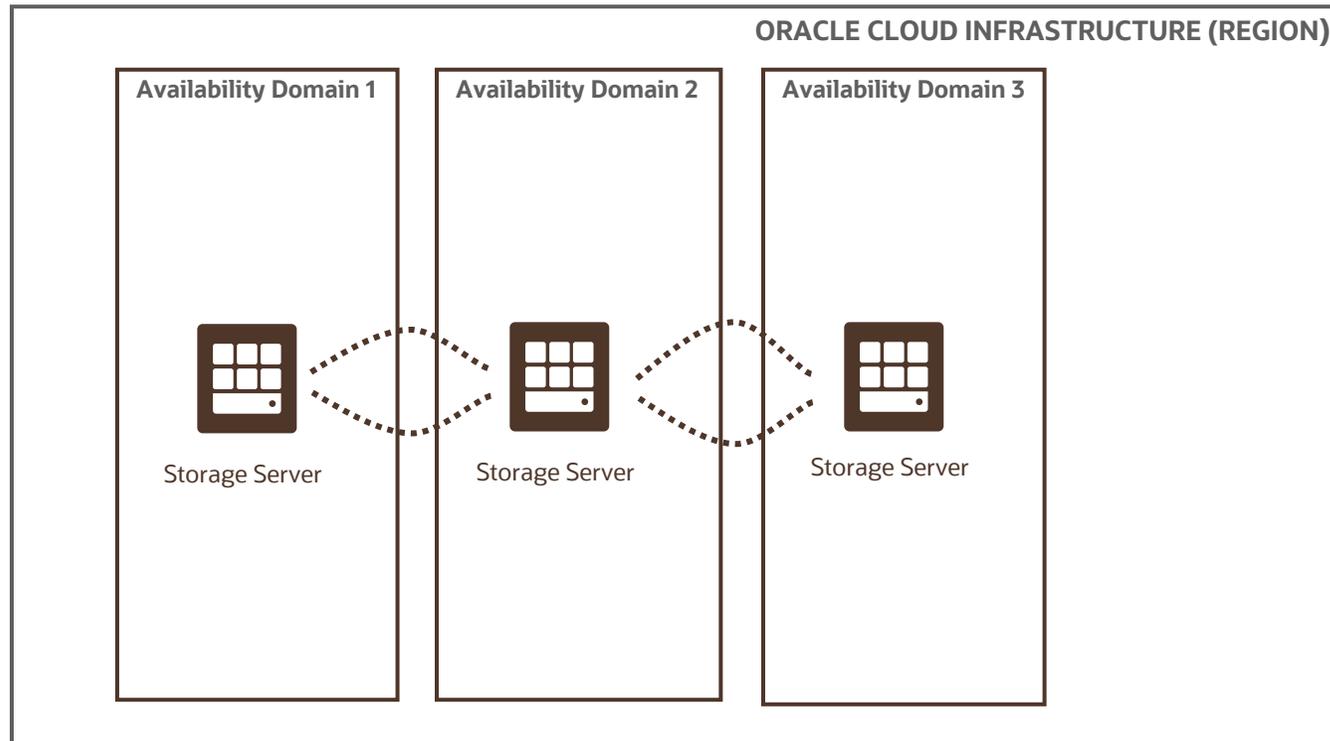
IPsec VPN Redundancy Models (Multiple CPE)
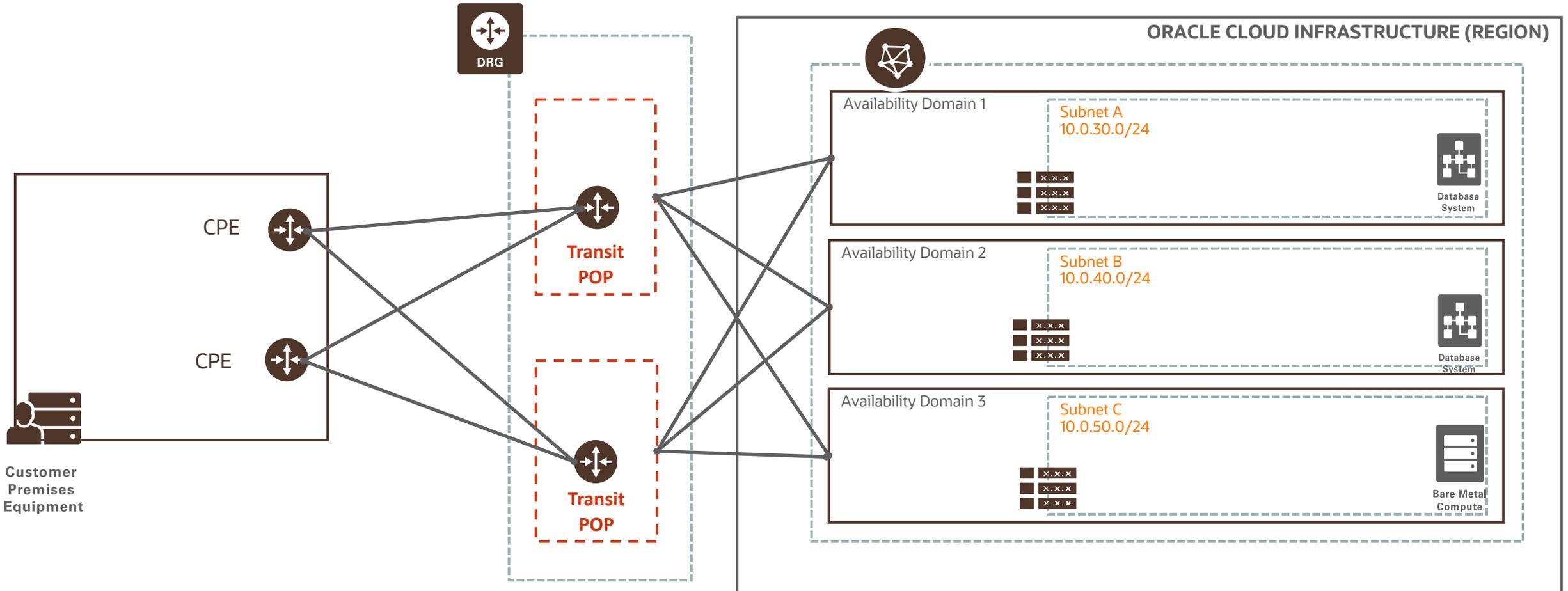
Redundant FastConnect
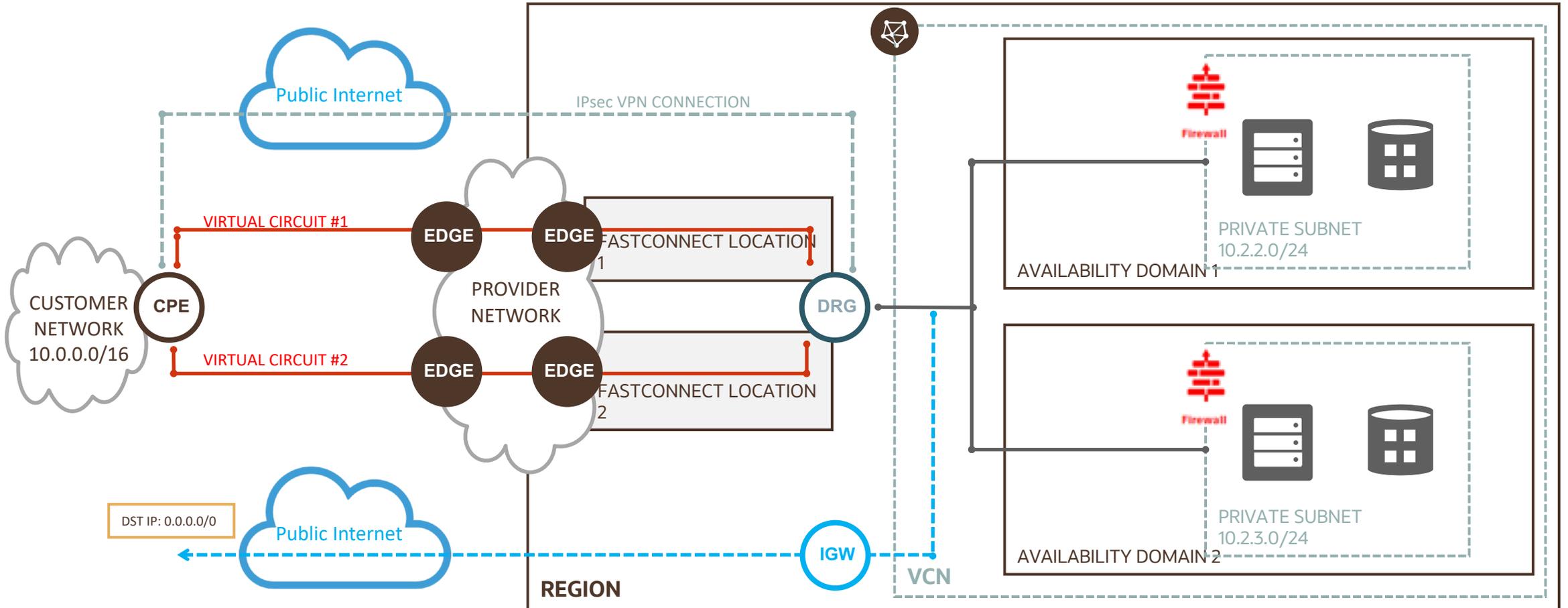
Storage

- **Object Storage:** Object Storage was designed to be highly durable. Multiple copies of the data are stored across servers in the availability domains. Data integrity is actively monitored using checksums. Corrupt data is auto detected and auto healed from redundant copies. Any loss of data redundancy is actively managed by recreating a copy of the data

ORACLE CLOUD INFRASTRUCTURE (REGION)

| Availability Domain 1	Availability Domain 2	Availability Domain 3
Storage Server	Storage Server	Storage Server

Storage

- **Block Volume:** policy-based backups to perform automatic, scheduled backups and retain them based on a backup policy. You can restore backup across availability domains
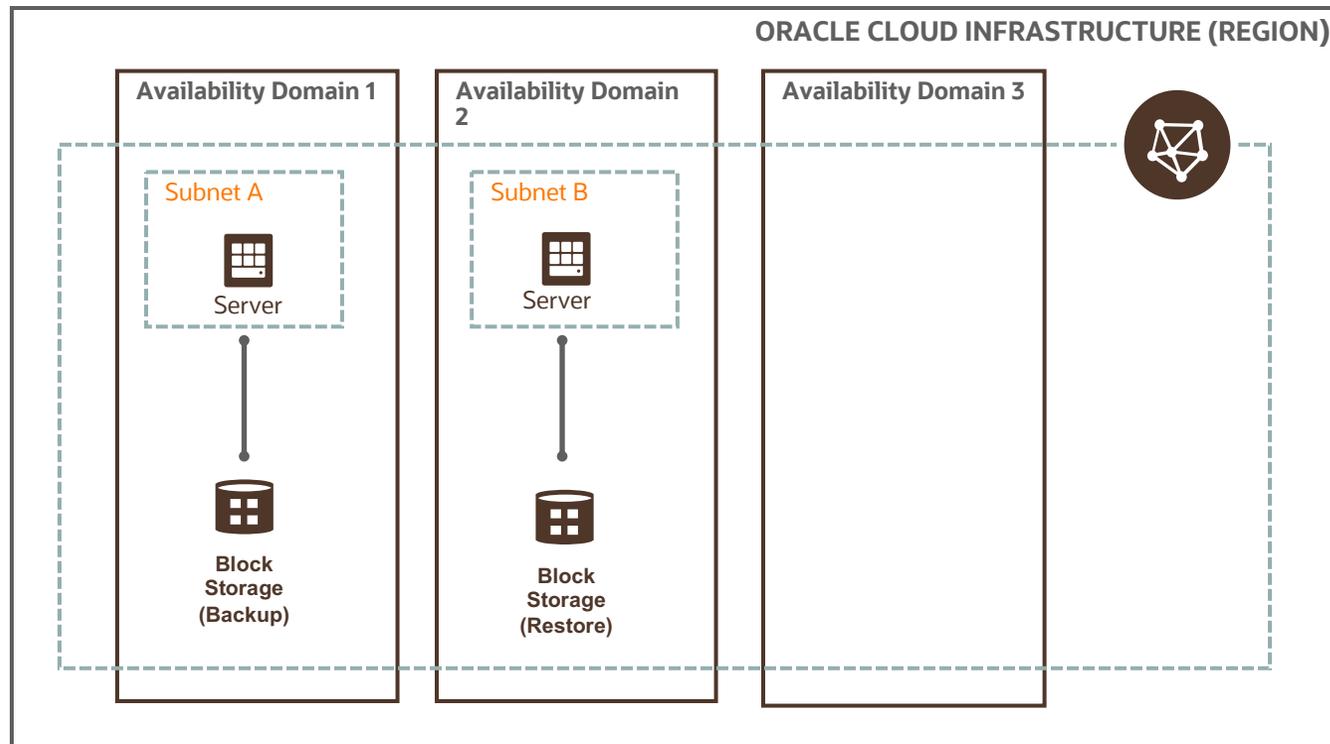
Storage

- **File Storage:** Durable, scalable, enterprise-grade network file system Ideal for Enterprise applications that need shared files (NAS)
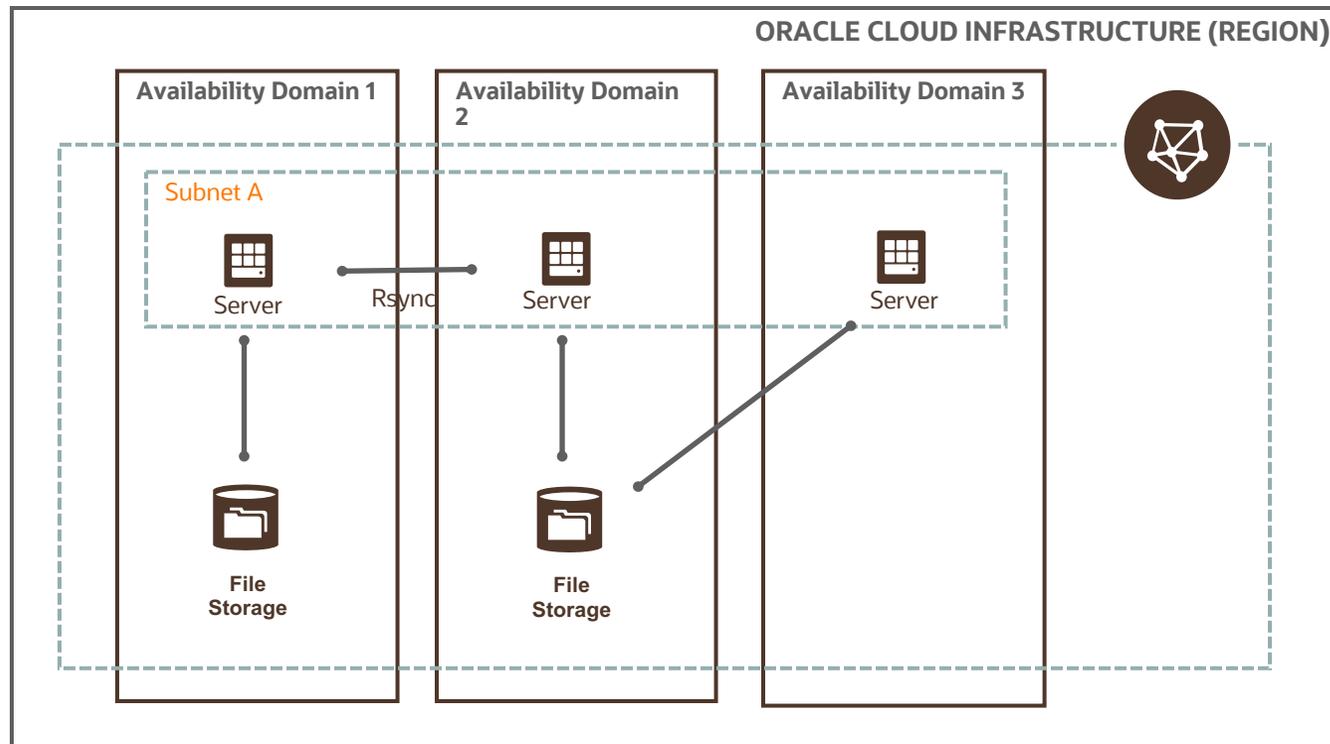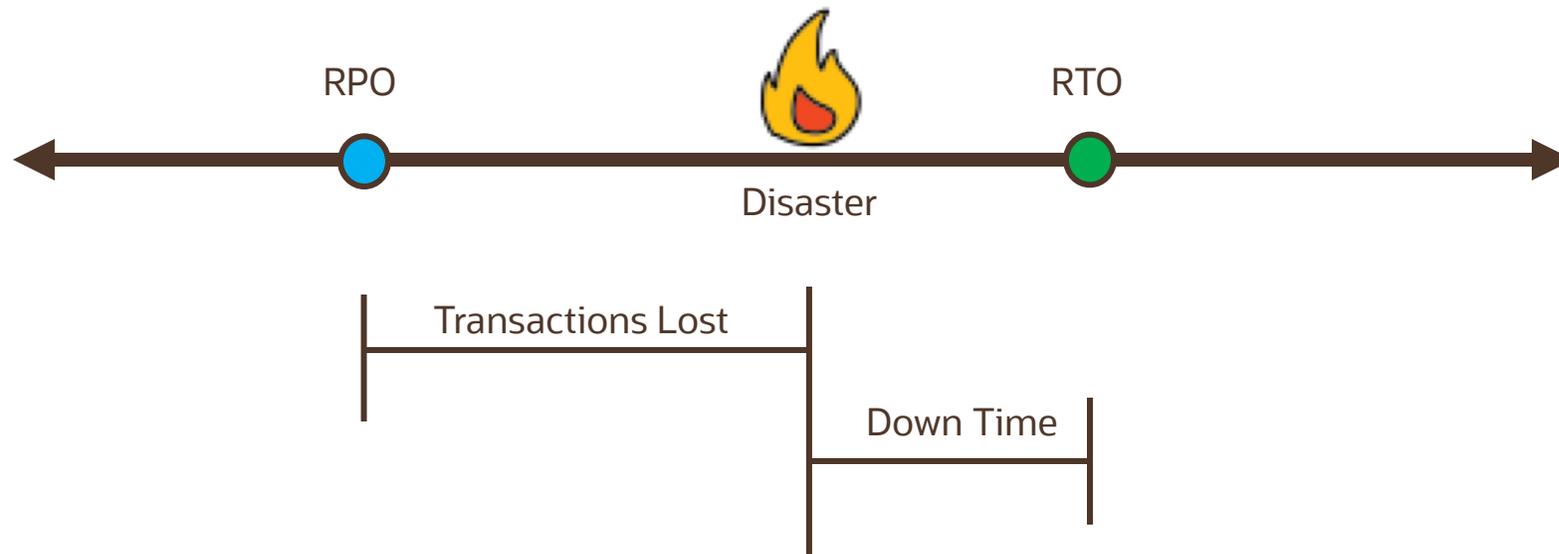
Disaster Recovery
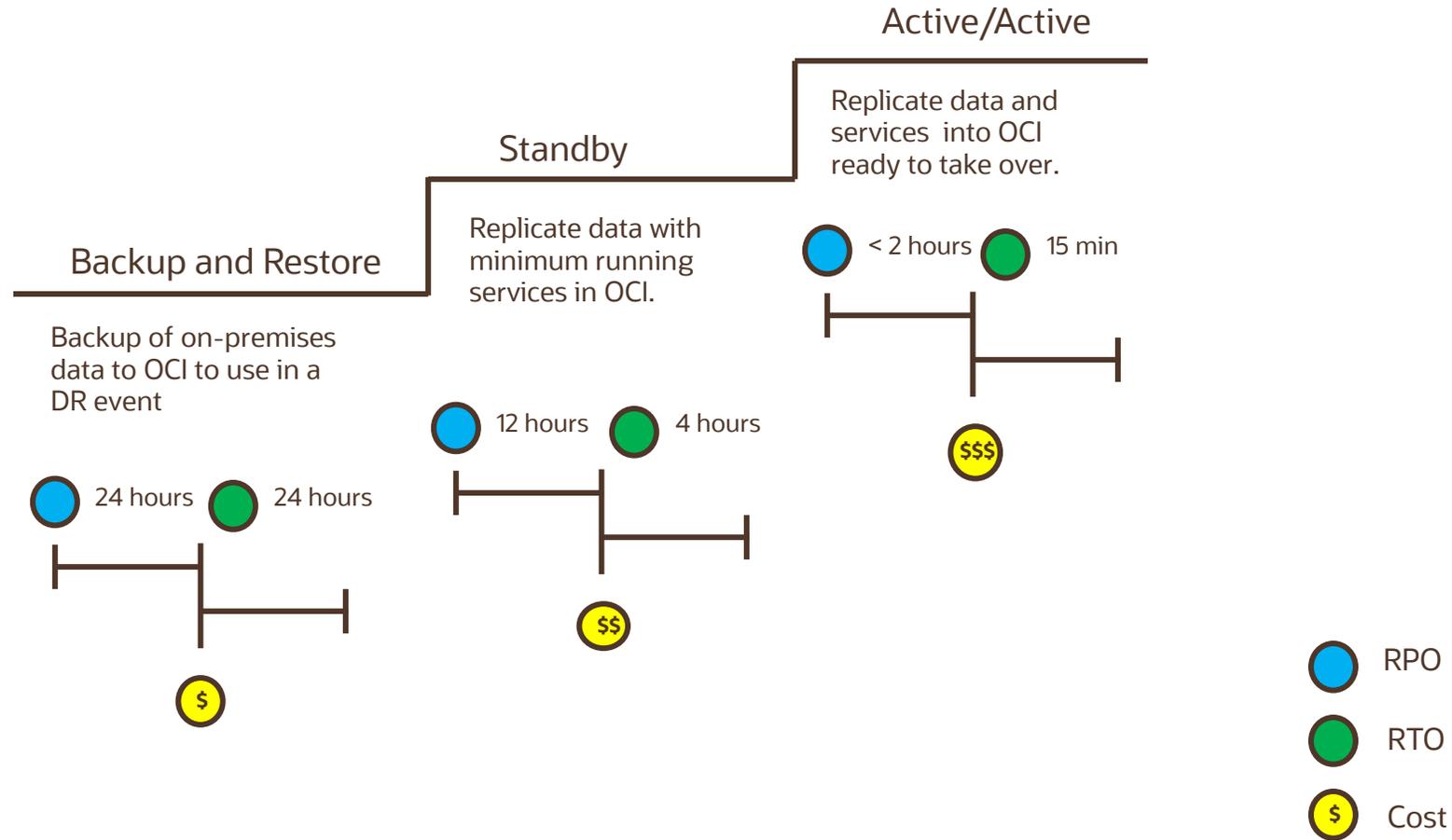
Disaster Recovery Terminology

- **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)

- In many cases, an organization may elect to use an outsourced disaster recovery provider to provide a stand-by site and systems rather than using their own remote facilities

Disaster Recovery RTO and RPO

RPO

RTO

Disaster

Transactions Lost

Down Time

Disaster Recovery Options

Active/Active

Replicate data and services into OCI ready to take over.

Standby

Replicate data with minimum running services in OCI.

Backup and Restore

Backup of on-premises data to OCI to use in a DR event

< 2 hours   15 min

$$$

12 hours   4 hours

$$

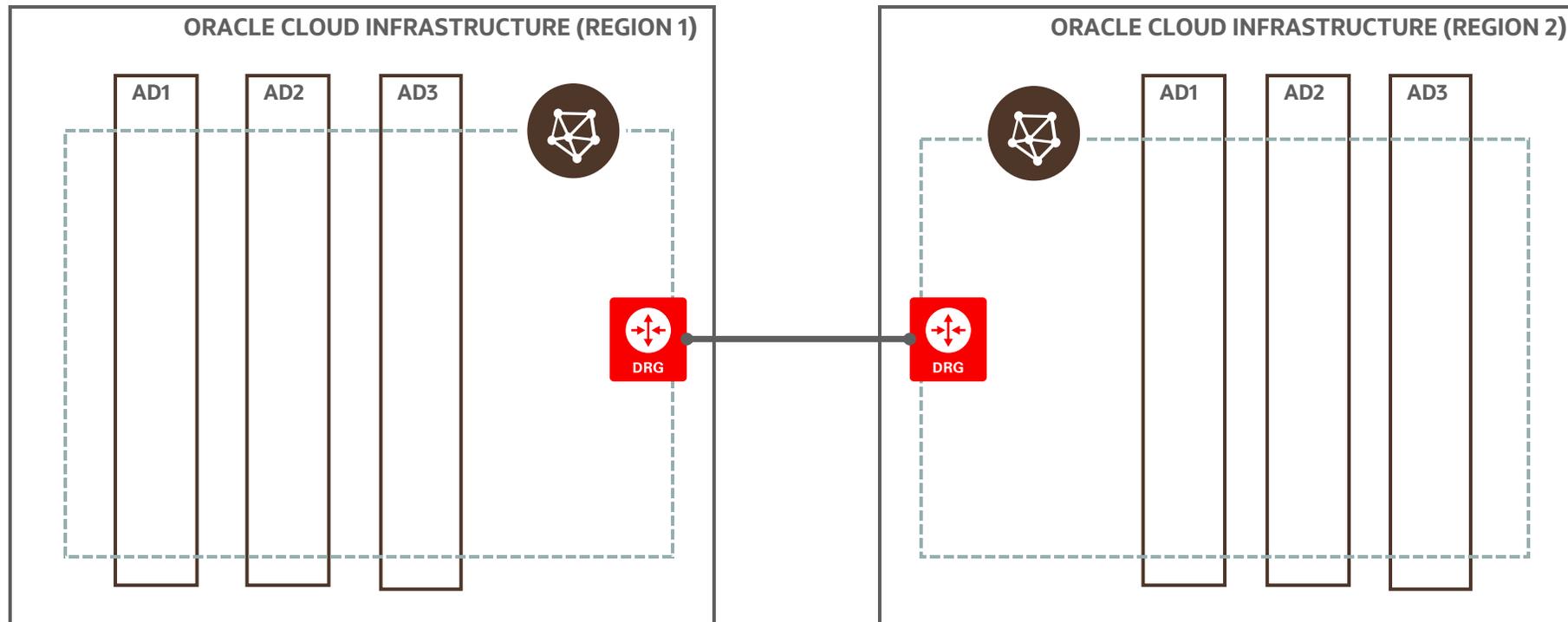24 hours   24 hours

$

RPO

RTO

$ Cost

Disaster Recovery for OCI

- Regions are **completely independent** of other regions and can be separated by vast distances—across countries or even continents.

- You can also deploy applications in different regions to:
  - mitigate the risk of region-wide events, such as large weather systems or earthquakes
  - meet varying requirements for legal jurisdictions, tax domains, and other business or social criteria
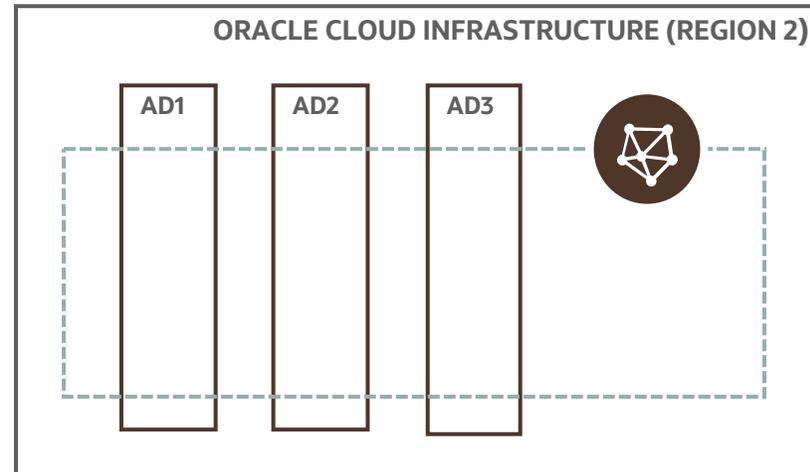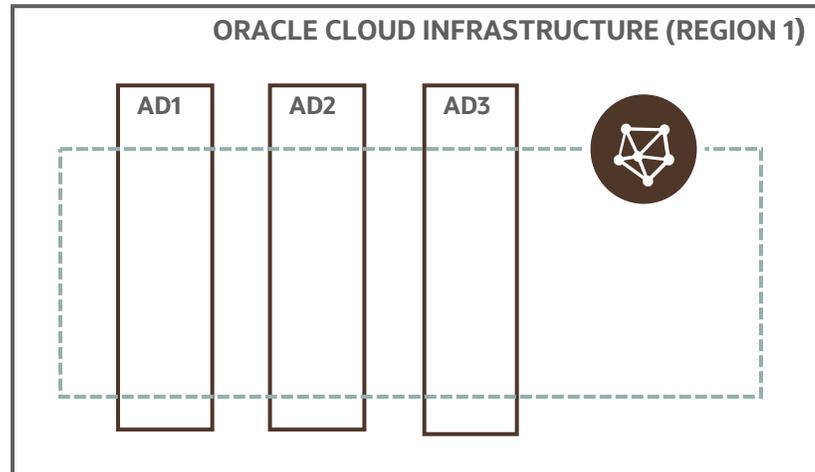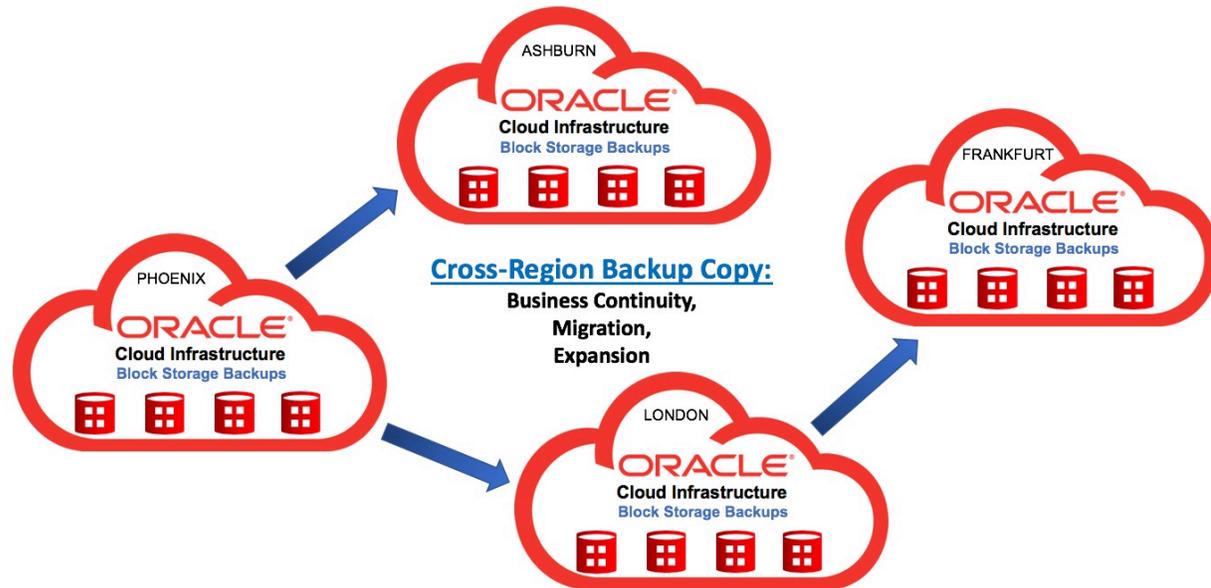
Disaster Recovery using multiple regions

- You can connect Regions using Remote VCN Peering.
- Using internal backbone, traffic never leaves Oracle Network.

Disaster Recovery using multiple regions

ASHBURN

ORACLE
Cloud Infrastructure
Block Storage Backups

PHOENIX

ORACLE
Cloud Infrastructure
Block Storage Backups

FRANKFURT

ORACLE
Cloud Infrastructure
Block Storage Backups

Cross-Region Backup Copy:
Business Continuity,
Migration,
Expansion

LONDON

ORACLE
Cloud Infrastructure
Block Storage Backups

- Cross region Block volume backup copy:
  - By copying block volume backups to another region at regular intervals, it makes it easier to rebuild applications and data in the destination region if a region-wide disaster occurs in the source region.

- Migration and expansion:
  - To easily migrate and expand your applications to another region.

DNS traffic management

- STEERING POLICIES

    - A framework to define the traffic management behavior for your zones. Steering policies contain rules that help to intelligently serve DNS answers.

- ATTACHMENTS

    - Allows you to link a steering policy to your zones. An attachment of a steering policy to a zone occludes all records at its domain that are of a covered record type, constructing DNS responses from its steering policy rather than from those domain's records. A domain can have at most one attachment covering any given record type.

- RULES

    - The guidelines steering policies use to filter answers based on the properties of a DNS request, such as the requests geo-location or the health of your endpoints.

- ANSWERS

    - Answers contain the DNS record data and metadata to be processed in a steering policy.
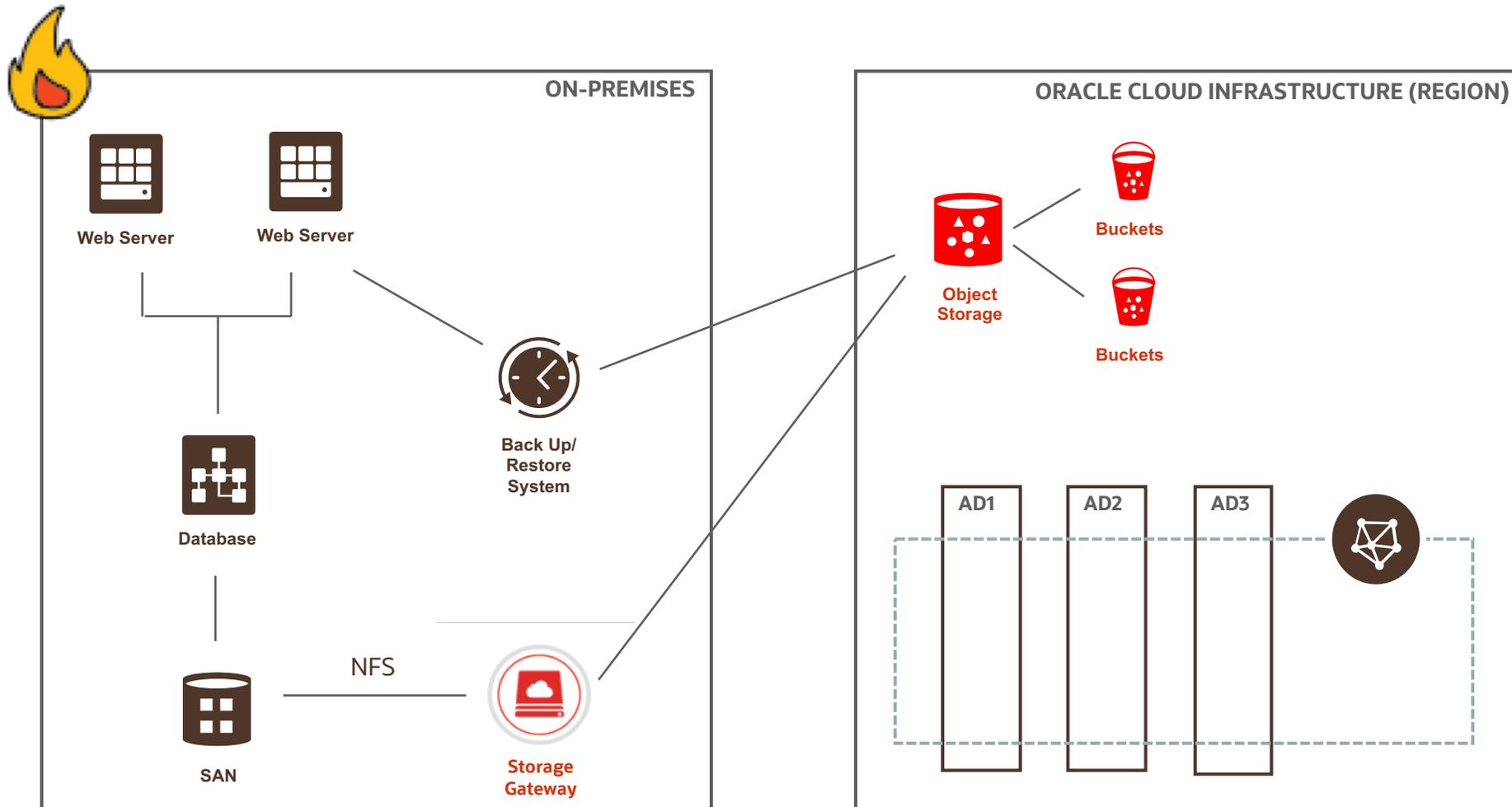
Failover
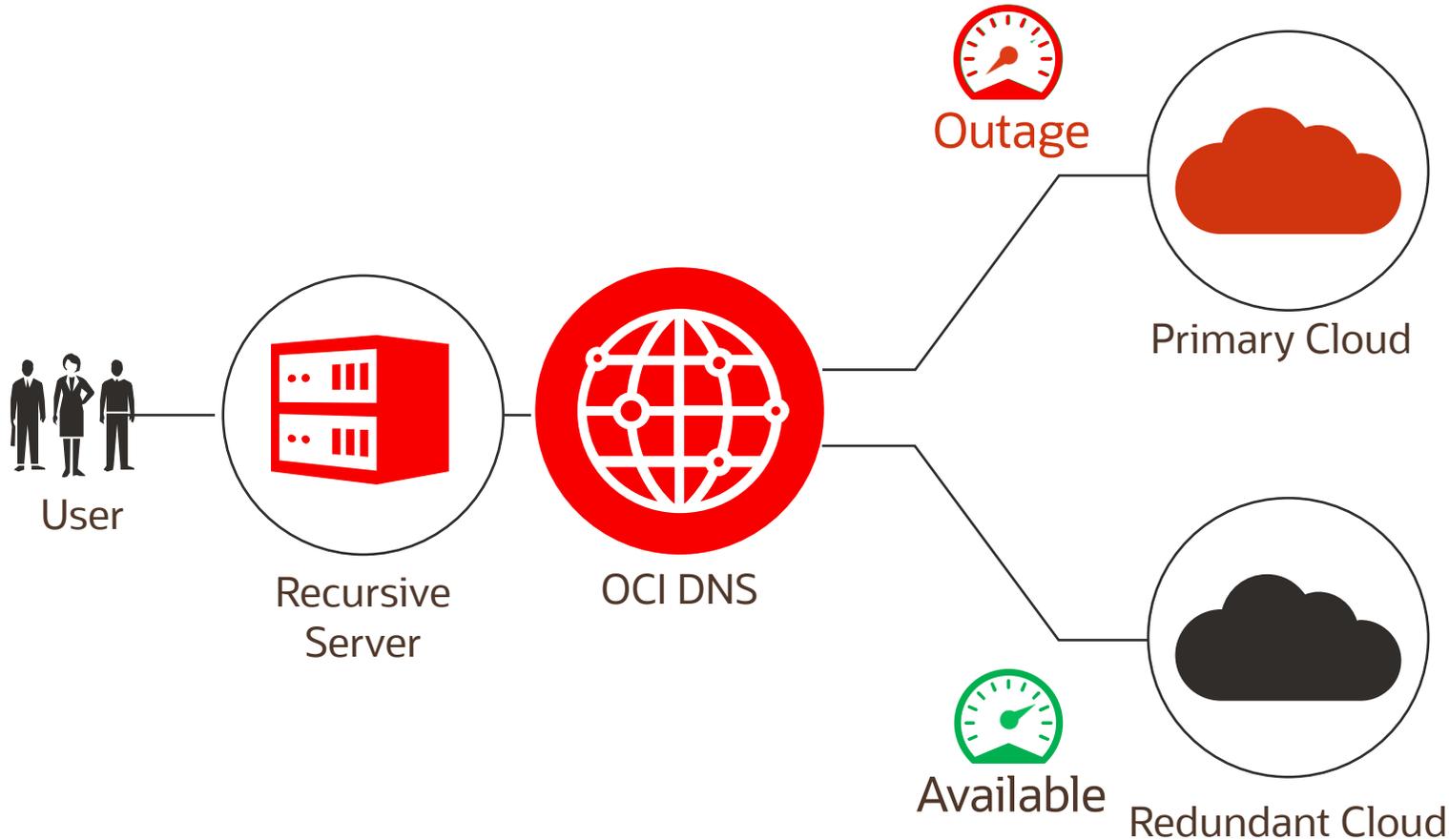
A -> B Failover

Primary asset is monitored from multiple points via Oracle Health Checks
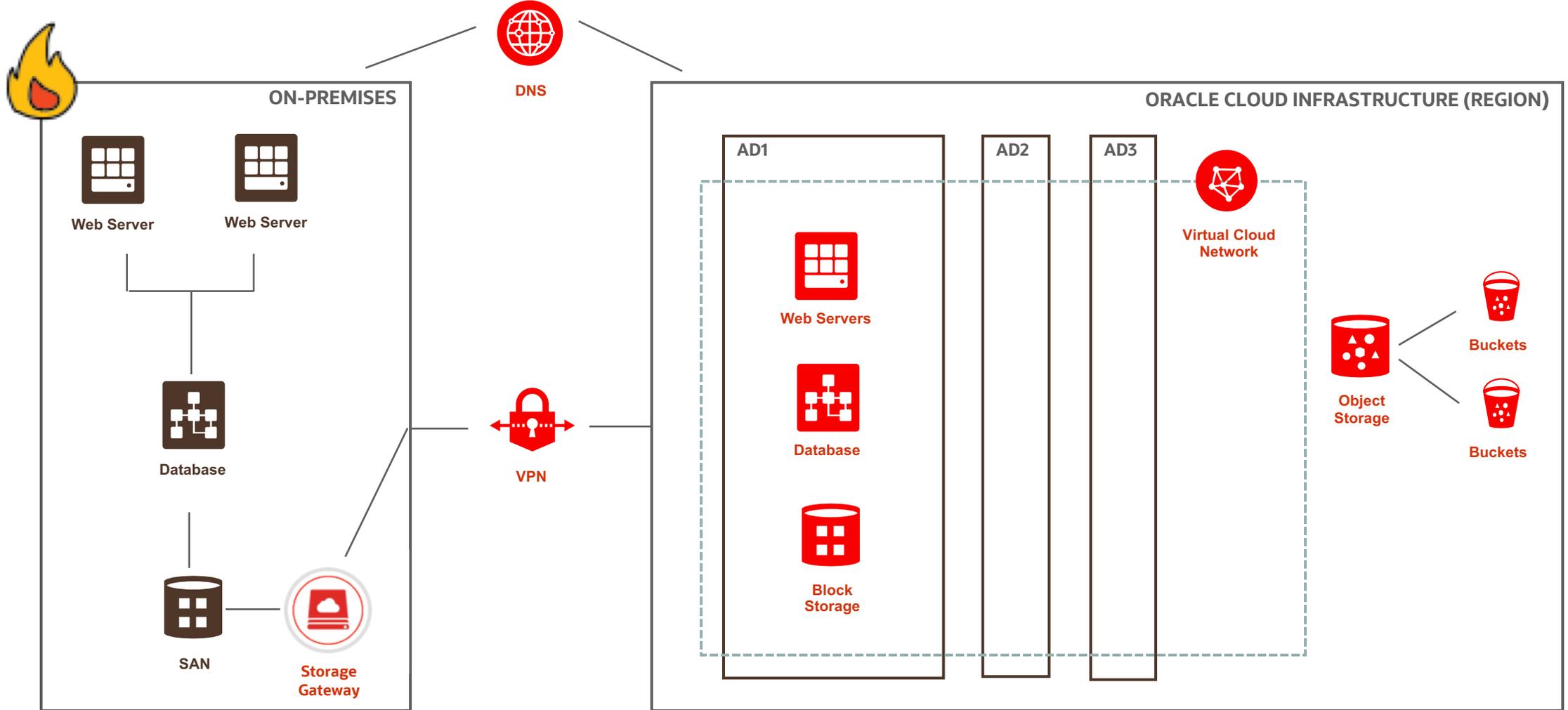
Traffic is automatically directed to a different endpoint as soon as service fails to respond

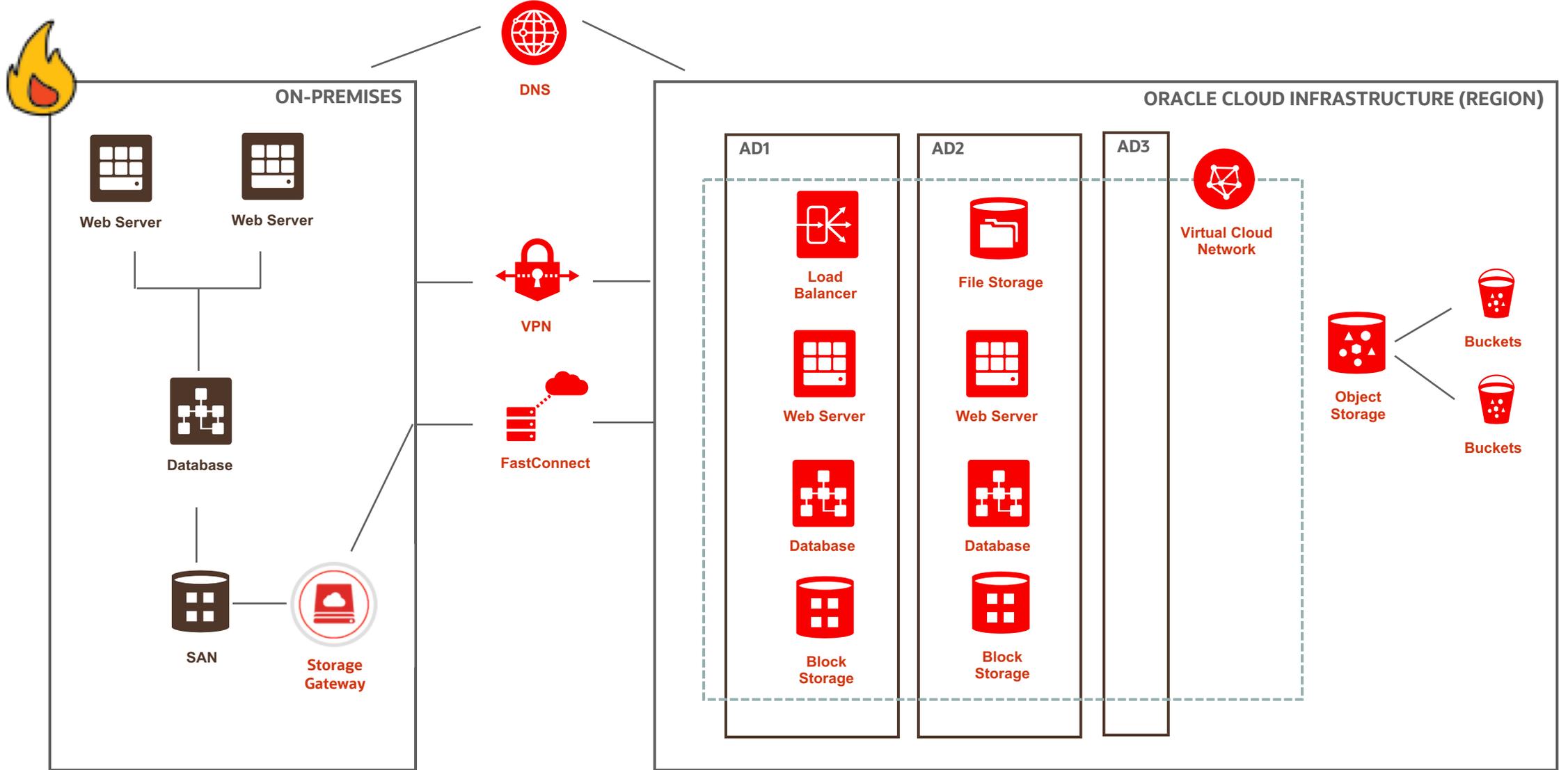Monitoring is powered by Oracle Health Checks

Backup and Restore Architecture

Standby Architecture

Active/Active Architecture

Database Strategies for DR

- **Active Data Guard**
  - Provides data protection and availability for Oracle Database in a simple and economical manner by maintaining an exact physical replica of the production copy at a remote location that is open read-only while replication is active.

- **GoldenGate**
  - Enables advanced logical replication that supports multi-master replication, hub and spoke deployment, and data transformation.
  - Provides customers flexible options to address the complete range of replication requirements, including heterogeneous hardware platforms.

Oracle Cloud always free tier:
oracle.com/cloud/free/

OCI training and certification:
oracle.com/cloud/iaas/training
oracle.com/cloud/iaas/training/certification
education.oracle.com/oracle-certification-path/pFamily_647

OCI hands-on labs:
ocitraining.qloudable.com/provider/oracle

Oracle learning library videos on YouTube:
youtube.com/user/OracleLearning

ORACLE