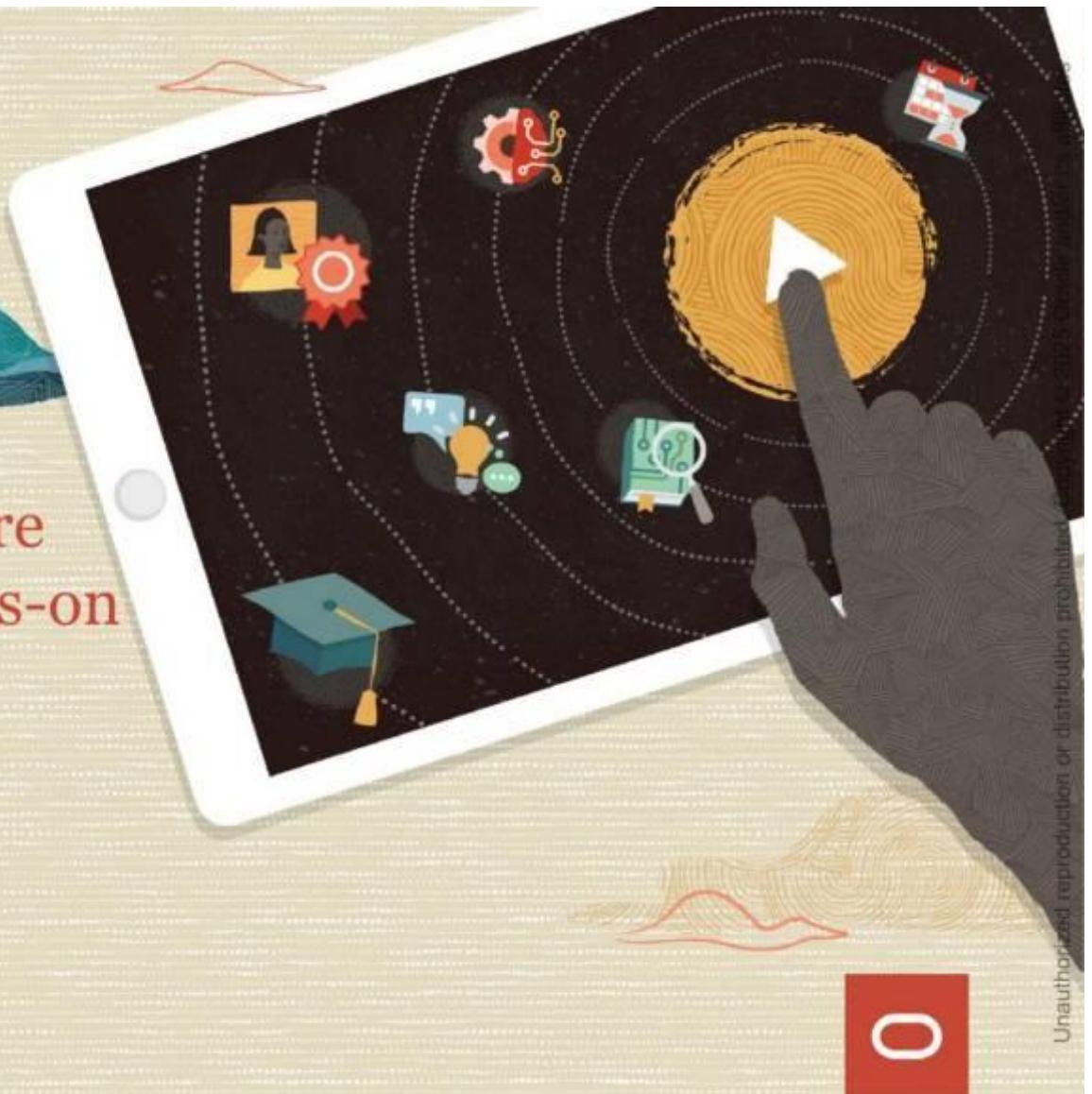




# Oracle Cloud Infrastructure Architect Associate: Hands-on Workshop

Student Guide – Volume I  
D1111074GC10

Learn more from Oracle University at [education.oracle.com](http://education.oracle.com)



**Copyright © 2025, Oracle and/or its affiliates.**

**Disclaimer**

This document contains proprietary information and is protected by copyright and other intellectual property laws. The document may not be modified or altered in any way. Except where your use constitutes "fair use" under copyright law, you may not use, share, download, upload, copy, print, display, perform, reproduce, publish, license, post, transmit, or distribute this document in whole or in part without the express authorization of Oracle.

The information contained in this document is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

**Restricted Rights Notice**

If this documentation is delivered to the United States Government or anyone using the documentation on behalf of the United States Government, the following notice is applicable:

**U.S. GOVERNMENT END USERS:** Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software" or "commercial computer software documentation" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

**Trademark Notice**

Oracle®, Java, MySQL, and NetSuite are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

**Third-Party Content, Products, and Services Disclaimer**

This documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

1002262025

## Table of Contents

<b>Module 01: OCI 2025 Architect Associate Course Overview</b>	<b>12</b>
Course Speakers	13
For whom is this course intended?	14
Course Outline	15
Measuring Your Progress: Take the Skill Checks to Test Your Knowledge	16
Get the Answers You Need: Use our "Ask Your Instructor" Form or Join the OU Community	17
Best practices and retention tips	18
<b>Module 02: Identity and Access Management Overview</b>	<b>19</b>
Introduction	20
What is OCI IAM?	21
OCI IAM: Authentication (AuthN)	23
OCI IAM Components	27
Summary	32
OCI IAM Identity Domains	33
What are OCI IAM identity domains?	34
Identity Domains	35
Identity Domains: Use Cases	36
Identity Domains: Identity Lifecycle Management	37
OCI IAM with Identity Domains	42
Identity Domain Types	43
<b>Module 03: Identity and Access Management - Basics</b>	<b>49</b>
Managing OCI IAM Identity Domains	50
Default Identity Domain	52
Default Domain	53
Dos and Don'ts for the Administrator Users	55
Creating Identity Domains	56
Why do we need multiple identity domains?	57

Creating Identity Domains	58
Demo	59
Creating Identity Domains	60
Demo: Creating Identity Domains	61
Creating Identity Domains	62
Demo: Creating Groups	63
Creating Groups	64
Managing Groups	66
Groups	67
Default Groups in Identity Domains	69
Demo: Creating Users	70
Creating Groups	71
Creating Users	72
Managing Users	73
Stages of the IAM User Life Cycle	74
User Lifecycle Management	75
Demo	76
Creating Groups	77
Understanding the Administrator Role	78
Administrator Roles: Key Points	79
Types of Administrator Roles	80
Demo	81
Assigning Administrative Roles	82
Demo: Understanding Administrator Role	83
Policies	84
Policies	86
Subjects Clause	87
Actions Clause	90
Placement	92
Demo: Policies	85
Compartments	93

Resource Compartments	96
Compartments Access	97
Interaction of Resources	98
Movement of Resources	99
Multiple Regions	100
Nested Compartments	101
Compartment Quotas	102
Scenario	103
Quota Syntax	104
Quota Examples	110
Types of Quota Policy Statement	111
Quota Examples	112
Budgets	113
Slide Number 13	
<b>Module 04: Identity and Access Management - Advanced</b>	<b>114</b>
Policy Inheritance and Attachment	115
Policy Inheritance	116
Demo: Policy Inheritance and Attachment	120
Conditional Policies	122
Conditions	125
Examples	127
Demo: Creating Users	128
Enforce Least Privileged: Advanced Policies	130
Permissions	131
Example	132
Tag Based Access Control	136
Example	140
Demo: Tag Based Access Control	142
Demo: Dynamic Groups	143
Scenario: Dynamic Groups	144
Network Sources	145

Demo: Network Sources .....	149
Scenario .....	150
Dynamic Groups .....	151
Terms .....	152
Resource Principals Patterns .....	153
Infrastructure Principals .....	154
Stacked Principals .....	155
Ephemeral Principals .....	156
Dynamic Groups .....	157
Policies .....	159
Summary .....	160
Optimizing IAM Policies: Part 1 .....	161
OCI IAM Policies .....	162
Eliminating Duplicate Policies .....	164
Removing Less-Permissive Policies .....	166
Policy Conditions and Inheritance .....	168
Removing Less-Permissive Policies .....	169
Consolidating Group Membership .....	170
Consolidating Group Membership: Same Members .....	171
Consolidating Group Membership: Different Members .....	172
Optimizing IAM Policies: Part 2 .....	173
Combining Policy Statements .....	174
Combining Policy Statements: Use case .....	177
Grouping Multiple Entities .....	178
Pattern-Based Optimization .....	180
Object-Level Granular Access Control for OCI Object Storage .....	182
OCI Object Storage .....	183
OCI Object Storage .....	184
Object-Level Permissions .....	185
Object IAM .....	186
Object IAM Policy Examples .....	187

Object IAM Policy Examples	188
Object IAM Policy Examples	189
Slide Number 9	
<b>Module 05: Expert Tip</b>	<b>190</b>
<b>Module 06: Networking - Virtual Cloud Network</b>	<b>191</b>
CIDR Block Prefixes	192
Virtual Cloud Network - Networking –Virtual Cloud Network	195
Virtual Cloud Network	196
VCN Components- Quick Overview	199
Virtual Cloud Network	200
Subnets	201
Types of Subnets	204
Demo: Create a VCN (Manually)	205
Demo: Create a VCN (Using Wizard)	206
Route Table	207
Route Table Basics	208
Route Table	209
Allowed Route Rule Target Type	210
Demo: Route Tables	211
Internet Gateway	212
Demo: Internet Gateway	215
NAT Gateway	216
Demo: NAT Gateway	219
Service Gateway	220
Demo: Service Gateway	223
Public Subnet	224
Demo: Public Subnet	227
Private Subnet	228
Demo: Private Subnet	231

VCN Security	232
Ways to Secure Your Network	233
VCN Security	234
Network Security Group	235
NSG as the Source or Destination of a Rule	237
Stateful Security Rules	238
Stateless Security Rules	239
Demo: Network Security Groups	240
Security List	241
SL + NSG	243
Demo: Security Lists	245
<b>Module 07: Networking - IP Management</b>	<b>246</b>
Overview of IP Management	247
IP Management Overview	248
Private IP	249
Public IP	250
Types of Public IPs	251
Reserved Public IP	252
Bring Your Own IP Address (BYOIP)	254
Bring Your Own IP (BYOIP)	255
BYOIP Benefits	256
BYOIP Workflow	257
Public IP Pools	258
Demo: IP Management	260
<b>Module 08: Networking - Connectivity</b>	<b>261</b>
VCN Connectivity Options	262
Local Peering Versus Remote Peering	263
Local Peering with DRG VCN Attachments	264
Connecting On-Premises to OCI	265
Considerations for Cloud Connectivity Options	266

Local VCN Peering	267
Local VCN Peering (Using LPGs)	268
Local VCN Peering (Using Upgraded DRG)	270
Demo: Local VCN Peering	271
Remote VCN Peering	272
Remote Peering Connection	273
Remote Peering (Across Regions)	274
Demo: Remote VCN Peering	275
BGP Basics	276
Border Gateway Protocol (BGP)	277
Dynamic Routing Gateway	280
DRG Attachments	282
DRG Route Tables & Route Distributions	283
DRG Use Cases	284
Demo: Dynamic Routing Gateway	286
Site-to-Site VPN	287
Site-to-Site VPN: Overview	288
Site-to-Site VPN: Use Cases	289
Customer-Premises Equipment	290
Site-to-Site VPN	291
Site-to-Site VPN: Tunnel Mode	292
Site-to-Site VPN: CPE Behind a NAT Device	293
Demo: Site-to-Site VPN	294
FastConnect Overview	295
Overview	296
FastConnect Concepts	297
FastConnect Connectivity Models	298
FastConnect with an Oracle Partner	299
FastConnect: With an Oracle Partner	300
Setup: FastConnect with an Oracle Partner	301
FastConnect with a Third-Party Provider	302

FastConnect Direct: With a Third-Party Provider	303
FastConnect with a Third-Party Provider	304
Setup: FastConnect with a Third-Party Provider	305
FastConnect Colocation with Oracle	306
FastConnect Direct: Colocation	308
Setup: FastConnect Colocation with Oracle	309
Demo: FastConnect	310
FastConnect Redundancy Best Practices	311
Oracle Partner	314
FastConnect Partner: Layer 2 Connections	315
FastConnect Partner: Layer 3 Connections	316
Third-Party Provider or Colocation with Oracle	317
FastConnect Direct: Colocation or Third-Party Provider	318
FastConnect with Site-to-Site VPN Backup	319
<b>Module 09: Expert Tip 2</b>	<b>320</b>
<b>Module 10: Networking - Load Balancer</b>	<b>321</b>
Load Balancer	322
OCI Load Balancing Service	323
Load Balancer Concepts	324
OCI Load Balancer Shapes	325
Content-Based Routing: Host Based	326
Content-Based Routing: Path Based	327
Load Balancer Policies	328
Load Balancing Policies	329
Round Robin	330
Least Connections	331
IP Hash	332
Load Balancing Policies	333
Load Balancer Health Checks	334
Health Check	335
Public Load Balancers	337

Public Load Balancer (Regional Subnets)	340
Public Load Balancer (AD-Specific Subnets)	341
Demo: Public Load Balancer	342
Private Load Balancers	343
Private Load Balancer	344
Demo: Private Load Balancer	345
Network Load Balancer	346
Demo: Network Load Balancer	349
Web Application Acceleration Overview	350
Use Cases	352
Web Application Acceleration Concepts	353
Web Application Acceleration	354
Demo: Web Application Acceleration	357

Oracle Cloud Infrastructure  
**OCI 2025 Architect Associate**

# Course Speakers

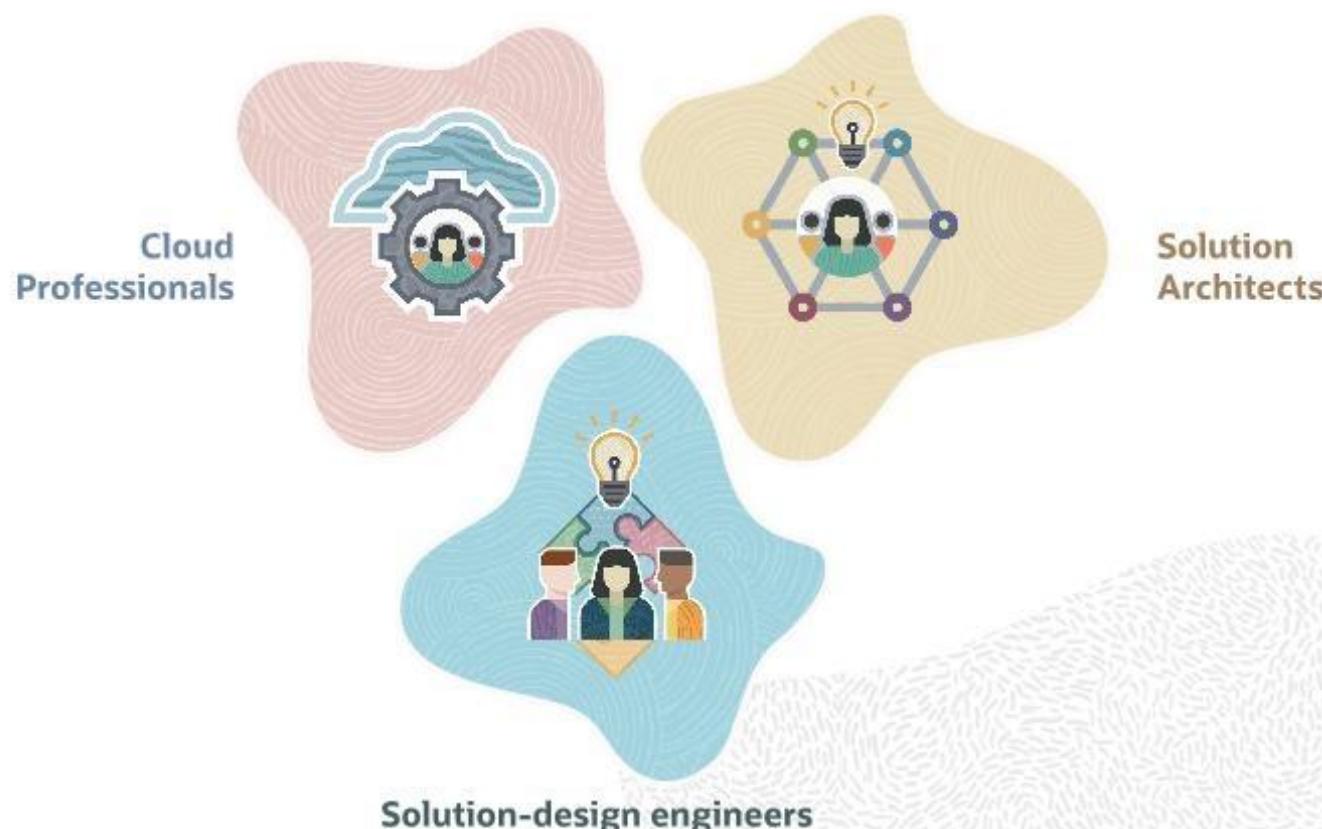


**Samvit Mishra**  
Senior Principal OCI  
Instructor



**Saurabh Patil**  
Senior OCI Instructor

# For whom is this course intended?



# Course Outline

- › IAM - Identity Domain Overview
- › IAM – Managing Identity Domains
  
- › Networking
  - Virtual Cloud Network
  - IP Management
  - Connectivity
  - Load Balancer
  - DNS Management
  - Network Command Center
  
- › Compute – Basics & Advanced
- › Storage
  - Object Storage : Basics & Advanced
  - Block Storage : Basics & Advanced
  - File Storage : Basics & Advanced

Expert Tips

Whiteboarding



## Measuring Your Progress: Take the Skill Checks to Test Your Knowledge



# Get the Answers You Need: Use our "Ask Your Instructor" Form or Join the OU Community

Ask the Instructor 

Ask Your Instructor

Oracle Cloud Infrastructure DevOps Professional

S110eOQSC0

undefined undefined

undefined

City

State

Topic to discuss or report

Community 



A stylized illustration of a woman with dark hair tied back, wearing a black top with an orange collar. She is waving her right hand towards a video conference interface. The interface shows four participants in separate video feeds: a man with a beard in a purple background, a person with a yellow background, a man in a green background, and a woman in a blue background. The entire scene is set against a white background with a teal wavy footer.

Oracle Cloud Infrastructure Architect Associate 17

Unauthorized reproduction or distribution prohibited. Copyright © 2025 Oracle and/or its affiliates

## Best practices and retention tips

Schedule breaks every hour.



Hands-on demonstrations



Take notes.



Review exam prep material.



Take practice exam before the certification exam.



Complete all skill checks in this course.



# Identity and Access Management Overview

# Oracle Cloud Infrastructure Introduction

## OCI Identity and Access Management (IAM)



# What is OCI IAM?

## Identity

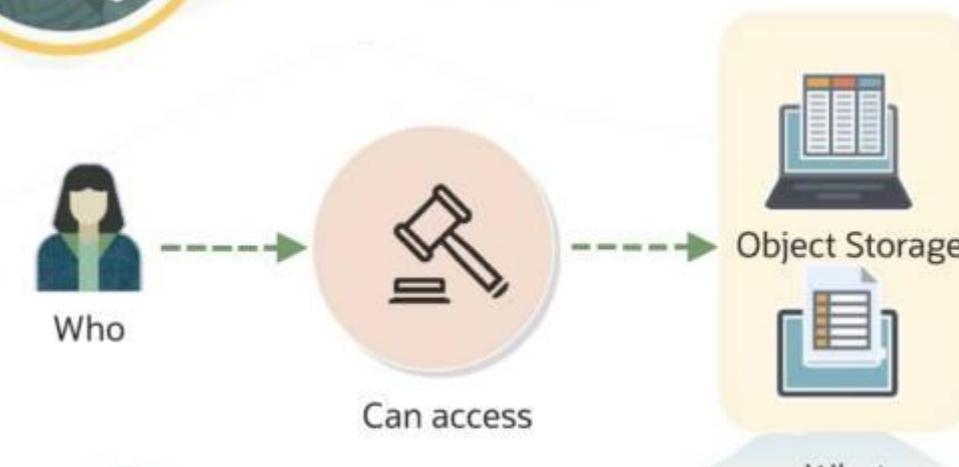
- Authentication
- Centralized identity lifecycle management
- Integration with existing identities and applications
- Secure and easy access

## Access Management

- Authorization
- Fine-grained access controls
- Define granular permission



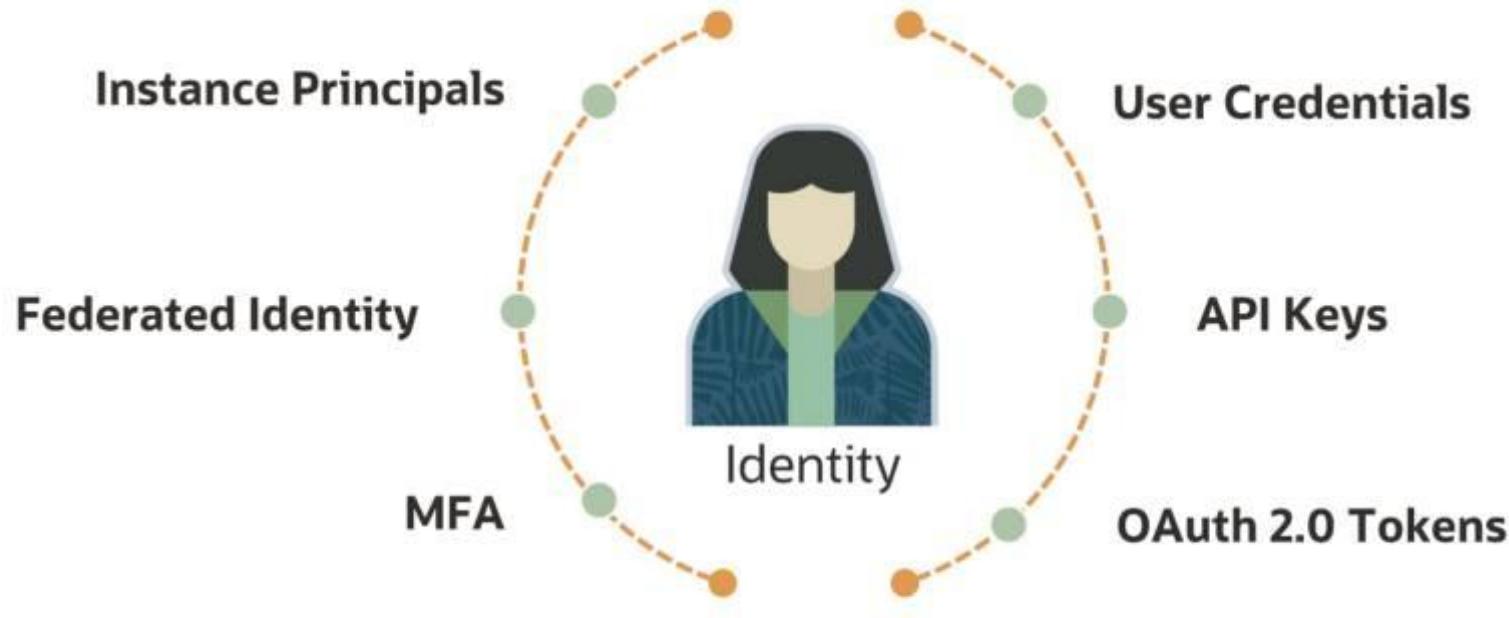
# What is OCI IAM?



## OCI IAM: Authentication (AuthN)



## OCI IAM: Authentication (AuthN)

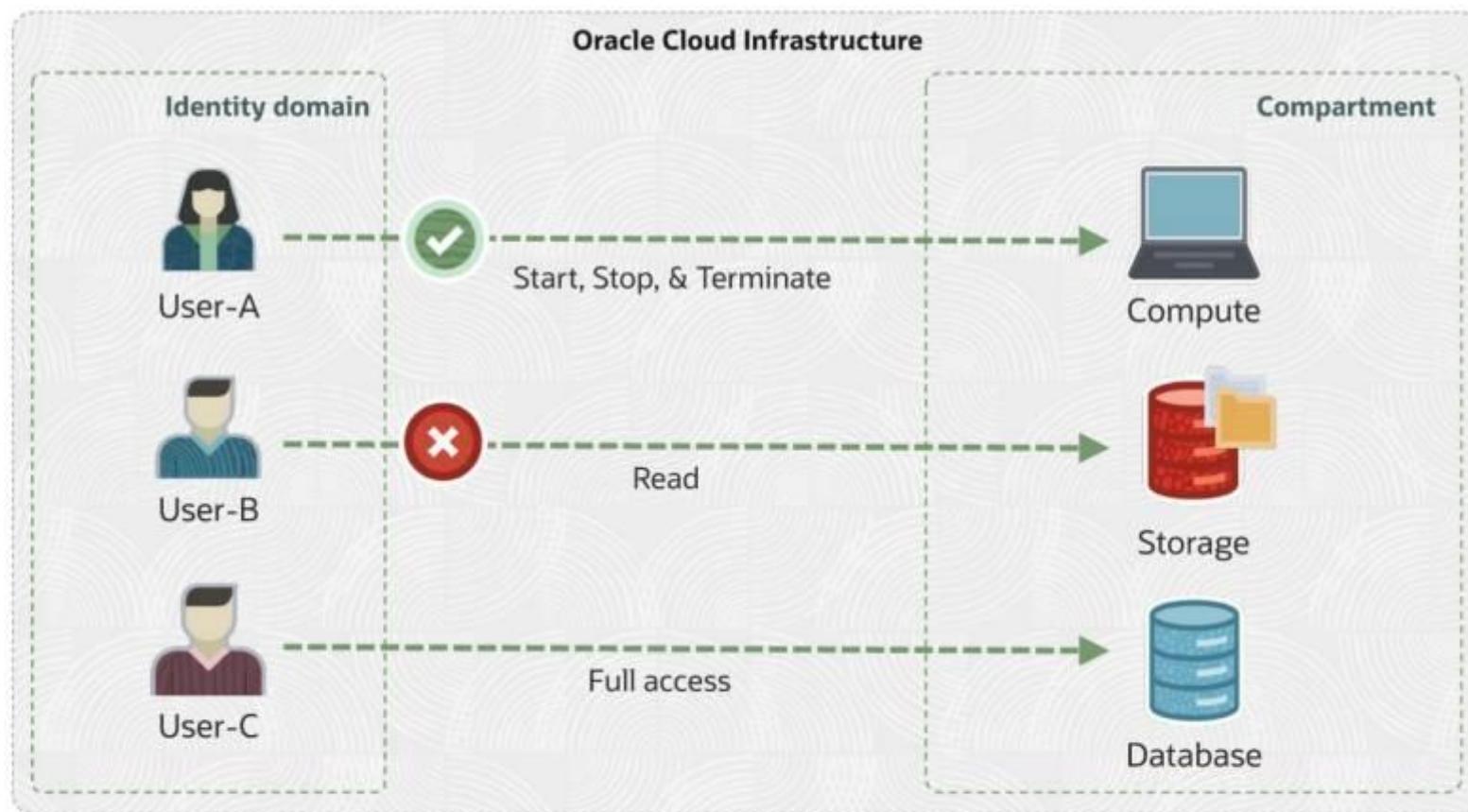


## OCI IAM: Authorization (AuthZ)

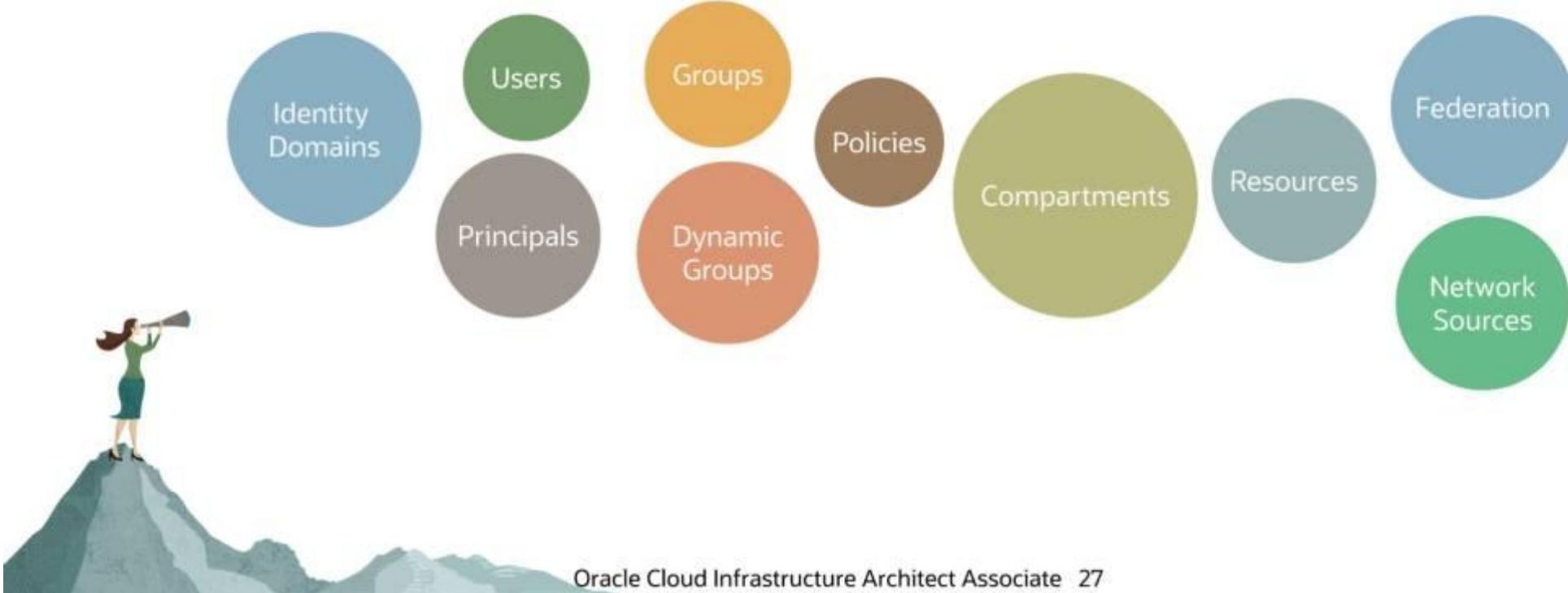
---



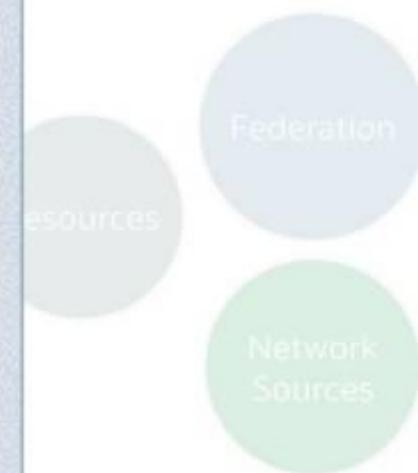
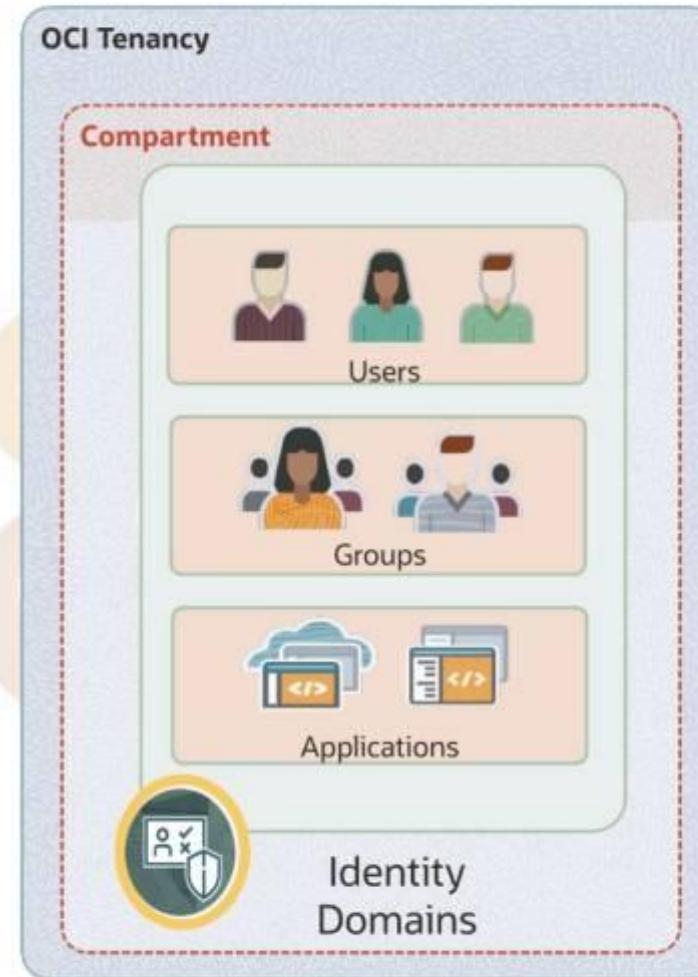
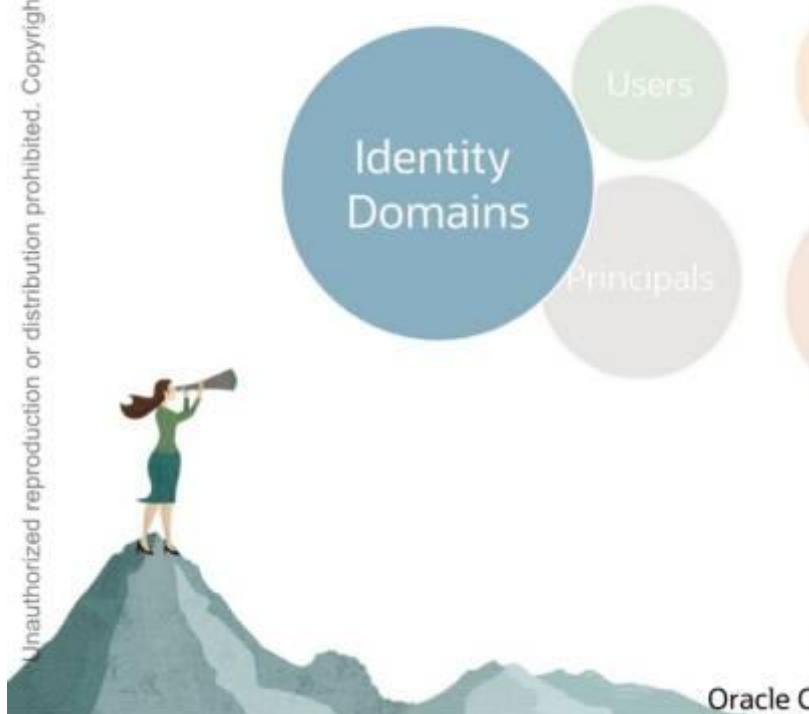
## OCI IAM: Authorization (AuthZ)



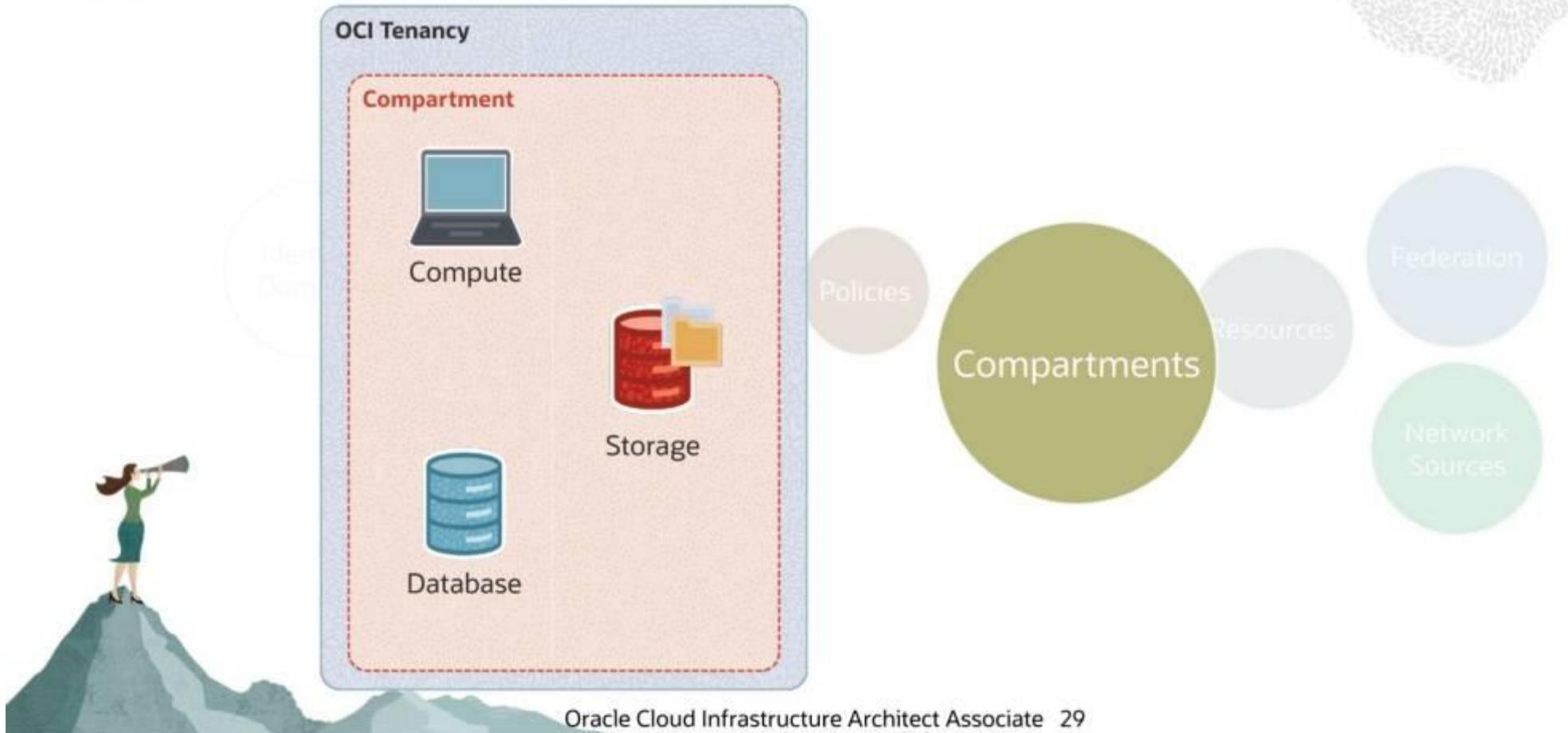
# OCI IAM Components



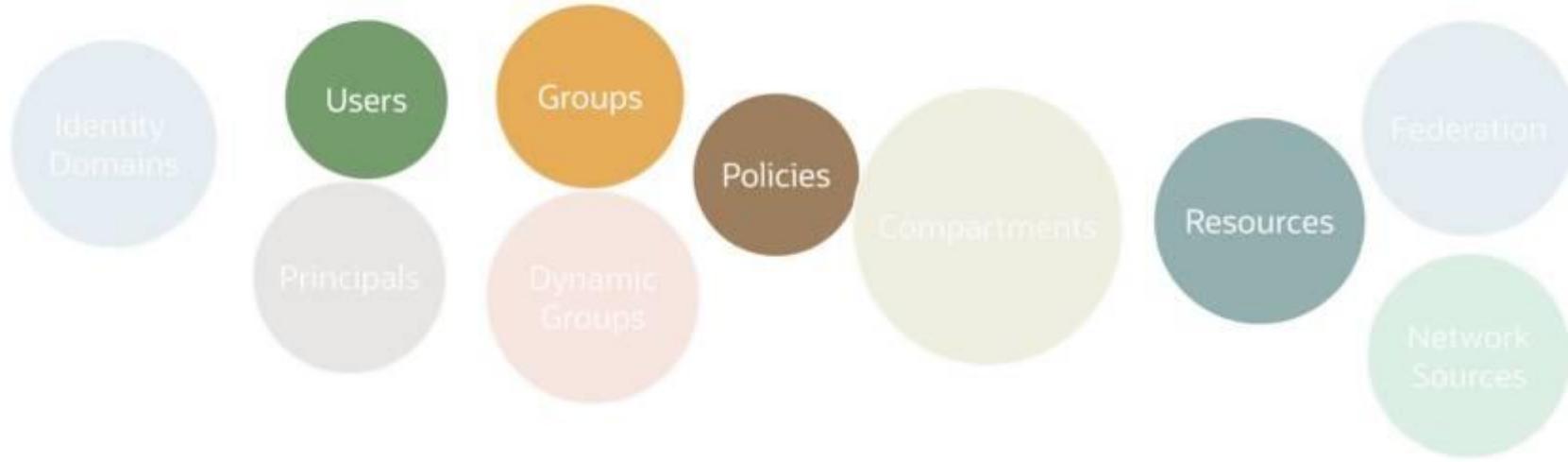
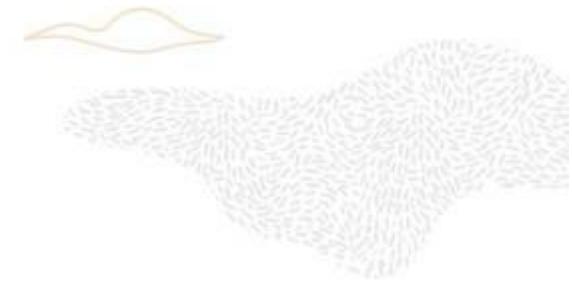
# OCI IAM Components

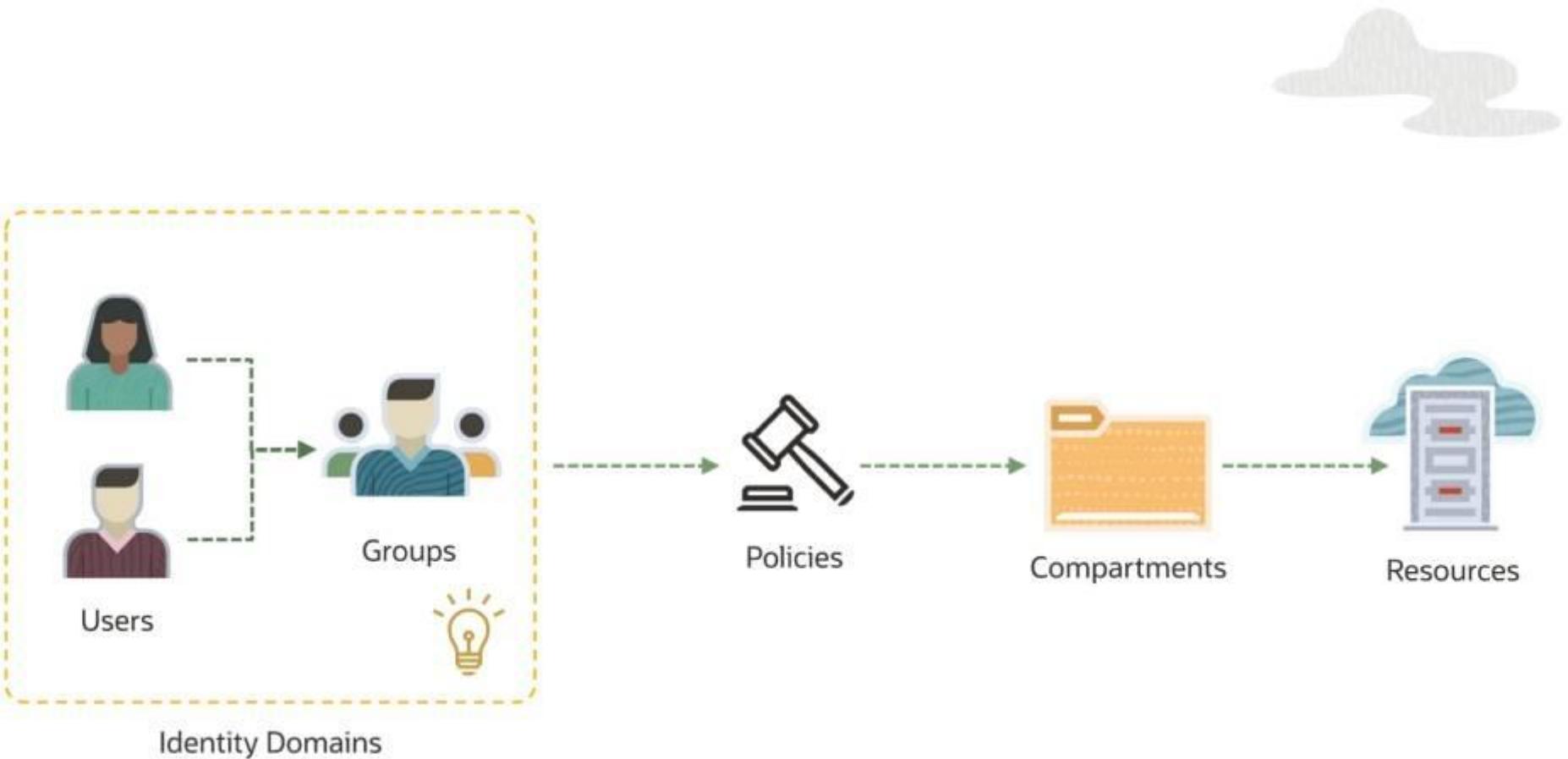


# OCI IAM Components

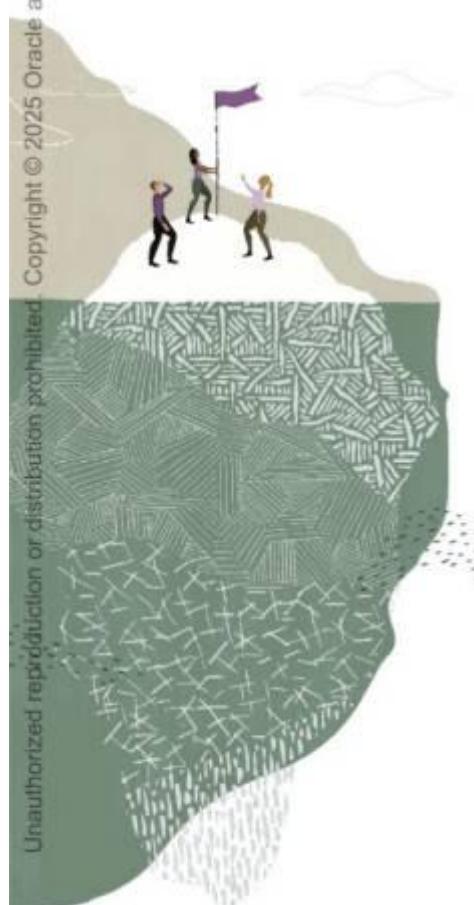


# OCI IAM Components





# Summary



What is OCI IAM?

AuthN

AuthZ

OCI IAM Components

Oracle Cloud Infrastructure

# OCI IAM Identity Domains

—  
**OCI Identity and Access Management (IAM)**



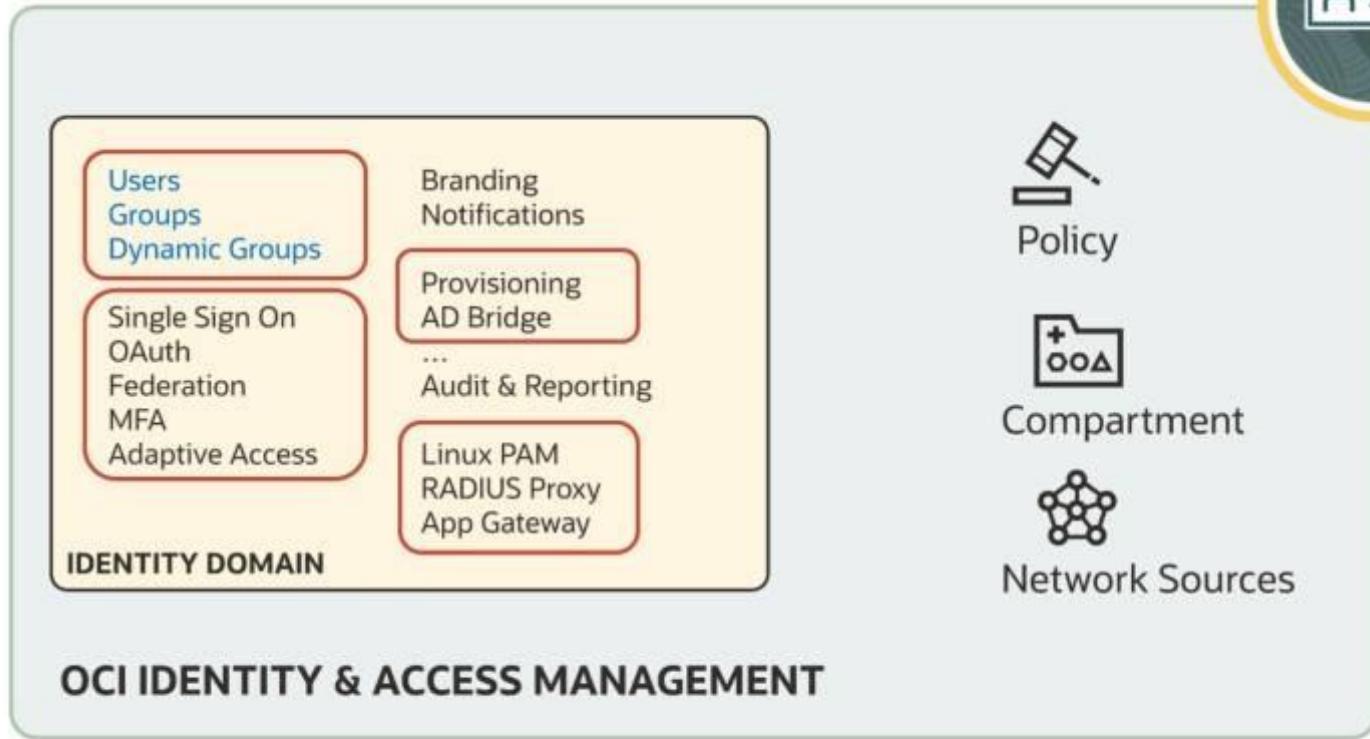
# What are OCI IAM identity domains?

A self-contained identity and access management service

Act as a container to manage **users, roles, federation, SSO, MFA**, and so on

Provide secure application integration through SSO, SAML, and OAuth

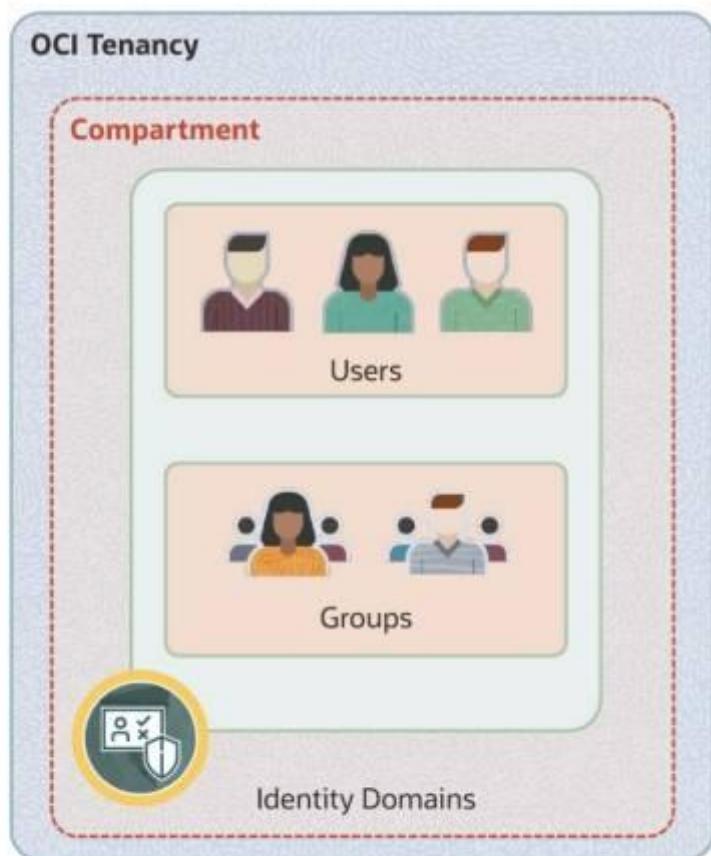
# Identity Domains



# Identity Domains: Use Cases

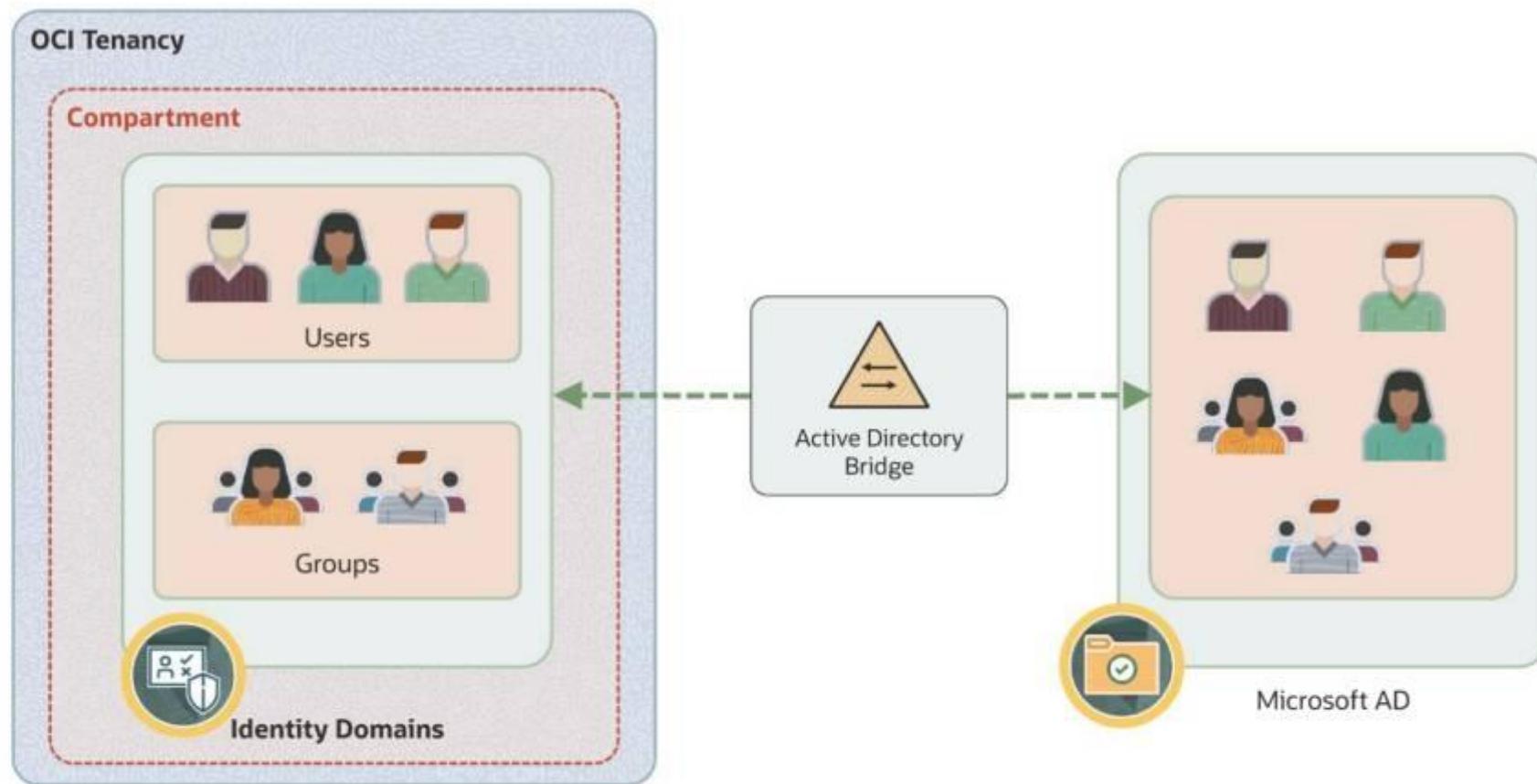


# Identity Domains: Identity Lifecycle Management

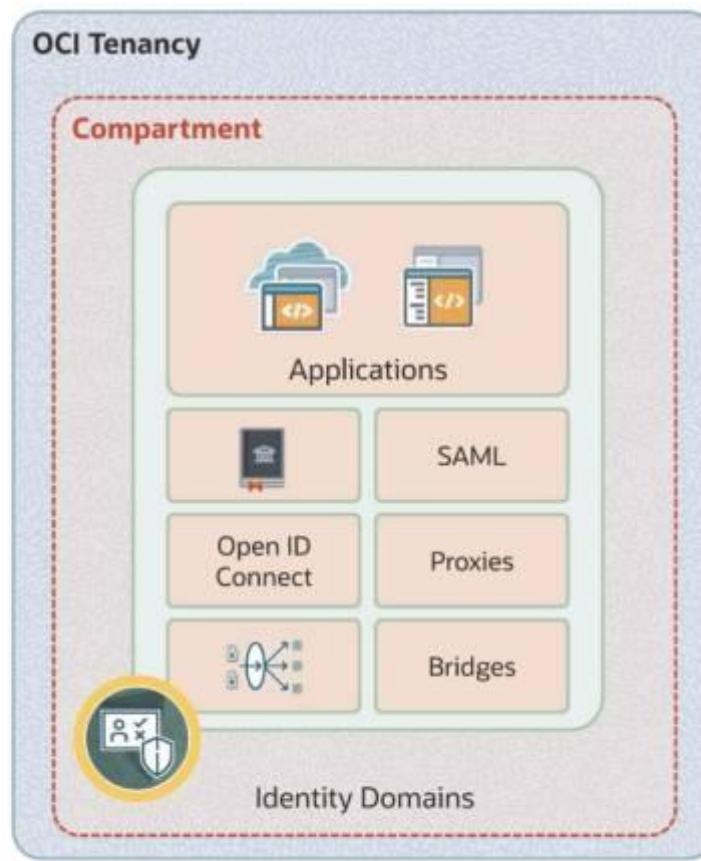


- Self-service registration
- Automated provisioning
- Sync with cloud/on-prem applications

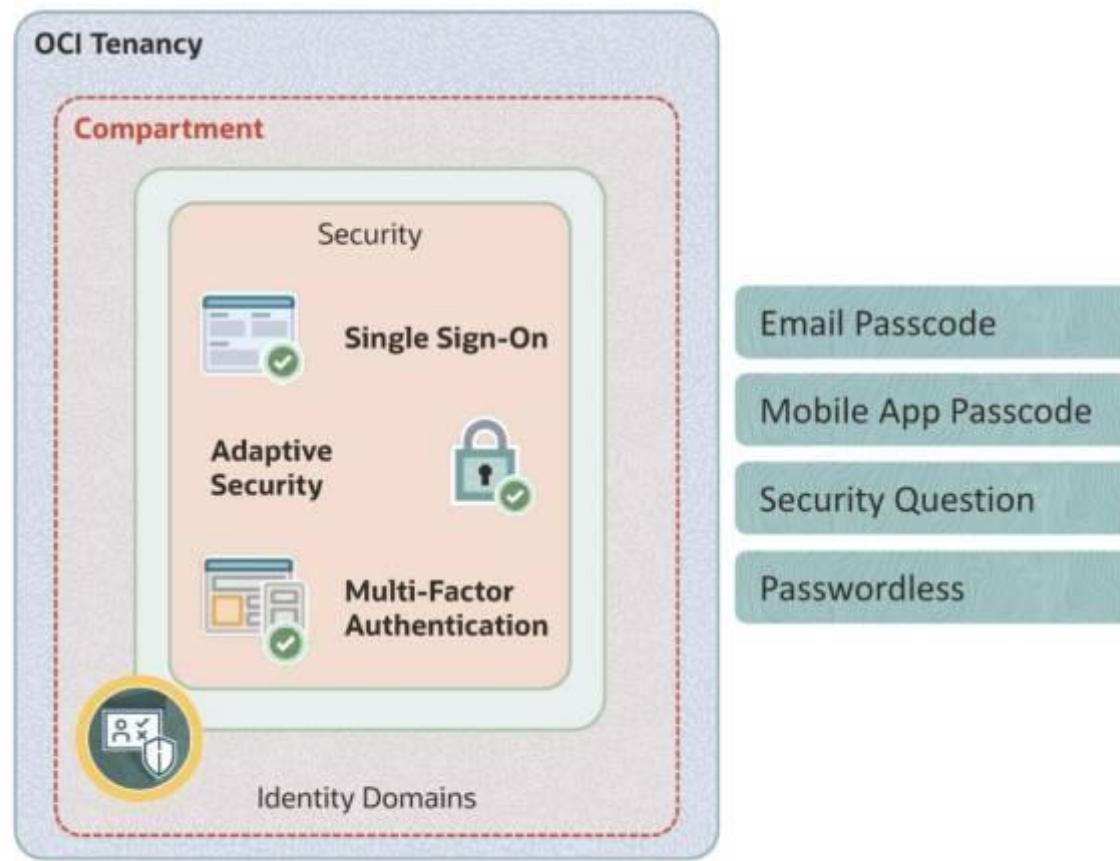
# Identity Domains: Identity Lifecycle Management

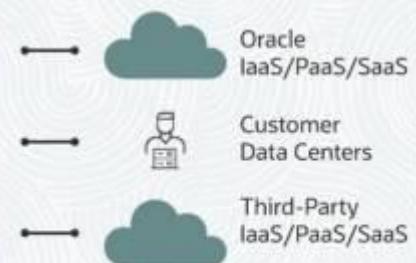
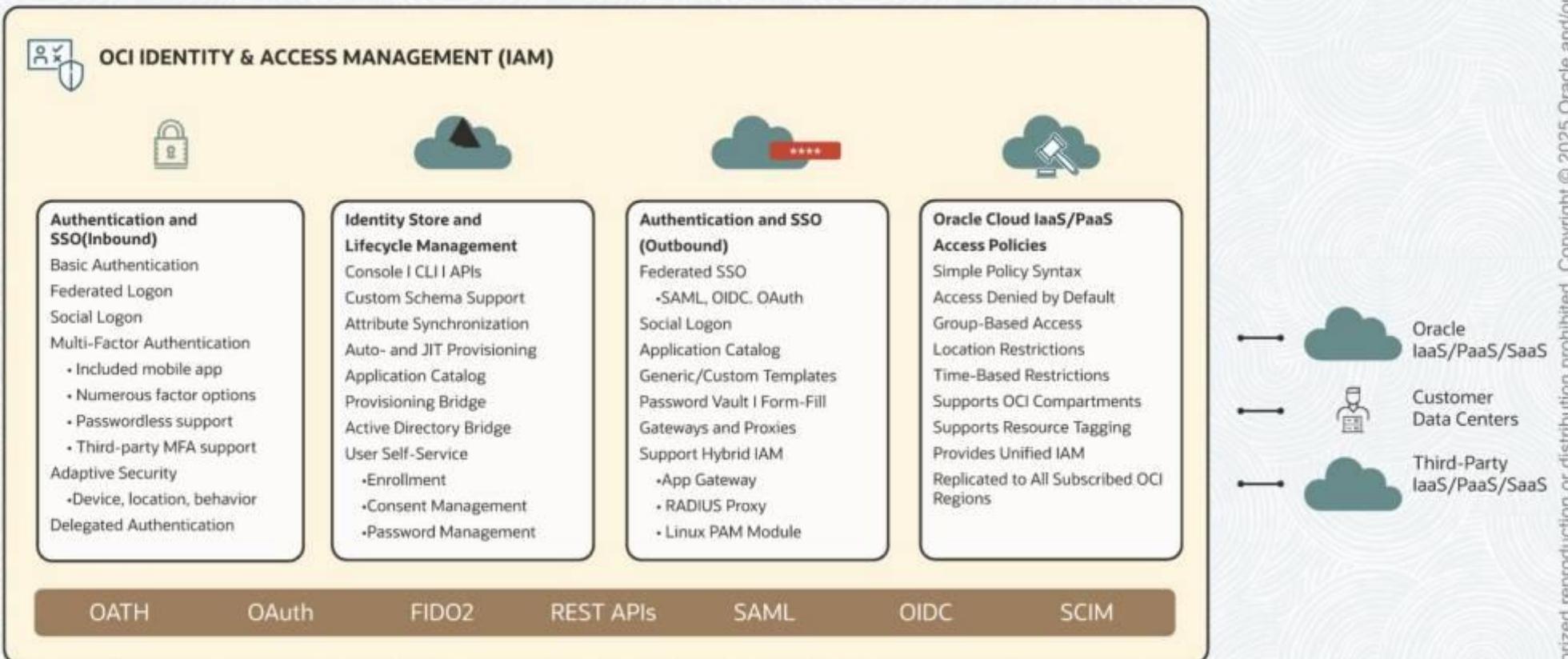


# Identity Domains: Identity Lifecycle Management



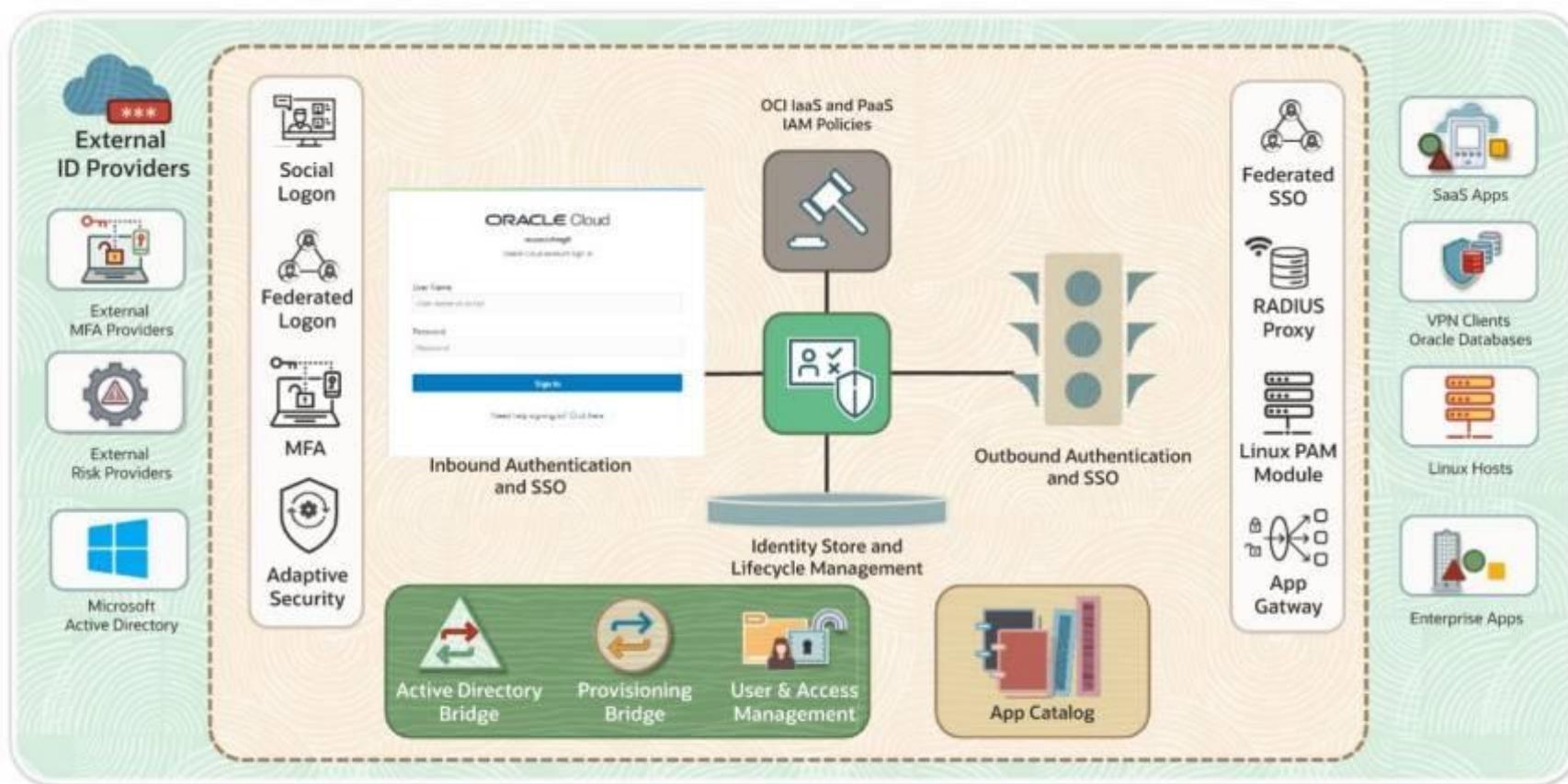
# Identity Domains: Identity Lifecycle Management







## OCI IAM with Identity Domains



## Oracle Cloud Infrastructure

# Identity Domain Types

### OCI Identity and Access Management (IAM)

Dr. Saurabh Patil

OU OCI Delivery Team

# Identity Domain Types

## Oracle Apps Premium

Authentication and Access Management for all of your Oracle apps:

- Unlimited support for Oracle Apps including hybrid IAM.
- Limit of 6 non-Oracle apps.
- Unlimited external Identity Providers.

## Free

Authentication and Access Management for Oracle Cloud (IaaS and PaaS services) with limits on usage and functionality.

- Limit of 2000 users.
- Limited feature support.
- Limit of 2 non-Oracle apps.
- Limit of 3 external Identity Providers.

## Premium

Enterprise Identity & Access Management for employee workforce scenarios.

- Includes all features.
- Broad support for hybrid IAM use-cases.
- Unlimited support for Oracle and non-oracle Apps.
- Unlimited external Identity Providers.

## External User

Identity storage, Access Management, and API security for consumer and non-employee use-cases.

- Provides social self-service, and consent management.
- Limited enterprise and hybrid IAM features.
- Excludes APP catalog provisioning connectors.

Helps manage IaaS and SaaS resources

Uses the Default identity domain to manage access to OCI resources



# Identity Domain Types

## Oracle Apps Premium

Authentication and Access Management for all of your Oracle apps.

- Unlimited support for Oracle Apps including hybrid IAM.
- Limit of 6 non-Oracle apps.
- Unlimited external Identity Providers.

## Free

Authentication and Access Management for Oracle Cloud (IaaS and PaaS services) with limits on usage and functionality.

- Limit of 2000 users.
- Limited feature support.
- Limit of 2 non-Oracle apps.
- Limit of 3 external Identity Providers.

## Premium

Enterprise Identity & Access Management for employee workforce scenarios.

- Includes all features.
- Broad support for hybrid IAM use-cases.
- Unlimited support for Oracle and non-oracle Apps.
- Unlimited external Identity Providers.

## External User

Identity storage, Access Management, and API security for consumer and non-employee use-cases.

- Provides social self-service, and consent management.
- Limited enterprise and hybrid IAM features.
- Excludes APP catalog provisioning connectors.

Helps manage SaaS, PaaS, GBU applications, and so on

Helps manage on-prem applications, such as JD Edwards, PeopleSoft, Oracle Linux, Oracle Database, and so on

Supports hybrid IAM use cases



# Identity Domain Types

## Oracle Apps Premium

Authentication and Access Management for all of your Oracle apps:

- Unlimited support for Oracle Apps including hybrid IAM.
- Limit of 6 non-Oracle apps.
- Unlimited external Identity Providers.

## Free

Authentication and Access Management for Oracle Cloud (IaaS and PaaS services) with limits on usage and functionality.

- Limit of 2000 users.
- Limited feature support.
- Limit of 2 non-Oracle apps.
- Limit of 3 external Identity Providers.

## Premium

Enterprise Identity & Access Management for employee workforce scenarios.

- Includes all features.
- Broad support for hybrid IAM use-cases.
- Unlimited support for Oracle and non-oracle Apps.
- Unlimited external Identity Providers.

## External User

Identity storage, Access Management, and API security for consumer and non-employee use-cases.

- Provides social self-service, and consent management.
- Limited enterprise and hybrid IAM features.
- Excludes APP catalog provisioning connectors.

Helps manage Oracle Apps as well as non-Oracle applications

Supports hybrid IAM use cases



# Identity Domain Types

## Oracle Apps Premium

Authentication and Access Management for all of your Oracle apps:

- Unlimited support for Oracle Apps including hybrid IAM.
- Limit of 6 non-Oracle apps.
- Unlimited external Identity Providers.

## Free

Authentication and Access Management for Oracle Cloud (IaaS and PaaS services) with limits on usage and functionality.

- Limit of 2000 users.
- Limited feature support.
- Limit of 2 non-Oracle apps.
- Limit of 3 external Identity Providers.

## Premium

Enterprise Identity & Access Management for employee workforce scenarios.

- Includes all features.
- Broad support for hybrid IAM use-cases.
- Unlimited support for Oracle and non-oracle Apps.
- Unlimited external Identity Providers.

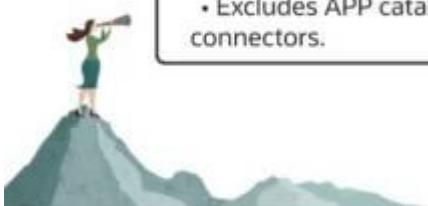
## External User

Identity storage, Access Management, and API security for consumer and non-employee use-cases.

- Provides social self-service, and consent management.
- Limited enterprise and hybrid IAM features.
- Excludes APP catalog provisioning connectors.

Helps manage consumer and non-employee use cases

Supports hybrid IAM use cases



# Identity Domain Types

## Oracle Apps Premium

Authentication and Access Management for all of your Oracle apps.

- Unlimited support for Oracle Apps including hybrid IAM.
- Limit of 6 non-Oracle apps.
- Unlimited external Identity Providers.

## Free

Authentication and Access Management for Oracle Cloud (IaaS and PaaS services) with limits on usage and functionality.

- Limit of 2000 users.
- Limited feature support.
- Limit of 2 non-Oracle apps.
- Limit of 3 external Identity Providers.

## Premium

Enterprise Identity & Access Management for employee workforce scenarios.

- Includes all features.
- Broad support for hybrid IAM use-cases.
- Unlimited support for Oracle and non-oracle Apps.
- Unlimited external Identity Providers.

## External User

Identity storage, Access Management, and API security for consumer and non-employee use-cases.

- Provides social self-service, and consent management.
- Limited enterprise and hybrid IAM features.
- Excludes APP catalog provisioning connectors.

The Default identity domain helps manage access to OCI resources.

Create additional identity domains based on specific needs.

Change domain types; restrictions apply.



# Identity and Access Management-Basics

Oracle Cloud Infrastructure

# Managing OCI IAM Identity Domains

## OCI Identity and Access Management (IAM)

Dr. Saurabh Patil

OU OCI Delivery Team

### Understanding Default Domain and Creating Identity Domains



Understanding the Default domain, home regions, and creating identity domains

### Managing Groups



Adding and managing groups and dynamic groups

### Managing Users



Creating and onboarding single and bulk users

### Managing Policies



Policies to control access to OCI resources

## Oracle Cloud Infrastructure

# Default Identity Domain

### OCI Identity and Access Management (IAM)

Dr. Saurabh Patil

OU OCI Delivery Team

# Default Domain

The screenshot shows the Oracle Cloud Identity Domains interface. The left sidebar has 'Domains' selected. The main area displays 'Domains in saurabhp (root) Compartment'. A table lists one domain:

Name	Domain type	Status	Users	Groups
Default	Free	Active	1	2

A red box highlights the 'Default' row. Below the table, it says 'Showing 1 domain' and 'Page 1'. To the right of the table, there are three green callout boxes with the following text:

- Store and manage users
- Federate and provision users
- Application secure using SSO, SAML, OAuth

On the far right, three more green callout boxes provide information about the domain:

- Can't be deactivated or deleted
- Can't be hidden from the sign-in page
- Is replicated to all regions

The screenshot shows the Oracle Cloud Infrastructure Identity service interface. The left sidebar lists navigation items: Identity domain, Overview, Users, **Groups**, Dynamic groups, Integrated applications, Oracle Cloud Services, Jobs, Reports, Security, Settings, Notifications, and Branding. The main content area is titled "Groups in Default Domain". It includes a search bar and a table with two rows:

<input type="checkbox"/>	Name	Description
<input type="checkbox"/>	All Domain Users	A group representing all users.
<input type="checkbox"/>	Administrators	Administrators

The "Administrators" row is highlighted with a red border. A status message at the bottom says "0 selected".

# Default Domain

## Administrators Group

- Default administrator automatically belongs in this group
- Cannot delete it; must have at least one user in this group
- Policy grants access to all OCI resources in your tenancy

## Administrator User

- Default Administrator user with superuser privileges
- Delegates administrative responsibilities

# Dos and Don'ts for the Administrator Users



- ✓ User and group management
- ✓ Delegated administration roles
- ✓ Multi-Factor Authentication (MFA) configuration
- ✓ Self-registration profiles and policies



- ✗ Don't add users to the Administrators group.
- ✗ Don't use the group for routine or non-administrative tasks.

# Oracle Cloud Infrastructure

## Creating Identity Domains

---

### OCI Identity and Access Management (IAM)

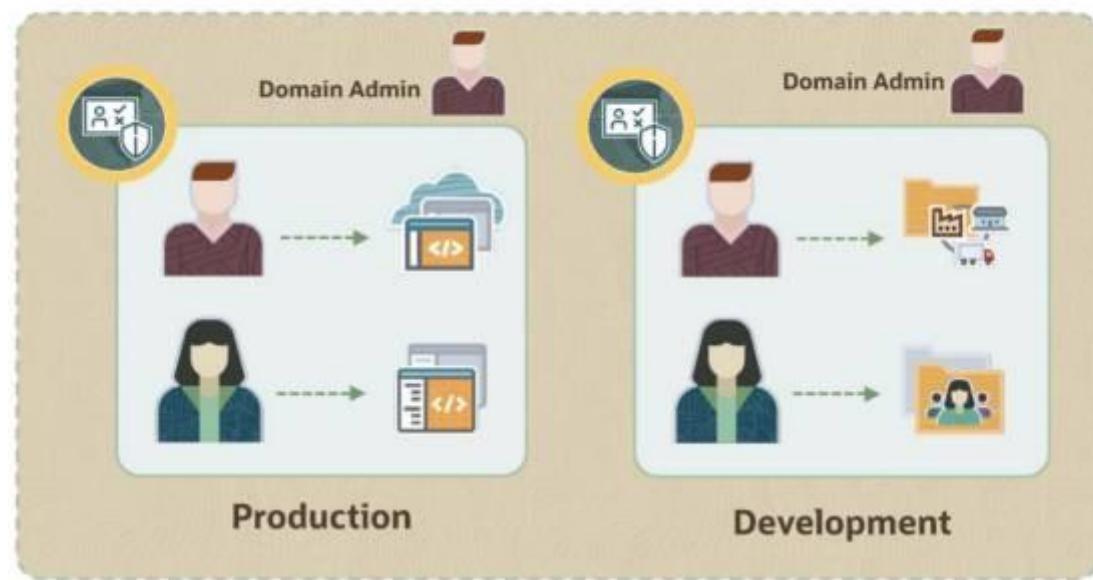
Dr. Saurabh Patil  
OU OCI Delivery Team

## Why do we need multiple identity domains?

Isolation of administrative control

Security and compliance

Simplified management



# Creating Identity Domains



## Identity Domain Administrators

- Manage users, groups, applications, and system configuration.
- Perform delegated administration.
- Enable/disable MFA configuration.
- Create self-registration profiles.

## Identity Domain Region

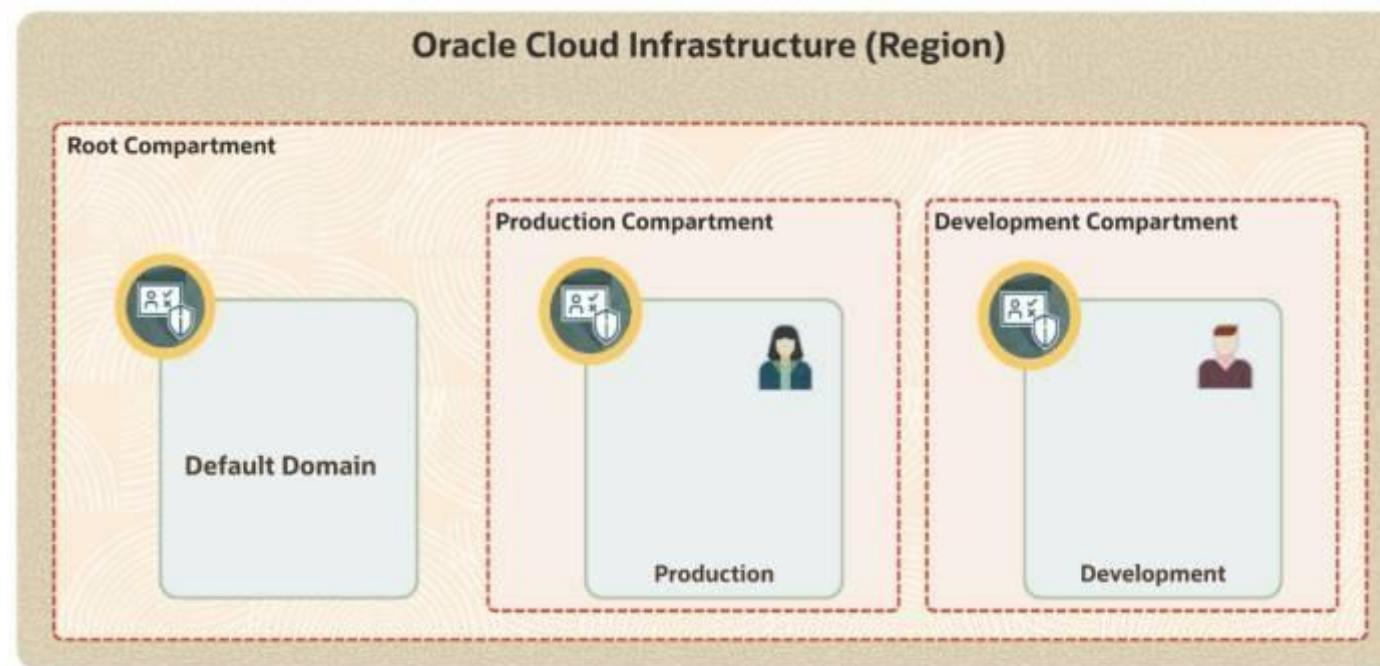
- Selecting Identity Domain Region
- Do not replicate to all regions of the tenancy.



# Demo

---

# Creating Identity Domains



## Oracle Cloud Infrastructure

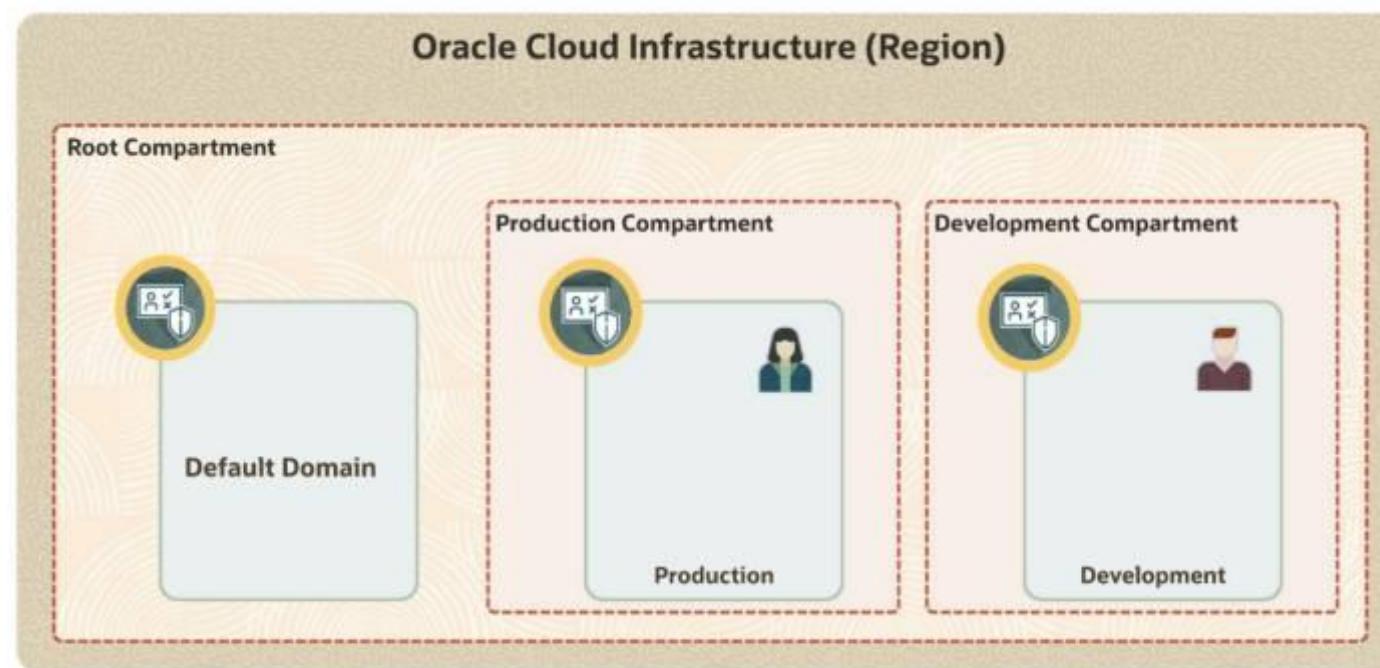
# Demo: Creating Identity Domains

### OCI Identity and Access Management (IAM)

Dr. Saurabh Patil

OU OCI Delivery Team

# Creating Identity Domains



## Oracle Cloud Infrastructure

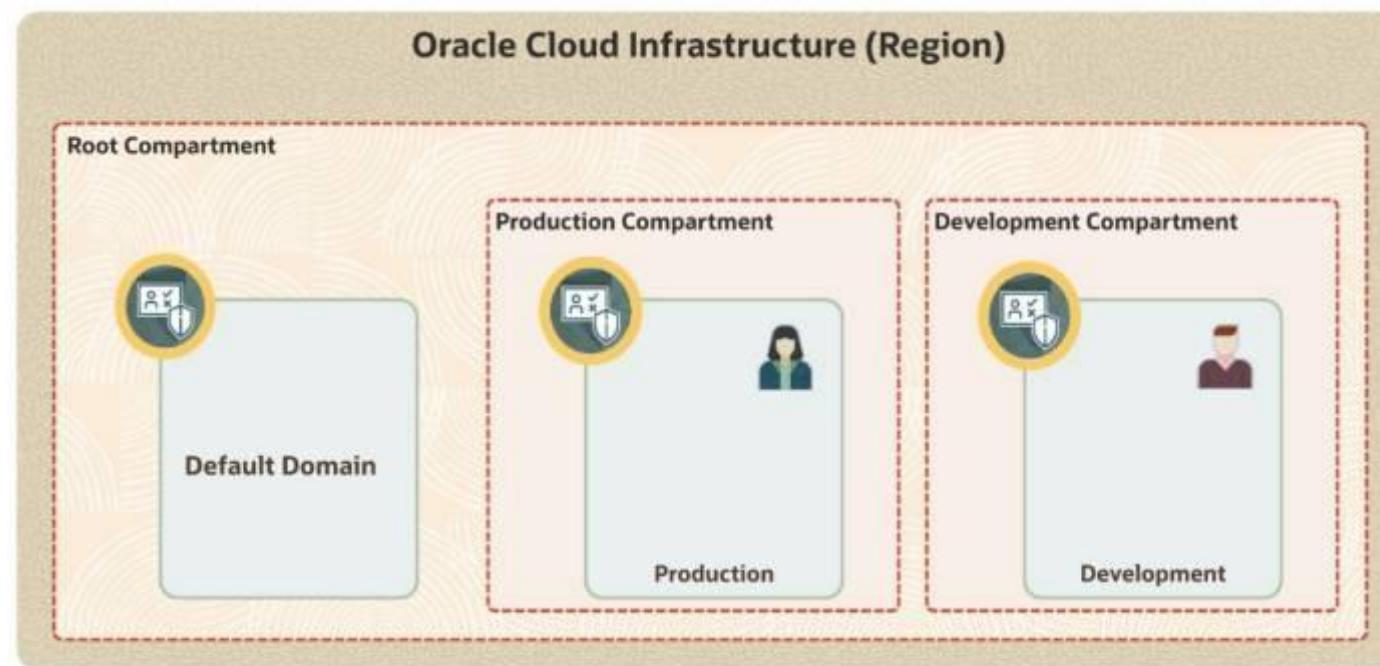
# Demo: Creating Groups

### OCI Identity and Access Management (IAM)

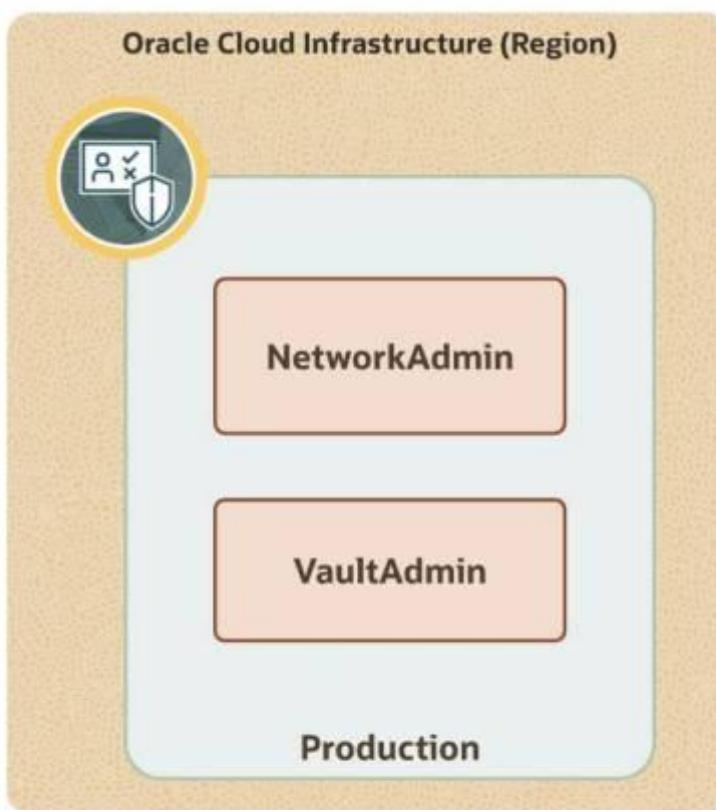
Dr. Saurabh Patil

OU OCI Delivery Team

## Creating Groups



# Creating Groups



# Oracle Cloud Infrastructure Managing Groups

## OCI Identity and Access Management (IAM)

Dr. Saurabh Patil  
OU OCI Delivery Team

## Groups

---



Collections of users



Network Admin



Instances

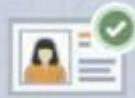


Certificate Manager

## Groups



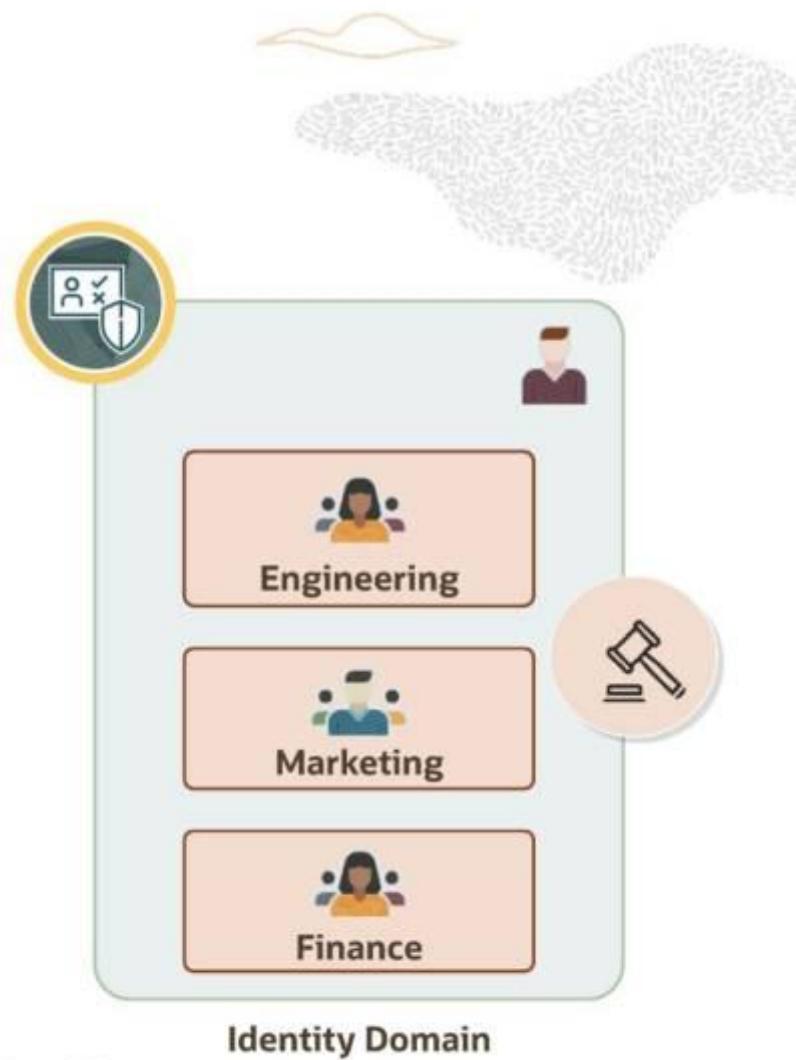
Collections of users



Simplify access management



Audit and compliance



# Default Groups in Identity Domains

## Groups in Production Domain

Groups in Production Domain		
<input type="text"/> Search by group name or description.		
<input type="button" value="Create group"/> <input type="button" value="More actions"/>		
<input type="checkbox"/>	Name	Description
<input type="checkbox"/>	All Domain Users	A group representing all users.
<input type="checkbox"/>	Domain Administrators	Domain Administrators

0 selected

## Domain Administrators

- The administrative user is part of the Domain Administrators group.
- This group can't be deleted.
- At least one user is required in the group.

## All Domain Users

- All users are, by default, part of All Domain Users group.
- This group can't be deleted.

## Oracle Cloud Infrastructure

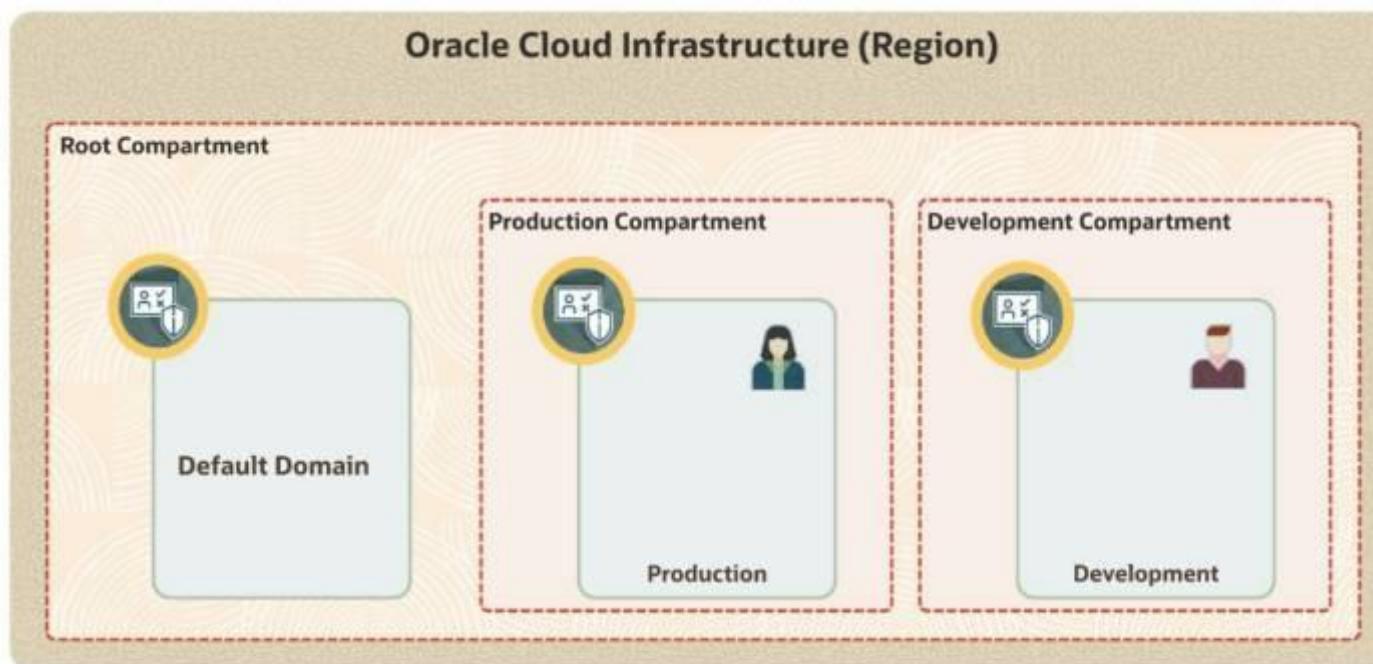
# Demo: Creating Users

### OCI Identity and Access Management (IAM)

Dr. Saurabh Patil

OU OCI Delivery Team

# Creating Groups



# Creating Users



Create User using Console



Create User using CSV import



# Oracle Cloud Infrastructure Managing Users

## OCI Identity and Access Management (IAM)

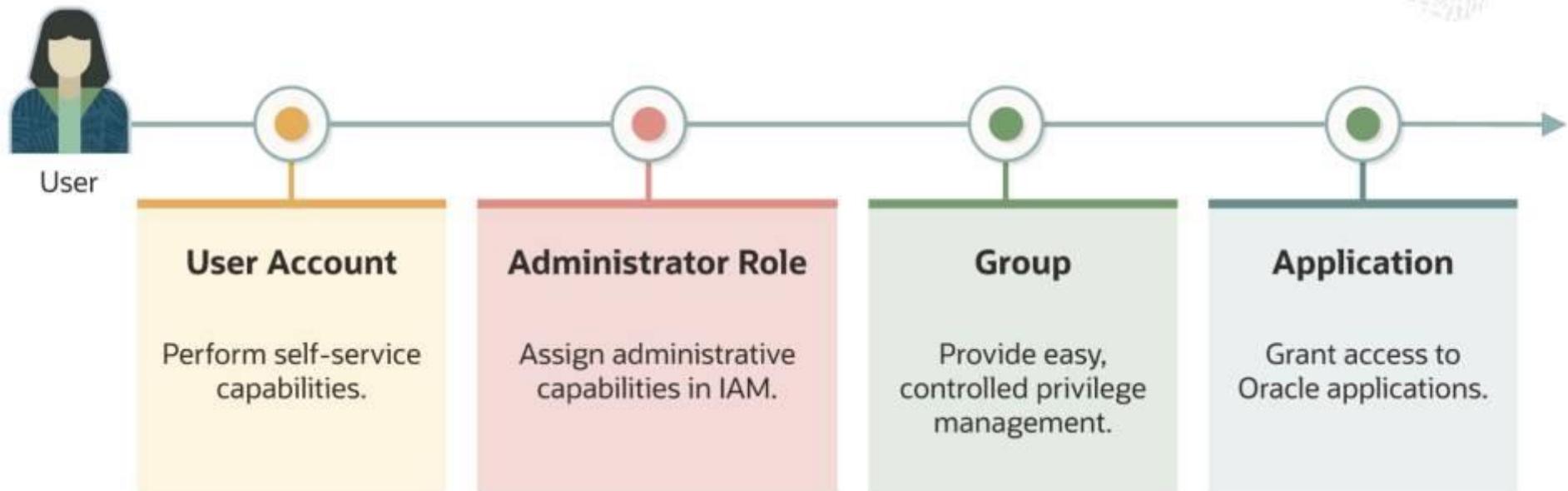
Dr. Saurabh Patil  
OU OCI Delivery Team



## Stages of the IAM User Life Cycle

Non-Existent	Activated	Deactivated
 User profile has not yet been created in the system	 User has active access to Oracle Cloud services and associated privileges	 User access to Oracle Cloud services and privileges is temporarily disabled; can be re-activated
Action	Action	Action
Create	Activate Modify Delete	Activate

# User Lifecycle Management

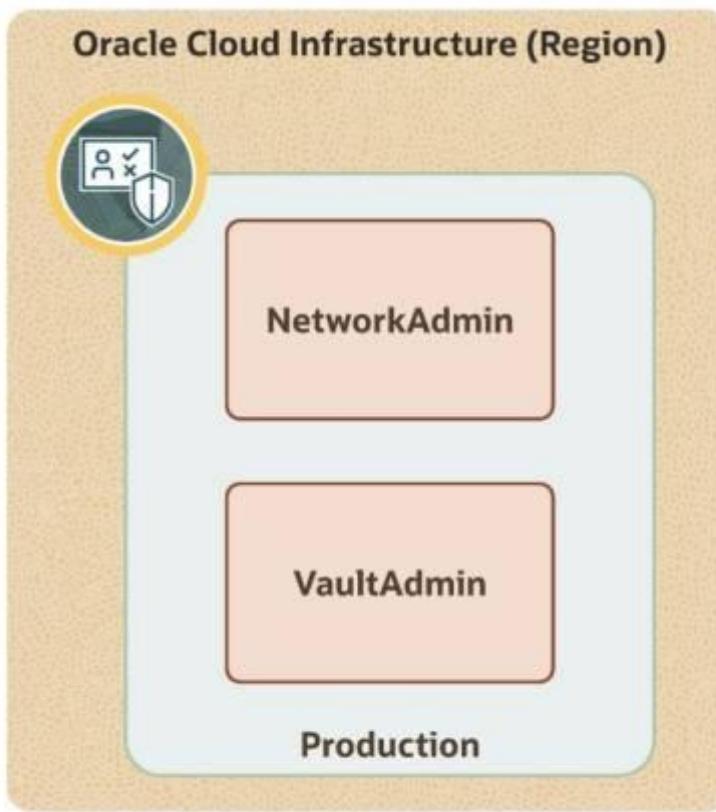




# Demo

---

# Creating Groups



## Oracle Cloud Infrastructure

# Understanding the Administrator Role

### OCI Identity and Access Management (IAM)

Dr. Saurabh Patil

OU OCI Delivery Team

Graphics team: Pls check the font and theme for correctness. pls change the color and feel of the shapes used here to match the redwood design. Animate each point.



## Administrator Roles: Key Points



Predefined roles with specific privileges



Roles associated with identity domains



Efficient delegation of administrative responsibilities



Using roles instead of traditional policies ensures structured access management

# Types of Administrator Roles

## Business Criticality

One strategy is to migrate noncritical data first and then move on to more important business-critical data

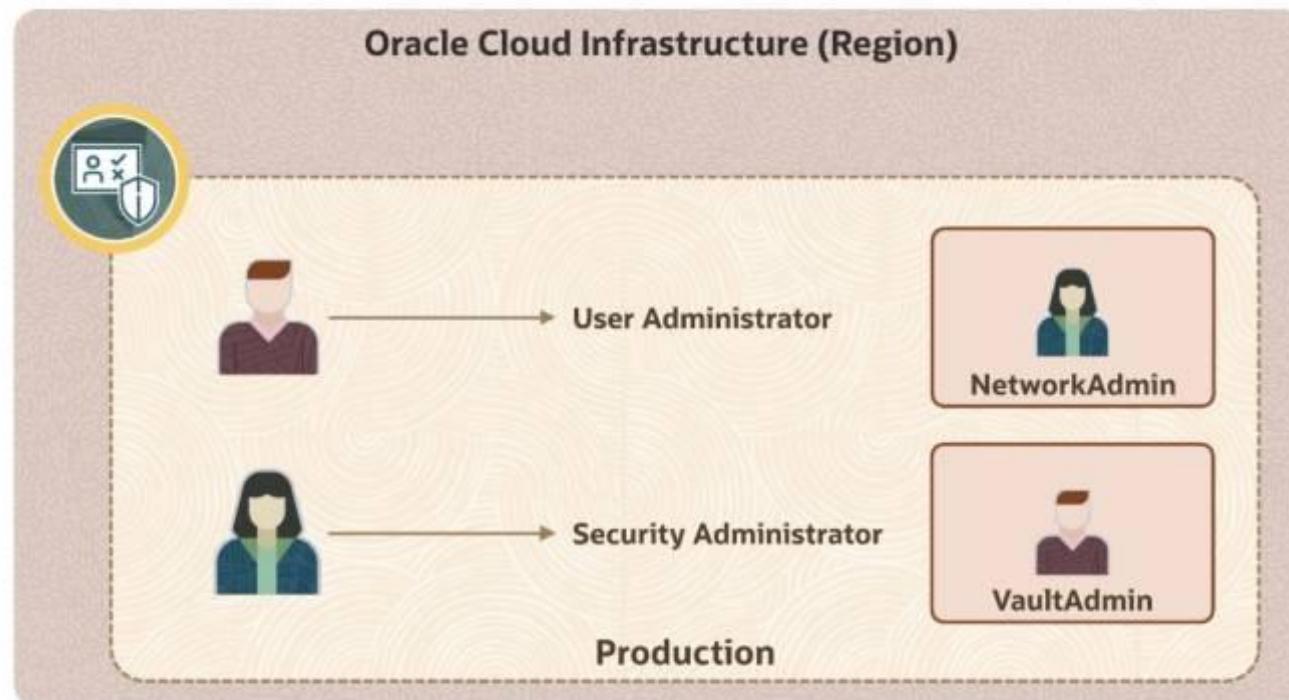




# Demo

---

# Assigning Administrative Roles



Oracle Cloud Infrastructure

# Demo: Understanding Administrator Role

OCI Identity and Access Management (IAM)

# Oracle Cloud Infrastructure Policies

## Identity and Access Management

Oracle Cloud Infrastructure

# Demo: Policies

—  
**OCI Identity and Access Management (IAM)**



# Policies



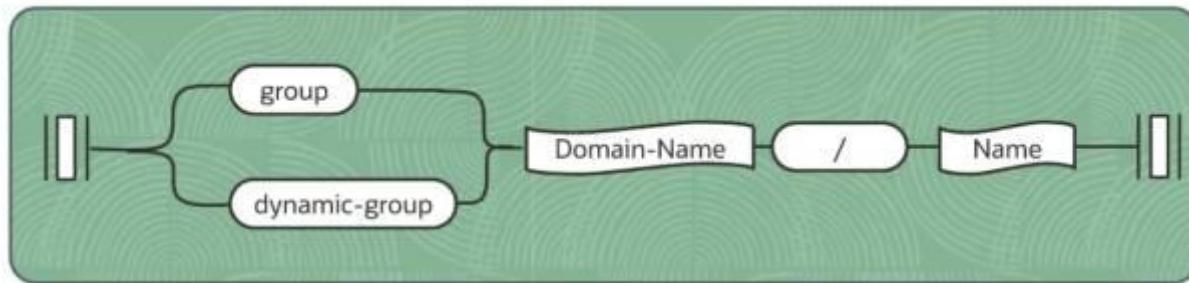
What permissions do you have?

Set using IAM Policies





## Subjects Clause



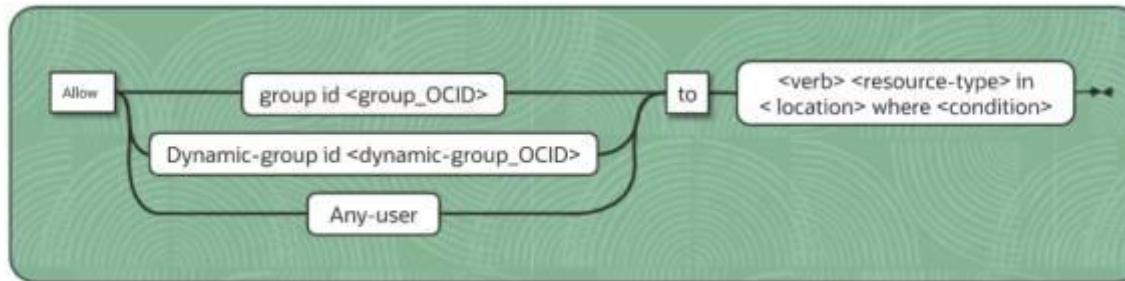
Subjects are a clause for providing access to authenticated actors:

- By membership in an Identity-registered group inside domains (for example, “group Production/Admins”)

Allow group 'Production'/'NetworkAdmin' to manage virtual-network-family in compartment Sandbox



# Subjects Clause



Allow group default/A-Admins, default/B-Admins to manage instance-family in compartment Projects-A-and-B

Subjects are a clause for providing access to authenticated actors:

- By membership in an Identity-registered group inside domains with OCID (for example, "group id OCID.group.dfd...sxxx")
- As a wildcard, with "any-user" (any request from the tenancy)
- More than one name or group can be named in Subjects element. These can be chained by kind (for example, "group Alice, Bob").



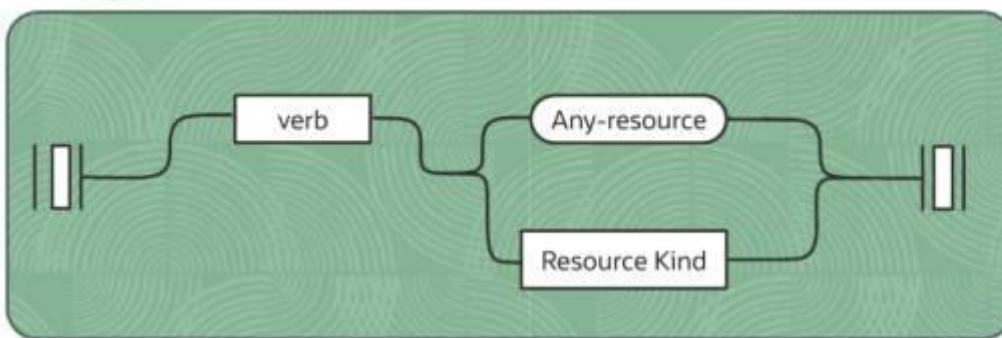
## Subjects Clause

Allow group NetworkAdmin to manage virtual-network-family in compartment Sandbox

Allow group 'Default'/'NetworkAdmin' to manage virtual-network-family in compartment Sandbox



## Actions Clause



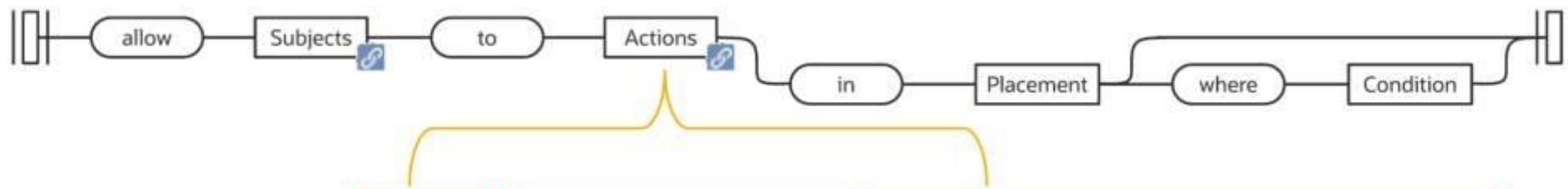
Services define one or more permissions that any given API call will require.

These are documented and bundled into convenient “verb resource” pairs (for example, “inspect objects”, “manage objects”) for Actions clauses.

Verb	Type of access	Permission Example
inspect	Permissions necessary to observe, enumerate and monitor, w/o access to confidential information	«inspect objects» Learn details about objects stored in buckets - quantity, confirmation of object existence, and so on, without getting access to the object itself
read	Permissions necessary to access but not alter resources	«read objects» Reads the contents of the object
use	Permissions to modify pre-existing resources	«reencrypt objects» Re-encrypt objects using a different key version
manage	Permissions to do anything to the resource kind	«create objects» Create or delete objects



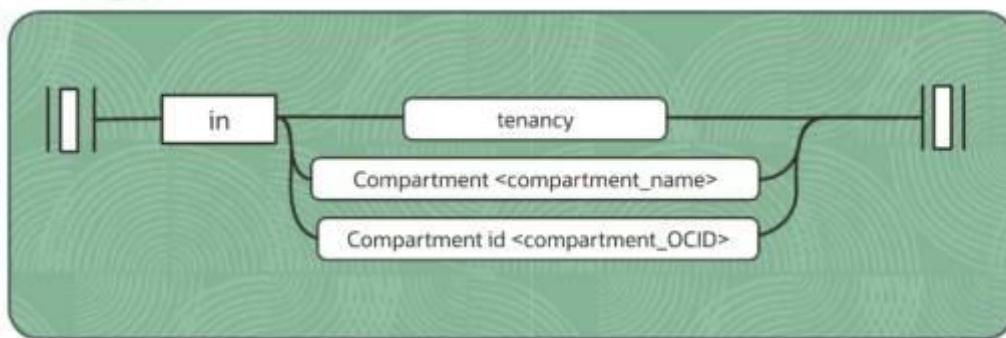
## Actions Clause



Verb	Aggregate resource-type	Individual resource type
inspect	all-resources	db-systems, db-nodes, db-homes, databases
read	database-family	instances, instance-images, volume-attachments, console-histories
	instance-family	
	object-family	buckets, objects
use	virtual-network-family	vcn, subnet, route-tables, security-lists, dhcp-options, and many more resources
manage	volume-family	Volumes, volume-attachments, volume-backups



# Placement



Placement determines the scope of the policy and where the action is allowed.

Examples:

- To specify a compartment by name
- To specify a compartment by OCID

Allow group 'Prod'/'NetworkAdmin' to manage virtual-network-family in compartment Sandbox

Allow group 'Prod'/'NetworkAdmin' to manage virtual-network-family in compartment id ocidl.compartment.oc1..aaaaaaaaayzfq...4fmameqh7lcdlihrvur7xq

## Oracle Cloud Infrastructure

# Compartments

### OCI Identity and Access Management (IAM)



# Compartment

Collection  
of related  
resources

Tenancy/ Root Compartment

Compartment Network



Virtual Cloud  
Network



Load  
Balancer

Compartment Storage



Block  
Storage



File  
Storage



Object  
Storage

Isolate and  
control  
access

Root Compartment can hold all the cloud resources

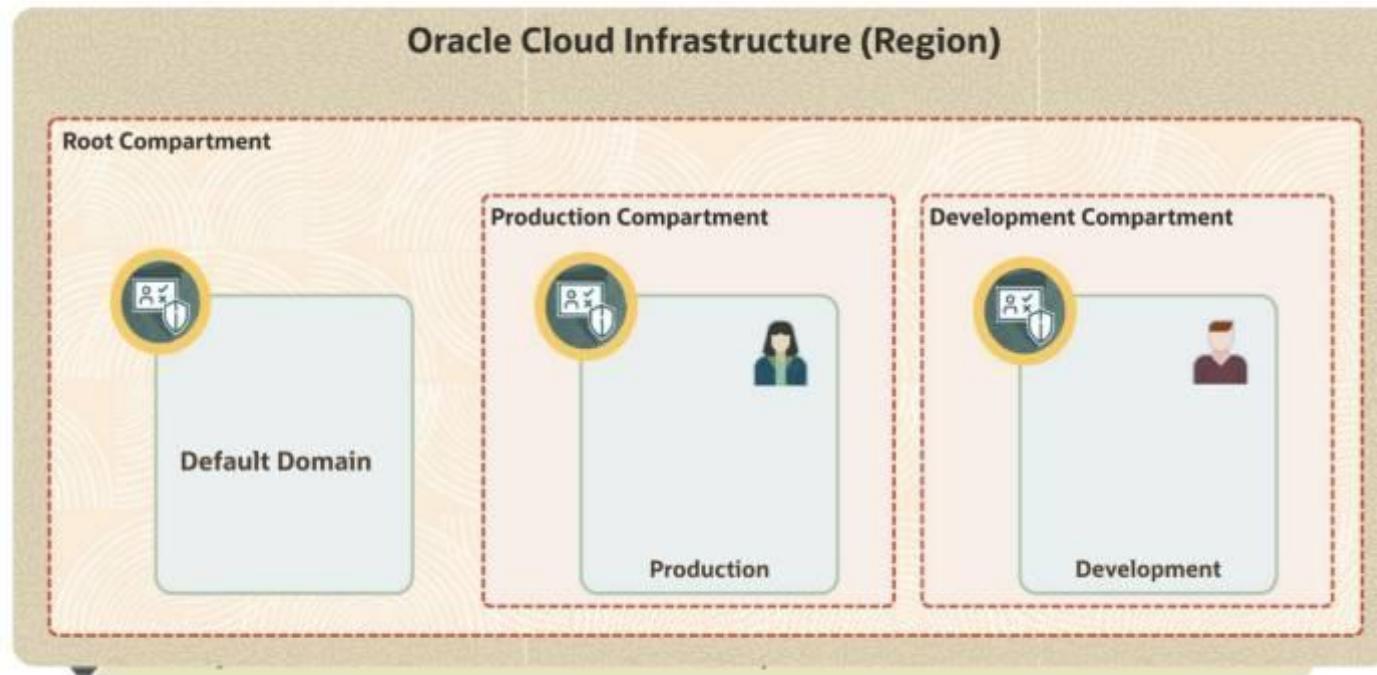


**Best practice:** Create dedicated compartments to isolate resources.



# Compartment

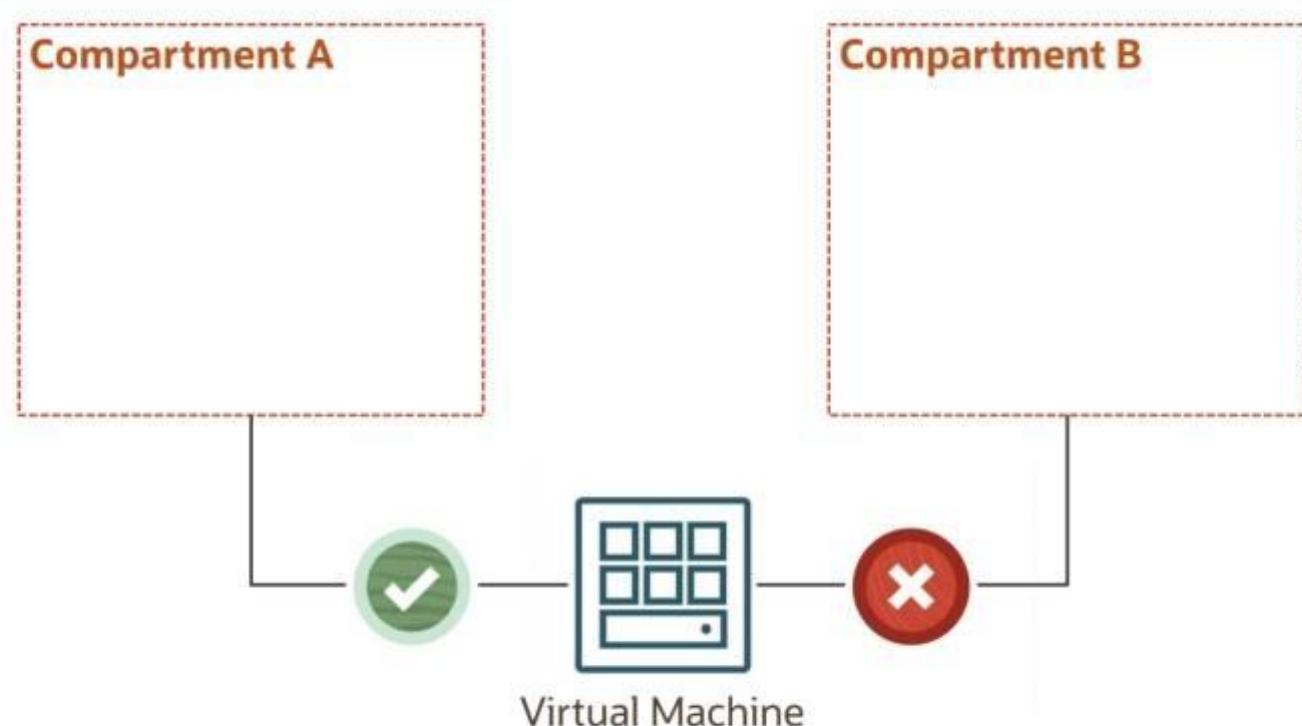
Collection  
of related  
resources



Isolate and  
control  
access

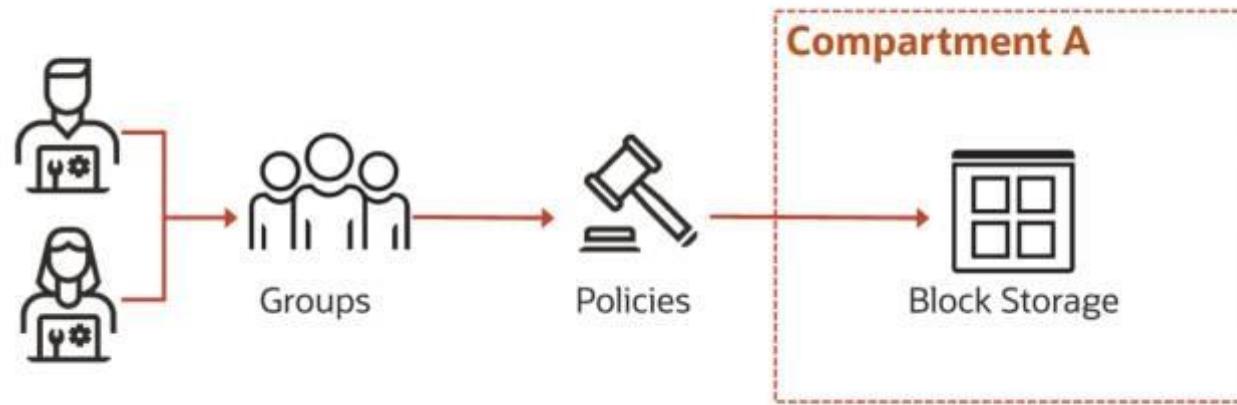
## Resource Compartments

Each resource belongs to a single compartment



# Compartments

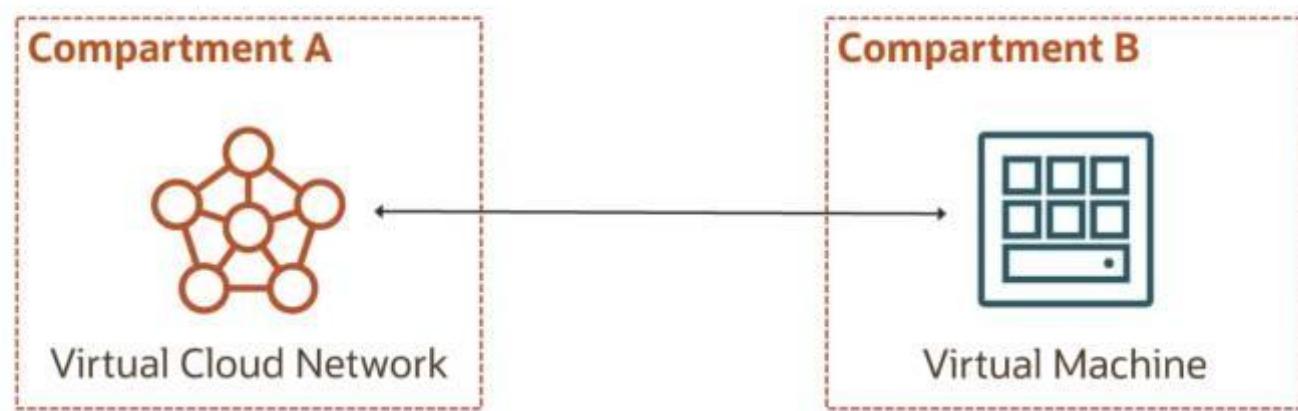
## Access



Users + Policies = Access to Compartments

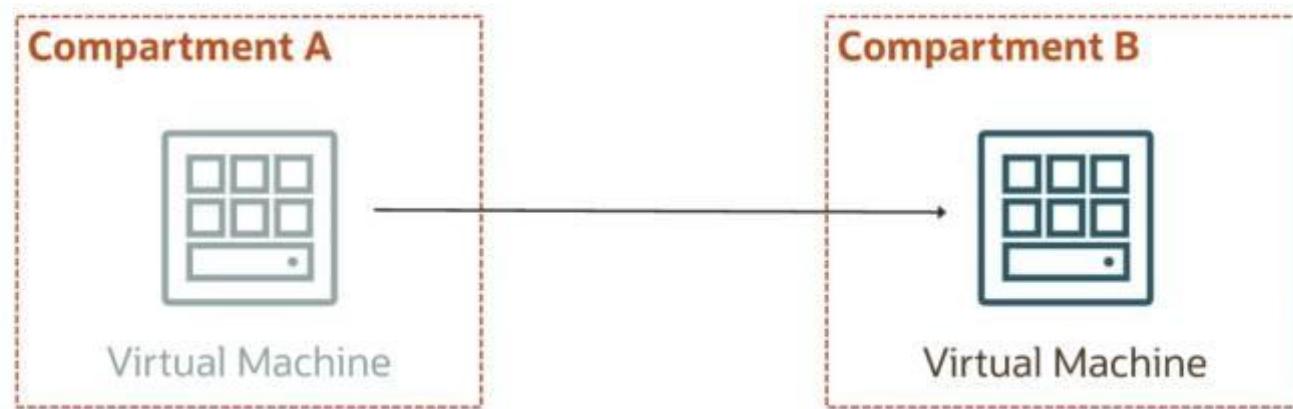
## Interaction of Resources

Resources can interact with other resources in different compartments.

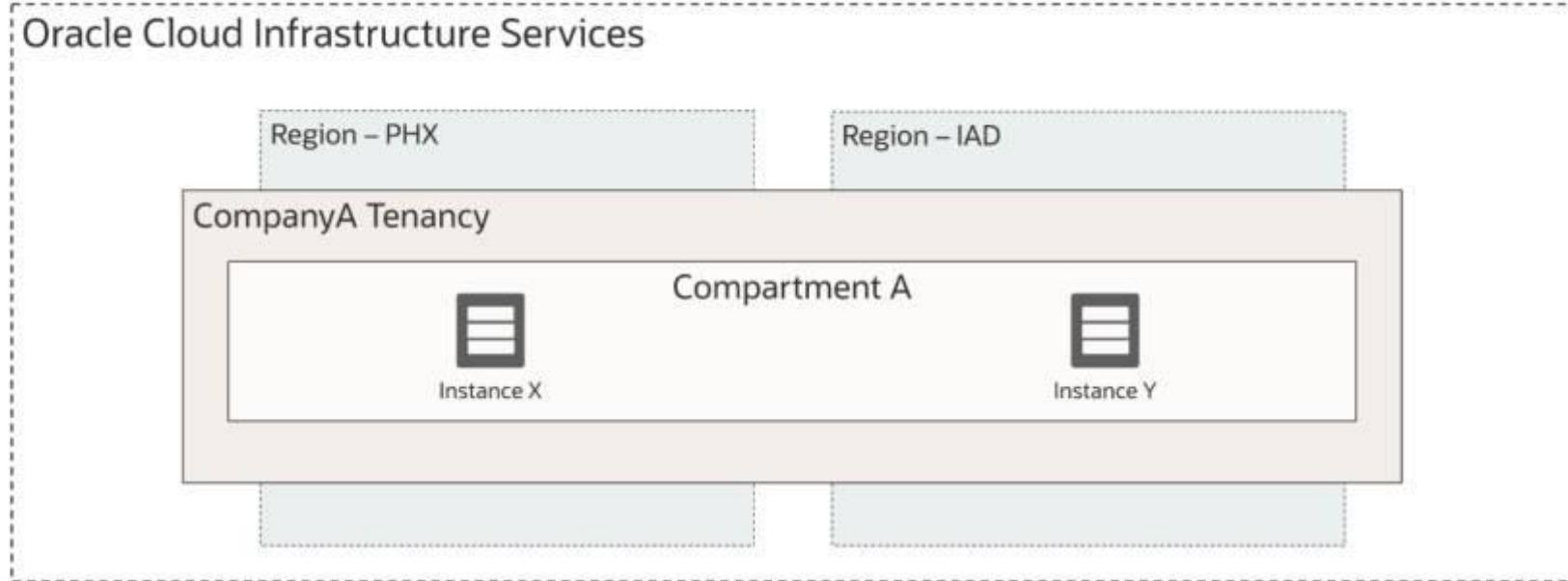


## Movement of Resources

Resources can be moved from one compartment to another.

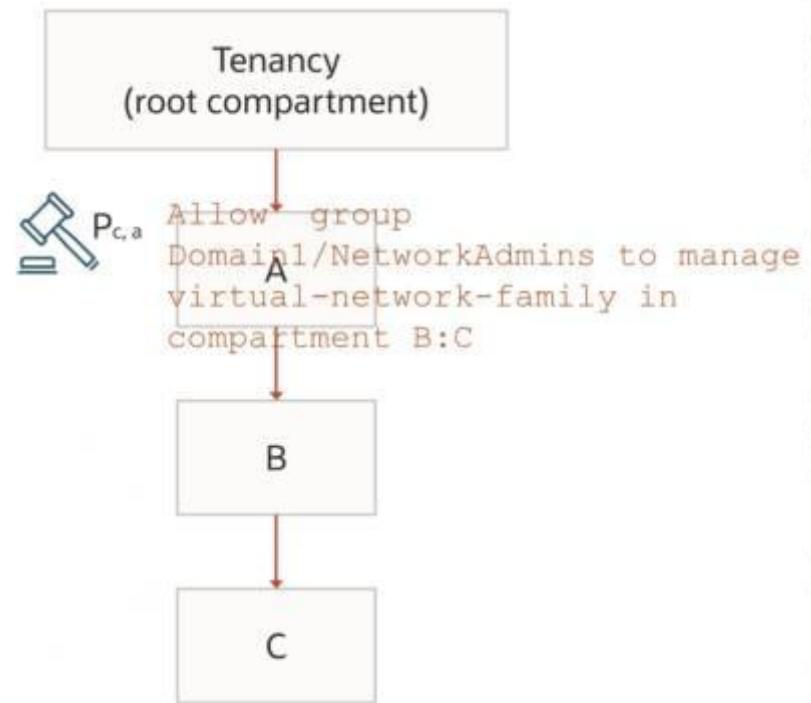


# Multiple Regions



Resources from multiple regions can be in the same compartment.

# Nested Compartments

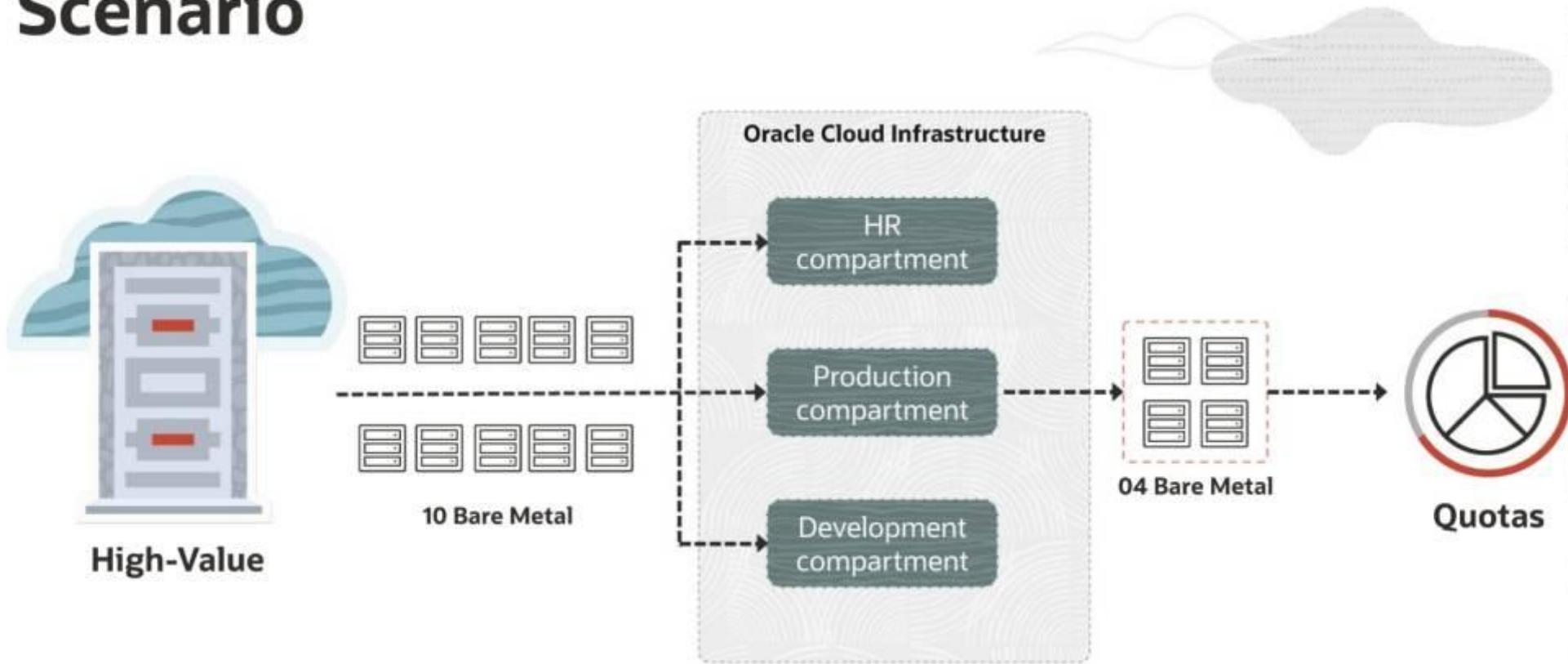


# Oracle Cloud Infrastructure Compartment Quotas

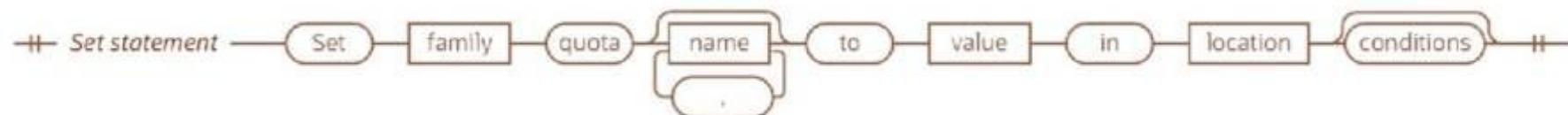
---

## OCI Identity and Access Management

# Scenario



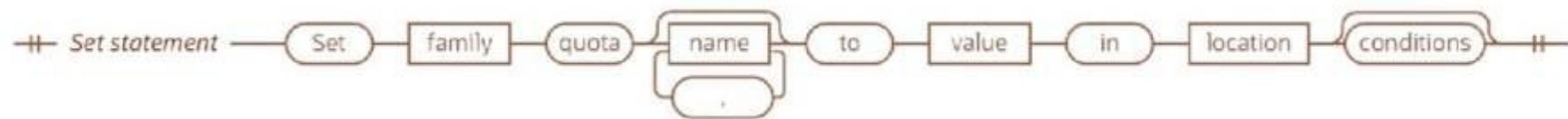
# Quota Syntax



**Don't allow more than four virtual cloud networks (VCN) in a compartment**

```
set <family>
  compute-core
  object-storage
  vcn
```

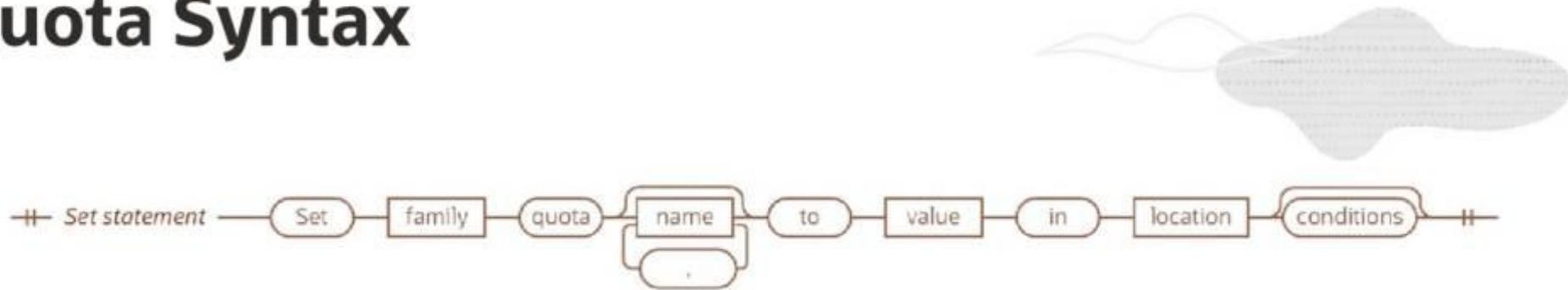
# Quota Syntax



**Don't allow more than four virtual cloud networks (VCN) in a compartment**

```
set vcn quota <quota-name>
      vcn-count
      reserved-public-ip-count
```

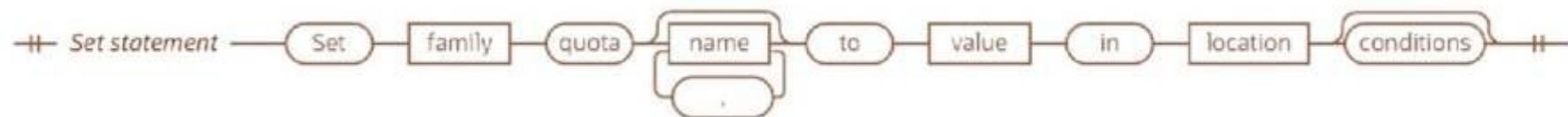
## Quota Syntax



**Don't allow more than four virtual cloud networks (VCN) in a compartment**

```
set vcn quota vcn-count to <value>
```

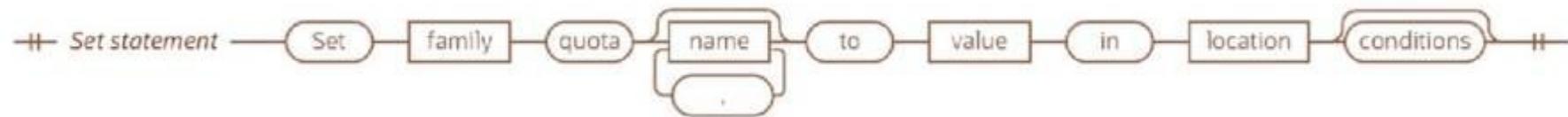
# Quota Syntax



**Don't allow more than four virtual cloud networks (VCN) in a compartment**

```
set vcn quota vcn-count to 4 in <location>
          tenancy
          compartment <name>
```

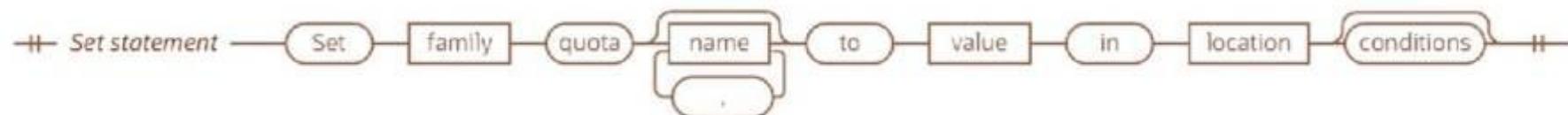
# Quota Syntax



**Don't allow more than four virtual cloud networks (VCN) in a compartment**

```
set vcn quota vcn-count to 4 in compartment production
```

# Quota Syntax



**Don't allow more than four virtual cloud networks (VCN) in a compartment**

```
set vcn quota vcn-count to 4 in compartment Production
```

# Quota Examples



Allocate only one Exadata resources in the entire tenancy

```
set database quota /*exadata*/ to 1 in tenancy
```

Don't allow more than 10 OCPUs for shapes in the VM.Standard2 and BM.Standard2 series in the entire tenancy

```
set compute-core quota standard2-core-count to 10 in tenancy
```

## Types of Quota Policy Statement

### Three Types



#### set

Sets the maximum number of a cloud resource that can be used for a compartment.



#### unset

Resets quotas back to the default service limits.



#### zero

Removes access to a cloud resource for a compartment.

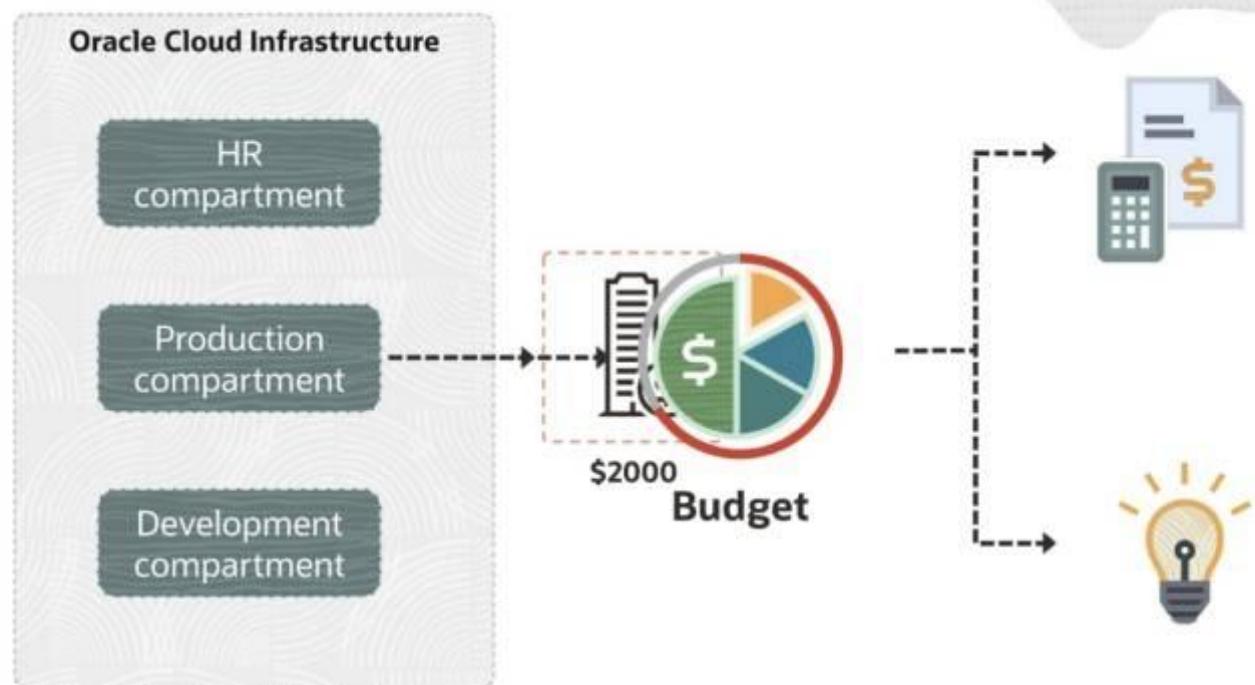
# Quota Examples



**Allocate all Exadata resources to the Production compartment**

```
zero database quota /*exadata*/ in tenancy  
unset database quota /*exadata*/ in compartment Production
```

# Budgets





# Identity and Access Management-Advanced

## Oracle Cloud Infrastructure

# Policy Inheritance and Attachment

### OCI Identity and Access Management (IAM)

Dr. Saurabh Patil

OU OCI Delivery Team

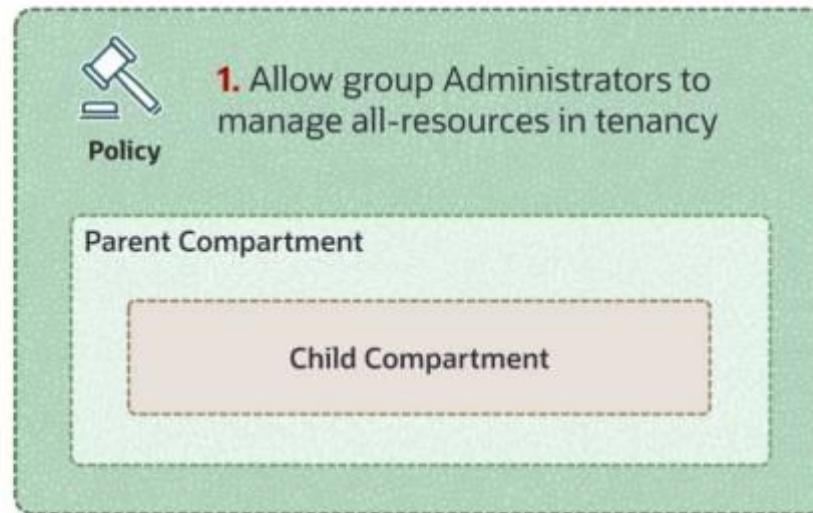
# Policy Inheritance

Concept of inheritance: Compartments inherit any policies from their parent compartment.

- OCI has a built-in policy for Administrators:  
**Allow group Administrators to manage all-resources in tenancy**
- Because of Policy Inheritance, the Administrators group can also do anything in any of the compartments in the tenancy.



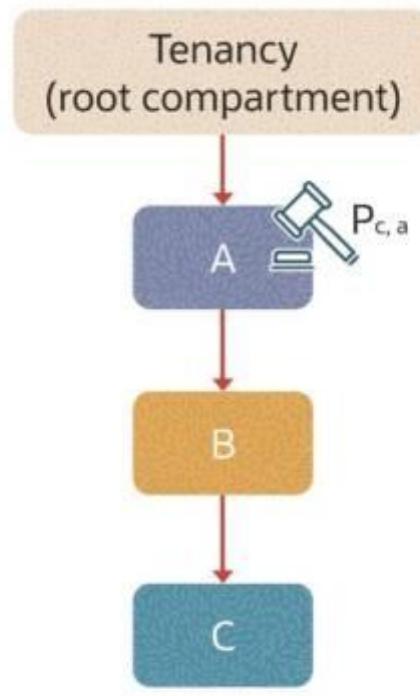
## Tenancy/Root Compartment



# Policy Inheritance

Three levels of compartments: A, B, and C

- Policies that apply to resources in compartment A also apply to resources in compartments B and C.
- PA, policy in compartment A:  
Allow group Domain1/NetworkAdmins to manage virtual-network-family in compartment A
- Policy PA allows the group NetworkAdmins to manage VCNs in compartments A, B, and C.

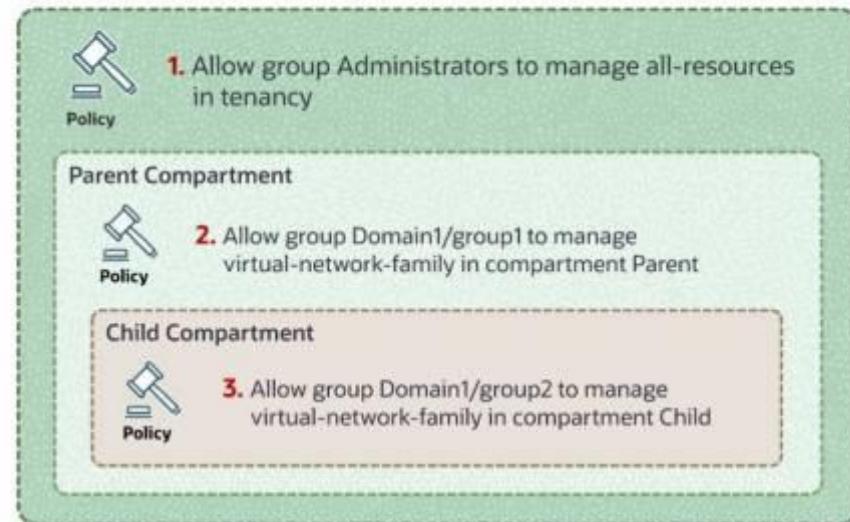


# Policy Attachment

- When you create a policy, you must attach it to a compartment (or tenancy).
- Where you attach it controls who can then modify it or delete it.
  - Attach it to tenancy (root compartment)
    - Anyone with access to manage policies in the tenancy can then change or delete it.
  - Attach to child compartment
    - Anyone with access to manage the policies in that compartment can change or delete it.

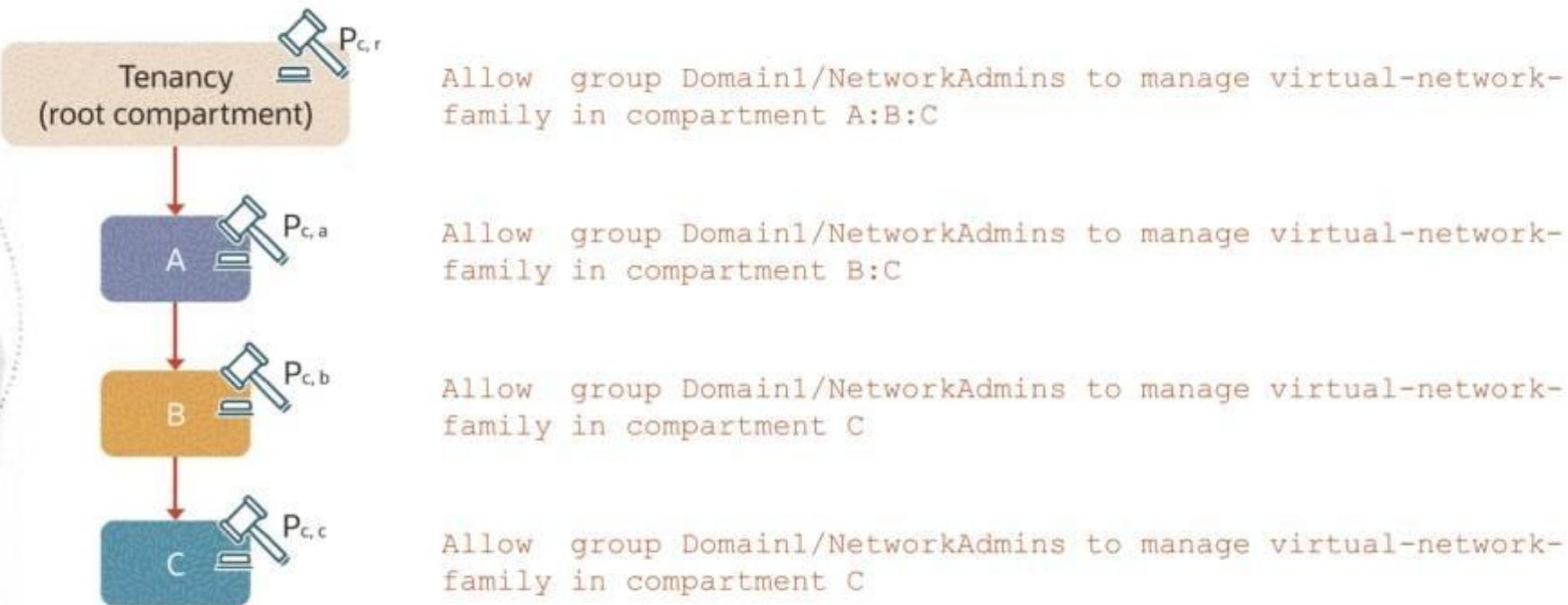


## Tenancy/Root Compartment



# Policy Attachment

You want to create a policy to allow NetworkAdmins to manage VCNs in compartment C.

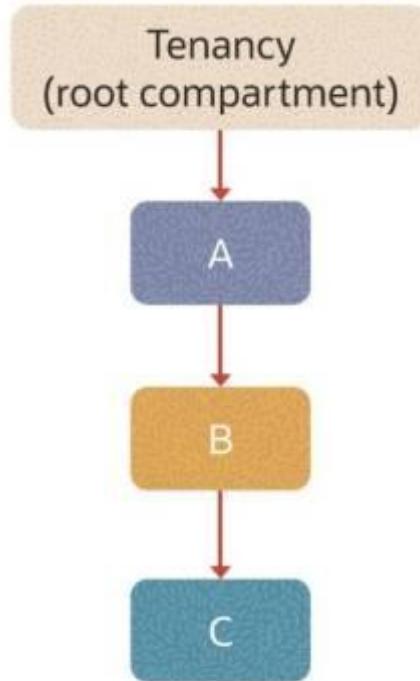


## Oracle Cloud Infrastructure

# Demo: Policy Inheritance and Attachment

### OCI Identity and Access Management (IAM)

Dr. Saurabh Patil  
OU OCI Delivery Team

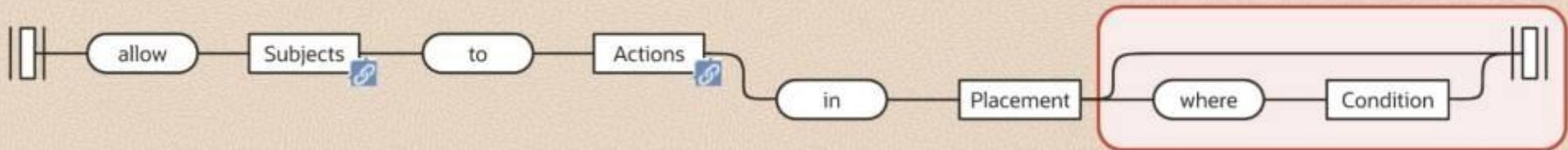


# Oracle Cloud Infrastructure Conditional Policies

## OCI Identity and Access Management (IAM)

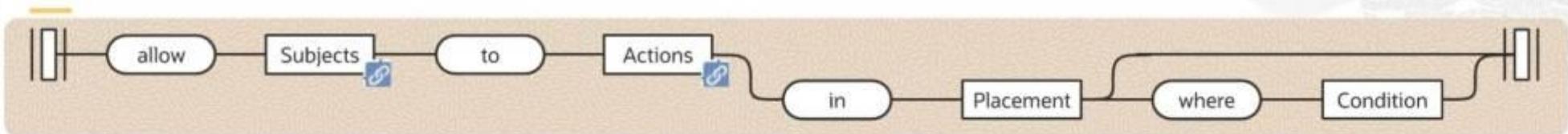
Dr. Saurabh Patil  
OU OCI Delivery Team

# Conditional Policies



- A Condition clause enables more complicated and fine-grain access control.
- Broadly, a condition evaluates to *True*, *False*, or *Not Applicable*

# Conditional Policies



Use variables when adding conditions to a policy.

- Variables are hierarchically named, prefixed accordingly with either `request` or `target` followed by a period (.).
  - **request** – Used for attributes about the request itself.
    - For example, `request.user.id` should contain the OCID of the user who made the request.
    - Suppose you need to allow users to list objects, and create a new object in a bucket.  
You may include  
`request.permission='OBJECT_CREATE', request.permission='OBJECT_INSPECT'`
  - **target** – Used for attributes about the resource/target of interest.
    - For example, to limit access to a specific bucket, add the condition where  
`target.bucket.name='<bucket_name>'`

# Conditions



- Syntax for a single condition: `variable =| != value`
  - `=| !=` returns true or false for every condition
  - `!=` inverts the result
- Syntax for multiple conditions: `any|all {<condition>, <condition>, ...}`
  - **any**: A condition set that starts with `any` is a disjunctive - **logical OR** - set of sub-conditions. Any condition within the `{ }` that results in true means that the condition is true.
  - **all**: A condition set that starts with `all` is a conjunctive - **logical AND** - set of sub-conditions. Every condition within the `{ }` must be true for the condition to be true.

# Conditions



Types of values used in conditions:

Type	Examples
String	'johnsmith@example.com' 'ocid1.compartment.oc1..aaaaaaaaaph...ctehnqg756a'
Pattern	single quotation marks are required around the value <code>/HR*/</code> (matches strings that start with "HR") <code>/*HR/</code> (matches strings that end with "HR") <code>/*HR*/</code> (matches strings that contain "HR")

# Examples



- Policy allows PHX-Admins to manage all aspects of all resources in US West  
Allow group DomainA/PHX-Admins to manage all-resources in tenancy `where request.region='PHX'`
- Policy enables the NetworkAdmins group to manage cloud networks in any compartment except the one specified  
Allow group DomainA/NetworkAdmins to manage virtual-network-family in tenancy `where target.compartment.id != 'ocid1'`
- Policy limits Autonomous Database access to databases and backups for a specific workload type  
Allow group DomainA/ADB-Admins to manage autonomous-database in tenancy `where target.workloadType = 'workload_type'`

## Oracle Cloud Infrastructure

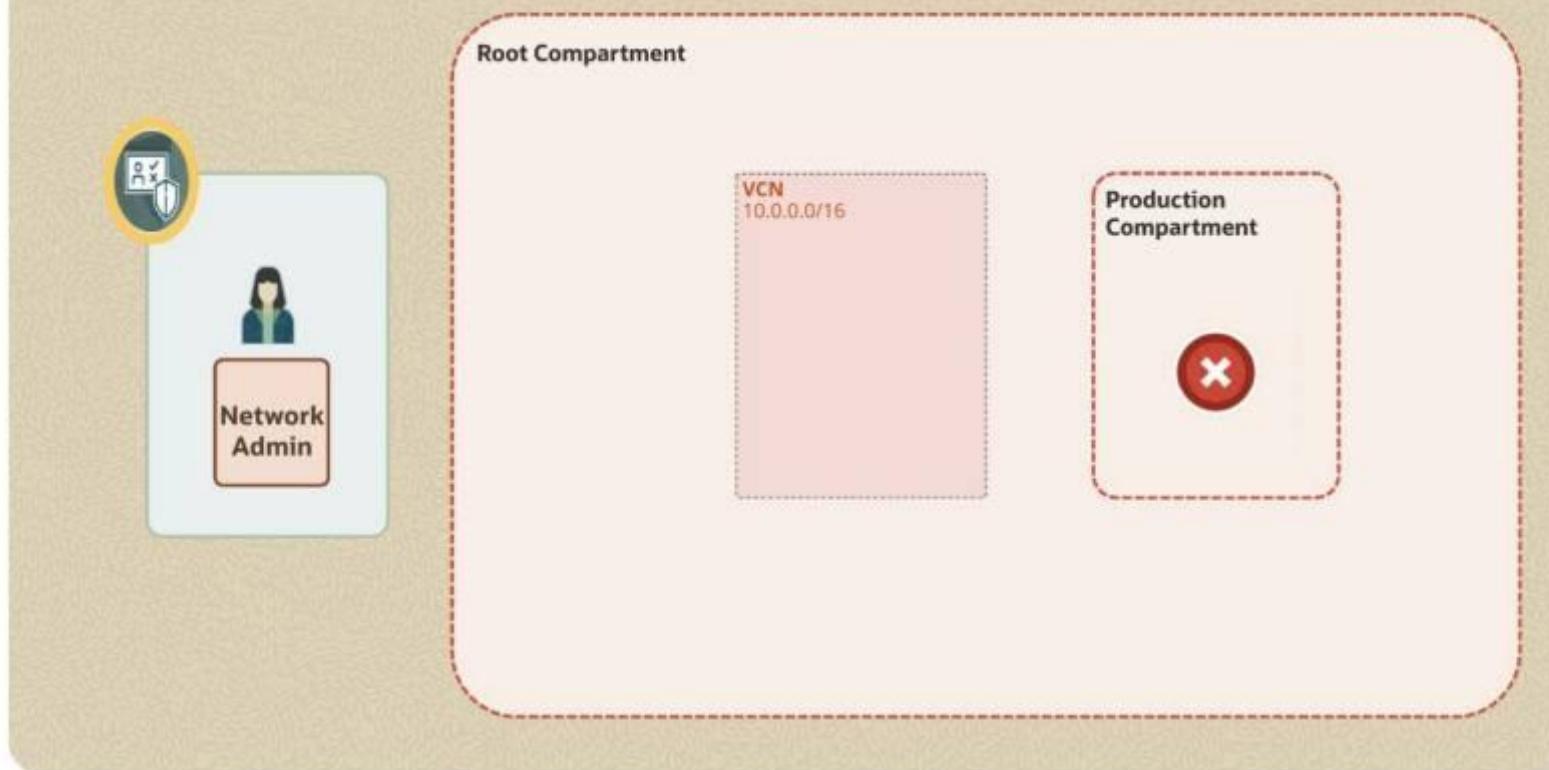
# Demo: Creating Users

### OCI Identity and Access Management (IAM)

Dr. Saurabh Patil

OU OCI Delivery Team

## Oracle Cloud Infrastructure (Region)



## Oracle Cloud Infrastructure

# Enforce Least Privileged: Advanced Policies

### OCI Identity and Access Management (IAM)

Dr. Saurabh Patil

OU OCI Delivery Team

# Permissions



- Permissions = Atomic units of AuthZ that control a user's ability to perform operations on resources
- Verbs simplify the process of granting multiple related permissions that cover a broad set of access.
- Policy (verb + resource-type) = Access to one or more predefined permissions
- Policy (e.g., inspect volumes) = Access to a permission called VOLUME\_INSPECT
- Each API operation requires the caller to have access to one or more permissions.

Verb + Resource type	Inspect Volumes	Read Volumes	Use Volumes	Manage Volumes
Permission	VOLUME_INSPECT	VOLUME_INSPECT	VOLUME_INSPECT VOLUME_UPDATE VOLUME_WRITE	VOLUME_INSPECT VOLUME_UPDATE VOLUME_WRITE VOLUME_CREATE VOLUME_DELETE VOLUME_MOVE
APIs	ListVolumes GetVolume	No extra	AttachVolume DetachVolume	CreateVolume DeleteVolume ChangeVolumeCompartment

# Example



## Policy-A

```
{ Allow group DomainA/AuditDG to manage objects in compartment AcmeCorp }
```

## Policy-B

```
{ Allow group DomainA/AuditDG to manage objects in compartment AcmeCorp where all { target.bucket.name = 'audit_logs_bucket', request.permission='OBJECT_CREATE' } }
```



## Example

Group XYZ to list, create, write, update, or move block volumes, but not delete them

```
{ Allow group DomainA/XYZ to manage groups in tenancy where  
any {  
request.permission='VOLUME_INSPECT',  
request.permission='VOLUME_CREATE',  
request.permission='VOLUME_WRITE',  
request.permission='VOLUME_UPDATE',  
request.permission='VOLUME_MOVE' }  
  
{ Allow group DomainA/XYZ to manage groups in tenancy where  
request.permission != 'VOLUME_DELETE'
```

Conditions based on specific API operations

```
{ Allow group DomainA/XYZ to manage groups in tenancy where  
any {  
request.operation='ListVolumes',  
request.operation='GetVolume',  
request.operation='AttachVolume',  
request.operation='CreateVolume',  
request.operation='ChangeVolumeCompartment' }
```

## Example



Group ObjectWriters can inspect and upload objects in any buckets in the compartment ABC:

```
{ Allow group DomainA/ObjectWriters to manage objects in  
compartment ABC where  
any {request.permission='OBJECT_CREATE',  
request.permission='OBJECT_INSPECT'  
}
```

To limit access to a specific bucket in a particular compartment, add the condition where target.bucket.name='<bucket\_name>':

```
{ Allow group DomainA/ObjectWriters to manage objects in  
compartment ABC where  
all {target.bucket.name = 'BucketA',  
any {request.permission='OBJECT_CREATE',  
request.permission='OBJECT_INSPECT'  
}}
```

## Example



Group Contractors can use instances only during specific time periods.

{ Allow DomainA/Contractors to use instances in compartment contractors where  
all { request.utctimestamp after '<TIME>',  
request.utc-timestamp before '<TIME>'  
}

Oracle Cloud Infrastructure

# Tag Based Access Control

—  
**Identity and Access Management**

# Tag-based Access Control



- Tag-based access control (TBAC) allows to define policies with tags that span compartments, groups, and resources
- Scope access based on the tags applied to a resource
- TBAC = conditions + set of tag variables
- Access can be controlled based on a tag
  - On the requesting resource (group, dynamic group, or compartment)
  - Or the target of the request (resource or compartment)

# Tag-based Access Control



Tag applied to requestor	Variable	Sample policy
Group	request.principal.group.tag.{tagNamespace}.{tagKeyDefinition} = '<value>'	allow any-user to manage instances in compartment HR where <code>request.principal.group.tag.Operations.Project= 'Prod'</code> Any user who belongs to a group that has been tagged with Operations.Project='Prod' can manage instances in HR compartment
Dynamic Group	request.principal.group.tag.{tagNamespace}.{tagKeyDefinition} = '<value>'	allow dynamic-group DomainA/InstancesA to manage object-family in compartment HR where <code>request.principal.group.tag.Operations.Project= 'Prod'</code> Instances in dynamic group InstancesA that has been tagged with Operations.Project='Prod' can manage objects in the compartment HR
Compartment	request.principal.compartment.tag.{tagNameSpace}.{tagKeyDefinition} = '<value>'	allow dynamic-group DomainA/InstancesA to manage object-family in compartment HR where <code>request.principal.compartment.tag.Operations.Project= 'Prod'</code> Instances in dynamic group InstancesA that also reside in a compartment that has been tagged with Operations.Project='Prod' can manage objects in the tenancy.

# Tag-based Access Control



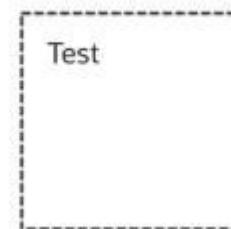
Tag applied to target	Variable	Sample policy
Resource	target.resource.tag.{tagNamespace}.{tagKeyDefinition}='<value>'	<pre>allow group DomainA/GroupA to manage all-resources in compartment HR where target.resource.tag.Operations.Project= 'Prod'</pre> <p>Policy allows GroupA to manage any resource that has been tagged with Operations.Project='Prod'</p>
Compartment	target.resource.compartment.tag.{tagNamespace}.{tagKeyDefinition}='<value>'	<pre>allow group DomainA/GroupA to manage all-resources in tenancy where target.resource.compartment.tag.Operations.Project= 'Prod'</pre> <p>Policy allows the members of GroupA to manage all resources in the tenancy that are in compartments that are tagged with the Operations.Project='Prod' tag.</p>

# Example



Set up a Test compartment for members of the three projects to share

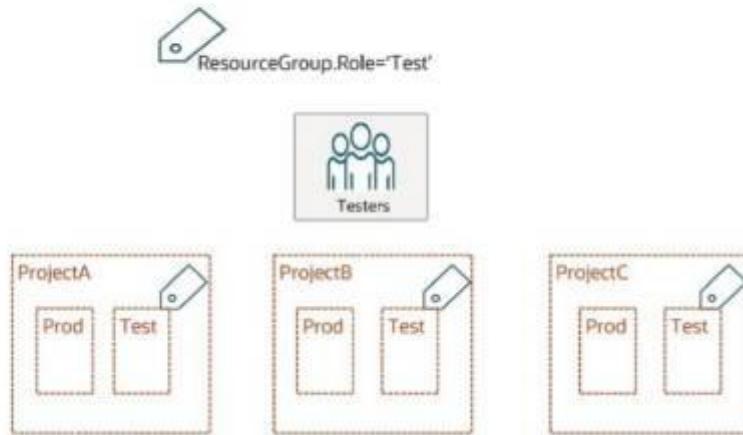
allow any-user to manage all-resources in compartment Test where  
`request.principal.group.tag.EmployeeGroup.Role = 'Admin'`



- All existing admin groups with the tag have access to Test compartment
- Any new group tagged with `EmployeeGroup.Role='Admin'` will have access without updating policy statements



# Example



Give test engineers access to the test compartments across all three projects in your Domain

allow group DomainA/Testers to use all-resources in Projects where

`target.resource.compartment.tag.ResourceGroup.Role='Test'`

- Allow group Testers to access the resources across all three test compartments.

Graphics team: Pls check the font and theme for correctness, pls change the color and feel of the shapes used here to match the redwood design. Animate each components. Recreate image.

Oracle Cloud Infrastructure

# Demo: Tag Based Access Control

—  
**OCI Identity and Access Management (IAM)**

Oracle Cloud Infrastructure

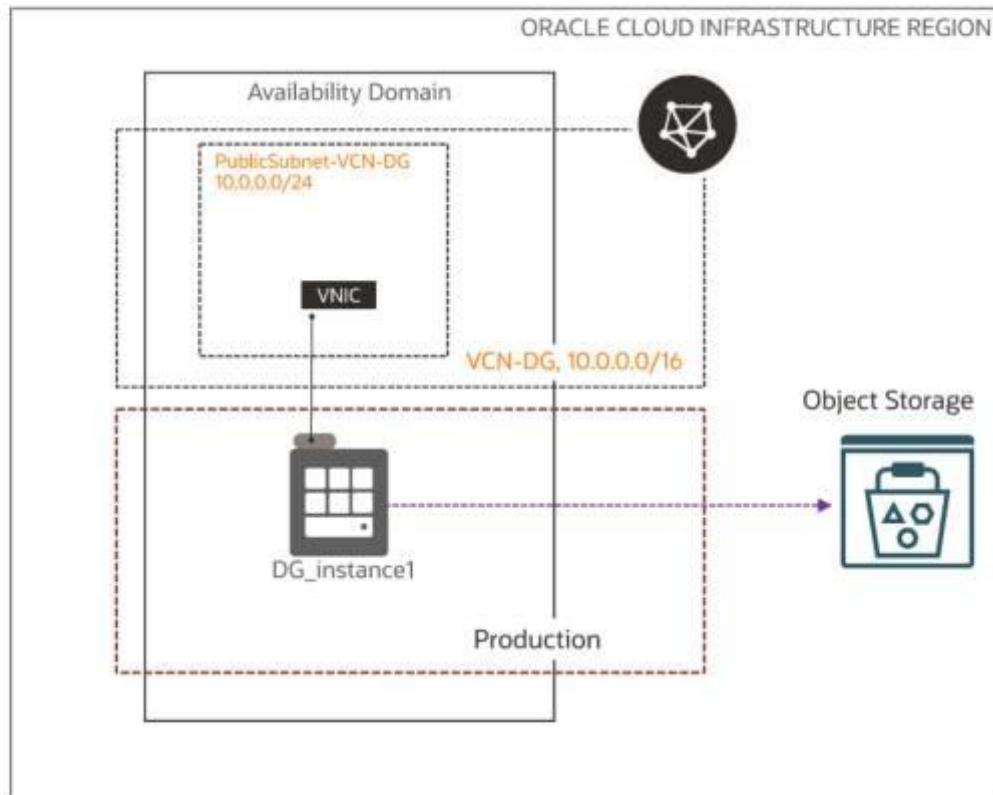
# Demo: Dynamic Groups

**OCI Identity and Access Management (IAM)**

Dr. Saurabh Patil

OU OCI Delivery Team

# Scenario: Dynamic Groups



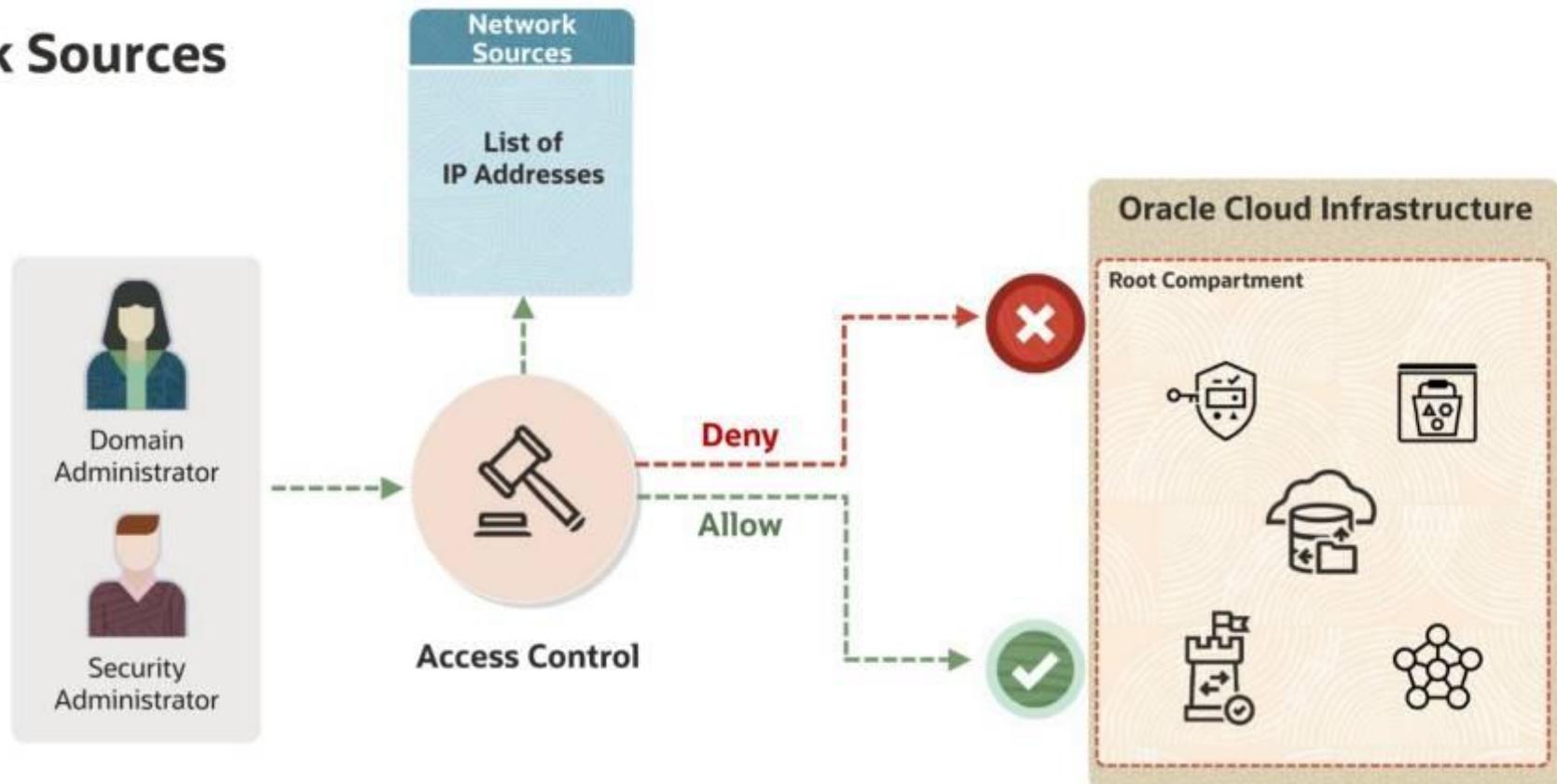
```
{ Any {instance.compartment.id = 'ocid'}
```

```
{ allow dynamic-group 'Production'/'DG-demo' to manage object-family in compartment Production }
```

# Oracle Cloud Infrastructure Network Sources

## OCI Identity and Access Management (IAM)

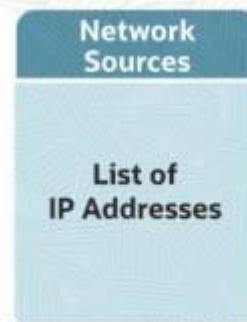
## Network Sources



# Network Sources



**Set of defined IP Addresses**



## Network Sources



### Policies

allow group <domain>/<group> to manage <resource> in tenancy  
where `request.networkSource.name='corpnet'`



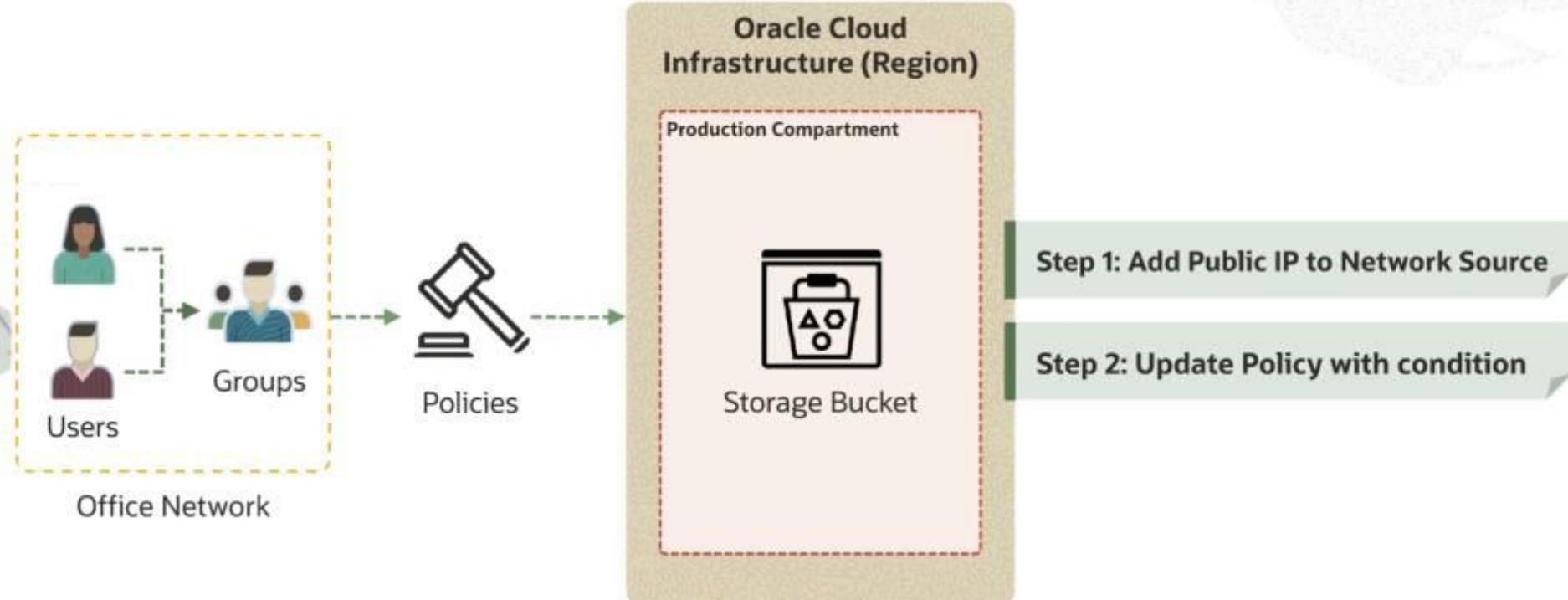
**Control access based on originating IP address**

Oracle Cloud Infrastructure

# Demo: Network Sources

OCI Identity and Access Management (IAM)

## Scenario



# Oracle Cloud Infrastructure Dynamic Groups

---

## OCI Identity and Access Management

## Terms

---

**Principal** - Identity of the caller trying to access/operate on a resource

**User** - Represents a human in an organization

**Instance** - Represents a unique compute VM host in any OCI tenancy

**Service** - An application developed and operated by OCI, that offers functionality to end customers

**Resource** - A unit-instance of an entity exposed by a service - a database, a Load Balancer



# Resource Principals Patterns



Infrastructure

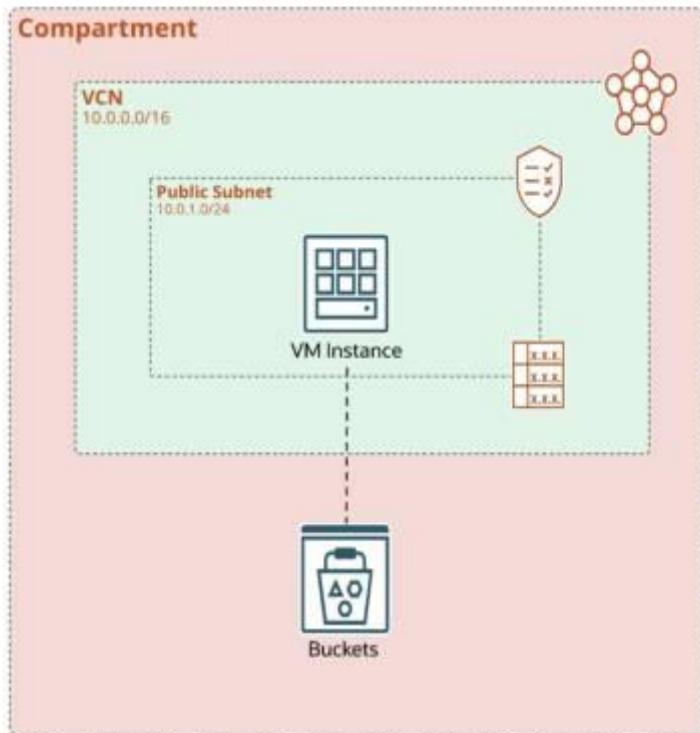


Stacked



Ephemeral

# Infrastructure Principals



## Analogy

- A birth certificate

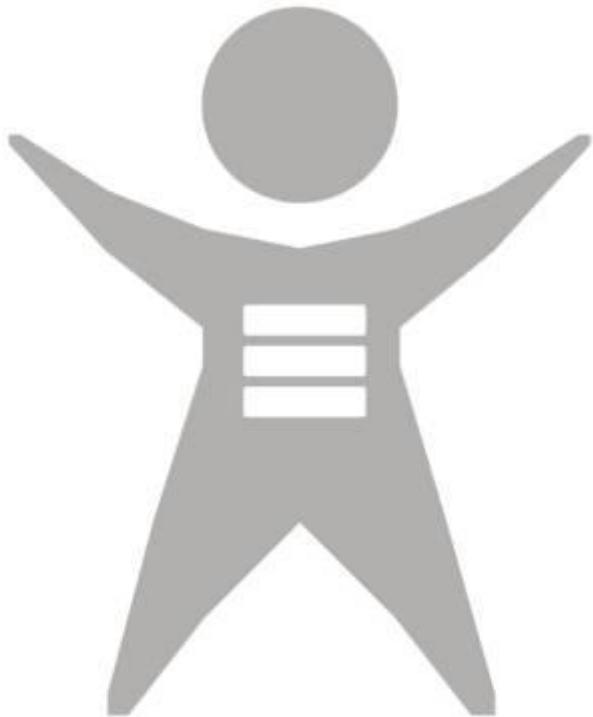
## Key Idea

- IAM service feature that enables instances to be authorized actors (or principals) to perform actions on service resources

## OCI example

- Instance Principal

# Stacked Principals



## Analogy

- Requesting a passport, having a birth certificate

## Key Idea

- Projecting one principal on top of another, a service controlling a resource, not the infrastructure, specifies the intention of the resource.
- It requires infrastructure to be hosting one resource, multiple infrastructures might host same resource for redundancy purpose.

## OCI example

- Oracle Database

# Ephemeral Principals



## Analogy

- A building temporarily badge issued valid for the day.

## Key Idea

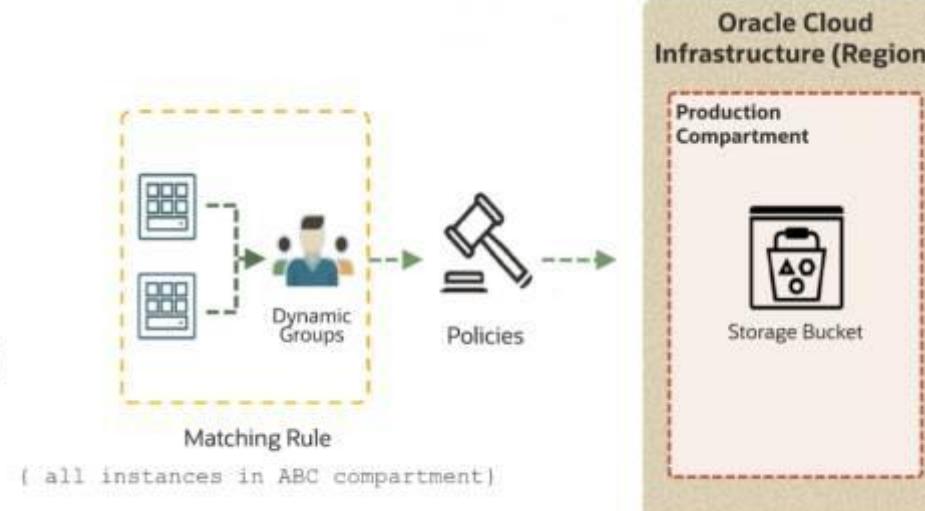
- Using injected identifiers, a service defines who the holder of a particular credential is for a short period of time.

## OCI example

- Oracle Function

# Dynamic Groups

- Allows Infrastructure, Stacked, Ephemeral resource principals to be grouped as “principal actors” (similar to other groups)
- Policies permit Dynamic Group principals to make API calls against OCI services
- When you create a dynamic group, rather than adding members explicitly to the group, you instead define a set of *matching rules* to define the group members
- E.g., a rule could specify that all instances in a particular compartment are members of the dynamic group. The members can change dynamically as instances are launched and terminated in that compartment.



# Dynamic Groups

To add all compute instances of a compartment to a dynamic group

```
All | Any {instance.compartment.id = '<compartment-ocid>'}
```

To add a specific compute instance to a dynamic group

```
All {instance.id = '<compartment-ocid>'}
```

Adding a resource to a dynamic group

```
Any {resource.type = 'dbaas', resource.compartment.id = 'ocid' }
```

# Policies

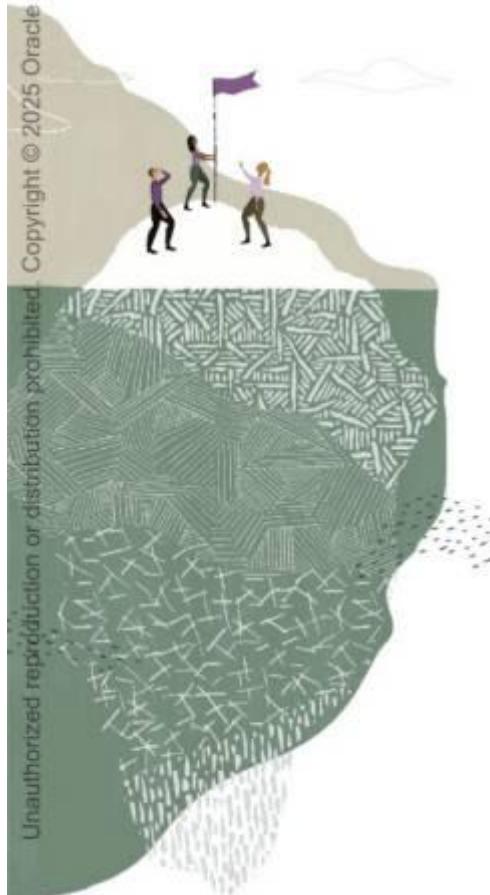
Policy to allow a dynamic group of instances to manage objects in tenancy

```
allow dynamic-group domain-name/InstanceB to manage objects in tenancy  
where all { target.bucket.name = 'Log', target.region.name = 'RegionB'}
```

Policy that allows a database to access objects in tenancy for backups

```
allow dynamic-group domain-name/DatabaseBackUps to manage objects in tenancy  
where all { target.bucket.name = 'DBBackup', target.region.name = 'RegionA'}
```

# Summary



Step 1: Create dynamic groups

Step 2: Define matching rules for memberships

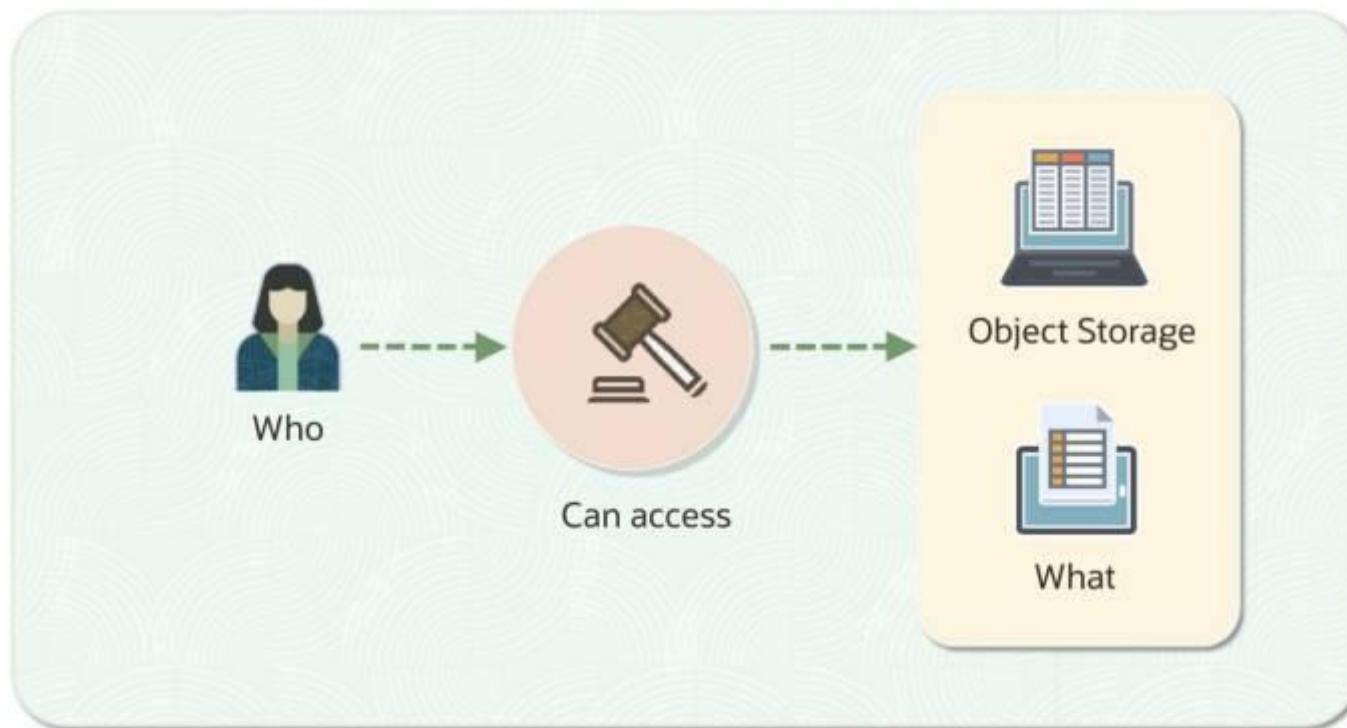
Step 3: Write policies for providing access

Oracle Cloud Infrastructure

# Optimizing IAM Policies: Part 1

**OCI Identity and Access Management (IAM)**

## OCI IAM Policies



# OCI IAM Policies

## Avoid OCI limits

- Too many policies = slower API calls = performance impact

## Security and compliance

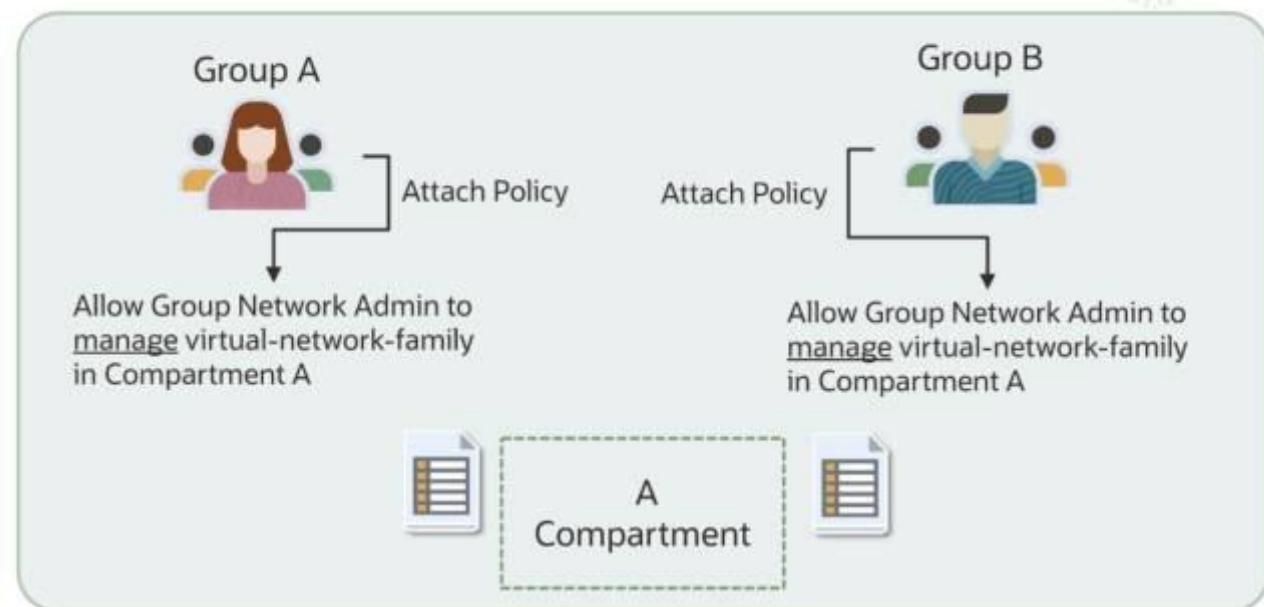
- OCI enforces limits on policies/statements
- Reduced policies = better scalability

## Simplified management

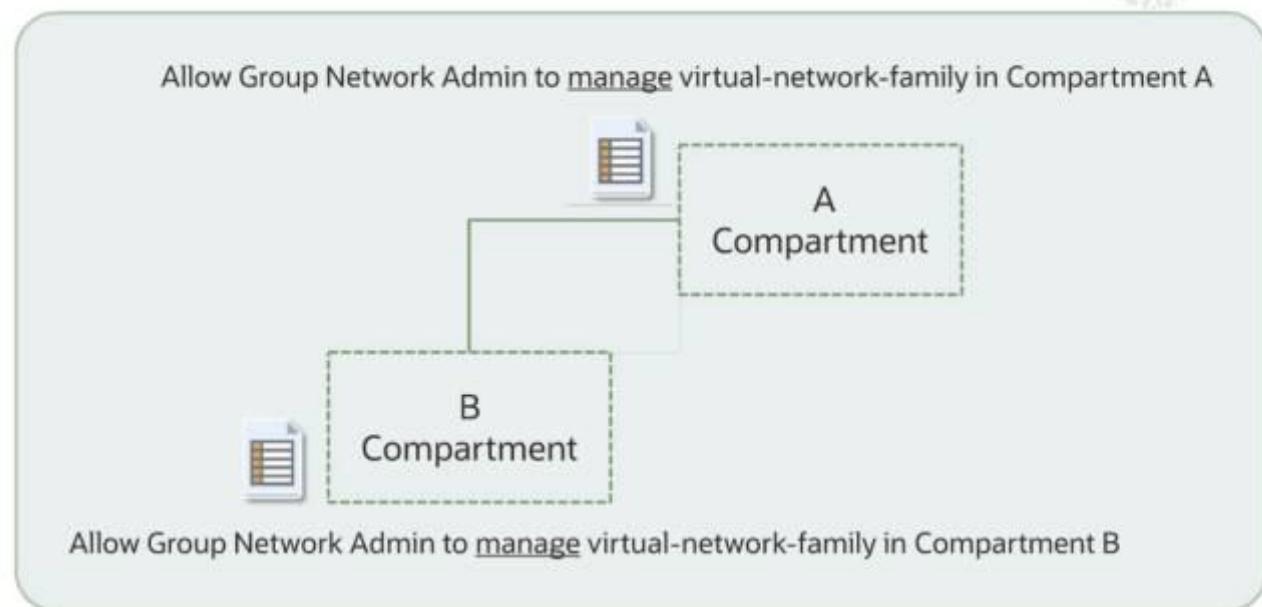
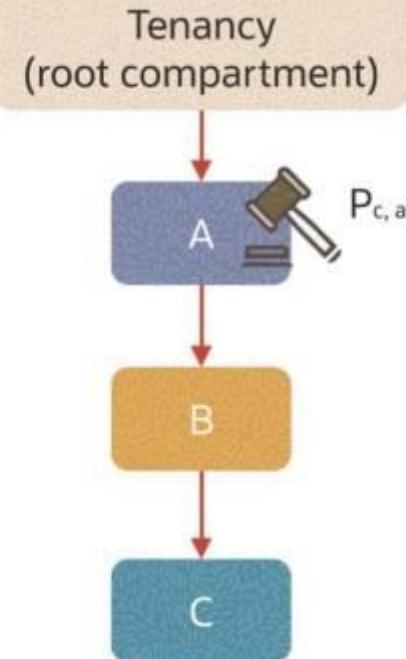
- Easier to manage, audit, and update fewer policies



## Eliminating Duplicate Policies

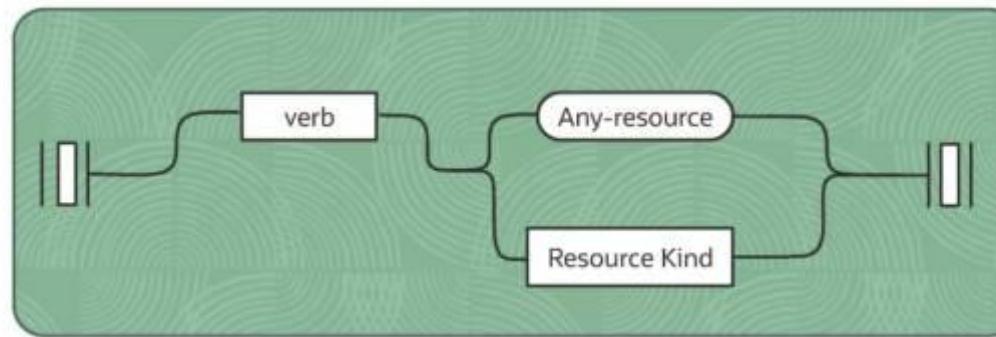


## Eliminating Duplicate Policies



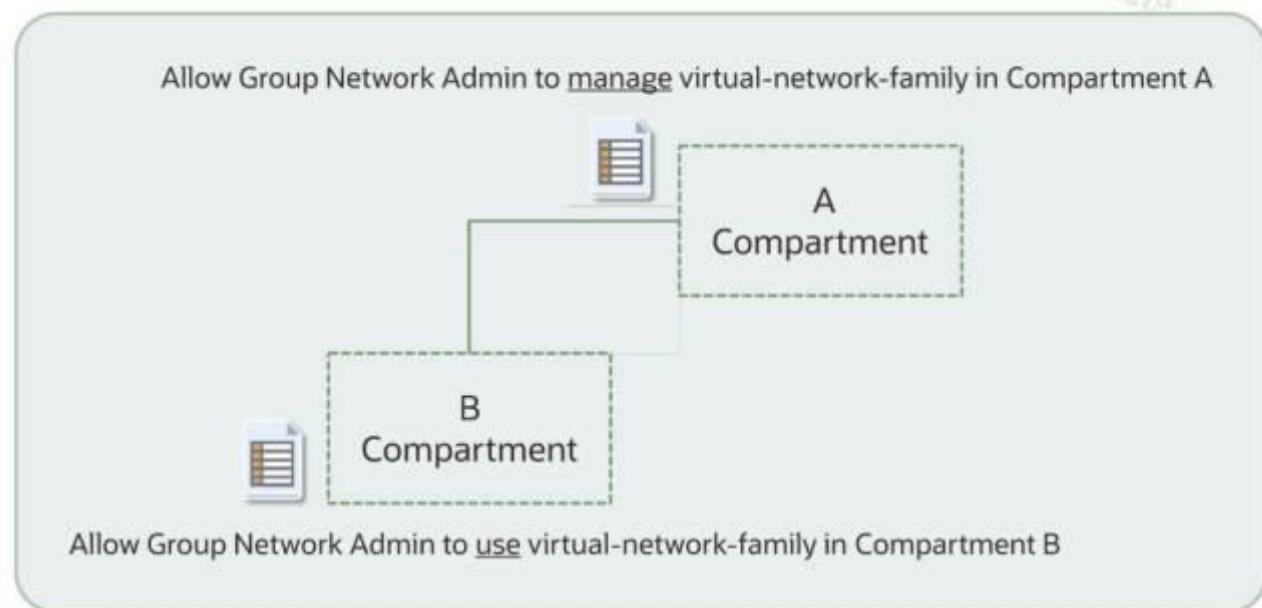
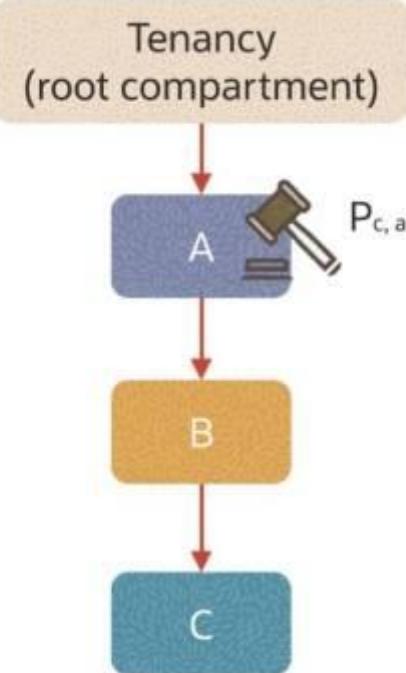


## Removing Less-Permissive Policies

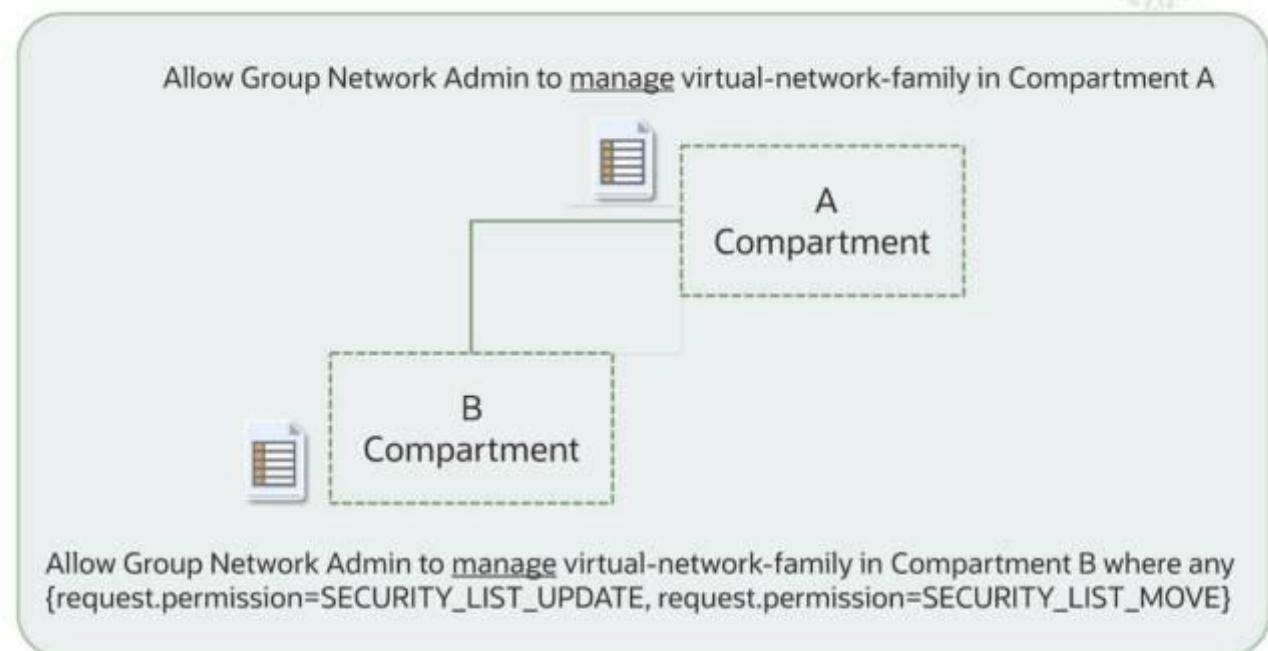
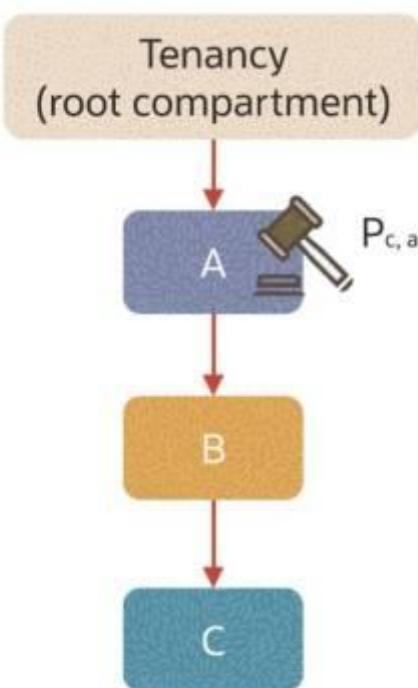


Verb	Type of access	Permission example
Inspect	Permissions necessary to observe, enumerate, and monitor, w/o access to confidential information	«inspect objects» Learn details about objects stored in buckets - quantity, confirmation of object existence, and so on, without getting access to the object itself
Read	Permissions necessary to access but not alter resources	«read objects» Read the contents of the object
Use	Permissions to modify pre-existing resources	«reencrypt objects» Re-encrypt objects using a different key version
Manage	Permissions to do anything to the resource kind	«create objects» Create or delete objects

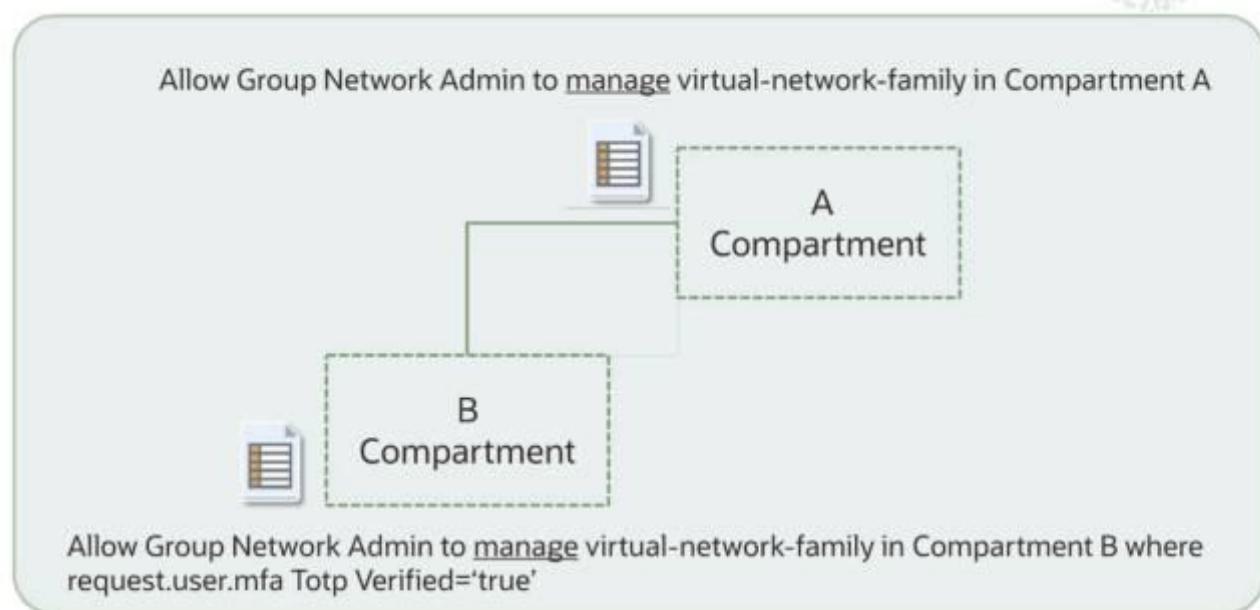
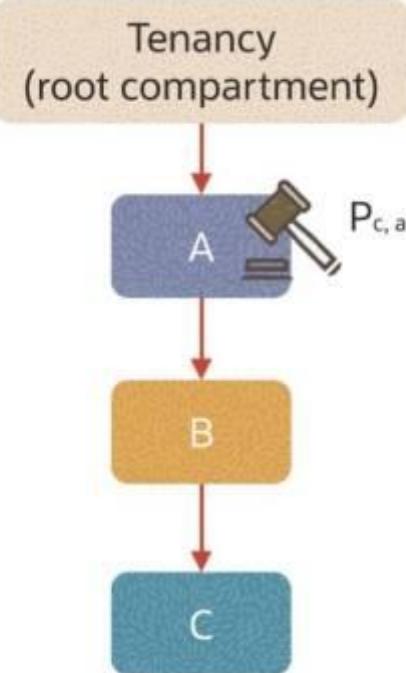
## Removing Less-Permissive Policies



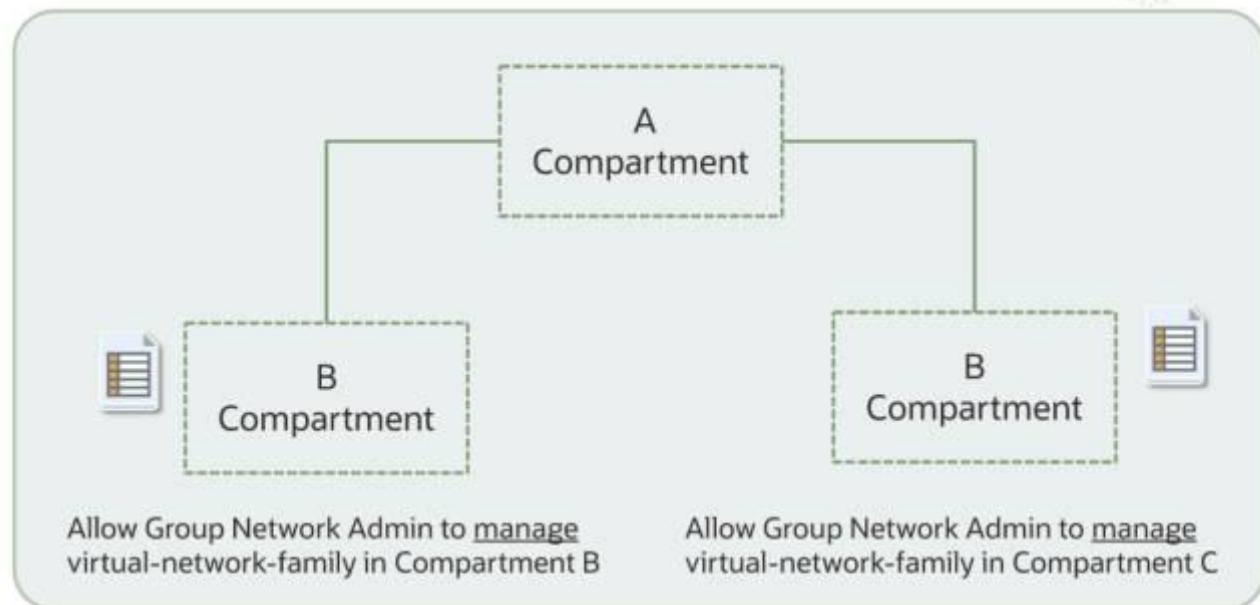
## Policy Conditions and Inheritance



## Removing Less-Permissive Policies

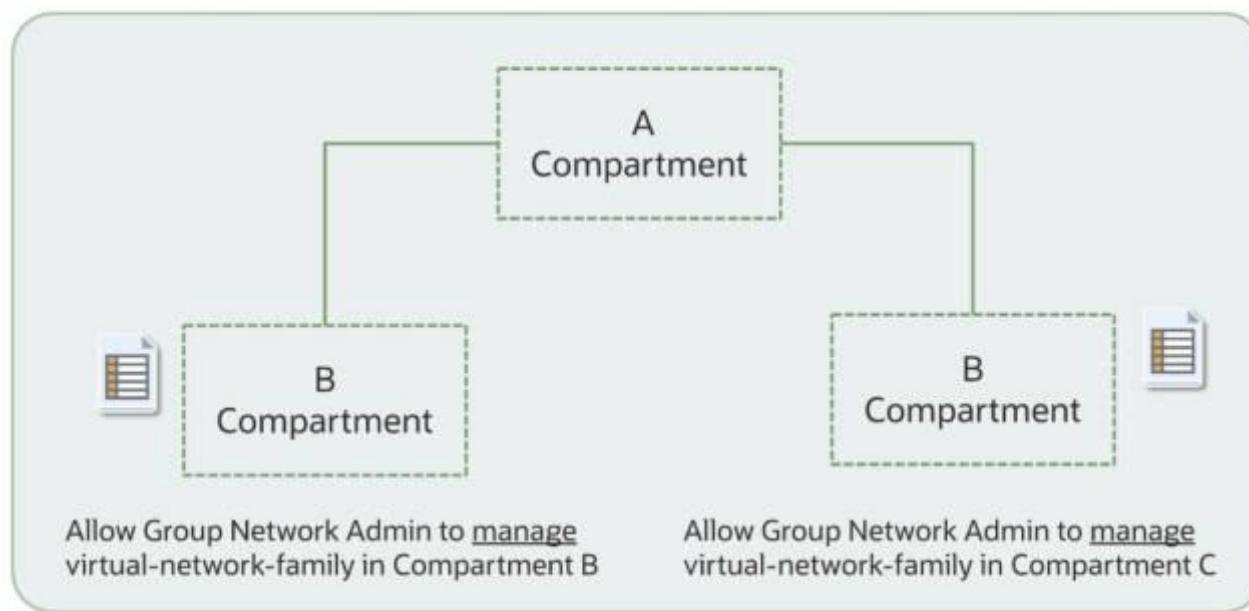


## Consolidating Group Membership



## Consolidating Group Membership: Same Members

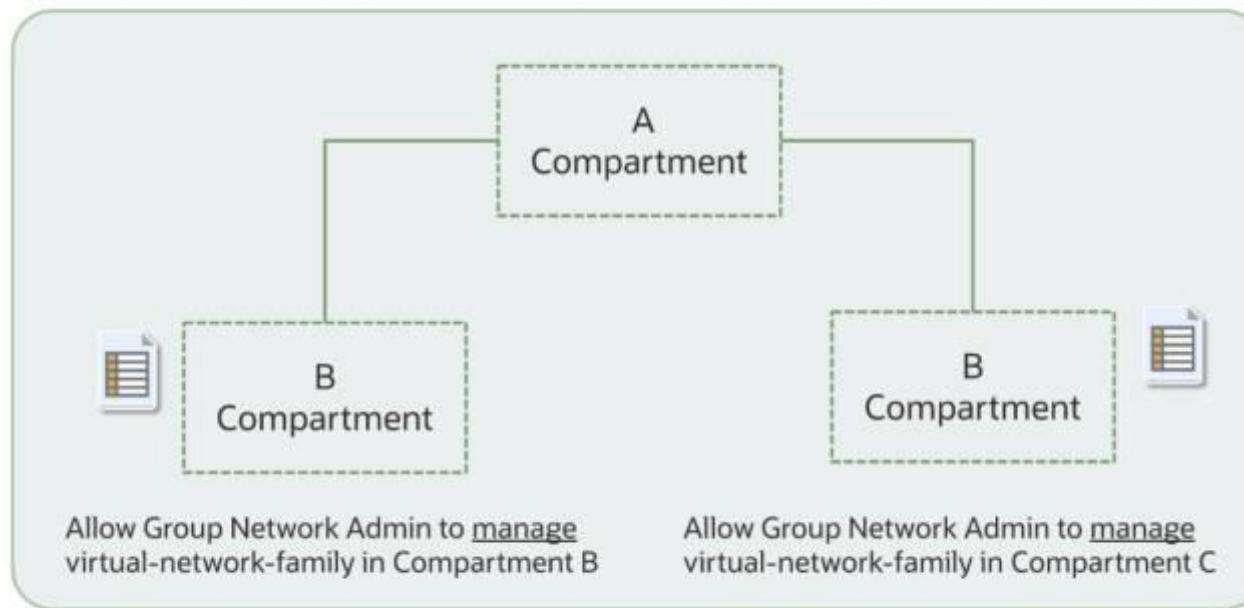
Allow group **NetworkAdminB,NetworkAdminC** to manage virtual-network-family in compartment A where any (target.compartment.name='B',target.compartment.name='C')





## Consolidating Group Membership: Different Members

```
Allow group NetworkAdminB,NetworkAdminC to manage virtual-network-family in compartment A  
where any  
(all { target.compartment.name='B',request.groups.id=OCID_of_NetworkAdminB },all (  
target.compartment.name='C', request.groups.id=OCID_of_NetworkAdminC))
```



Oracle Cloud Infrastructure

# Optimizing IAM Policies: Part 2

**OCI Identity and Access Management (IAM)**

## Combining Policy Statements



Policy

Allow group X to **use subnets** in Compartment A

- SUBNET\_READ
- SUBNET\_ATTACH
- SUBNET\_DETACH

use	READ +	no extra	LaunchInstance (also need use vnics , use network-security-groups , and manage instance-family )
	SUBNET_ATTACH		TerminateInstance (also need manage instance-family , and use volumes if a volume is attached)
	SUBNET_DETACH		AttachVnic (also need manage instances , use network-security-groups , and either use vnics or use instance-family )
			DetachVnic (also need manage instances and either use vnics or use instance-family )
			CreatePrivateIp, DeletePrivateIp (both also need use private-ips and use vnics )

## Combining Policy Statements



Policy

Allow group X to **manage instances** in Compartment A

INSTANCE\_CREATE\_IMAGE  
INSTANCE\_POWER\_ACTIONS  
INSTANCE\_ATTACH\_VOLUME  
INSTANCE\_DETACH\_VOLUME  
INSTANCE\_CREATE  
INSTANCE\_DELETE  
INSTANCE\_ATTACH\_SECONDARY\_VNIC  
INSTANCE\_DETACH\_SECONDARY\_VNIC  
INSTANCE\_MOVE

## Combining Policy Statements



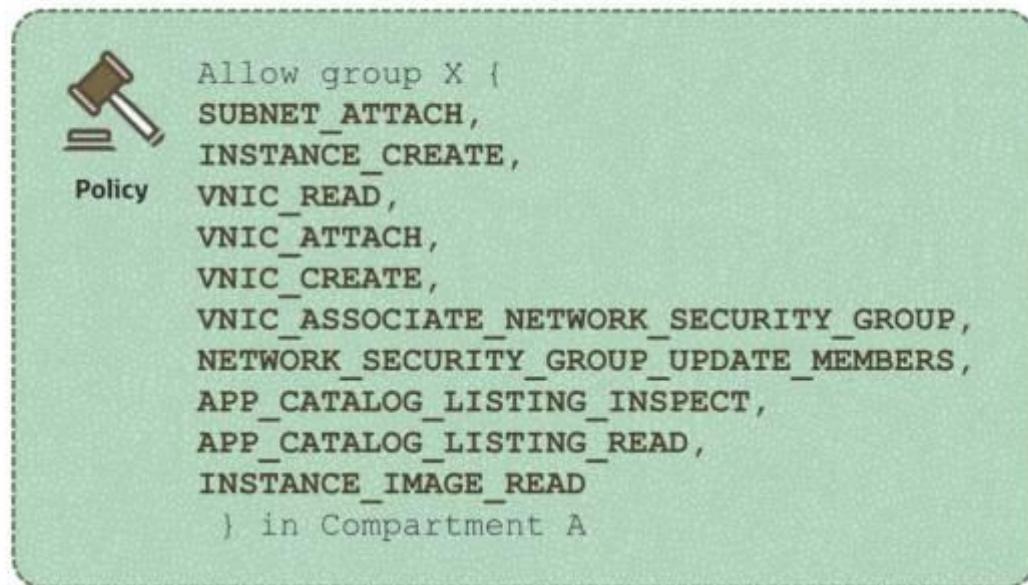
1. Allow group X to **use subnets** in Compartment A
2. Allow group X to **manage instances** in Compartment A
3. Allow group X to **read app-catalog-listing** in Compartment A

Allow group X { SUBNET\_READ, SUBNET\_ATTACH, SUBNET\_DETACH,  
INSTANCE\_INSPECT, INSTANCE\_READ, INSTANCE\_UPDATE,  
INSTANCE\_CREATE\_IMAGE, INSTANCE\_POWER\_ACTIONS,  
INSTANCE\_ATTACH\_VOLUME, INSTANCE\_DETACH\_VOLUME } in Compartment A

## Combining Policy Statements: Use case

To allow Group X to launch compute instance, you need the following IAM policies:

- Launch a new compute instance  
*Allow group X to manage instances in Compartment A*
- Attach it to a subnet in Compartment A.  
*Allow group X to use subnets in Compartment A*
- Assign it to a Network Security Group  
*Allow group X to use network-security-groups in Compartment A*



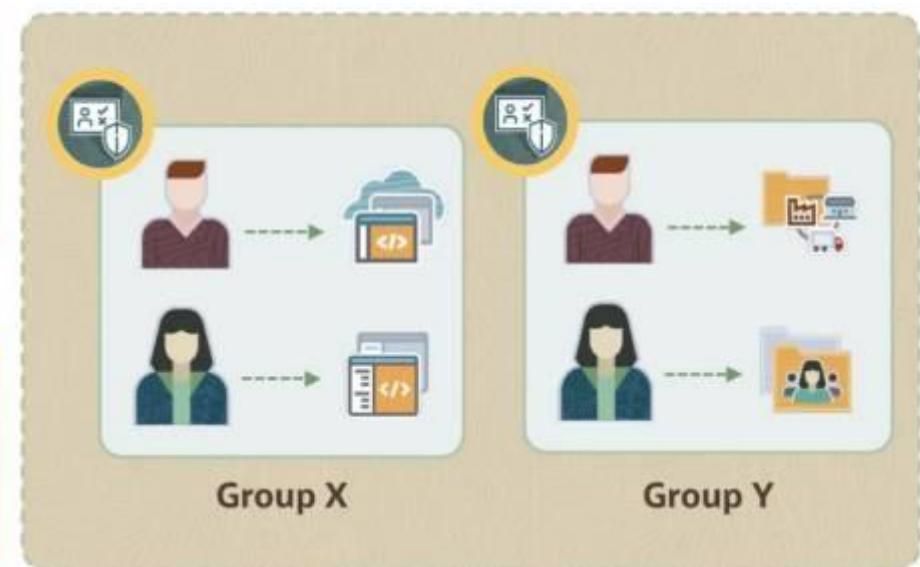
# Grouping Multiple Entities

## Before:

```
Allow group X to use subnets in Compartment A  
Allow group Y to use subnets in Compartment A  
Allow group X to use instances in Compartment A  
Allow group Y to use instances in Compartment A
```

## After:

```
Allow group X, Y to use subnets in Compartment A  
Allow group X, Y to use instances in Compartment A
```



# Grouping Multiple Entities

## Before:

```
Allow group X to use subnets in Compartment A  
Allow group Y to use subnets in Compartment A  
Allow group X to use instances in Compartment A  
Allow group y to use instances in Compartment A
```

## After:

```
Allow group X, Y to use subnets in Compartment A  
Allow group X, Y to use instances in Compartment A
```

```
Allow group X, Y {  
  SUBNET_READ,  
  SUBNET_ATTACH,  
  SUBNET_DETACH,  
  INSTANCE_INSPECT,  
  INSTANCE_READ,  
  INSTANCE_UPDATE,  
  INSTANCE_CREATE_IMAGE,  
  INSTANCE_POWER_ACTIONS,  
  INSTANCE_ATTACH_VOLUME,  
  INSTANCE_DETACH_VOLUME  
} in Compartment A
```

## Pattern-Based Optimization



Policy

Allow group ProjectXAdmin to manage all-resources in compartment  
**ProjectXProduction**

Allow group ProjectXAdmin to manage all-resources in compartment  
**ProjectXDev**



Policy

Allow group ProjectYAdmin to manage all-resources in compartment  
**ProjectYProduction**

Allow group ProjectYAdmin to manage all-resources in compartment  
**ProjectYDev**

**Combine:**

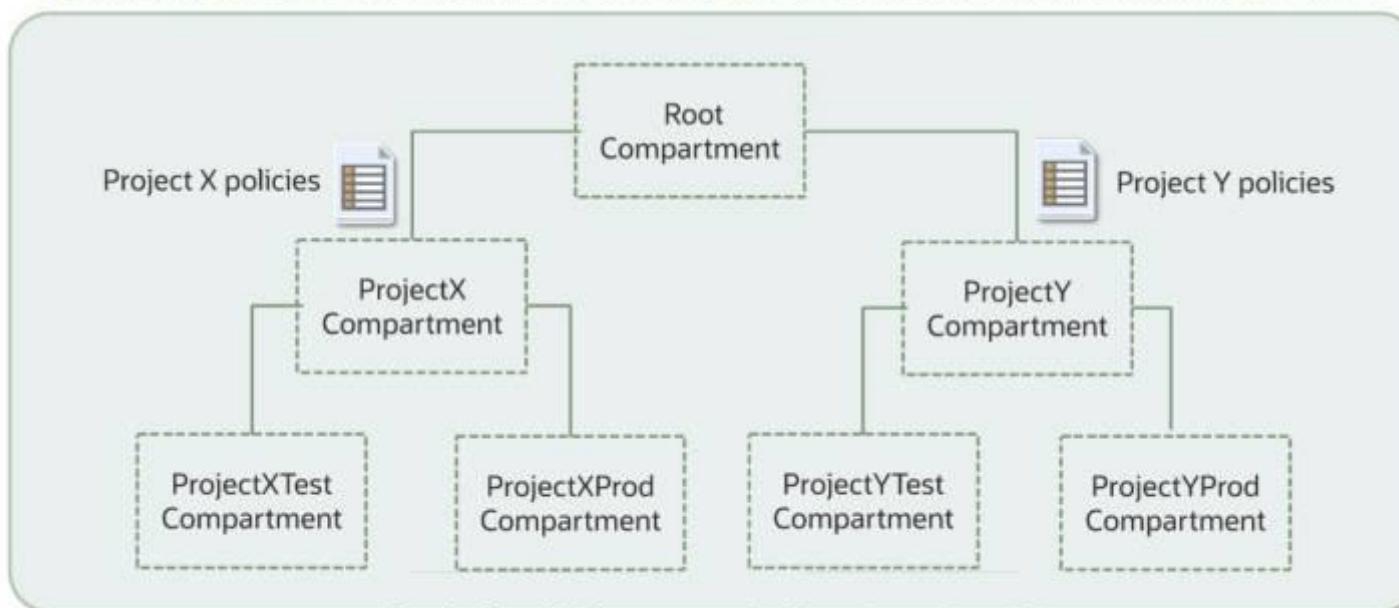
Allow group ProjectXAdmin to manage all-resources in tenancy where  
**target.compartment.name=/ProjectX\*/**

Allow group ProjectYAdmin to manage all-resources in tenancy where  
**target.compartment.name=/ProjectY\*/**

## Pattern-Based Optimization

Allow group ProjectXAdmin to manage all-resources in tenancy where  
**target.compartment.name=/ProjectX\*/**

Allow group ProjectYAdmin to manage all-resources in tenancy where  
**target.compartment.name=/ProjectY\*/**





Oracle Cloud Infrastructure

# Object-Level Granular Access Control for OCI Object Storage

OCI Identity and Access Management (IAM)

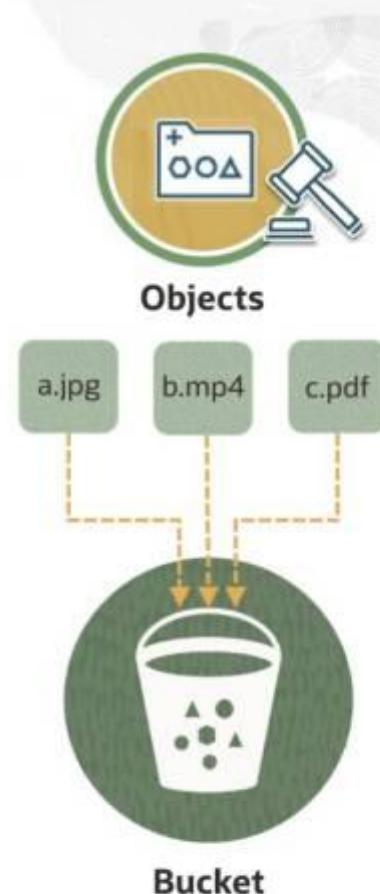
# OCI Object Storage

Object Storage is an internet-scale, high-performance storage platform that offers reliable and cost-efficient data durability.

- > **Internet Scale and High Performance:** Designed to handle large datasets with ease and provides fast and efficient data retrieval
- > **Reliable and Durable:** Data redundantly stored and actively monitored for integrity, ensuring its safety and availability
- > **Objects & Buckets:**

## Use Cases

- > **Analytics Data Storage:** Ideal for holding large volumes of data for analysis and processing
- > **Rich Content Repository:** Perfectly suited for storing images, videos, and other multimedia content



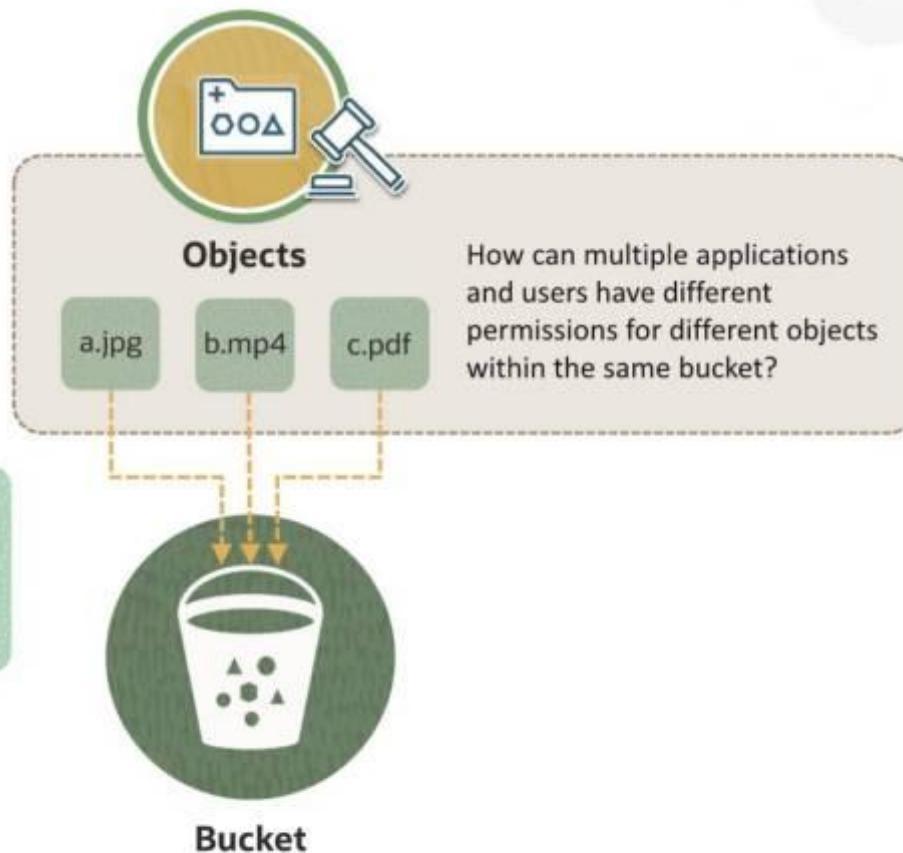
# OCI Object Storage

## Bucket-Level IAM Policy

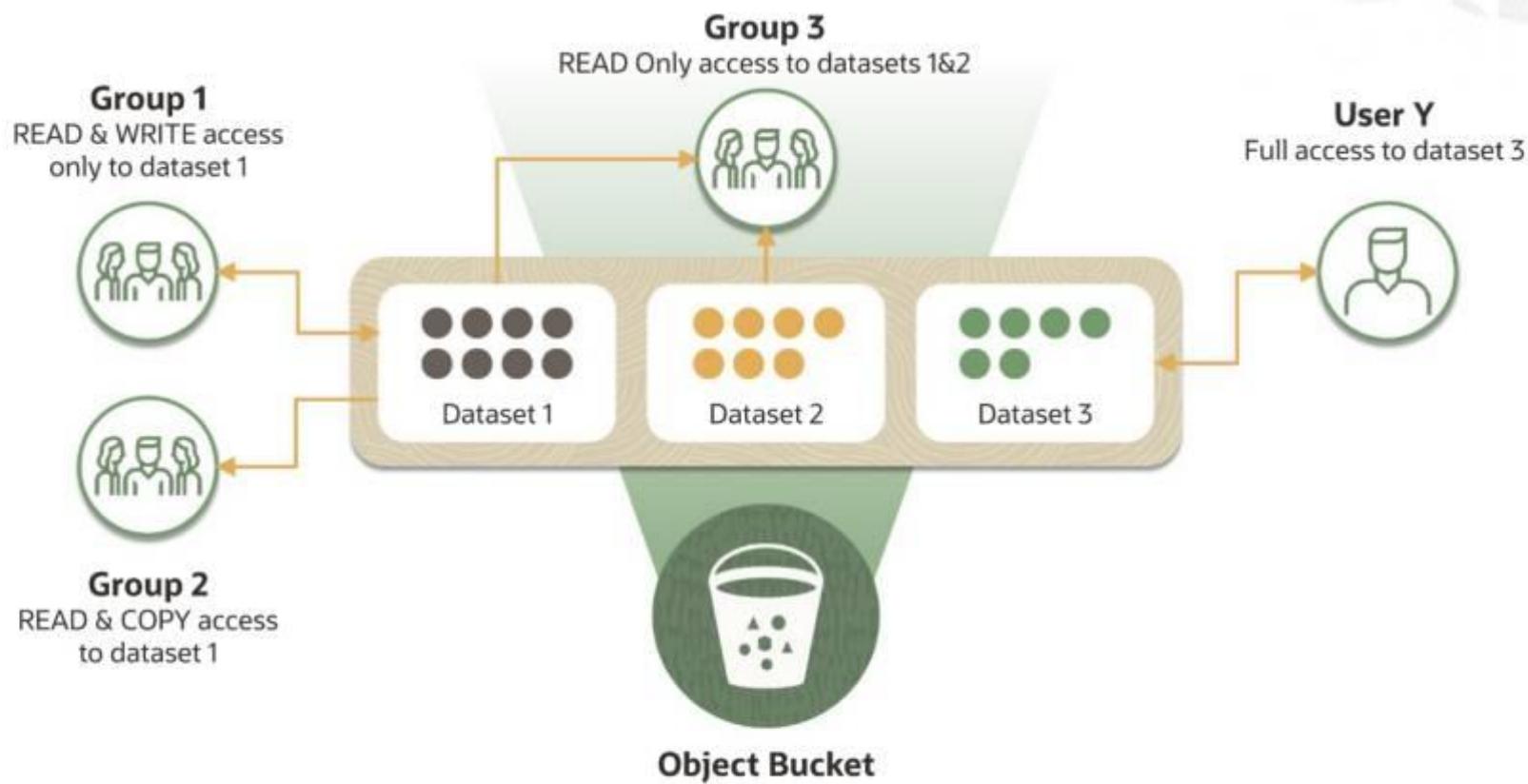
Allow group Domain1/ObjectAdmins to manage buckets in tenancy

Allow group Domain1/ObjectAdmins to manage objects in tenancy

Allow group Domain1/ObjectWriters to manage objects in compartment ABC  
where all {target.bucket.name= 'BucketA',  
any {request.permission= 'OBJECT\_CREATE',  
request.permission='OBJECT\_INSPECT'}}



# Object-Level Permissions



# Object IAM

- Object IAM enables you to create fine-grained access control **at the object level** within a bucket.
- Use the IAM policy variable **target.object.name** to define permissions for specific objects or object patterns.

## Granular Control

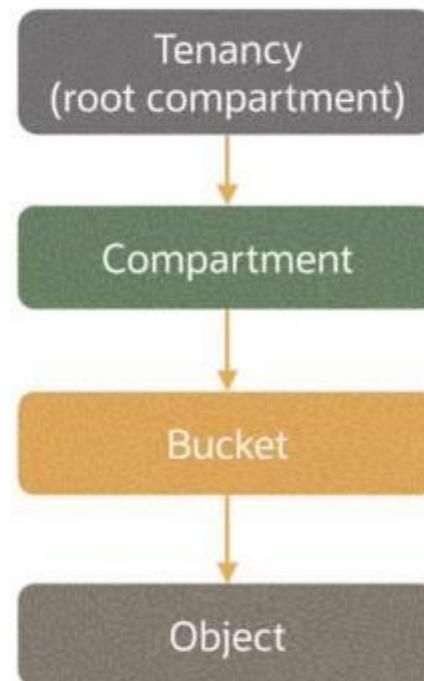
Manage access for individual objects or groups of objects

## Enhanced Security

Restrict operations such as Read, Write, Delete, or Copy

## Scalability

Supports large buckets with millions of objects shared by multiple users and applications



# Object IAM Policy Examples

Full Access

Allows full access to a group for a folder 'prod' in a bucket 'test-bucket'

```
Allow group test-group TO manage objects IN TENANCY where  
all {target.bucket.name = 'test-bucket', target.object.name = 'prod/*'}
```

Read-Only  
Access

Allows read-only access to a group for a folder 'dev' in a bucket 'test-bucket'

```
Allow group test-group TO manage objects IN TENANCY where  
all {target.bucket.name = 'test-bucket', target.object.name = 'dev/*',  
any{request.permission='OBJECT_INSPECT', request.permission='OBJECT_READ'}}
```

# Object IAM Policy Examples

Write-Once  
Access

Allows write-once (no overwrites) and no read or delete access to a group for a folder 'prod' in a bucket 'test-bucket'

```
Allow group test-group TO manage objects IN TENANCY where  
all {target.bucket.name = 'test-bucket', target.object.name = 'prod/*',  
any{request.permission='OBJECT_CREATE'}}}
```

Read and  
Write Access

Allows read and write access to a group for a folder 'dev' in a bucket 'test-bucket' (no listing or overwriting)

```
Allow group test-group TO manage objects IN TENANCY where  
all {target.bucket.name = 'test-bucket', target.object.name = 'dev/*',  
any{request.permission='OBJECT_CREATE', request.permission='OBJECT_READ'}}}
```

# Object IAM Policy Examples

Access for  
Specific Files

Grants all access for a specific user for an object pattern  
'\* .pdf' in the bucket 'test-bucket'

Allow any-user TO manage objects IN TENANCY where  
all {target.bucket.name = 'test-bucket', target.object.name = '\* .pdf',  
request.user.id='ocid1.user.oc1..aaaaaaaaaswqb2h3qd4lrf6enng4mtfu5gio6il57a'}

# Expert Tip

---

# Networking - Virtual Cloud Network

# Oracle Cloud Infrastructure

## CIDR Block Prefixes

---

### Networking – Virtual Cloud Network

## CIDR Notation

CIDR prefix representation: A.B.C.D/x

Components of a CIDR prefix:

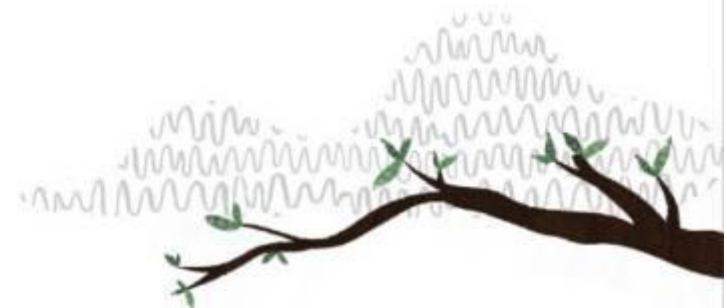
- Network address (A.B.C.D)
- Network prefix or mask (/x)

Subnetting allows dividing CIDR prefixes to smaller ones

CIDR notation: 192.168.1.0/24

- First 24 bits are the network address
- Last 8 bits are the host address

## CIDR: Example



192.168.1.0/24 would equate to IP range 192.168.1.0 – 192.168.1.255

- › 128 64 32 16 8 4 2 1 ->  $2^7 \ 2^6 \ 2^5 \ 2^4 \ 2^3 \ 2^2 \ 2^1 \ 2^0$
- › 192 is represented as 1 1 0 0 0 0 0 0

192.168.1.2

1	1	0	0	0	0	0	0	1	0	0	0	0	1	0
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

/24 subnet mask

1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

Logical AND

1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

Oracle Cloud Infrastructure

# Virtual Cloud Network

## Networking – Virtual Cloud Network

# Virtual Cloud Network



Virtual private network inside an Oracle region

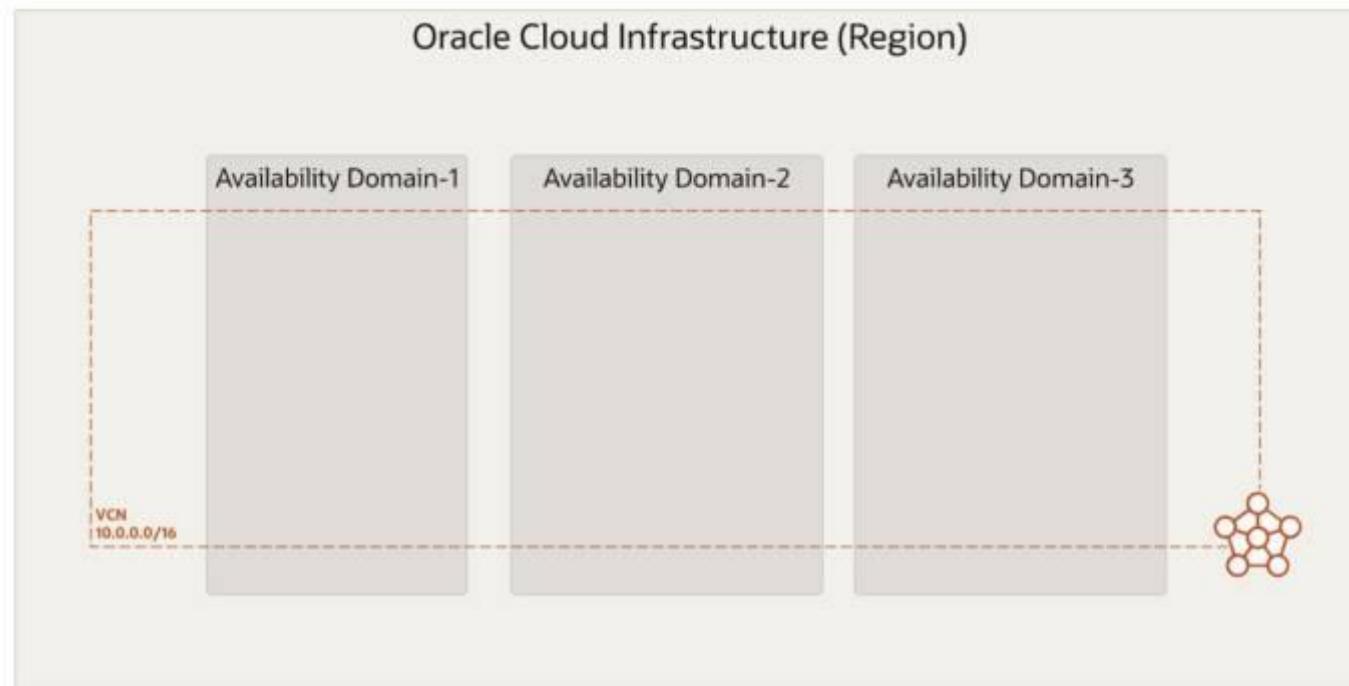
Resides in a single region but can span multiple Availability Domains

Software-defined network

Can have one or more CIDR blocks (IPv4 and IPv6, if enabled)

Can modify CIDR blocks after VCNs are created

# Virtual Cloud Network



## Allowed VCN Size and Address Ranges

The allowable VCN size range is /16 to /30.

The first two and the last IP addresses in each subnet is reserved.

You receive a /56 if you use an Oracle-allocated IPv6 prefix.

You can create a VCN with a BYOIPv6 prefix.

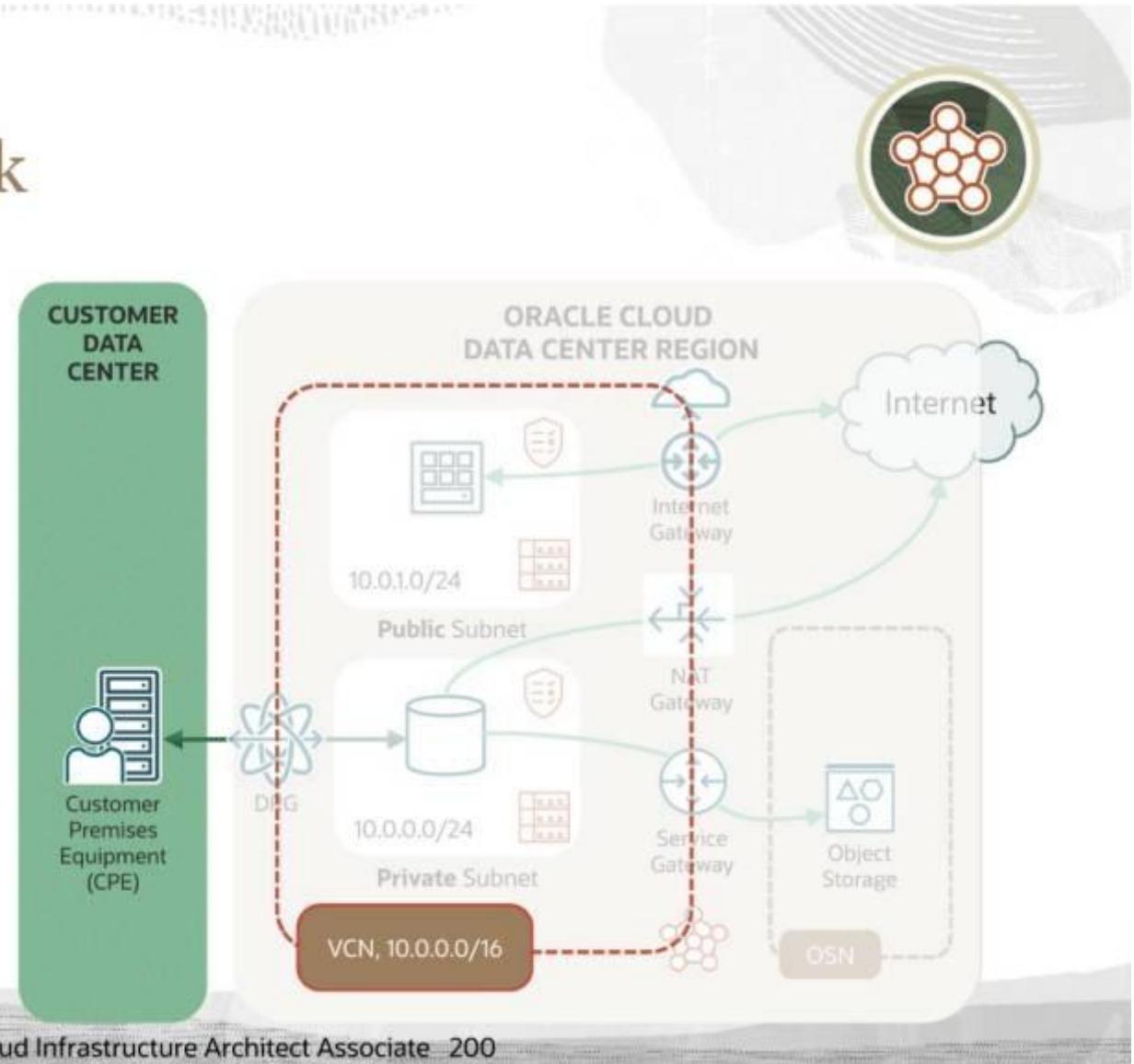
## Oracle Cloud Infrastructure

# VCN Components - Quick Overview

### Networking – Virtual Cloud Network

# Virtual Cloud Network

- › Subnet
- › Route Table
- › DHCP Options
- › Gateways
- › Network Security Group
- › Security List

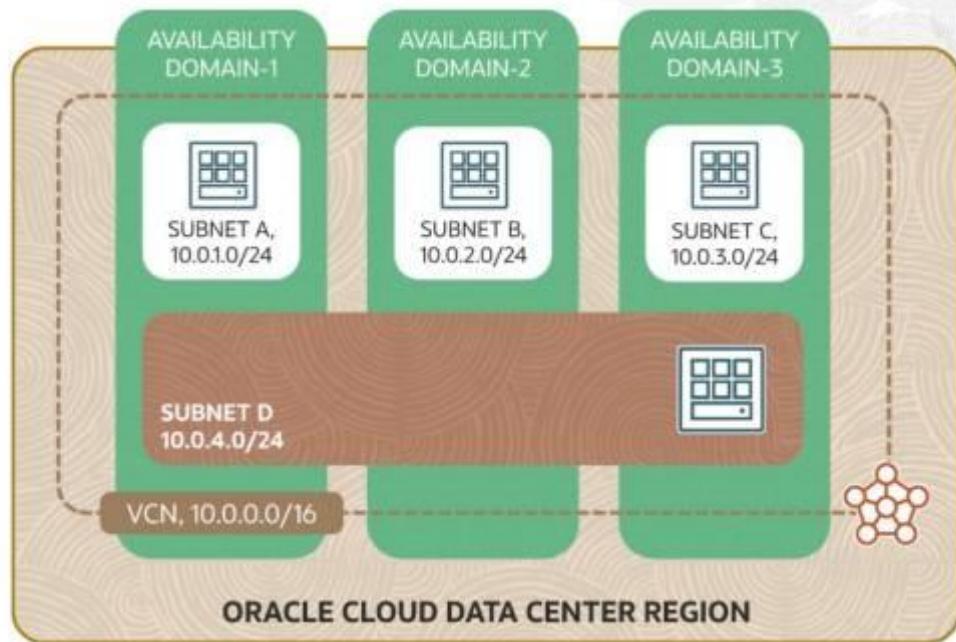


# Oracle Cloud Infrastructure Subnets

## Networking – Virtual Cloud Network

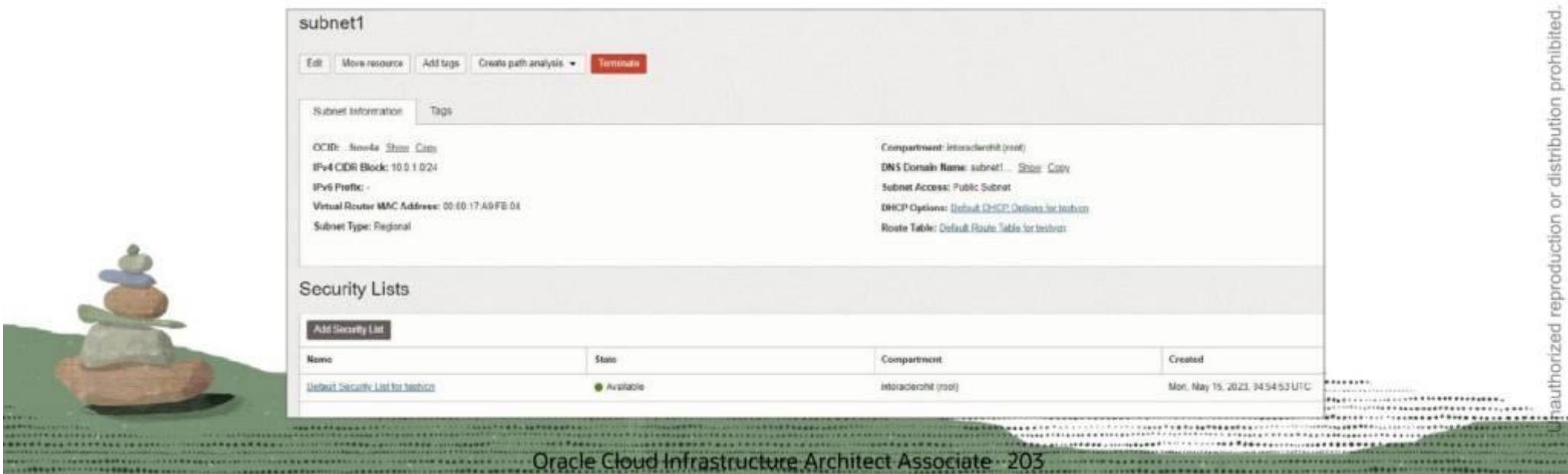
# Subnets

- A VCN is subdivided into subnets.
- Each subnet has a contiguous range of IPs described in CIDR notation.
- Subnet IP ranges cannot overlap.
- A subnet can grow or shrink after creation.
- Each subnet can be:
  - AD-specific: Contained in a single AD in a multi-AD region
  - Regional (recommended): Spans all three ADs in a multi-AD region



# Subnets

- Subnets act as a unit of configuration.
- Instances are placed in subnets.
- Instances draw their network configuration from their subnet.



The screenshot shows the Oracle Cloud Infrastructure (OCI) Subnet details page for a subnet named "subnet1".

**Subnet Information:**

- OCID: `1nw4k` [Show](#) [Copy](#)
- IPv4 CIDR Block: `10.0.1.0/24`
- IPv6 Prefix: -
- Virtual Router MAC Address: `00:0D:17:A9:FB:04`
- Subnet Type: Regional

**Compartment:** intraderchit (root)

**DNS Domain Name:** `subnet1` [Show](#) [Copy](#)

**Subnet Access:** Public Subnet

**DHCP Options:** [Default DHCP Options for testvzn](#)

**Route Table:** Default Route Table for testvzn

**Security Lists:**

Add Security List			
Name	Status	Compartment	Created
<a href="#">Default Security List for testvzn</a>	<span>Available</span>	intraderchit (root)	Mon, May 15, 2023, 04:54:53 UTC

**Page Footer:** Oracle Cloud Infrastructure Architect Associate · 203

# Types of Subnets

## Private

Contains private IP addresses assigned to VNICs

Holds private servers such as database servers and doesn't allow public IP addresses

## Public

Contains both private and public IP addresses assigned to VNICs

Allows public IP addresses for instances in a subnet

The choice of public or private happens during subnet creation, and you can't change it later.

Oracle Cloud Infrastructure

# Demo: Create a VCN (Manually)

—  
**Networking – Virtual Cloud Network**

## Oracle Cloud Infrastructure

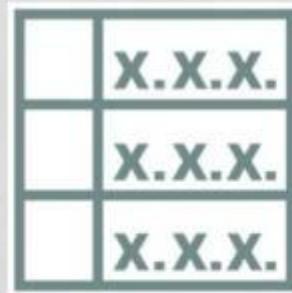
# Demo: Create a VCN (Using Wizard)

### Networking – Virtual Cloud Network

# Oracle Cloud Infrastructure Route Table

## Networking – Virtual Cloud Network

# Route Table Basics



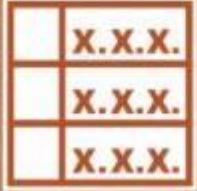
The traffic is sent out of VCN.

Subnet is associated with a Route Table.

VCN local routing automatically handles traffic within the VCN's subnets.

Most specific rule wins in case of overlapping rules.

The traffic is dropped in case of no route rule match.



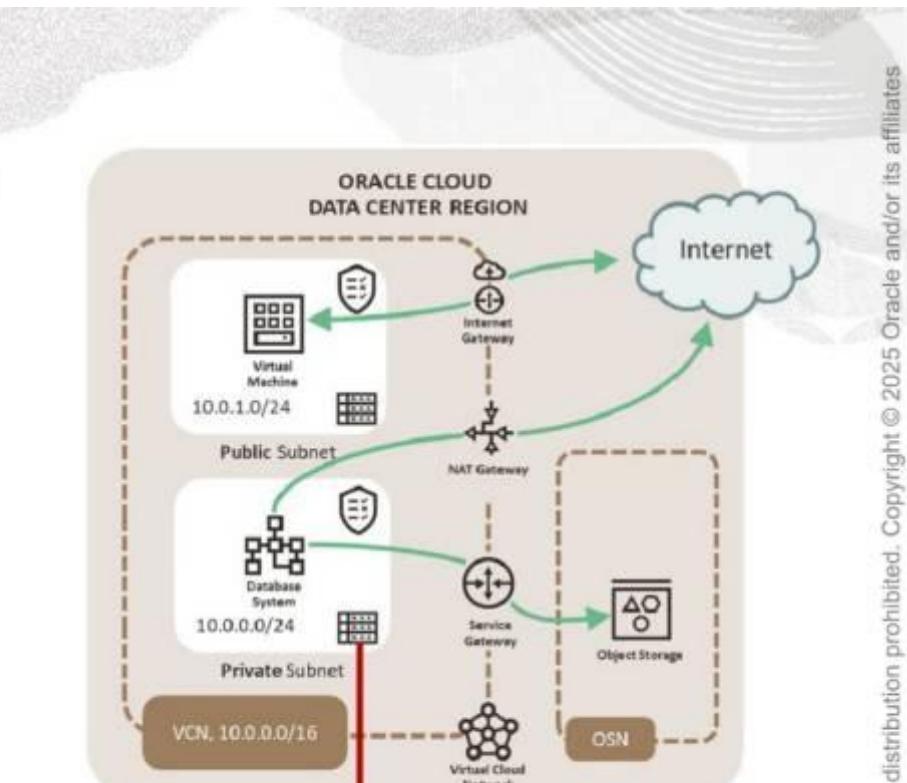
# Route Table

Consists of a set of route rules  
Each rule specifies the:

- › Destination CIDR block
- › Route target (the next hop) for traffic that matches that CIDR

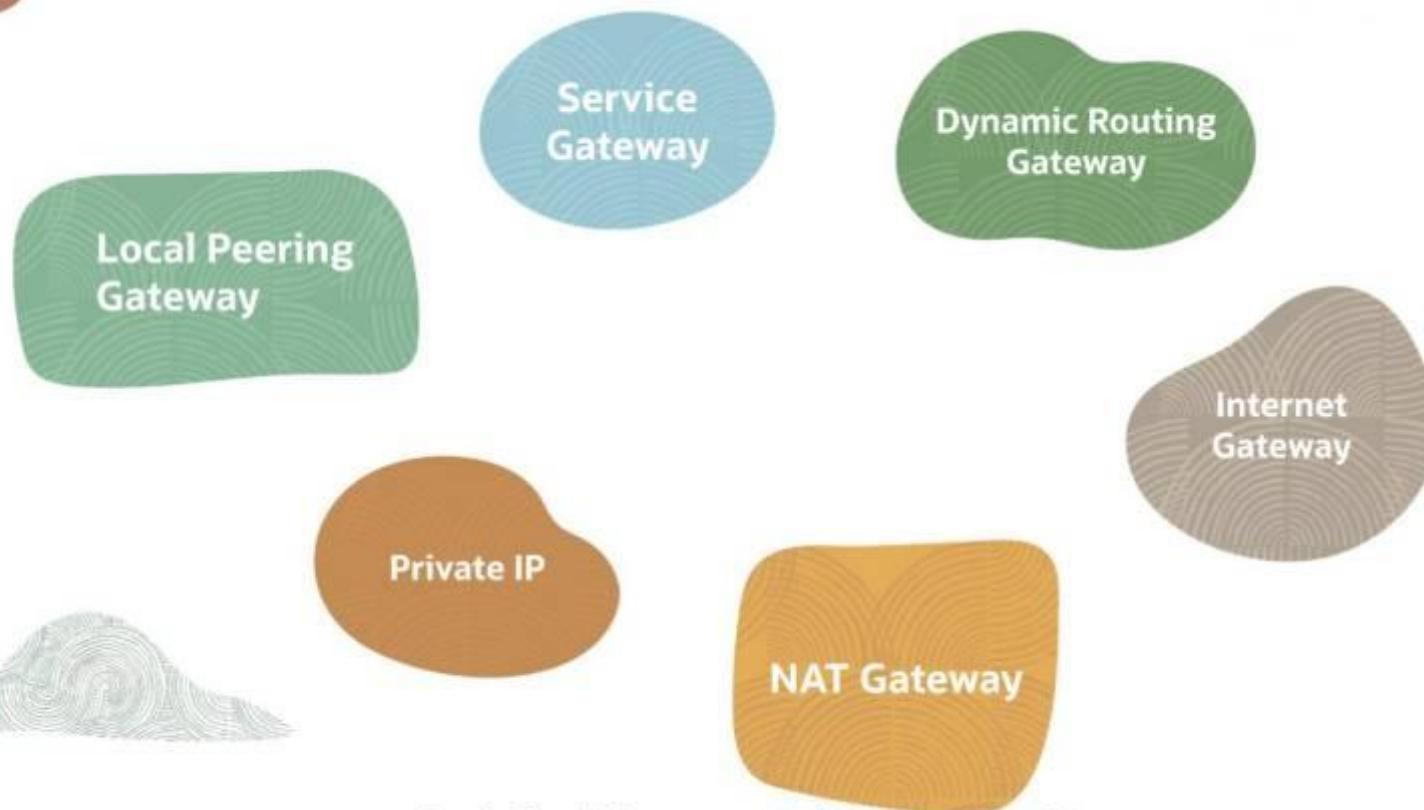
Create Route Table		
Name	State	Number of Rules
Custom Route Table	● Available	0
Default Route Table for Isolated	● Available	0

Destination CIDR	Target Type
0.0.0.0/0	NAT Gateway
Object Storage	Service Gateway





## Allowed Route Rule Target Type



Oracle Cloud Infrastructure

# Demo: Route Tables

—  
**Networking – Virtual Cloud Network**

# Oracle Cloud Infrastructure

## Internet Gateway

---

### Networking – Virtual Cloud Network

# Internet Gateway



Internet  
Gateway

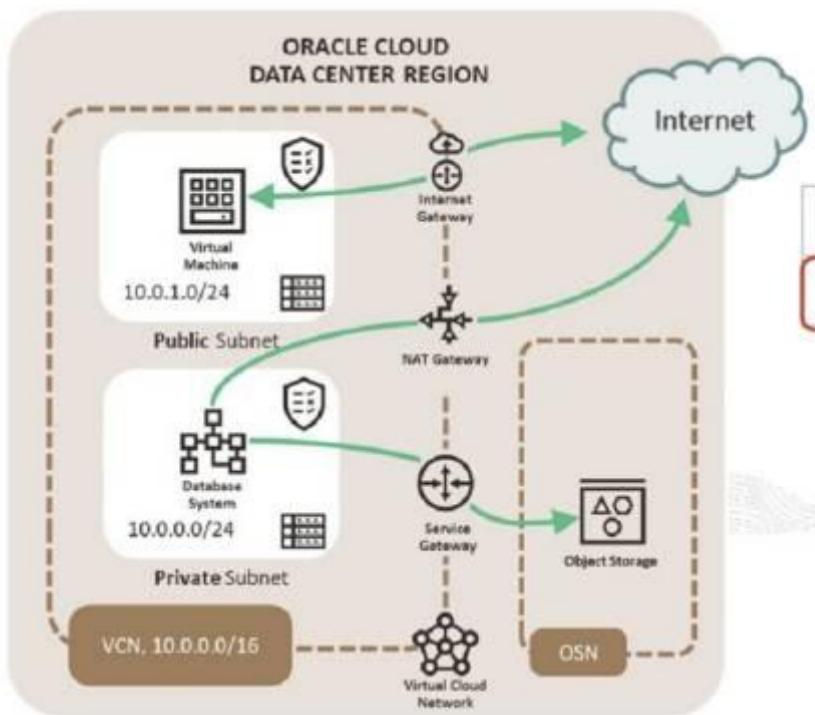
Enables direct connectivity to the Internet

Supports both egress and ingress traffic

Only one Internet Gateway per VCN



# Internet Gateway



Destination CIDR	Route target
0.0.0.0/0	Internet Gateway

Oracle Cloud Infrastructure

# Demo: Internet Gateway

—  
**Networking – Virtual Cloud Network**

## Oracle Cloud Infrastructure

# NAT Gateway

### Networking – Virtual Cloud Network

# NAT Gateway



NAT Gateway

Instances in a private subnet don't have public IP addresses.

It gives instances in a private subnet access to the Internet.

It does not allow connections initiated from the Internet to the private subnet.

It is highly available and supports TCP, UDP, and ICMP ping traffic.



# NAT Gateway

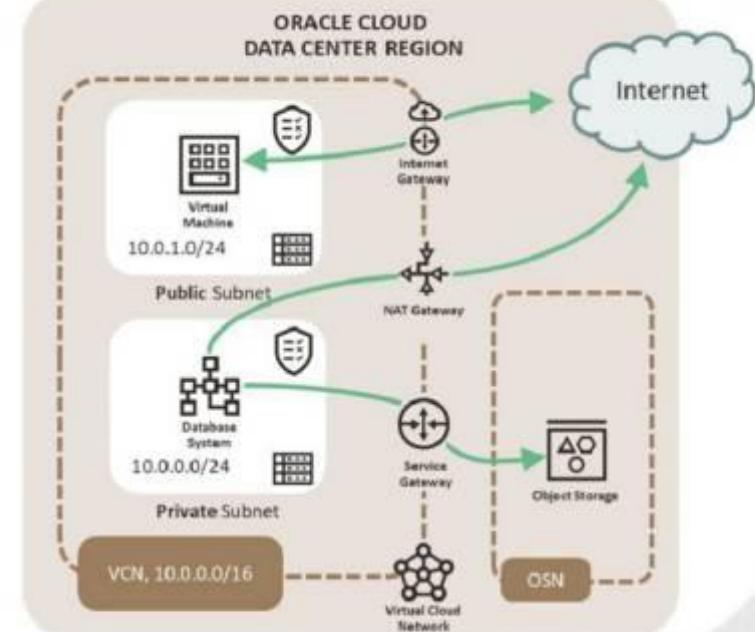
Maximum of 20,000 concurrent connections

Can use an Ephemeral or Reserved IP address

Routing for a NAT Gateway

Can be used only by resources within the VCN

## NAT Gateway



## Oracle Cloud Infrastructure

# Demo: NAT Gateway

---

### Networking – Virtual Cloud Network

## Oracle Cloud Infrastructure

# Service Gateway

### Networking – Virtual Cloud Network

# Service Gateway



**Oracle Services Network** is reserved for Oracle services.

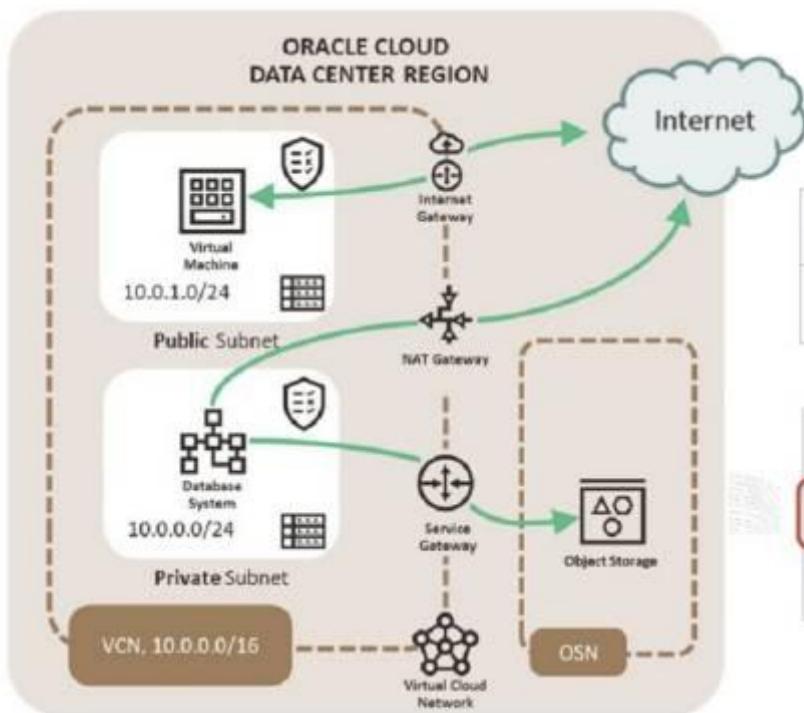
Services have public IP addresses.

Access the **Oracle Services Network** without the traffic going over the Internet

Secure, private path for network traffic

No internet gateway or NAT gateway required

# Service Gateway



Destination CIDR	Route target
0.0.0.0/0	Internet Gateway
Destination CIDR	Route target
OSN services in region	Service Gateway
0.0.0.0/0	NAT Gateway

Regional - enables access only to supported Oracle services *in the same region* as the VCN.

Oracle Cloud Infrastructure

# Demo: Service Gateway

—  
**Networking – Virtual Cloud Network**

# Oracle Cloud Infrastructure Public Subnet

## Networking – Virtual Cloud Network

# Public Subnet

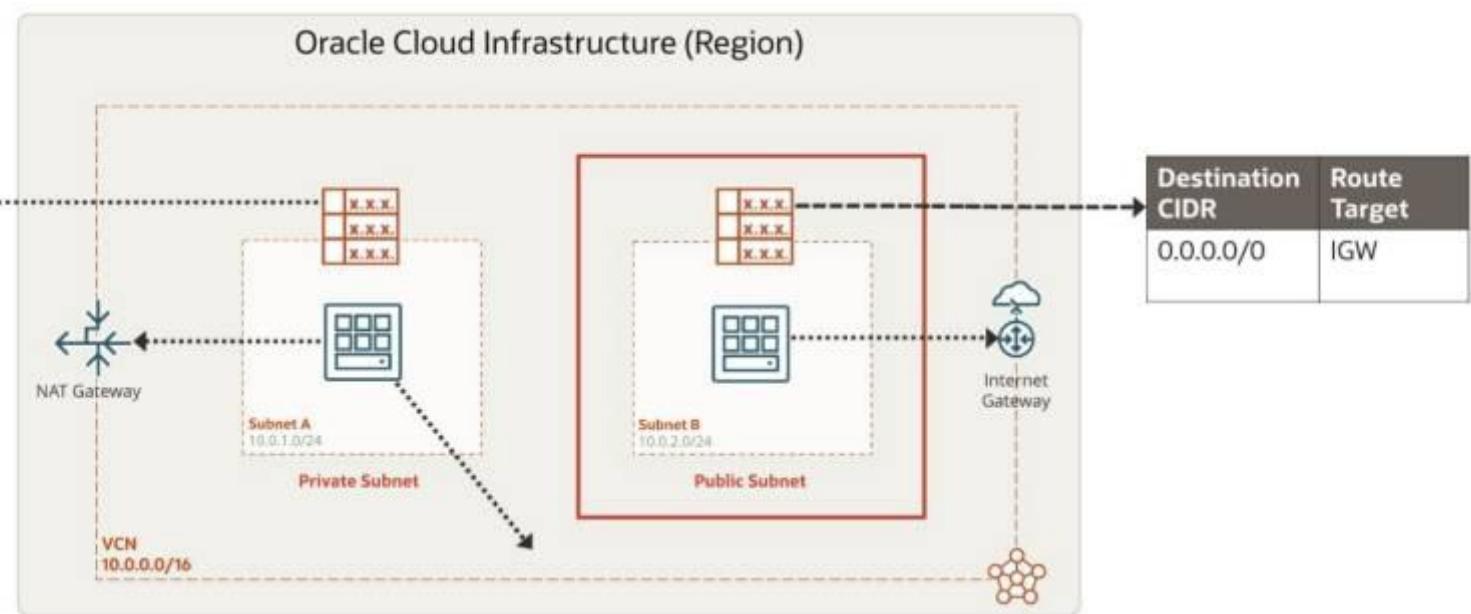


- Allows public IP addresses for instances in a subnet
- Can allocate a public IP address to the Instance (vNIC)
- Internet communication permitted by using the Internet Gateway

Subnet Access	
<b>Private Subnet</b>	Prohibit public IP addresses for Instances in this Subnet
<b>Public Subnet</b>	Allow public IP addresses for Instances in this Subnet <input checked="" type="checkbox"/>



# Public Subnet



## Oracle Cloud Infrastructure

# Demo: Public Subnet

---

### Networking – Virtual Cloud Network

## Oracle Cloud Infrastructure

# Private Subnet

### Networking – Virtual Cloud Network

# Private Subnet

- Does not allow public IP addresses for instances in a subnet
- Can allocate only private IP addresses to the Instance (vNIC)
- Internet communication permitted by using the NAT Gateway



Subnet Access

Private Subnet

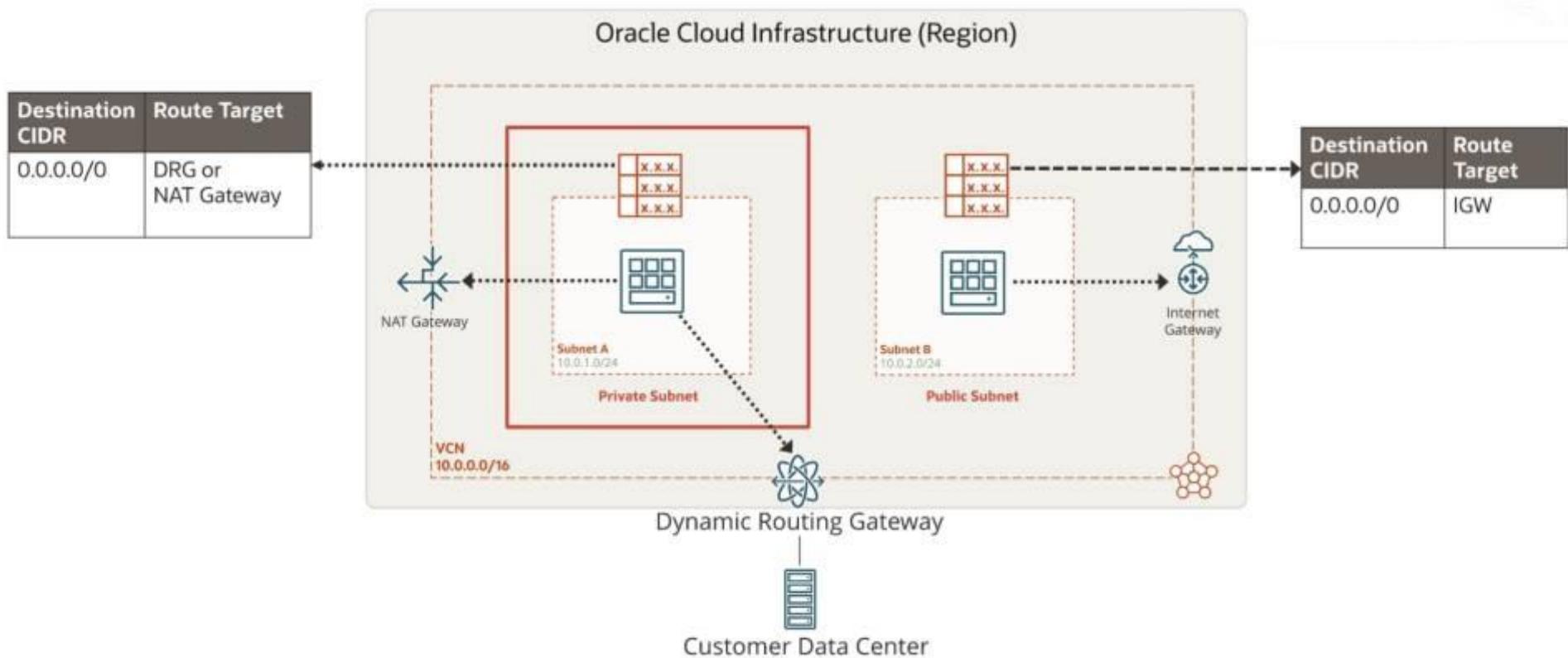
Prohibit public IP addresses for Instances in this Subnet

Public Subnet

Allow public IP addresses for Instances in this Subnet



# Private Subnet



## Oracle Cloud Infrastructure

# Demo: Private Subnet

---

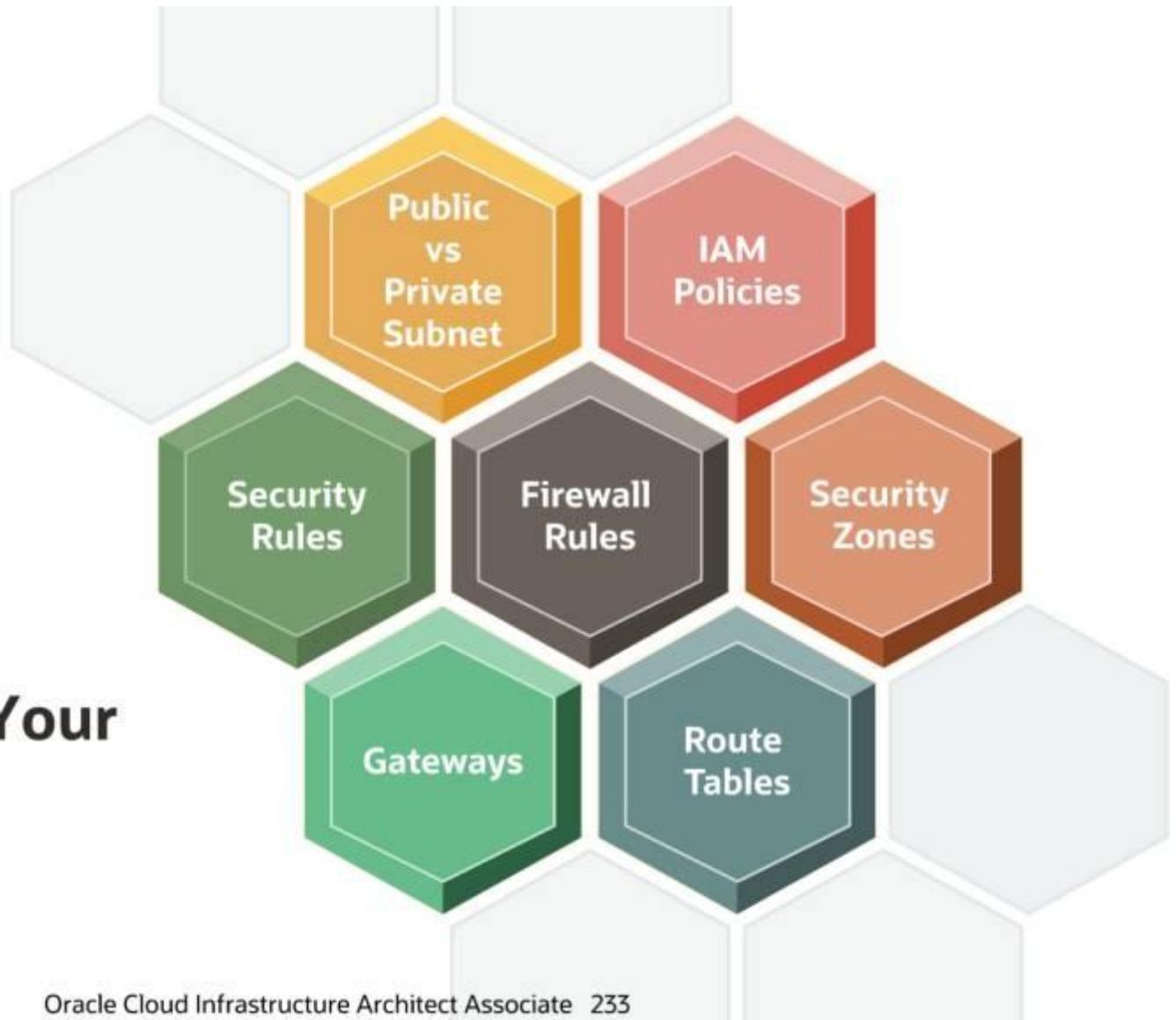
### Networking – Virtual Cloud Network

Oracle Cloud Infrastructure

# VCN Security

—  
**Networking – Virtual Cloud Network**

# Ways to Secure Your Network



# VCN Security

- Two virtual firewall features to control traffic:
  - Security Lists (associated with subnet)
  - Network Security Groups (associated with VNIC)
- SL alone, NSG alone, or both together can be used.
- Up to five Security Lists to a subnet can be associated.
- A VNIC can be added to a maximum of five NSGs.
- Each VCN comes with a default security list; you can delete the rules if you require.

# Oracle Cloud Infrastructure Network Security Group

---

## Networking – Virtual Cloud Network

# Network Security Group

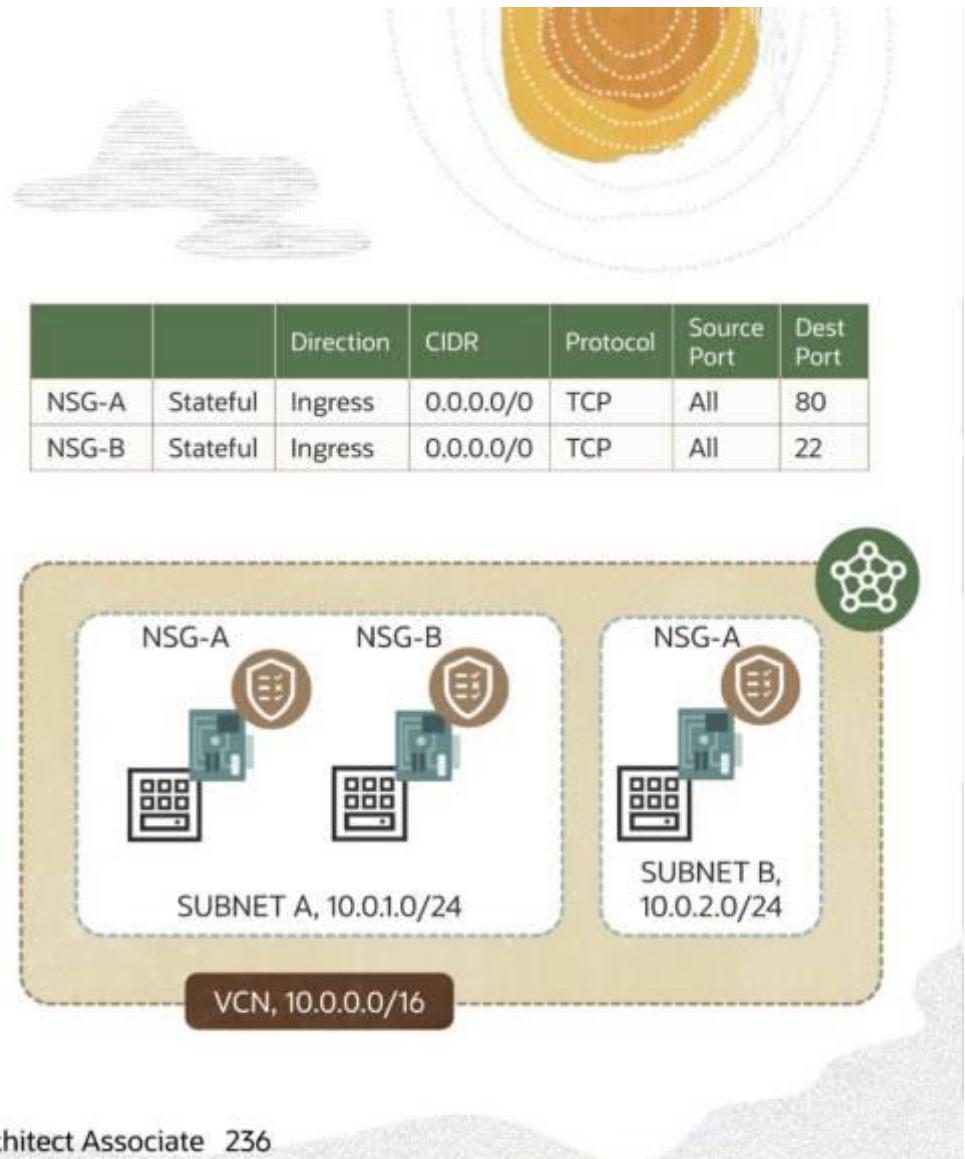
Virtual firewall

For resources having same security posture

Consists of a set of VNICs and a set of security rules

Supported Resources

VCN does not have a default NSG.



# NSG as the Source or Destination of a Rule

- Specify an NSG as the source of traffic (for ingress rules) or the traffic's destination (for egress rules).
- Easily write rules to control traffic between two different NSGs. The NSGs must be in the same VCN.

# Stateful Security Rules

Automatically allow response traffic

Indicates that you want to use connection tracking for any traffic that matches the rule

Optional: add one or more rules to the network security group. [Learn more about security rules](#)

**Rule**

Stateless (Optional)

Direction: **Ingress** (Optional)

Source Type: CIDR

Source CIDR: 0.0.0.0/0

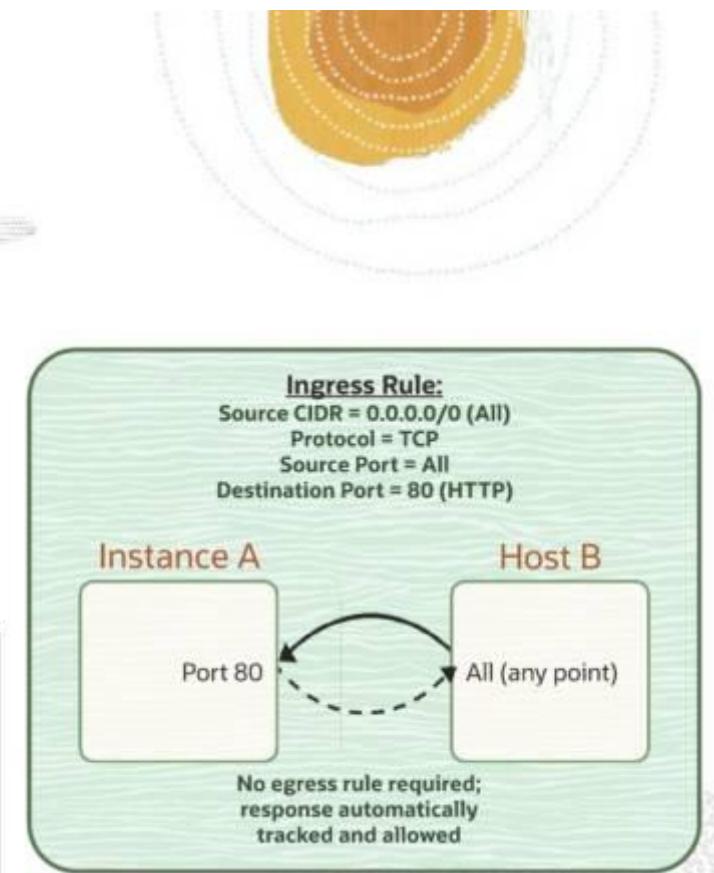
Allows: Allows TCP traffic 80

Description: Customer  
For HTTP access

Source IP address: 4.0.4.253.254.253.255 (1.234.567.890 IP addresses)

Destination Port Range: Optional

Port 80

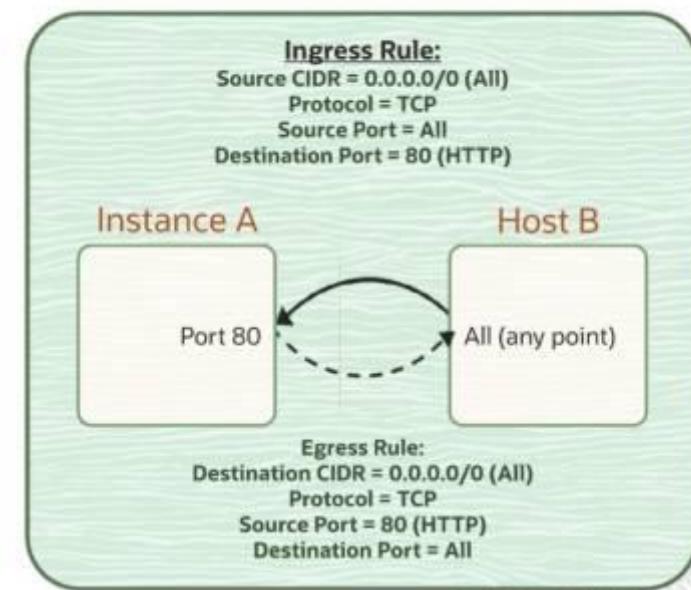


# Stateless Security Rules

Does not automatically allow response traffic

Indicates that you do NOT want to use connection tracking for any traffic that matches the rule

Recommended if you have a high-volume internet-facing website (for the HTTP/HTTPS traffic)



Oracle Cloud Infrastructure

# Demo: Network Security Groups

—  
**Networking – Virtual Cloud Network**

## Oracle Cloud Infrastructure

# Security List

### Networking – Virtual Cloud Network

# Security List

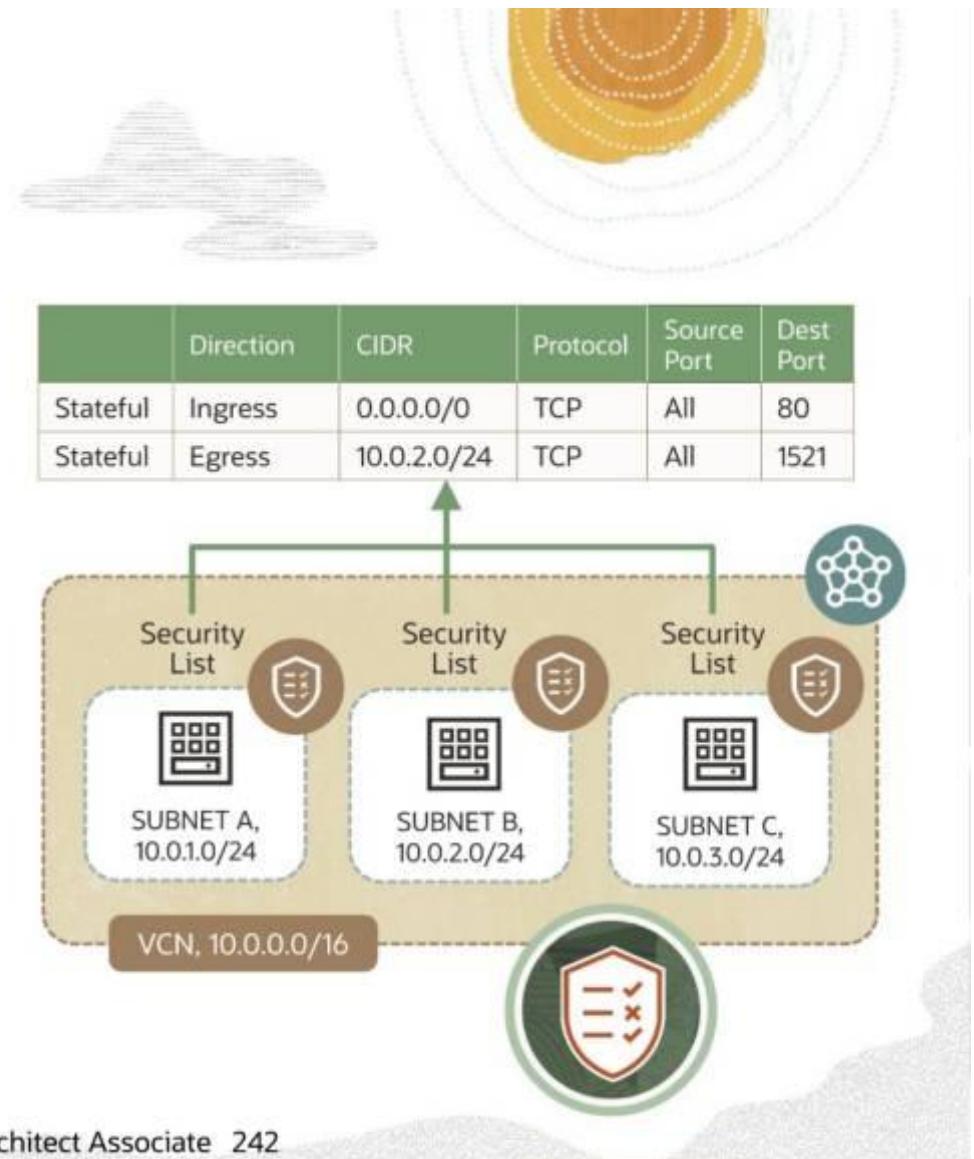
Common set of firewall rules

Associated with a subnet

Applied to instances launched inside the subnet

Consists of rules that specify the types of traffic allowed in and out of the subnet

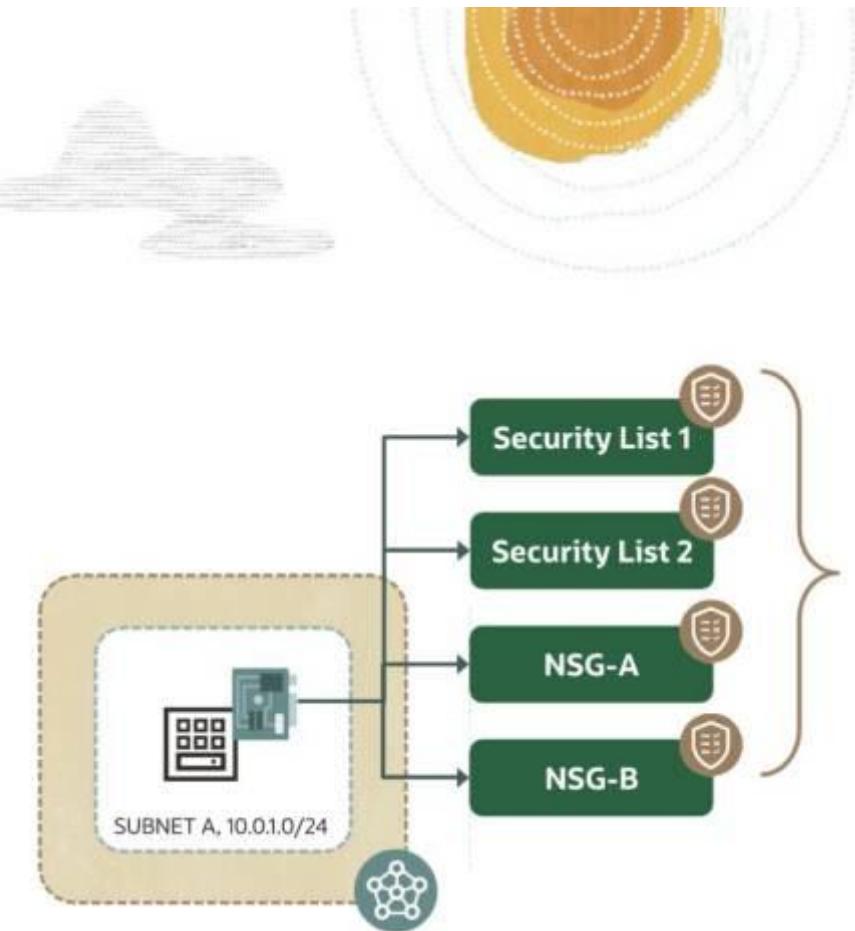
Is enforced at the VNIC level



## SL + NSG

Use SLs alone, NSGs alone, or both together.

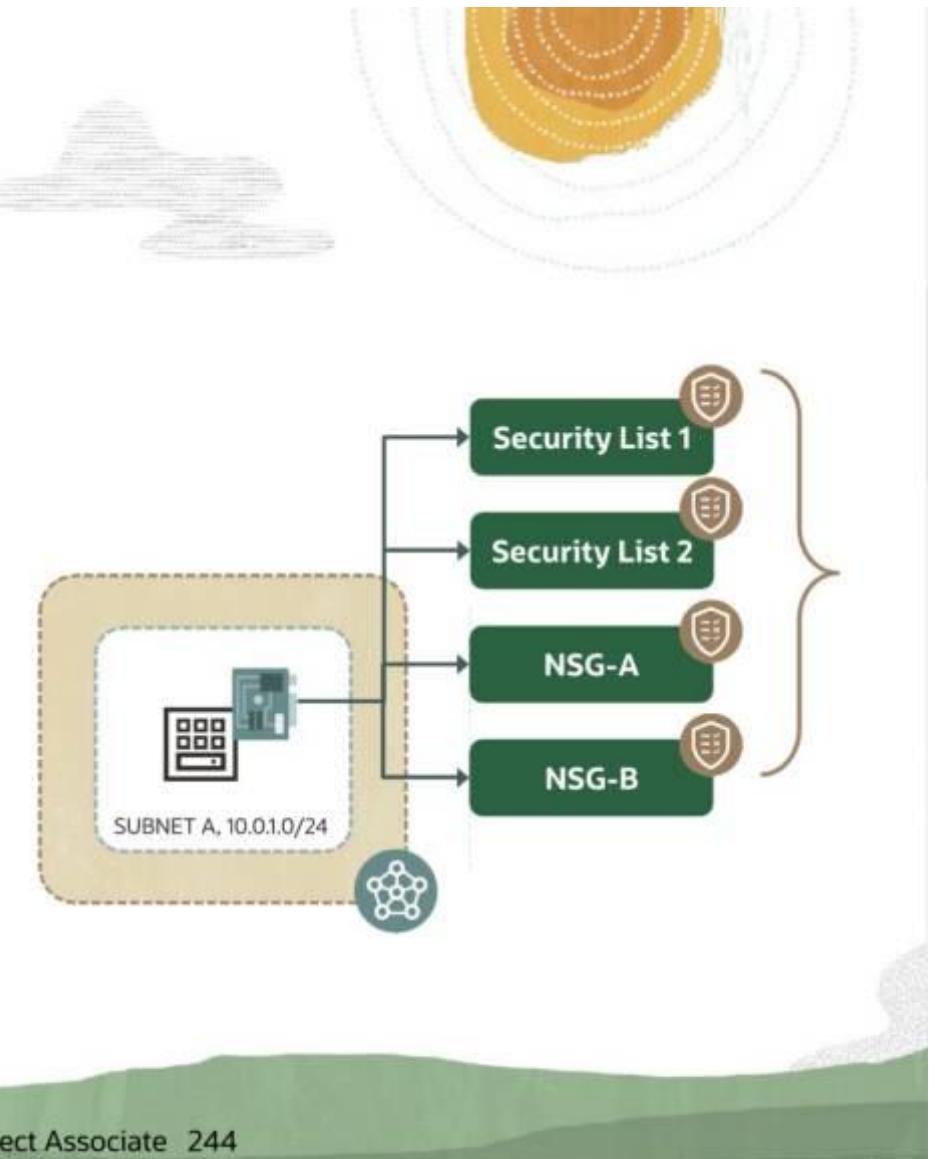
To enforce security rules for all VNICs in a VCN, put the rules in one SL, and then associate that SL with all the subnets in the VCN.



## SL + NSG

If you choose to use both SLs and NSGs, the set of rules that apply to a given VNIC is the union of:

- › The security rules in the SLs associated with the VNIC's subnet
- › The security rules in all NSGs that the VNIC is in
- › A packet in question is allowed if any rule in any of the relevant lists and groups allows the traffic



Oracle Cloud Infrastructure

# Demo: Security Lists

—  
**Networking – Virtual Cloud Network**



# Networking - IP Management

Oracle Cloud Infrastructure

# Overview of IP Management

## IP Management



# IP Management Overview

Public IP addresses

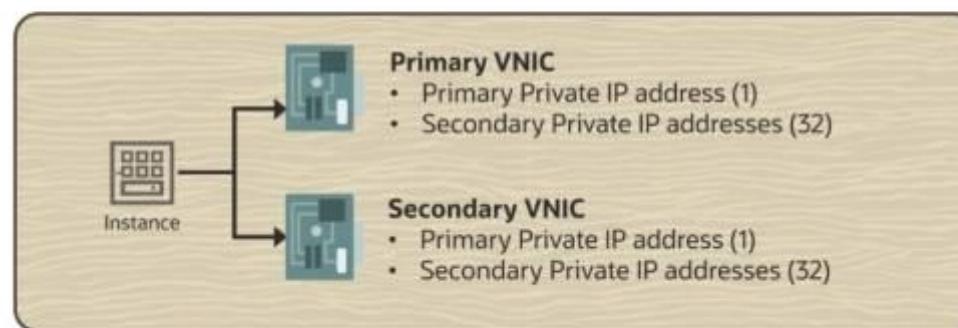
Bring Your own IP

Private IP addresses

IP Pools

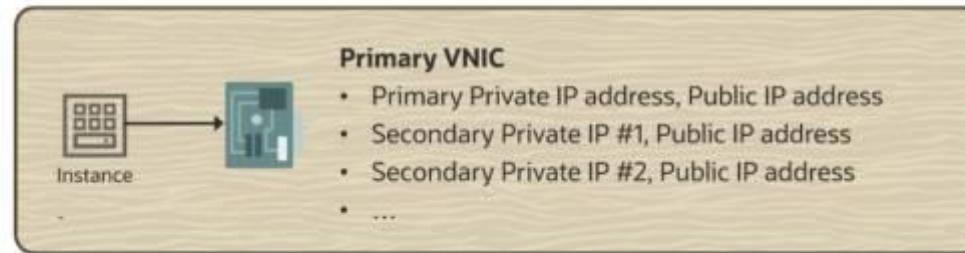
# Private IP

- Each instance has at least one Primary Private IP address.
- A Private IP can have an optional Public IP assigned to it (when public subnet is used).
- Every VNIC has one Primary Private IP address and can have additional Private IPs called Secondary Private IPs.



# Public IP

- It is reachable from the Internet; assigned to a Private IP object on the resource.
- For a Public IP to be reachable over the Internet, its VCN must have an Internet Gateway.
- Public Subnet must have Route Table and Security Lists configured.
- It is possible to assign a resource multiple Public IPs across one or more VNICs.



# Types of Public IPs

## Ephemeral

Temporary and existing for the lifetime of the instance.

## Reserved

Persistent and existing beyond the lifetime of the instance it's assigned to.

There is no charge for using Public IP

# Oracle Cloud Infrastructure Reserved Public IP

---

## IP Management

## Reserved Public IP

- ✓ Persistent
- ✓ Exists beyond the lifetime of instances
- ✓ Unassign and reassign whenever you like
- ✓ No automatic deletion
- ✓ Reduce security risk by dynamically assigning public IP addresses when needed

Reserve public IP address	
Create a reserved IP address from Oracle's IP addresses or from a public IP pool you've previously created.	
Reserved public IP address name	DemoResPubIP
Create in Compartment	intoraclearohit (root)
IP address source in intoraclearohit (root) <small>Optional</small>	<a href="#">(Change compartment)</a>
Oracle	
<a href="#">Show advanced options</a>	

Oracle Cloud Infrastructure

# Bring Your Own IP Address (BYOIP)

—  
**IP Management**

# Bring Your Own IP (BYOIP)

Bring your own IP address space to OCI.

You must have ownership of the public IPv4 CIDR block/IPv6 prefix.

There is a formal validation of ownership at Regional Internet Registry (RIR).

Move your CIDR blocks that have a minimum size of /24 and a maximum of /8.

Imported IPv6 prefix must be /48 or larger.

IP Addresses are managed through IP Pools – groups of IP addresses.



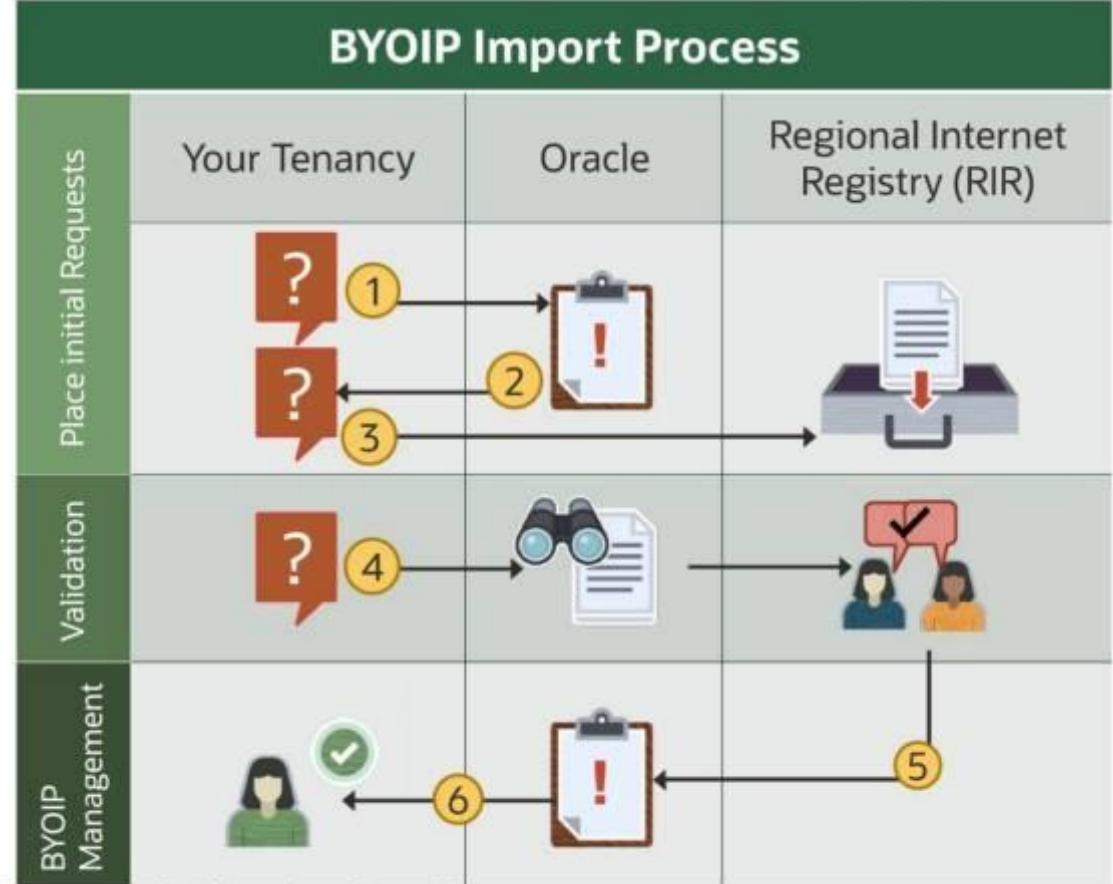
## BYOIP Benefits

---



## BYOIP Workflow

1. Request Import
2. Token is issued
3. Presented to RIR
4. Create a ROA with RIR
5. Finish Import
6. Provision Addresses



# Oracle Cloud Infrastructure Public IP Pools

---

## IP Management

## Public IP Pools

- ✓ Set of IPv4 CIDR blocks allocated to a tenancy
- ✓ Can be all or part of a BYOIP CIDR block
- ✓ Only available for your tenancy
- ✓ Available as a source for IP allocation when launching a:
  - ✓ NAT Gateway
  - ✓ Load Balancer
  - ✓ Compute Instance
- ✓ Launch resources with an IP directly allocated
- ✓ Minimum size of /28 to a maximum size of /24

IPv6 addresses do not use the IP Pools functionality.

Oracle Cloud Infrastructure

# Demo: IP Management

—  
**Networking – IP Management**

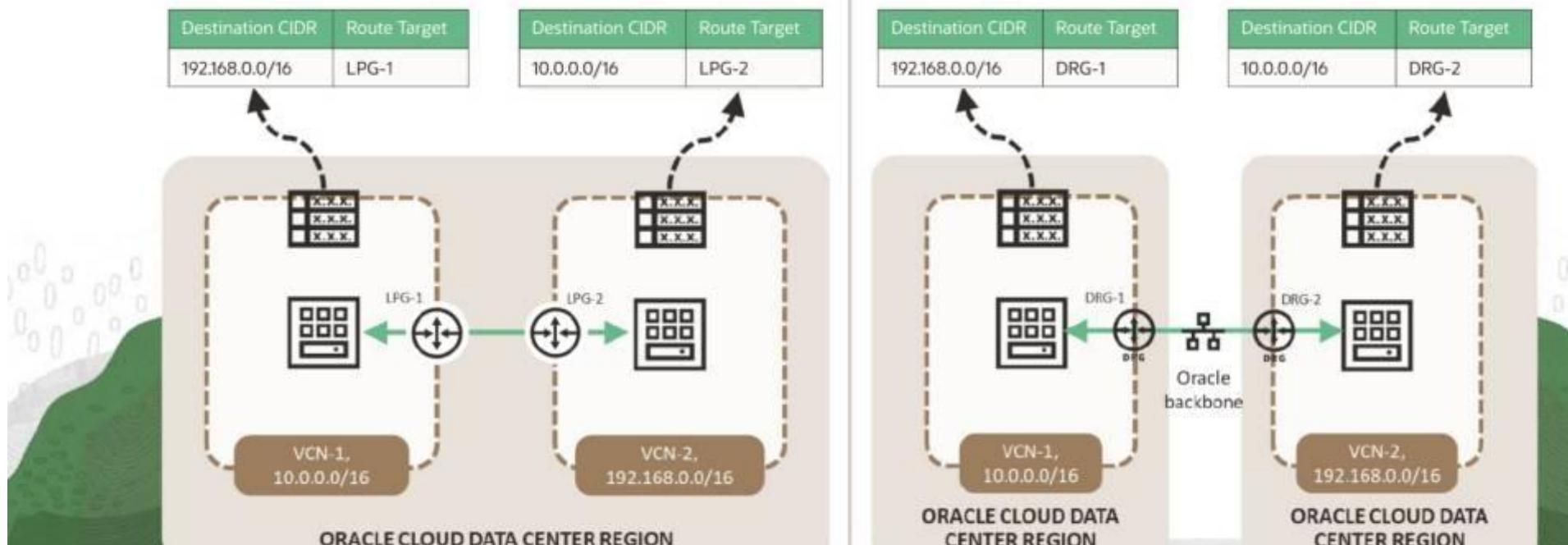
# Networking - Connectivity

Oracle Cloud Infrastructure

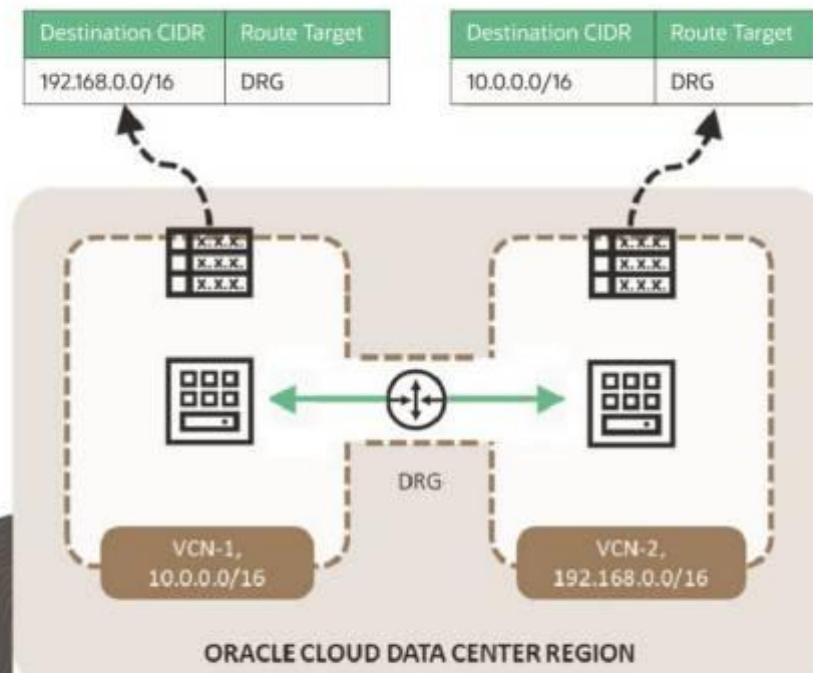
# VCN Connectivity Options

## Networking – Connectivity

# Local Peering Versus Remote Peering

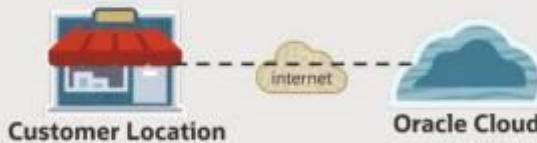


# Local Peering with DRG VCN Attachments



## Connecting On-Premises to OCI

### Public Internet



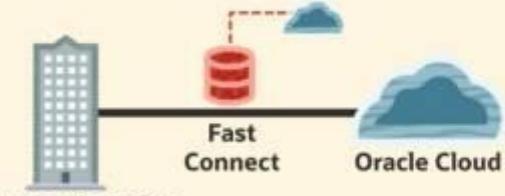
- Connectivity over Internet via Internet Gateway or NAT Gateway
- For apps in development, or in test/pilot phase

### Site-to-Site VPN



- Secure connectivity over Internet
- No throughput guarantee
- OCI-managed service
- Free service

### FastConnect



- Dedicated, secure connectivity
- Low latency interconnect
- High Bandwidth – up to 100 Gbps
- OCI Managed service
- Competitive pricing
- For business-critical applications

# Considerations for Cloud Connectivity Options

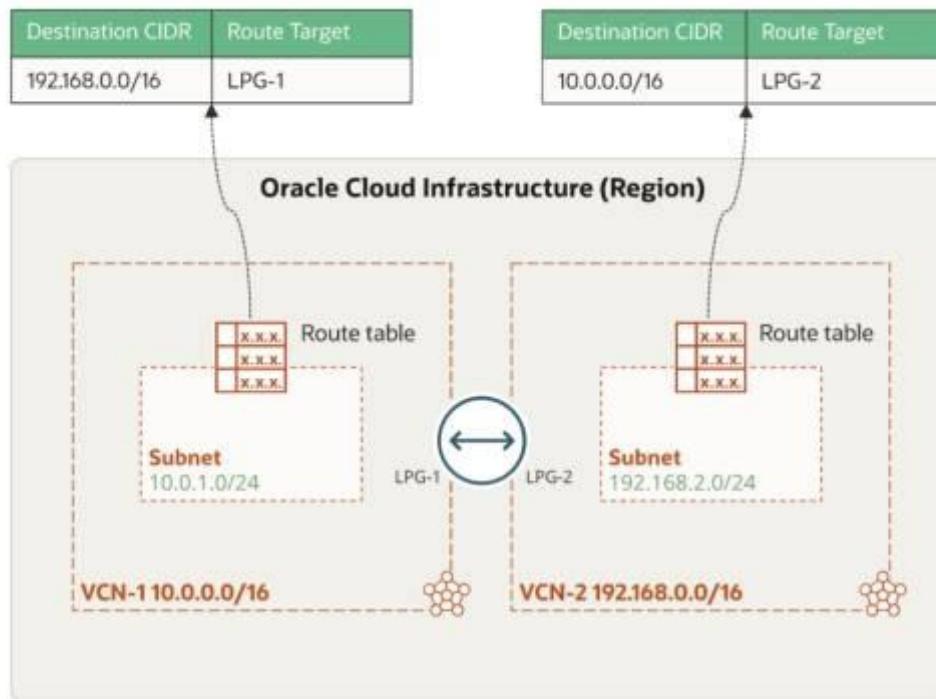


Cloud Connectivity Option	Considerations
<b>FastConnect</b>	Higher data throughput, lower latency, consistent performance Network costs may be higher than Internet costs
<b>Site-to-Site VPN</b>	Added layer of tunneled encryption to Internet connections; recommended for Proofs of Concept (POCs)
<b>Public Internet</b>	Best effort performance Suited for SaaS applications and consumer/SMB use

# Oracle Cloud Infrastructure Local VCN Peering

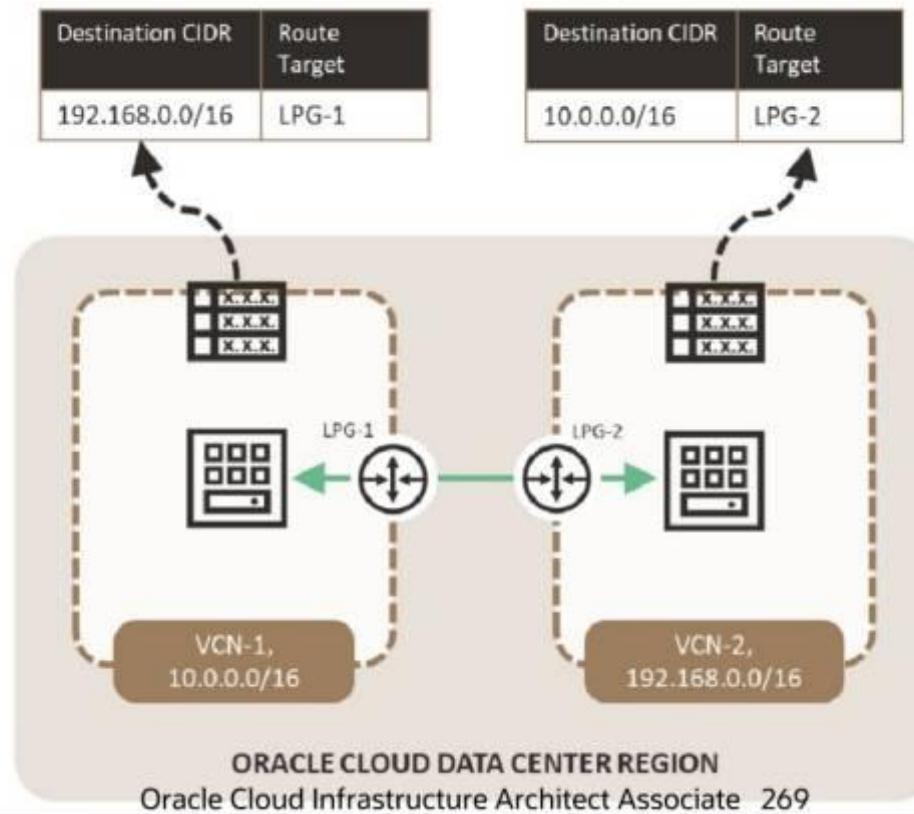
## Networking – Connectivity

# Local VCN Peering (Using LPGs)

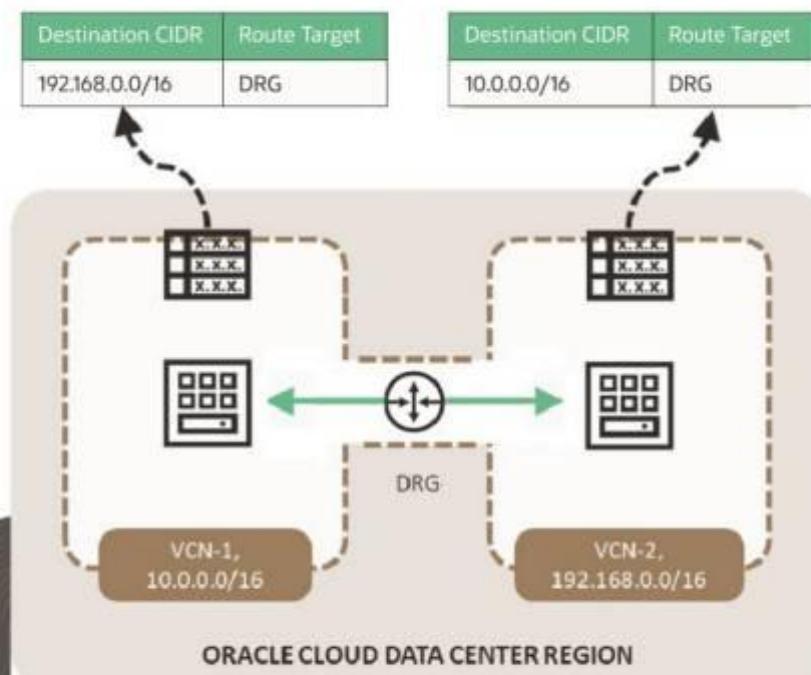


- › Connect two VCNs in the same region
- › Resources can communicate by using private IP addresses.
- › A Local Peering Gateway (LPG) is required for each VCN peered locally.
- › The two VCNs shouldn't have overlapping CIDRs.
- › A connection between those two Local Peering Gateways
- › Supporting route rules
- › Supporting security rules

# Local VCN Peering (Using LPGs)



# Local VCN Peering (Using Upgraded DRG)



Oracle Cloud Infrastructure

# Demo: Local VCN Peering

—  
**Networking – Connectivity**

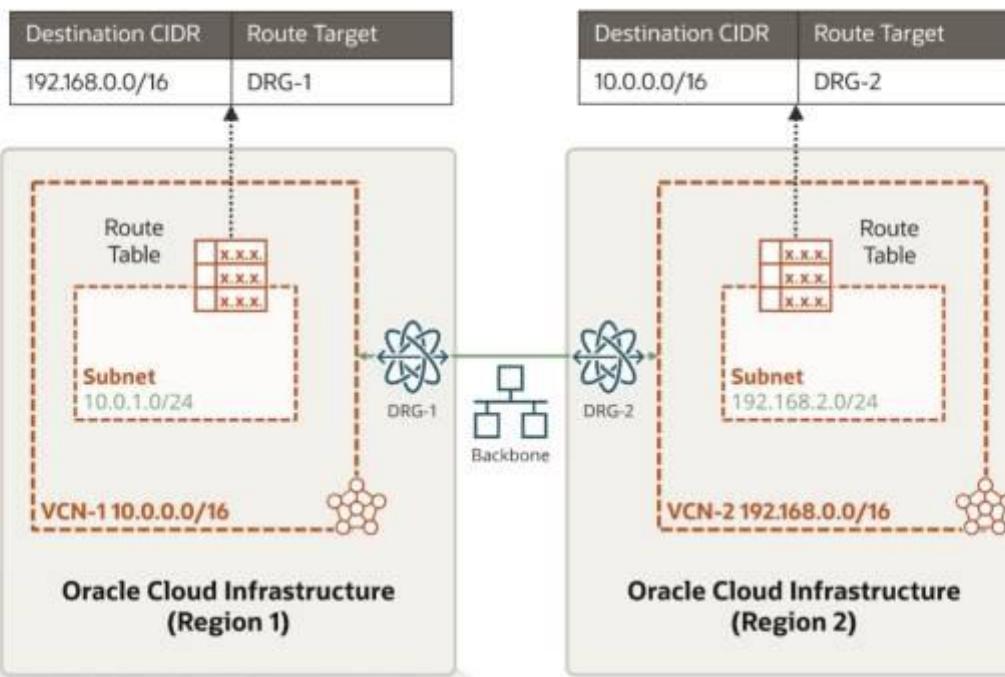
# Oracle Cloud Infrastructure

## Remote VCN Peering

---

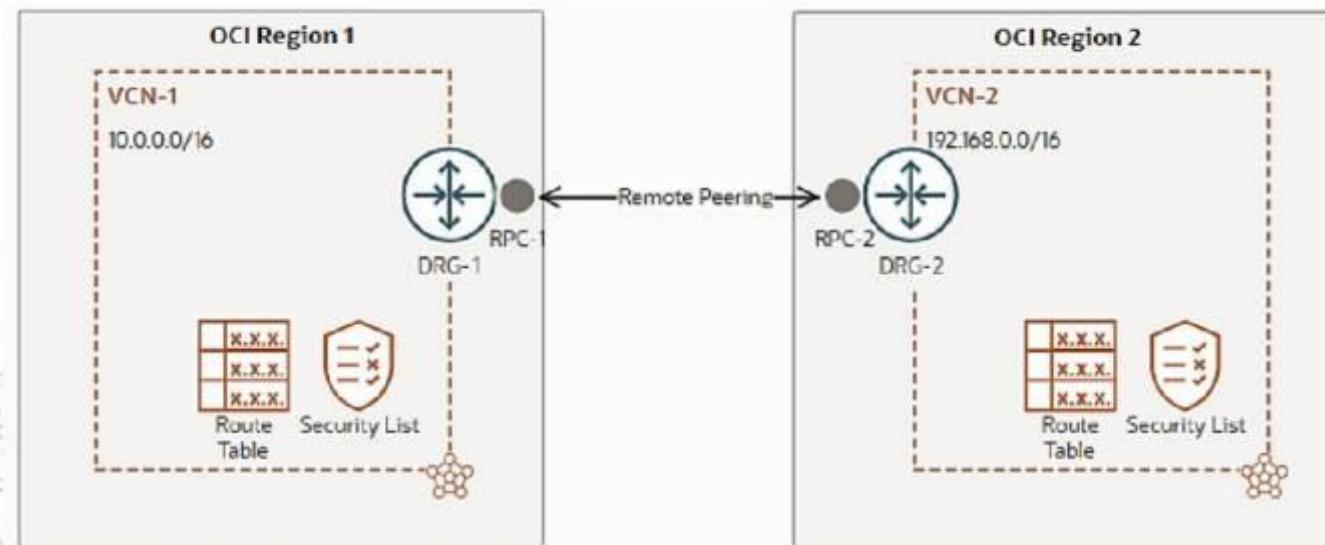
### Networking – Connectivity

# Remote Peering Connection



- Connect two VCNs so that their resources can communicate using private IP addresses.
- It requires a remote peering connection (RPC) to be created on the DRGs.
- RPC's job is to act as a connection point for a remotely peered VCN.
- VCNs must not have overlapping CIDRs.
- Typically, RPC is for VCNs located in different regions. But it can be used for VCNs in the same region too.
- Legacy DRGs will not support connecting DRGs in different tenancies.

# Remote Peering (Across Regions)



Oracle Cloud Infrastructure

# Demo: Remote VCN Peering

—  
**Networking – Connectivity**

# Oracle Cloud Infrastructure BGP Basics

## Networking – Connectivity

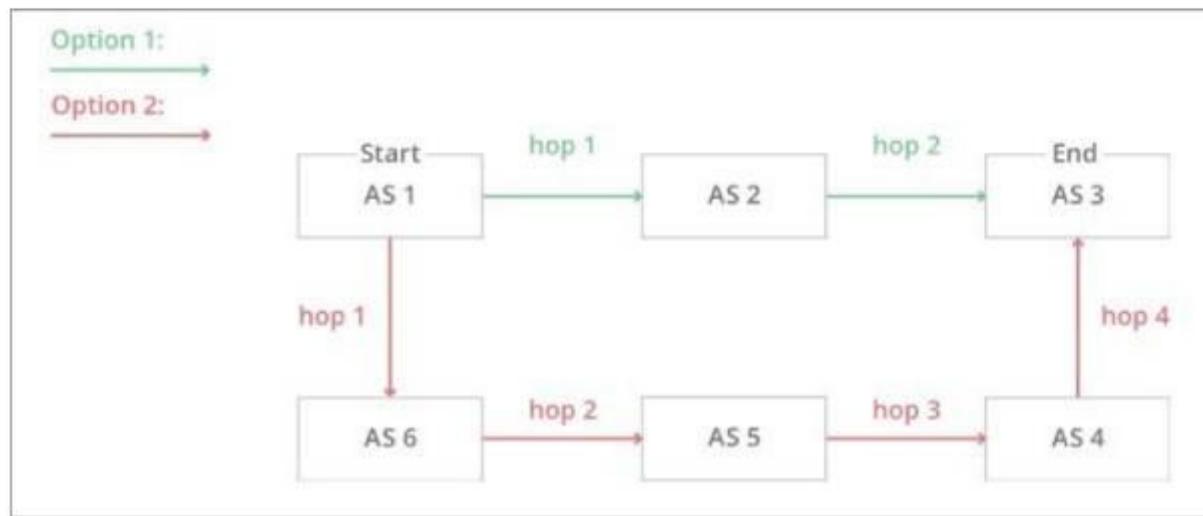
# Border Gateway Protocol (BGP)

---

- Routing protocol for the Internet
- Exchange routing information between autonomous systems (AS)
- Autonomous Systems: Collection of connected IP networks
- Looks at all of the available paths that data could travel
- Picks the best route, which usually means hopping between autonomous systems

# Border Gateway Protocol (BGP)

Picks the best route, which usually means hopping between autonomous systems



# Border Gateway Protocol (BGP)



Site-to-Site VPN can use either BGP or static routing, or a combination.



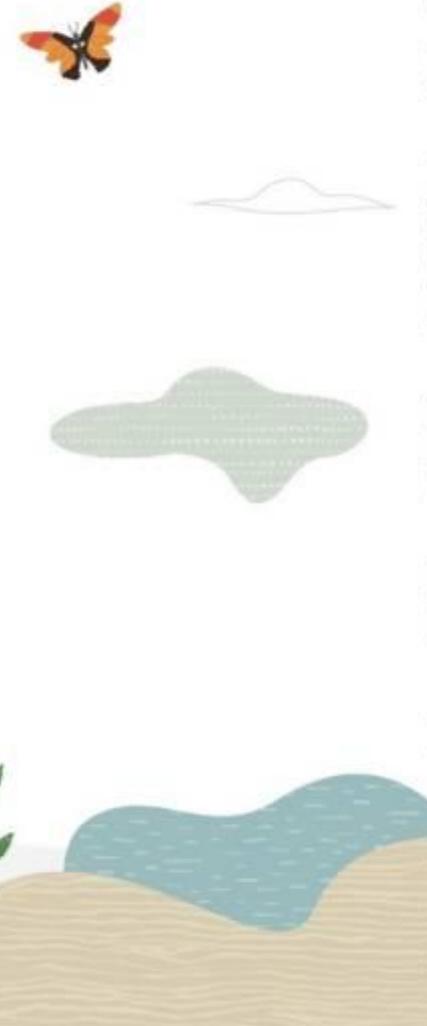
FastConnect always uses BGP for route advertisements.

Oracle Cloud Infrastructure

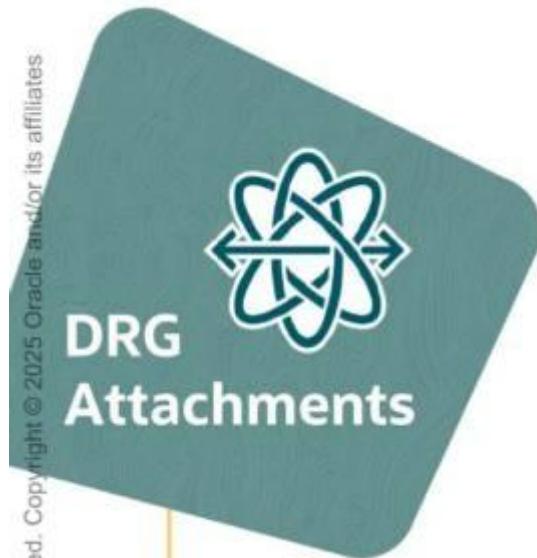
# Dynamic Routing Gateway

**Networking – Connectivity**

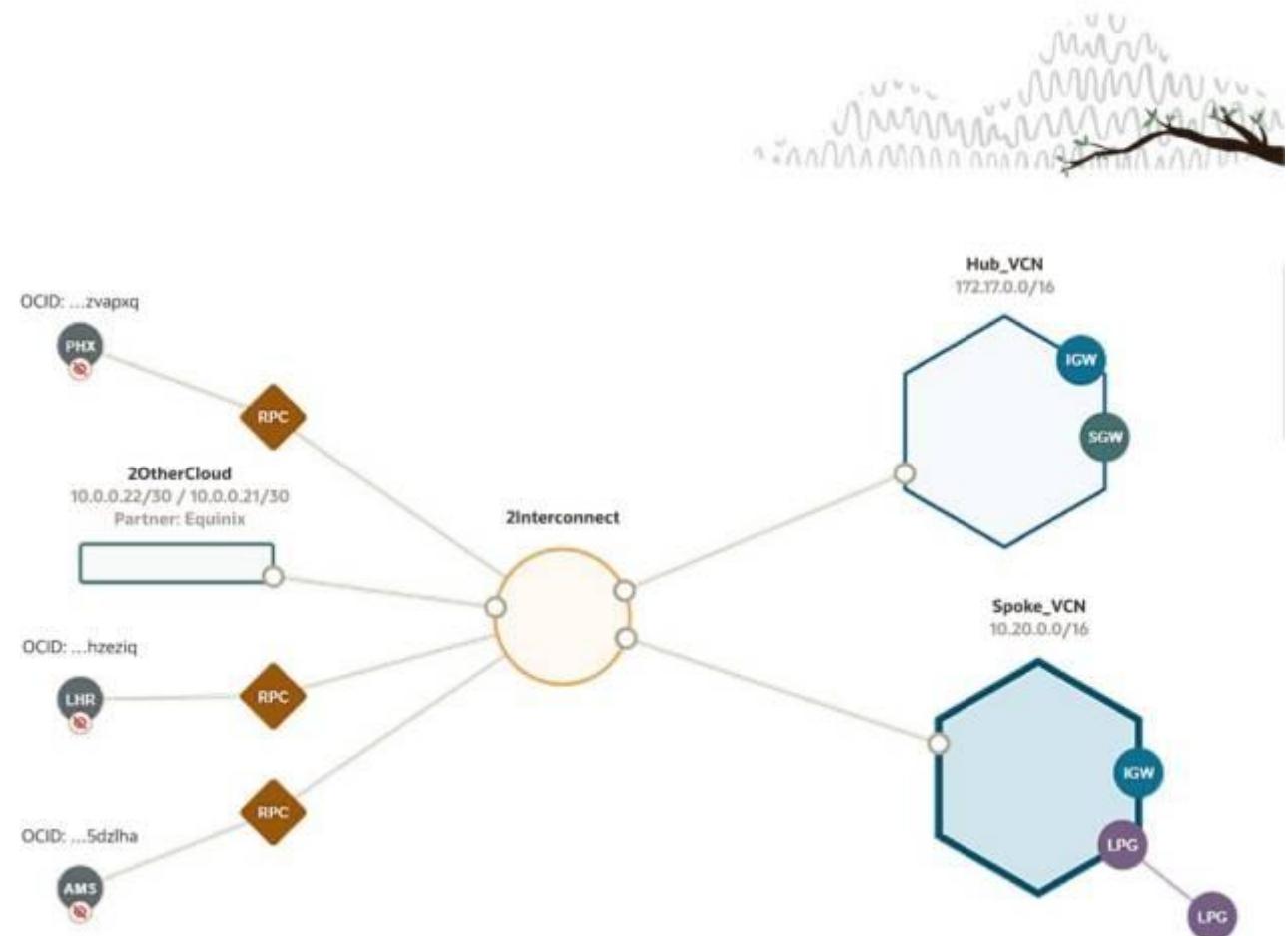
## Dynamic Routing Gateways



- Virtual Router
- Provides a path for traffic between on-premises and VCNs
- Each DRG attachment has an associated route table.
- Static routes
- Import route distributions
- Can attach:
  - VCNs
  - Remote Peering Connections
  - Site-to-Site VPN IPSec tunnels
  - FastConnect virtual circuits



- VCN attachments
- RPC attachments
- IPSEC\_TUNNEL attachments
- VIRTUAL\_CIRCUIT attachments
- LOOPBACK attachments





## DRG Route Tables & Route Distributions

When you create a DRG, two default route tables are created:

- VCN attachments
- All other attachments

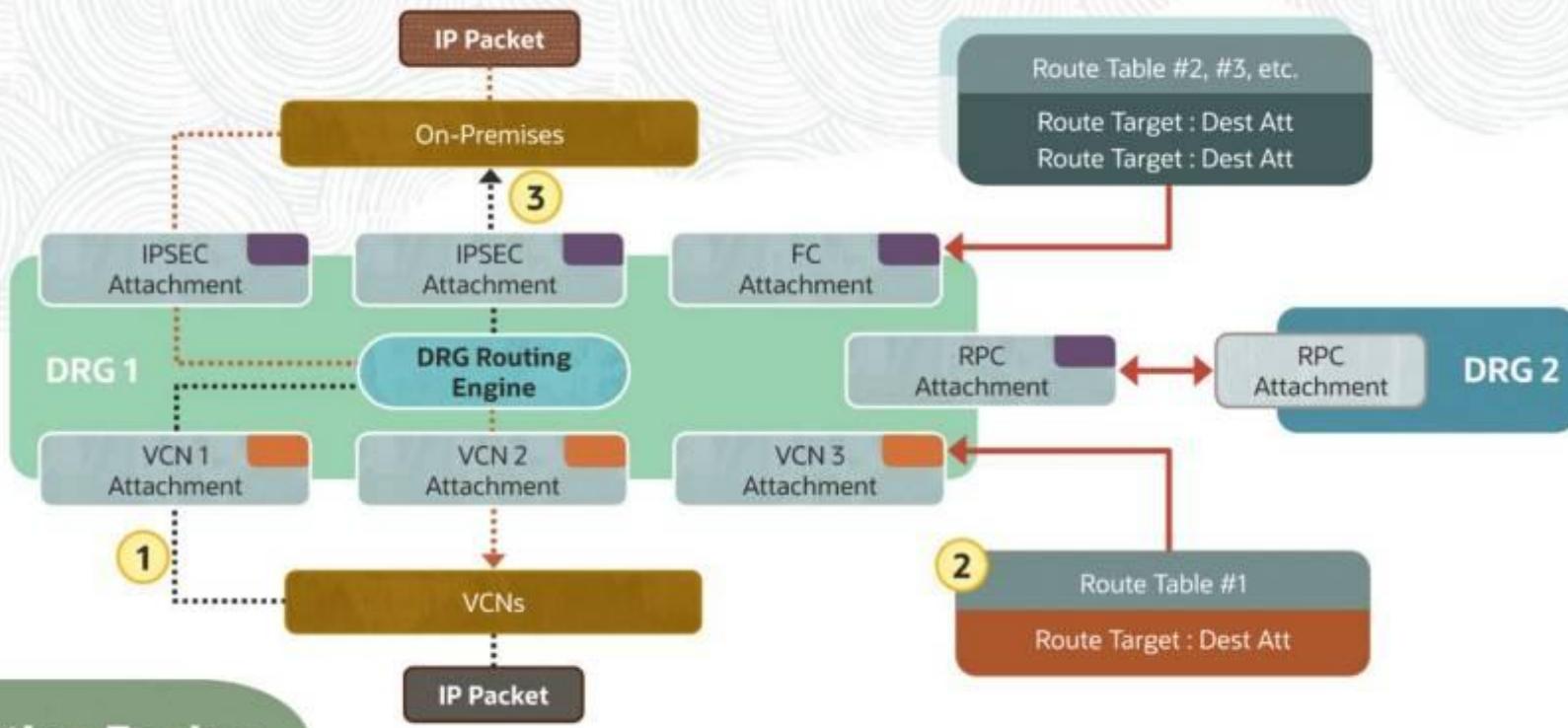
Assign a different route table and policy to each network resource attached to your DRG

Equal cost multi-path (ECMP) routing

- 
- Simplified configuration
  - High availability
  - Increased scale
  - Complex routing



## DRG Use Cases



## DRG Routing Engine

- 1: Packet arrives into DRG from VCN (VCN attachment) or on-premises (FC/IPSEC attachment) or remote region (RPC attachment).
- 2: A route lookup is performed on the route table associated with the ingress attachment.
- 3: The packet is forwarded by the DRG routing engine out to an Egress attachment.

Oracle Cloud Infrastructure

# Demo: Dynamic Routing Gateway

—  
**Networking – Connectivity**

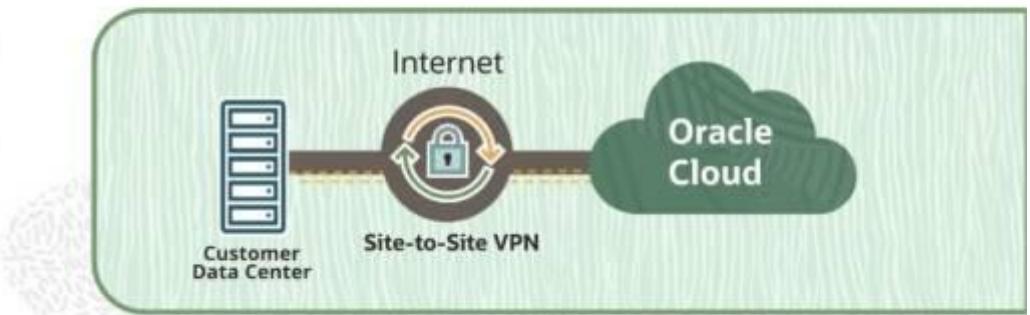
# Oracle Cloud Infrastructure Site-to-Site VPN

## Networking – Connectivity

# Site-to-Site VPN: Overview

- Offers a simple and secure way to connect your corporate network to Oracle Cloud Infrastructure over your existing Internet connection
- Encrypts your data and tunnels it through the public Internet for enhanced security and privacy with an IPSec VPN connection

Features
Site-to-site VPN for a secure connection between your network and the Oracle Cloud
High availability with two tunnels connected to redundant Oracle routers
Industry-standard Internet Key Exchange version 1 (IKEv1 and IKEv2) protocol



# Site-to-Site VPN: Use Cases



Use for Proof of Concept



Connect multiple locations to the cloud



Securely connect your existing infrastructure to the cloud



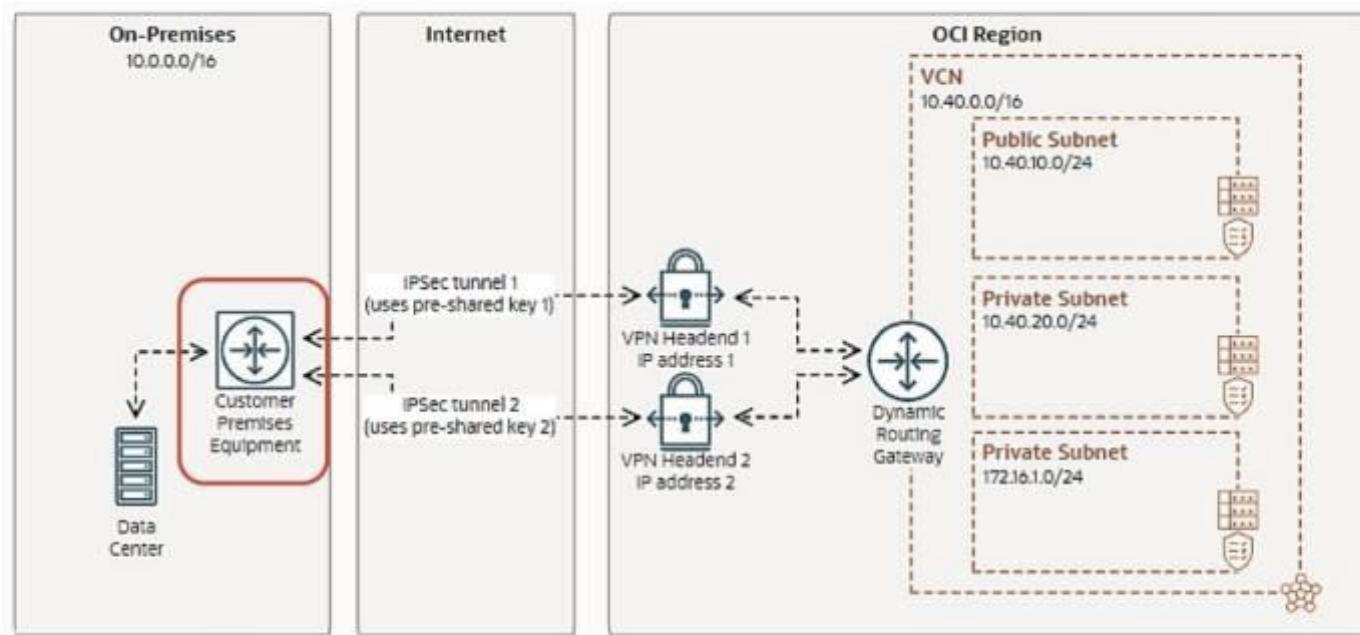
Build redundant connectivity for Oracle FastConnect



# Customer-Premises Equipment

## Verified equipment vendors

- › Check Point
- › Cisco
- › Fortinet
- › Furukawa
- › Juniper
- › Libreswan
- › NEC
- › Palo Alto
- › WatchGuard
- › Yamaha

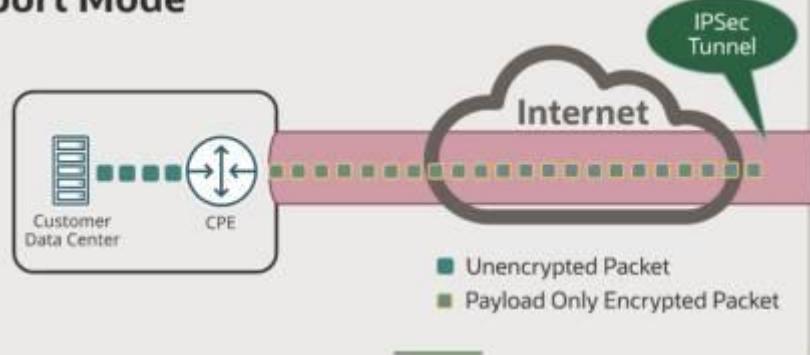


# Site-to-Site VPN

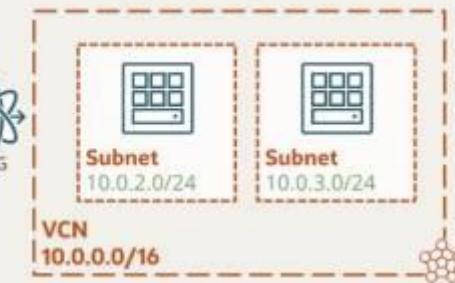
- OCI VPN supports IKEv1 and IKEv2.
- Dynamic Routing Gateway (DRG) - VPN headend at OCI end.
- Customer Premise Equipment (CPE).
  - Actual VPN router in your on-premises network (hardware or software)
  - When setting up the VPN, you create a **virtual representation** of your on-premises router, which is known as CPE object.
  - To create a CPE Object – Name, Outside Public IP address
- IPsec Connection
  - After creating the CPE object and DRG, you connect them by creating an IPsec connection, which results in two redundant IPsec tunnels.
  - Static Routing and BGP Routing supported

# Site-to-Site VPN: Tunnel Mode

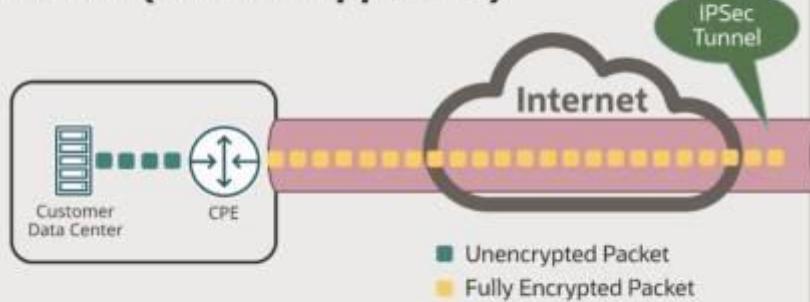
## Transport Mode



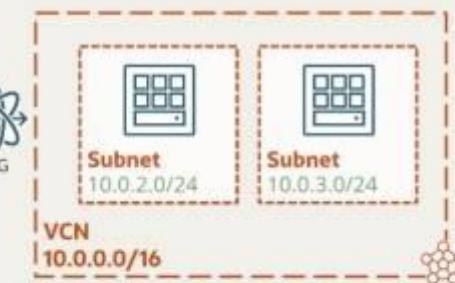
## Oracle Cloud Infrastructure (Region)



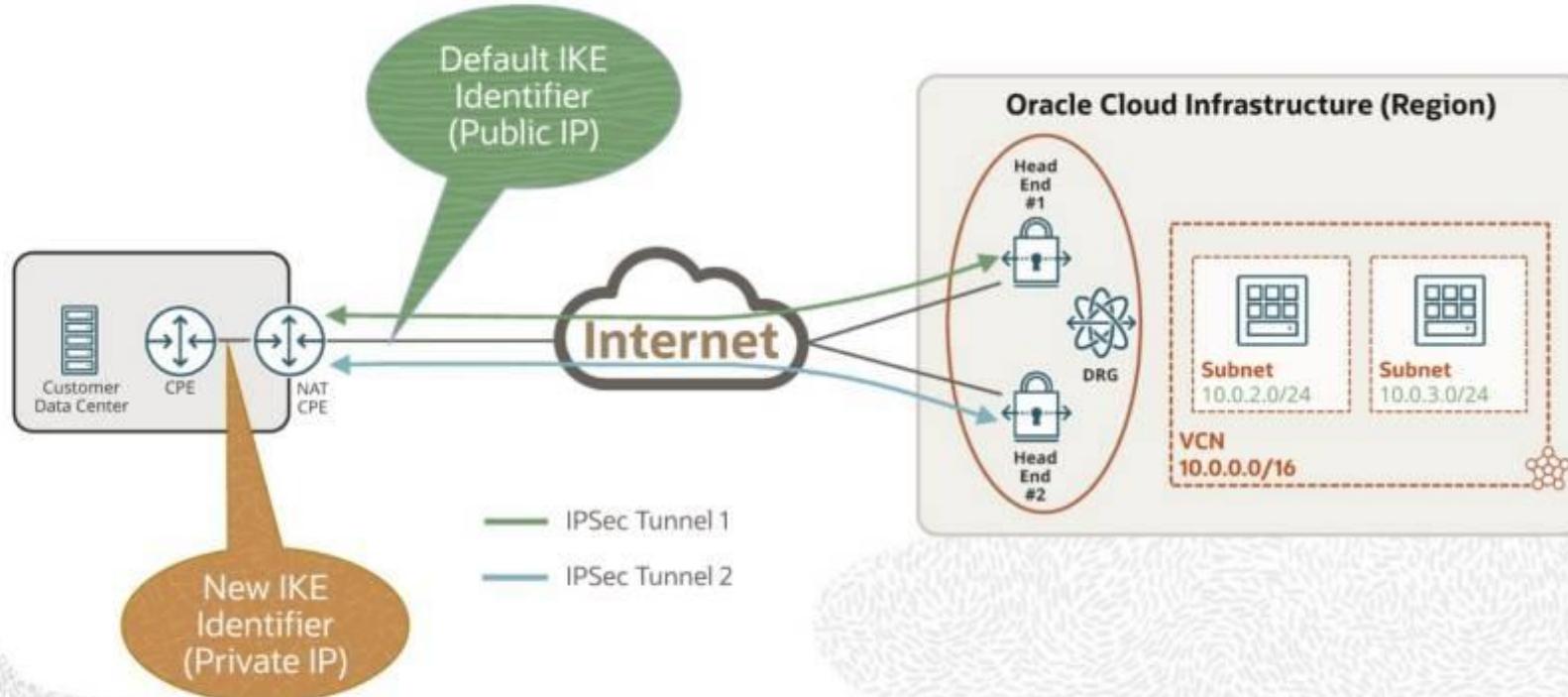
## Tunnel Mode (Oracle Supported)



## Oracle Cloud Infrastructure (Region)



# Site-to-Site VPN: CPE Behind a NAT Device



Oracle Cloud Infrastructure

# Demo: Site-to-Site VPN

—  
**Networking – Connectivity**

## Oracle Cloud Infrastructure FastConnect Overview

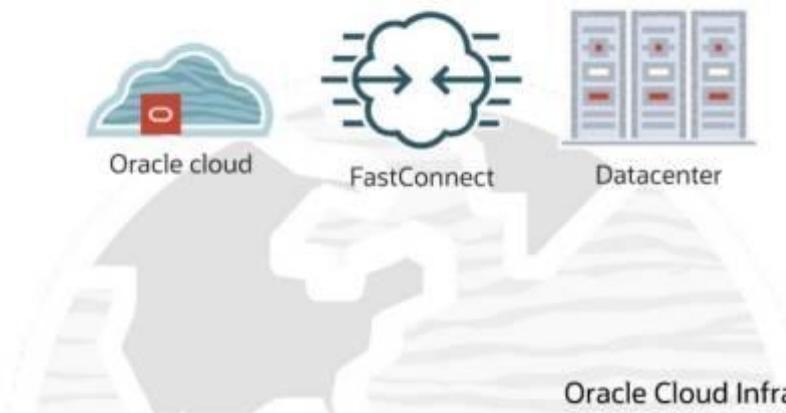
### Networking - Connectivity

# Overview

Dedicated, Private Connection

High bandwidth

No data transfer charges



- Flexible connection options
  - ✓ Oracle Partners
  - ✓ Third-Party Provider
  - ✓ Colocation with Oracle
- Data does not traverse the Internet
- Extend existing infrastructure into a VCN in OCI (Private Peering)
- Access public services in OCI without using the Internet (Public Peering)

# FastConnect Concepts

FastConnect  
Location

Colocation

Physical Device

Metro Area

Cross-Connect

Logical Device

Oracle Partner

Virtual Circuit

Letter of  
Authorization

Third-Party  
Provider

## FastConnect Connectivity Models

### FastConnect: With an Oracle Partner

- Connectivity between customer and Oracle through a pre-established FastConnect Connectivity Partner
- Most flexible and typically least expensive to deploy

### FastConnect Direct: Colocation

- Direct connection between customer and Oracle via fiber cross-connect
- Good model if customer is already collocated in the same data center facility

### FastConnect Direct: With a Third-Party Provider

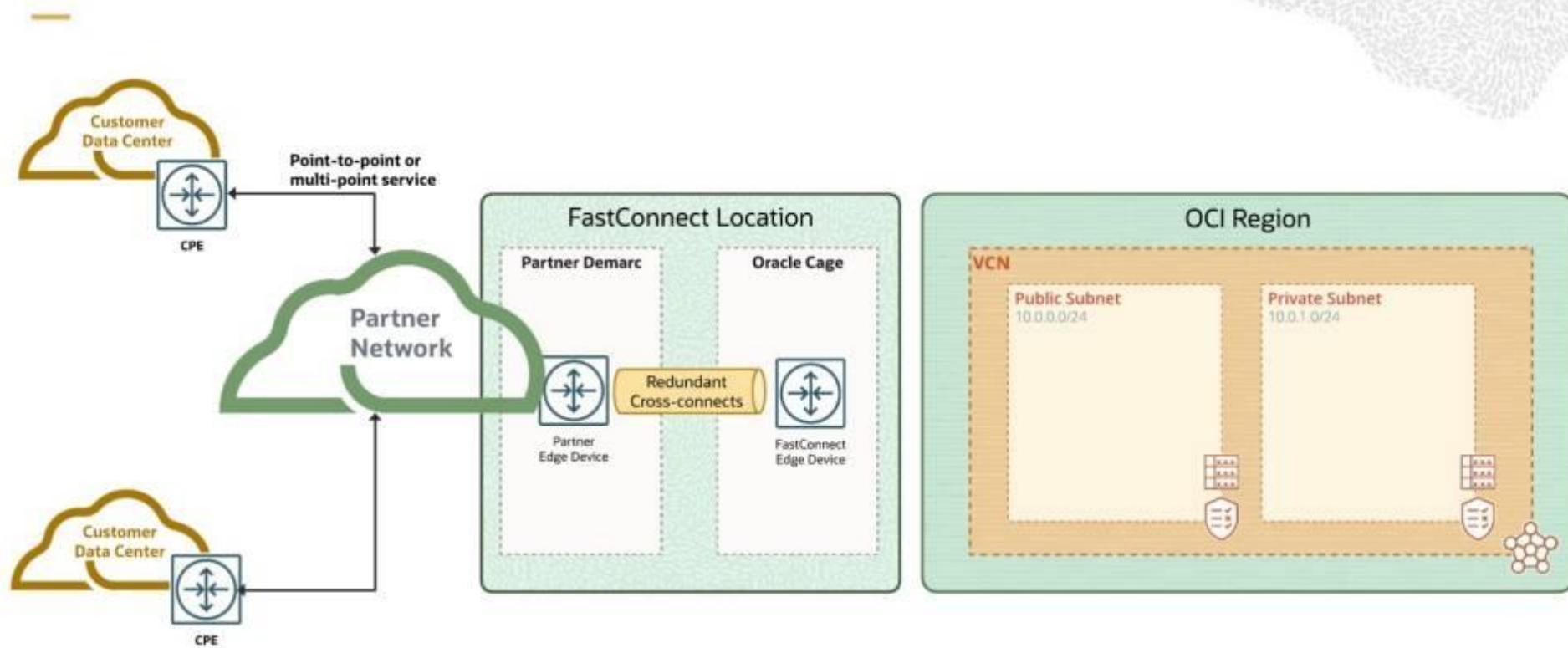
- Direct connection between customer and Oracle with a private or dedicated circuit from a third-party network carrier
- Good model if customer has an existing relationship with certain network carriers and/or if the customer data center is not served by any of Oracle's FastConnect partners

Oracle Cloud Infrastructure

# FastConnect with an Oracle Partner

—  
**Networking - Connectivity**

## FastConnect: With an Oracle Partner



# Setup: FastConnect with an Oracle Partner

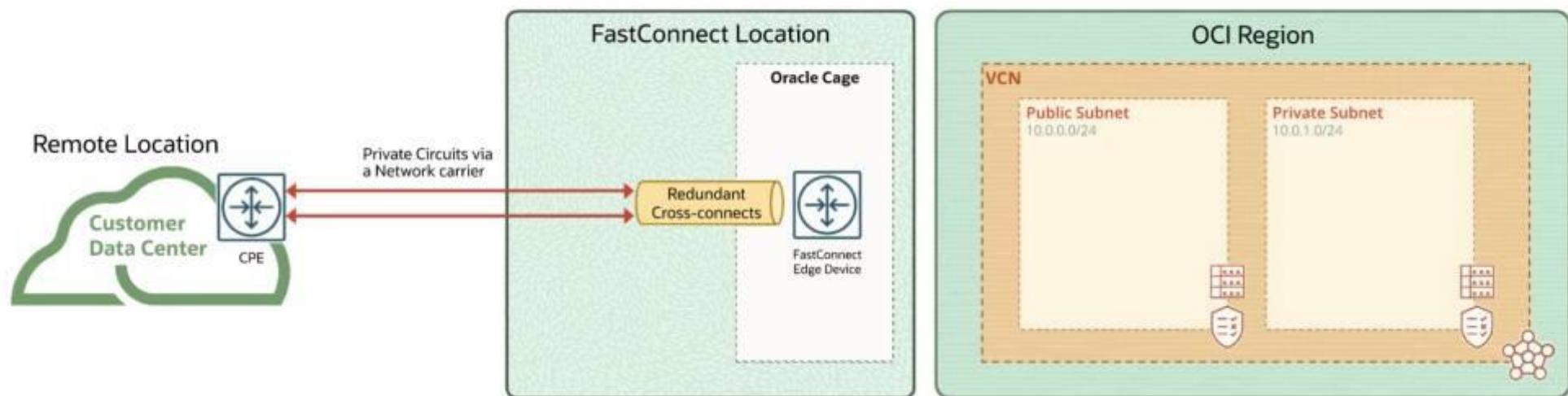
Oracle Partner Setup			
	On-Premises Edge	Oracle Partner	Oracle Console
Learn and Plan		<b>1</b> Set up connection to Oracle Partner	
Set up Connection with Oracle	<b>5</b> Configure your edge	<b>4</b> Give Oracle Partner Information about virtual circuits	<b>2</b> Set up DRG (private virtual circuit only) <b>3</b> Set up Virtual Circuits
Validate Connectivity	<b>6</b> Check light levels <b>7</b> Confirm interfaces are up <b>If the BGP session goes from your edge to Oracle</b> <b>8a</b> Ping the Oracle BGP IP address <b>8b</b> Confirm BGP session to Oracle is established <b>If the BGP session goes from your edge to the Oracle Partner</b> <b>9a</b> Ping the Oracle Partner's edge <b>9b</b> Confirm BGP session to Oracle Partner is established <b>9c</b> Ping the Oracle BGP IP address <b>10</b> Test the connection		

## Oracle Cloud Infrastructure

# FastConnect with a Third-Party Provider

### Networking : Connectivity

## FastConnect Direct: With a Third-Party Provider



## FastConnect with a Third-Party Provider

- Third-party network carrier
- Responsible for physical connection between on-premises network and Oracle's FastConnect edge devices
- Oracle provides an LOA.
- Provide the LOA to carrier.
- Carrier provisions the circuit.
- Suitable if you have existing relationships with certain network carriers

# Setup: FastConnect with a Third-Party Provider

Third-Party Provider Setup			
Set up initial components	On-Premises Edge	Provider	Oracle Console
Third-party provider sets up physical connection at their data center	<ul style="list-style-type: none"><li>4 Check light levels for each cross-connect</li><li>5 Confirm interfaces are up for each cross-connect</li></ul>	<ul style="list-style-type: none"><li>3 Forward the LOA</li></ul>	<ul style="list-style-type: none"><li>1 Set up DRG (private virtual circuit only)</li><li>2 Set up cross-connect group and cross-connect</li></ul> <ul style="list-style-type: none"><li>4 Check light levels for each cross-connect</li><li>5 Confirm interfaces are up for each cross-connect</li></ul>
Activate and create other components			<ul style="list-style-type: none"><li>6 Activate each cross-connect</li><li>7 Set up virtual circuit</li></ul>
Configure your edge and validate connection	<ul style="list-style-type: none"><li>8 Configure your edge</li><li>9 Ping the Oracle BGP IP address across cross-connect group</li><li>10 Confirm BGP session to Oracle is established</li><li>11 Test the connection</li></ul>		

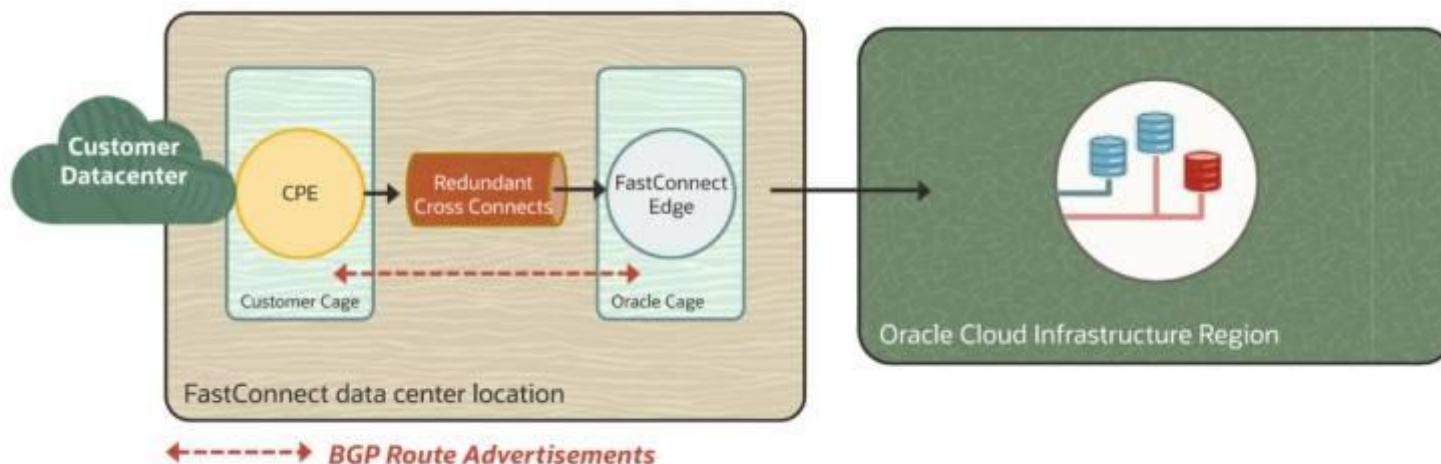
Oracle Cloud Infrastructure

# FastConnect Colocation with Oracle

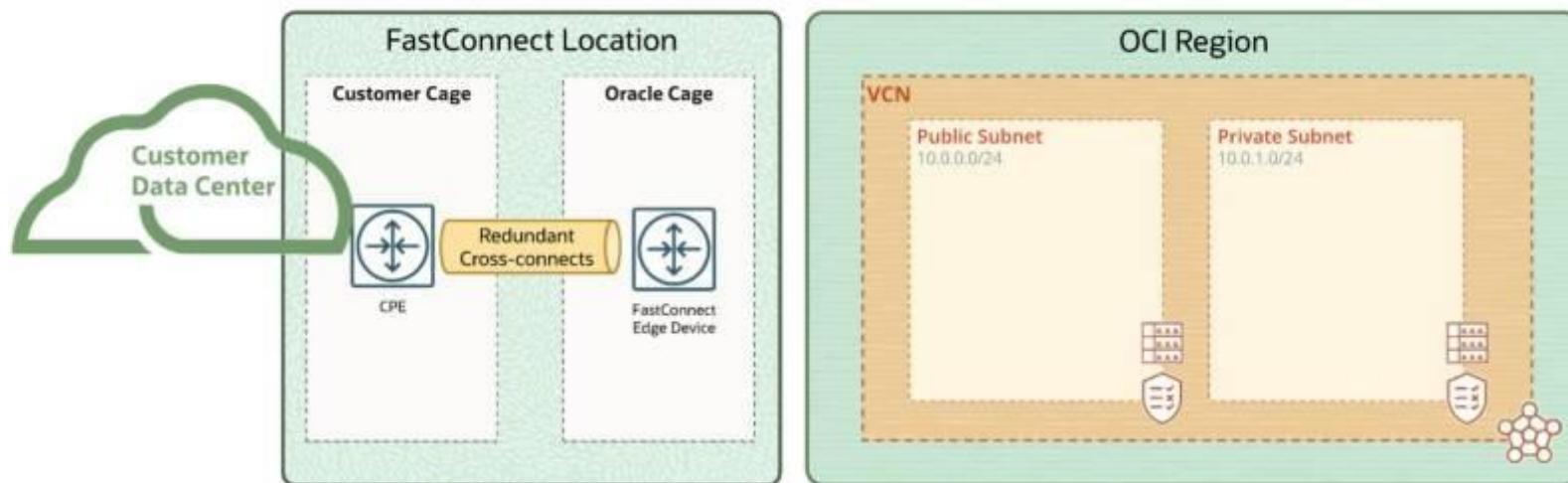
—  
**Networking: Connectivity**

## FastConnect: Colocation with Oracle

- Establish connectivity from your network equipment in the colocation to OCI services provisioned in that colocation facility
- Oracle provides an LOA.
- Provide the LOA to data center provider.
- Direct cross-connect is established.
- Suitable if you already have presence at an Oracle FastConnect location



## FastConnect Direct: Colocation



# Setup: FastConnect Colocation with Oracle

Colocation setup			
Set up initial components	On-Premises Edge	FastConnect location	Oracle Console
			<ol style="list-style-type: none"><li>1 Set up DRG (private virtual circuit only)</li><li>2 Set up cross-connect group (LAG) and cross-connect</li></ol>
Set up physical fiber cable		<ol style="list-style-type: none"><li>3 Submit LOA and request cabling</li><li>4 Check light levels for each cross-connect</li><li>5 Confirm interfaces are up for each cross-connect</li></ol>	
Activate and create other components			<ol style="list-style-type: none"><li>6 Activate each cross-connect</li><li>7 Set up virtual circuit</li></ol>
Configure your edge and validate connection	<ol style="list-style-type: none"><li>8 Configure your edge</li><li>9 Ping the Oracle BGP IP address across cross-connect group</li><li>10 Confirm BGP session to Oracle is established</li><li>11 Test the connection</li></ol>		

## Oracle Cloud Infrastructure

# Demo: FastConnect

---

### Networking – Connectivity

## Oracle Cloud Infrastructure

# FastConnect Redundancy Best Practices

### Networking - Connectivity

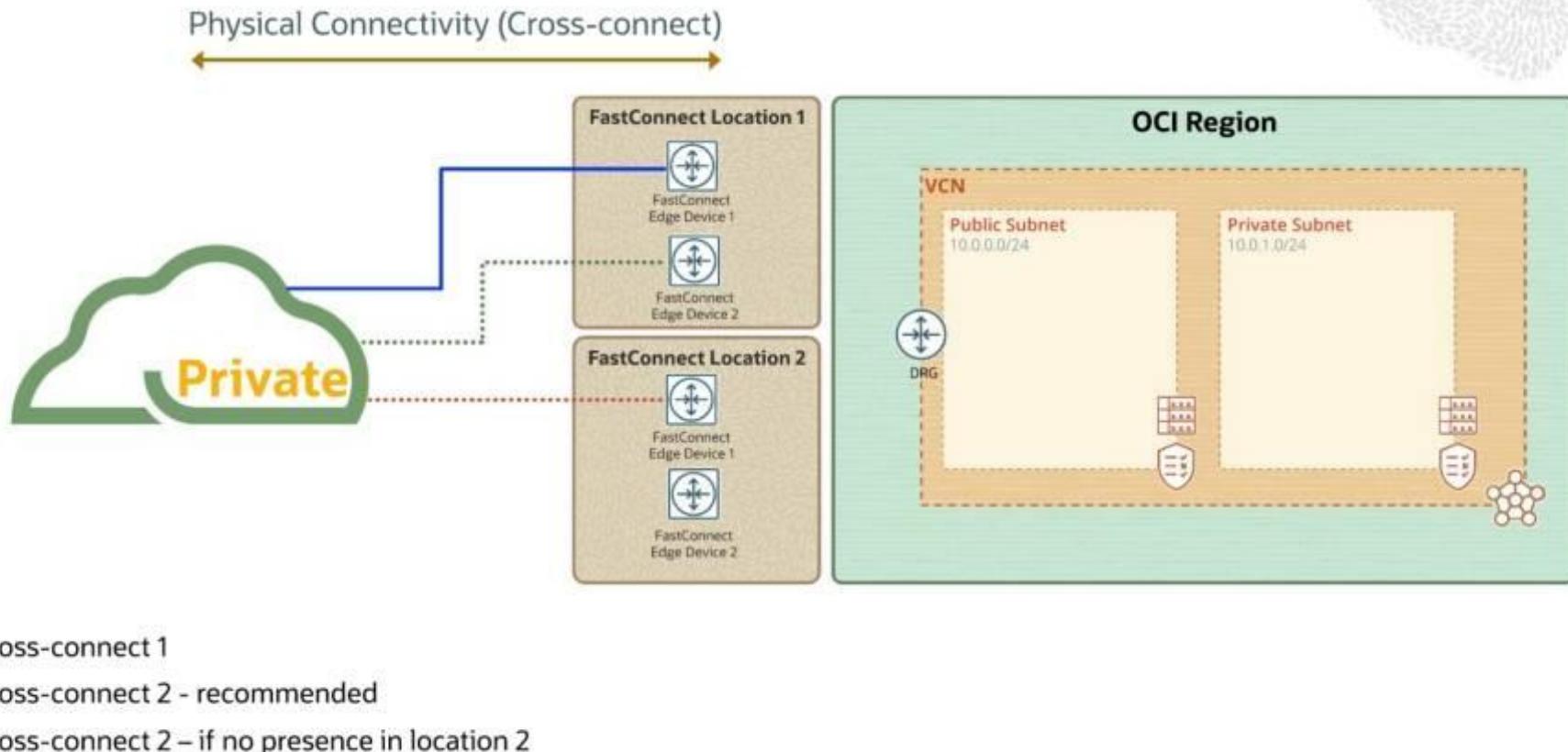
# FastConnect Redundancy Best Practices

---

For FastConnect redundancy, Oracle provides:

- Multiple partners for each region
- Multiple physical connections between each Oracle partner and Oracle (for a given region)
- At least one FastConnect location for each region
- A minimum of two FastConnect routers in each FastConnect location

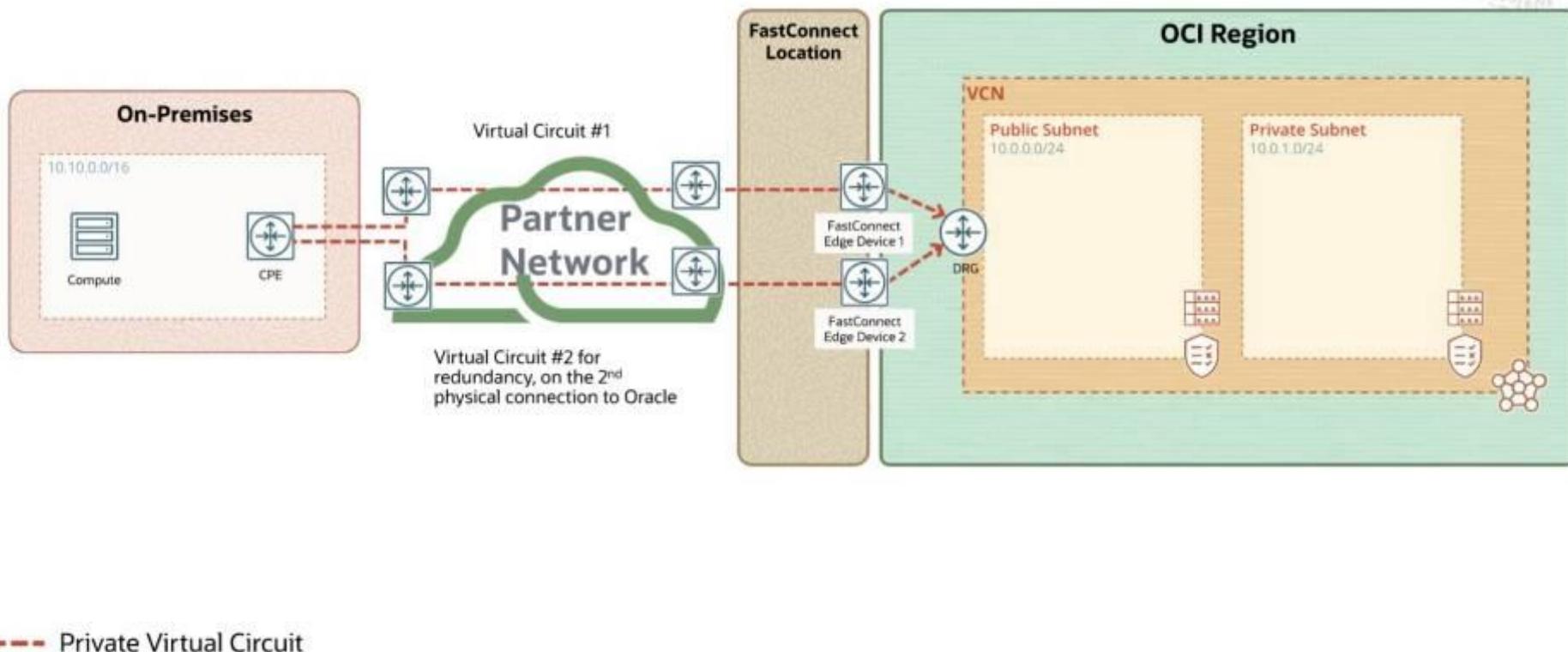
## FastConnect Location Physical Overview



## Oracle Partner

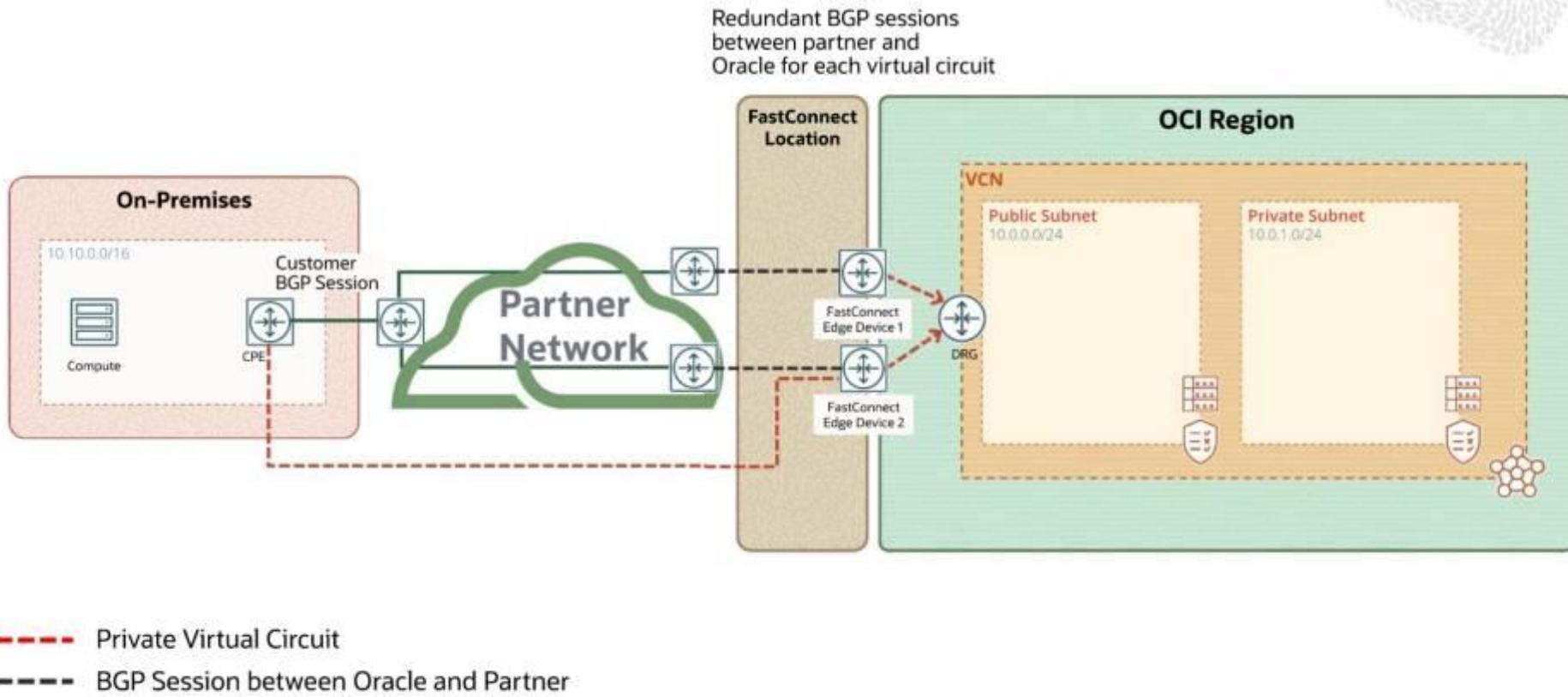
- Oracle handles:
  - Redundancy of physical connection between partner and Oracle
  - Redundancy of routers in FastConnect locations
- Customer handles:
  - Redundancy of physical connection between existing network and Oracle partner

## FastConnect Partner: Layer 2 Connections





## FastConnect Partner: Layer 3 Connections

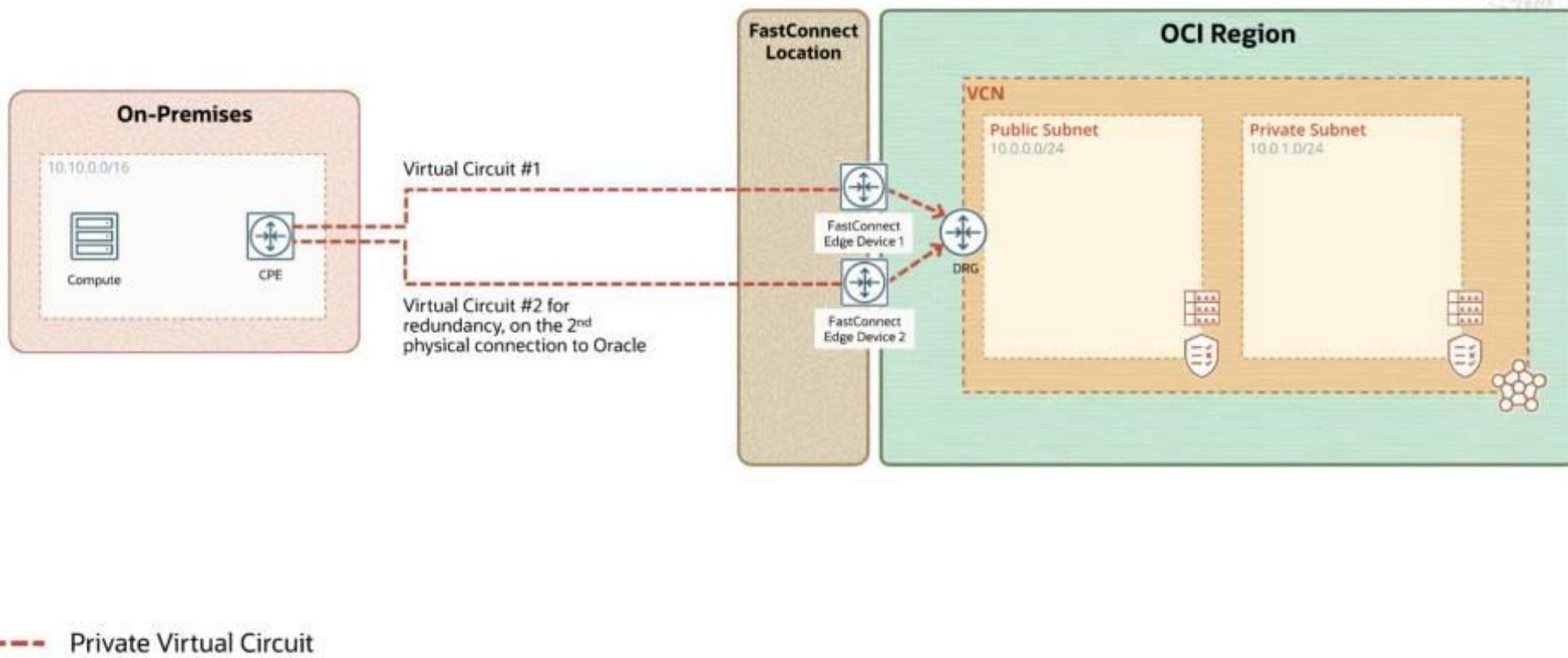


## Third-Party Provider or Colocation with Oracle

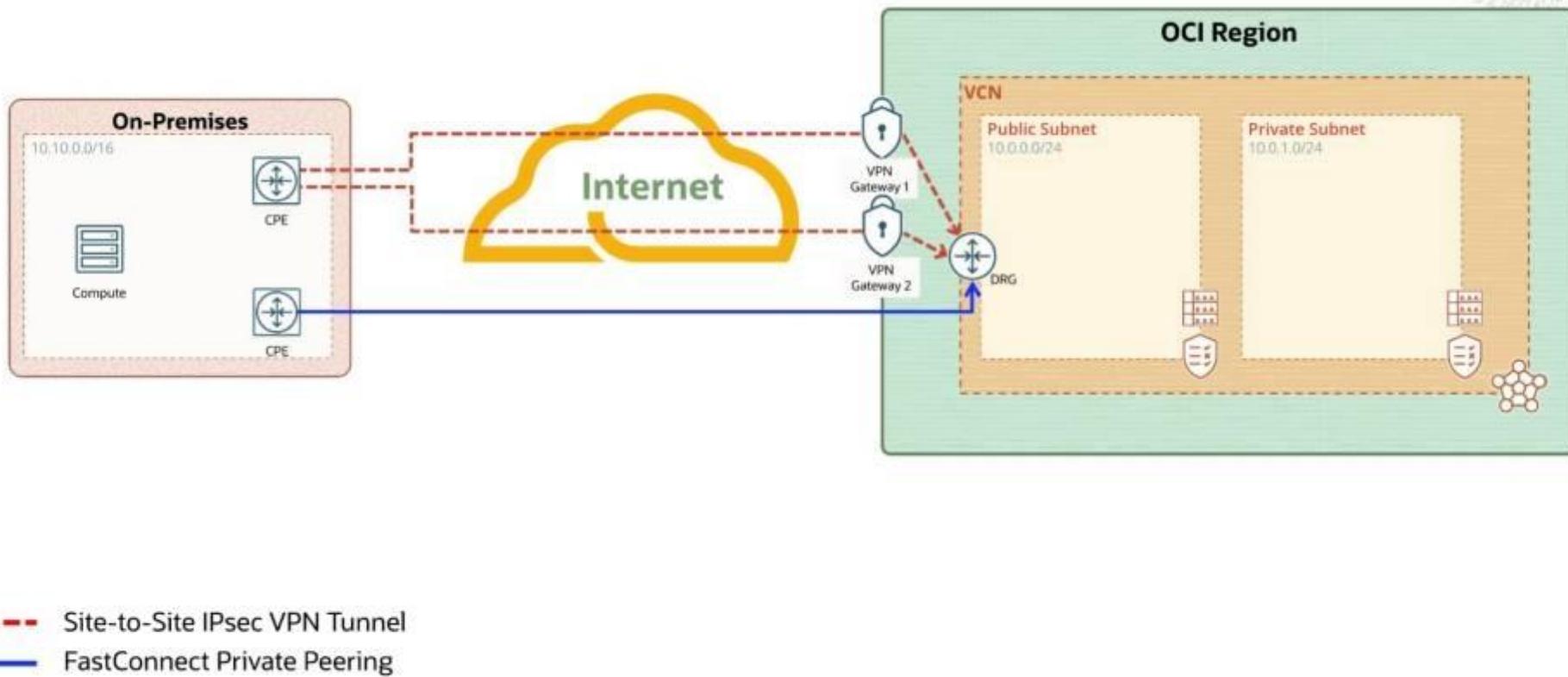
- Oracle handles:
  - Redundancy of routers in FastConnect locations
- Customer handles:
  - Redundancy of physical connection between existing network and Oracle



## FastConnect Direct: Colocation or Third-Party Provider



## FastConnect with Site-to-Site VPN Backup



# Expert Tip

---

# Networking - Load Balancer

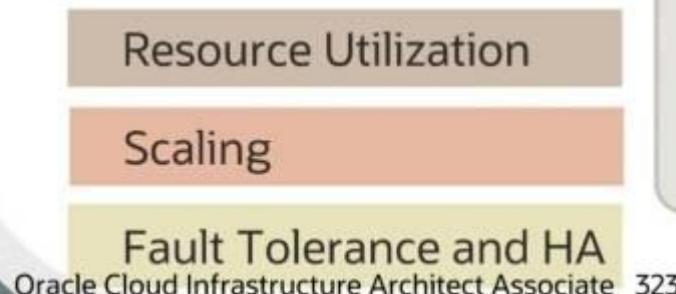
# Oracle Cloud Infrastructure Load Balancer

## Networking – Load Balancer

# OCI Load Balancing Service



- Sits between the client and the back end
- Enables public and private load balancer options
- Supported protocols include HTTP, HTTP/2, TCP, and HTTPS
- Supports advanced features such as session persistence and path-based routing
- Supports SSL termination, point-to-point SSL, and SSL tunneling



# Load Balancer Concepts



# OCI Load Balancer Shapes



- › Flexible Shapes
- › Define a minimum and maximum bandwidth (10 - 8000 Mbps)
  - Minimum bandwidth provides instant readiness for load.
  - Maximum bandwidth allows control of maximum cost.

Choose the minimum bandwidth ⓘ

10 Mbps

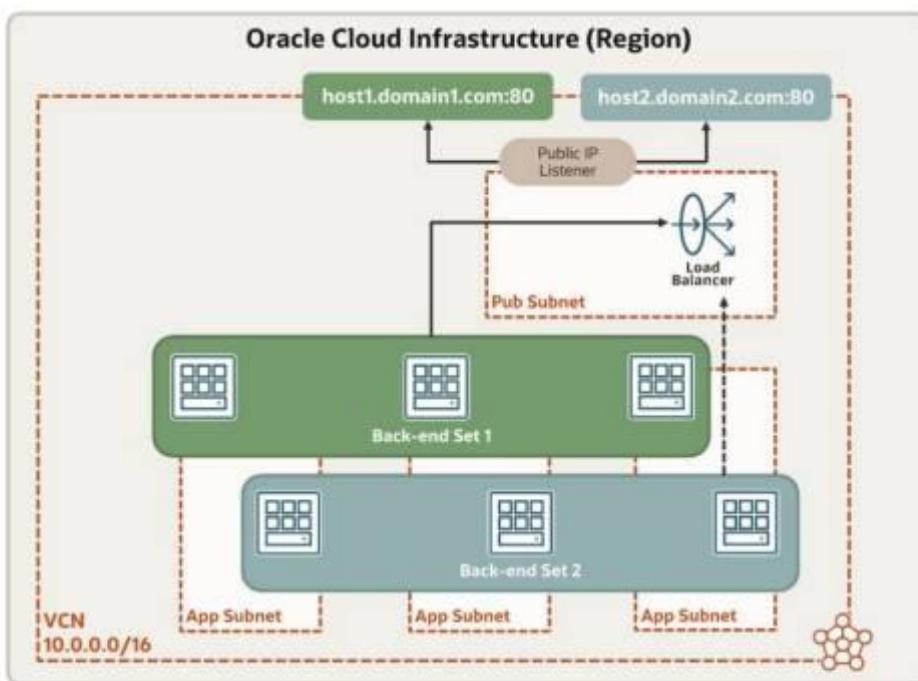
10 Mbps 8000 Mbps

Choose the maximum bandwidth Optional ⓘ

10 Mbps

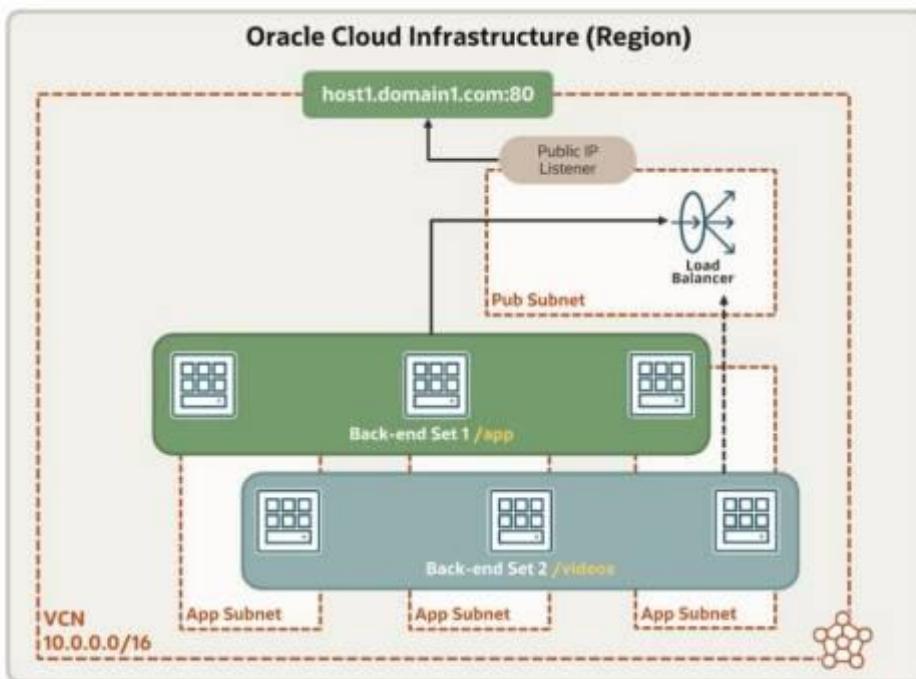
10 Mbps 8000 Mbps

# Content-Based Routing: Host Based



Multiple websites using a single load balancer

# Content-Based Routing: Path Based



Optimize resource utilization by routing to independent back-end sets based on the URI paths.

Oracle Cloud Infrastructure

# Load Balancer Policies

**Networking – Load Balancer**

# Load Balancing Policies



Round Robin



Least  
Connections



IP Hash



Control traffic distribution to back-end servers

# Round Robin

- Default load balancer policy
- Distributes incoming traffic sequentially to each server in a back-end set list
- Works best when:
  - ✓ Backend servers have similar capacity
  - ✓ Processing load required by each request does not vary significantly



# Least Connections

- Route incoming nonsticky request traffic to the back-end server with fewest active connection
- Help maintain equal distribution of active connections
- Assign a weight to each back-end server



# IP Hash

- Uses incoming request's source IP address as a hashing key
- Routes nonsticky traffic to the same back-end server
- Routes request from the same client to the same back-end server



# Load Balancing Policies

Load balancer policy decisions apply differently for:

- TCP load balancer
- Cookie-based session persistent HTTP requests (sticky requests)
- Nonsticky HTTP requests



Oracle Cloud Infrastructure

# Load Balancer Health Checks

**Networking – Load Balancer**

# Health Check

- › Confirms availability of back-end servers
- › Continuously monitor back-end servers
- › Configure TCP-level or HTTP-level
- › Configure your health check protocol to match your application or service
- › Activated for:
  - Back end
  - Back-end Set
  - Overall Load Balancer



# Health Check



## Specify health check policy

A health check is a test to confirm the availability of backend servers. A health check can be a request or a connection attempt. Based on a time interval you specify, the load balancer applies the health check policy to continuously monitor backend servers.

### Protocol

HTTP

Ensure your backend set's health check protocol matches the listener protocol.

### Port Optional

80

Ensure your backend set's health check port number matches the backend's port number.

Force plaintext health checks (i)

### Interval in milliseconds Optional

10000

### Timeout in milliseconds Optional

3000

A minimum value of 3 seconds is recommended, otherwise the health check might fail.

### Number of retries Optional

3

### Status code Optional

200

### URL path (URI)

/

### Response body regex Optional

# Oracle Cloud Infrastructure Public Load Balancers

---

## Networking – Load Balancer

# Public Load Balancer



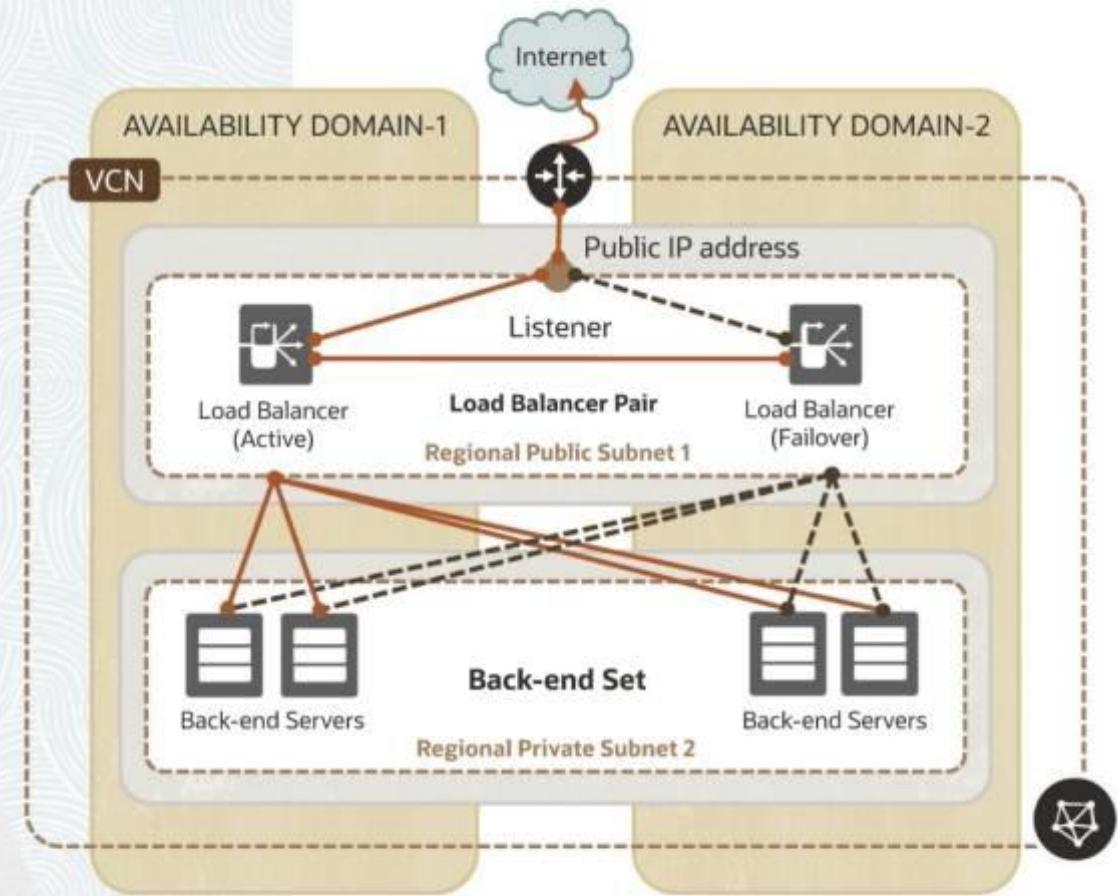
- › Has a public IP address
- › Accepts traffic from the Internet
- › Regional
- › For a multi-AD region, a public load balancer requires either a regional subnet or two availability domain-specific subnets.
- › Primary load balancer and a standby load balancer

# Public Load Balancer

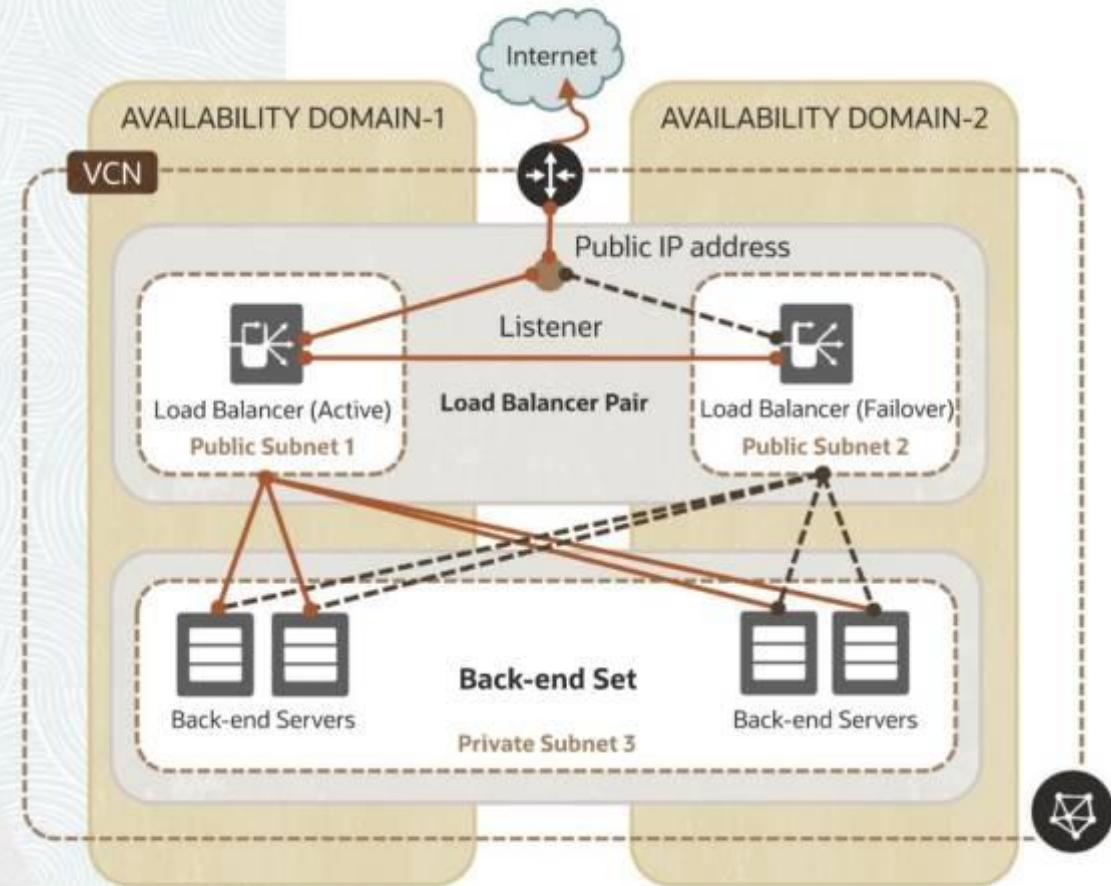


- › The Load Balancing service supports AD failover in the event of an AD outage in an OCI multi-AD region.
- › A floating Public IP is attached to the primary load balancer.
- › The service treats the two load balancers as equivalent, and you cannot denote one as "primary."

# Public Load Balancer (Regional Subnets)



# Public Load Balancer (AD-Specific Subnets)



Oracle Cloud Infrastructure

# Demo: Public Load Balancer

—  
**Networking – Load Balancer**

Oracle Cloud Infrastructure

# Private Load Balancers

## Networking – Load Balancer

# Private Load Balancer



- Assigned a private IP address that serves as an entry point for incoming traffic.
- Requires only one subnet to host both the primary and standby load balancers
- Accessible only from within the VCN
- The assigned floating private IP address is local to the host subnet.
- The primary and standby load balancers each require an extra private IP address from that subnet.



Oracle Cloud Infrastructure

# Demo: Private Load Balancer

—  
**Networking – Load Balancer**

# Oracle Cloud Infrastructure

## Network Load Balancer

---

### Networking – Load Balancer

# Network Load Balancer

- Operates at the connection level
- Provides the benefits of source and destination IP addresses, and port preservation
- Designed to handle volatile traffic patterns
- Offers high throughput while maintaining ultra low latency
- No bandwidth configuration requirement

# Network Load Balancer

- Ideal load balancing solution for latency-sensitive workloads
- Load Balancing Policy:
  - 5-Tuple Hash  
(source IP and port, destination IP and port, protocol)
  - 3-Tuple Hash  
(source IP, destination IP, protocol)
  - 2-Tuple Hash  
(source IP/destination IP )

Oracle Cloud Infrastructure

# Demo: Network Load Balancer

—  
**Networking – Load Balancer**

Oracle Cloud Infrastructure

# Web Application Acceleration Overview

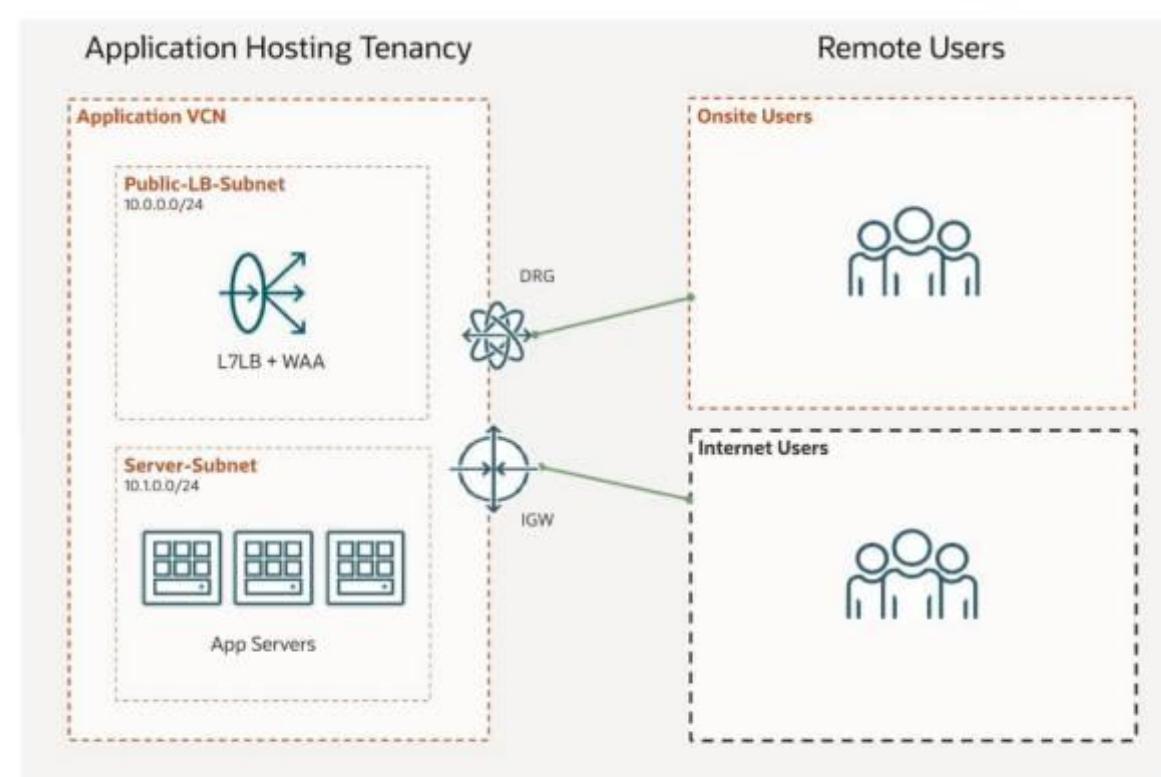
## Networking – Load Balancer

# Web Application Acceleration: Overview

## Anticipated outcomes:

Improve customer experience

Reduce application latency and system load



# Use Cases

**Scenario 1: Improve application performance and decrease server load**

Action: Leverage WAA caching

**Scenario 2: Decrease network load and further reduce latency**

Action: Utilize WAA compression

Oracle Cloud Infrastructure

# Web Application Acceleration Concepts

## Networking – Load Balancer

# Web Application Acceleration



Works with Layer 7 http/https protocols only

Only HEAD and GET requests are cached.

Only responses that return HTTP status code 200 are cached.

Cached content might not stay current with content on the back-end servers until the cache expires or is purged.

# Web Application Acceleration

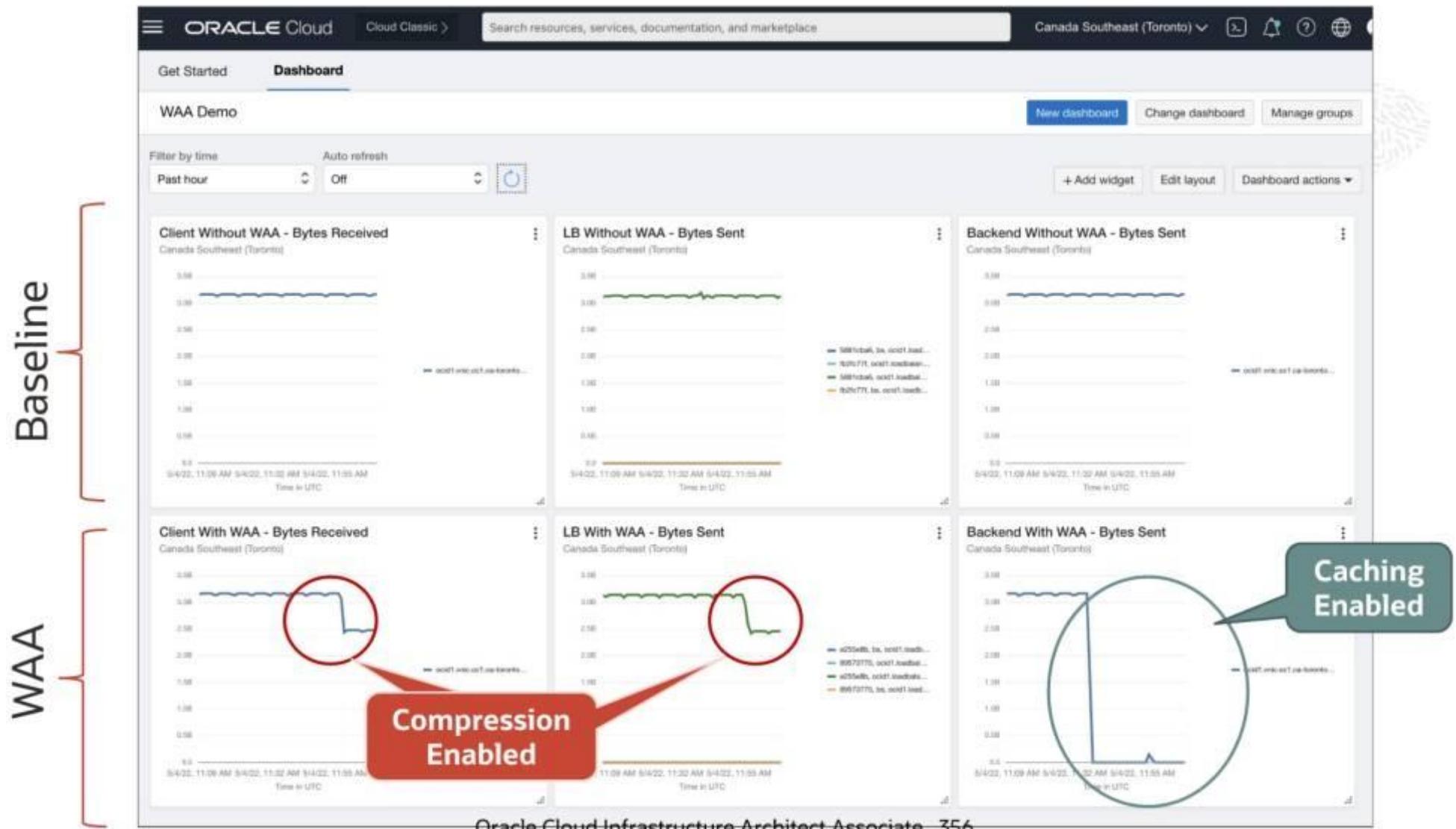


Content is cached until it expires or is purged even if the file is removed from the back-end server.

The maximum size of the cache is 100 MB.

Responses that return the Set-Cookie header are not cached.

Oracle recommends you do not cache dynamic pages because they can leak information.



Oracle Cloud Infrastructure

# Demo: Web Application Acceleration

—  
**Networking – Load Balancer**

