

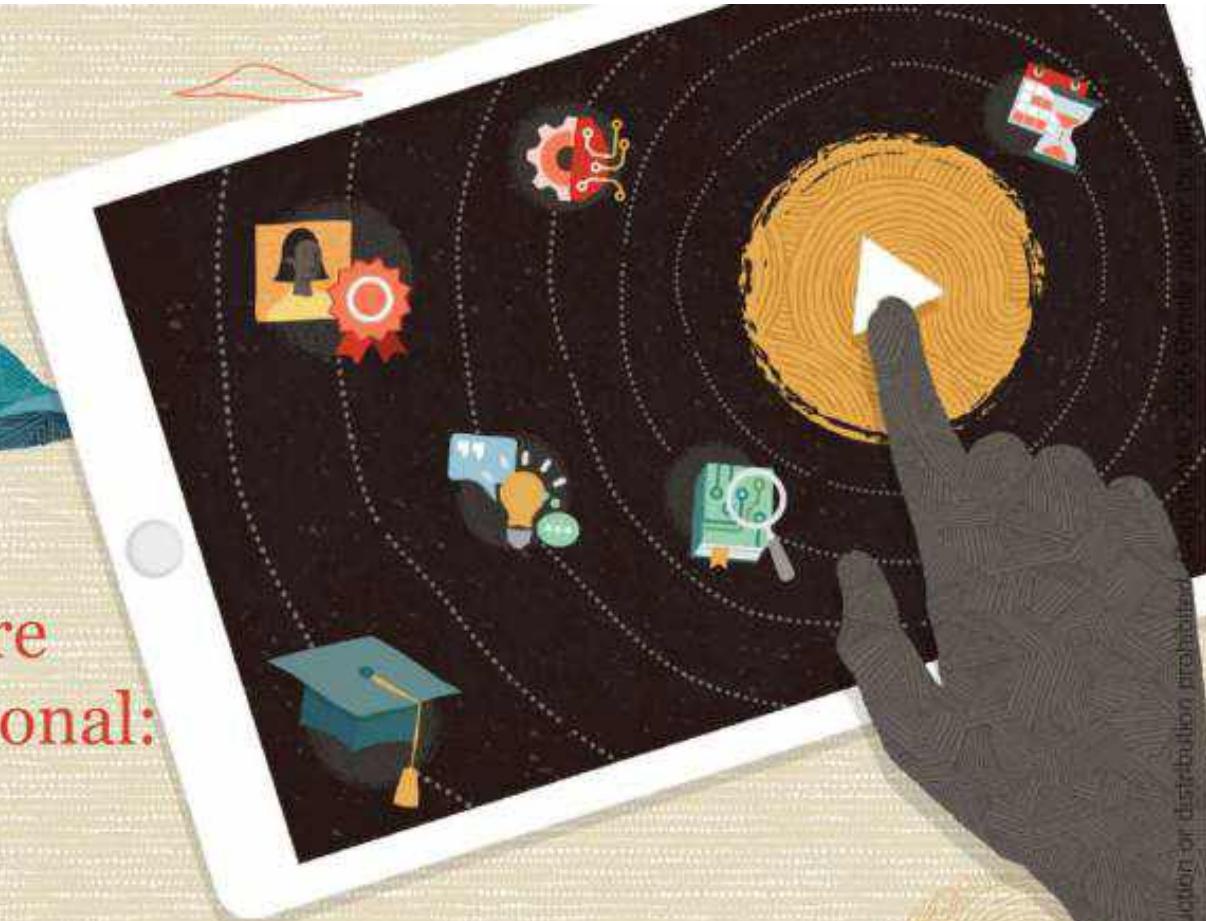


# Oracle Cloud Infrastructure Cloud Operations Professional: Hands-on Workshop

Student Guide – Volume I

D1111263GC10

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

1003042025

## Table of Contents

<b>Module 01: Course Overview</b>	<b>11</b>
Oracle Cloud Infrastructure Cloud Operations Professional	12
Day 0: Tenancy Administration	15
Day 1: Environment Deployment	16
Day 2: Scaling, Optimization, and Business Continuity	
<b>Module 02: Identity and Access Management Overview</b>	<b>18</b>
Introduction	19
What is OCI IAM?	20
OCI IAM: Authentication (AuthN)	22
OCI IAM: Authorization (AuthZ)	24
OCI IAM Components	26
OCI IAM Identity Domains	31
What are OCI IAM identity domains?	32
Identity Domains	33
Identity Domains: Use Cases	34
Identity Domains: Identity Lifecycle Management	35
OCI IAM with Identity Domains	40
Identity Domain Types	41
Identity Domain Types	42
<b>Module 03: Identity and Access Management Basics</b>	<b>47</b>
Managing OCI IAM Identity Domains	48
Default Identity Domain	50
Default Domain	51
Dos and Don'ts for the Administrator Users	53
Creating Identity Domains	54
Why do we need multiple identity domains?	55
Creating Identity Domains	56
Demo: Creating Identity Domains	58

Creating Identity Domains	59
Demo: Creating Groups	60
Creating Groups	61
Managing Groups	63
Groups	64
Default Groups in Identity Domains	66
Demo: Creating Users	67
Creating Groups	68
Creating Users	69
Managing Users	70
Stages of the IAM User Life Cycle	71
User Lifecycle Management	72
Creating Groups	73
Understanding the Administrator Role	74
Administrator Roles: Key Points	75
Types of Administrator Roles	76
Assigning Administrative Roles	77
Policies	78
Policies	79
Subjects Clause	80
Actions Clause	83
Placement	85
Compartments	86
Compartment	87
Resource Compartments	89
Compartments Access	90
Interaction of Resources	91
Movement of Resources	92
Multiple Regions	93
Nested Compartments	94
Compartment Quotas	95

Scenario	96
Quota Syntax	97
Quota Examples	103
Types of Quota Policy Statement	104
Quota Examples	105
Budgets	106
Demo: Policies	107
Demo: Understanding Administrator Role	108
<b>Module 04: Identity and Access Management-Advanced</b>	<b>109</b>
Demo: Policy Inheritance and Attachment	110
Tenancy	111
Policy Inheritance and Attachment	112
Policy Inheritance	113
Policy Attachment	115
Conditional Policies	117
Conditions	120
Examples	122
Demo: Creating Users	123
Oracle Cloud Infrastructure (Region)	124
Enforce Least Privileged: Advanced Policies	125
Permissions	126
Example	127
Tag Based Access Control	131
Example	135
Demo: Dynamic Groups	137
Scenario: Dynamic Groups	138
Network Sources	139
Demo: Tag Based Access Control	143
Demo: Network Sources	144
Scenario	145

<b>Dynamic Groups</b>	<b>146</b>
Terms	147
Resource Principals Patterns	148
Infrastructure Principals	149
Stacked Principals	150
Ephemeral Principals	151
Dynamic Groups	152
Policies	154
<b>Module 05: Security Posture</b>	<b>155</b>
What is Cloud Security Posture Management?	156
Problem with Cloud Security	157
Cloud Security Posture Management (CSPM) capabilities	158
DevSecOps	159
Cloud Security Posture Management Outcomes	160
Cloud Security Posture Management Benefits	161
Cloud Guard Introduction	162
Cloud Guard	163
Supported Services	165
CIS OCI Foundations Benchmark	166
Reporting Region	167
Cloud Guard Concepts	168
Cloud Guard: Overview	169
Cloud Guard Concepts: Targets and Detectors	170
Cloud Guard Concepts: Detector Rules and Recipes	171
Cloud Guard Concepts: Problems and Responders	172
Cloud Guard Concepts: Responder Rules and Recipes	173
Cloud Guard Problems	174
Scenario: Public Bucket	175
Cloud Guard Concepts: Problems	176
Processing Reported Problems	177
Cloud Guard – Manage Detector Recipes	179

Detector Rules and Recipes	180
Configuration Detector Rules (Oracle-Managed)	181
Activity Detector Rules (Oracle-managed)	182
Compartment Inheritance	183
Cloud Guard Responder Recipes	184
Managing Responder Recipes	185
Managed Lists	187
Cloud Guard Notifications	189
Cloud Guard Notifications	190
Integration with Events and Notification Services	191
Security Zones and Security Advisor	192
Security Zones	193
Security Zone Concepts	195
Security Zone Policies	196
Security Advisor	197
<b>Module 06: Billing and Licensing</b>	<b>198</b>
Manage Cost with Budgets and Budget Alerts	199
Overview Course Big Picture	200
Module 8 Billing & Cost Management	201
Budgets	202
Understand Cost with Cost Analysis	206
Module 8 Billing & Cost Management	207
Cost Analysis	208
Calculate and Optimize Cost: Compute	224
Compute Pricing	225
Cost Optimization for Compute	238
Scaling	239
Autoscaling	240
Calculate and Optimize Cost: Block Storage	249
Block Storage Cost	250
Volume Performance Units (VPUs)	255

Auto-tuning	258
<b>Calculate and Optimize Cost: File Storage</b>	<b>260</b>
File Storage Cost	261
<b>Calculate and Optimize Cost: Object Storage</b>	<b>277</b>
Object Storage Tiers	278
Object Storage Costs	279
Optimize Cost: Object Storage	289
Life Cycle Management	290
Auto-Tiering	295
<b>Calculate and Optimize Cost: Networking</b>	<b>298</b>
Ingress & Egress Cost	299
VPN Connect vs FastConnect Pricing	301
FastConnect Pricing	302
<b>Software Licensing on OCI</b>	<b>303</b>
Licensing Models	304
Licensing Mobility through Software Assurance	311
<b>Module 07: Service Limits and Compartment Quotas</b>	<b>313</b>
<b>Governance &amp; Administration</b>	<b>314</b>
View and Manage Service Limits	315
Service Limit	316
View Service Limits and Usage	317
When You Reach a Service Limit	318
Demo	319
Request a Service Limit Increase	320
<b>Governance &amp; Administration</b>	<b>321</b>
Set Resource Caps with Quotas	322
Compartment Quotas	323
Types of Quota Policy Statements	324
Demo	325
Create a Quota Policy	326
<b>Cloud Advisor</b>	<b>327</b>

In this Lesson...	328
What Is Cloud Advisor?	329
How Cloud Advisor Works	330
Benefits of Using Cloud Advisor	331
Recommendation Categories & Statuses	332
Cloud Advisor Calculations	333
High Availability Recommendation Calculations	334
Performance Recommendation Calculations	335
Cost Management Recommendations	336
Recommendation Profiles	337
Recommendation Profile: Load Balancers	338
Recommendation Profile: Compute Instances	339
Organization Management	340
Organization Management: Overview	341
Why choose multitenancy approach?	342
Manage Multitenancy	343
Cost Reporting Integration	344
<b>Module 08: OCI Command Line Interface (CLI) and Software Development Kit (SDK)</b>	<b>345</b>
Interacting with OCI	346
Interacting with OCI	347
REST API	348
Cloud Console	350
Command Line Interface (CLI)	352
Software Development Kit (SDK)	354
OCI CLI Authentication	356
Recall	357
Authentication	358
API Key	361
Security Token	362
Instance and Resource Principles	364
Cloud Shell	365

OCI CLI Syntax	367
Recall	368
Syntax	370
Example	375
Option Types	380
Generating Examples	381
Advanced Examples	382

# Course Overview



Oracle Cloud Infrastructure  
**Cloud Operations Professional**

---





## Day 0

### Tenancy Administration

You've just received a tenancy and need to set it up

#### Identity and Access Management



#### Security Posture



#### Billing and Licensing



#### Governance and Administration



## Day 1

### Environment Deployment

You've just received an architecture and need to deploy it.

OCI Command Line Interface (CLI) and SDK



Resource & Configuration Management



Deploy a Monolithic Architecture



Secrets and Encryption

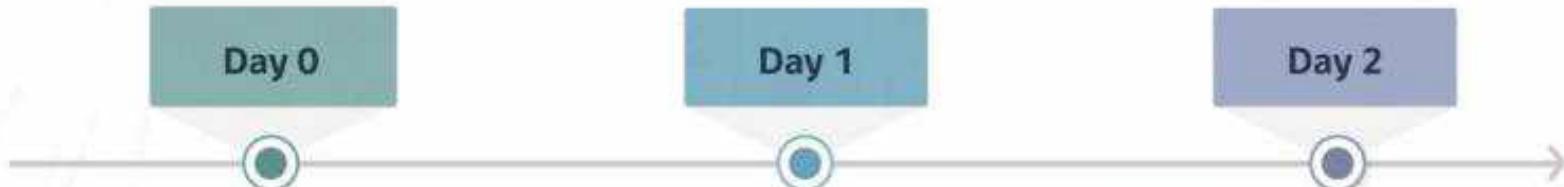


## *Prerequisites*

- Basic familiarity with core OCI services
- Hands-on experience with the Cloud Console
- Some familiarity with System Operations (SysOps)

## *Recommended Preparation*

- OCI Foundations Associate
- OCI Architect Associate





# Identity and Access Management Overview

## Oracle Cloud Infrastructure

# Introduction

### OCI Identity and Access Management (IAM)



# What is OCI IAM?

## Identity

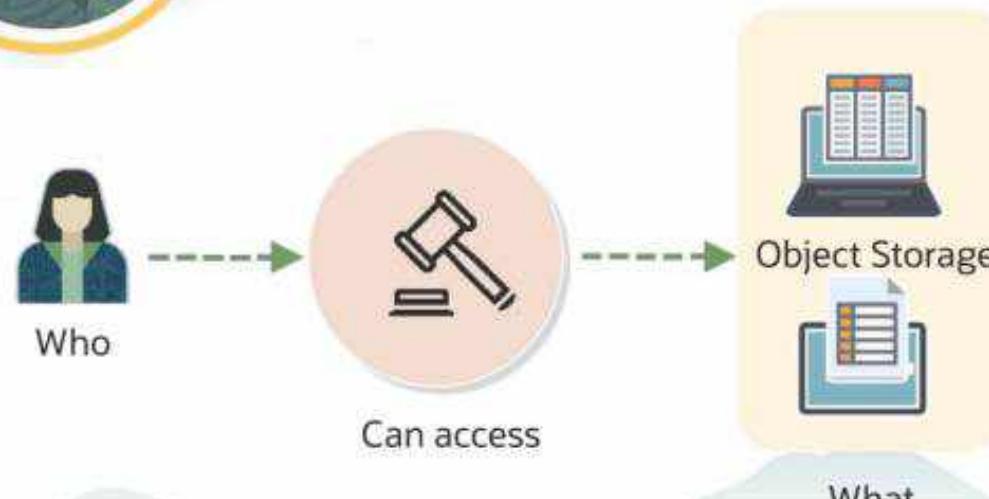
- Authentication
- Centralized identity lifecycle management
- Integration with existing identities and applications
- Secure and easy access

## Access Management

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



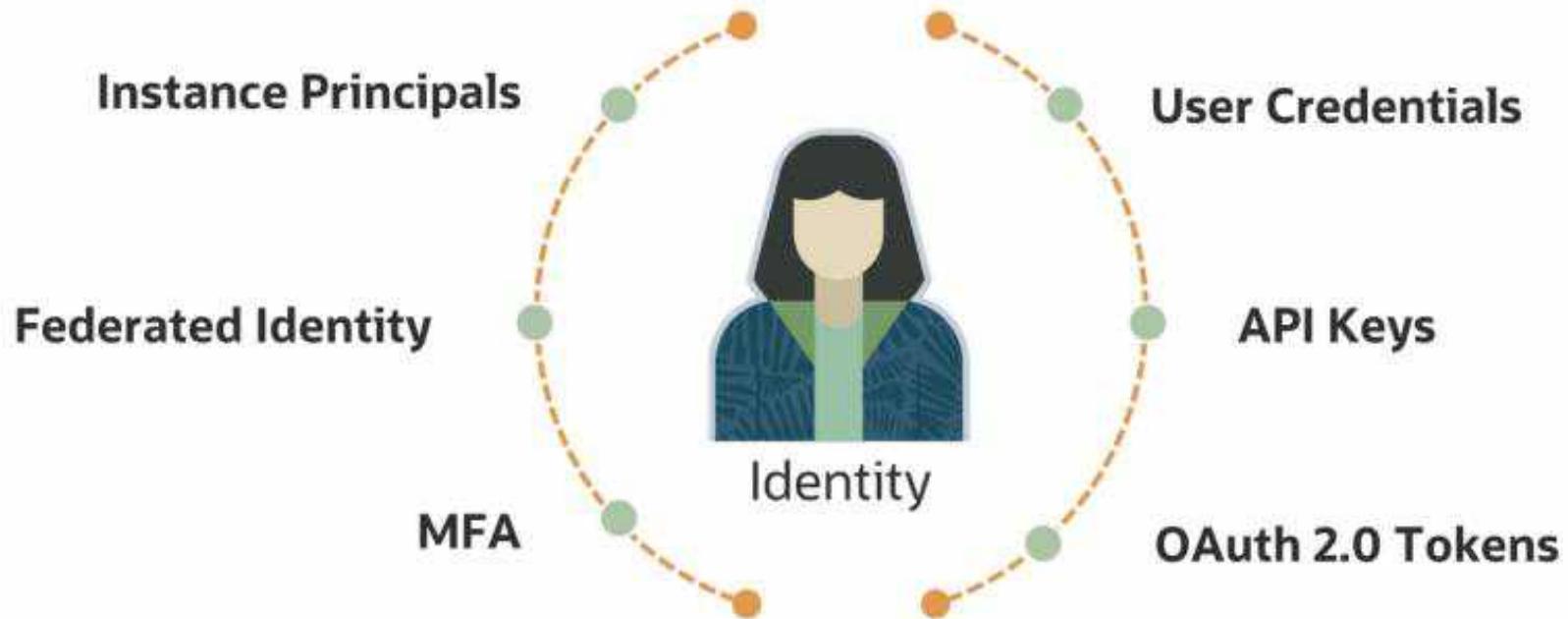
# What is OCI IAM?



# OCI IAM: Authentication (AuthN)



## OCI IAM: Authentication (AuthN)

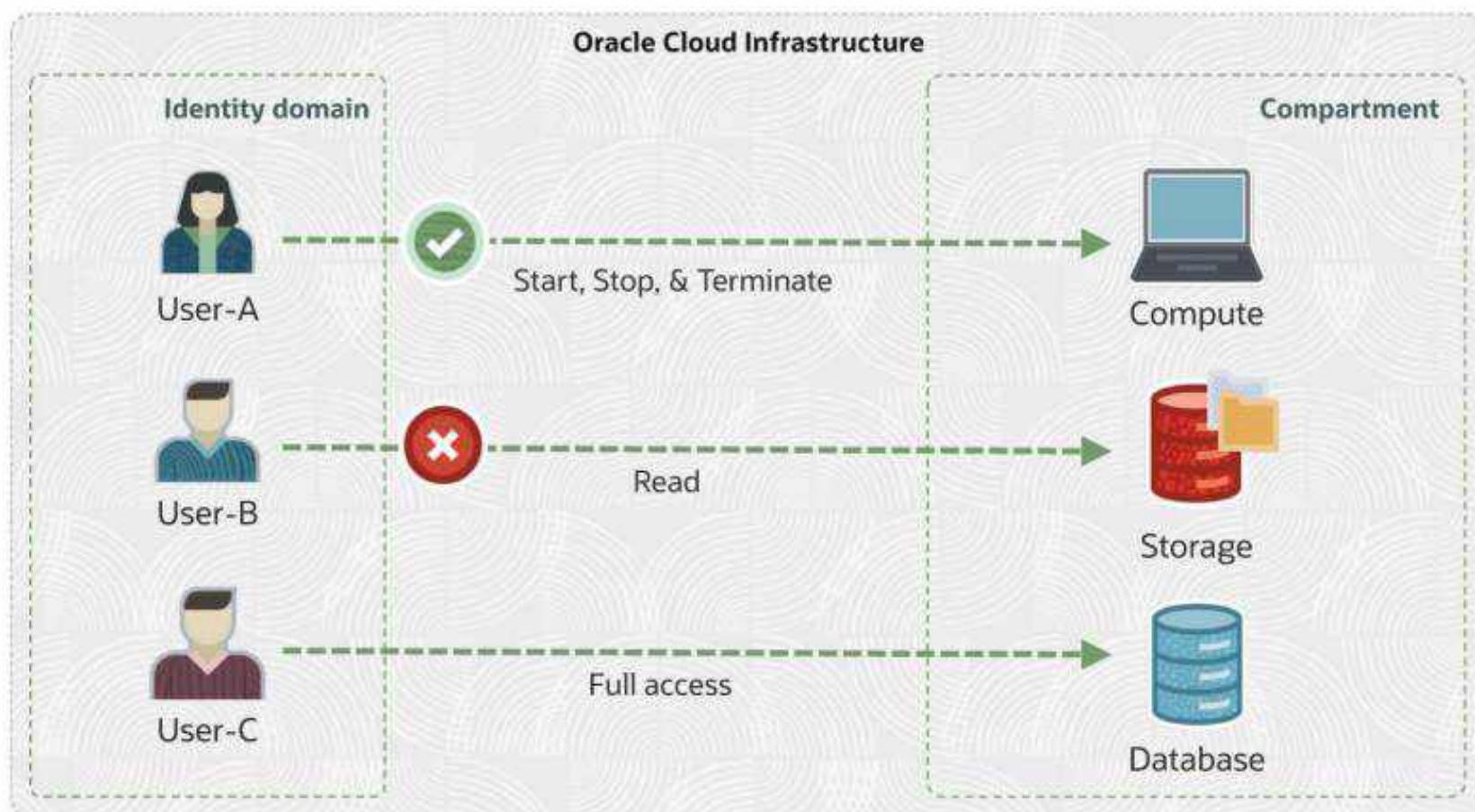


## OCI IAM: Authorization (AuthZ)

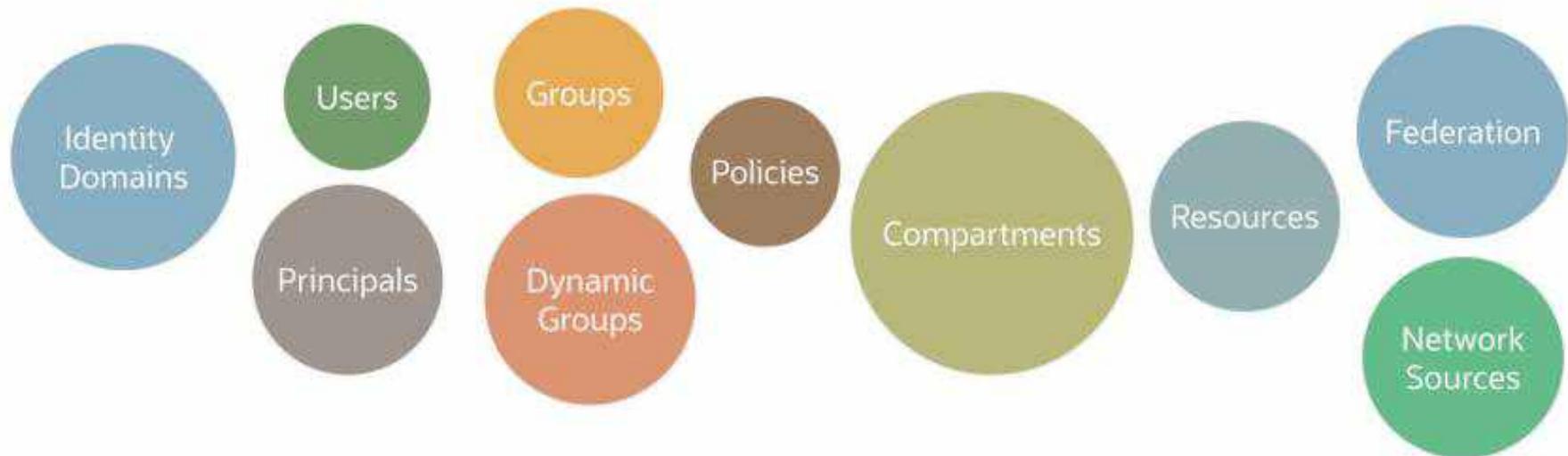
---



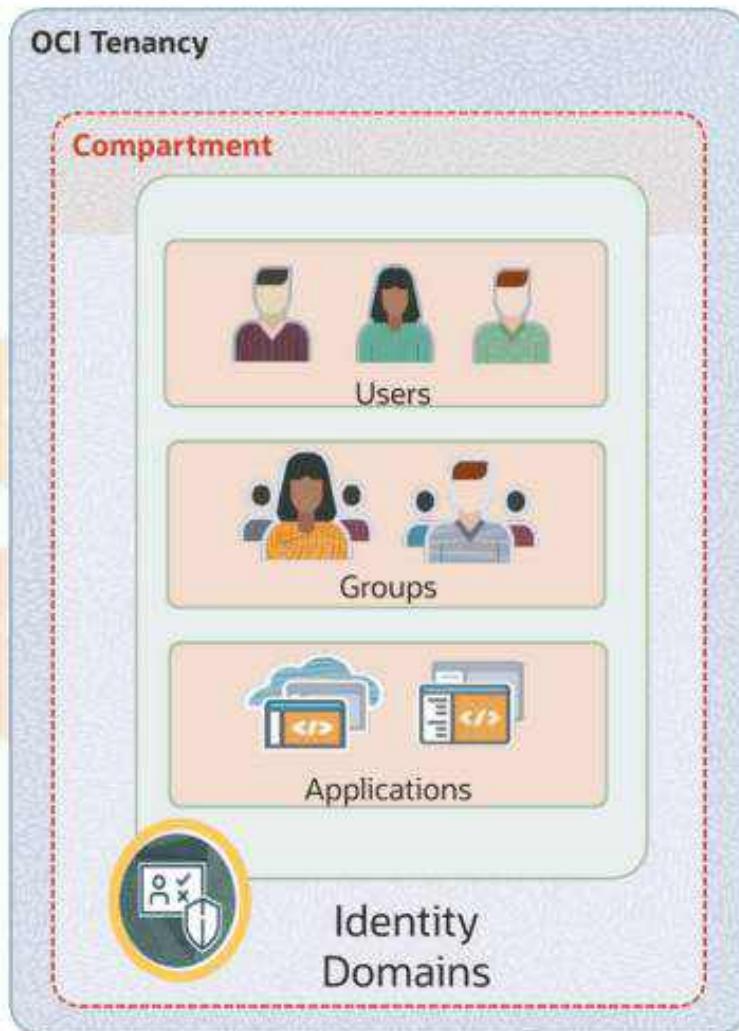
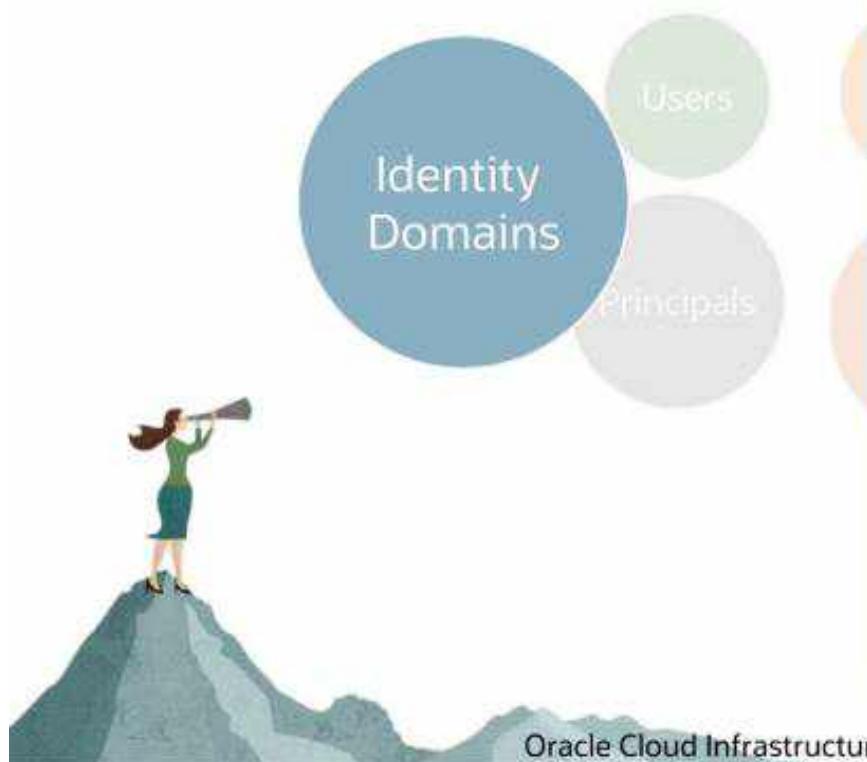
# OCI IAM: Authorization (AuthZ)



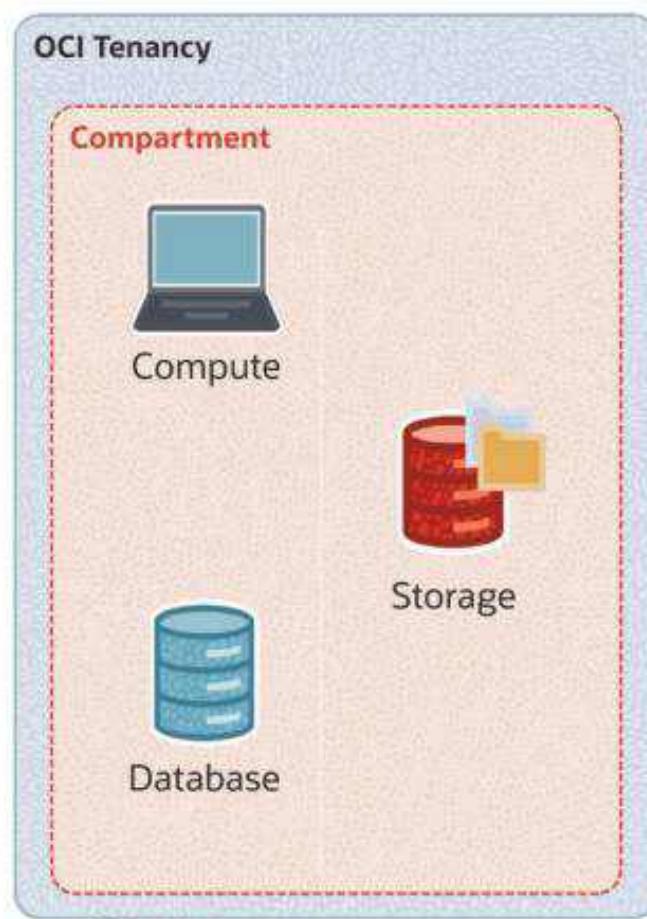
# OCI IAM Components



# OCI IAM Components



# OCI IAM Components



Policies

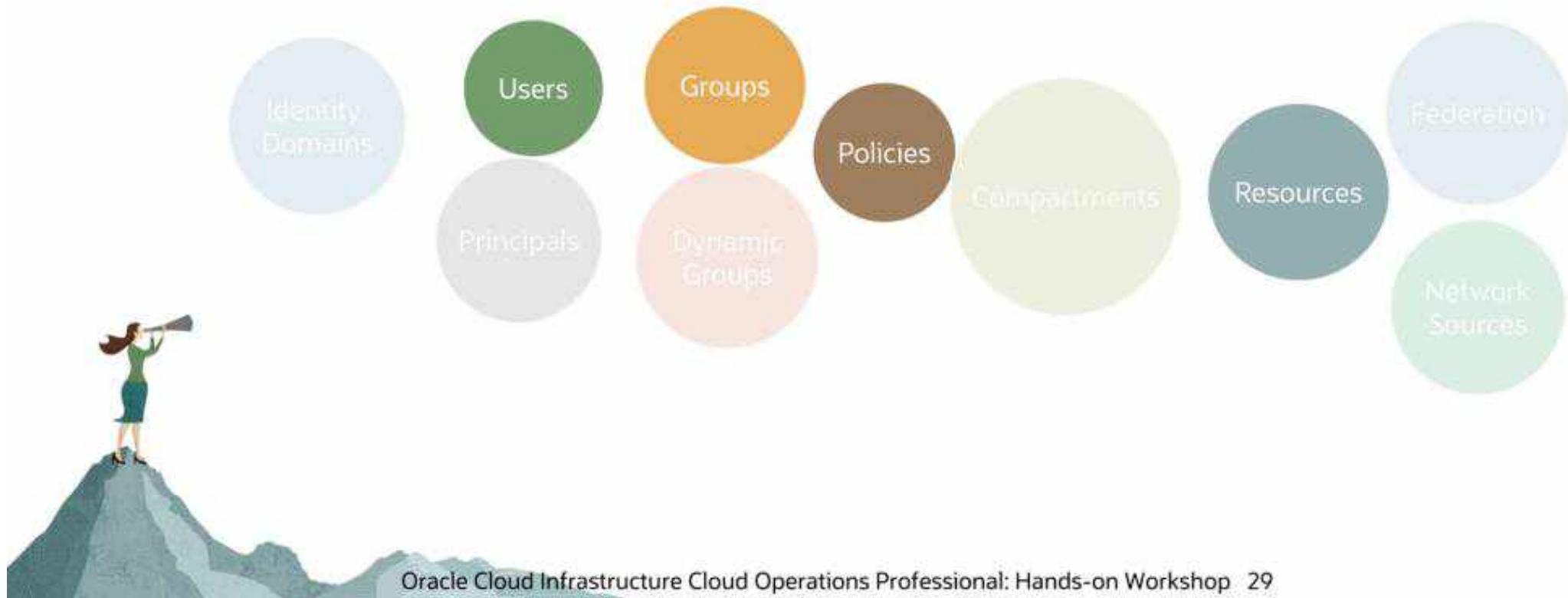
Compartments

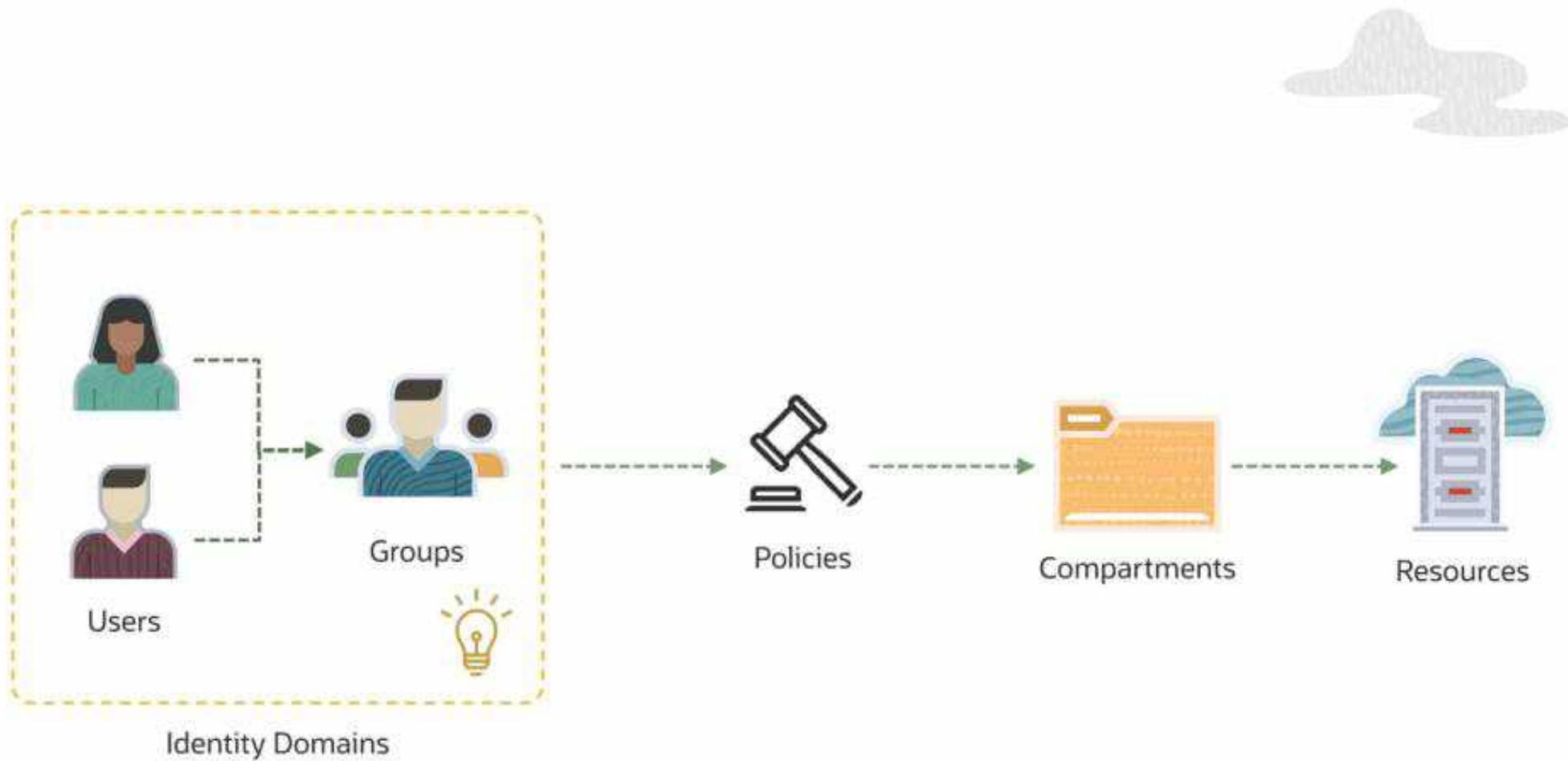
Resources

Federation  
Network Sources



# OCI IAM Components





Oracle Cloud Infrastructure

# OCI IAM Identity Domains

OCI Identity and Access Management (IAM)



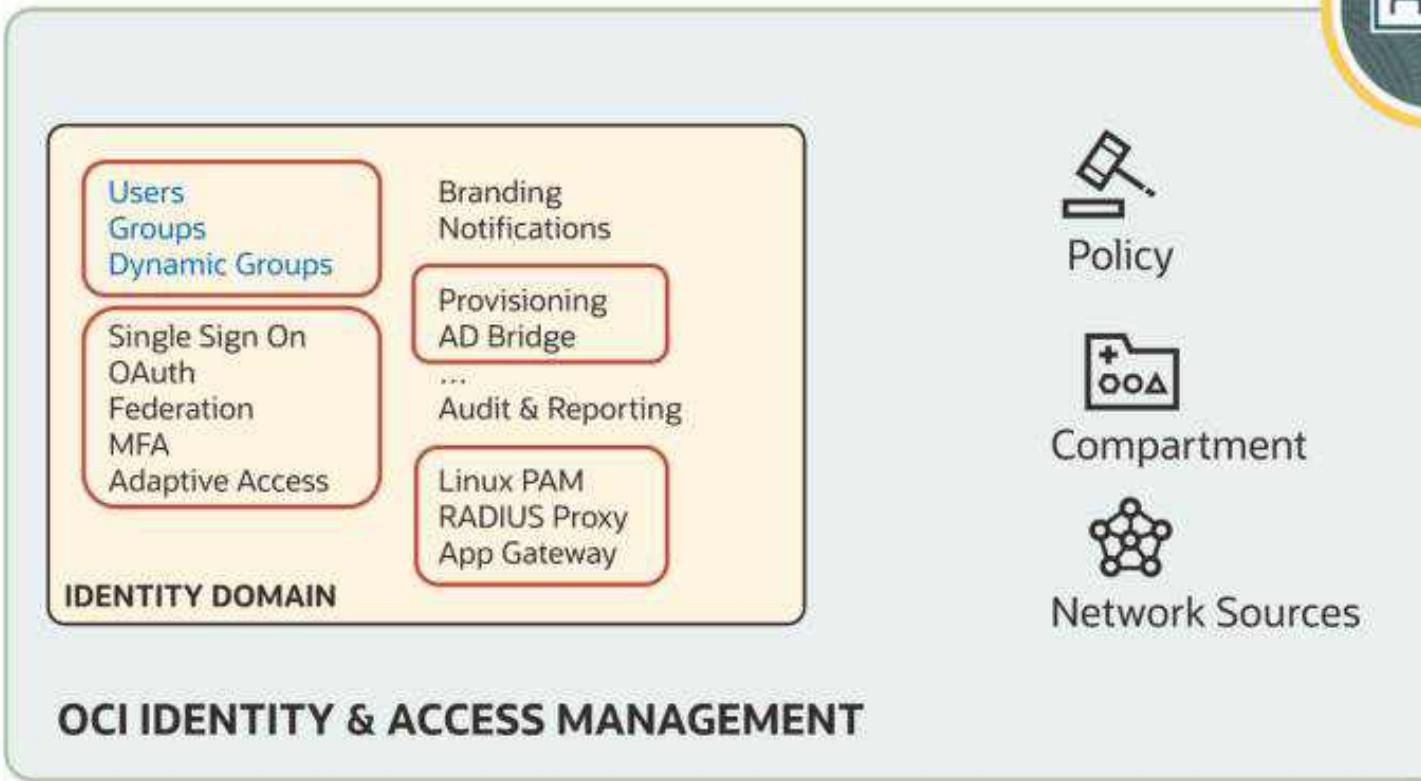
# What are OCI IAM identity domains?

A self-contained identity and access management service

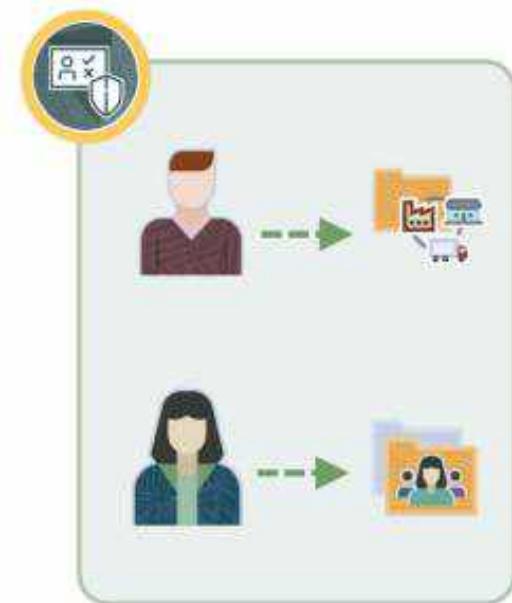
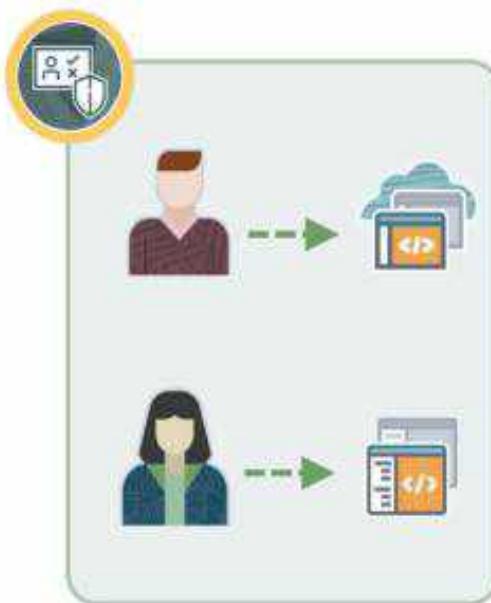
Act as a container to manage **users, roles, federation, SSO, MFA**, and so on

Provide secure application integration through SSO, SAML, and OAuth

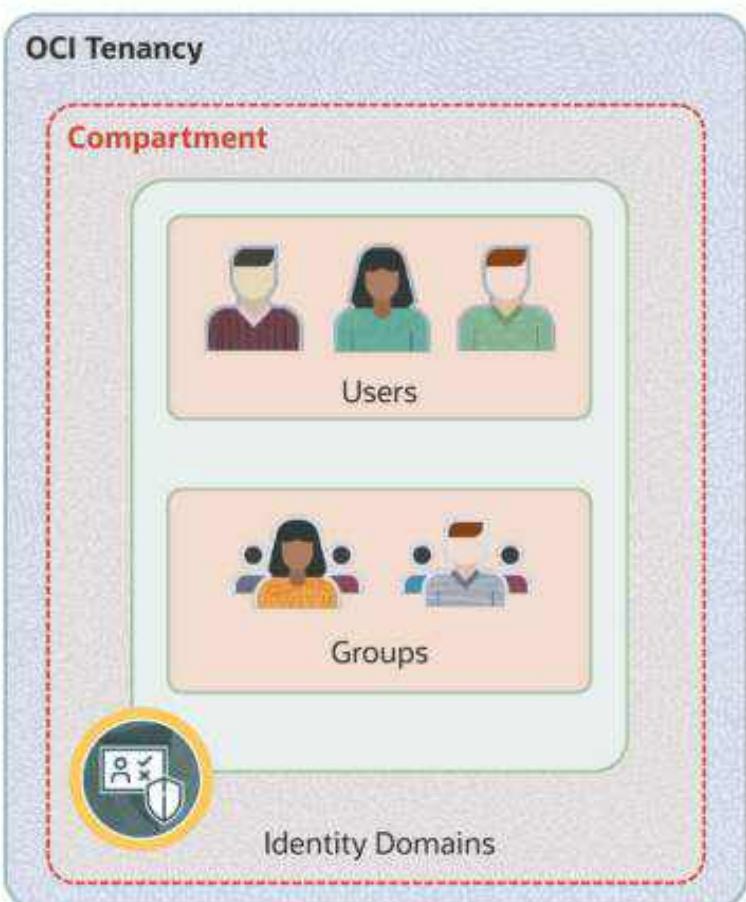
# Identity Domains



# Identity Domains: Use Cases

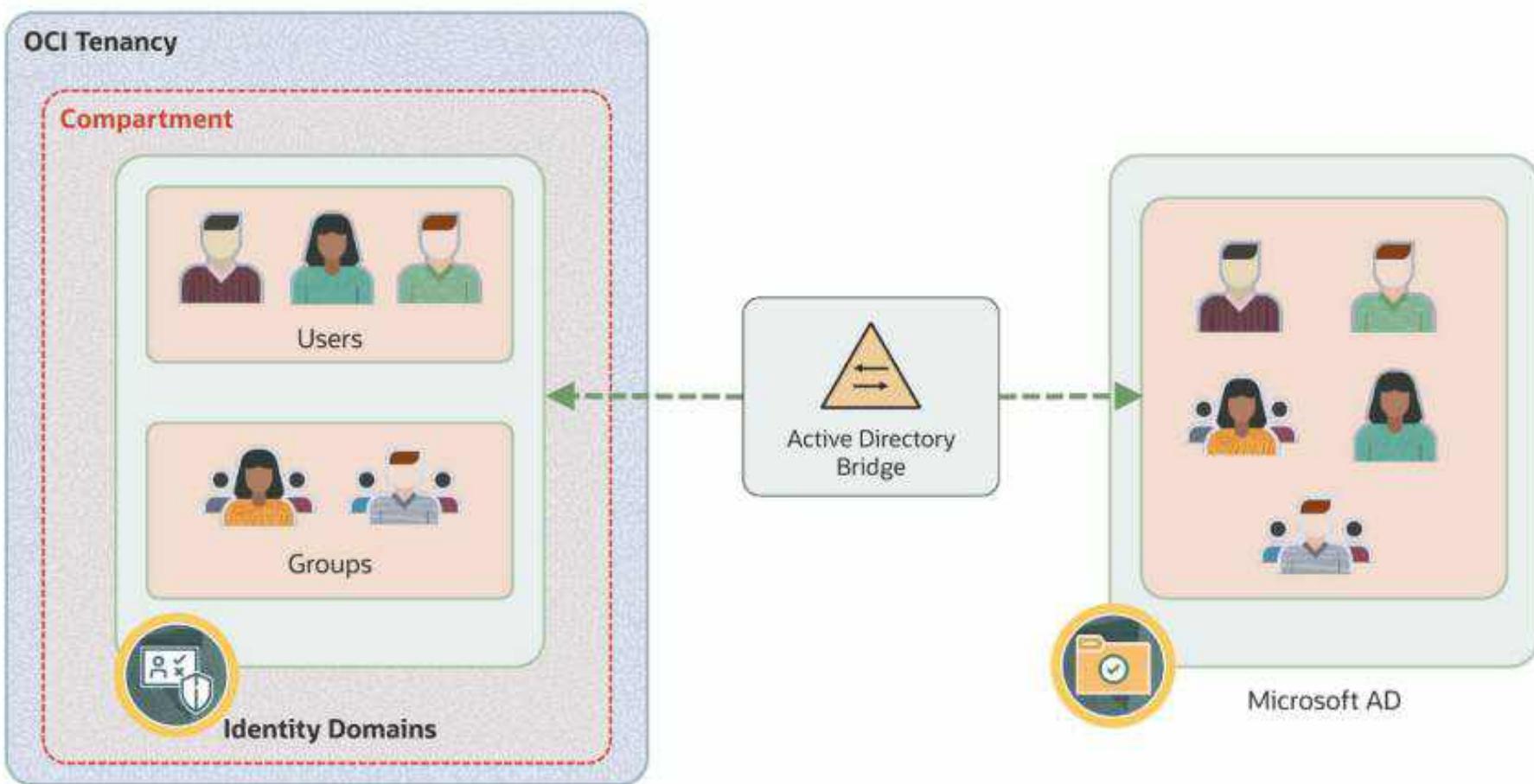


# Identity Domains: Identity Lifecycle Management

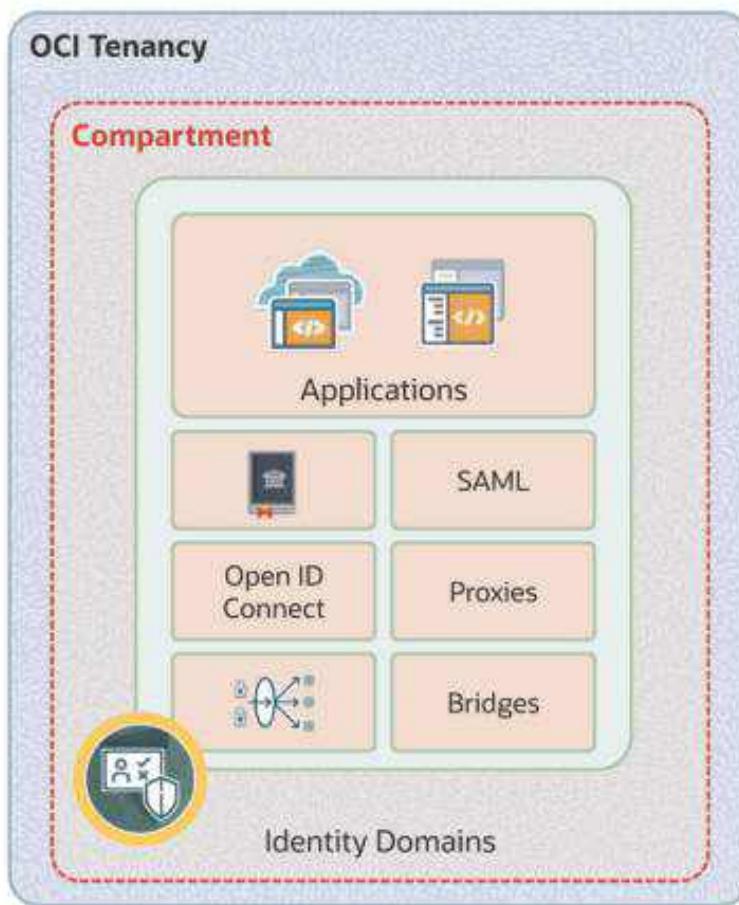


- Self-service registration
- Automated provisioning
- Sync with cloud/on-prem applications

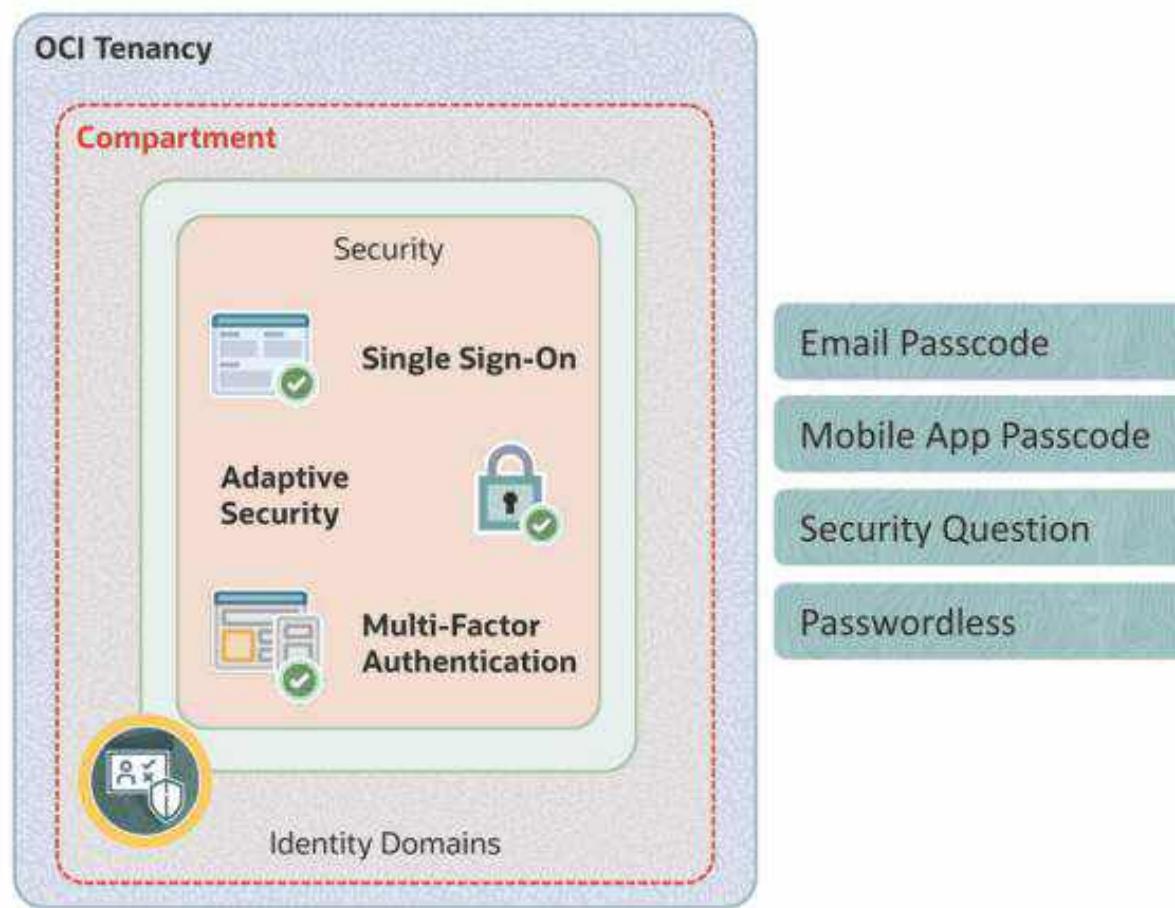
# Identity Domains: Identity Lifecycle Management

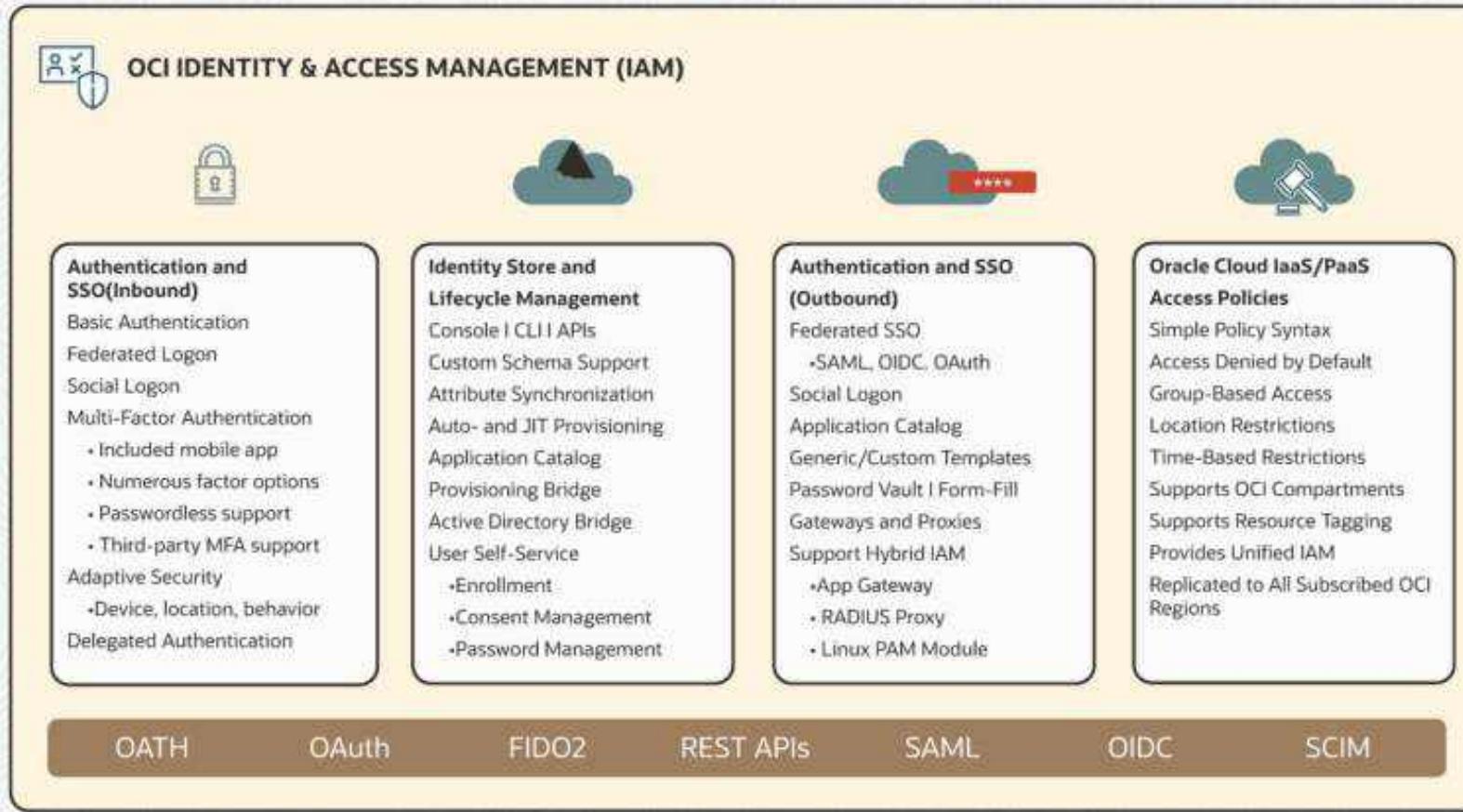


# Identity Domains: Identity Lifecycle Management

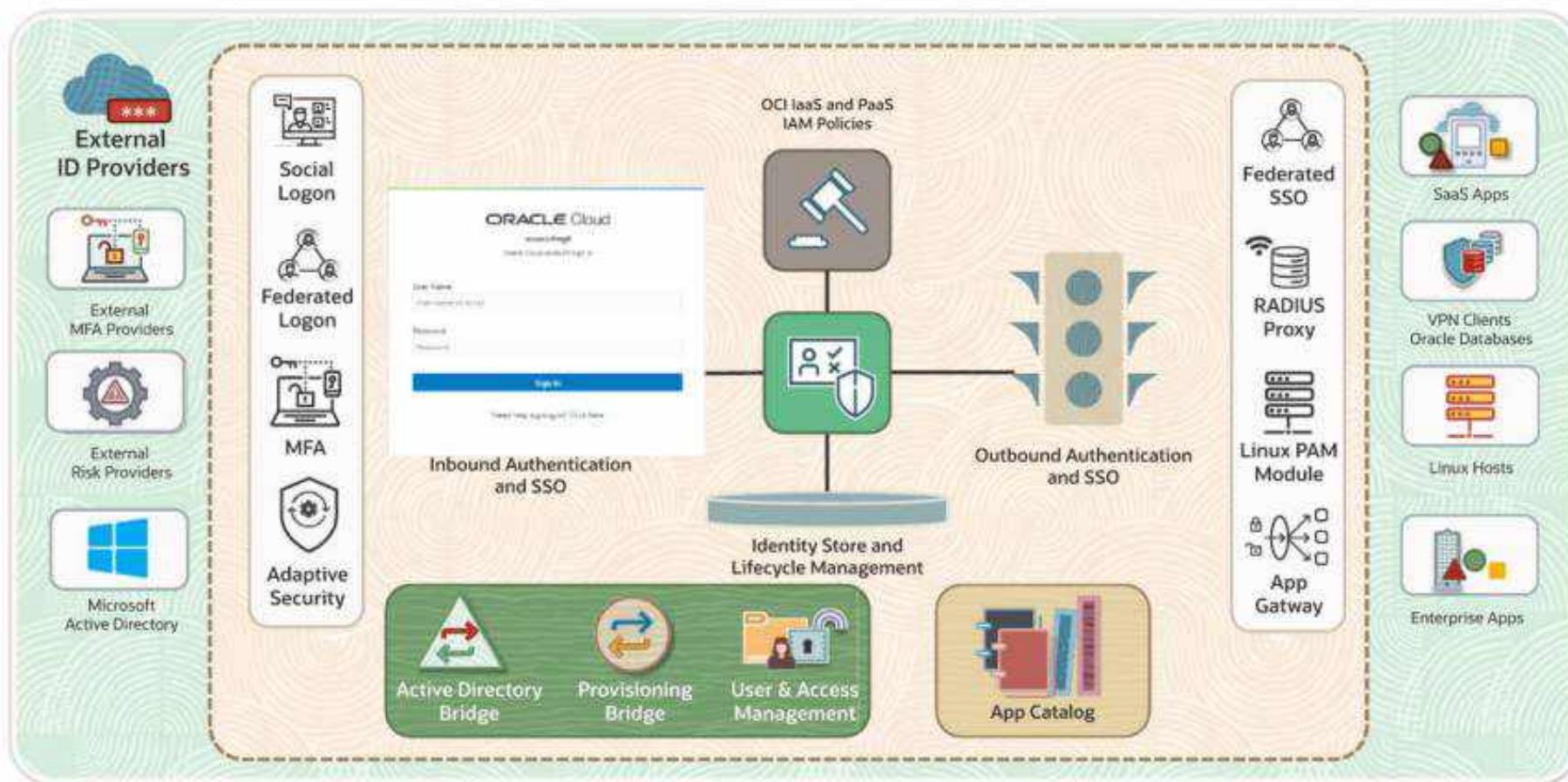


# Identity Domains: Identity Lifecycle Management





# OCI IAM with Identity Domains



**Oracle Cloud Infrastructure**

# Identity Domain Types

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

# 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)

## **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)

# Default Domain

The screenshot shows the Oracle Cloud Infrastructure Identity service interface. The left sidebar has 'Identity' selected, with 'Domains' highlighted. The main area title is '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'. On the left, under 'Compartments', 'saurabhp (root)' is selected. At the bottom left, there are 'Tag filters' and 'no tag filters applied'. On the right, 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 right side, there are three more green callout boxes with the following text:

- 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 includes links for Overview, Users, Groups (which is selected), 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 features a search bar and buttons for "Create group" and "More actions". A table lists two groups: "All domain Users" (description: "A group representing all users") and "Administrators" (description: "Administrators"). The "Administrators" row is highlighted with a red border. At the bottom of the table, it says "0 selected".

# Default Domain

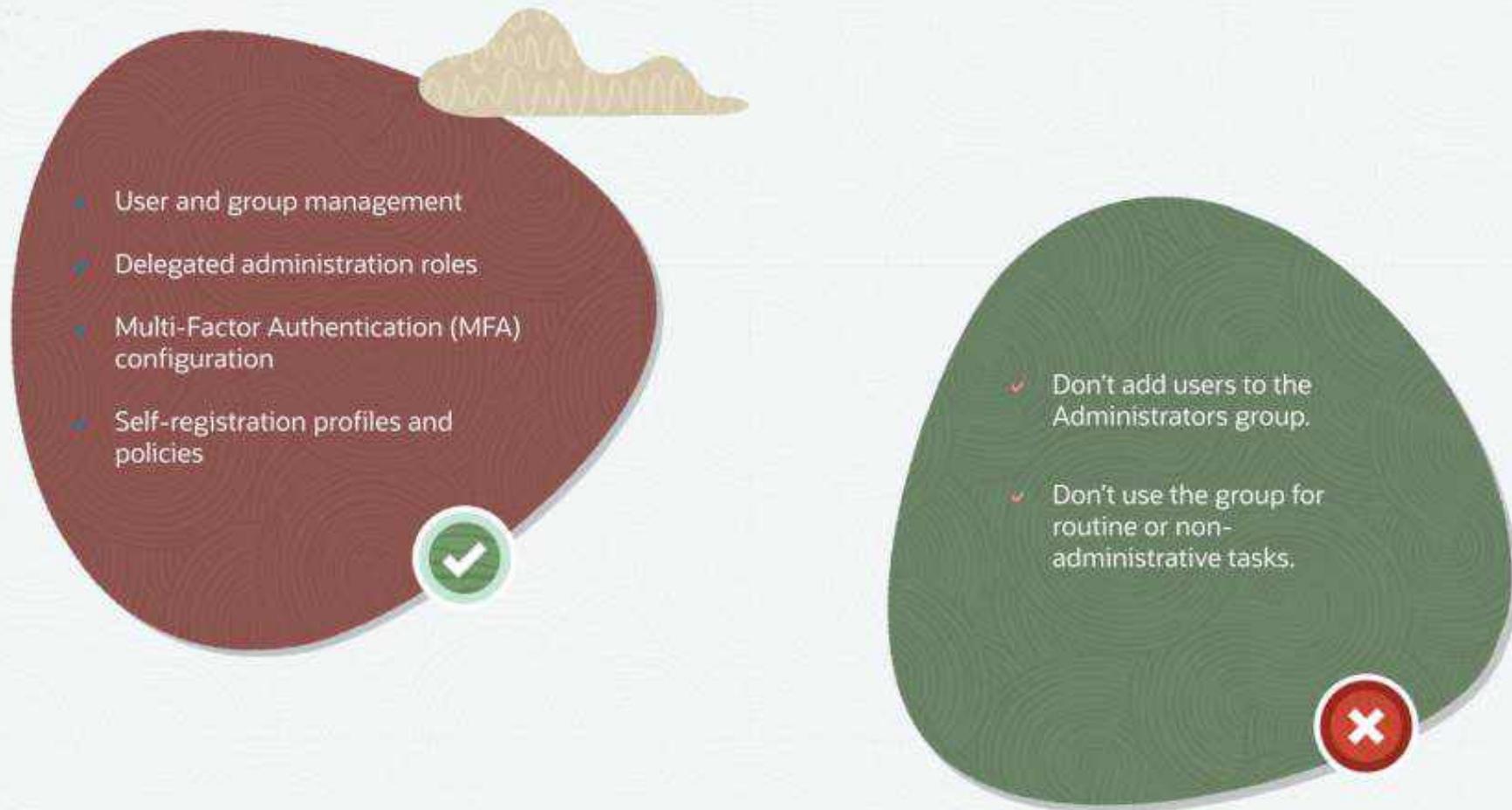
## Administrators Group

- 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



Oracle Cloud Infrastructure

# Creating Identity Domains

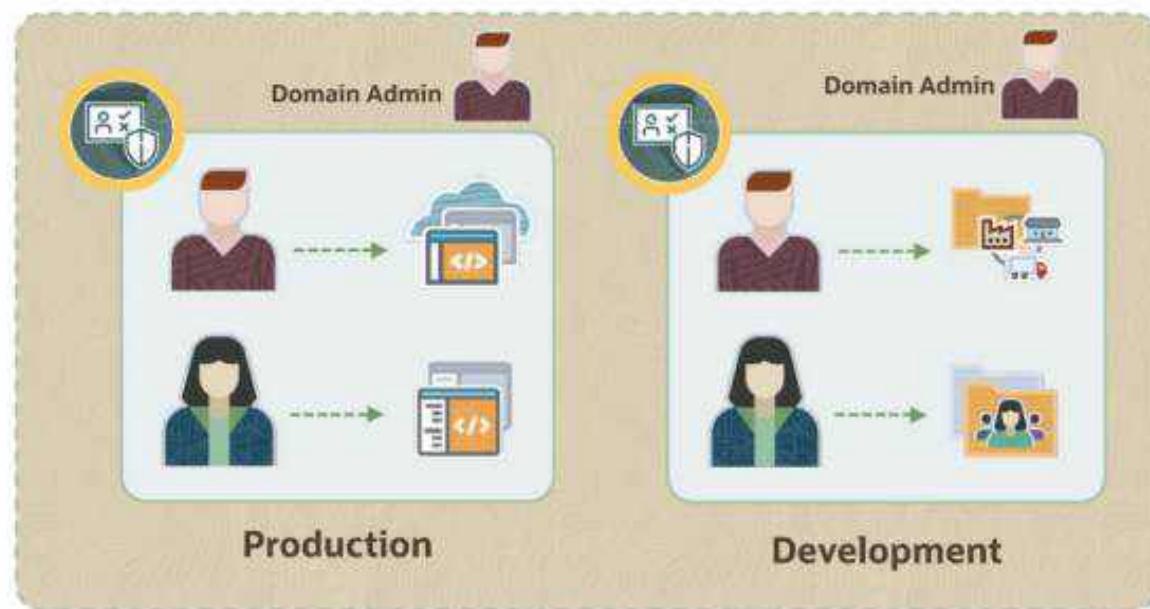
OCI Identity and Access Management (IAM)

# Why do we need multiple identity domains?

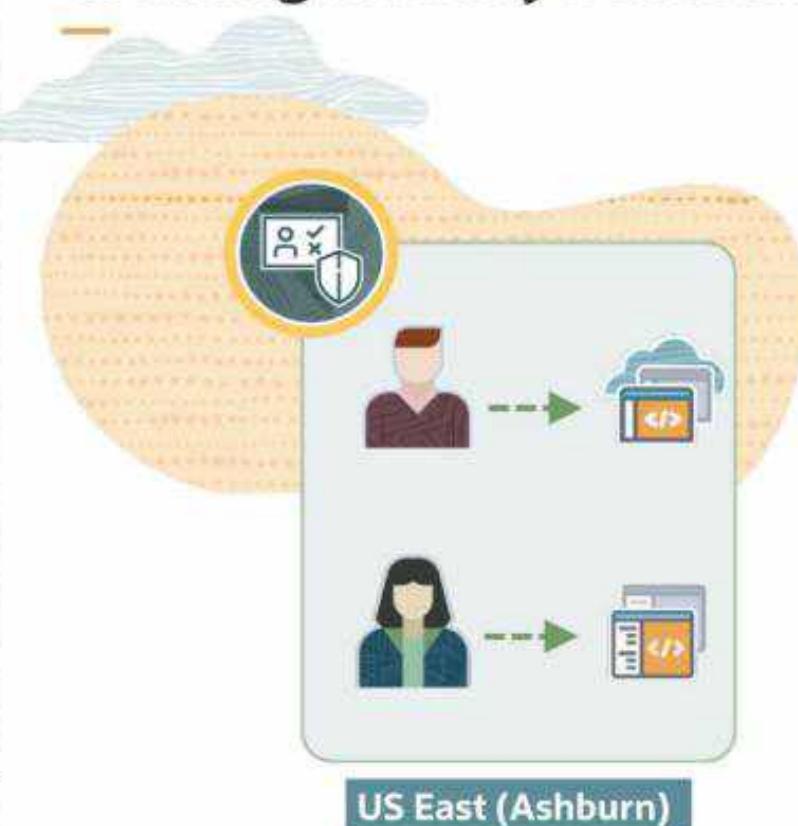
Isolation of administrative control

Security and compliance

Simplified management



# Creating Identity Domains



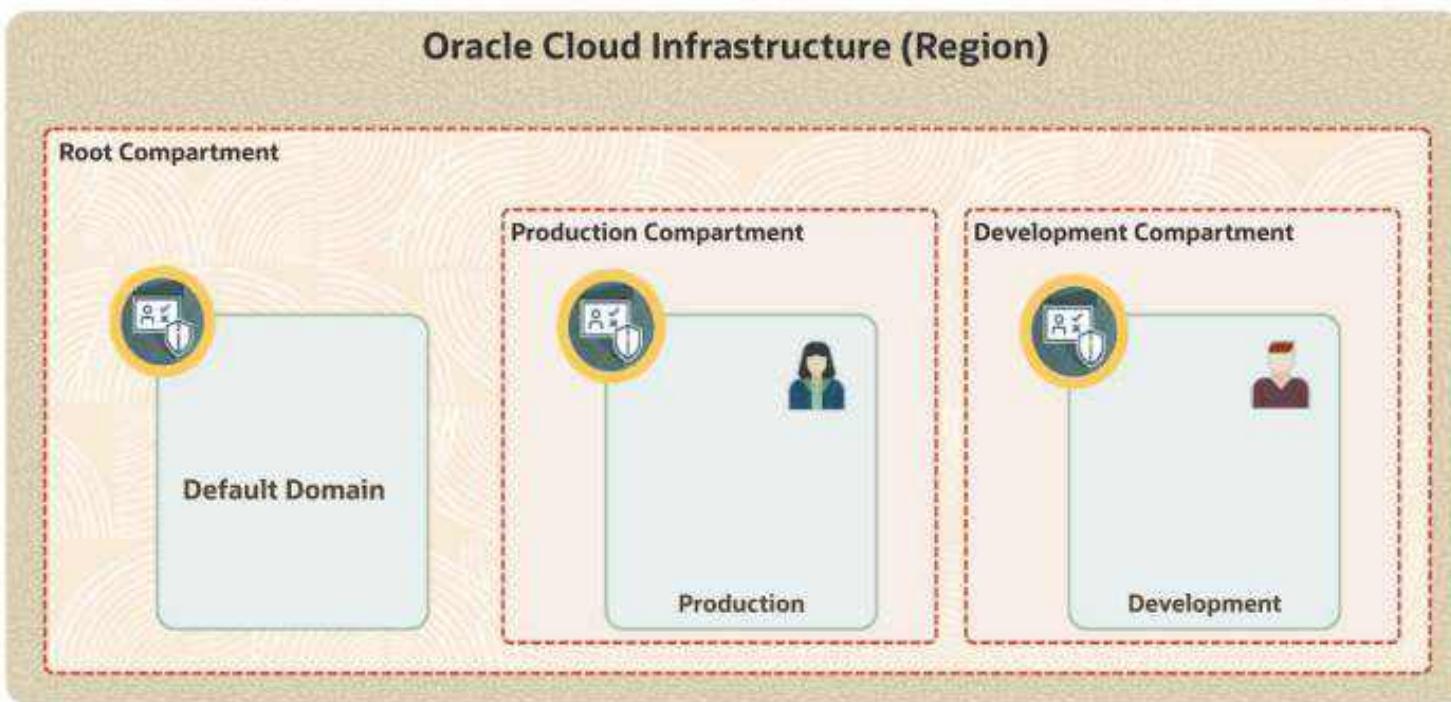
## Identity Domain Administrators

- 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.

# Creating Identity Domains

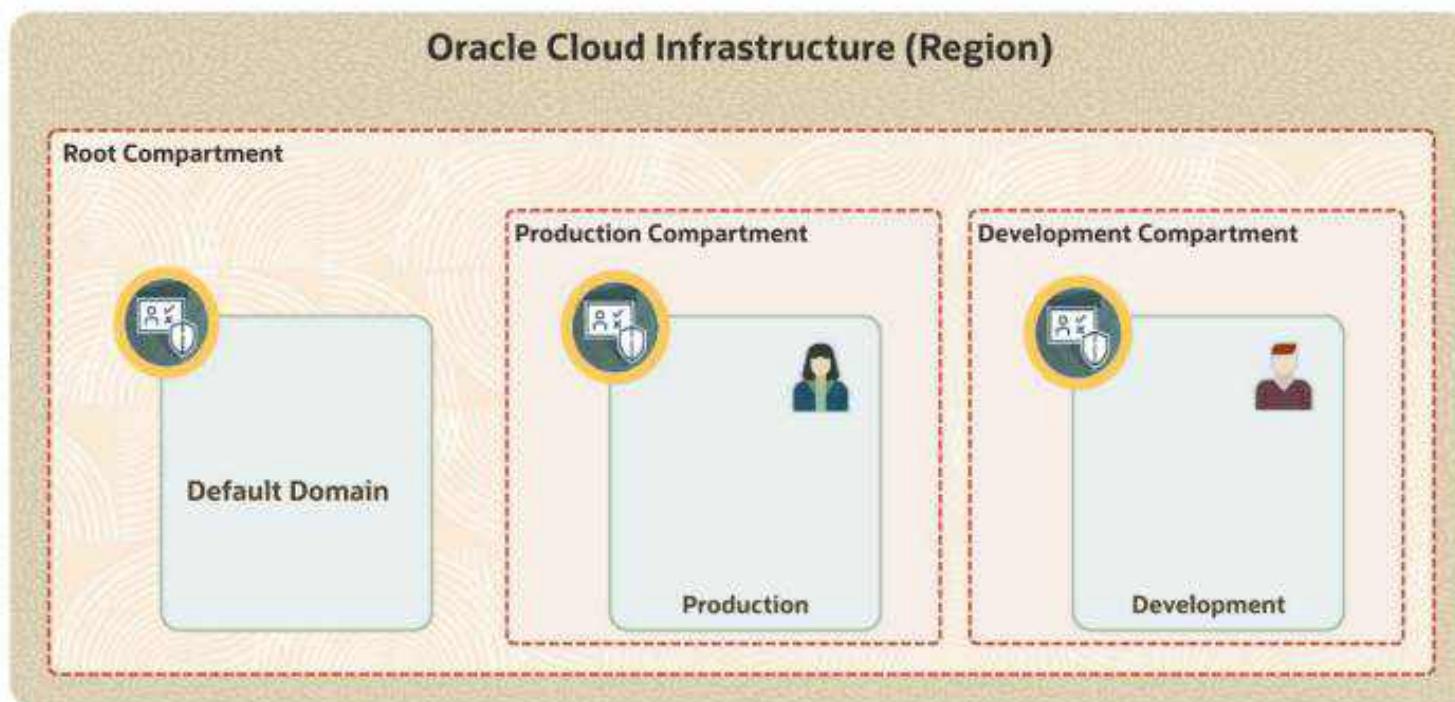


Oracle Cloud Infrastructure

# Demo: Creating Identity Domains

OCI Identity and Access Management (IAM)

# Creating Identity Domains

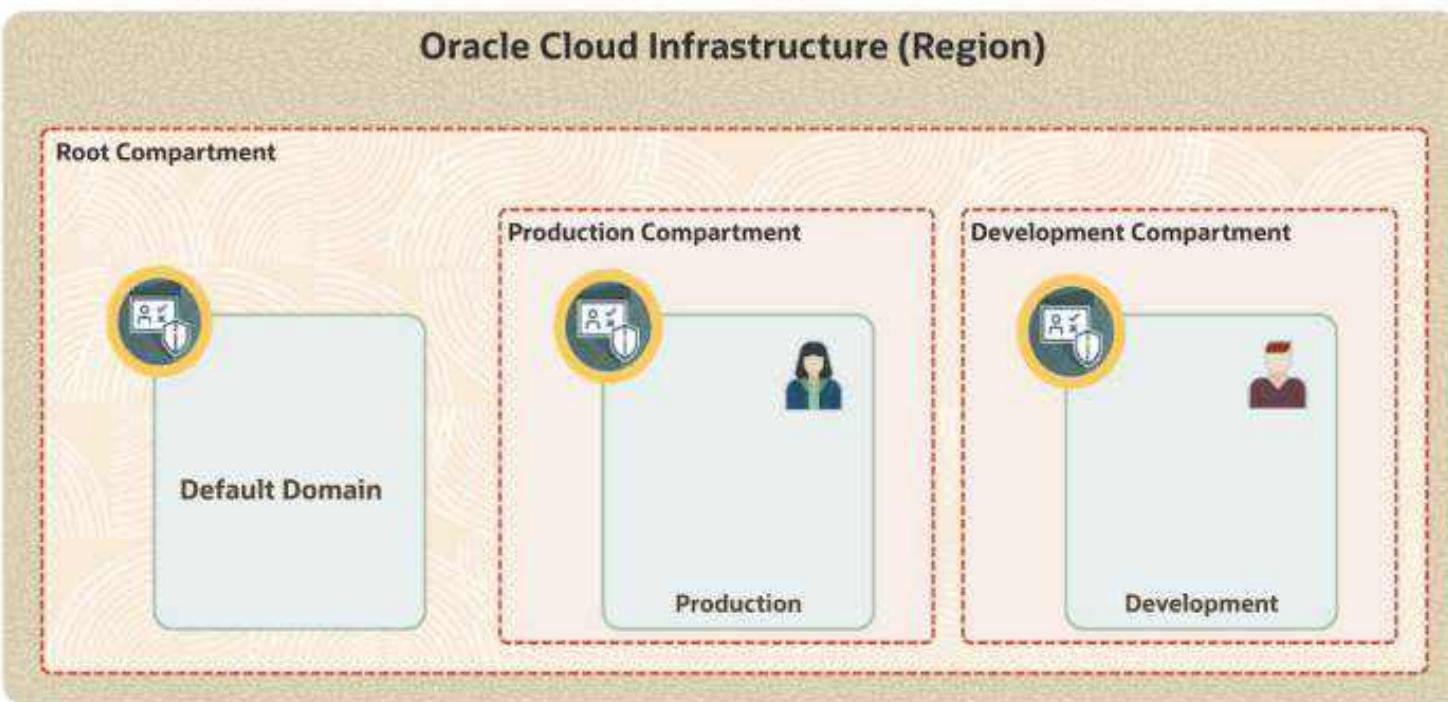


Oracle Cloud Infrastructure

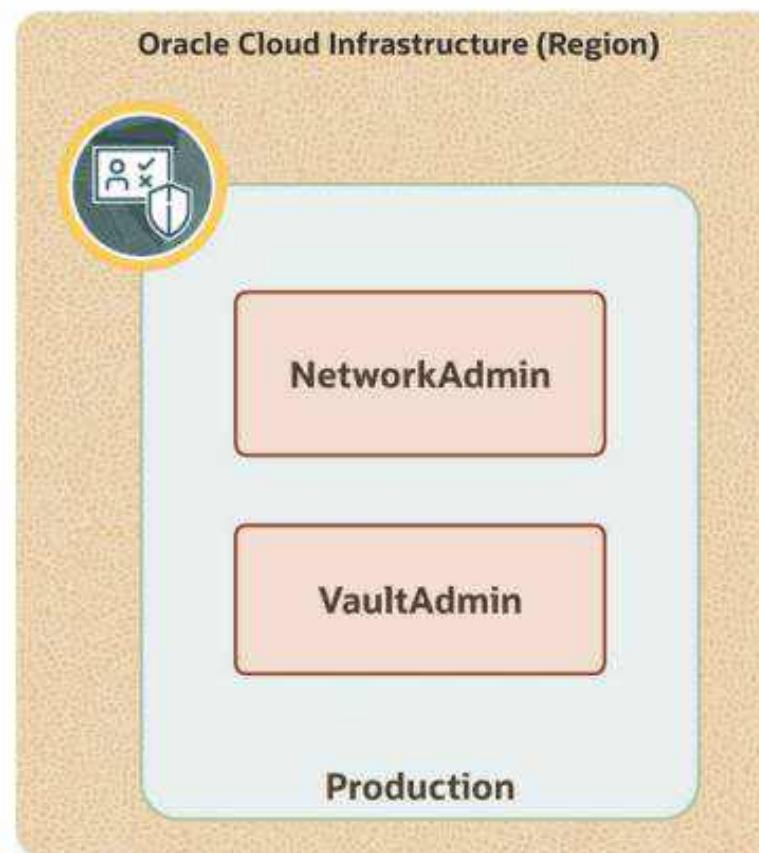
# Demo: Creating Groups

OCI Identity and Access Management (IAM)

# Creating Groups



# Creating Groups



# Oracle Cloud Infrastructure Managing Groups

OCI Identity and Access Management (IAM)

# Groups

---



Collections of users



Network Admin



Instances



Certificate Manager

# Groups



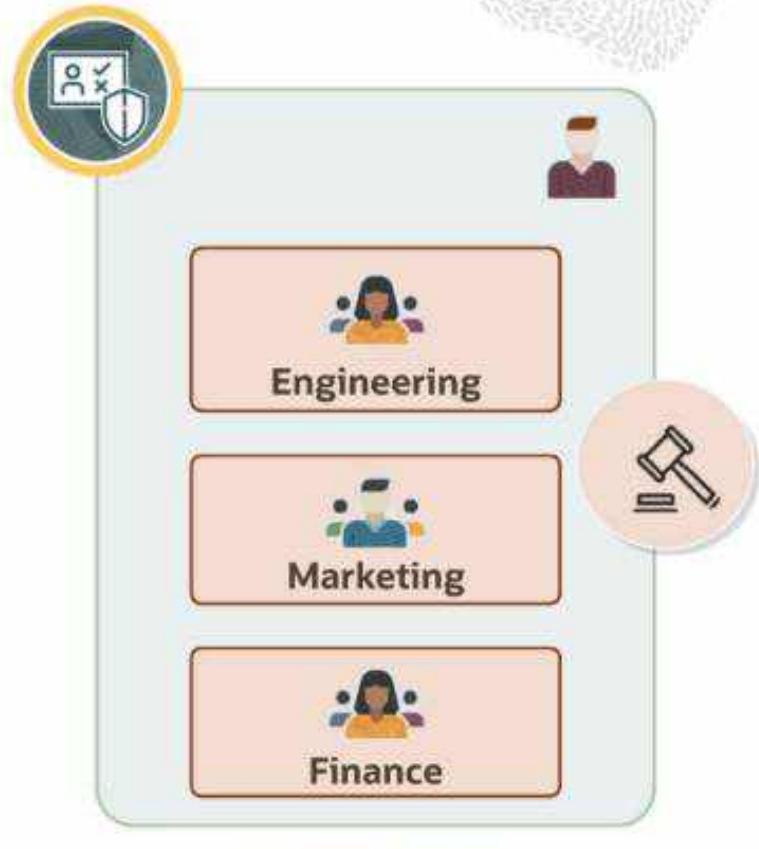
Collections of users



Simplify access management



Audit and compliance



Identity Domain

# Default Groups in Identity Domains

## Groups in Production Domain

Search by group name or description.

Create group    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

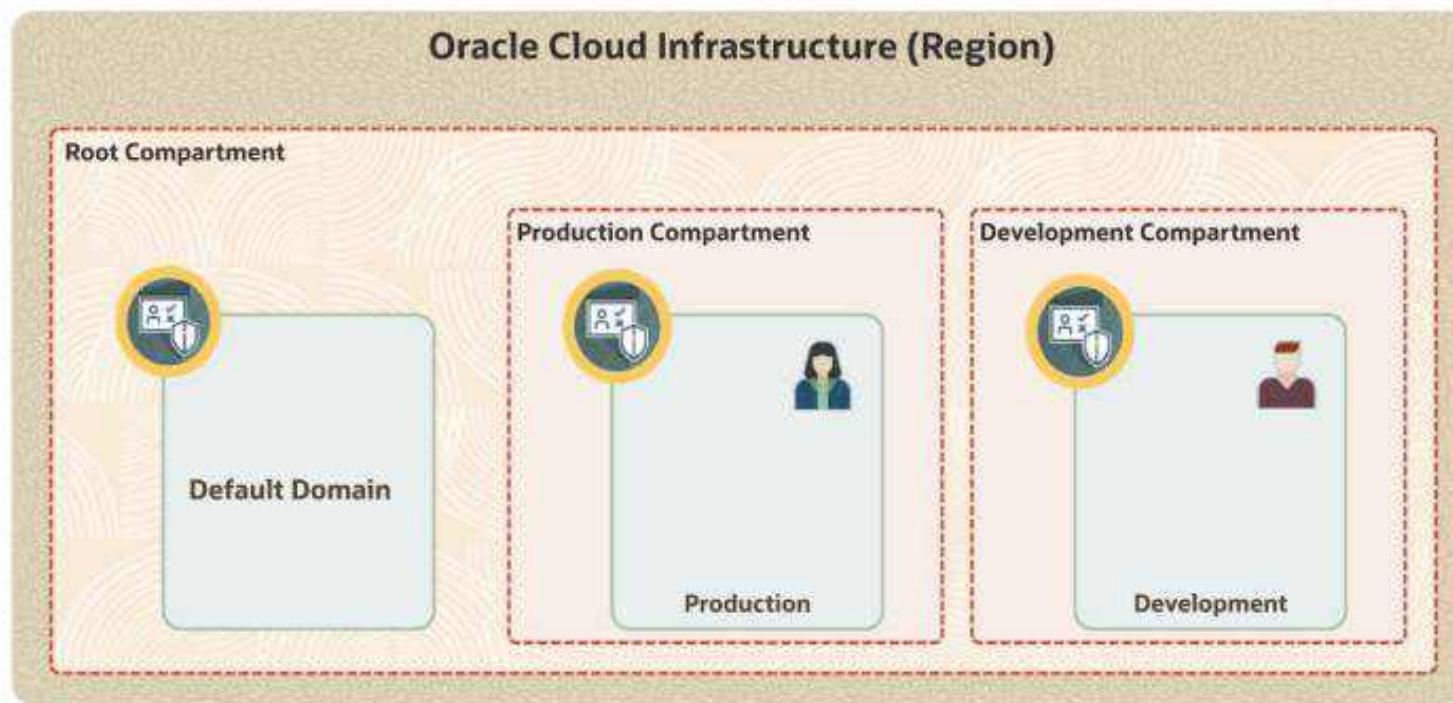
- All users are, by default, part of All Domain Users group.
- This group can't be deleted.

**Oracle Cloud Infrastructure**

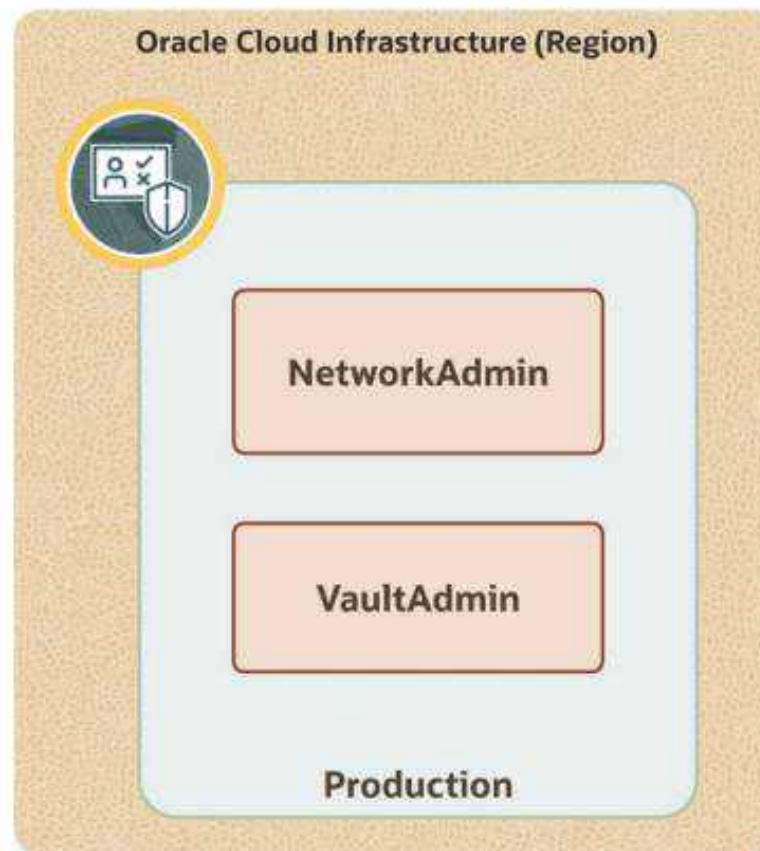
# Demo: Creating Users

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

# Creating Groups



# Creating Users



Create User using Console



Create User using CSV import



# Oracle Cloud Infrastructure Managing Users

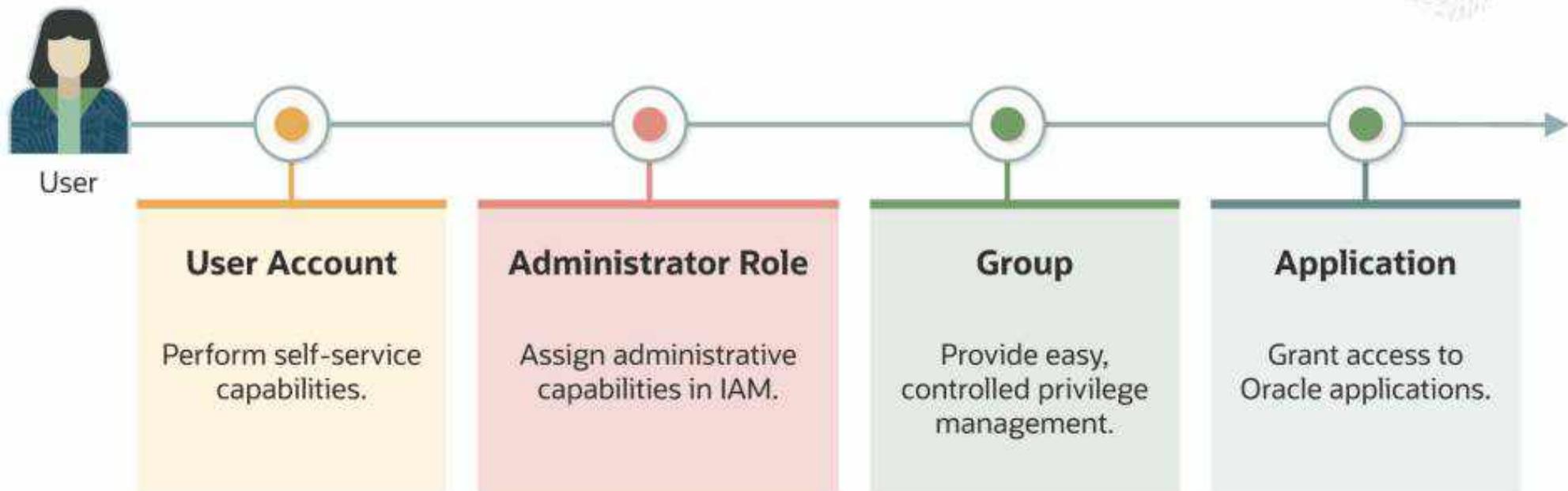
**OCI Identity and Access Management (IAM)**



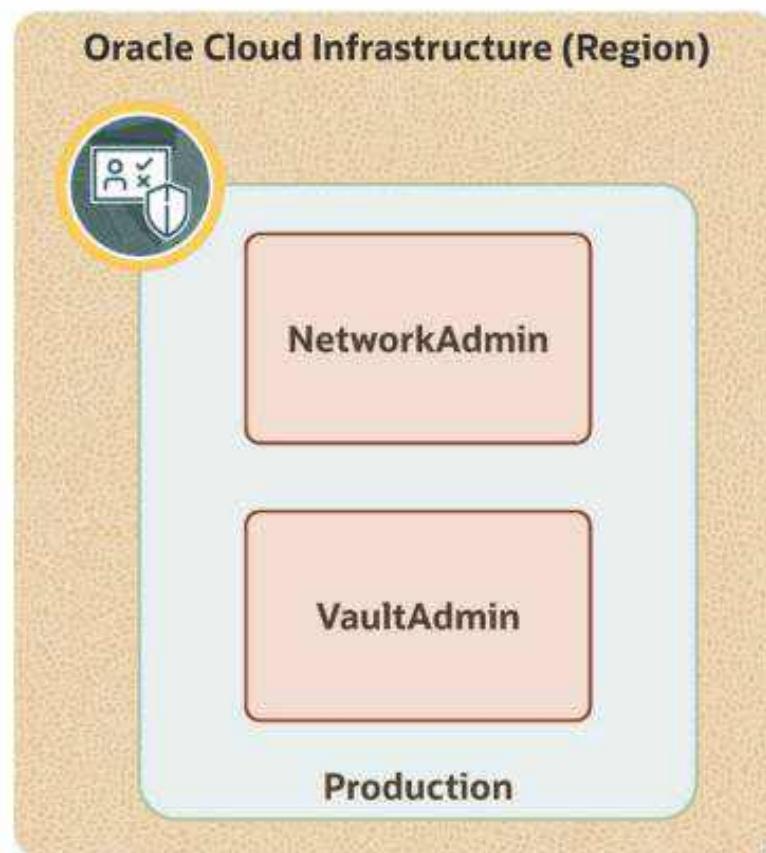
# Stages of the IAM User Life Cycle



# User Lifecycle Management



# Creating Groups



Oracle Cloud Infrastructure

# Understanding the Administrator Role

OCI Identity and Access Management (IAM)

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**

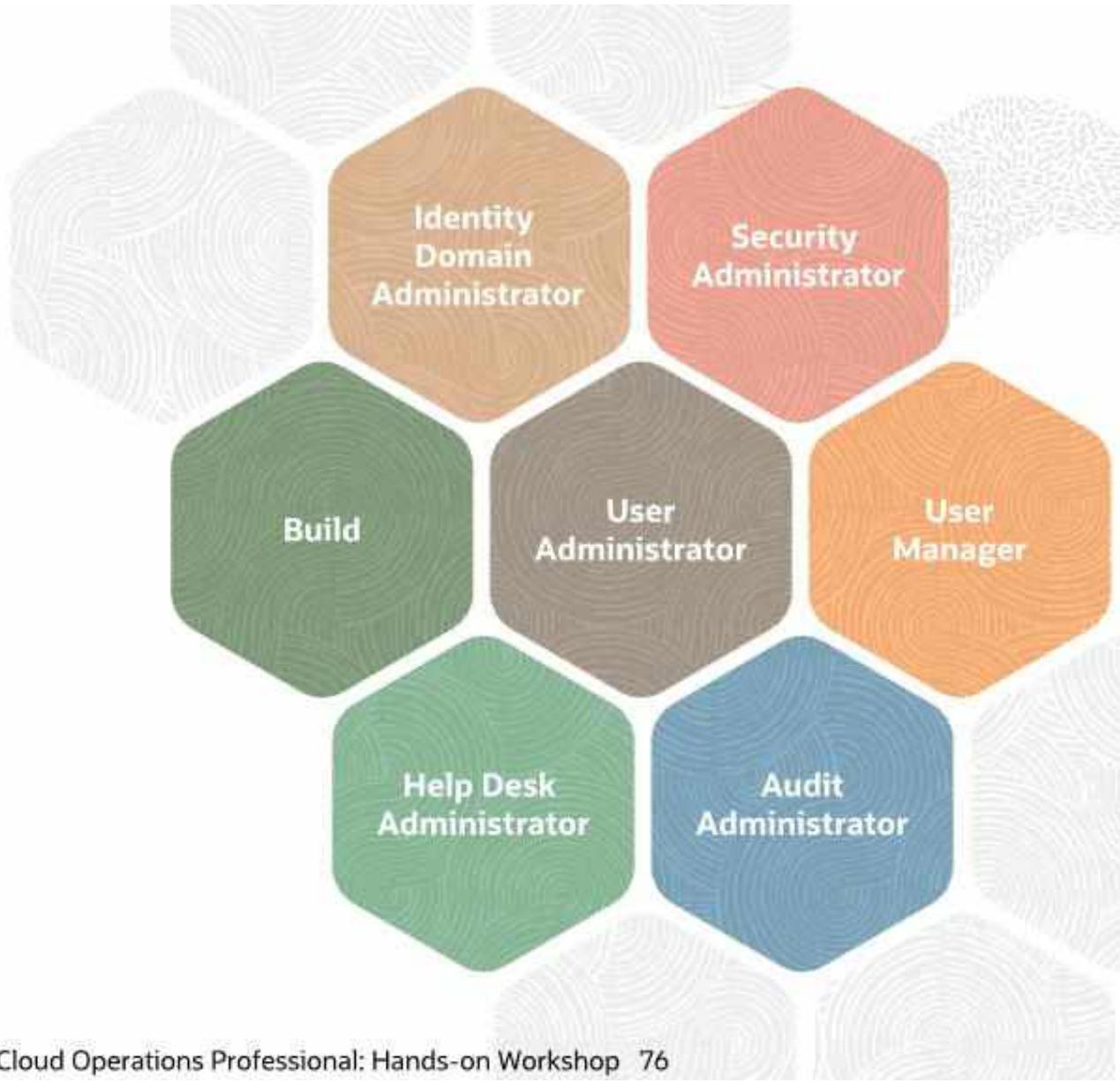


**Using roles instead of traditional policies ensures structured access management**

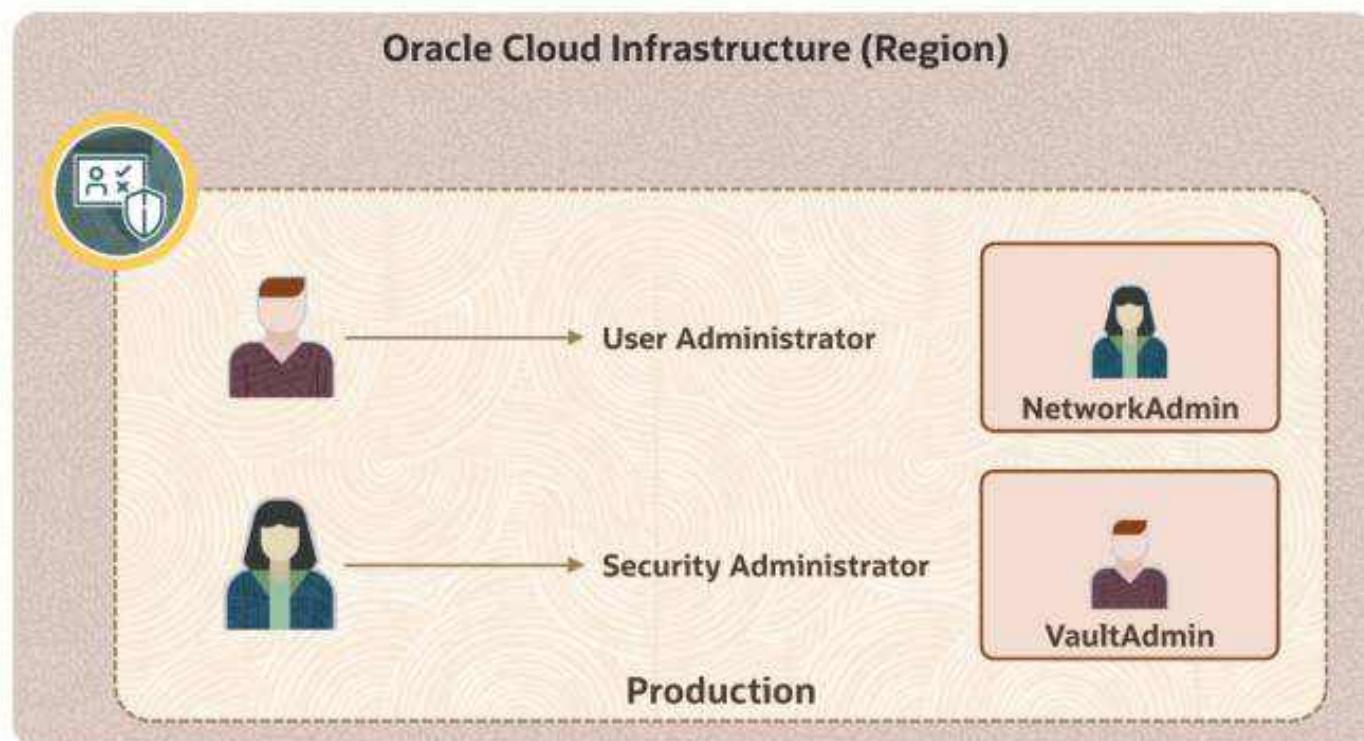
# Types of Administrator Roles

## Business Criticality

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



# Assigning Administrative Roles



# Oracle Cloud Infrastructure Policies

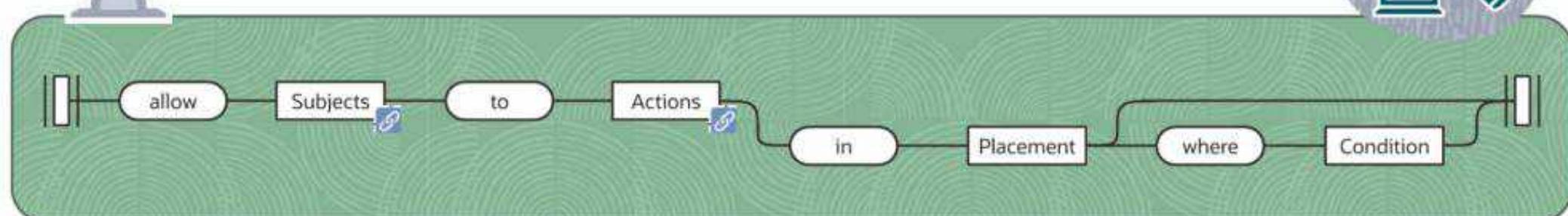
## Identity and Access Management

# Policies



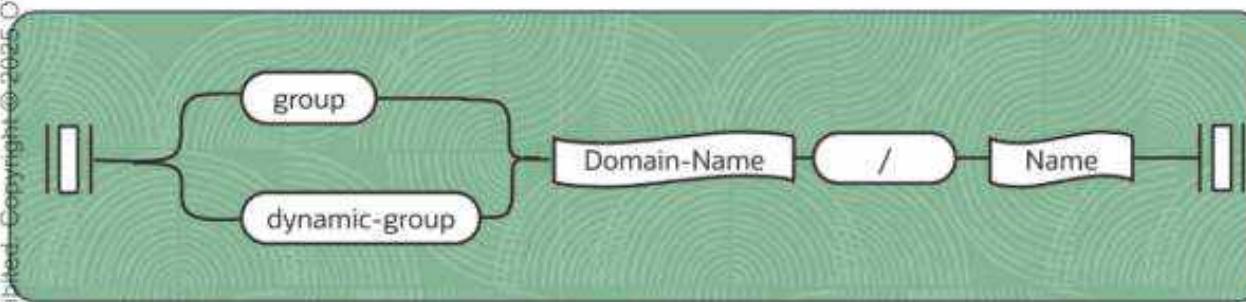
What permissions do you have?

Set using IAM Policies





# Subjects Clause



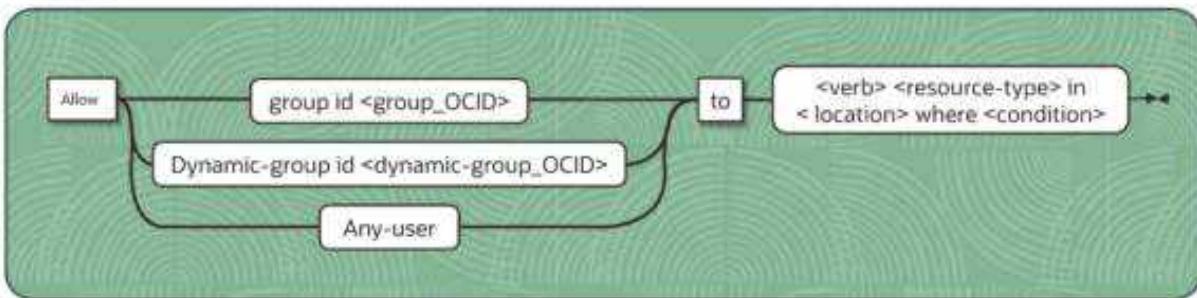
Subjects are a clause for providing access to authenticated actors:

- 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").



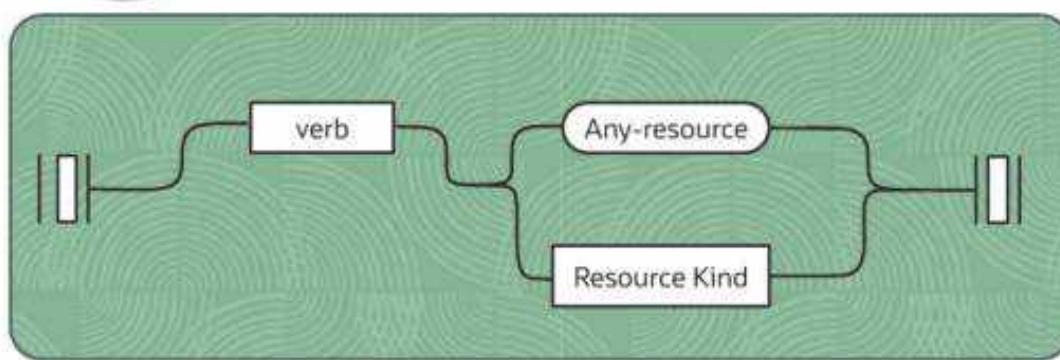
## Subjects Clause

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



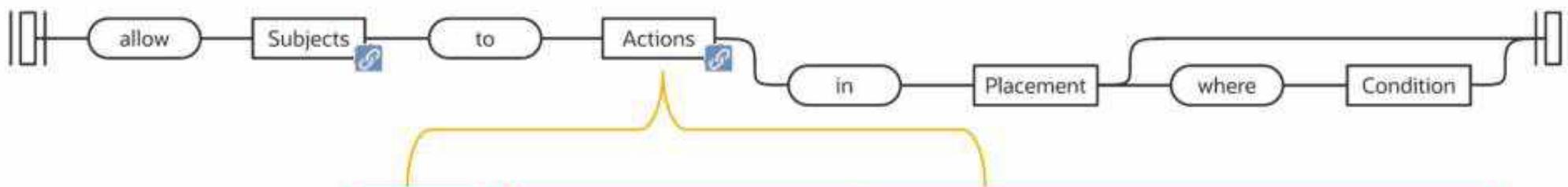
Services define one or more permissions that any given API call will require.

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



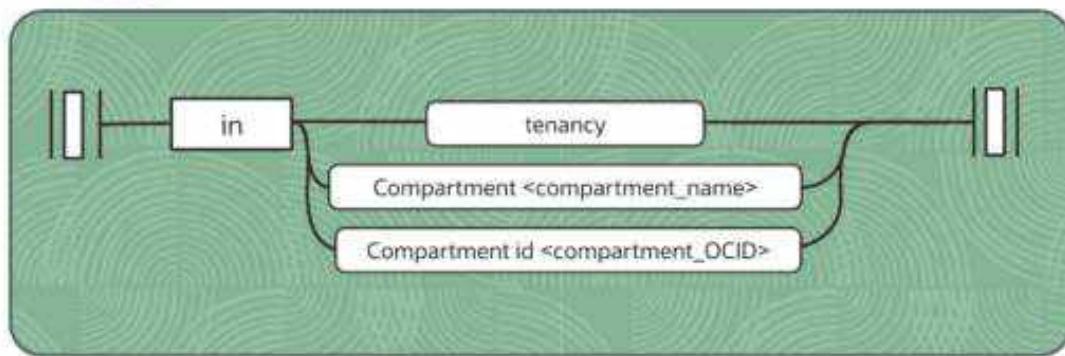
## Actions Clause



Verb	Aggregate resource-type	Individual resource type
inspect	all-resources	
read	database-family	db-systems, db-nodes, db-homes, databases
	instance-family	instances, instance-images, volume-attachments, console-histories
use	object-family	buckets, objects
	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...4fmameqh71cdlihrvur7xq

# 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



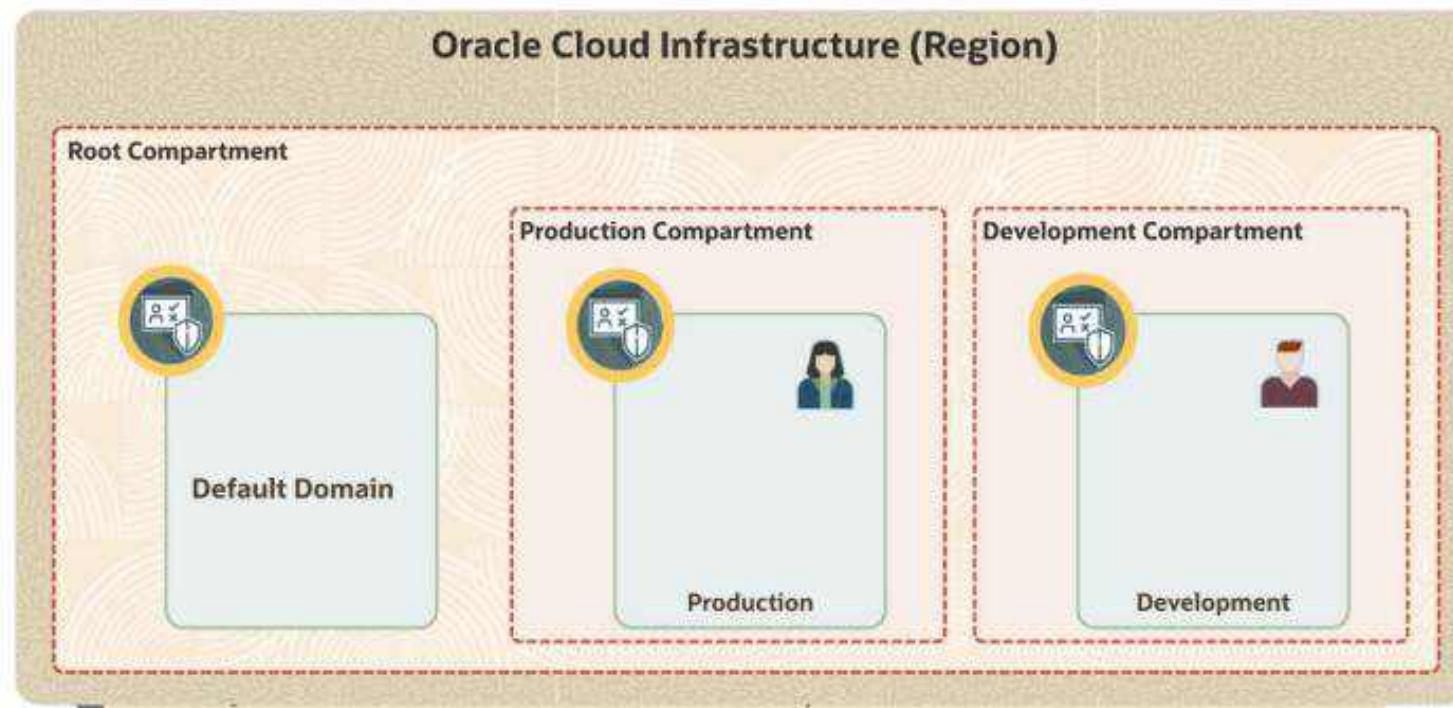
**Best practice:** Create dedicated compartments to isolate resources.



# Compartment

## Oracle Cloud Infrastructure (Region)

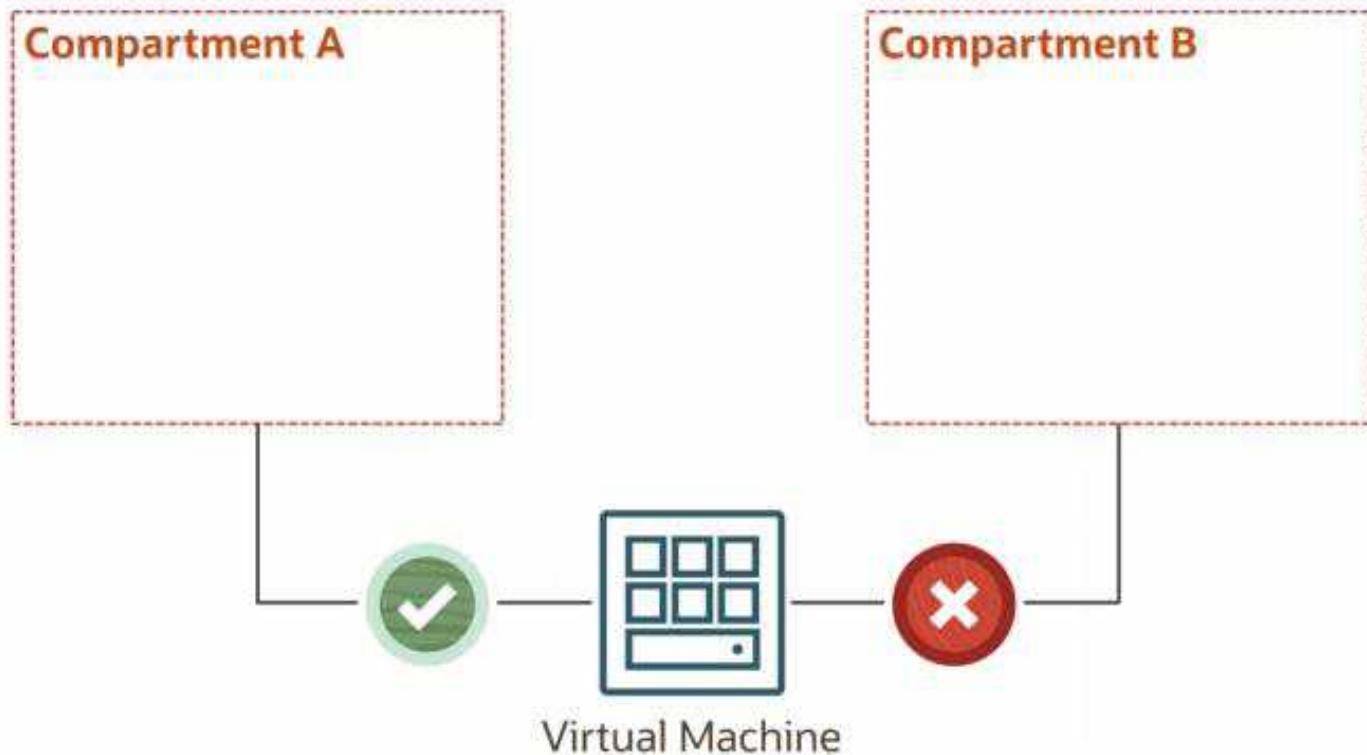
Collection  
of related  
resources



Isolate and  
control  
access

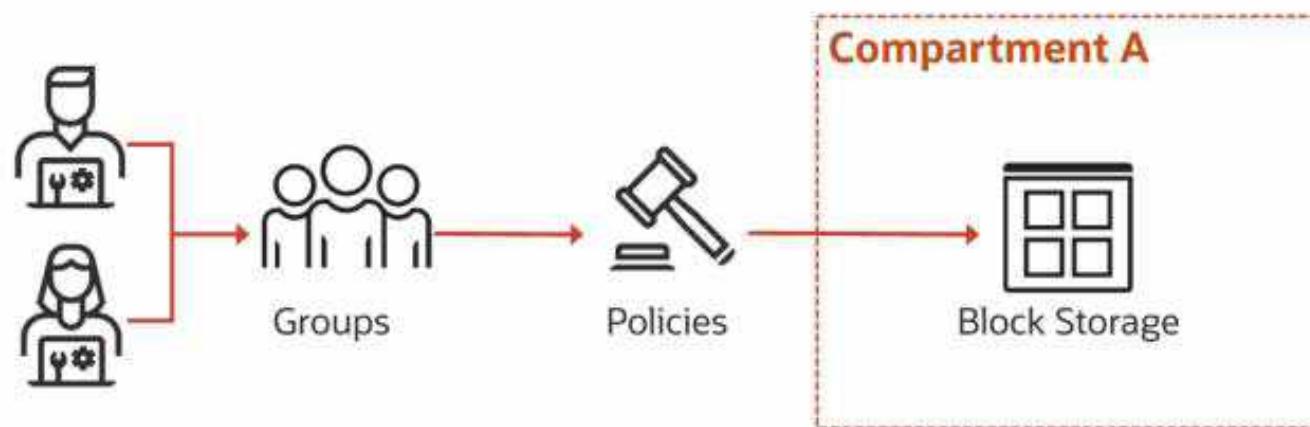
## Resource Compartments

Each resource belongs to a single compartment



# Compartments

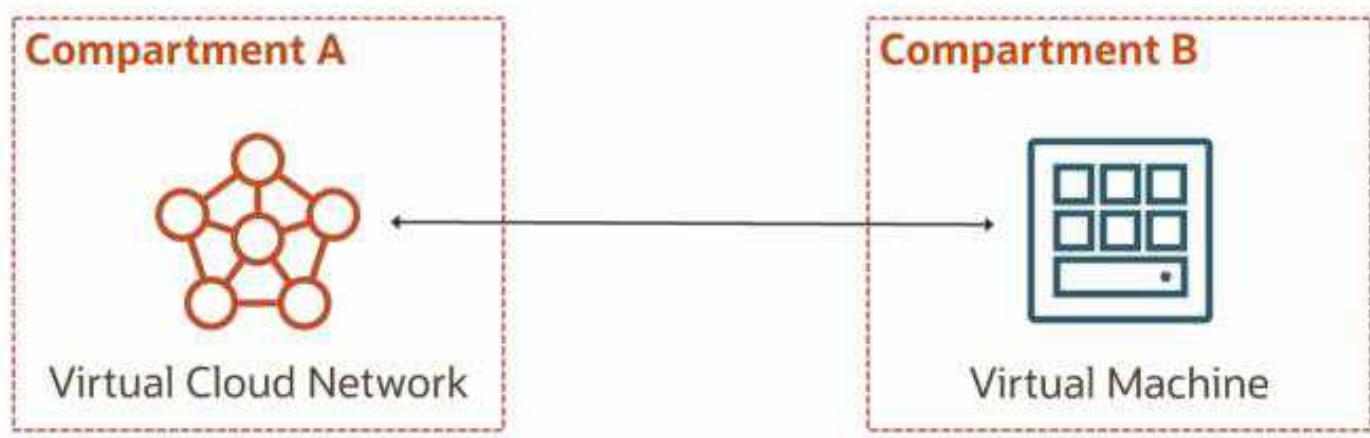
## Access



Users + Policies = Access to Compartments

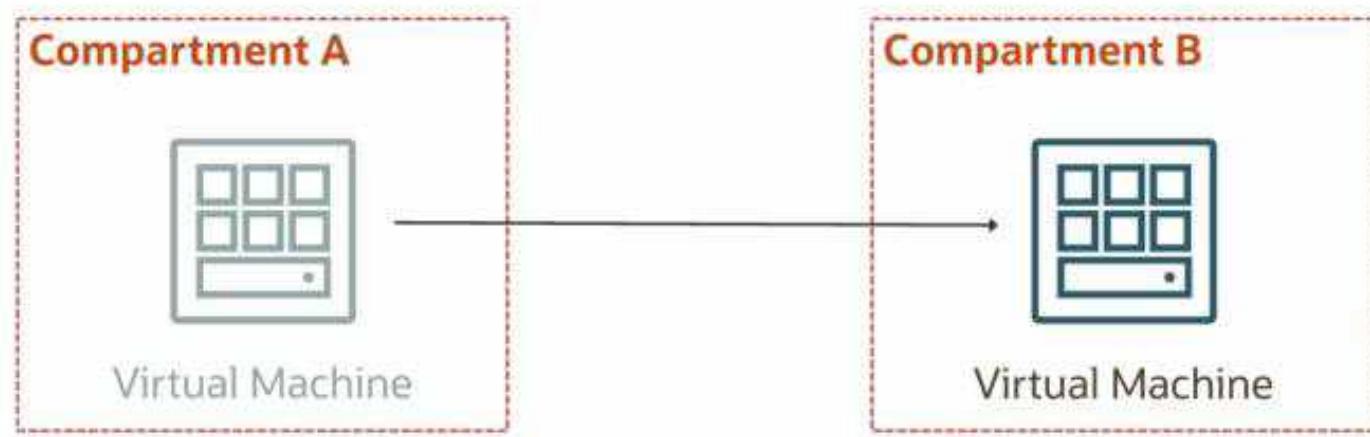
## Interaction of Resources

Resources can interact with other resources in different compartments.

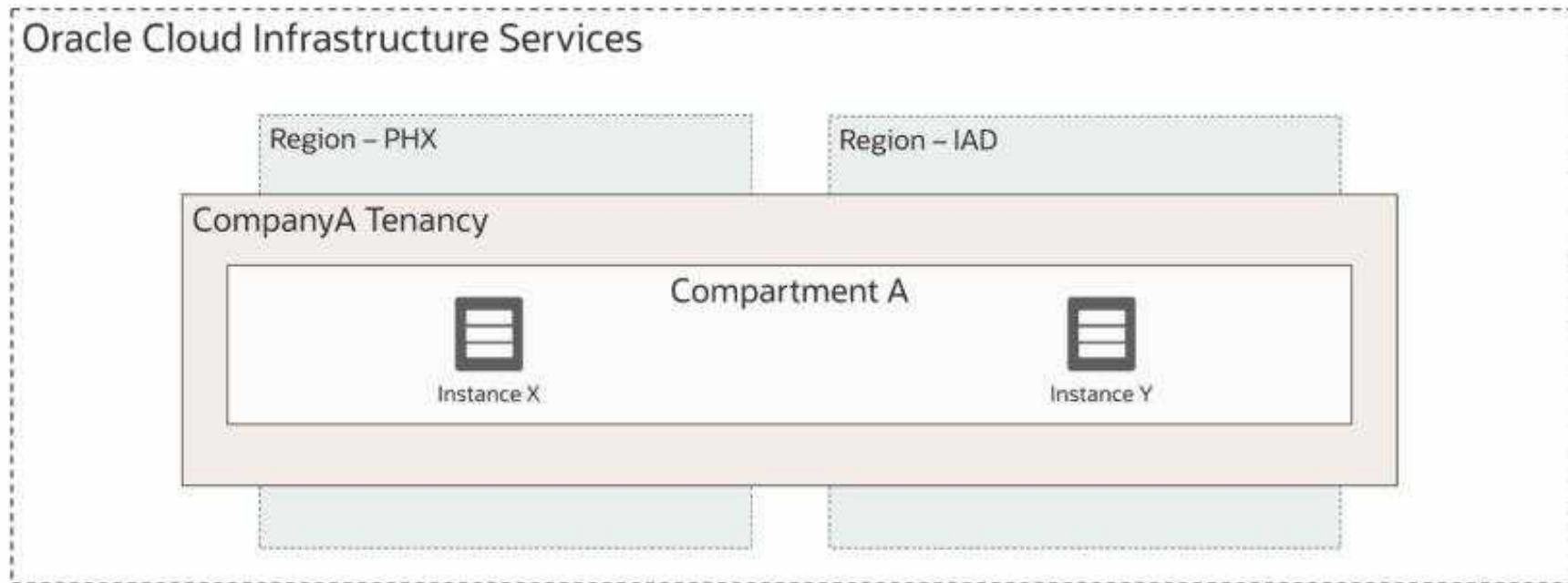


## Movement of Resources

Resources can be moved from one compartment to another.

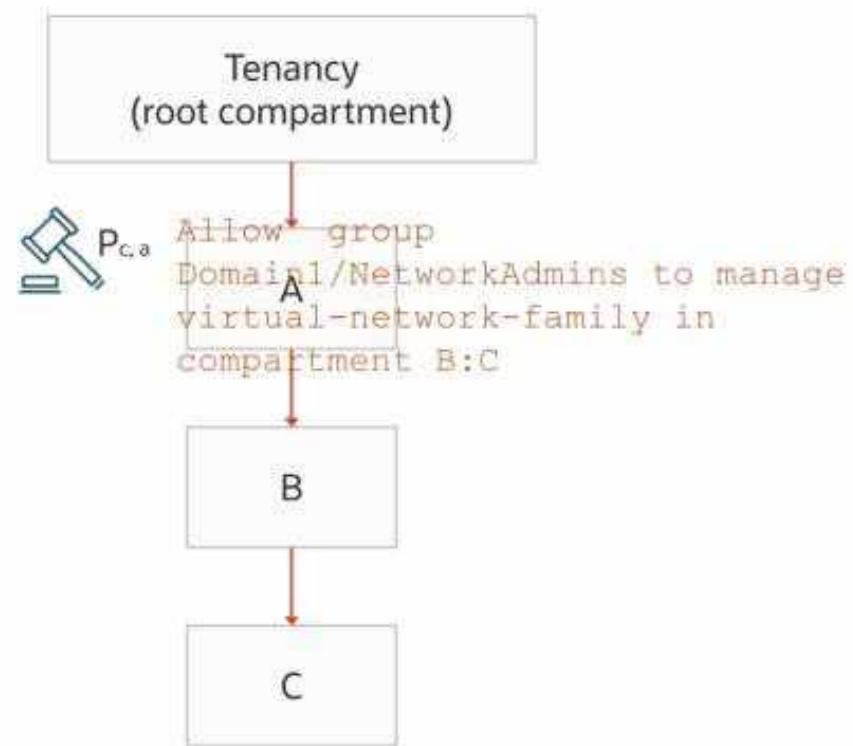


# Multiple Regions



Resources from multiple regions can be in the same compartment.

# Nested Compartments

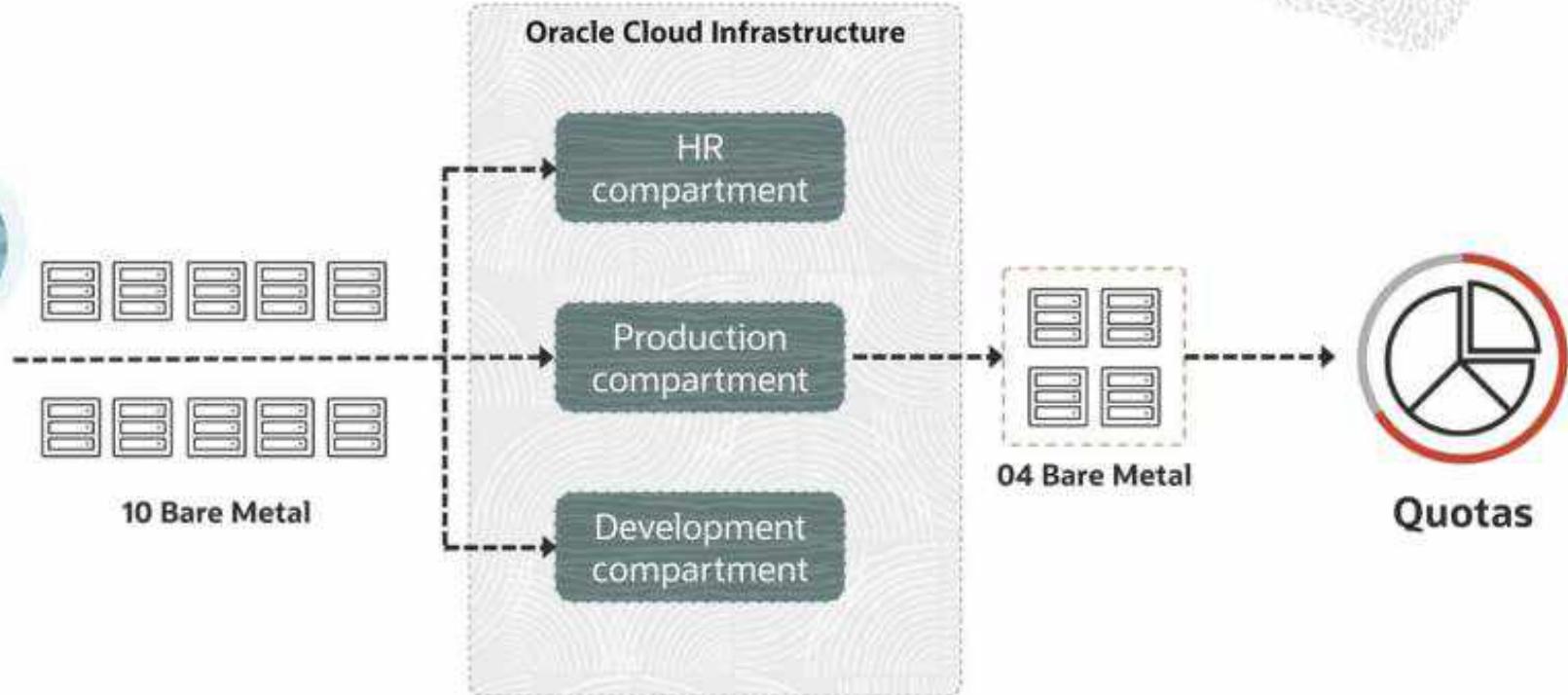


# Oracle Cloud Infrastructure Compartment Quotas

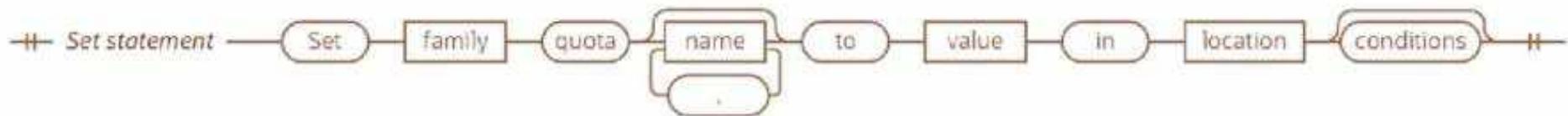
---

## OCI Identity and Access Management

## Scenario



## Quota Syntax

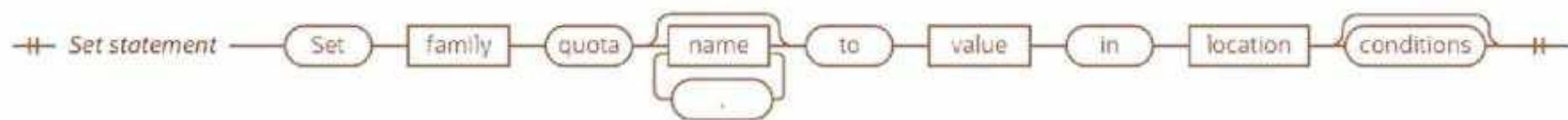


**Don't allow more than four virtual cloud networks (VCN) in a compartment**

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



## Quota Syntax

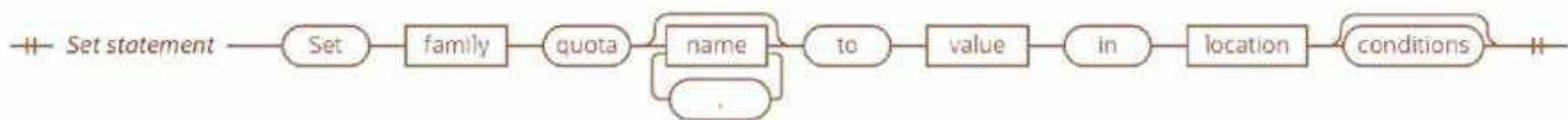


**Don't allow more than four virtual cloud networks (VCN) in a compartment**

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



## Quota Syntax

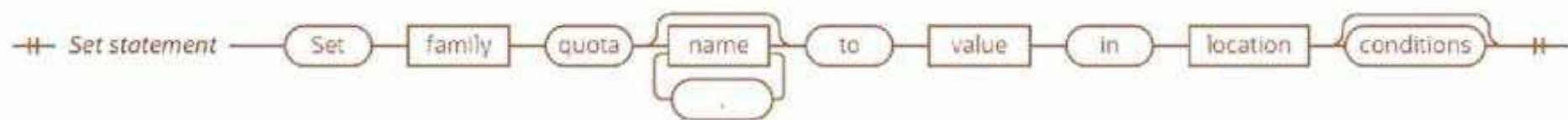


**Don't allow more than four virtual cloud networks (VCN) in a compartment**

```
set vcn quota vcn-count to <value>
        4
        10
        50
```



## Quota Syntax

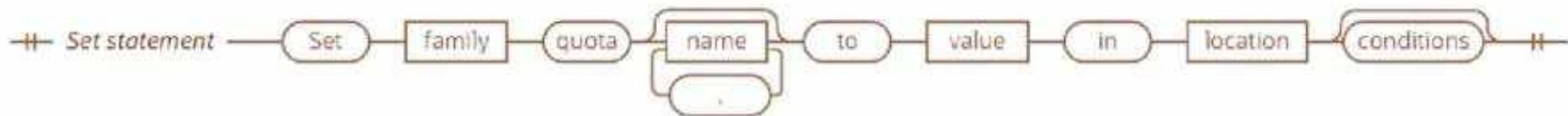


**Don't allow more than four virtual cloud networks (VCN) in a compartment**

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



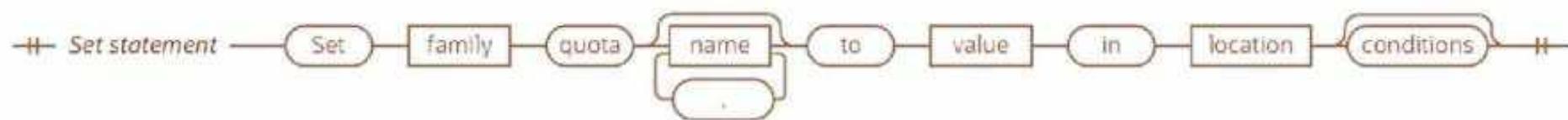
## Quota Syntax



**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.



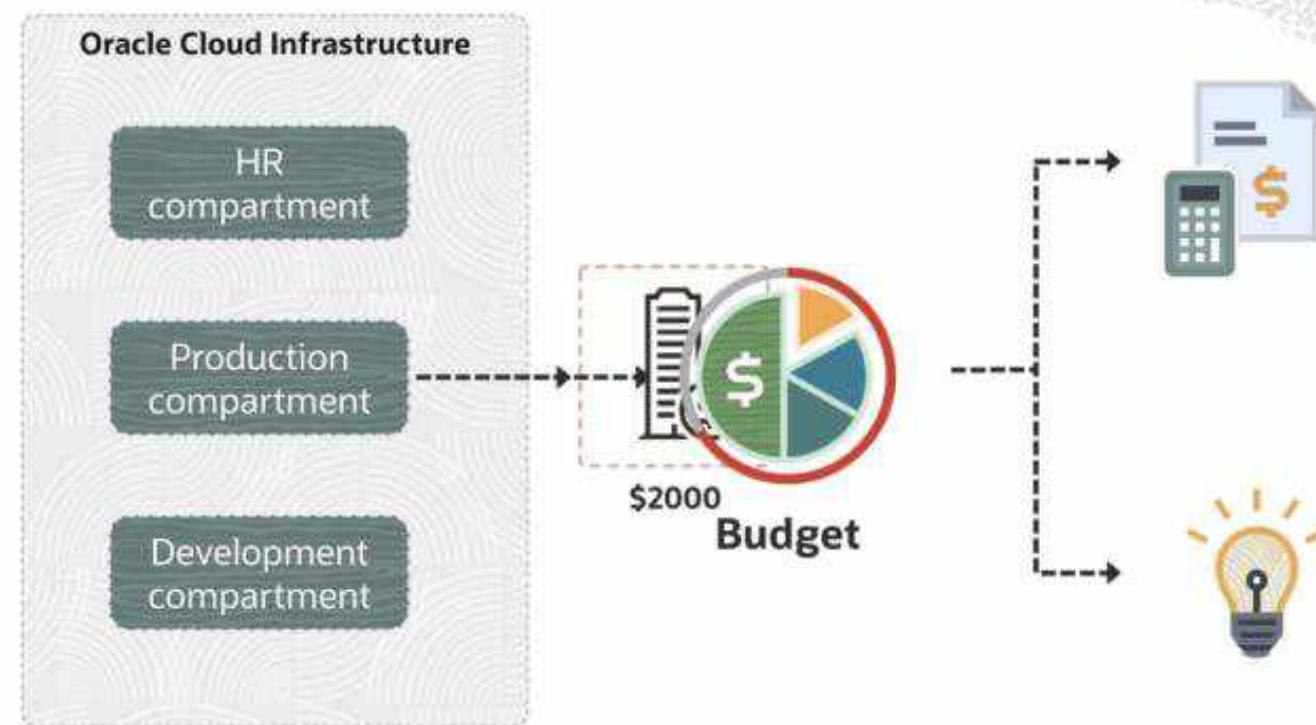
## Quota Examples

---

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

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

# Budgets



## Oracle Cloud Infrastructure

# Demo: Policies

### OCI Identity and Access Management (IAM)

Oracle Cloud Infrastructure

# Demo: Understanding Administrator Role

OCI Identity and Access Management (IAM)

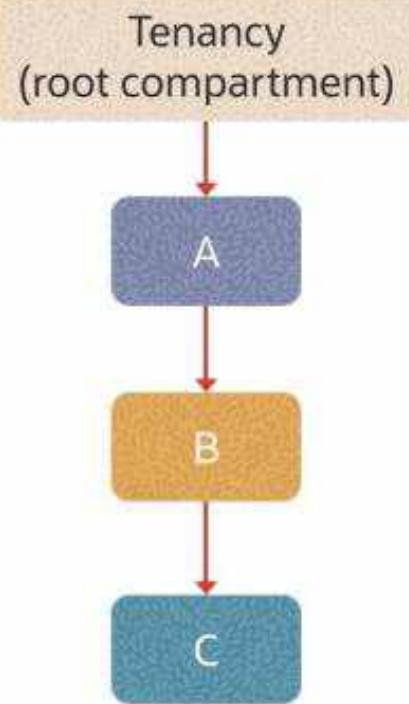


# Identity and Access Management-Advanced

## Oracle Cloud Infrastructure

# Demo: Policy Inheritance and Attachment

### OCI Identity and Access Management (IAM)



Oracle Cloud Infrastructure

# Policy Inheritance and Attachment

OCI Identity and Access Management (IAM)

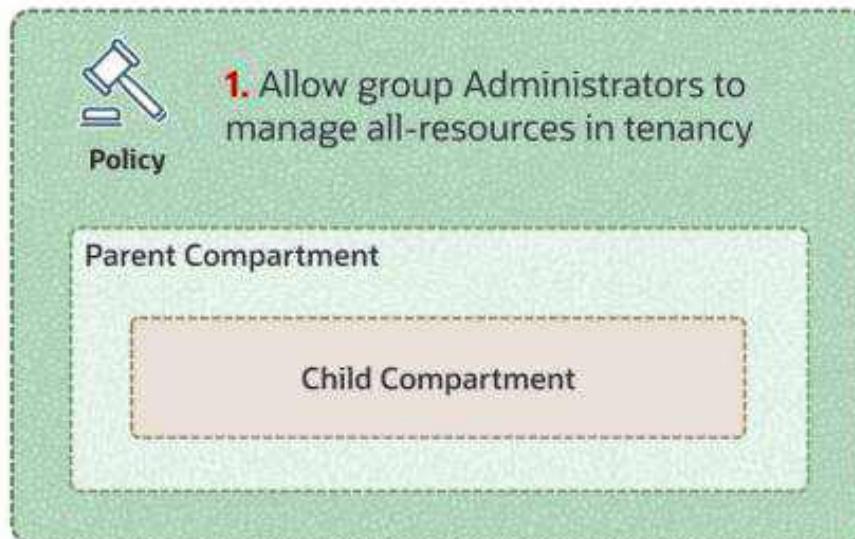
# Policy Inheritance

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.



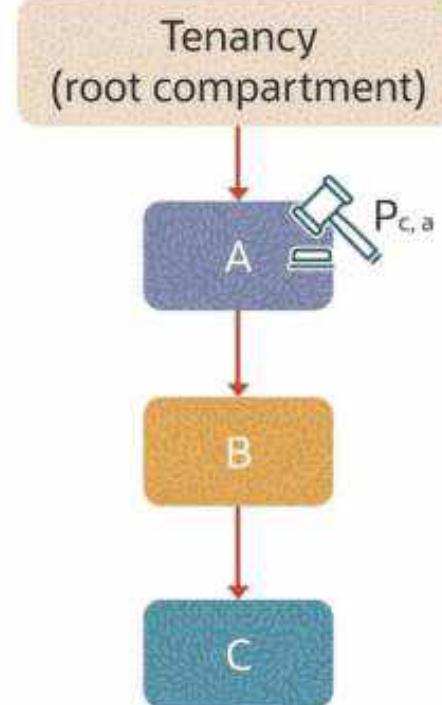
## Tenancy/Root Compartment



# 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.

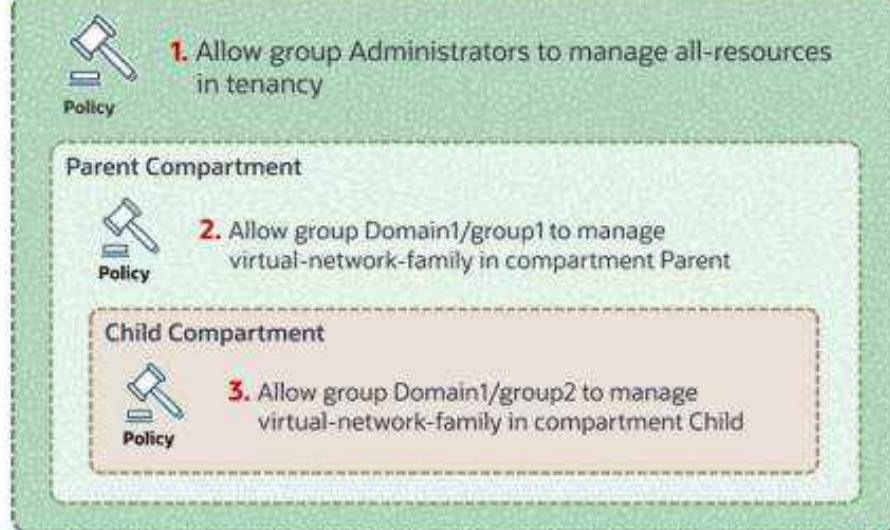


# Policy Attachment

- 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 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.

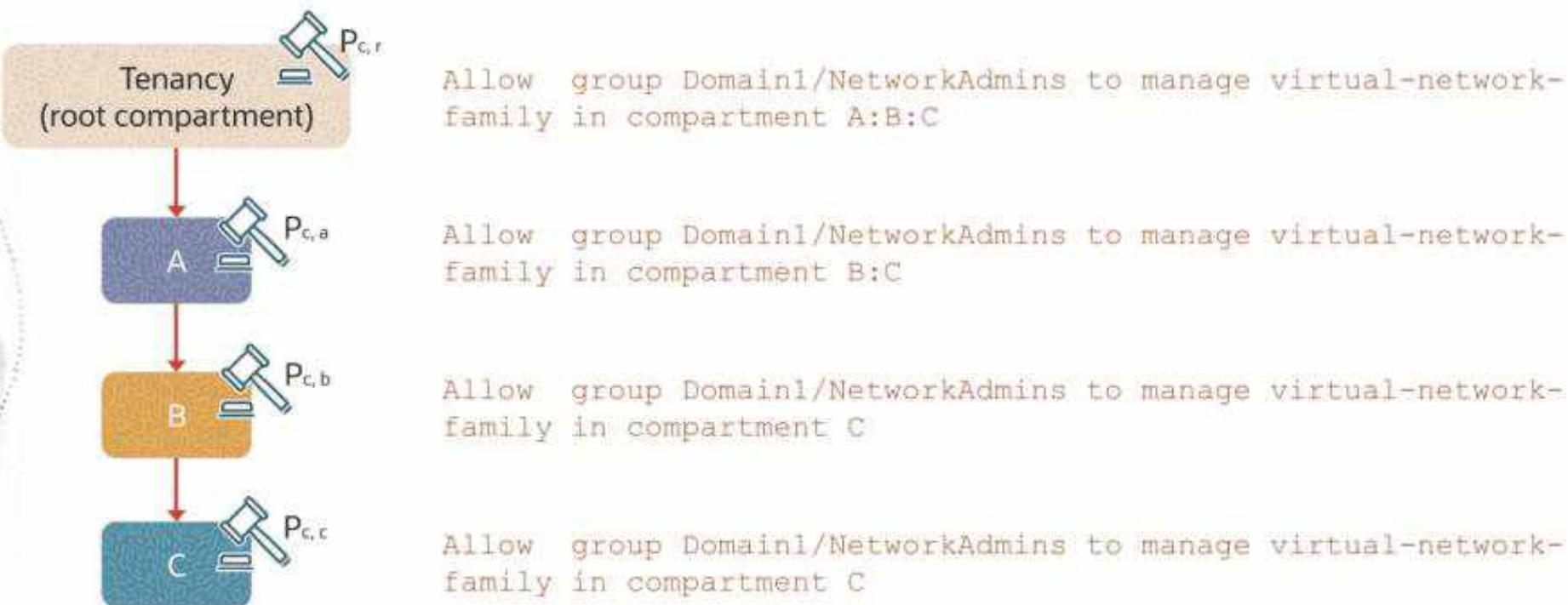


## Tenancy/Root Compartment



# Policy Attachment

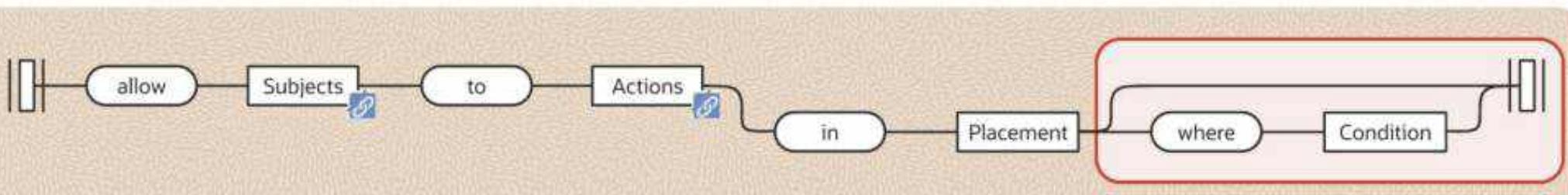
You want to create a policy to allow NetworkAdmins to manage VCNs in compartment C.



# Oracle Cloud Infrastructure Conditional Policies

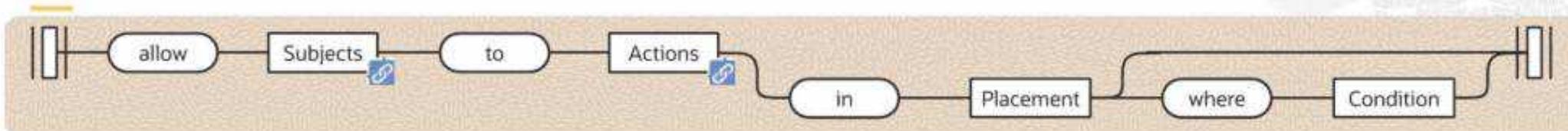
OCI Identity and Access Management (IAM)

# 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`
  - `=` or `!=` 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

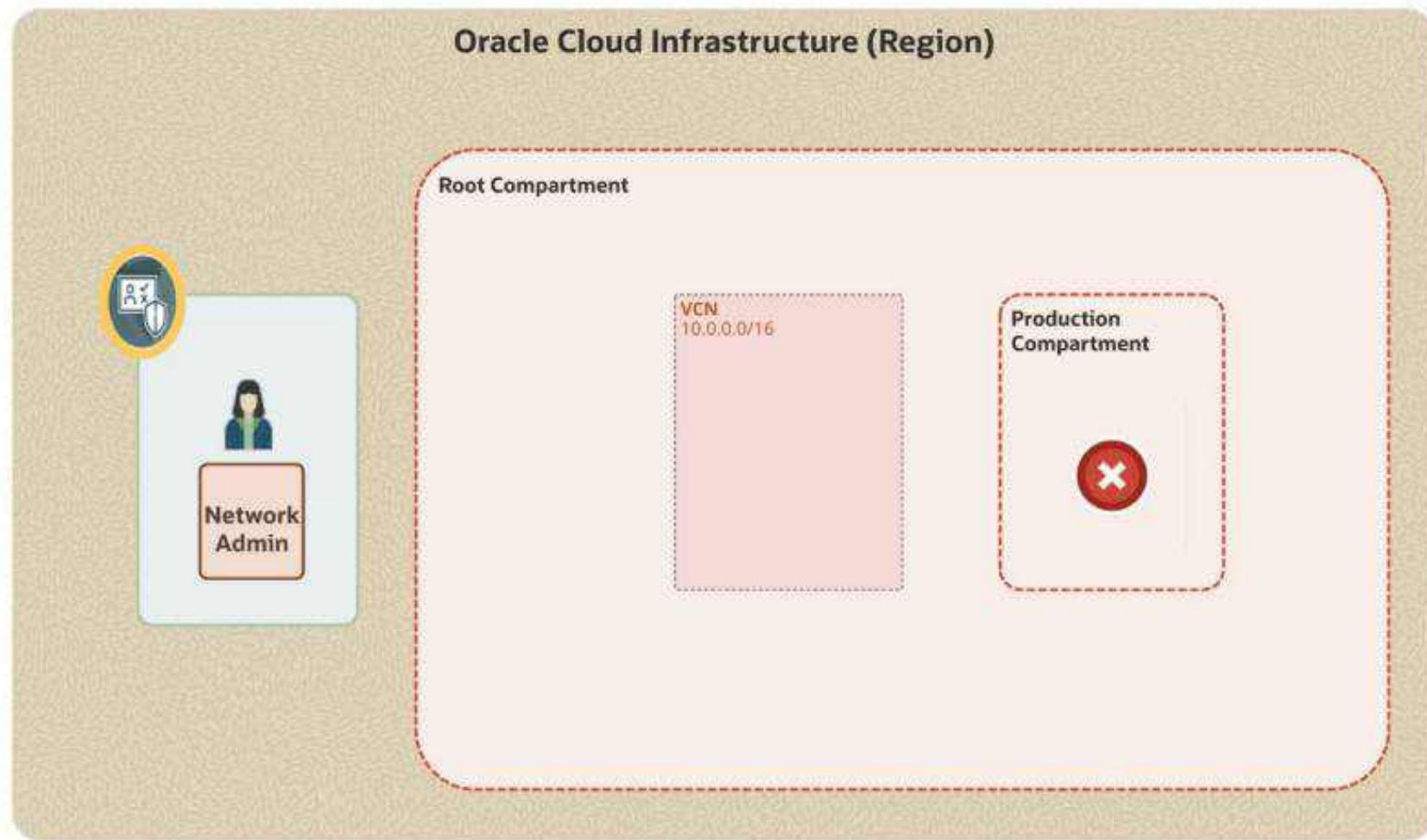
Allow group DomainA/NetworkAdmins to manage virtual-network-family in tenancy  
`where target.compartment.id != 'ocid1'`

- 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



## Oracle Cloud Infrastructure

# Enforce Least Privileged: Advanced Policies

### OCI Identity and Access Management (IAM)

# 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.{tagName space}.{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.

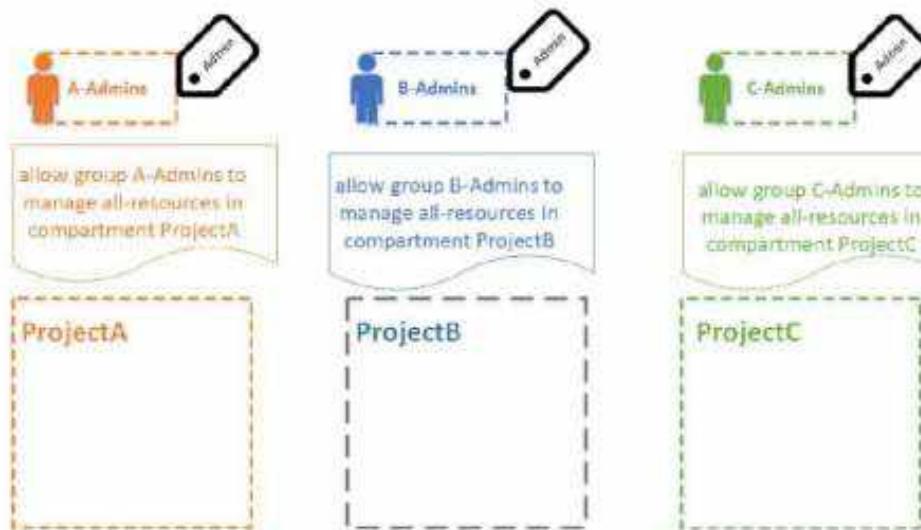
# Tag-based Access Control



Tag applied to target	Variable	Sample policy
Resource	target.resource.tag.{tagNamespace}.{tagKeyDefinition}='<value>'	<p>allow group DomainA/GroupA to manage all-resources in compartment HR where</p> <pre>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>'	<p>allow group DomainA/GroupA to manage all-resources in tenancy where</p> <pre>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

EmployeeGroup.Role='Admin'



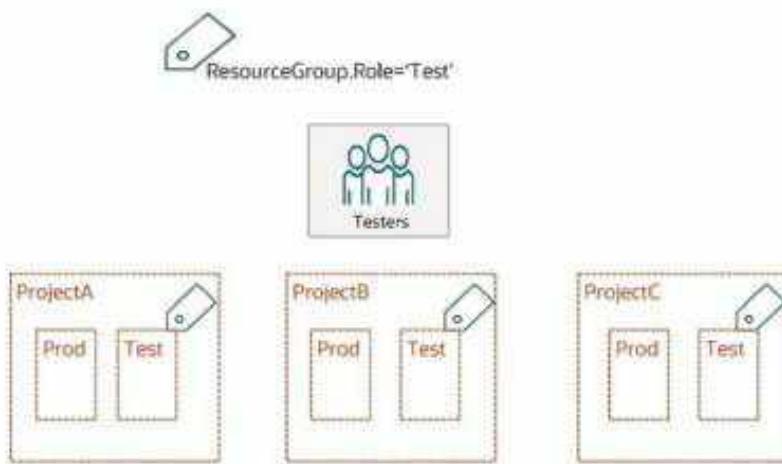
Set up a Test compartment for members of the three projects to share

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.

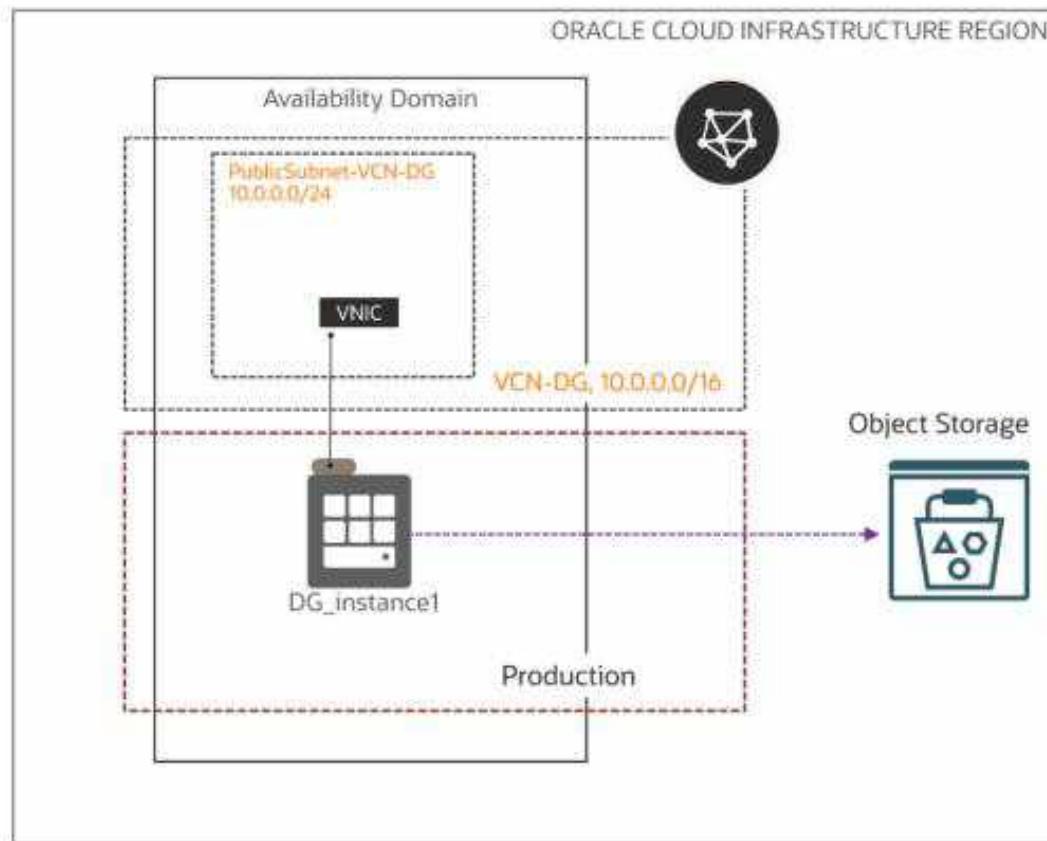
Graphics team: Pls check the font and theme for correctness. pls change the color and feel of the shapes used here to match the redwood design. Animate each components. Recreate image.

Oracle Cloud Infrastructure

# Demo: Dynamic Groups

OCI Identity and Access Management (IAM)

# Scenario: Dynamic Groups



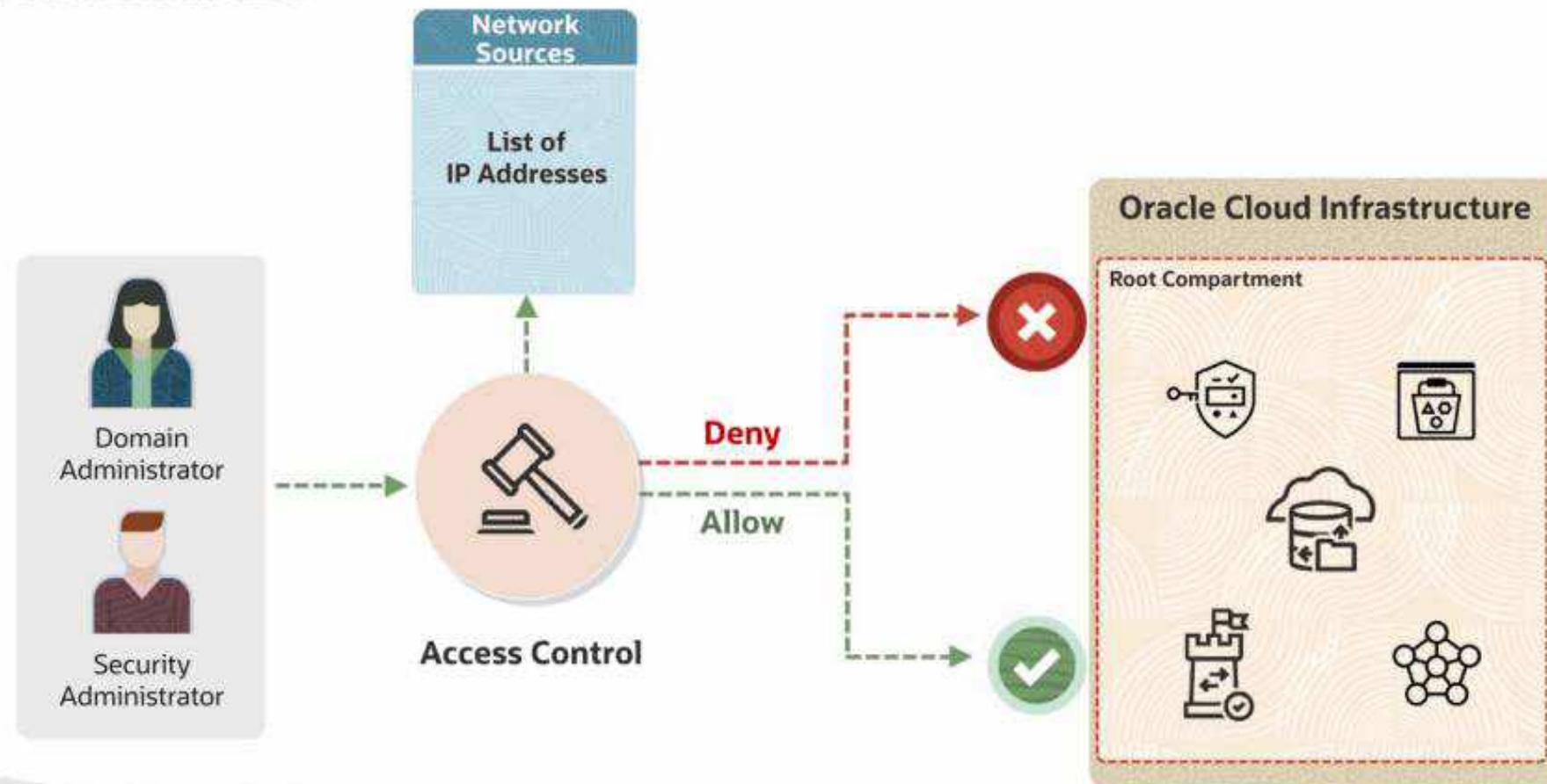
{ Any {instance.compartment.id = 'ocid'}

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

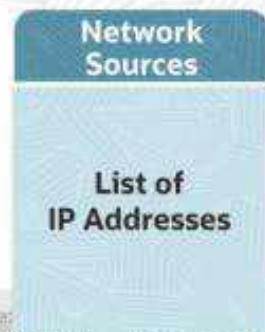
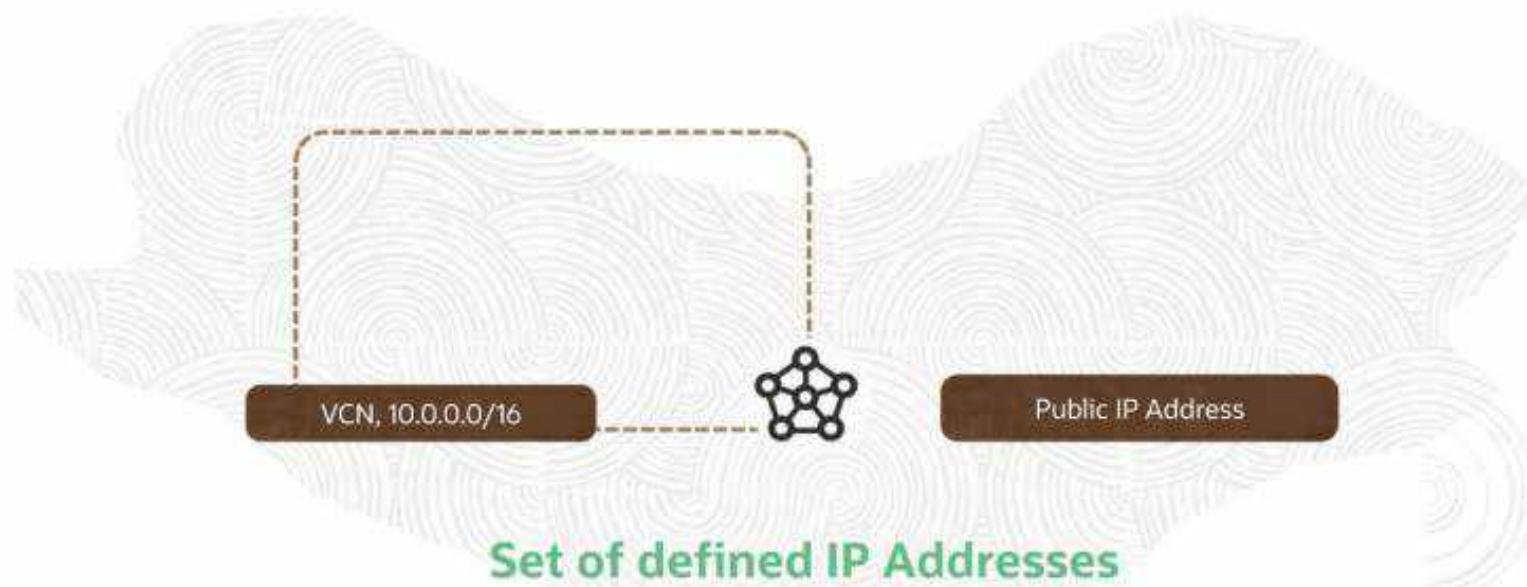
# Oracle Cloud Infrastructure Network Sources

## OCI Identity and Access Management (IAM)

# Network Sources



# Network Sources



## 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: Tag Based Access Control

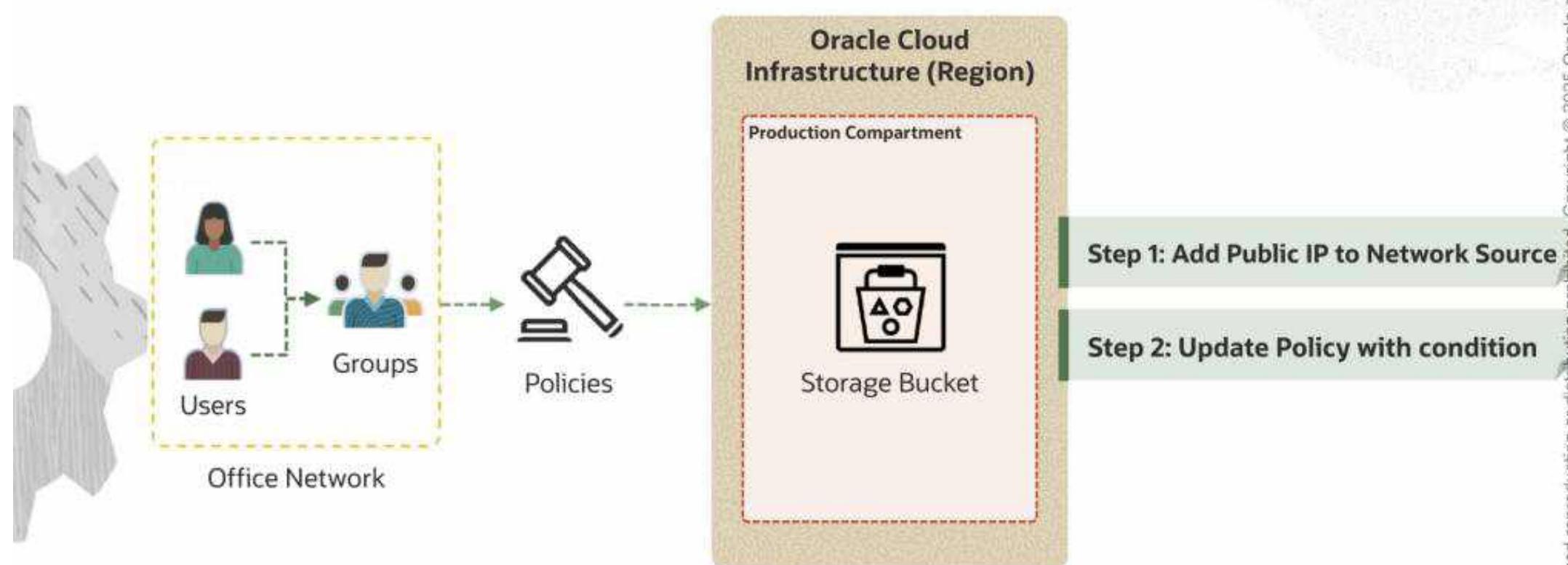
OCI Identity and Access Management (IAM)

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

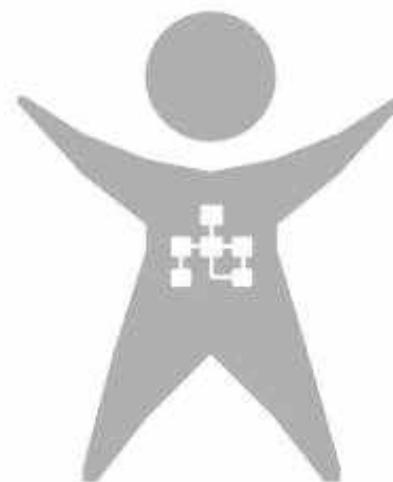
**Instance** - Represents a unique compute VM host in any OCI tenancy

**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

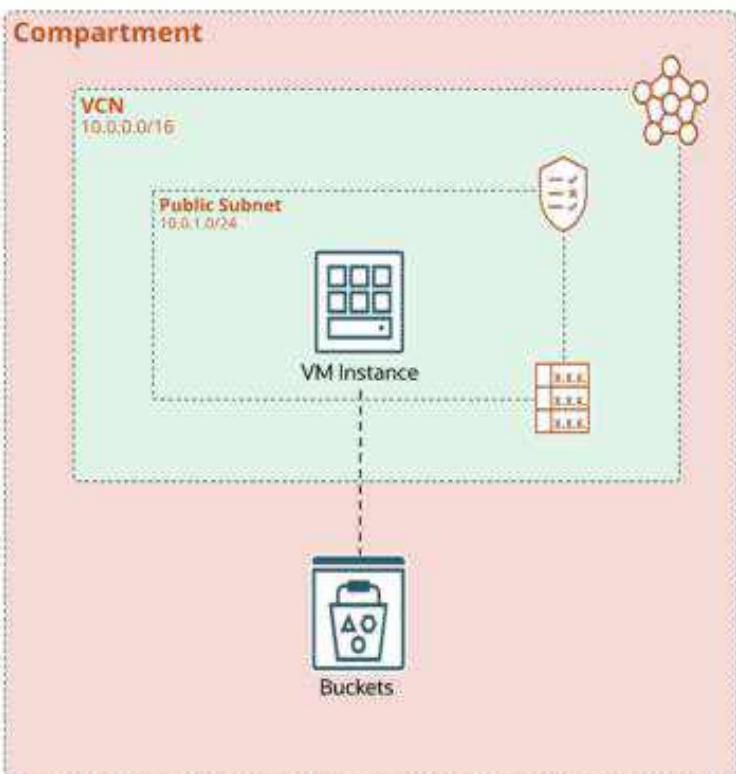


Stacked



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 temporary badge issued valid for the day.

## Key Idea

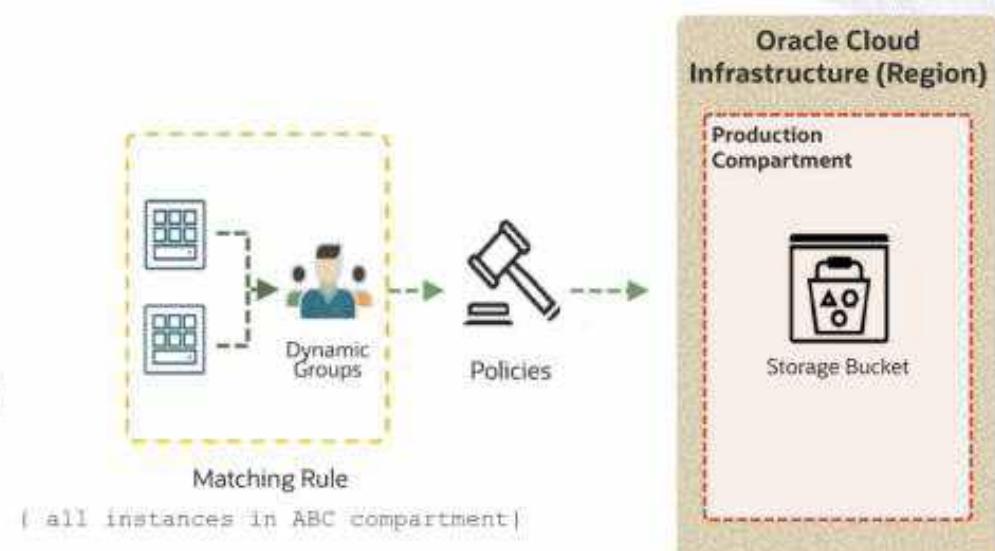
- Using injected identifiers, a service defines who the holder of a particular credential is for a short period of time.

## 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'}
```

# Security Posture

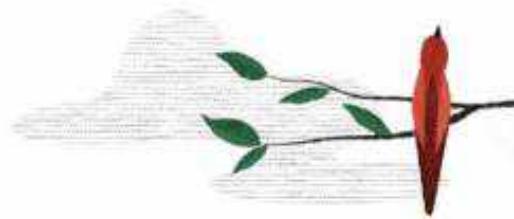
# What is Cloud Security Posture Management?

# Problem with Cloud Security



What would you say is the one of the major problems in cloud security?

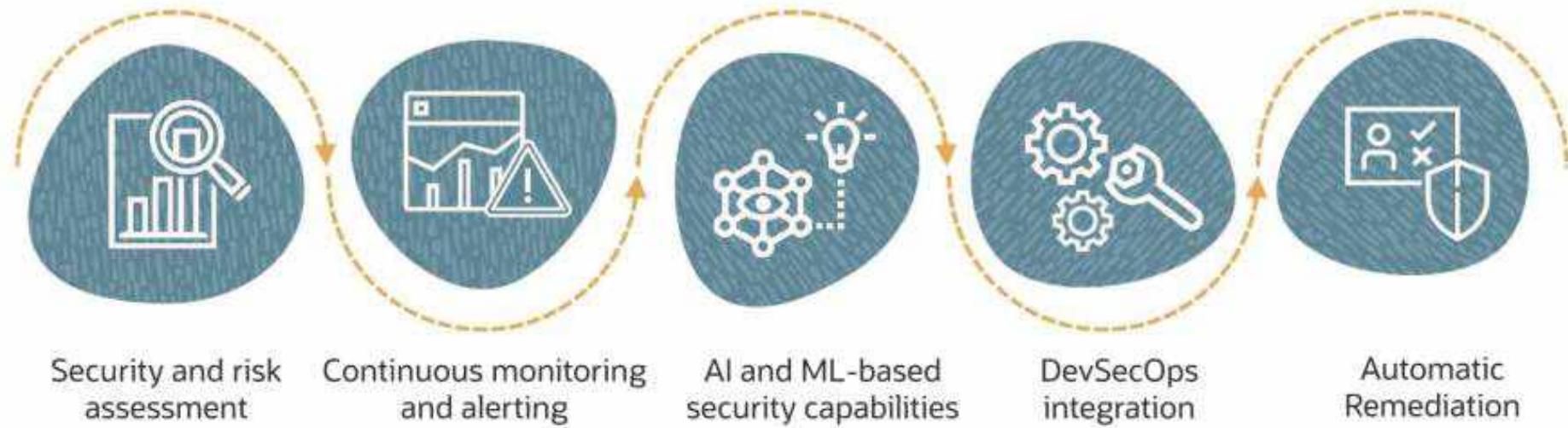
**Misconfigurations!**



# Cloud Security Posture Management (CSPM) capabilities



A continuous process of monitoring a cloud environment to improve security

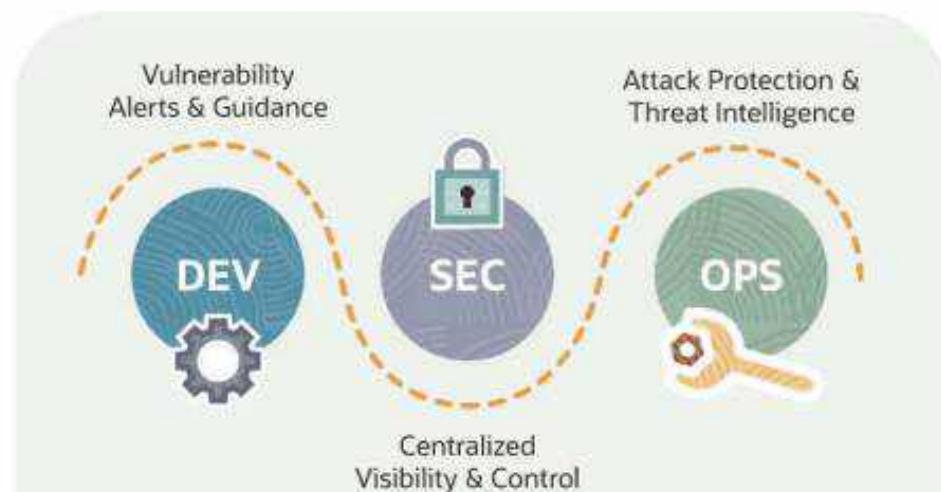


# DevSecOps



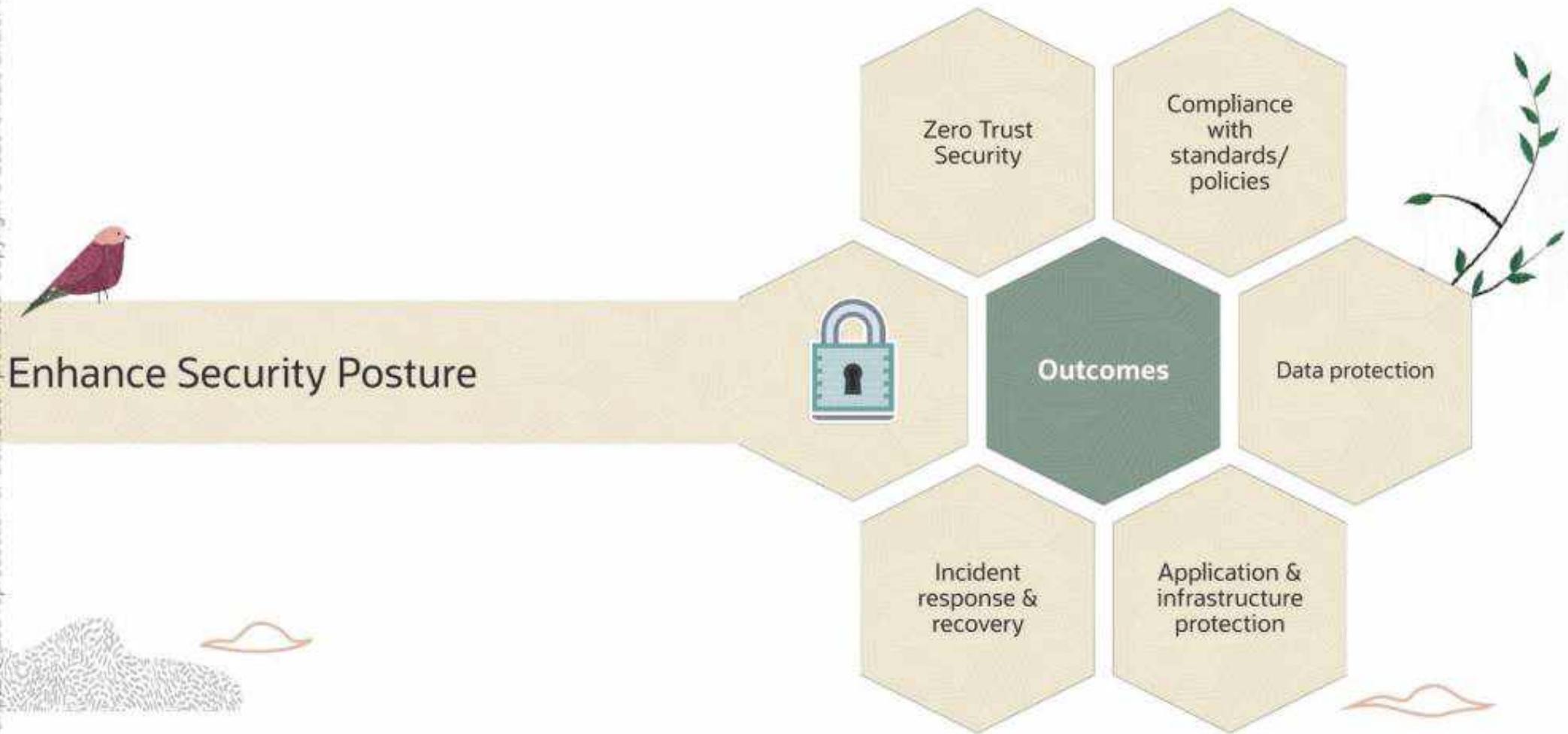
Security is a shared responsibility that is part of the entire development and operations cycle to produce applications and services.

## Automated security testing



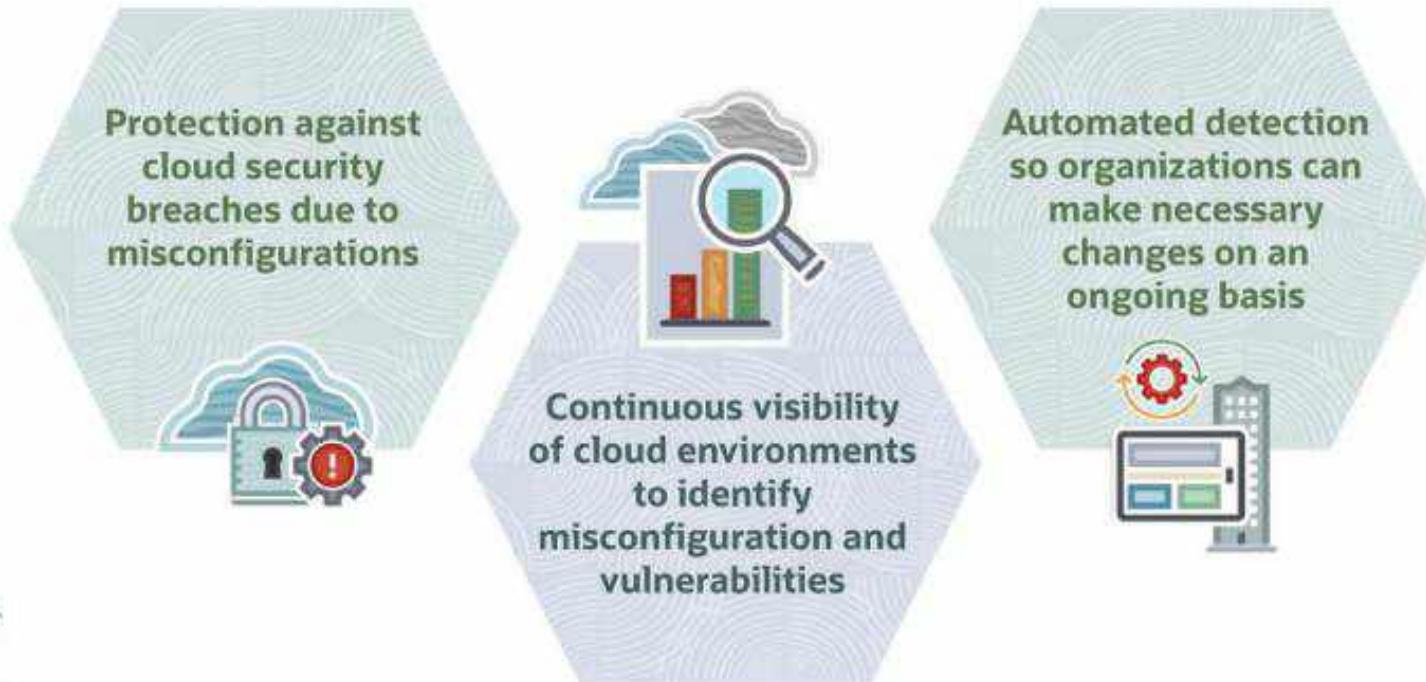
## Integrated security tooling

# Cloud Security Posture Management Outcomes



# Cloud Security Posture Management Benefits

Continuous cloud security improvement/adaptation to reduce attacks



# Cloud Guard Introduction

## OCI Security



# Cloud Guard

Detects **misconfigured resources** and **insecure activity** across tenants and provides security admins with the visibility to triage and resolve cloud security issues

ORACLE Cloud Search for resources, services, and documentation US West (San Jose) ⌂ ⓘ ⓘ

Cloud Guard

- Overview
- Problems
- Recommendations
- Targets
- Responder Activity
- Responder Recipes
- Detector Recipes
- Managed Lists
- Data Masking
- Settings

Overview

Security Score Rating ⓘ **Excellent** Security Score 98

Risk Score ⓘ **2575**

Security Recommendations ⓘ

- Resolve VCN Security List allows traffic to restricted port problems 1
- Resolve Suspicious Ip Activity problems in target sandbox-CG

[View Recommendations](#)

Problems Snapshot

34 Total

Critical	High	Medium	Low	Mitig
0	0	0	0	34

Problems

Grouped by Resource Type

Resource Type	Critical	High	Medium	Low	Mitig
Instance	0	0	0	0	34
User	0	0	0	0	34
Blockchain	0	0	0	0	34
VCN	0	0	0	0	34
Bucket	0	0	0	0	34
NSG	0	0	0	0	34
Policy	0	0	0	0	34

User Activity Problems

Responder Status

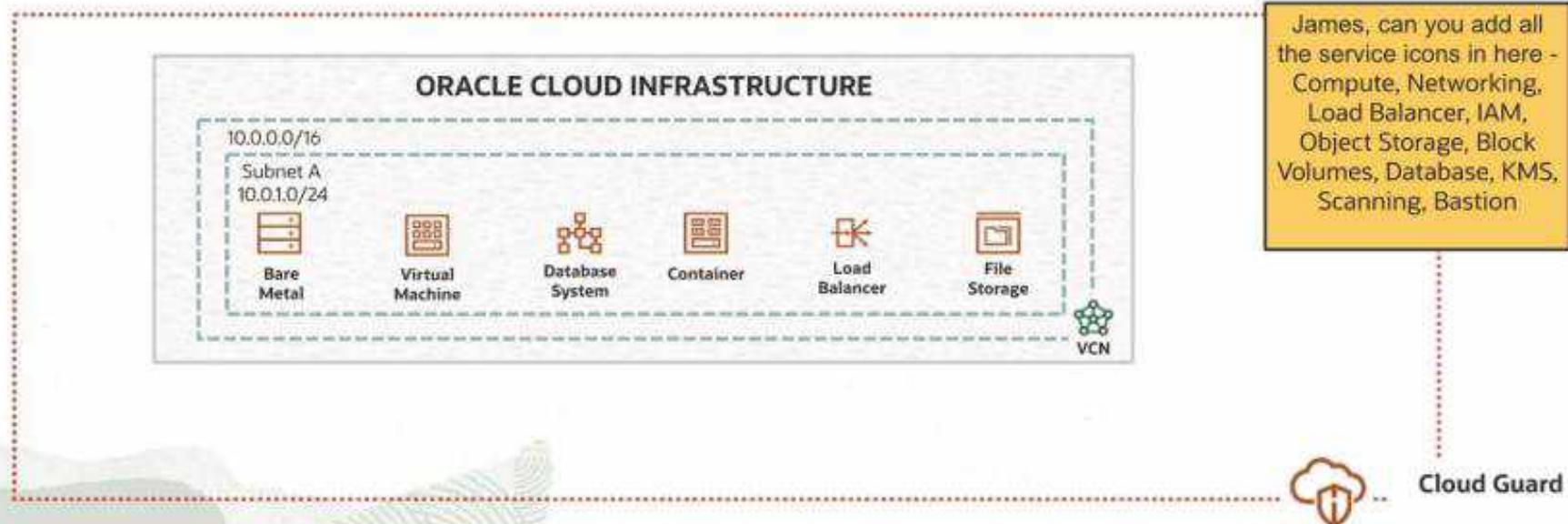
23 Total Pending

Recently Performed Remediations

Responder Name	Resource	Region	Execution Type
No items found.			

# Supported Services

Compute, Networking, Load Balancer, IAM, Object Storage, Block Volumes, Database, KMS, Scanning, Bastion



# CIS OCI Foundations Benchmark

Provides visibility into specific non-compliant CIS security configurations

- CIS\_OCI\_V1.1\_IAM
- CIS\_OCI\_V1.1\_MONITORING
- CIS\_OCI\_V1.1\_NETWORK
- CIS\_OCI\_V1.1\_OBJECTSTORAGE

Cloud Guard > Detector Recipes > Recipe Details

## Edit Detector Rule

Help

**Name:** Object Storage bucket is encrypted with Oracle-managed key

**Description:** Encryption of storage buckets provides an additional level of security on your data. Management of encryption keys is critical to protecting and accessing protected data. Some customers want to identify storage buckets encrypted Oracle-managed keys in order to apply their own key lifecycle management to the bucket. [Learn more](#).

**Status:** Enabled

**Risk Level:** Minor

**Labels:** CIS\_OCI\_V1.1\_OBJECTSTORAGE, ObjectStorage, KMS



4.2 Ensure Object Storage Buckets are encrypted with a Customer Managed Key (CMK) (Manual)

#### Profile Applicability:

- Level 2

#### Description:

Oracle Object Storage buckets support encryption with a Customer Managed Key (CMK). By default, Object Storage buckets are encrypted with an Oracle managed key.

Encryption of storage buckets provides an additional level of security on your data. Management of encryption keys is critical to protecting and accessing protected data. Some customers want to identify storage buckets encrypted Oracle-managed keys in order to apply their own key lifecycle management to the bucket.

#### Rationale:

Encryption of Object Storage buckets with a Customer Managed Key (CMK) provides an additional level of security on your data by allowing you to manage your own encryption key lifecycle management for the bucket.

#### Cloud Guard

To Enable Cloud Guard Auditing:

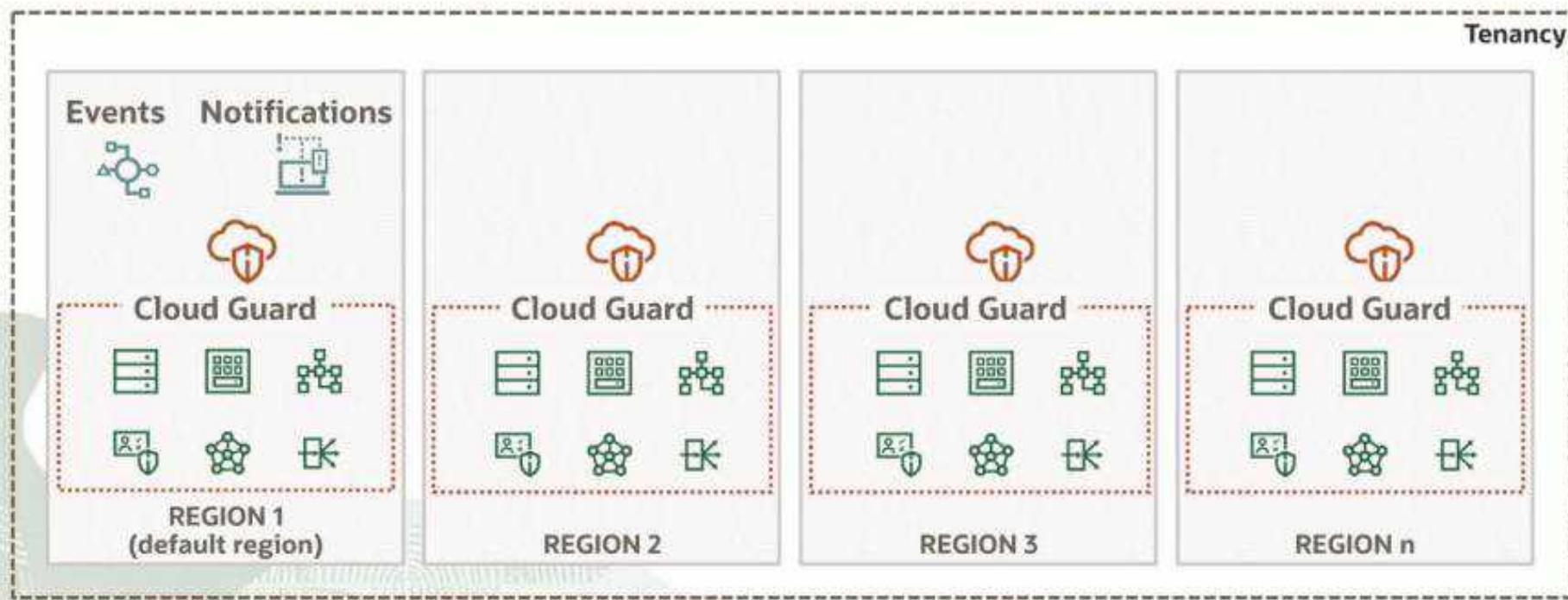
Ensure Cloud Guard is enabled in the root compartment of the tenancy. For more information about enabling Cloud Guard, please look at the instructions included in Recommendation 3.15.

#### From Console:

1. Type `cloud_guard` into the Search box at the top of the Console.
2. Click `Cloud Guard` from the "Services" submenu.
3. Click `Detector Recipes` in the Cloud Guard menu.
4. Click `OCI Configuration Detector Recipe (Oracle Managed)` under the Recipe Name column.
5. Find `Object Storage bucket is encrypted with Oracle-managed key` in the Detector Roles column.
6. Verify that the `Object Storage bucket is encrypted with Oracle-managed key` Detector Rule is Enabled.

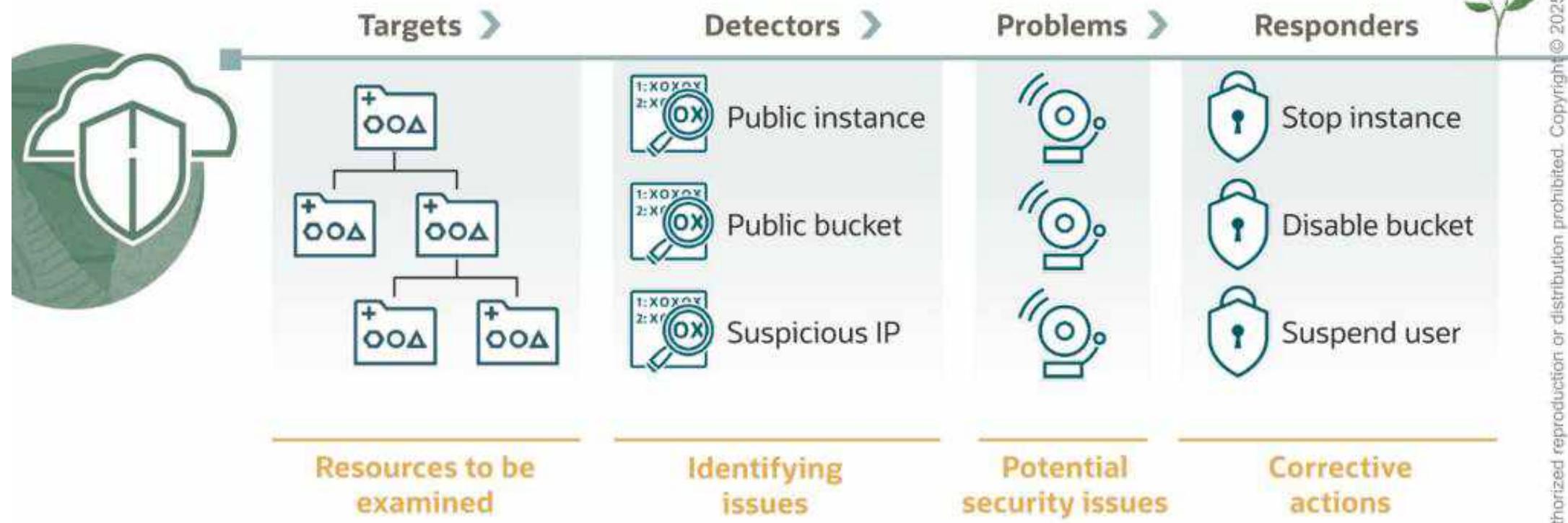
# Reporting Region

Targets in all regions can be monitored, though the reporting region is the default region of the tenancy. Integration with Events and Notification services happen only in the Reporting Region.



# Cloud Guard Concepts

# Cloud Guard: Overview



# Cloud Guard Concepts: Targets and Detectors



## Target

Sets the scope of resources to be examined

Consists of compartments and sub-compartments

## Targets

Targets identify a compartment to be monitored by Cloud Guard. [Learn More](#)

<input type="checkbox"/>	Target Name	Compartment	Recipes	Created	
<input type="checkbox"/>	C06_CG	C06	2	19 hours ago	

## Detector

Identifies issues with resources or user actions and alerts when an issue is found

Configuration and Activity detectors

Detector recipes consist of rules



## Detector Recipes

To create your own recipe, clone an existing Oracle managed recipe from the root compartment. [Learn More](#)

<input type="checkbox"/>	Recipe Name	Oracle Managed	Type	Created	
<input type="checkbox"/>	OCI Configuration Detector Recipe (Oracle Managed)	Yes	Configuration	20 days ago	
<input type="checkbox"/>	OCI Activity Detector Recipe (Oracle Managed)	Yes	Activity	20 days ago	
<input type="checkbox"/>	Custom Configuration Detector	No	Configuration	19 hours ago	

# Cloud Guard Concepts: Detector Rules and Recipes



## Detector rules

Provide a specific definition of a class of resources, with specific actions or configurations, that cause a detector to report a problem.

## Detector recipes (collection of detector rules)

Provide the baselines for examining the resources and activities in the target.

### Detector Rules

<input type="checkbox"/> Detector Rules	Risk Level	Status	Settings Configured	Conditional Group	<input type="checkbox"/> Filter by detector rule
<input type="checkbox"/> API key is too old	Medium	Enabled	Yes	No	
<input type="checkbox"/> Block Volume is encrypted with Oracle-managed key	Medium	Enabled	Not Allowed	No	
<input type="checkbox"/> Block Volume is not attached	Medium	Enabled	Not Allowed	No	
<input type="checkbox"/> Bucket is public	Critical	Enabled	Not Allowed	No	

Description: Object Storage supports anonymous, unauthenticated access to a bucket. A public bucket that has read access enabled for anonymous users allows anyone to obtain object metadata, download bucket objects, and optionally list bucket contents.

Associated Responders: Make Bucket Private

# Cloud Guard Concepts: Problems and Responders

## Problem

Any action or setting on a resource that could potentially cause a security threat

### Problems

A problem is any action or setting on a resource that could potentially cause a security threat. All list scope and filter settings are persistent and in place until they are cleared or reset. [Learn More](#)

<input type="checkbox"/> Problem Name	Risk Level	Detector Type	Resource	Target
VCN Security List allows traffic to restricted port	Critical	Configuration	vnclt-1	CSE_CG
Bucket is public	Critical	Configuration	publicbucket	CSE_CG
VCN Security List allows traffic to restricted port	Critical	Configuration	vnclt-1	CSE_CG
Database is not backed up automatically	High	Configuration	pitchb-	CSE_CG

## Responder

A corrective action that Cloud Guard can take when a detector has identified a problem

### Responder Recipes

To create your own recipe, clone an existing Oracle managed recipe from the root compartment [Learn More](#).

<input type="button" value="Clone"/>	<input type="checkbox"/> Filter by recipe name
Recipe Name	Oracle Managed
OCI Responder Recipe (Oracle Managed)	Yes



# Cloud Guard Concepts: Responder Rules and Recipes

## Responder rules

Define the specific actions to take. If any one responder rule is triggered, it triggers the responder

## Responder recipes (collection of responder rules)

Define the action or set of actions to take in response to a problem that a detector identified

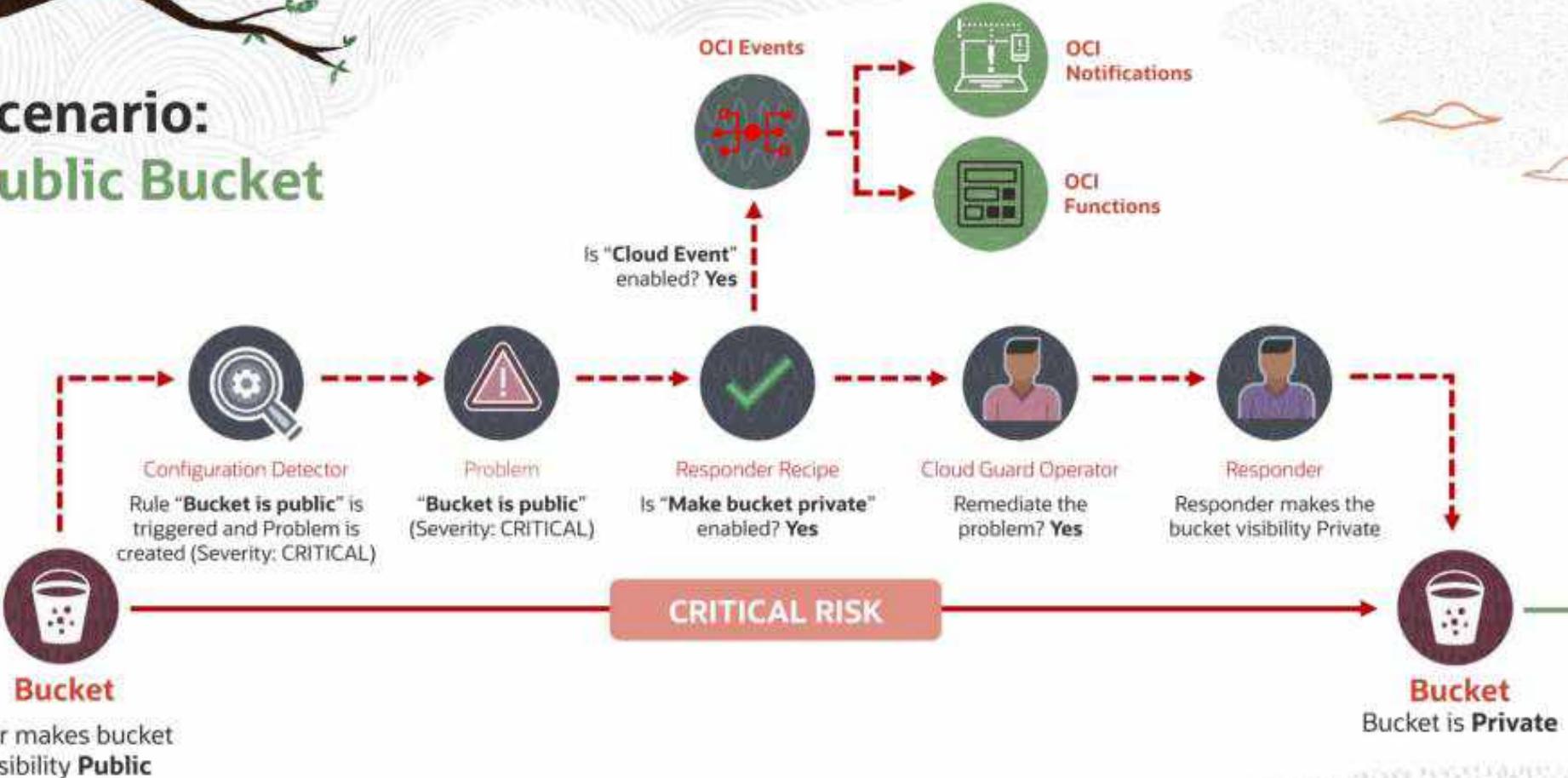
### Responder Rules

<input type="checkbox"/>	Responder Rules	Type	Status	Conditional Group		
<input type="checkbox"/>	Cloud Event	NOTIFICATION	Enabled	No		
<input type="checkbox"/>	Delete IAM Policy	REMEDIATION	Enabled	No		
<input type="checkbox"/>	Delete Internet Gateway	REMEDIATION	Enabled	No		<input checked="" type="checkbox"/>

Description: Deletes Internet Gateway associated with a VCN  
Configuration: Post Remediation Notification: Enabled

# Cloud Guard Problems

## Scenario: Public Bucket



# Cloud Guard Concepts: Problems



## Problems can be:

**Remediated:** Fixed by using Cloud Guard responder

**Resolved:** Fixed by other processes

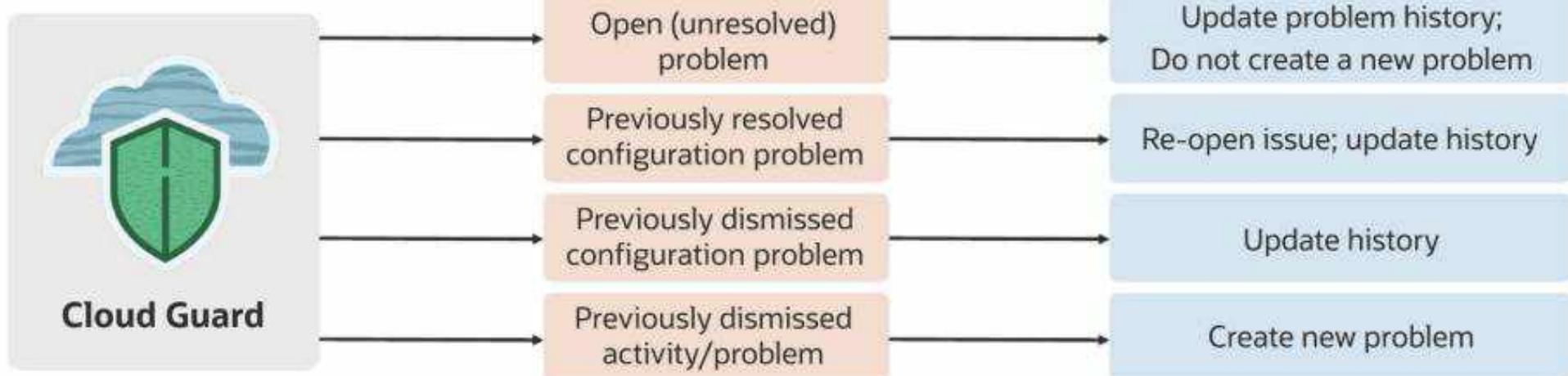
**Dismissed:** Ignored/closed



### Database is not backed up automatically

Enabling automatic backup ensures that you will be able to restore the database

[Remediate](#) [Mark as Resolved](#) [Dismiss](#)





## Processing Reported Problems

Is at the core of Cloud Guard functionality

Involves prioritizing problems to focus on highest risks.

### Overview page:

#### Problems

A problem is any action or setting on a resource that could potentially cause a security threat. You can clear or reset. [Learn More](#).

<input type="checkbox"/> Problem Name	Risk Level
<a href="#">VCN Security list allows traffic to restricted port</a>	Critical
<a href="#">Bucket is public</a>	Critical
<a href="#">VCN Security list allows traffic to restricted port</a>	Critical
<a href="#">Database is not backed up automatically</a>	High
<a href="#">Instance has a public IP address</a>	High
<a href="#">Database System has public IP address</a>	High
<a href="#">Instance has a public IP address</a>	High

# Processing Reported Problems

Examines problem details to determine what's happening

## Problem page



A screenshot of a Cloud Guard Problem Details page. At the top left is a large red square icon with a white letter 'P' and the word 'OPEN' below it. To the right, the title 'Database is not backed up automatically' is displayed in bold. Below the title is a descriptive text: 'Enabling automatic backup ensures that you will be able to restore the database with minimal data loss, if there is a catastrophic hardware failure.' A horizontal button bar follows, containing 'Home' (highlighted in blue), 'Mark as Resolved', and 'Dismiss'. Underneath, there are two main sections: 'General Information' and 'Recommendation'. The 'General Information' section lists: Problem OCID: mAjycuApq, Status: Open, Detector Type: Configuration, Resource Name: pth, Risk Level: High, and Resource Type: DB System. The 'Recommendation' section contains the instruction: 'Ensure that automatic backup is enabled.'

Resolves each problem to ensure that risks are countered  
and “false alarms” do not continue in the future

## Responder Activity page

Responder Activity					
Responders related to this problem					
Responder Name	Time Updated	Activity	Responder Execution Status	Comment	
Cloud Event	Tue, Feb 23, 2021, 09:27:11 UTC	Completed	<span style="color: green;">●</span> Succeeded	Successfully responded	
Enable DB Backup	Tue, Feb 23, 2021, 09:27:11 UTC	Started	<span style="color: yellow;">●</span> Awaiting input	Automatically Triggered	
Cloud Event	Tue, Feb 23, 2021, 09:27:11 UTC	Started	<span style="color: green;">●</span> Succeeded	Automatically Triggered	

# Cloud Guard – Manage Detector Recipes

# Detector Rules and Recipes

---

- A detector is a Cloud Guard component that identifies potential security problems, based **on resource configuration or activity**.
- Detector rules are combined into a Detector Recipe.
- Cloud Guard supports two types of detector recipes:
  - Oracle-Managed recipes are provided by Oracle and you can't modify them.
  - User-Managed recipes are created by cloning an Oracle-managed recipe. You can modify user-managed recipes as needed.

# Configuration Detector Rules (Oracle-Managed)



## Compute Resources

- + Instance has a public IP address
- + Instance is publicly accessible
- + Instance is running on Oracle public image
- + Instance is running without required Tags

## Database Resources

- + Database is not backed up automatically
- + Database patch is not applied
- + Database System has public IP address
- + Database System is publicly accessible
- + Database System patch is not applied
- + Database System version is not sanctioned
- + Database version is not sanctioned

## Networking Resources

- + Load balancer allows weak cipher suites
- + Load balancer allows weak SSL communication
- + Load balancer has no backend set
- + Load balancer has no inbound rules or listeners
- + Load balancer SSL certificate expiring soon
- + NSG egress rule contains disallowed IP/port
- + NSG ingress rule contains disallowed IP/port
- + VCN has Internet Gateway attached
- + VCN has Local Peering Gateway attached
- + VCN has no inbound Security List
- + VCN Security list allows traffic to non-public port from all sources (0.0.0.0/0)
- + VCN Security list allows traffic to restricted port
- + VNIC without associated network security group

# Activity Detector Rules (Oracle-managed)



## IAM Resources

- + IAM API keys created
- + IAM API keys deleted
- + IAM Auth Token created
- + IAM Auth Token deleted
- + IAM Customer Keys created
- + IAM Customer Keys deleted
- + IAM Group created
- + IAM Group deleted
- + IAM OAuth 2.0 credentials created
- + IAM OAuth 2.0 credentials deleted
- + IAM User capabilities modified
- + IAM User created
- + IAM User UI password created or reset
- + Security policy modified

## Networking Resources

- + DRG attached to a VCN
- + DRG created
- + DRG deleted
- + DRG detached from a VCN
- + Subnet changed
- + Subnet deleted
- + VCN created
- + VCN deleted
- + VCN DHCP Option changed
- + VCN Internet Gateway created
- + VCN Internet Gateway terminated
- + VCN Local Peering Gateway changed
- + VCN Network Security Group deleted

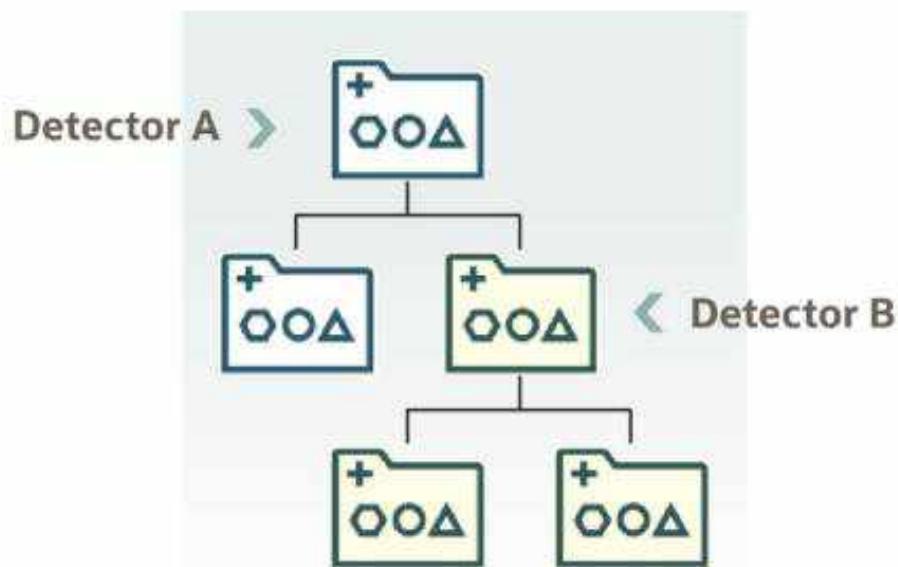
## Compute Resources

- + Export Image
- + Import Image
- + Instance terminated
- + Update Image

## Database Resources

- + Database System terminated

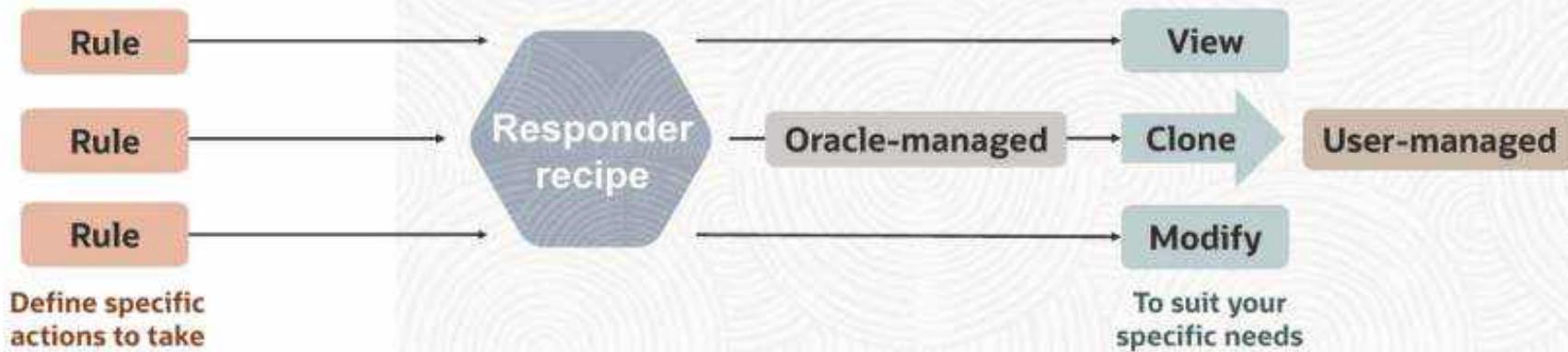
# Compartment Inheritance



- Apply detector recipes to compartments.
- Detector A applies to all compartments in the hierarchy.
- When a compartment hierarchy has detector recipes applied to a compartment at a different level, whenever the rules conflict, the rules from the detector recipe applied at a lower level override the rules from any applied at a higher level.
- Detector B applies to the compartments shaded and rules override.

# Cloud Guard Responder Recipes

# Managing Responder Recipes



# Managing Responder Recipes



Cloud Guard > Responder Recipes > Recipe Details

## OCI Responder Recipe (Oracle Managed)

This is an Oracle managed Oracle Cloud Infrastructure recipe with notification and remediation responder rules. To create your own recipe, clone an existing Oracle managed recipe from the root compartment. [Learn More](#).

[Clone](#)

[Details](#)

OCID: zwcwzvqf8 Show Copy  
Created: Wed, Feb 10, 2021, 11:39:57 UTC  
Compartment: ocusvcstrng6 (root)

**Resources**

**Responder Rules**

	Responder Rules	Type	Status	Conditional Group
<input type="checkbox"/>	Cloud Event	NOTIFICATION	Enabled	No
<input type="checkbox"/>	Delete IAM Policy	REMEDIATION	Enabled	No
<input type="checkbox"/>	Delete Internet Gateway	REMEDIATION	Enabled	No
Description: Deletes Internet Gateway associated with a VCN Configuration: Post Remediation Notification: Enabled Conditional Group: None				
<input type="checkbox"/>	Delete Public IP(s)	REMEDIATION	Enabled	No



# Managed Lists

## Reusable list of parameters

Set the scope for detector and responder rules

Apply configurations to detectors

## Trusted Oracle IP address space

All the Oracle IP addresses that you want to regard as trusted when you define rules for detectors and responders

## Your own managed lists

Cloud Guard lets you define your own managed lists as needed under different categories

# Managed Lists

**Cloud Guard**

## Managed Lists

Managed lists provide a centralized location for detector rule configuration. You can define a list one time and use it in multiple rules. [Learn More](#)

List Name	Type	Total Entries	Feed Provider	Created
Oracle CloudGuard CIDR Managed List	CIDR Block	184	Oracle	19 days ago

Showing 1 item < 1 of 1 >

**Create Managed List**

**Basic Information**

Lists are used to provide the same value across multiple rules.

**List Name:** CustomManagedList

**Description:** (Optional) Enter a description.

**Commitment Assignment:**  `ocid1.list@1 (list)`

**List Type:** Choose One

- Choose One
- CIDR Block
- City
- Country
- Generic List
- Groups
- IPv4 Address
- IPv6 Address
- Region
- Resource OCID
- State or Province
- Tags
- Users

**Next** **Cancel**

# Cloud Guard Notifications

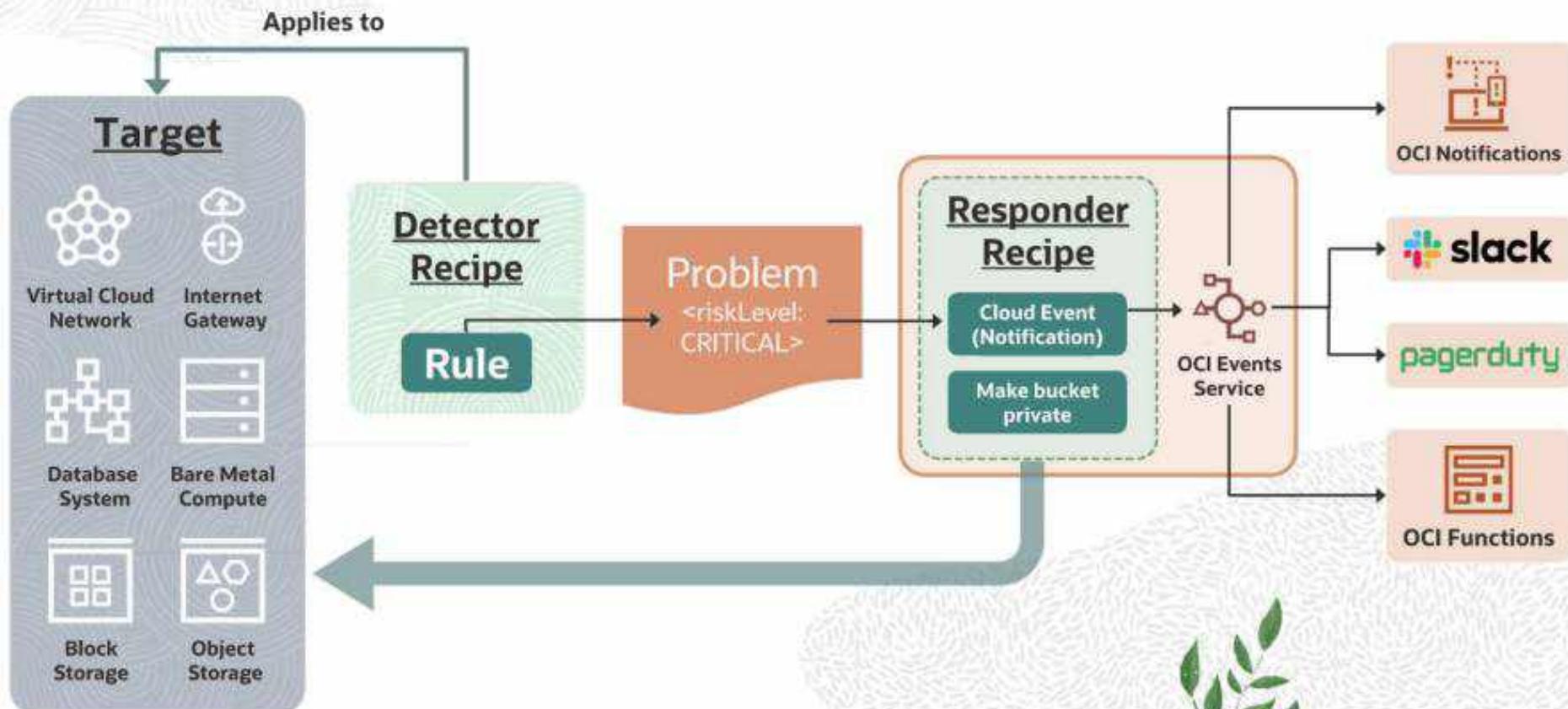


## Cloud Guard Notifications

- Use OCI Events and Notifications services to send notifications, whenever Cloud Guard detects a problem for which you want to be notified.
- The Notification Responder Cloud Event can emit problem details to the Events Service.
- The Cloud Event responder rule is part of the responder recipe, which must be attached to the corresponding targets.
- Set up Events and Notifications from your Cloud Guard Reporting region, which aggregates problems from the monitored regions, and send out the Cloud Event from the Reporting region.
- The compartment you select for the event rule must be either the one where the resource exists, or a parent of that compartment.
- If you are processing problems entirely within Cloud Guard, you do not need to configure notifications.



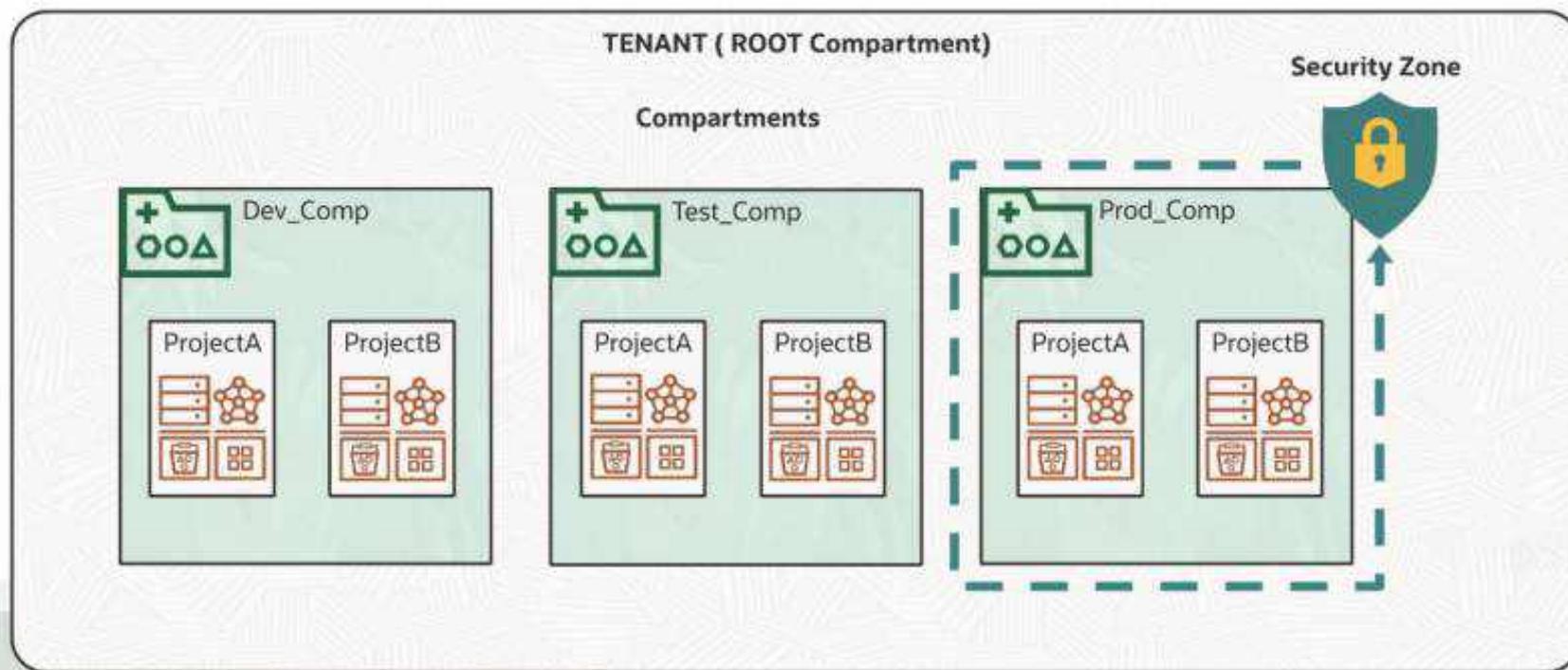
# Integration with Events and Notification Services



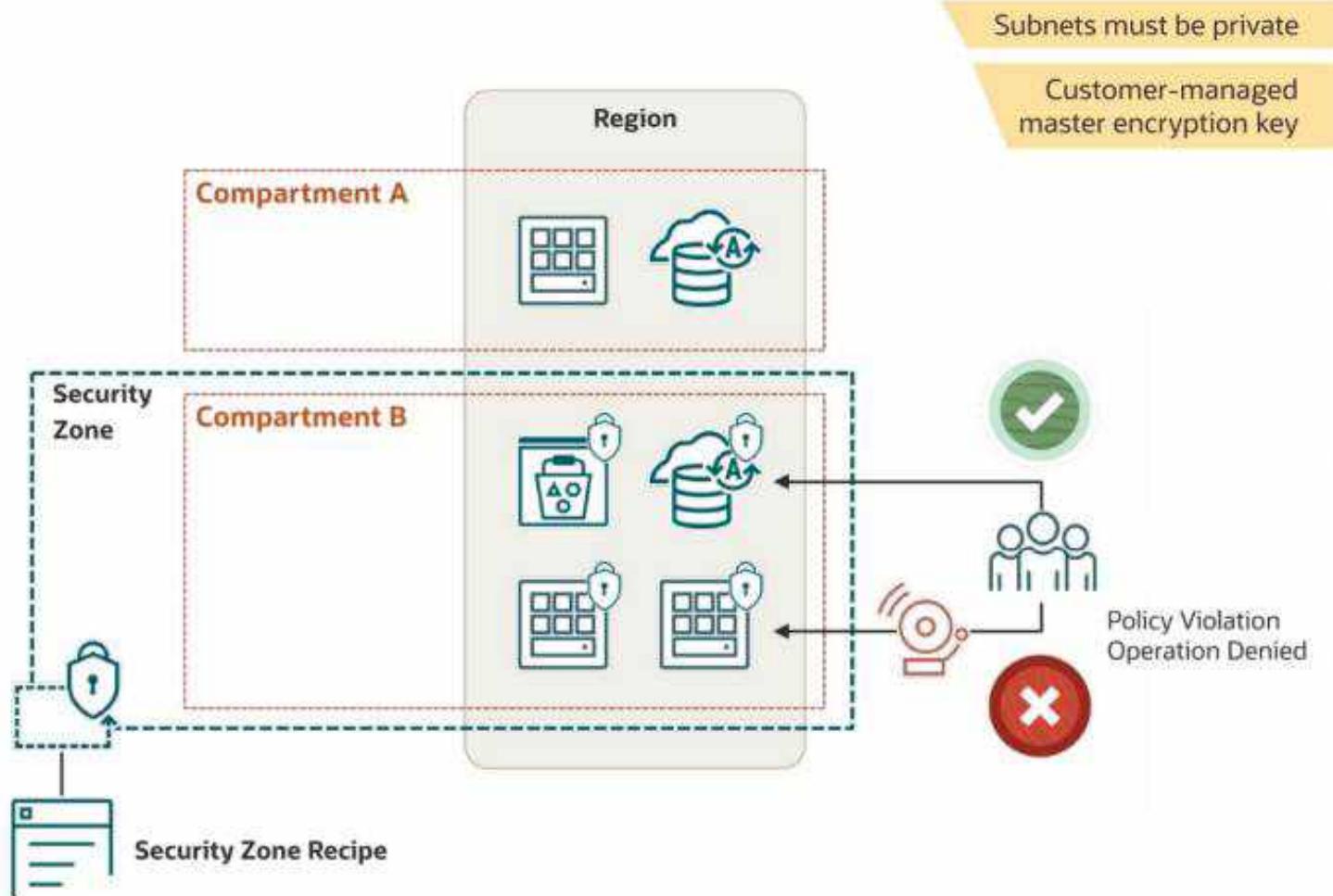
# Security Zones and Security Advisor

# Security Zones

Proactively enforce security policies on OCI resources in a compartment



# Security Zones



# Security Zone Concepts

- Security Zone
  - An association between a compartment and a security zone recipe
- Security Zone Recipe
  - A collection of security zone policies
- Security Zone Policy
  - A security requirement for resources in a security zone
- Policy validation for resource tasks
  - If a policy is violated, then the operation is denied.

The screenshot shows the Oracle Cloud Infrastructure Security Zones interface. At the top, there's a navigation bar with 'Security Zones > Recipes > Recipe Details'. Below it is a large green circular icon with a white 'R' and the word 'ACTIVE' underneath. To the right, there's a section titled 'Maximum Security Recipe - 20200914' with a 'Details' button and an 'OCIO: ...' link. Underneath this is a 'Policies' section with a 'Policy Statement' table containing ten rows of DENY statements for various volume operations. On the left side, there are tabs for 'Resources' and 'Policies', and a 'Associated Security Zones' section.

Policy Statement
DENY ATTACHED_BLOCK_VOLUME_NOT_IN_SECURITY_ZONE_MOVE_TO_COMPARTMENT_IN_SECURITY_ZONE
DENY ATTACHED_BOOT_VOLUME_NOT_IN_SECURITY_ZONE_MOVE_TO_COMPARTMENT_IN_SECURITY_ZONE
DENY BLOCK_VOLUME_IN_SECURITY_ZONE_ATTACH_TO_INSTANCE_NOT_IN_SECURITY_ZONE
DENY BLOCK_VOLUME_IN_SECURITY_ZONE_MOVE_TO_COMPARTMENT_NOT_IN_SECURITY_ZONE
DENY BLOCK_VOLUME_NOT_IN_SECURITY_ZONE_ATTACH_TO_INSTANCE_IN_SECURITY_ZONE
DENY BLOCK_VOLUME_WITHOUT_VAULT_KEY
DENY BOOT_VOLUME_IN_SECURITY_ZONE_ATTACH_TO_INSTANCE_NOT_IN_SECURITY_ZONE
DENY BOOT_VOLUME_IN_SECURITY_ZONE_MOVE_TO_COMPARTMENT_NOT_IN_SECURITY_ZONE
DENY BOOT_VOLUME_NOT_IN_SECURITY_ZONE_ATTACH_TO_INSTANCE_IN_SECURITY_ZONE
DENY BOOT_VOLUME_WITHOUT_VAULT_KEY



Restrict  
Resource  
Movement

Deny Public  
Access

Restrict  
Resource  
Association

Ensure Data  
Security

Require  
Encryption

Use Oracle  
Approved  
Configuration

Ensure Data  
Durability



## Security Advisor



### Secure Object Storage Buckets

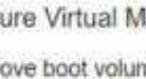
Improve data security by creating a bucket and encrypting it with a key that you manage.



### Secure File Systems

Improve file storage security by creating a file system and encrypting it with a key that you manage.

[Create Secure File System](#)



### Secure Virtual Machine Instances

Improve boot volume security by creating a virtual machine instance and encrypting the attached boot volume with a key that you manage.



[Create Secure Instance](#)

### Secure Block Volumes

Improve data security by creating a block volume and encrypting it with a key that you manage.

[Create Secure Block Volume](#)



# Billing and Licensing



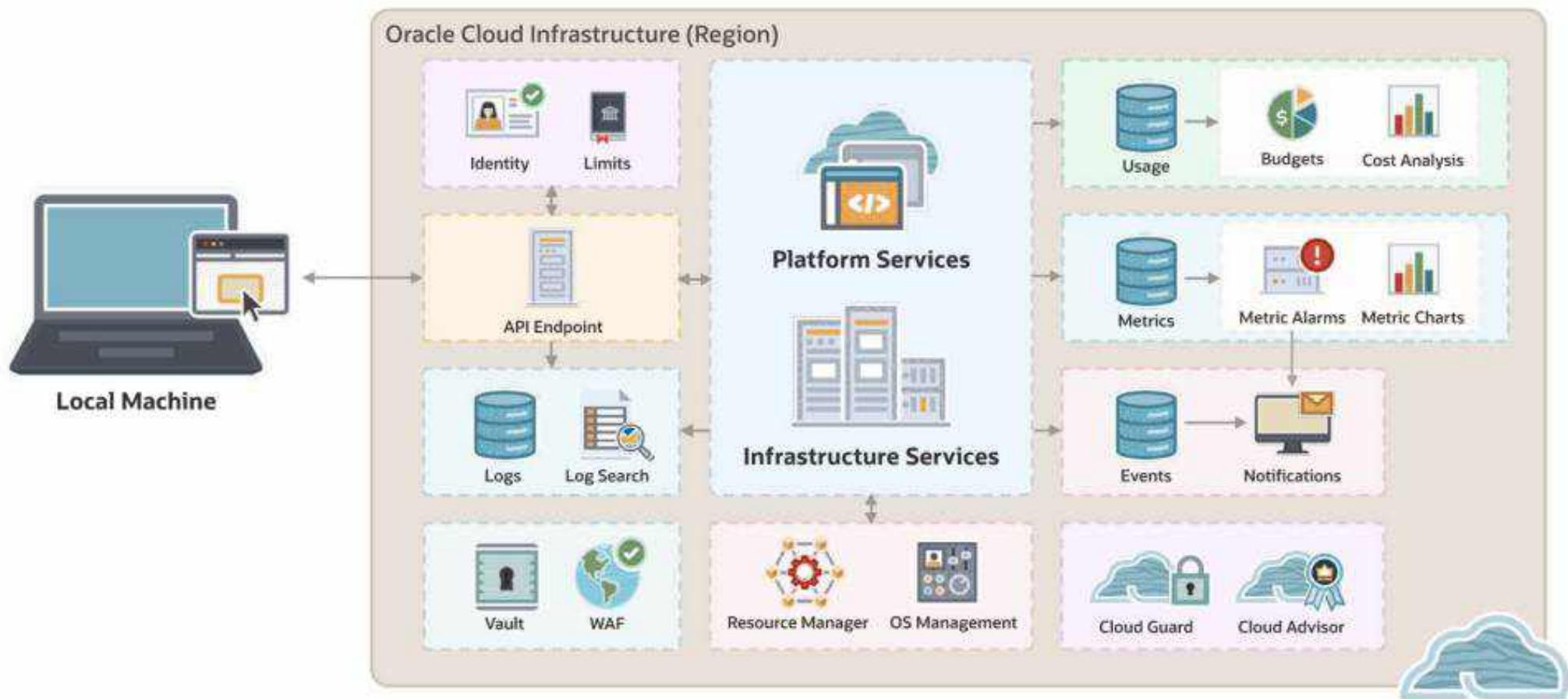
## Oracle Cloud Infrastructure

# Manage Cost with Budgets and Budget Alerts

### Automated Email Alerts

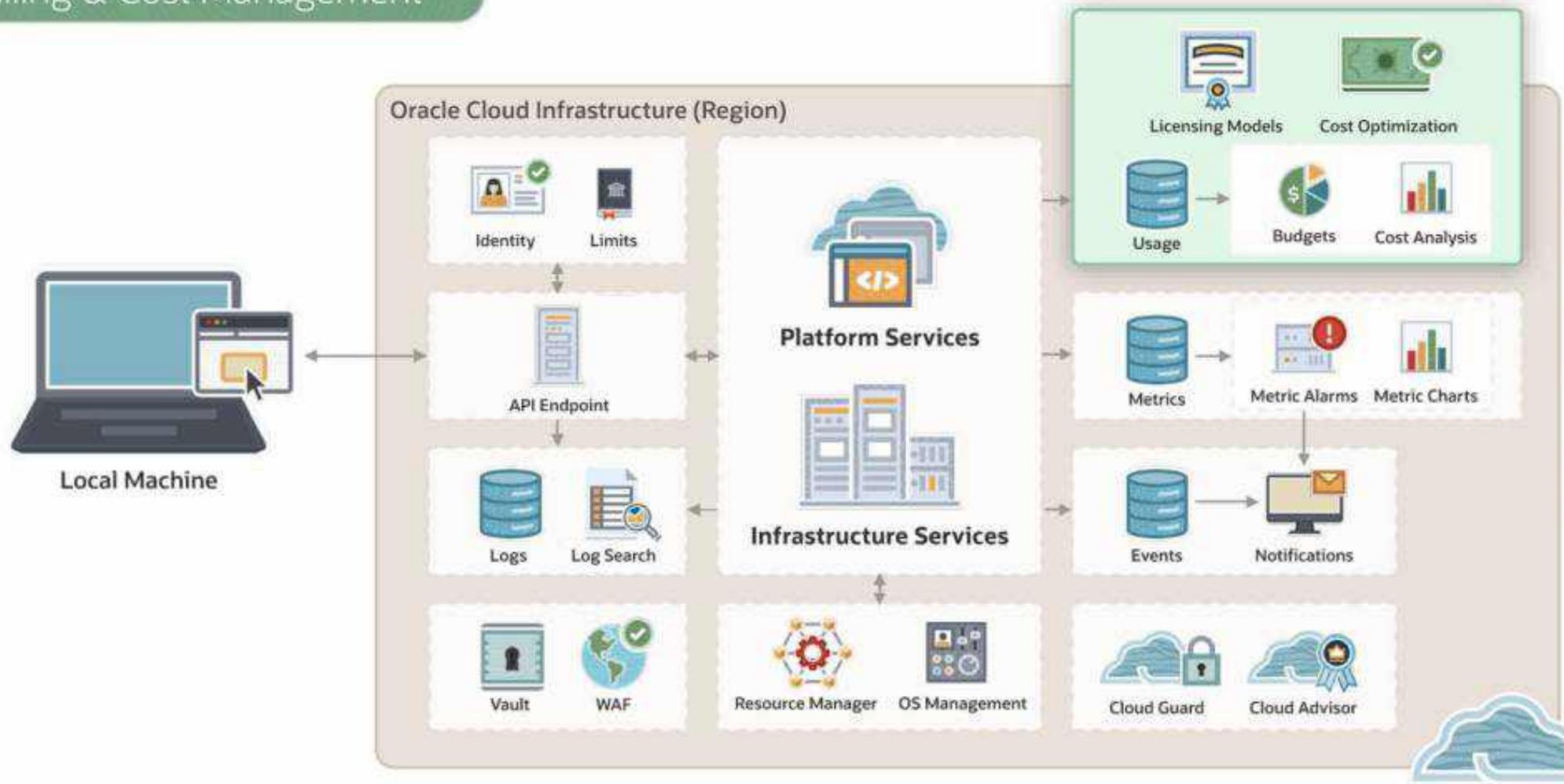
## Overview

### Course Big Picture



## Module 8

### Billing & Cost Management

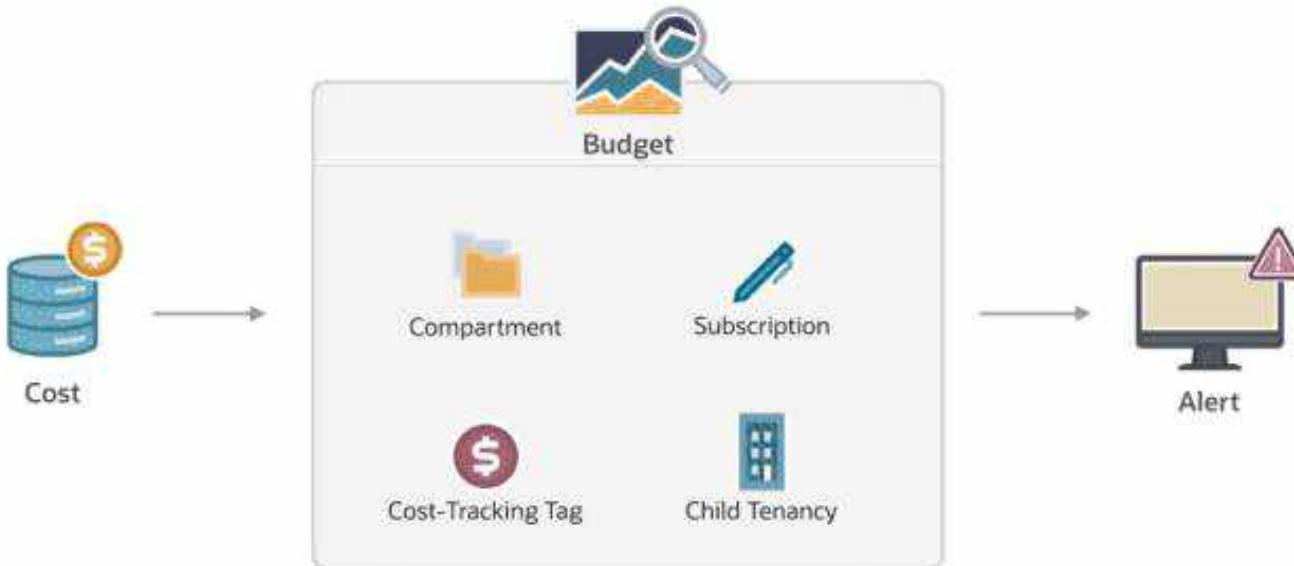


# Budgets

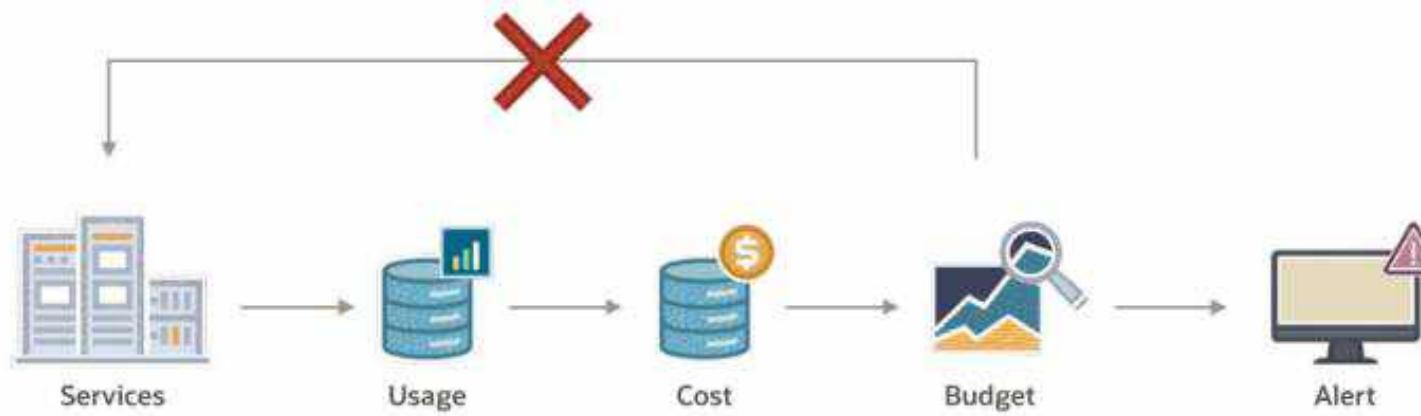


Forecasting is done with linear extrapolation

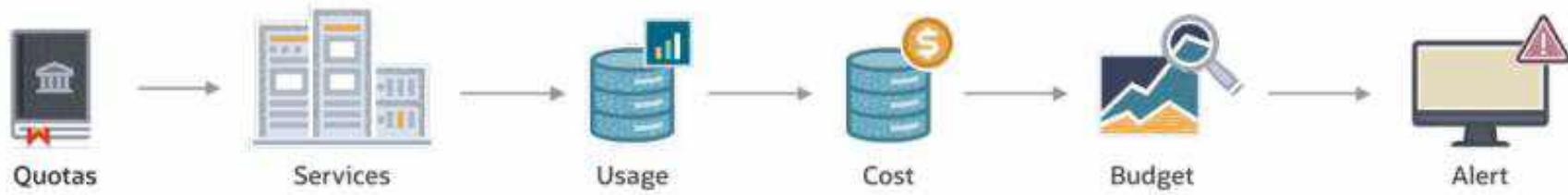
# Budgets



# Budgets



# Budgets

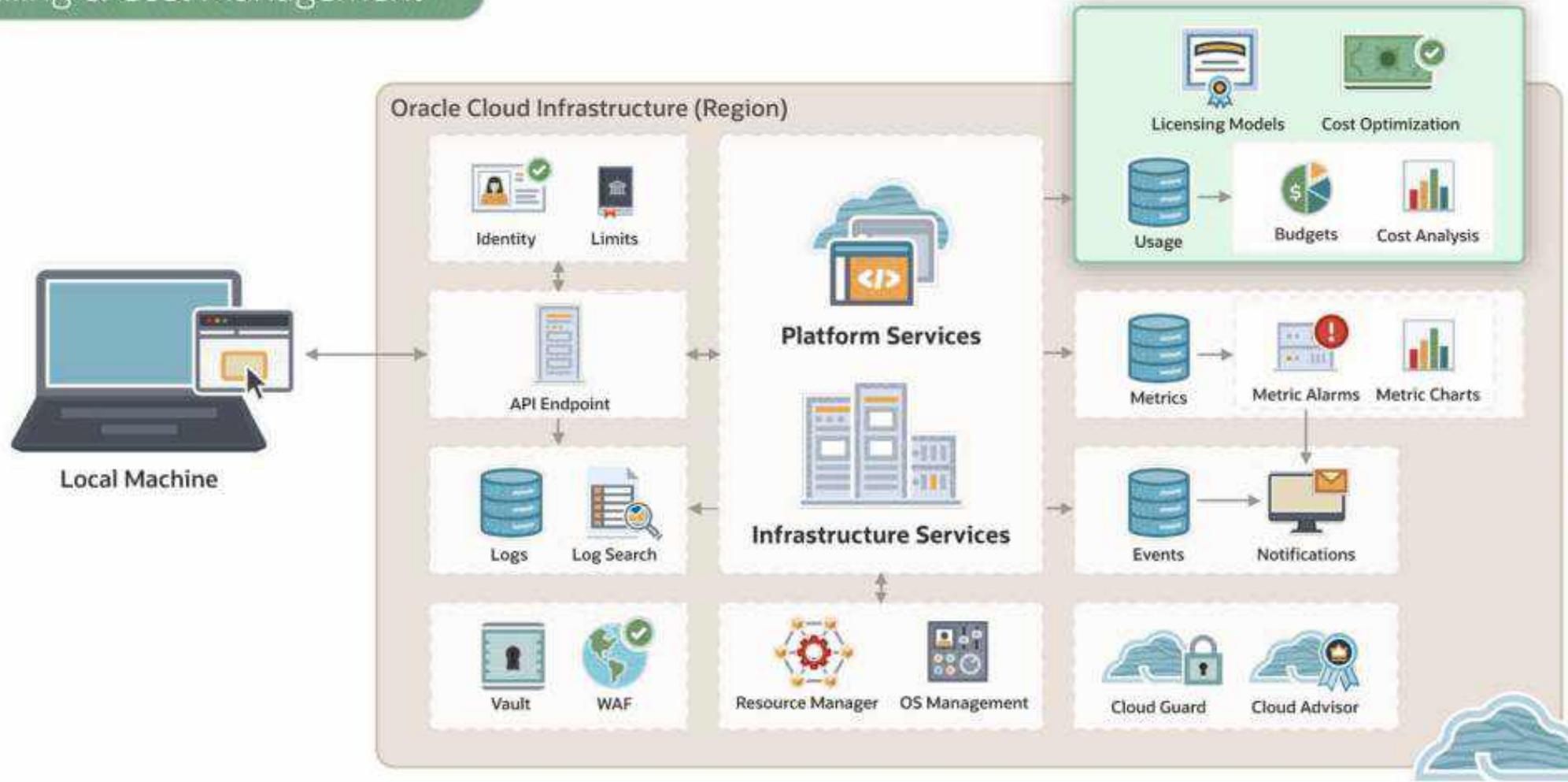


# Understand Cost with Cost Analysis

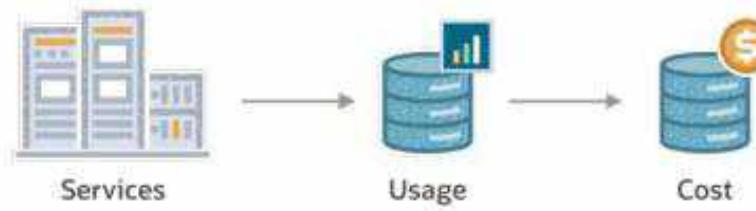
## Dashboards and Reports

## Module 8

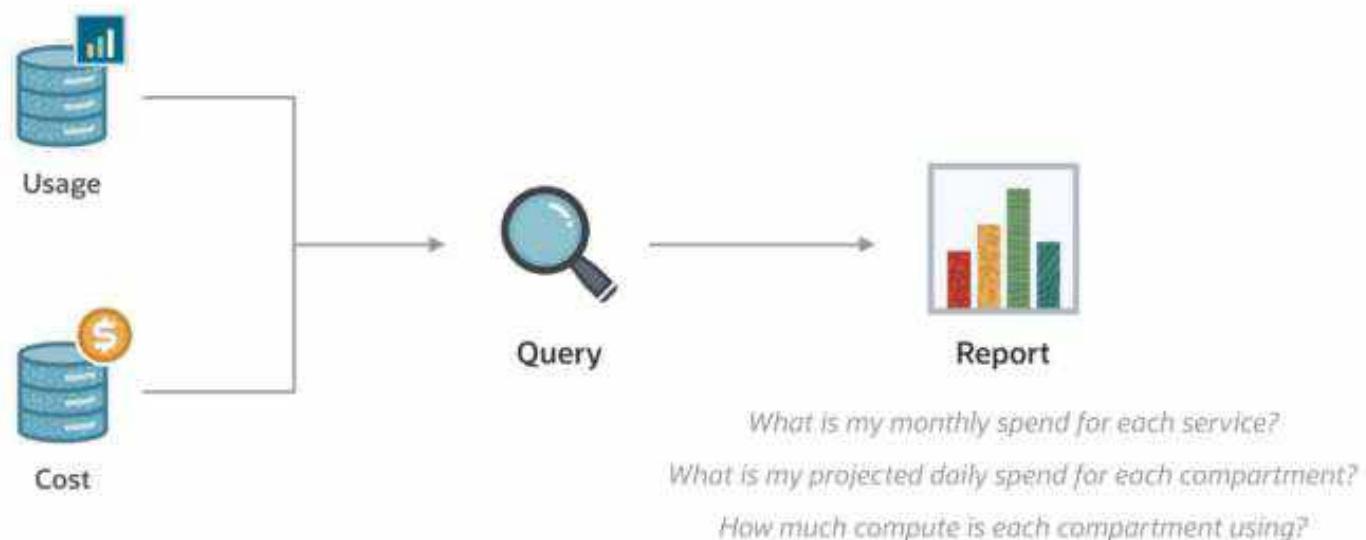
### Billing & Cost Management



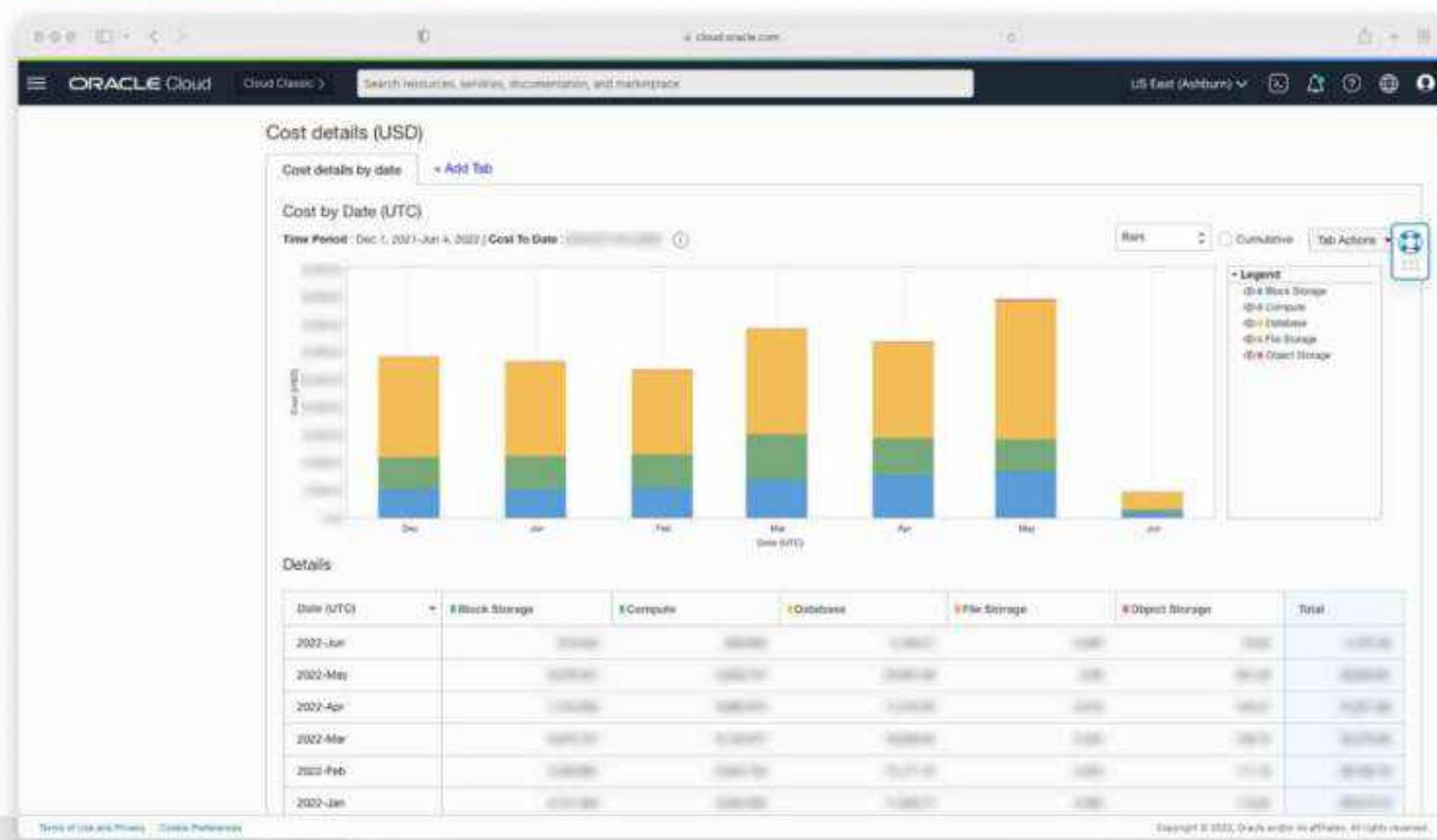
# Cost Analysis



# Cost Analysis



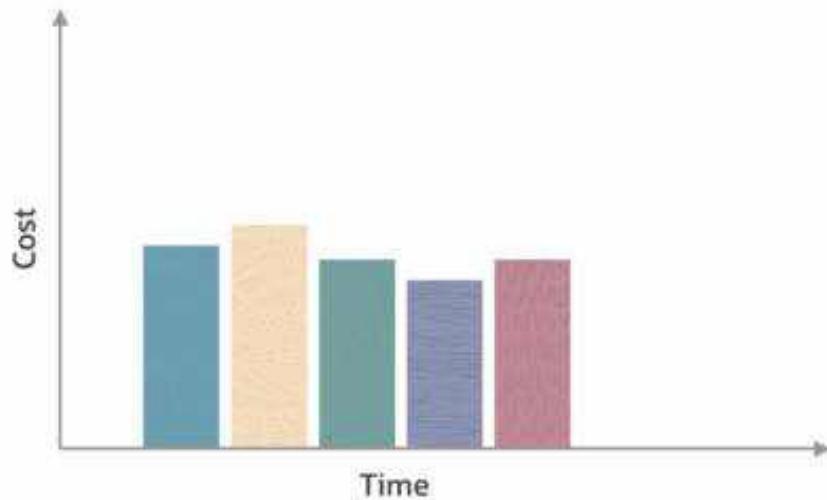
# Cost Analysis



# Cost Analysis



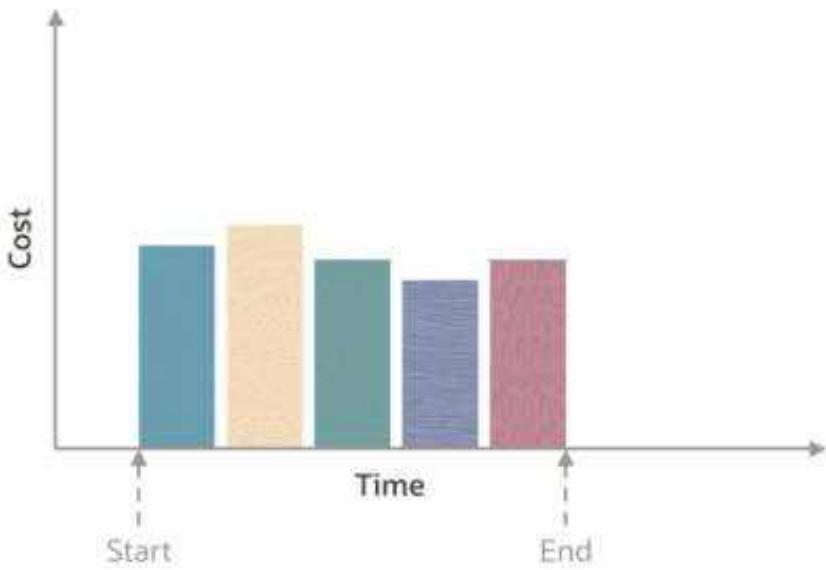
Report



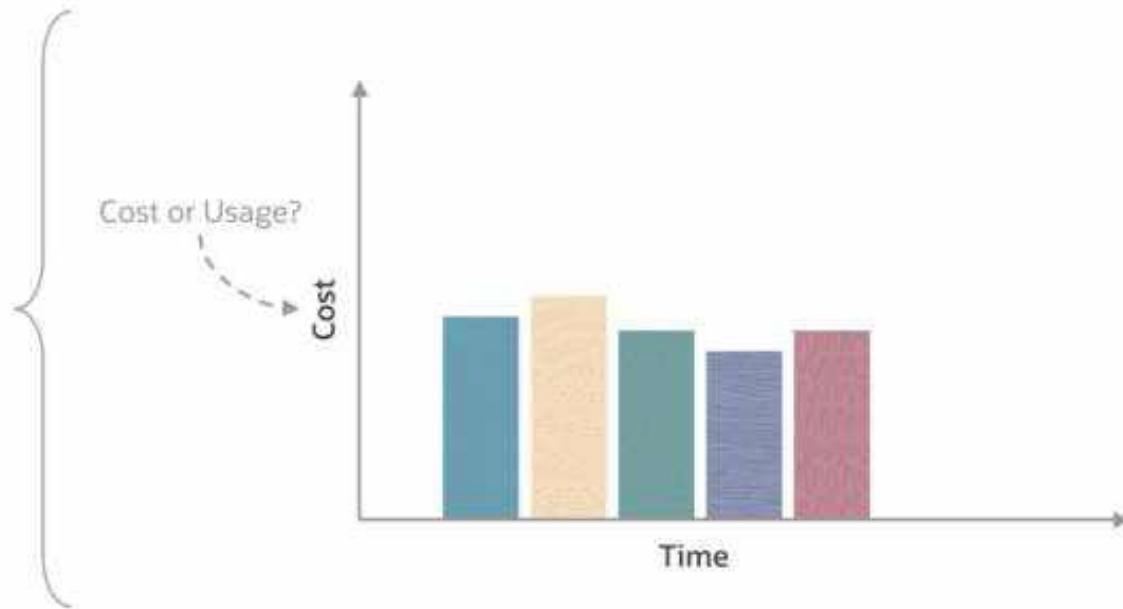
# Cost Analysis



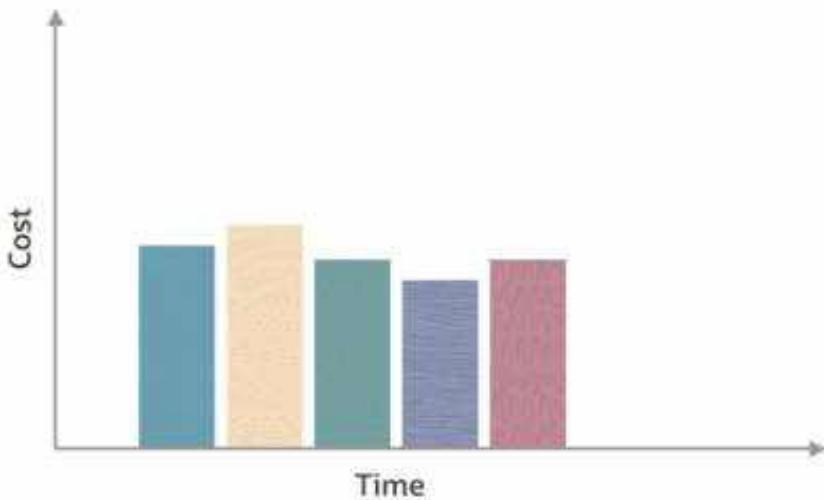
# Cost Analysis



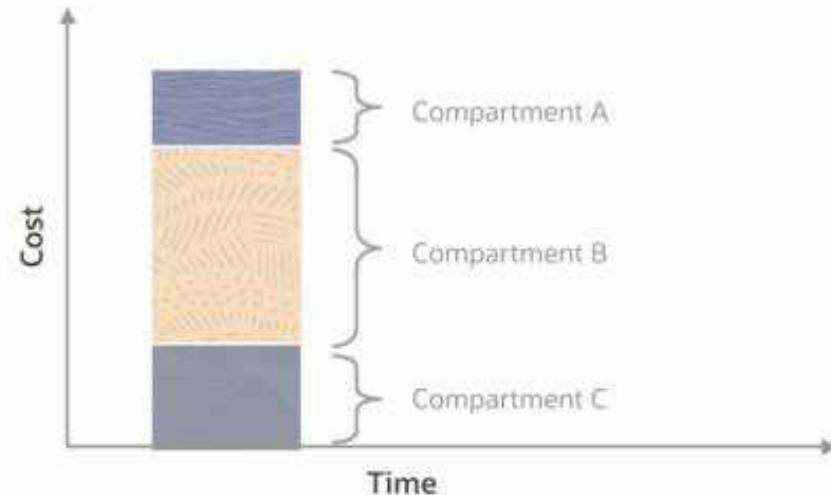
# Cost Analysis



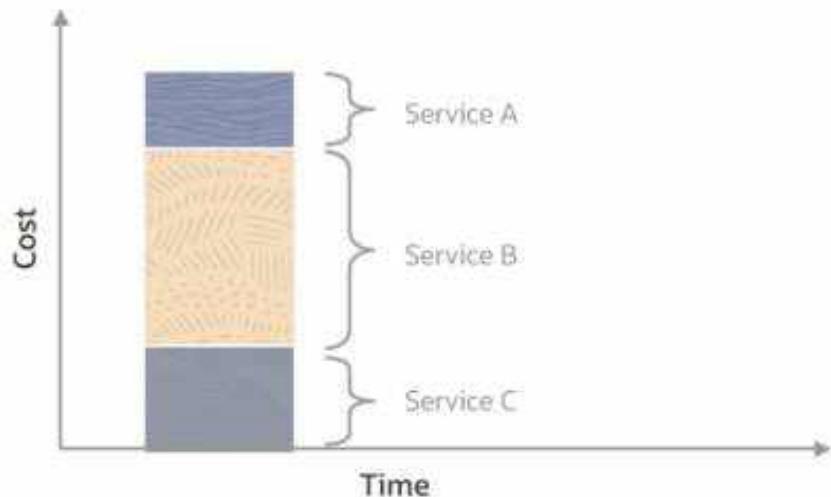
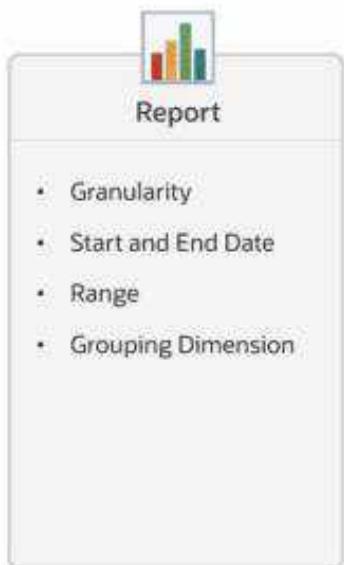
# Cost Analysis



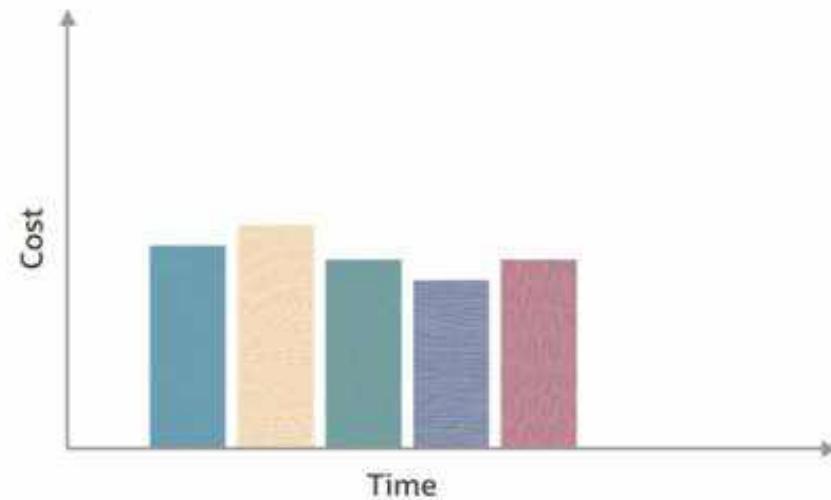
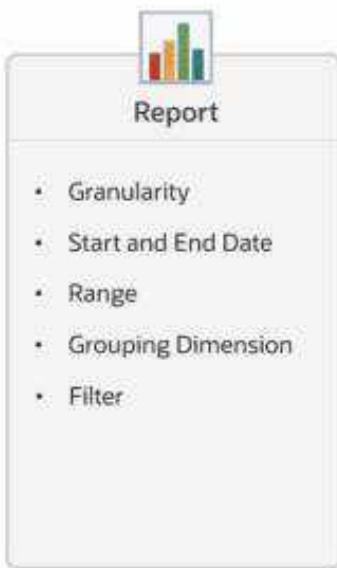
# Cost Analysis



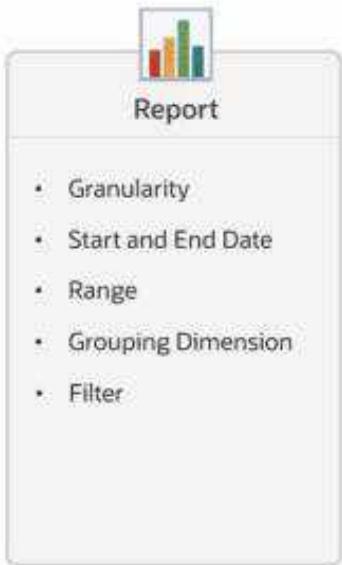
# Cost Analysis



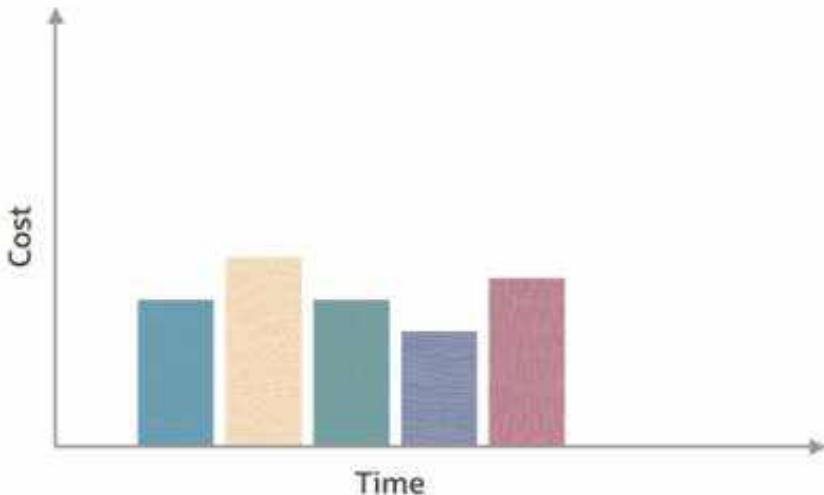
## Cost Analysis



# Cost Analysis



Compartment = Dev

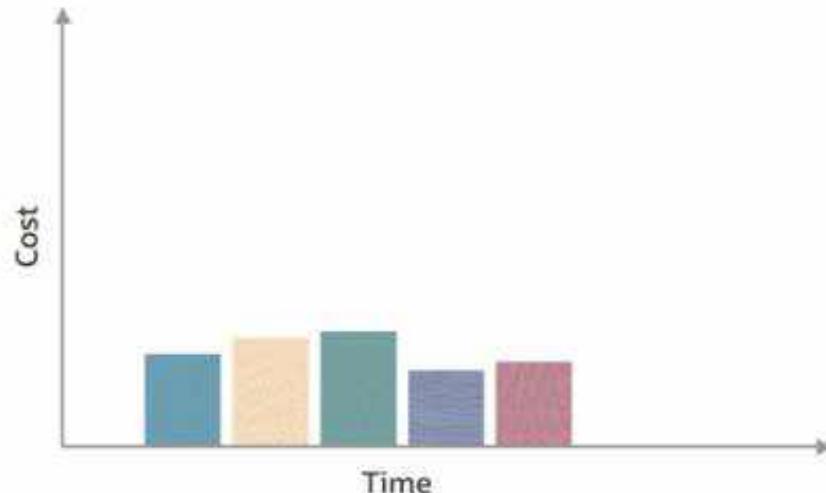


# Cost Analysis

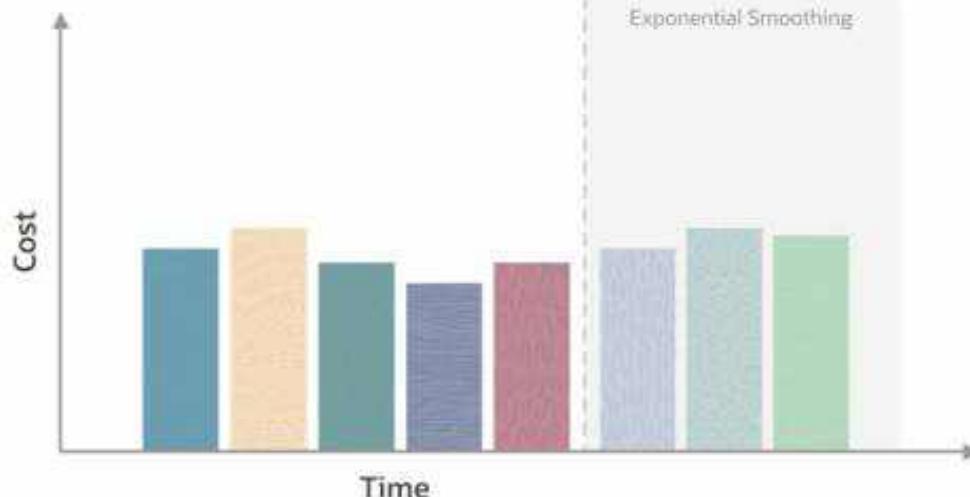
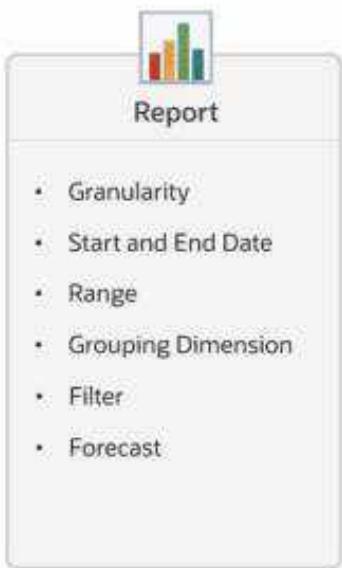


Compartment = Dev

Service = Compute, Block Storage



# Cost Analysis

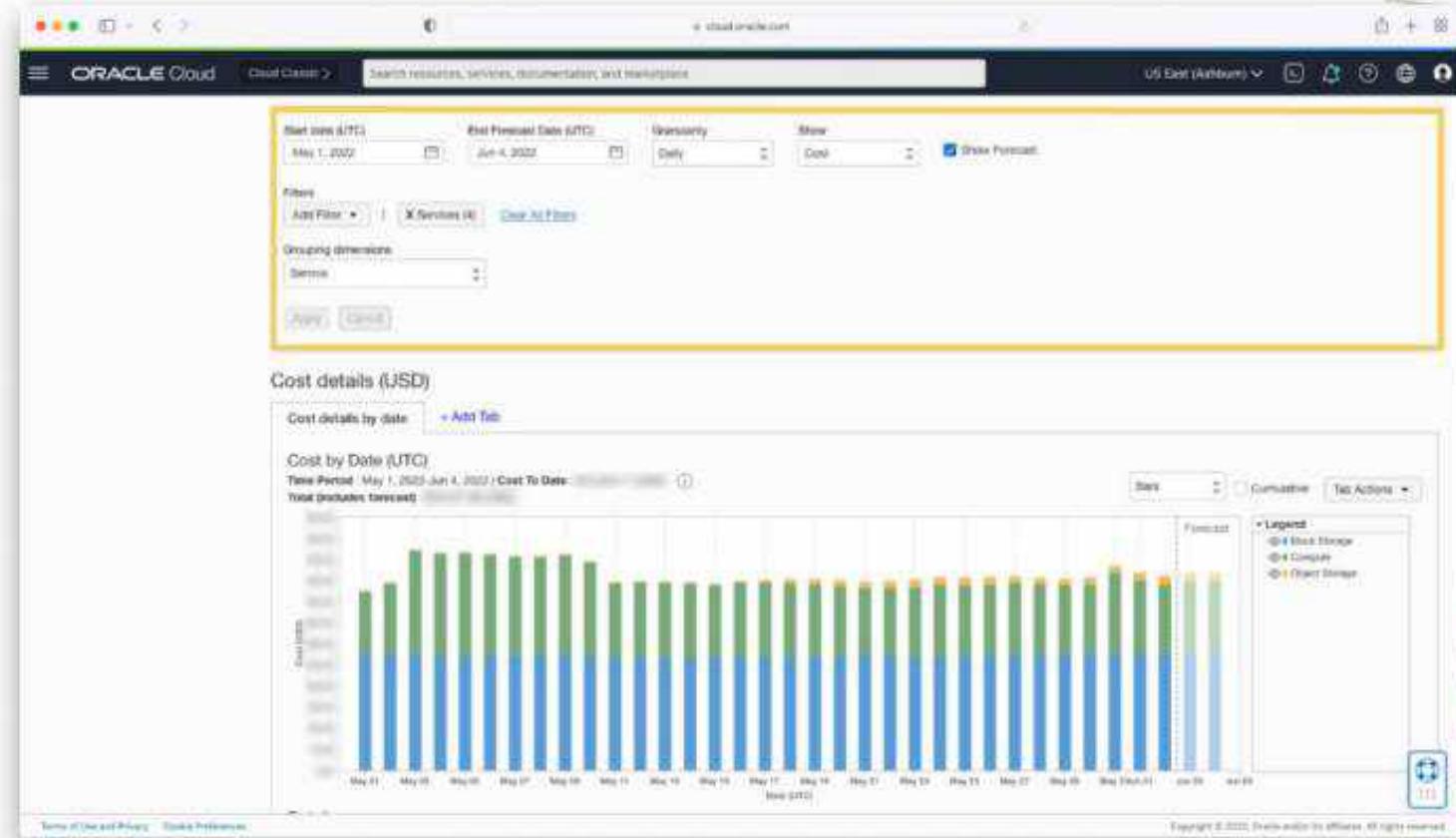


# Cost Analysis



### Report

- Granularity
- Start and End Date
- Range
- Grouping Dimension
- Filter
- Forecast



# Cost Analysis



ORACLE Cloud    Oracle Classic    Search resources, services, documentation, and marketplace    US East (Ashburn)    Notifications    Help    Log Out

Cost Management    Cost and Usage Reports    Budgets

### Cost and Usage Reports

Cost and usage reports are CSV files generated daily that show usage data for each resource in your tenancy. The CSV files are stored in an object storage bucket that is accessible using a cross-tenancy policy. [Learn more](#)

Name	Created	Size
reports-cost-csv-00010000000000000000000000000000.csv.gz	Sat, 04 Jun 2022 19:22:09 GMT	4.94 MB
reports-cost-csv-00010000000000000000000000000001.csv.gz	Sat, 04 Jun 2022 12:37:46 GMT	3 MB
reports-cost-csv-00010000000000000000000000000002.csv.gz	Sat, 04 Jun 2022 08:24:55 GMT	4.23 MB
reports-cost-csv-00010000000000000000000000000003.csv.gz	Sat, 04 Jun 2022 03:10:37 GMT	4.18 MB
reports-cost-csv-00010000000000000000000000000004.csv.gz	Fri, 03 Jun 2022 21:54:56 GMT	4.5 MB
reports-cost-csv-00010000000000000000000000000005.csv.gz	Fri, 03 Jun 2022 20:22:31 GMT	11.6 MB
reports-cost-csv-00010000000000000000000000000006.csv.gz	Fri, 03 Jun 2022 16:38:34 GMT	9.08 MB
reports-cost-csv-00010000000000000000000000000007.csv.gz	Fri, 03 Jun 2022 11:24:28 GMT	7.68 MB
reports-cost-csv-00010000000000000000000000000008.csv.gz	Fri, 03 Jun 2022 06:08:20 GMT	57.79 KB
reports-cost-csv-00010000000000000000000000000009.csv.gz	Fri, 03 Jun 2022 00:26:40 GMT	4.27 MB
reports-cost-csv-00010000000000000000000000000010.csv.gz	Thu, 02 Jun 2022 20:02:11 GMT	17.6 MB
reports-cost-csv-00010000000000000000000000000011.csv.gz	Thu, 02 Jun 2022 18:50:11 GMT	4.18 MB
reports-cost-csv-00010000000000000000000000000012.csv.gz	Thu, 02 Jun 2022 13:21:55 GMT	5 MB
reports-cost-csv-00010000000000000000000000000013.csv.gz	Thu, 02 Jun 2022 07:50:38 GMT	4.36 MB
reports-cost-csv-00010000000000000000000000000014.csv.gz	Thu, 02 Jun 2022 02:45:59 GMT	4.7 MB
reports-cost-csv-00010000000000000000000000000015.csv.gz	Wed, 01 Jun 2022 21:18:46 GMT	4.18 MB
reports-cost-csv-00010000000000000000000000000016.csv.gz	Wed, 01 Jun 2022 20:40:43 GMT	17.6 MB
reports-cost-csv-00010000000000000000000000000017.csv.gz	Wed, 01 Jun 2022 15:54:29 GMT	4.2 MB

[Terms of Use and Privacy](#)    [Close Preferences](#)

Copyright © 2025, Oracle and/or its affiliates. All rights reserved.



## Oracle Cloud Infrastructure

### Calculate and Optimize Cost: Compute

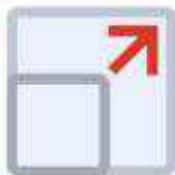
#### OCPUs, vCPUs, and Auto-scaling

# Compute Pricing

Considerations:



Shape



Size



Time



Capacity Type

# Compute Pricing



Considerations:



Shape



Size



Time



Capacity Type



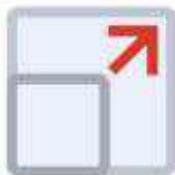
OS Licenses

# Compute Pricing

Considerations:



Shape



Size



Time

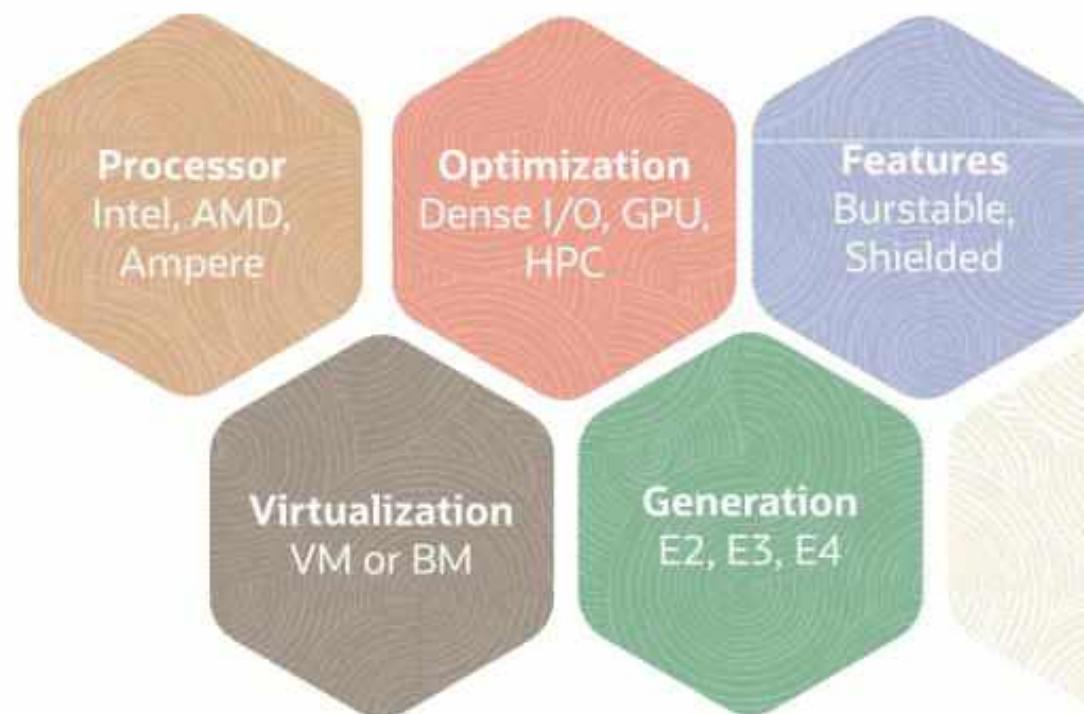


Capacity Type

# Compute Pricing



Shape

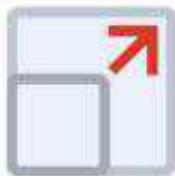


# Compute Pricing

Considerations:



Shape



Size

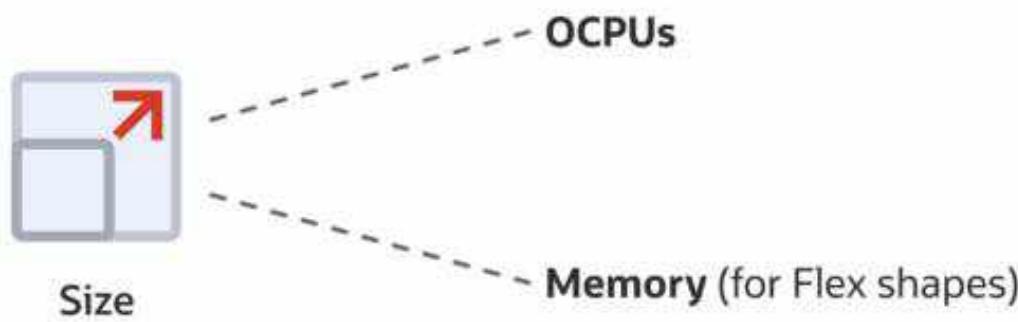


Time

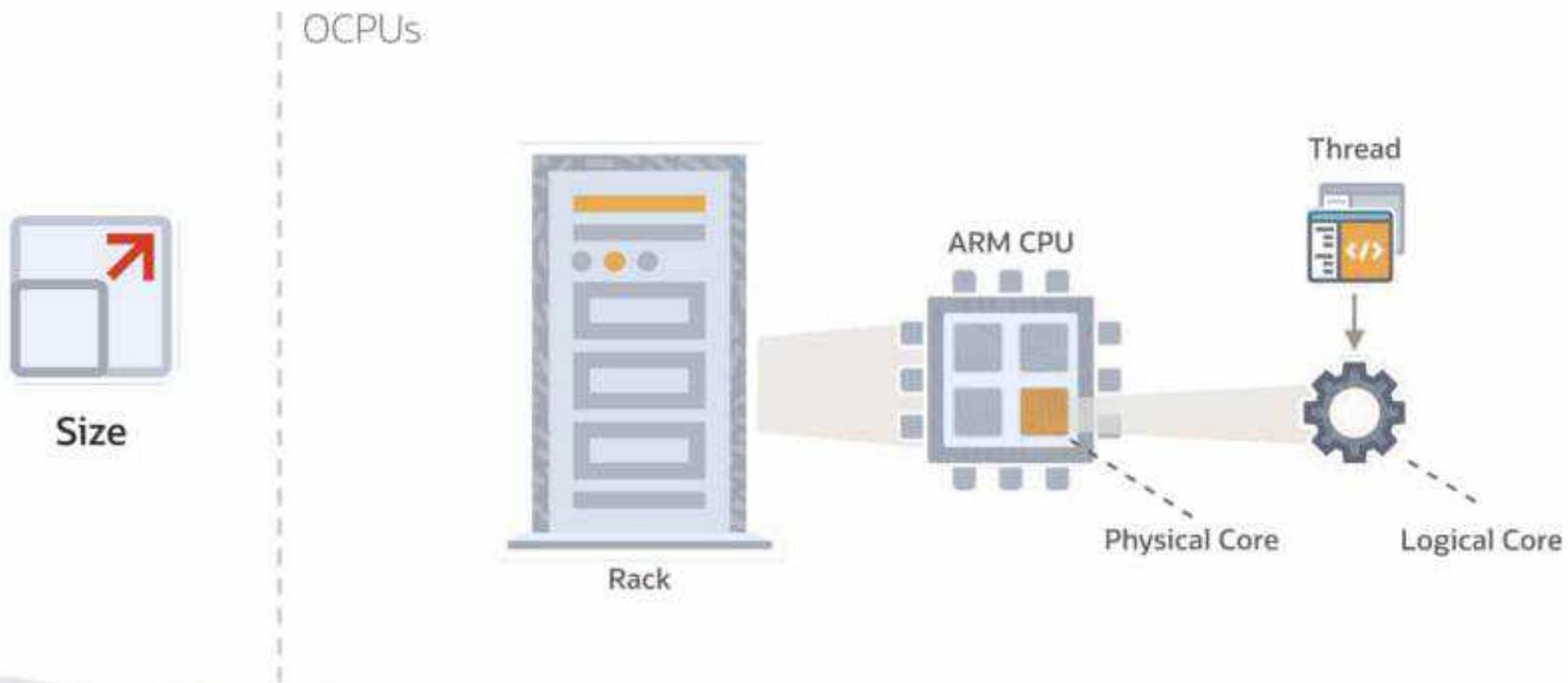


Capacity Type

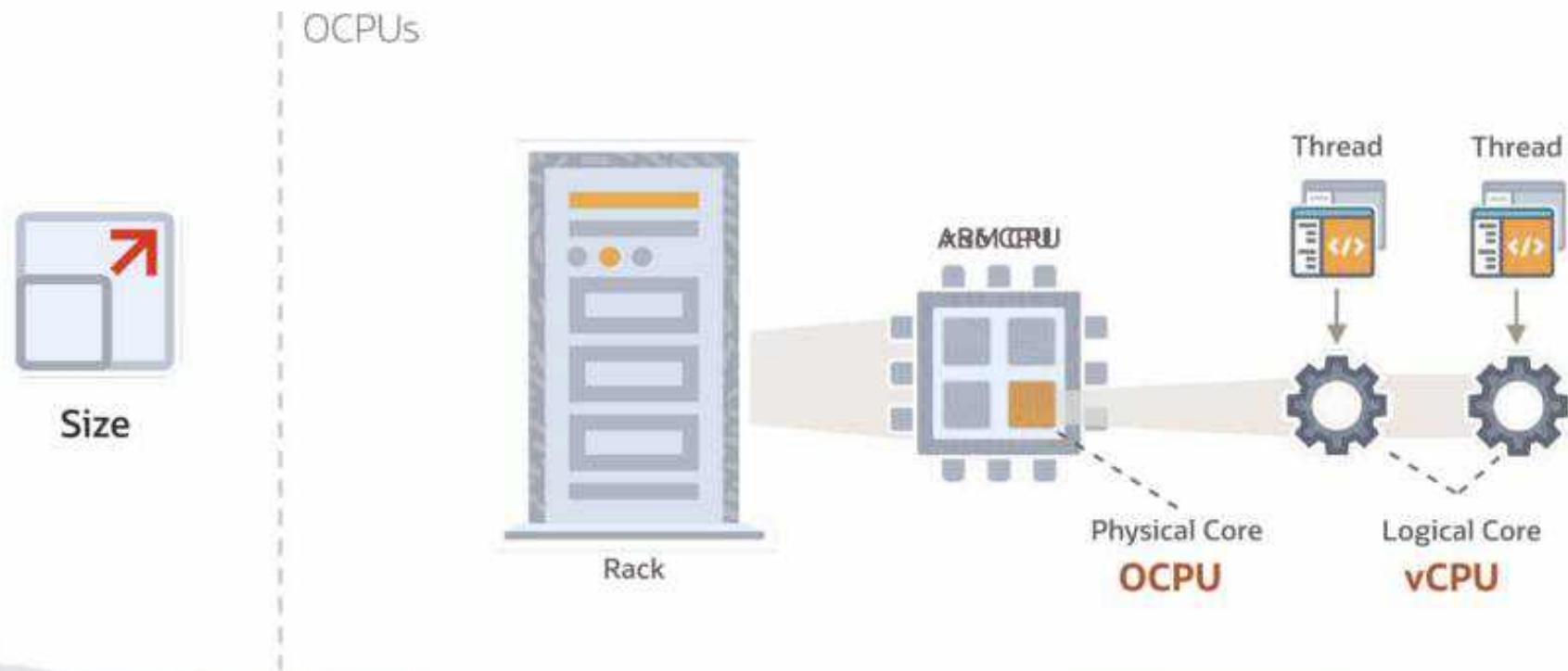
# Compute Pricing



# Compute Pricing



# Compute Pricing



# Compute Pricing

Considerations:



Shape



Size



Time



Capacity Type

# Compute Pricing



Time

Per-second granularity, one-minute minimum

# Compute Pricing

Considerations:



Shape



Size



Time



Capacity Type

# Compute Pricing



On-demand



Preemptible



50%

Reserved



85%

Dedicated



# Compute Pricing

Consider



Compute Type

My Configuration ... SHARE VM STANDARD ALFAE PROCESSOR VMFPU OCPU : MEMORY 8GB CAPACITY TYPE ON-DEMAND Estimated Monthly Cost \$4.25

Service: Compute - Virtual Machine Utilization: 1 Instance x 744 hrs/month Hourly Equivalent Price: \$0.0000 Estimated Monthly Cost: \$0.00

Shape: Processor Ampers Shape: VM Standard Alfae Disk: 1 1 OCPU equals to 1 vCPU Max. Total max 80 vCPUs allocated. Max. 8 vCPUs per OCPU.

Memory (GB): 8 OS Image: alfaimage1 Linux

Pricing Options: Learn more about capacity types Capacity Type: On-Demand

Each instance gets free from 2,000 OCPU hours and 16 GB memory per month for free on Oracle Net price. All Compute instances using the VM Standard Alfae image (2 vCPUs and 2GB of memory) in Oracle VM Compute shapes, OCPU equals to 1 vCPU.

Service: Storage - Block Volumes Estimated Monthly Cost: \$4.25

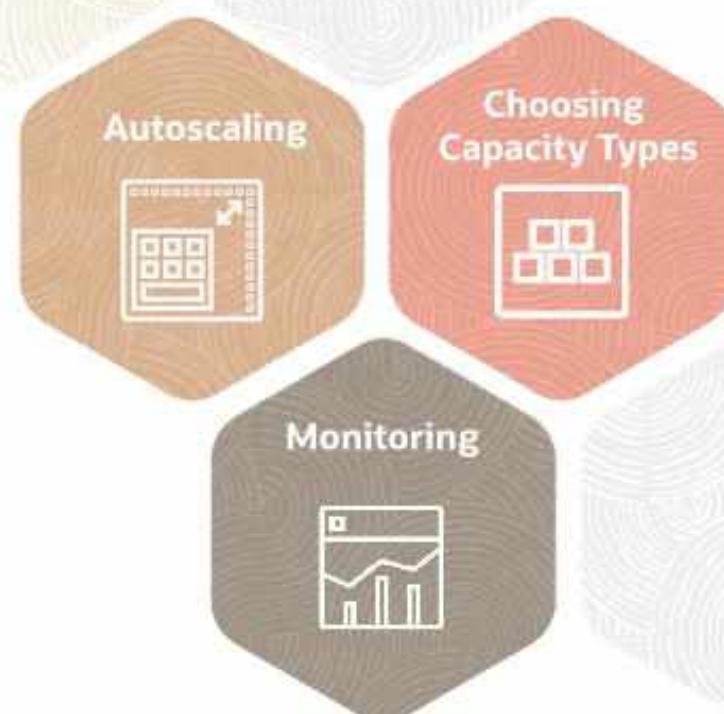
Storage capacity (TB): 100 Performance Level: Balanced IOPS: 1000 Max IOPS: 25000 Max Throughput (Mbps): 100

Apply 200GB Free Tier Discount

Block Volume service tier fee is deducted from entire monthly 200GB total/tenancy. If there are multiple clusters for this same tenancy, only total 200GB can be applied.

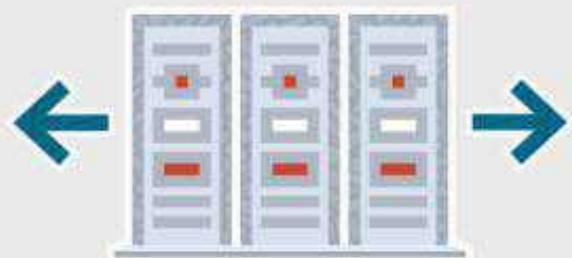
Compute - Standard - E5 - Memory 50.0015 Gigabyte per hour

# Cost Optimization for Compute

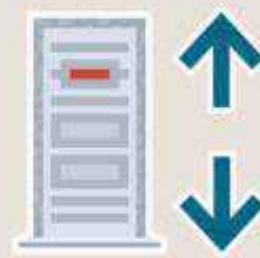


# Scaling

## Horizontal Scaling



## Vertical Scaling



# Autoscaling

**Schedule-Based**

**Metric-Based**

# Autoscaling

Schedule-Based



One-time or recurring

Metric-Based

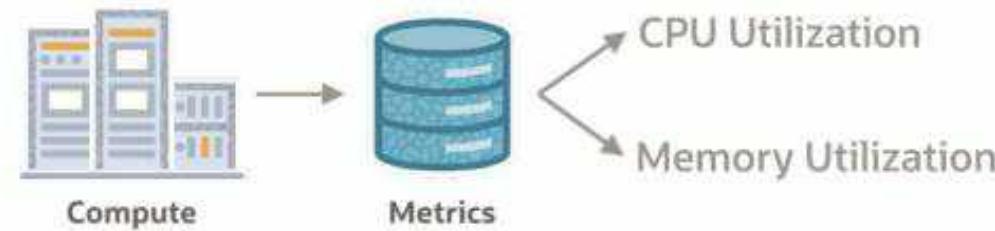


Predictable demand

# Autoscaling

Schedule-Based

Metric-Based



A

S

M

cloud.oracle.com

US West (Phoenix)

Create autoscaling configuration

1 Add basic details  
2 Configure autoscaling policy  
3 Review

Previous Next Cancel

Terms of Use and Privacy | Cookie Preferences

Copyright © 2022, Oracle and/or its affiliates. All rights reserved.

This screenshot shows the Oracle Cloud Infrastructure (OCI) Create autoscaling configuration wizard. The user is currently on Step 2: Configure autoscaling policy. The interface includes a navigation bar with tabs for Add basic details, Configure autoscaling policy (which is highlighted in blue), and Review. Below the tabs, there is a large, mostly empty text area with placeholder text: "Configure autoscaling policy". At the bottom of the wizard, there are buttons for Previous, Next, and Cancel, along with links for Terms of Use and Privacy and Cookie Preferences. The footer of the page contains the copyright notice: "Copyright © 2022, Oracle and/or its affiliates. All rights reserved."

A  
S  
M

cloud.oracle.com

US West (Phoenix)

Create autoscaling configuration

Add basic details

Configure autoscaling policy

Review

Cooldown in seconds: 300

Previous Next Cancel

Terms of Use and Privacy | Cookie Preferences

Copyright © 2025, Oracle and/or its affiliates. All rights reserved.

cloud.oracle.com

US West (Phoenix)

## Create autoscaling configuration

1 Add basic details  
2 Configure autoscaling policy  
3 Review

Cooldown in seconds: 300

Performance metric: CPU utilization

Previous Next Cancel

Terms of Use and Privacy | Cookie Preferences

Copyright © 2022, Oracle and/or its affiliates. All rights reserved.

This screenshot shows the Oracle Cloud Infrastructure (OCI) Create autoscaling configuration wizard. The user is currently on Step 2, "Configure autoscaling policy". The configuration includes setting the cooldown period to 300 seconds and selecting CPU utilization as the performance metric. The sidebar on the left shows the steps: Add basic details, Configure autoscaling policy (which is active), and Review. At the bottom, there are Previous, Next, and Cancel buttons, along with links for Terms of Use and Privacy and Cookie Preferences. The copyright notice at the bottom right indicates the content is from 2022.

A  
S  
M

The screenshot shows a web browser window for Oracle Cloud at [cloud.oracle.com](https://cloud.oracle.com). The title bar says "Create autoscaling configuration". The left sidebar has three steps: 1. Add basic details (disabled), 2. Configure autoscaling policy (selected), and 3. Review. The main content area is titled "Configure autoscaling policy". It includes fields for "Cooldown in seconds" (set to 300), "Performance metric" (set to "CPU utilization"), and a "Scale-out rule" section with "Scale-out operator" set to "Greater than (>)" and "Threshold percentage" set to 75. At the bottom are "Previous", "Next", and "Cancel" buttons, along with links for "Terms of Use and Privacy" and "Cookie Preferences". A watermark for "Oracle Cloud Infrastructure Cloud Operations Professional: Hands-on Workshop" is visible on the right.

cloud.oracle.com

US West (Phoenix)

Create autoscaling configuration

Add basic details

Configure autoscaling policy

Review

Cooldown in seconds

300

Performance metric

CPU utilization

Scale-out rule

Scale-out operator

Greater than (>)

Threshold percentage

75

Number of instances to add

1

Previous Next Cancel

Terms of Use and Privacy

Cookie Preferences

Copyright © 2025, Oracle and/or its affiliates. All rights reserved.

cloud.oracle.com

US West (Phoenix)

Create autoscaling configuration

Add basic details

Configure autoscaling policy

Review

Cooldown in seconds: 300

Performance metric: CPU utilization

Scale-out rule:

- Scale-out operator: Greater than (>)
- Threshold percentage: 75
- Number of instances to add: 1

Scale-in rule:

- Scale-in operator: Less than (<)
- Threshold percentage: 25
- Number of instances to remove: 1

Previous Next Cancel

Terms of Use and Privacy | Cookie Preferences

Copyright © 2022, Oracle and/or its affiliates. All rights reserved.

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

cloud.oracle.com

US West (Phoenix)

## Create autoscaling configuration

Add basic details

Configure autoscaling policy

Review

Cooldown in seconds: 300 (Minimum value is 300 seconds)

Performance metric: CPU utilization

Scale-out rule:

- Scale-out operator: Greater than (>)
- Threshold percentage: 75
- Number of instances to add: 1

Scale-in rule:

- Scale-in operator: Less than (<)
- Threshold percentage: 25
- Number of instances to remove: 1

Scaling limits:

- Minimum number of instances: 1
- Maximum number of instances: 10
- Initial number of instances: 5

Previous Next Cancel

Terms of Use and Privacy | Cookie Preferences

Copyright © 2025, Oracle and/or its affiliates. All rights reserved.

## Oracle Cloud Infrastructure

# Calculate and Optimize Cost: Block Storage

### Storage Cost, VPUs, and Auto-tuning

# Block Storage Cost

Considerations:



Size



Performance

# Block Storage Cost



Size

\$0.0255 per GB per month

*As of June 2022*

# Block Storage Cost



Size

\$0.0255 per GB per month  
*As of June 2022*

\$12.75 per 500 GB per month  
*As of June 2022*

# Block Storage Cost

Considerations:



Size



Performance

# Block Storage Cost



Volume Performance Units (VPUs)

	Starting at 10 VPUs	IOPS per GB	Max IOPS per Volume	KBPS per GB	Max MBPS per Volume
Performance	+ 10 VPU	15	25,000	120	200

## Volume Performance Units (VPUs)

	IOPS per GB	Max IOPS per Volume	KBPS per GB	Max MBPS per Volume
10 VPUs	60	25,000	480	480
20 VPUs	75	50,000	600	680
30 VPUs	90	75,000	720	880
40 VPUs	105	100,000	840	1,080
:	:	:	:	:
120 VPUs	225	300,000	1,800	2,680

## Volume Performance Units (VPUs)

10 VPUs = \$0.017 per GB

	IOPS per GB	Max IOPS per Volume	KBPS per GB	Max MBPS per Volume	
0 VPUs	2	3,000	240	480	Lower Cost
10 VPUs	60	25,000	480	480	Balanced
20 VPUs	75	50,000	600	680	Higher Performance
30 VPUs	90	75,000	720	880	
40 VPUs	105	100,000	840	1,080	
:	:	:	:	:	Ultra High Performance
120 VPUs	225	300,000	1,800	2,680	

## Volume Performance Units (VPUs)

10 VPUs = \$0.017 per GB

	Lower Cost	Balanced	Higher Performance	30 VPUs	120 VPUs	Storage Cost
500 GB	\$0	\$8.50	\$17	\$25.50	\$102	\$12.75
1 TB	\$0	\$17	\$34	\$51	\$204	\$25.50

# Auto-tuning



The screenshot shows the Oracle Cloud Block Storage interface for creating a new block volume. The left sidebar lists various storage options like Block Volumes, Block Volume Backups, and Boot Volumes. The main panel is titled "Create block volume" and has a "Name" field containing "dkVS-PHX-AD-1". Under "Volume Size and Performance", the "Custom" radio button is selected, showing a size of "1024 GB". The "Target Volume Performance" section includes a "VPU" slider set to "Balanced" between 10 and 125. To the right, "Target Volume Performance" details show "IOPS: 25000 IOPS" and "Throughput: 480 MB/s". A yellow box highlights the "Auto-tune Performance" toggle switch, which is turned "On". Below it, a note explains that auto-tuning changes performance to lower cost when detached and automatically adjusts when reattached. At the bottom are "Create Block Volume" and "Cancel" buttons.

## Oracle Cloud Infrastructure

### Calculate and Optimize Cost: File Storage

#### Utilization, Clones, and Snapshots

# File Storage Cost



\$0.30 per GB capacity per month

As of June 2022



Capacity automatically scales based on utilization



# File Storage Cost



\$0.30 per GB capacity per month

As of June 2022



Capacity automatically scales based on utilization



1 TB → \$300 per month

# File Storage Cost

Caveats:



Metadata



Clones/Snapshots

# File Storage Cost



Metadata



512 bytes for each directory entry

Hardlinks add directory entries



8192 bytes for each symlink

# File Storage Cost

Caveats:



Metadata



Clones/Snapshots

# File Storage Cost



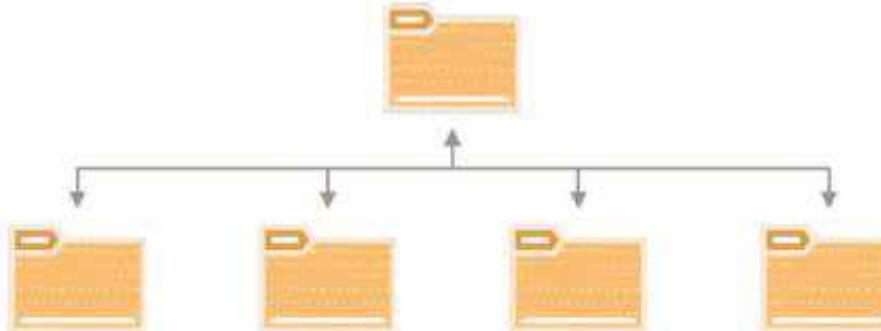
Clones/Snapshots

Clones/Snapshots ← → Hardware Failure Resiliency

# File Storage Cost



Clones/Snapshots



File Storage already uses 5-way replication

# File Storage Cost



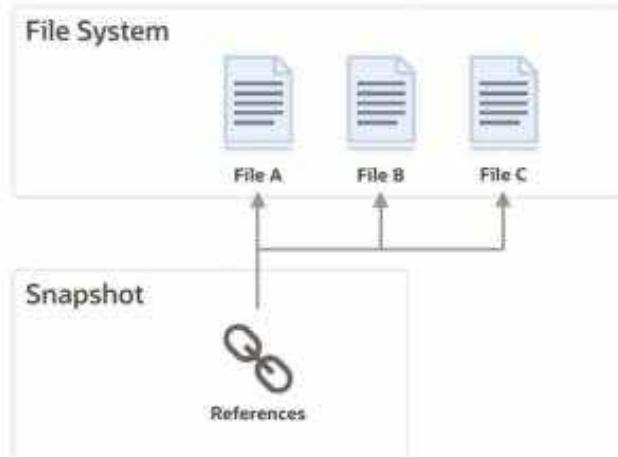
Clones/Snapshots

Clones/Snapshots ←  → Versioning



# File Storage Cost

## Copy-on-Write



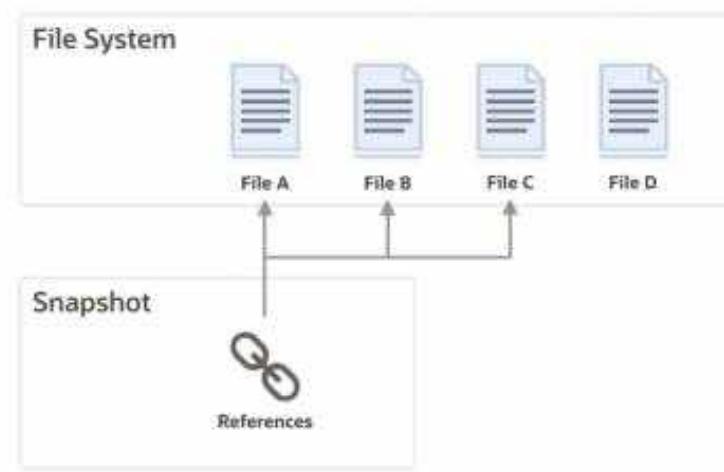
Clones/Snapshots

# File Storage Cost



Clones/Snapshots

## Copy-on-Write

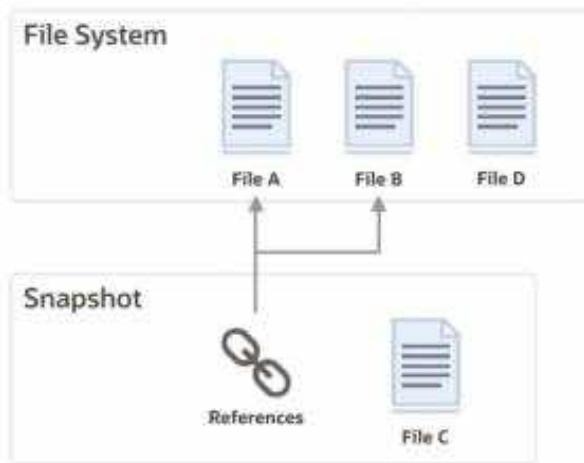


# File Storage Cost



Clones/Snapshots

## Copy-on-Write

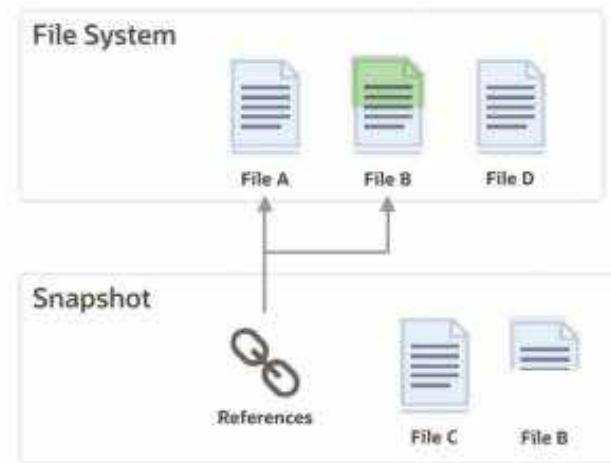


# File Storage Cost



Clones/Snapshots

## Copy-on-Write

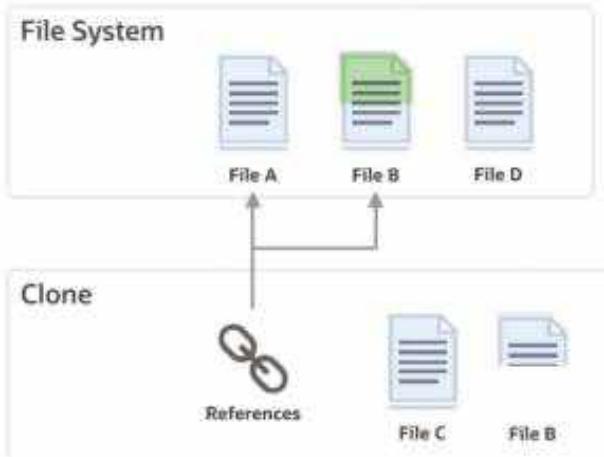


# File Storage Cost



Clones/Snapshots

## Copy-on-Write

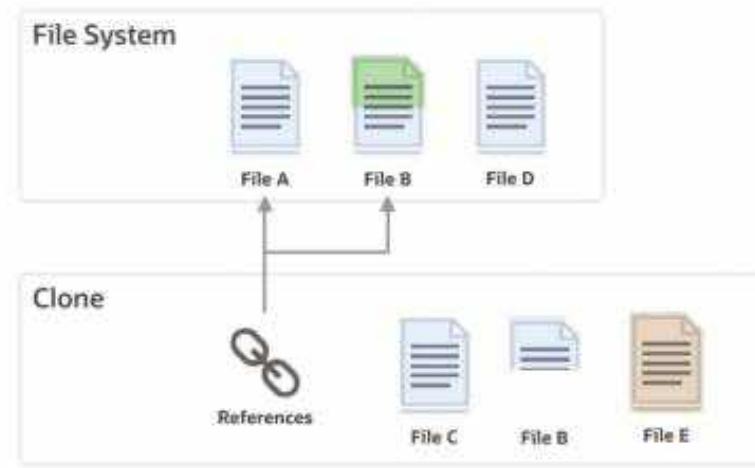


# File Storage Cost



Clones/Snapshots

## Copy-on-Write

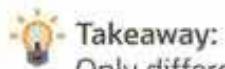


# File Storage Cost

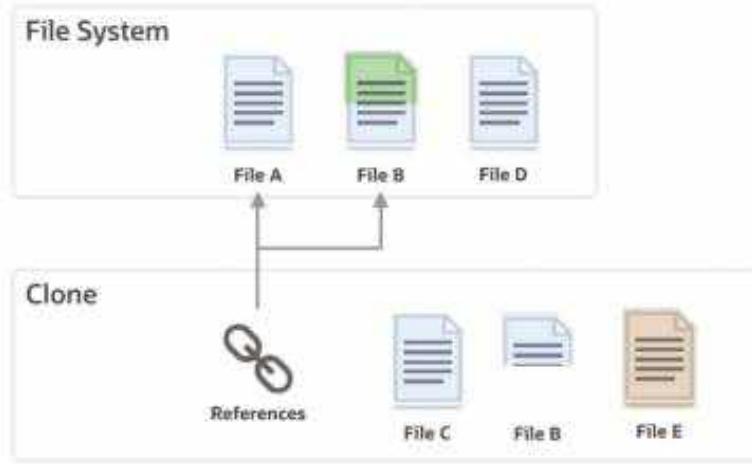


Clones/Snapshots

## Copy-on-Write



Takeaway:  
Only differentiated data adds utilization



# File Storage Cost

Caveats:



Metadata



Clones/Snapshots

## Oracle Cloud Infrastructure

# Calculate and Optimize Cost: Object Storage

## Storage Tiers and Life Cycle Management

# Object Storage Tiers



# Object Storage Costs

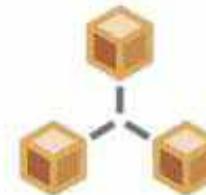
Considerations:



Storage



Transactions



Network Egress

First 10 TB egress each month is free

# Object Storage Costs



Considerations:



Storage  
per GB per month



Transactions

# Object Storage Costs



Considerations:



Transactions

**Standard** – per 10,000 requests per month  
(first 50,000 per month free)

**Infrequent Access** – per GB retrieved per month

**Archive** - none  
(but billed for Standard during download window)

# Object Storage Costs



Prices as of June 2022	Standard	Infrequent Access	Archive
Storage (per GB per month)	\$0.0255	\$0.01	
Transactions	\$0.0034 <small>10,000 Requests per Month (first 50,000 free)</small>	\$0.01 <small>GB Storage Retrieved Per Month</small>	

# Object Storage Costs



Prices as of June 2022	Standard	Infrequent Access	Archive
Storage (per GB per month)	\$0.0255	\$0.01	
Transactions	\$0.0034 <small>10,000 Requests/GB Month 100,000 Requests</small>	\$0.02 <small>GB Storage Retrieved Per Month</small>	\$0.01

# Object Storage Costs



Prices as of June 2022	Standard	Infrequent Access	Archive
Storage (per GB per month)	\$0.0255	\$0.01	\$0.0026
Transactions	\$0.0034 <small>10,000 Requests per Month (first 50,000 free)</small>	\$0.01 <small>GB Storage Retrieved Per Month</small>	N/A

# Object Storage Costs



Prices as of June 2022	Standard	Infrequent Access	Archive
Storage (per GB per month)	\$0.0255	\$0.01	\$0.0026
	<p>↓ 1000 GB</p> <p>\$25.50</p>	<p>↓ 1000 GB</p> <p>\$10</p>	<p>↓ 1000 GB</p> <p>\$2.60</p>

# Object Storage Costs



Prices as of June 2022	Standard	Infrequent Access	Archive
Storage (per GB per month)	\$0.0255	\$0.01	\$0.0026
	<p>↓ 1000 GB</p> <p>\$25</p>	<p>↓ 1000 GB</p> <p>\$10</p>	<p>↓ 1000 GB</p> <p>\$3</p>

My Estimate [Configure and estimate costs for OCI products](#) | [Learn more](#)

[Start for Free](#) [USD - US Dollar](#) [Estimated Monthly Cost: \\$38.62](#)

**Object Storage** [Estimated Monthly Cost: \\$25.24](#)

**SERVICE** **Storage - Object Storage** [Edit](#) [Estimate monthly cost](#) **\$25.24**

**Storage Type:** Standard **Object Storage - Storage:** 1,000 **Object Storage - Requests:** 3

Gigabyte Storage Capacity Per Month: Unit price: \$0.025 10,000 Requests per Month (at \$0.0001/Request) Unit price: \$0.0001 Requests/Day = 10,000 Requests

**Object Storage** [Estimated Monthly Cost: \\$10.80](#)

**SERVICE** **Storage - Object Storage** [Edit](#) [Estimate monthly cost](#) **\$10.80**

**Storage Type:** Infrequent Access **Infrequent Access Storage - S:** 1,000 **Infrequent Access Storage - R:** 100

Gigabyte Storage Capacity Per Month: Unit price: \$0.0100 10,000 Requests per Month: Unit price: \$0.0100 Requests/Day = 10,000 Requests

**Object Storage** [Estimated Monthly Cost: \\$2.57](#)

**SERVICE** **Storage - Object Storage** [Edit](#) [Estimate monthly cost](#) **\$2.57**

**Storage Type:** Archive **Archive Storage - Storage:** 1,000

Gigabyte Storage Capacity Per Month: Unit price: \$0.0030

# Object Storage Costs



	Minimum Retention Period
Infrequent Access	31 days
Archive	90 days



If you delete prior to retention requirement, you are billed for the **full retention period**.

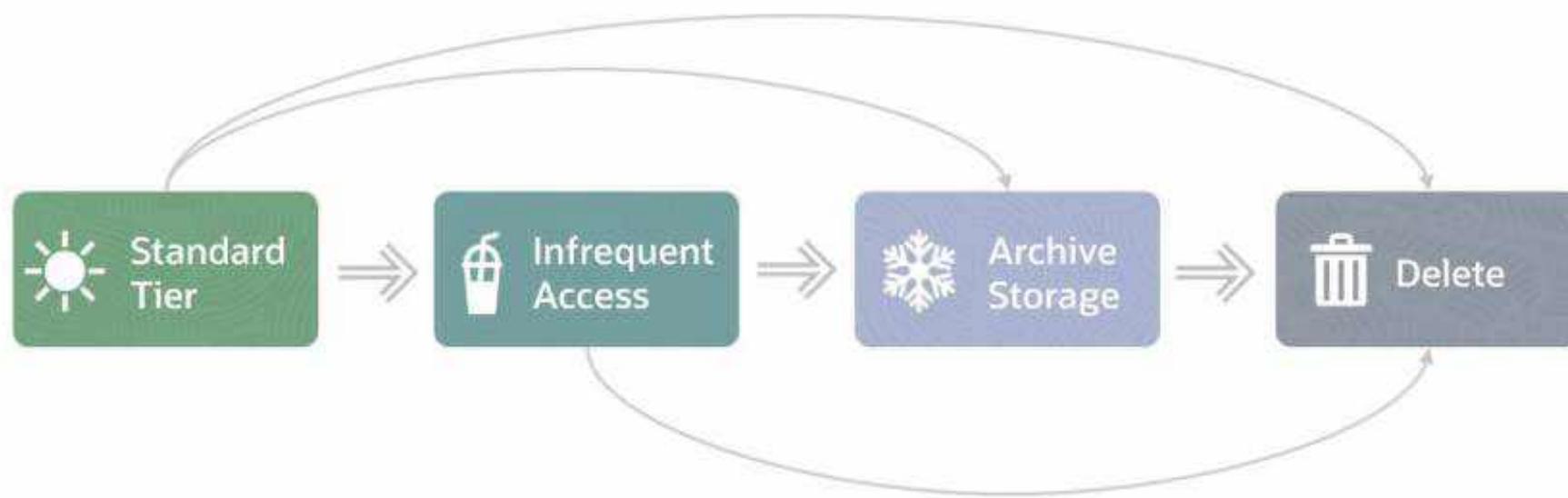


Deleting **versioned** data does not result in true data removal, so no penalty is incurred.

# Optimize Cost: Object Storage

**Life Cycle Management, Auto-Tiering**

# Life Cycle Management



# Life Cycle



## Create Lifecycle Rule

Name

Example Rule

Target

**Latest Version of Objects**  
Create a lifecycle rule that applies to the latest version of either:

- All objects in the bucket
- Objects that match the object name filters that you specify

**Previous Versions of Objects**  
Create a lifecycle rule that applies to the previous versions of either:

- All objects in the bucket
- Objects that match the object name filters that you specify

**Uncommitted Multipart Uploads**  
Create a lifecycle rule that deletes uncommitted or failed multipart uploads.

Lifecycle Action

Move to Archive

Number of Days

Archive objects that are older than 30 days and that match any of the specified object name filters.

Object Name Filters (Optional)

Use object name filters to specify which objects the lifecycle rule applies to. You can choose objects using prefixes and pattern matching. If no name filter is specified, the rule applies to all objects in the bucket. [Learn more about using object name filters](#)

You can add object filters in any order. Object Lifecycle Management takes care of the evaluation precedence.

+ Add Filter

**Create** **Cancel**

Delete

# Life Cycle



## Create Lifecycle Rule

Name: Example Rule

Target:

- Latest Version of Objects**  
Create a lifecycle rule that applies to the latest version of either:
  - All objects in the bucket
  - Objects that match the object name filters that you specify
- Previous Versions of Objects**  
Create a lifecycle rule that applies to the previous versions of either:
  - All objects in the bucket
  - Objects that match the object name filters that you specify
- Uncommitted Multipart Uploads**  
Create a lifecycle rule that deletes uncommitted or failed multipart uploads.

Lifecycle Action: Move to Archive

Number of Days: 30

Archive objects that are older than 30 days and that match any of the specified object name filters.

Object Name Filters (Optional)

Use object name filters to specify which objects the lifecycle rule applies to. You can choose objects using prefixes and pattern matching. If no name filter is specified, the rule applies to all objects in the bucket. [Learn more about using object name filters](#)

You can add object filters in any order. Object Lifecycle Management takes care of the evaluation precedence.

+ Add Filter

**Create** **Cancel**

Delete

# Life Cycle



## Create Lifecycle Rule

Name

Example Rule

Target

### Latest Version of Objects

Create a lifecycle rule that applies to the latest version of either:

- All objects in the bucket
- Objects that match the object name filters that you specify

### Previous Versions of Objects

Create a lifecycle rule that applies to the previous versions of either:

- All objects in the bucket
- Objects that match the object name filters that you specify

### Uncommitted Multipart Uploads

Create a lifecycle rule that deletes uncommitted or failed multipart uploads.

### Lifecycle Action

Move to Archive

### Number of Days

30

Archive objects that are older than 30 days and that match any of the specified object name filters.

### Object Name Filters (Optional)

Use object name filters to specify which objects the lifecycle rule applies to. You can choose objects using prefixes and pattern matching. If no name filter is specified, the rule applies to all objects in the bucket. [Learn more about using object name filters](#)

You can add object filters in any order. Object Lifecycle Management takes care of the evaluation precedence.

+ Add Filter



Create

Cancel

Delete

# Life Cycle



## Create Lifecycle Rule

Name: Example Rule

Target:

- Latest Version of Objects**  
Create a lifecycle rule that applies to the latest version of either:
  - All objects in the bucket
  - Objects that match the object name filters that you specify
- Previous Versions of Objects**  
Create a lifecycle rule that applies to the previous versions of either:
  - All objects in the bucket
  - Objects that match the object name filters that you specify
- Uncommitted Multipart Uploads**  
Create a lifecycle rule that deletes uncommitted or failed multipart uploads.

Lifecycle Action: Move to Archive

Number of Days: 30

Archive objects that are older than 30 days and that match any of the specified object name filters.

**Object Name Filters (Optional)**

Use object name filters to specify which objects the lifecycle rule applies to. You can choose objects using prefixes and pattern matching. If no name filter is specified, the rule applies to all objects in the bucket. [Learn more about using object name filters](#)

You can add object filters in any order. Object Lifecycle Management takes care of the evaluation precedence.

+ Add Filter

**Create** **Cancel**

Delete

# Auto-Tiering



Moves objects between standard and infrequent access based on access patterns

# Auto-Tiering



Auto-tiering does **not** incur any minimum retention penalties.

Moves objects between standard and infrequent access based on access patterns

# Auto-Tiering

## Edit Auto-Tiering

Auto-Tiering directs Object Storage to automatically move objects that you have not accessed for 31 days to the Infrequent Access tier. If Object Storage moved objects to the Infrequent Access tier that are subsequently accessed more frequently, the objects are automatically moved back to the Standard tier without incurring retrieval and prorated storage fees.

Enable Auto-Tiering

[Save Changes](#) [Cancel](#)

Moves objects

## Oracle Cloud Infrastructure

# Calculate and Optimize Cost: Networking

## Ingress, Egress, VPN, and FastConnect

# Ingress & Egress Cost



Ingress is **free**.



Egress up to **10TB/month** is free.



Egress beyond 10TB/month is charged based on **region**.

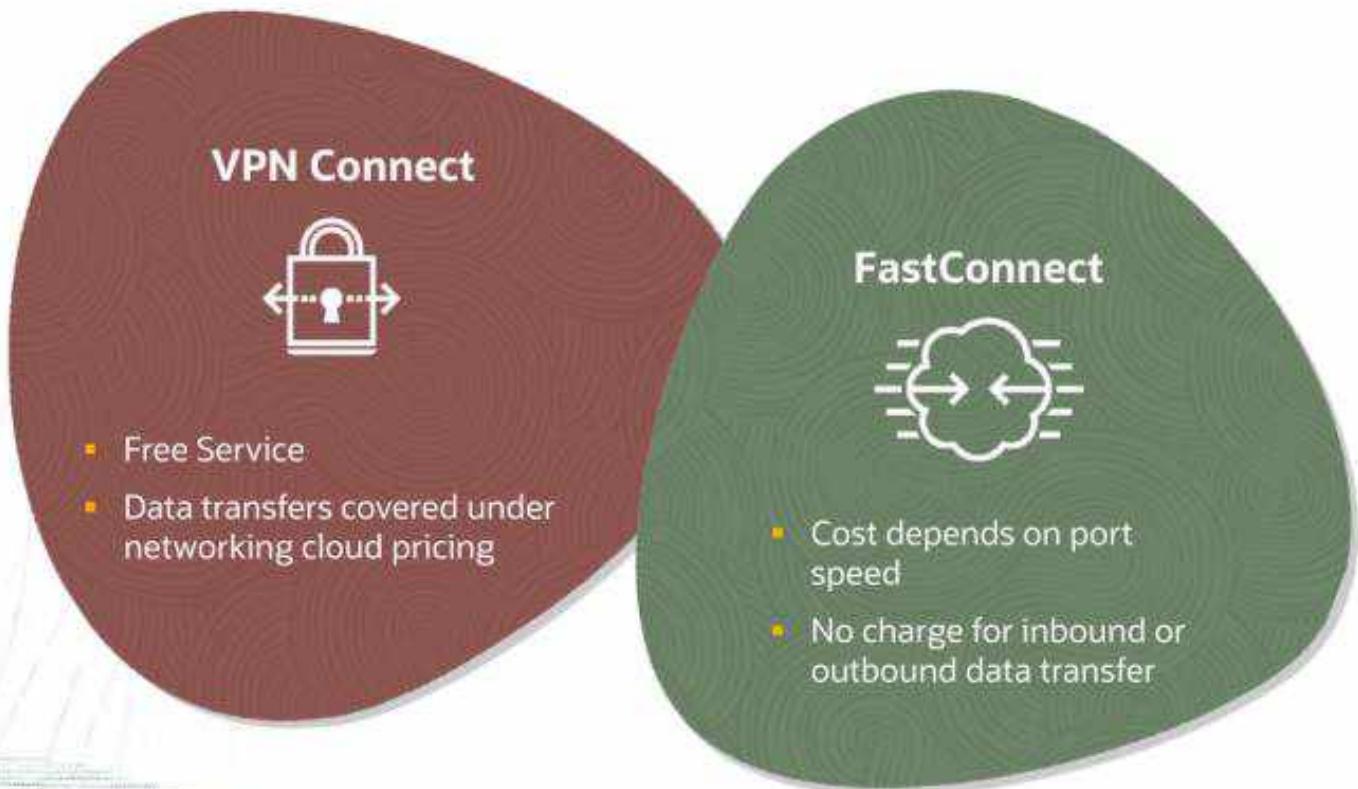
# Ingress & Egress Cost



Egress beyond 10TB/month is charged based on **region**.

Region of Origin	GB per Month
› North America, Europe, and UK	\$0.0085
› APAC, Japan and South America	\$0.025
› Middle East and Africa	\$0.05

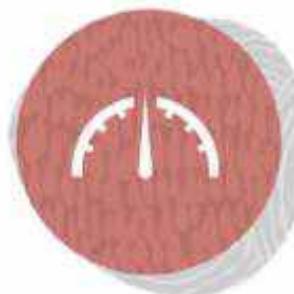
## VPN Connect vs FastConnect Pricing



## FastConnect Pricing



**1 Gbps**  
**\$0.2125**  
Per Port Hour  
↓  
**\$158**  
Per Port Month



**10 Gbps**  
**\$1.275**  
Per Port Hour  
↓  
**\$949**  
Per Port Month



**100 Gbps**  
**\$10.75**  
Per Port Hour  
↓  
**\$7998**  
Per Port Month

## Oracle Cloud Infrastructure

### Software Licensing on OCI

#### Oracle, Microsoft, and Third-party Licenses

# Licensing Models

## License Included

- › Software is licensed on-demand
- › Billed for software and infrastructure

## Bring Your Own License (BYOL)

- › Use existing license
- › Billed only for infrastructure

cloud.oracle.com

ORACLE Cloud Search resources, services, documentation, and marketplace.

US West (Phoenix)

Roving Edge Exportability

Publisher

Category

Price

Any

Any

Any

Any

ORACLE E-Business Suite

Altair

CHECK POINT

CloudGuard Next-Gen Firewall with Threat Prevention and...

Advanced Threat Prevention for OCI and Hybrid Cloud...

Type: Image Price: Free

Altair PBS Professional

Workload Manager and Batch Queuing Software

Type: Image Price: BYOL

Aviatrix Secure Networking Platform

Multi-Cloud Cross-Region Aviatrix Controller (PayAsYouGo version)

Type: Stack Price: Paid

Oracle Enterprise Session Border Controller

Enabling highly secure and reliable voice, video and unified...

Type: Image Price: BYOL

Rackware Migration Manager (RMM)

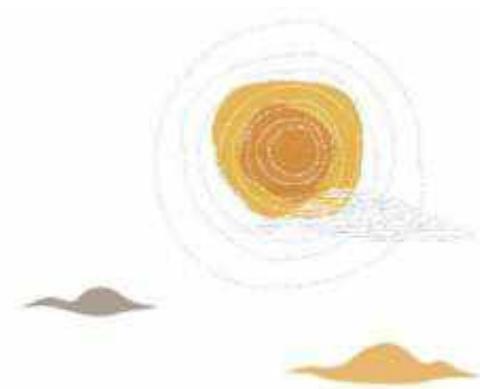
Migrate running workloads into Oracle Cloud Infrastructure

Type: Image Price: Paid

Terms of Use and Privacy | Cookie Preferences

Copyright © 2022, Oracle and/or its affiliates. All rights reserved.

# Licensing Models



## License Included

- › Software is licensed on-demand
- › Billed for software and infrastructure

For Oracle Database:

- › Can use any database options
- › No additional support fees

## Bring Your Own License (BYOL)

- › Use existing license
- › Billed only for infrastructure

For Oracle Database:

- › Can only use options in existing license
- › Continue paying support stream

The screenshot shows the Oracle Cloud interface for creating a Database System. The top navigation bar includes the Oracle Cloud logo, a search bar, and various account settings. The main title is "Create DB System". On the left, there are two tabs: "DB System Information" (selected) and "Database Information".  
  
The central area is titled "Choose a license type" and contains two options:

- License Included**: Subscribes to new Oracle Database software licenses and the Database service.
- Bring Your Own License (BYOL)**: Allows bringing organization's Oracle Database software licenses to the Database service. A link to "Learn more" is provided.

  
Below this, the section "Specify the network information" includes:

- "Virtual cloud network in": A dropdown menu with "Change Compartment" and "Select a virtual cloud network".
- "Client subnet in": A dropdown menu with "Change Compartment" and "Select a virtual cloud network first". A note below states: "Do not use a subnet that overlaps with 172.16.16/28, which is used by the Oracle Clusterware private interconnect on the database instance."
- A checkbox for "Use network security groups to control traffic" with a help icon.
- "Hostname prefix": A text input field.
- "Host domain name": A dropdown menu with "Read Only".

  
At the bottom, there are "Next" and "Cancel" buttons, along with links for "Terms of Use and Privacy" and "Cookie Preferences". A copyright notice at the bottom right reads: "Copyright © 2022, Oracle and/or its affiliates. All rights reserved."

# Licensing Models

## License Included

- › Software is licensed on-demand
- › Billed for software and infrastructure

For Microsoft Windows:

- › Three options
  - › Platform Image
  - › Bring your own image (BYOI) on a VM

## Bring Your Own License (BYOL)

- › Use existing license
- › Billed only for infrastructure

For Microsoft Windows:

In the console, when you provision a VM compute instance:

The screenshot shows two overlapping windows from the Oracle Cloud Infrastructure console.

**Create compute instance** window (left):

- Image and shape**: A section describing what a shape is and showing a Windows Server 2019 Standard image build from 2022-05-29-0.
- Image**: Shows the Windows Server 2019 Standard image icon.
- Shape**: Shows an AMD VM.Standard.E4.Flex shape.
- Networking**: Buttons for Create, Save as stack, and Cancel.

**Browse all images** window (right):

- Image source**: A list of sources including Platform Images (selected), Oracle Images, Partner Images, Custom Images, Community Images, Boot volumes, and Image OCID.
- Table**: A list of available images with columns for Image name, OS version, Image build, and Advanced options.

Image name	OS version	Image build	
Canonical Ubuntu	22.04	2022-05-17-0	<a href="#">Advanced options</a>
CentOS	8 Stream	2022-05-28-0	<a href="#">Advanced options</a>
Oracle Autonomous Linux	7.9	2022-05-0	<a href="#">Advanced options</a>
Oracle Linux	8	2022-05-31-0	<a href="#">Advanced options</a>
Oracle Linux Cloud Developer	8	2022-05-22-0	<a href="#">Advanced options</a>
Windows	Server 2019 Standard	2022-05-20-0	<a href="#">Advanced options</a>

# Licensing Models

## License Included

- › Software is licensed on-demand
- › Billed for software and infrastructure

For Microsoft Windows:

- › Three options
  - › Platform Image
  - › Bring your own image (BYOI) on a VM
  - › Bring your own Hyper-V on a BM

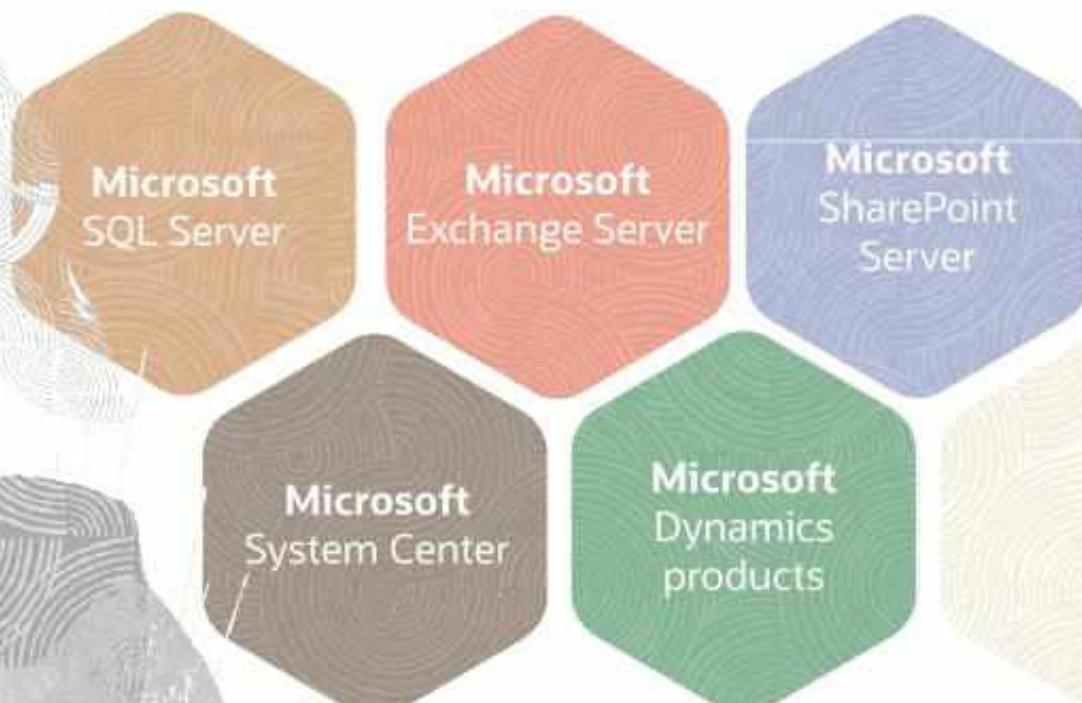
## Bring Your Own License (BYOL)

- › Use existing license
- › Billed only for infrastructure

For Microsoft Windows:

- › Bring your own image (BYOI) on a BM
- › Requires License Mobility through active Software Assurance

# Licensing Mobility through Software Assurance



## Bring Your Own License (BYOL)

- › Use existing license
  - › Billed only for infrastructure
- For Microsoft Windows:
- › Bring your own image (BYOI) on a BM
  - › Requires License Mobility through active Software Assurance

Microsoft | **Licensing** Learn Purchase Manage Get Support Licensing News All Microsoft

# License Mobility through Software

With License Mobility through Software Assurance, you can deploy certain server application licenses purchased under your Volume Licensing agreement in an Authorized Mobility Partner's datacenter.



Why use License Mobility? How to use License Mobility

Use License Mobility to extend the value of your server application licenses by deploying them on-premises or in the cloud, and to take advantage of the lowest cost computing infrastructure for changing business priorities.

## Why use License Mobility?

### Enhanced deployment value

License Mobility through Software Assurance enhances the value of volume licenses with Software Assurance by extending their use to the cloud. This benefit can also help you lower your operating costs by using an Authorized Mobility Partner's shared infrastructure.

### Flexible deployment choices

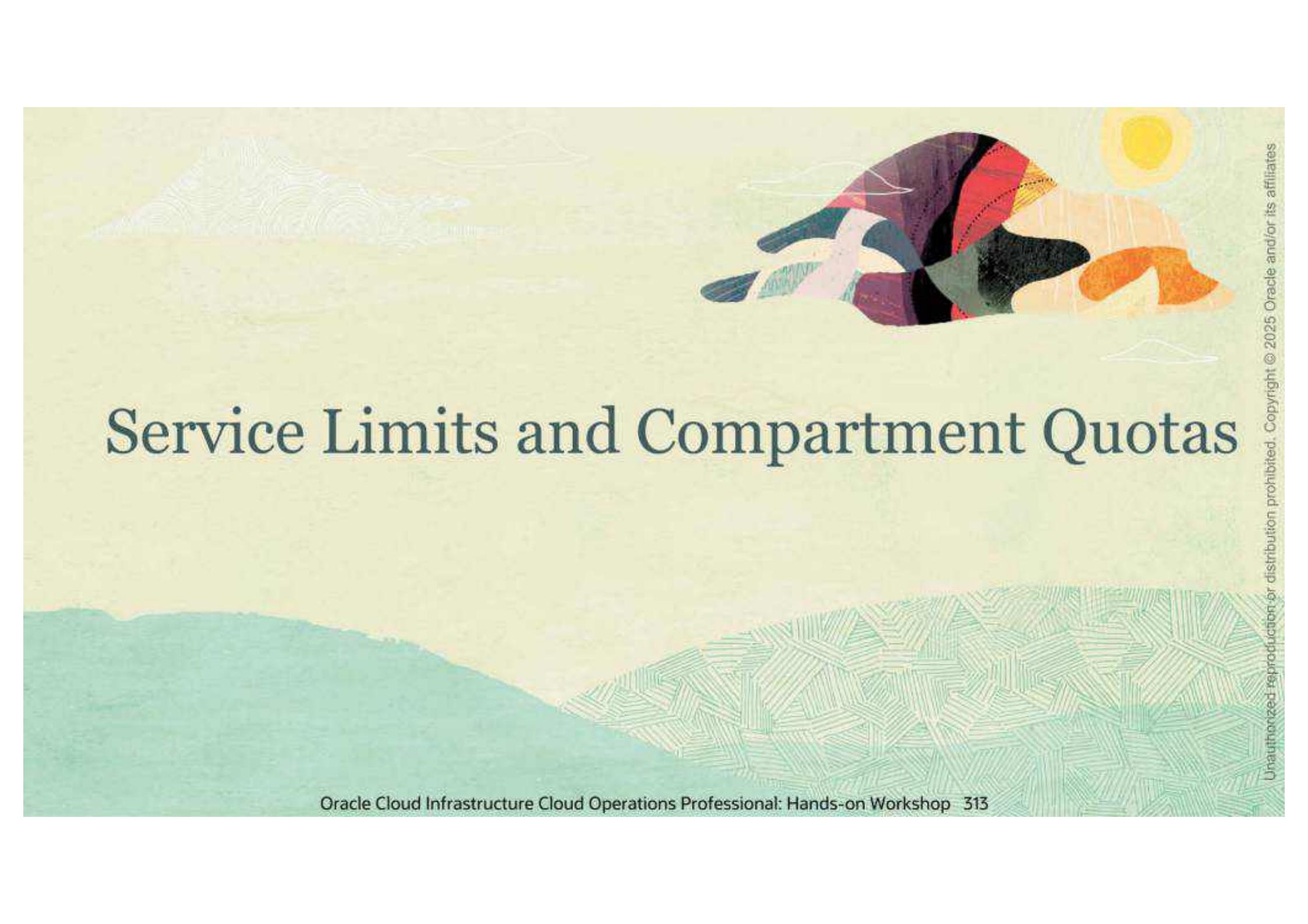
By extending License Mobility to the cloud, Software Assurance lets you choose between deploying on-premises or through an Authorized Mobility Partner's Infrastructure as a Service (IaaS) offering. Such instances can be run on shared hardware with the applications dedicated to your organization.

### Application server coverage

Application server products eligible for License Mobility through Software Assurance, including Microsoft Exchange Server, Microsoft SharePoint Server, and Microsoft SQL Server, are identified in the [Microsoft Product Terms](#).

For SQL Server customers with core-based licensing and Software Assurance coverage, broader benefits are available under [Azure Hybrid Benefit rights](#). The steps described below do not apply to Azure Hybrid Benefit use.

Windows Server is not eligible for License Mobility through Software Assurance and must be provided by your chosen Authorized Mobility Partner.



# Service Limits and Compartment Quotas



# Governance & Administration

Operations Associate

## Oracle Cloud Infrastructure

# View and Manage Service Limits

# Service Limit



Is the quota or allowance set on a resource

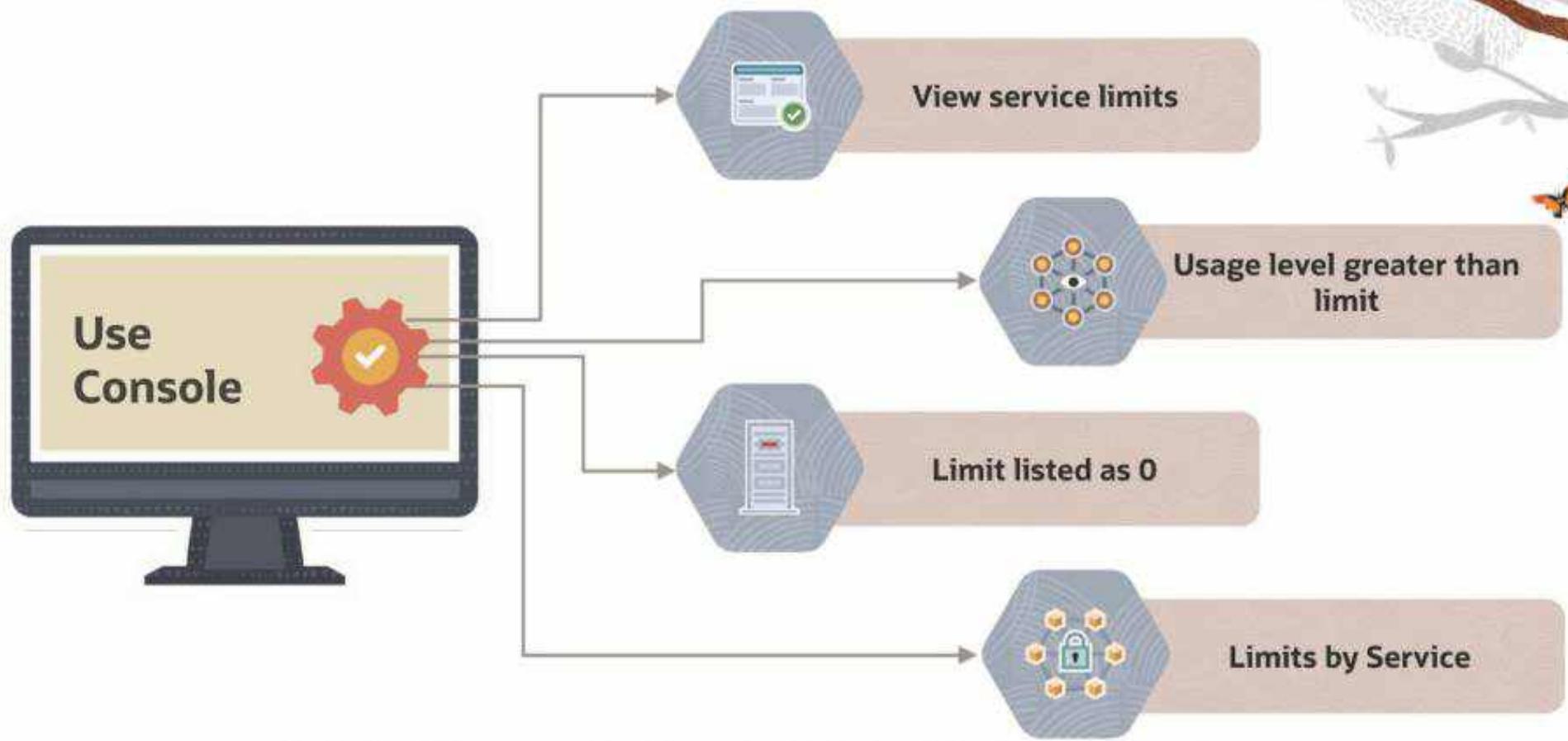
Is configured for tenancy

Has limits set by Oracle Sales Representative

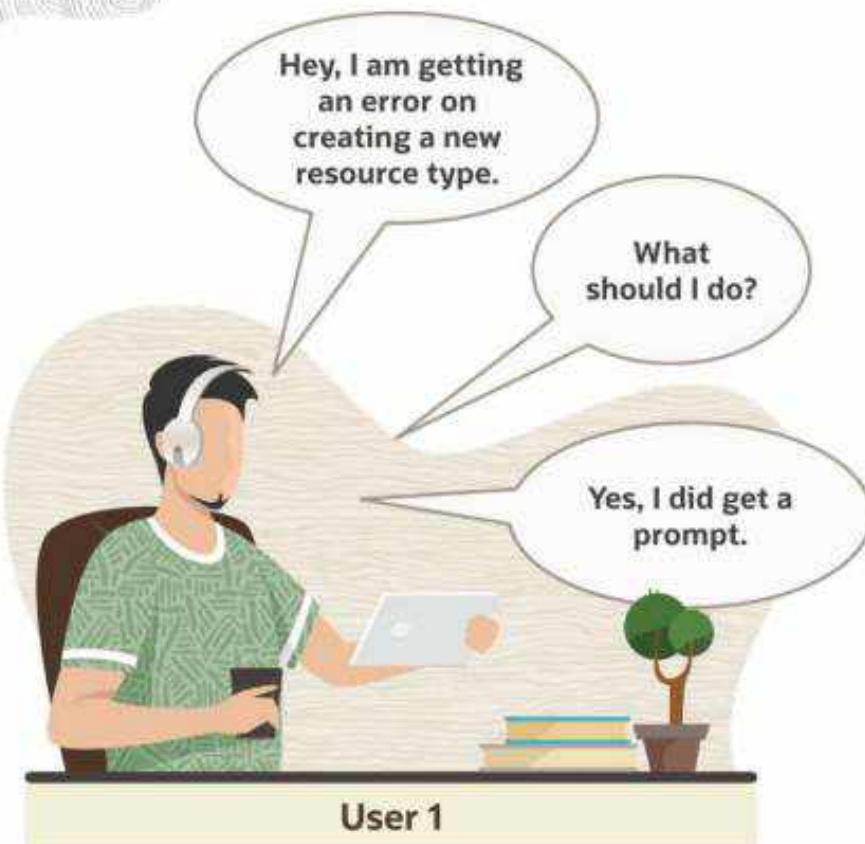
May be increased



## View Service Limits and Usage



# When You Reach a Service Limit



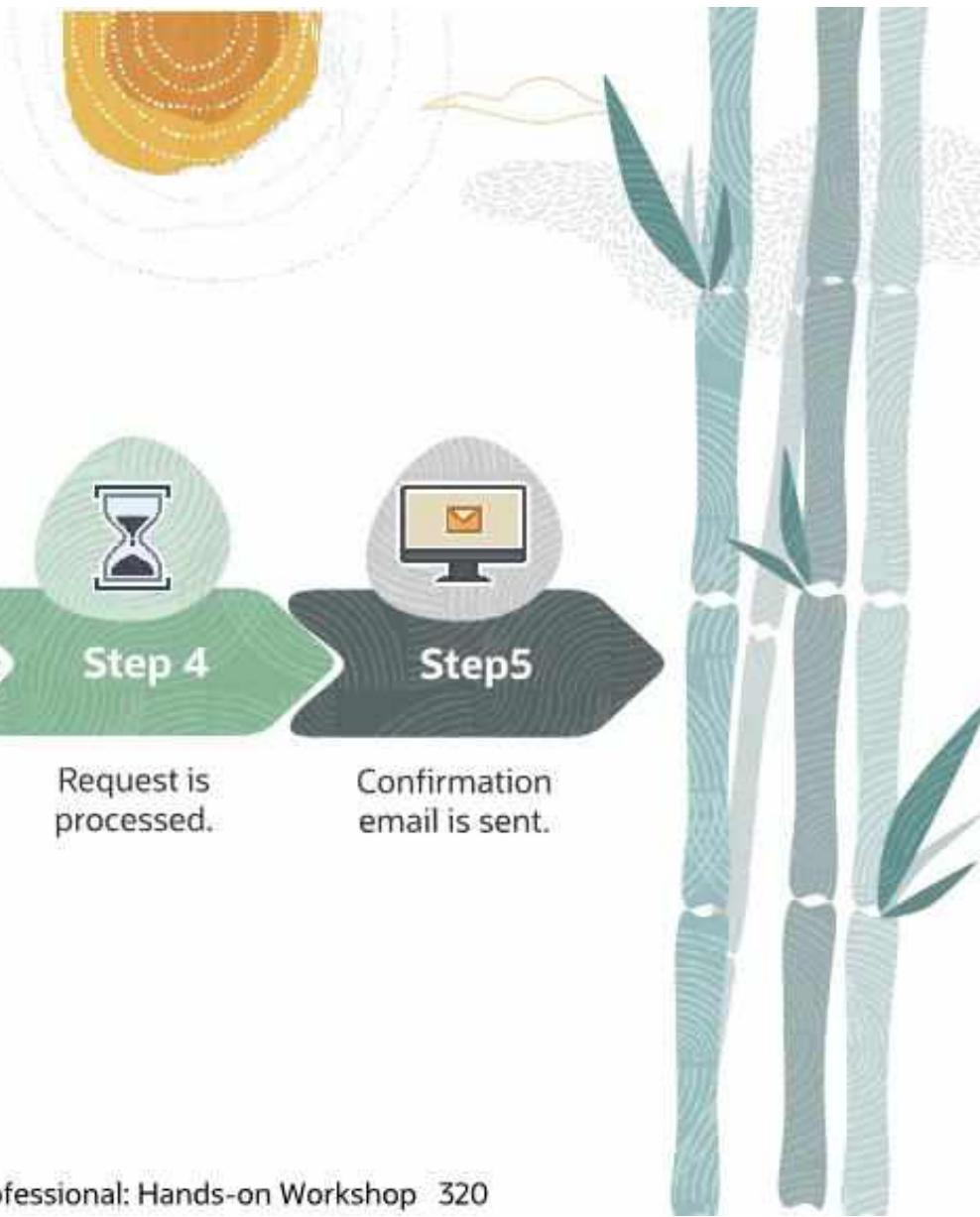
## Submit Request



# Demo

---

## Request a Service Limit Increase





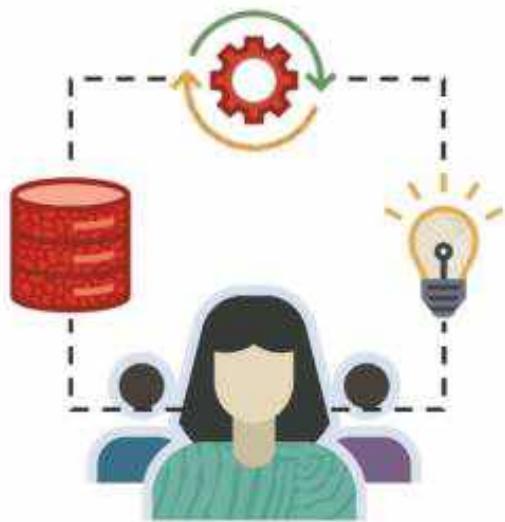
# Governance & Administration

Operations Associate

Oracle Cloud Infrastructure

# Set Resource Caps with Quotas

# Compartment Quotas



Control resource consumption



Set by administrators



Set using policy statements

# Types of Quota Policy Statements



**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



# Demo

---

## Create a Quota Policy



# Oracle Cloud Infrastructure Cloud Advisor

## In this Lesson...

- ❖ What is Cloud Advisor?
- ❖ How Cloud Advisor works?
- ❖ Benefits of using Cloud Advisor
- ❖ Recommendation Categories & Statuses
- ❖ Cloud Advisor Calculations





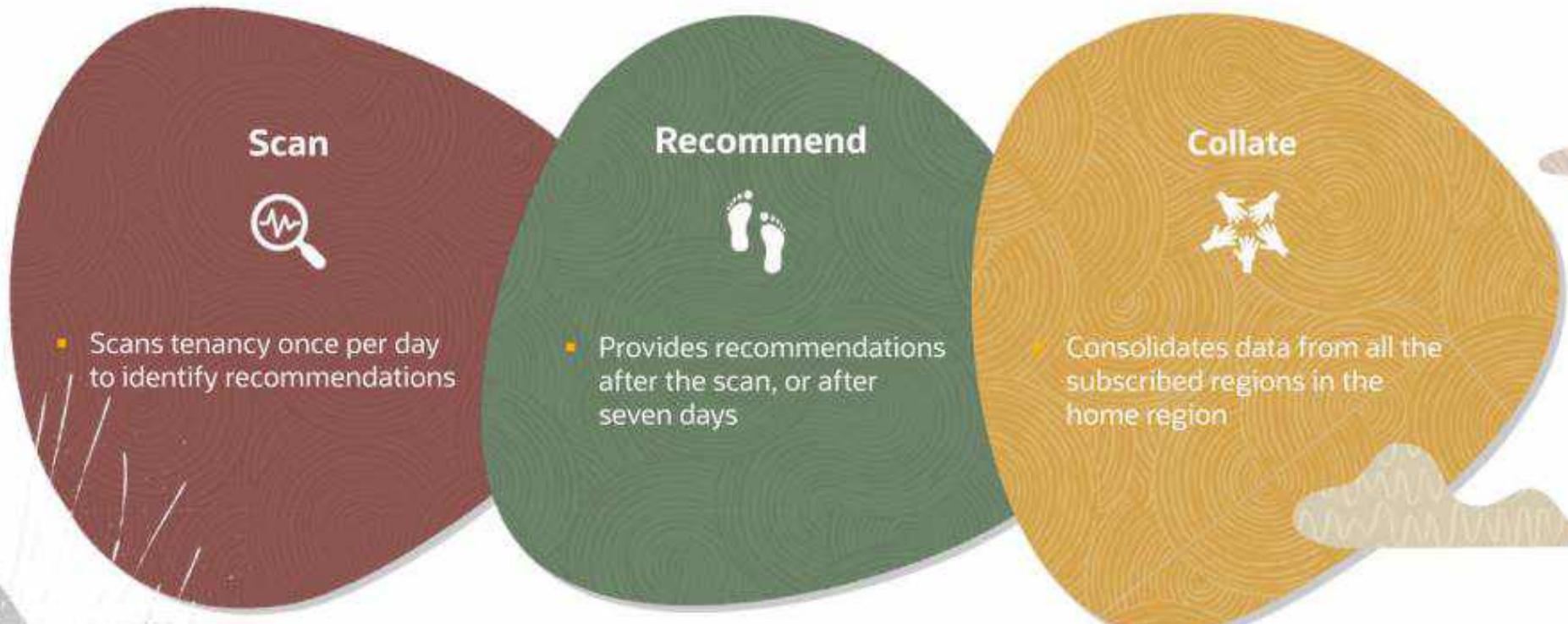
# What Is Cloud Advisor?

Finds inefficiencies in your tenancy and helps address them using guided solutions

- Required IAM Policy  
Allow group OptimizerAdmins to manage optimizer-api-family in tenancy
- Check or update Enrollment Status

<p>Cloud Advisor</p> <hr/> <p><a href="#">Overview</a></p> <p><a href="#">Recommendations</a></p> <p><a href="#">Work Requests</a></p> <p><a href="#">History</a></p> <p><a href="#">Settings</a></p>	<p><b>Settings</b></p> <hr/> <p>Cloud Advisor is <u>currently active</u>. Cloud Advisor provides recommendations to help you maximize cost savings and improve security in your tenancy. It finds inefficiencies in your tenancy and provides guided solutions explaining how to fix them. In addition, built-in Cloud Guard recommendations help you see and address security vulnerabilities.</p> <p><a href="#">Disable Cloud Advisor</a></p> <hr/> <p><b>Customizations and overrides</b></p>
---	---

# How Cloud Advisor Works

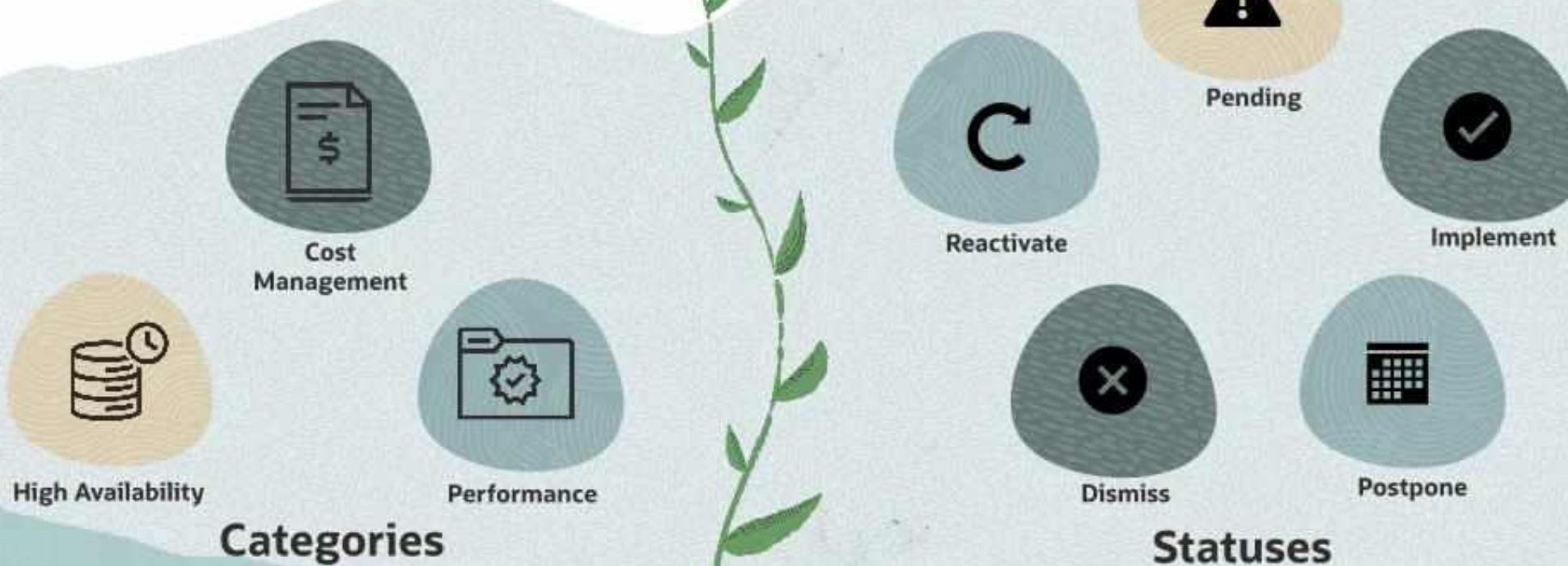




## Benefits of Using Cloud Advisor



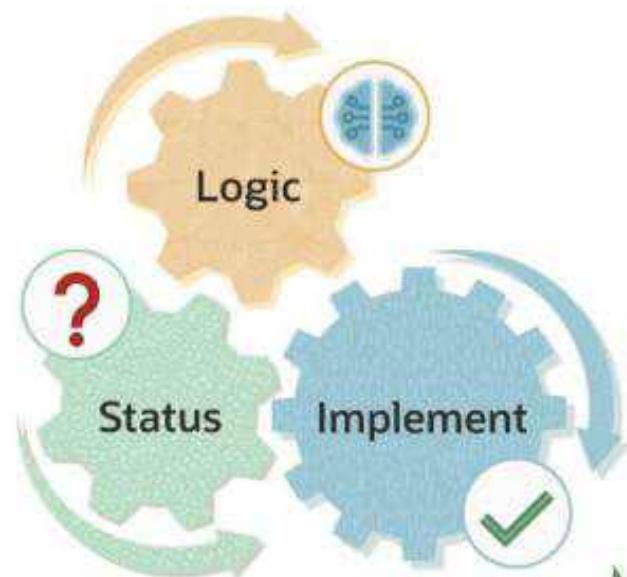
# Recommendation Categories & Statuses



# Cloud Advisor Calculations

# High Availability Recommendation Calculations

Improve fault tolerance

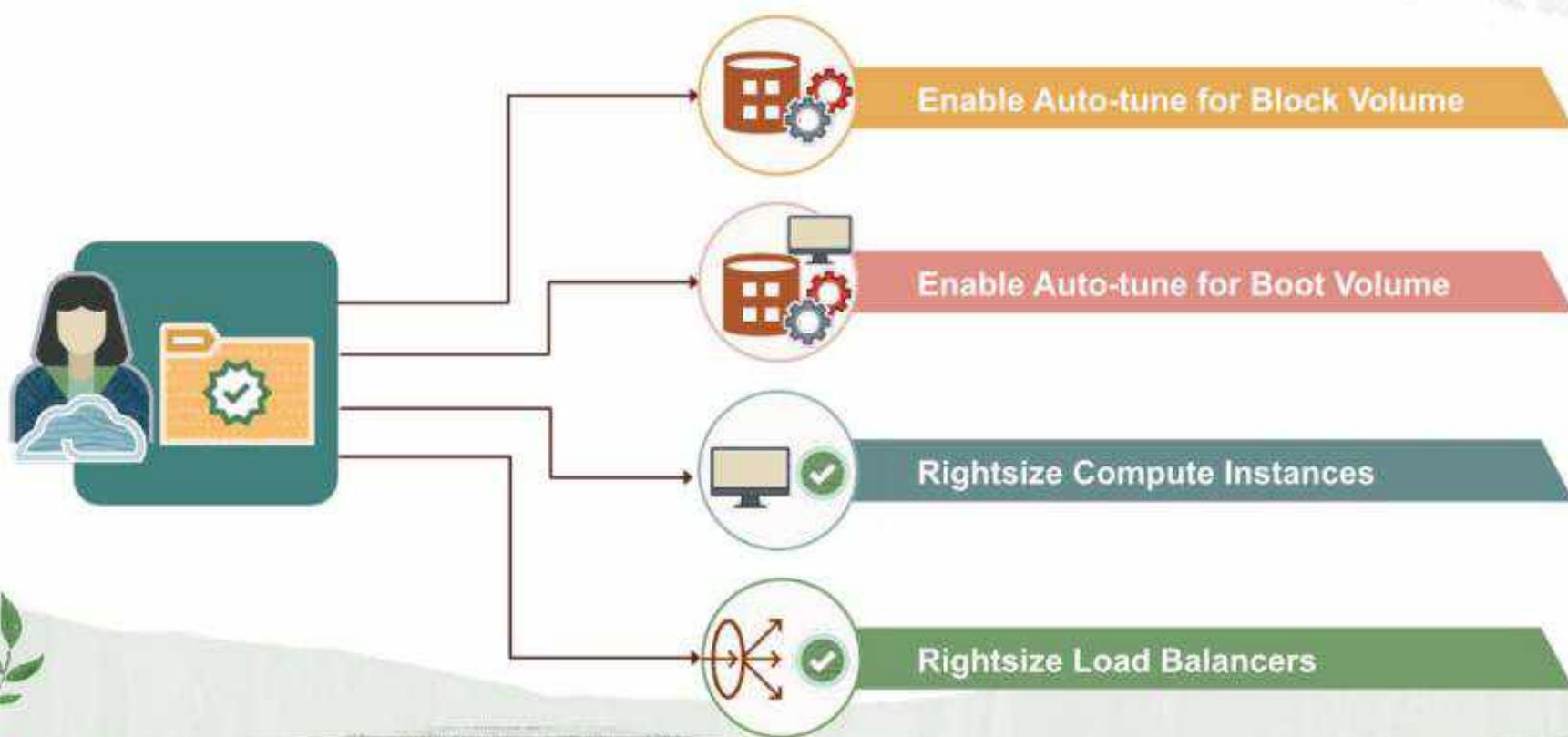


When all VMs are in a single fault domain

Spread instances across multiple fault domains

Pending to Implemented after next scan

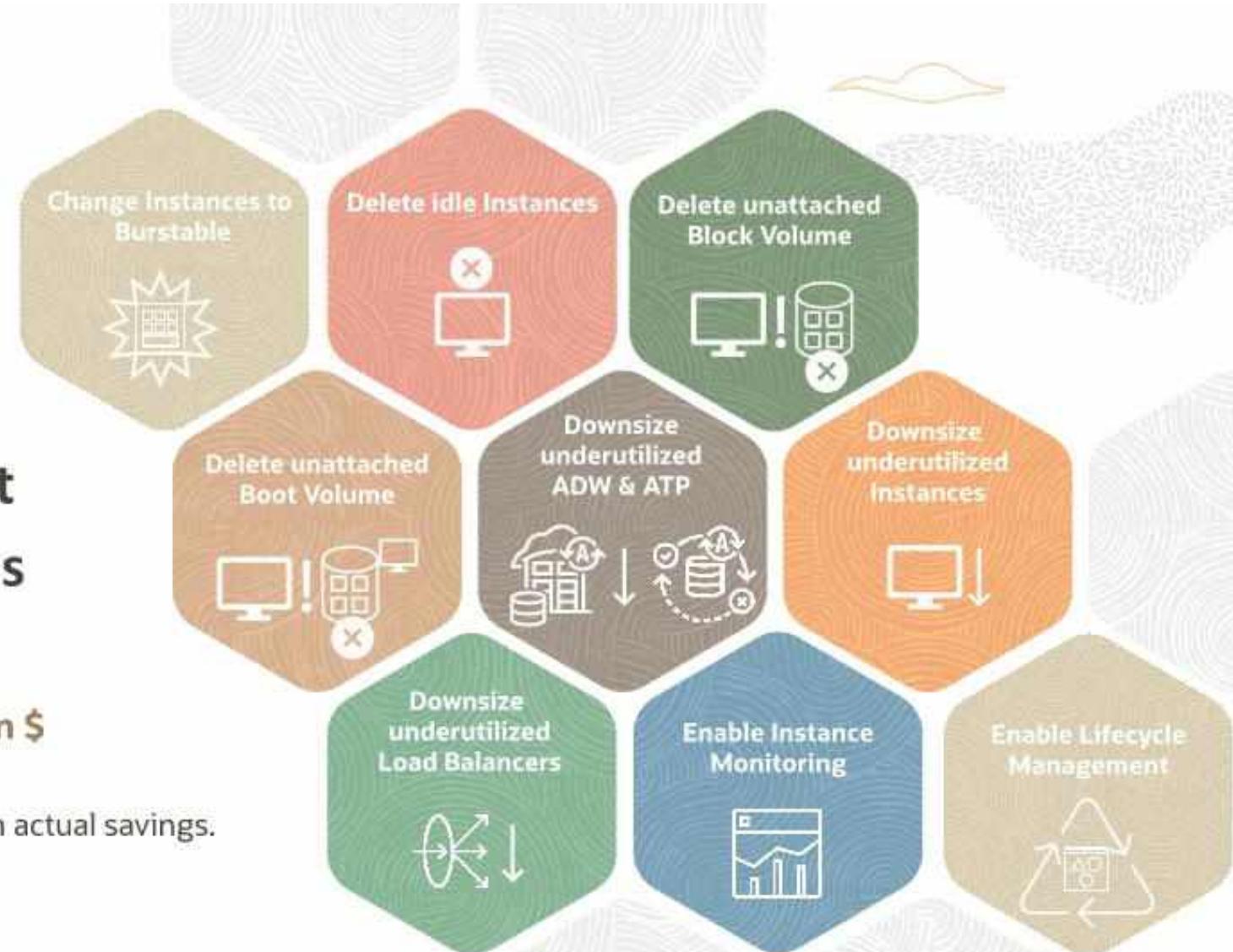
# Performance Recommendation Calculations



## Cost Management Recommendations

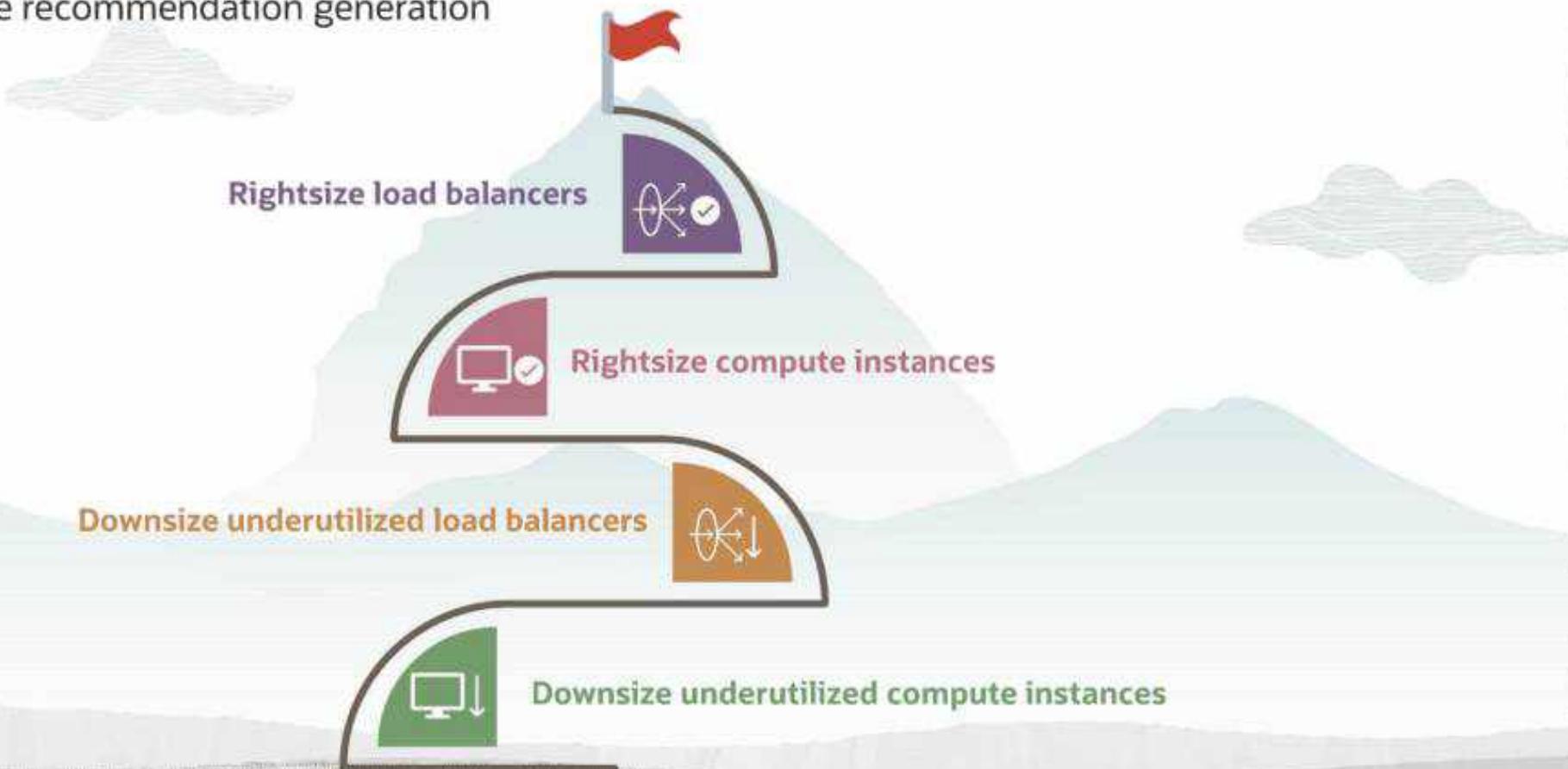
Shows estimated savings in \$

Estimated savings may vary from actual savings.



# Recommendation Profiles

Customize recommendation generation



# Recommendation Profile: Load Balancers

Profiles to rightsize or downsize load balancers



Description	Rightsize	Downsize
Conservative	PeakBandwidth > 95% max bandwidth	PeakBandwidth < 85% min bandwidth
Standard	PeakBandwidth > 85% max bandwidth	PeakBandwidth < 90% min bandwidth
Aggressive	PeakBandwidth > 75% max bandwidth	PeakBandwidth < 95% min bandwidth

# Recommendation Profile: Compute Instances

Profiles to rightsize or downsize Compute Instances



Description	Rightsize	Downsize
Conservative	avg or p95 CPU > 95% max memory > 95%	avg or p95 CPU < 5% max memory < 10% max network < 3%
Standard	avg or p95 CPU > 80% max memory > 80%	avg or p95 CPU < 10% max memory < 10% max network < 3%
Aggressive	avg or p95 CPU > 60% max memory > 60%	avg or p95 CPU < 15% max memory < 10% max network < 3%

Oracle Cloud Infrastructure  
**Organization Management**

# Organization Management: Overview

The Organization Management enables you to manage multiple tenancies and map the subscriptions. There are two types of tenancies involved.



## Parent Tenancy

A tenancy that is associated with the primary funded subscription



## Child Tenancy

A new or existing tenancy that is mapped to another subscription

You can invite new or existing child tenancies to join the parent tenancy and become a part of the same organization.

# Why choose multitenancy approach?

- 
- Monitor cost and usage information centrally.
  - Deploy strong level of data isolation.
  - Avoid cost overages and get consolidated billing.
  - Involve separate security and governance settings.

# Manage Multitenancy

The following actions can be performed from the **Organization Management** page of the console to manage multiple tenancies:

## Create

Create a new child tenancy from a parent tenancy and remap if required.

## Invite

Invite an existing tenancy to consume from your subscription.

## Revoke and Remove

Revoke an invitation sent to a child tenancy and remove an invited tenancy.

## Map Subscription

Map the tenancies to the subscriptions as needed.

## Cost Reporting Integration

The multitenancy approach with Organization Management helps you manage the cost and usage in an effective way.

A parent tenancy can:

- View the cost and usage information across tenancies
- Use the cost analysis and reporting features to manage organization's spending
- Gain better insights on the subscription entirely and the granular breakdown of the spending

A child tenancy can:

- View the cost and usage information of its tenancy
- Create budget in the child tenancy



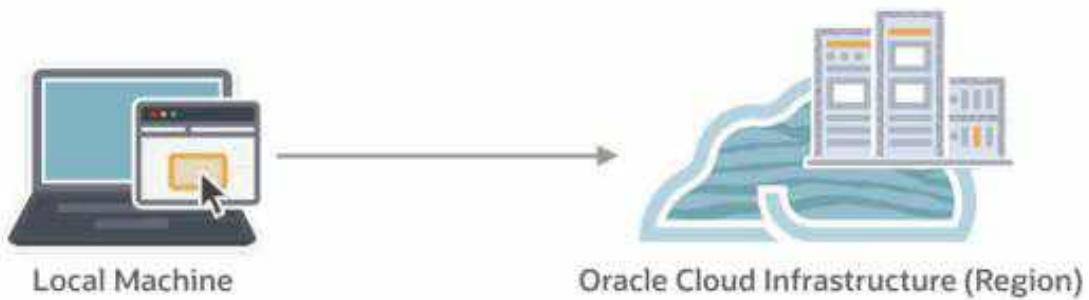
# OCI Command Line Interface (CLI) and Software Development Kit (SDK)

Oracle Cloud Infrastructure

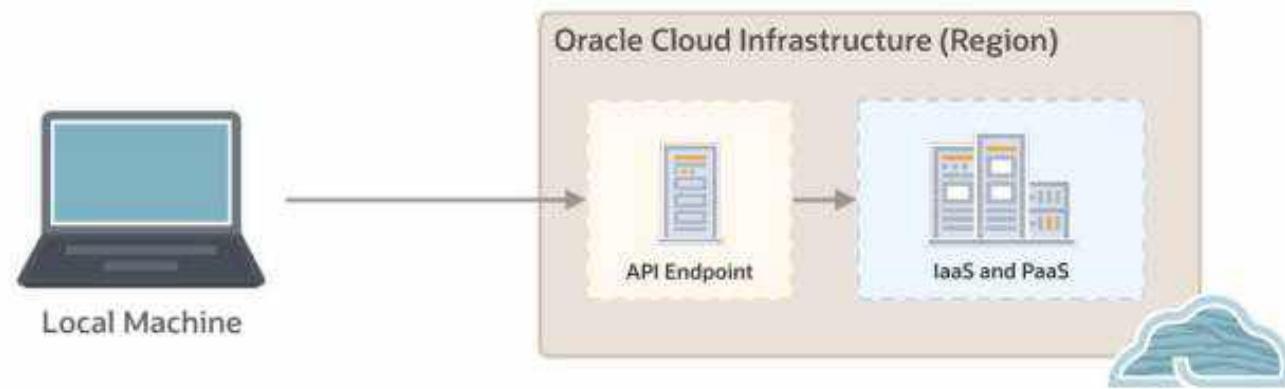
# Interacting with OCI

**The Console, CLI, SDK, and REST API**

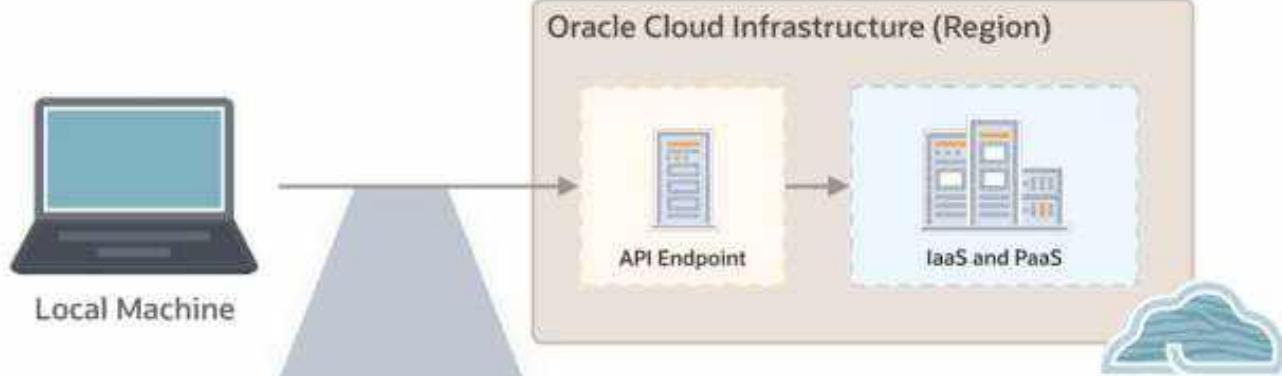
## Interacting with OCI



## REST API



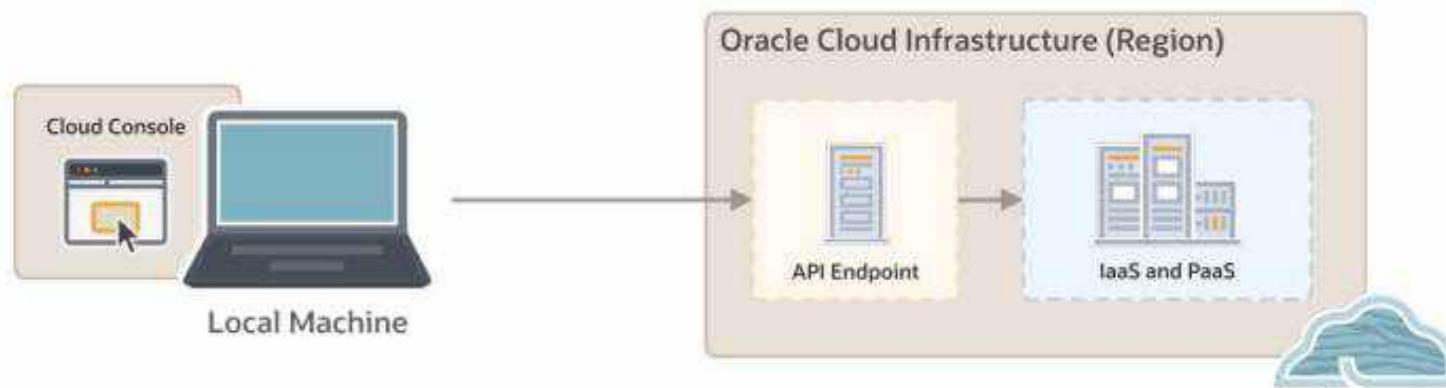
## REST API



### Example API Request

```
POST https://iaas.us-phoenix-1.oraclecloud.com/20160918/vcn  
host: iaas.us-phoenix-1.oraclecloud.com  
opc-retry-token: 239787fs987  
Content-Type: application/json  
HTTP headers required for authentication  
Other HTTP request headers per the HTTP spec  
{  
    "compartmentId": "ocid1.compartment.oc1..exampleid",  
    "displayName": "Virtual Cloud Network",  
    "cidrBlock": "172.16.0.0/16"  
}
```

## Cloud Console



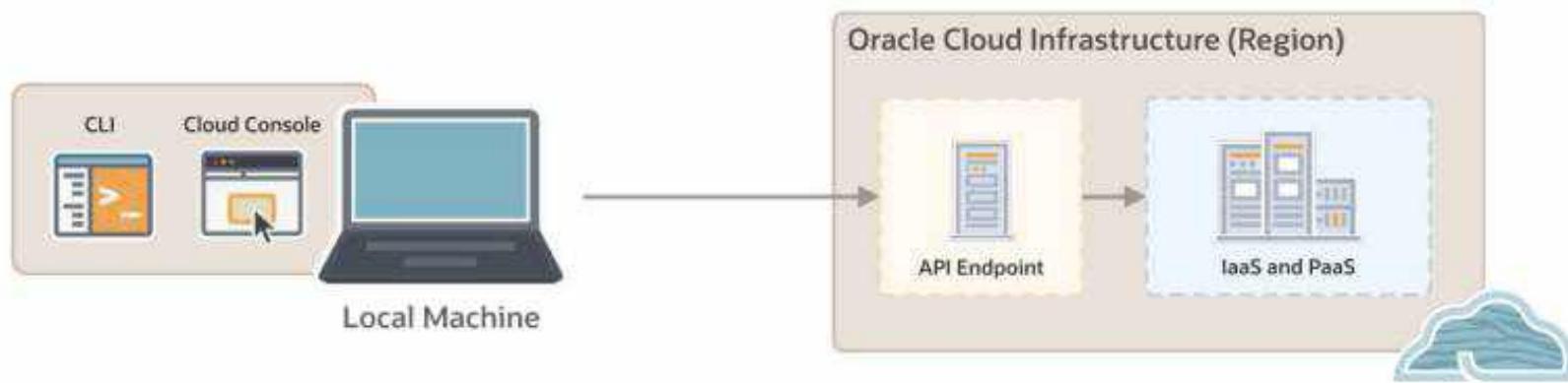
## Cloud Console



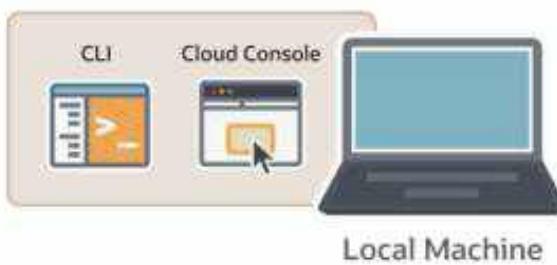
Local Machine

A screenshot of the Oracle Cloud Get Started dashboard. The top navigation bar includes 'Get Started' and 'Dashboard'. The main area is titled 'Quickstarts' and contains four cards: 'Deploy the result of the next race' (with a 'Deploy Now' button), 'Deploy Containerized Workloads' (with a 'Deploy Now' button), 'Deploy a one-click Apache Autonomous Database using ARDS' (with a 'Deploy Now' button), and 'Deploy a MySQL in a Container' (with a 'Deploy Now' button). Below this is a section titled 'Launch Resources' with four cards: 'Create a VPC instance' (with a 'Create Now' button), 'Create an ADP database' (with a 'Create Now' button), 'Create an Autonomous Database' (with a 'Create Now' button), and 'Create a MySQL instance' (with a 'Create Now' button). On the right side of the dashboard, there is a sidebar titled 'Account Center' containing 'User Management' (with a 'User Management' button), 'Cost Management Settings' (with a 'Cost Management Settings' button), and 'What's New' (with a 'What's New' button). The 'What's New' section lists several recent updates.

## Command Line Interface (CLI)



## Command Line Interface (CLI)



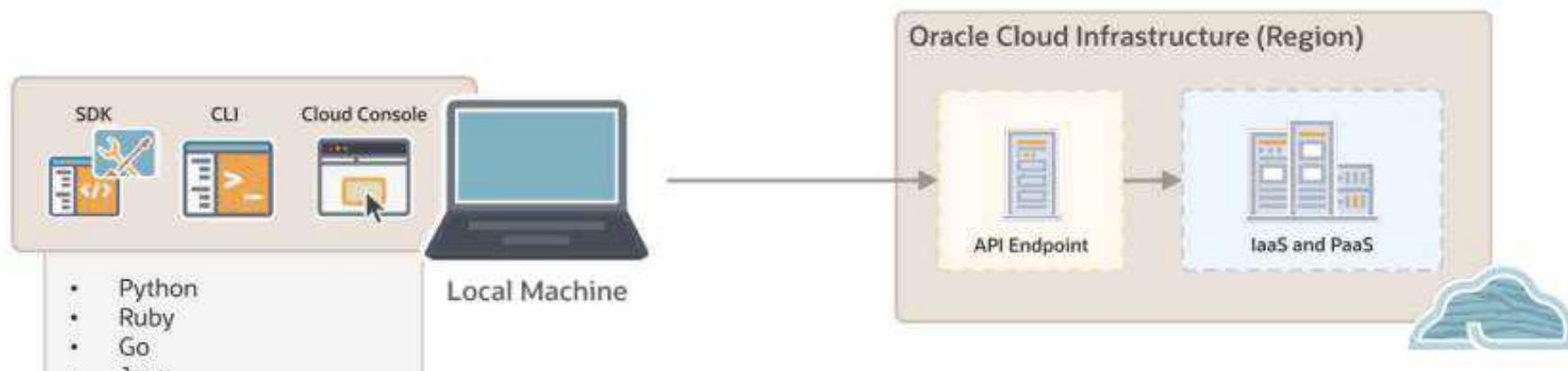
```
[myinstance@myhost ~] $ oci compute
Usage: oci compute [OPTIONS] COMMAND [ARGS]...

Compute Service CLI

Options:
  -?, -h, --help  For detailed help on any of these individual commands, enter
                  <command> --help.

Commands:
  boot-volume-attachment      Represents an attachment between a...
  capacity-reservation        A template that defines the...
  console-history             An instance's serial console data.
  dedicated-vm-host           A dedicated virtual machine host...
  dedicated-vm-host-instance  Condensed instance data when...
  device                      Device Path corresponding to the...
  global-image-capability-schema Global Image Capability Schema
  global-image-capability-schema-version Global Image Capability Schema...
  image                       A boot disk image for launching an...
  image-capability-schema     Image Capability Schema
  image-shape-compatibility-entry An image and shape that are...
  instance                     A compute host.
  instance-console-connection The 'InstanceConsoleConnection'...
  measured-boot-report        The measured boot report for a...
  pxe                         Partition Image Catalog (PIC).
  shape                       A compute instance shape that can...
```

## Software Development Kit (SDK)



## Software Development Kit (SDK)



A screenshot of a code editor showing a Python script named 'sdk-example.py'. The code uses the OCI Python SDK to create a virtual network. It imports the necessary modules, creates a configuration object, and then creates a client for the VirtualNetworkClient. It defines a 'ven\_model' object with compartment details and CIDR blocks, and finally creates the virtual network using the client.

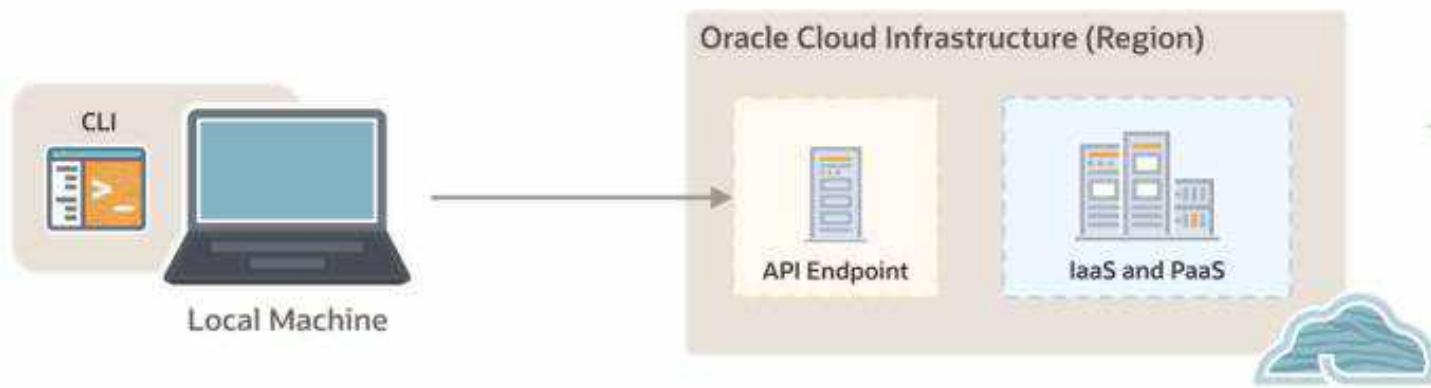
```
 sdk-example.py - pyv  
sdk-example.py •  
sdk-example.py ...  
1 import os  
2  
3 import oci  
4  
5 # Create a Configuration  
6 config = oci.config.from_file()  
7  
8 # Create a Client  
9 from oci.core import VirtualNetworkClient  
10 client = VirtualNetworkClient(config)  
11  
12 # Create a Model  
13 from oci.core.models import CreateVcnDetails  
14 vcn_model = CreateVcnDetails(  
15     compartment_id=os.environ.get('compartment_ocid'),  
16     cidr_blocks=['10.0.0.0/24', '172.16.0.0/24'],  
17     display_name='50K VCN',  
18 )  
19  
20 # Create the VCN  
21 client.create_vcn(vcn_model)
```

# Oracle Cloud Infrastructure OCI CLI Authentication

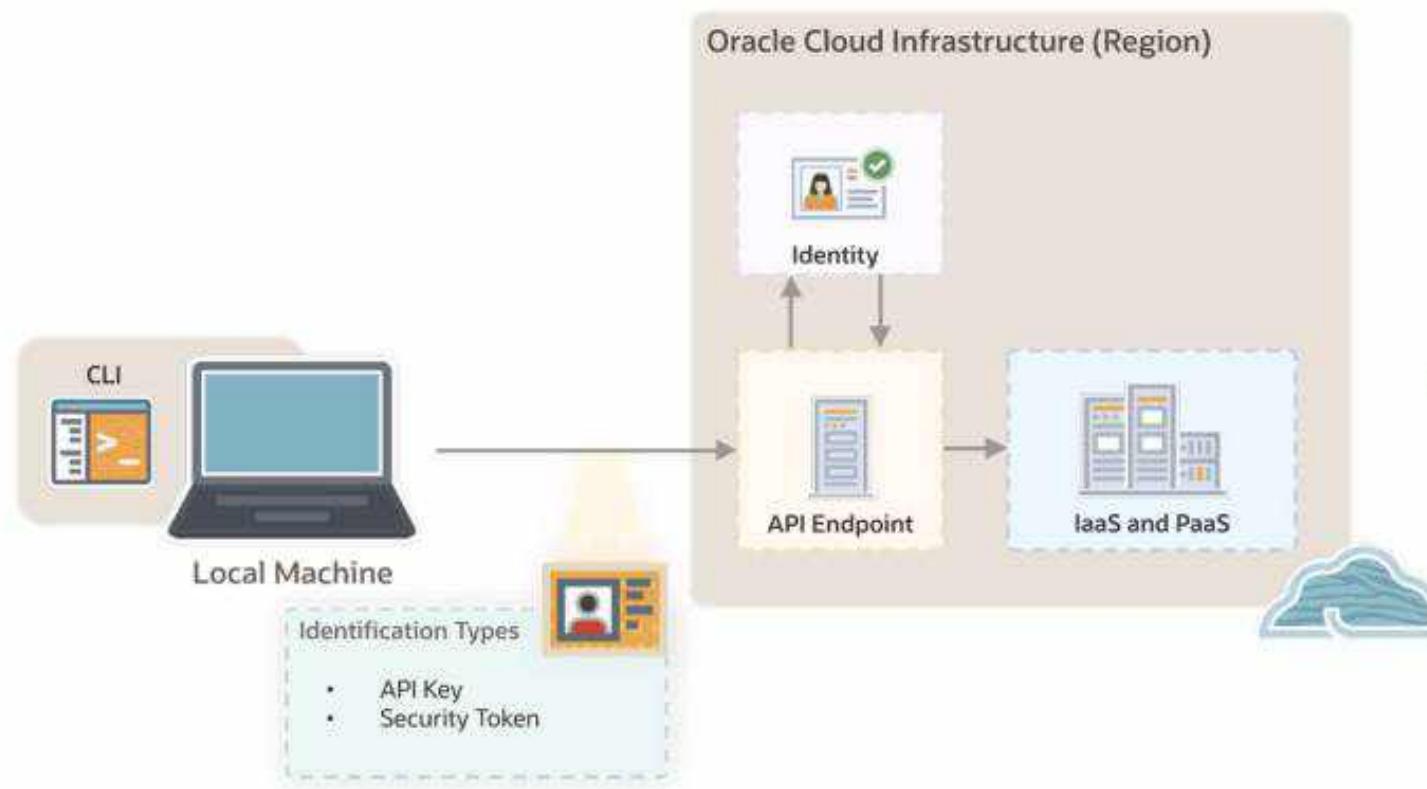
API Keys, Security Tokens, Instance Principles, and more...

## Recall

---



# Authentication



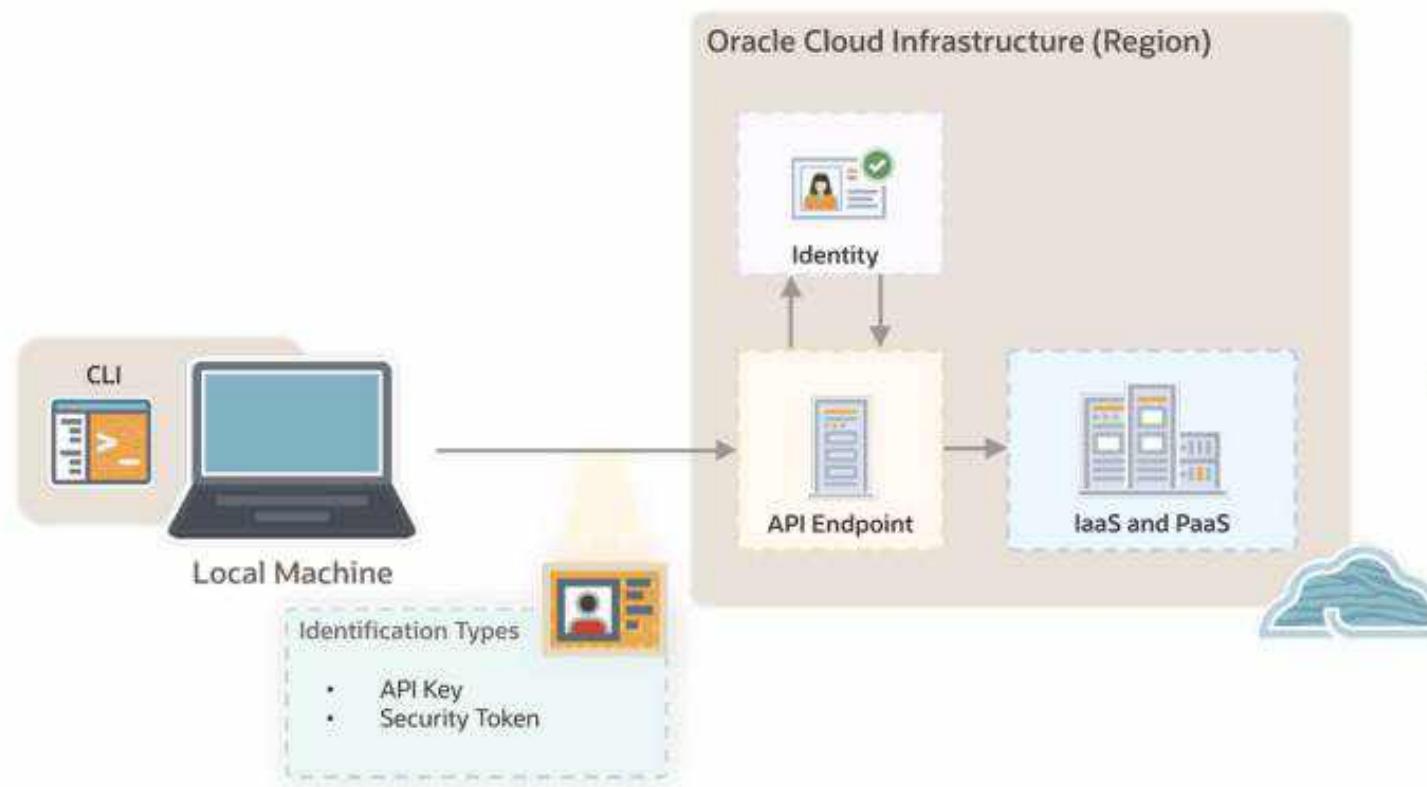
# Authentication

Oracle Cloud Infrastructure (Region)

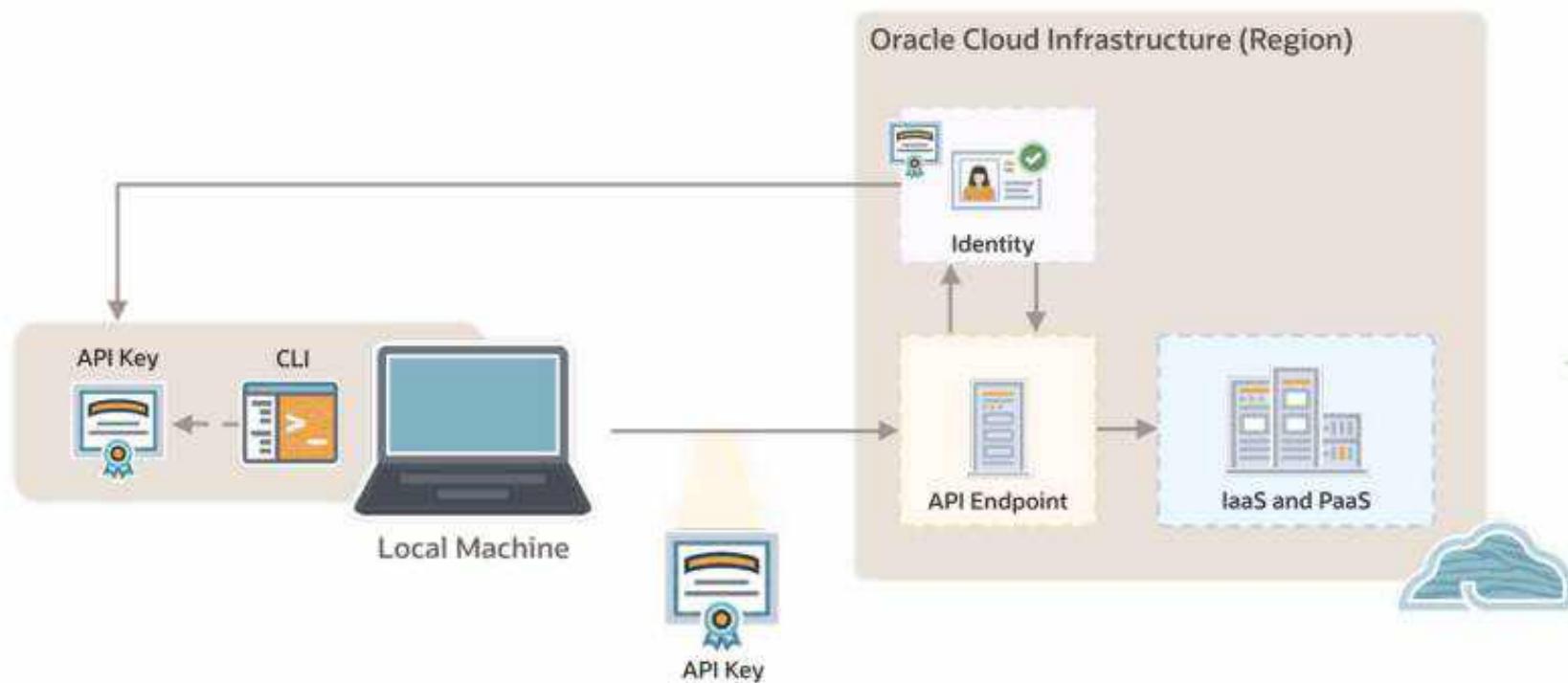
## Example API Request

```
POST https://iaas.us-phoenix-1.oraclecloud.com/20160918/vcns
host: iaas.us-phoenix-1.oraclecloud.com
opc-retry-token: 239787fs987
Content-Type: application/json
HTTP headers required for authentication
Other HTTP request headers per the HTTP spec
{
    "compartmentId": "ocid1.compartment.oc1..exampleid",
    "displayName": "Virtual Cloud Network",
    "cidrBlock": "172.16.0.0/16"
}
```

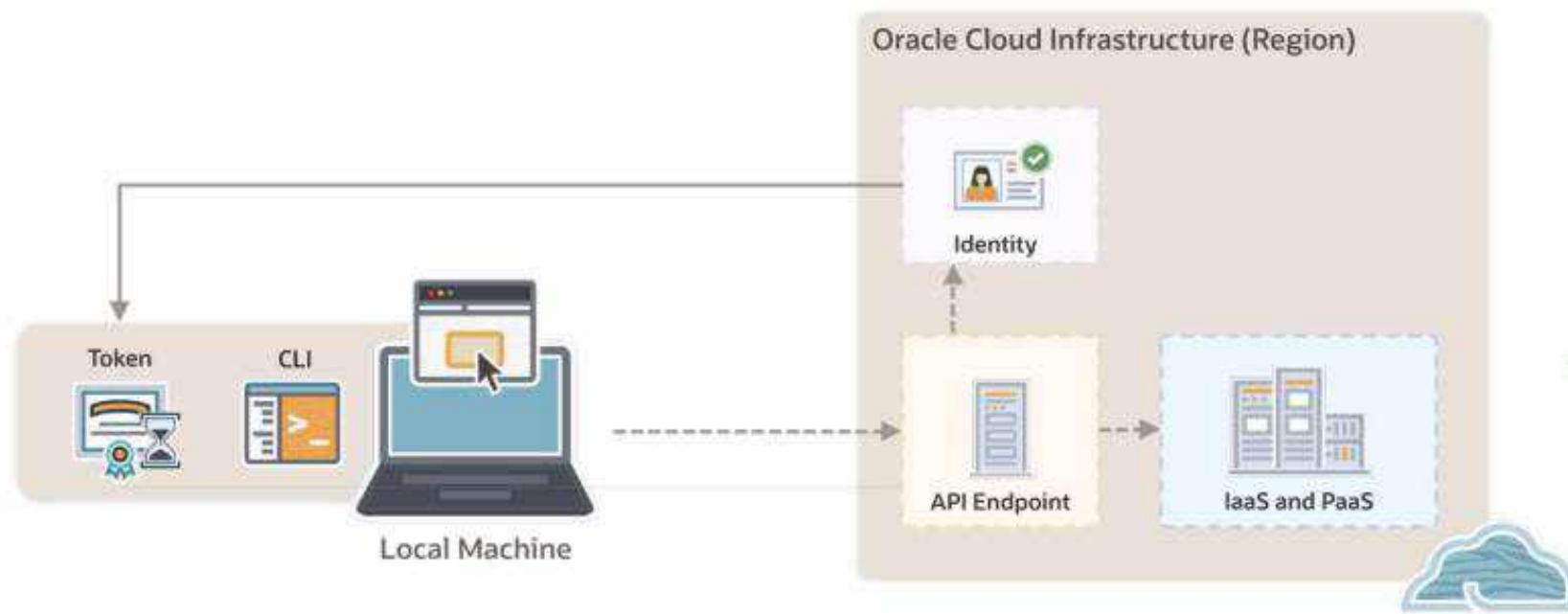
# Authentication



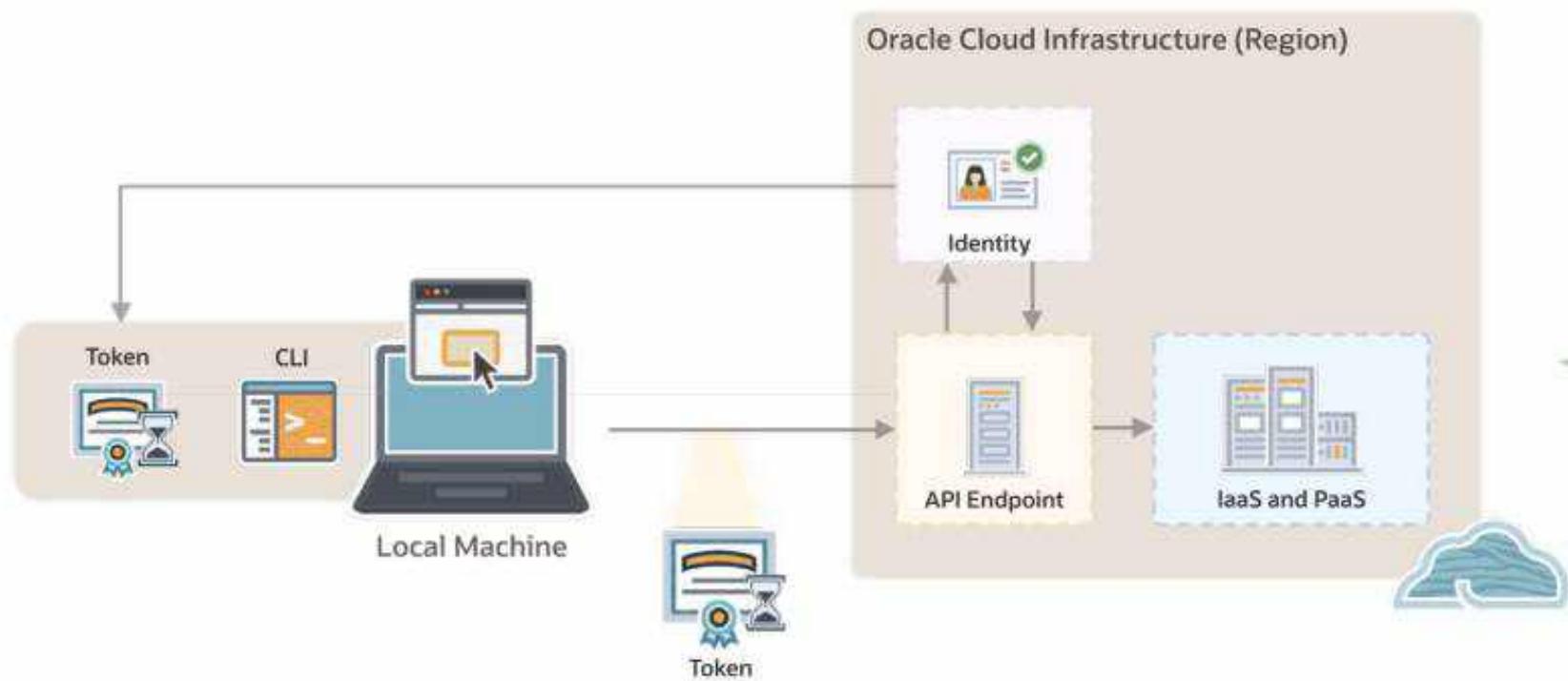
# API Key



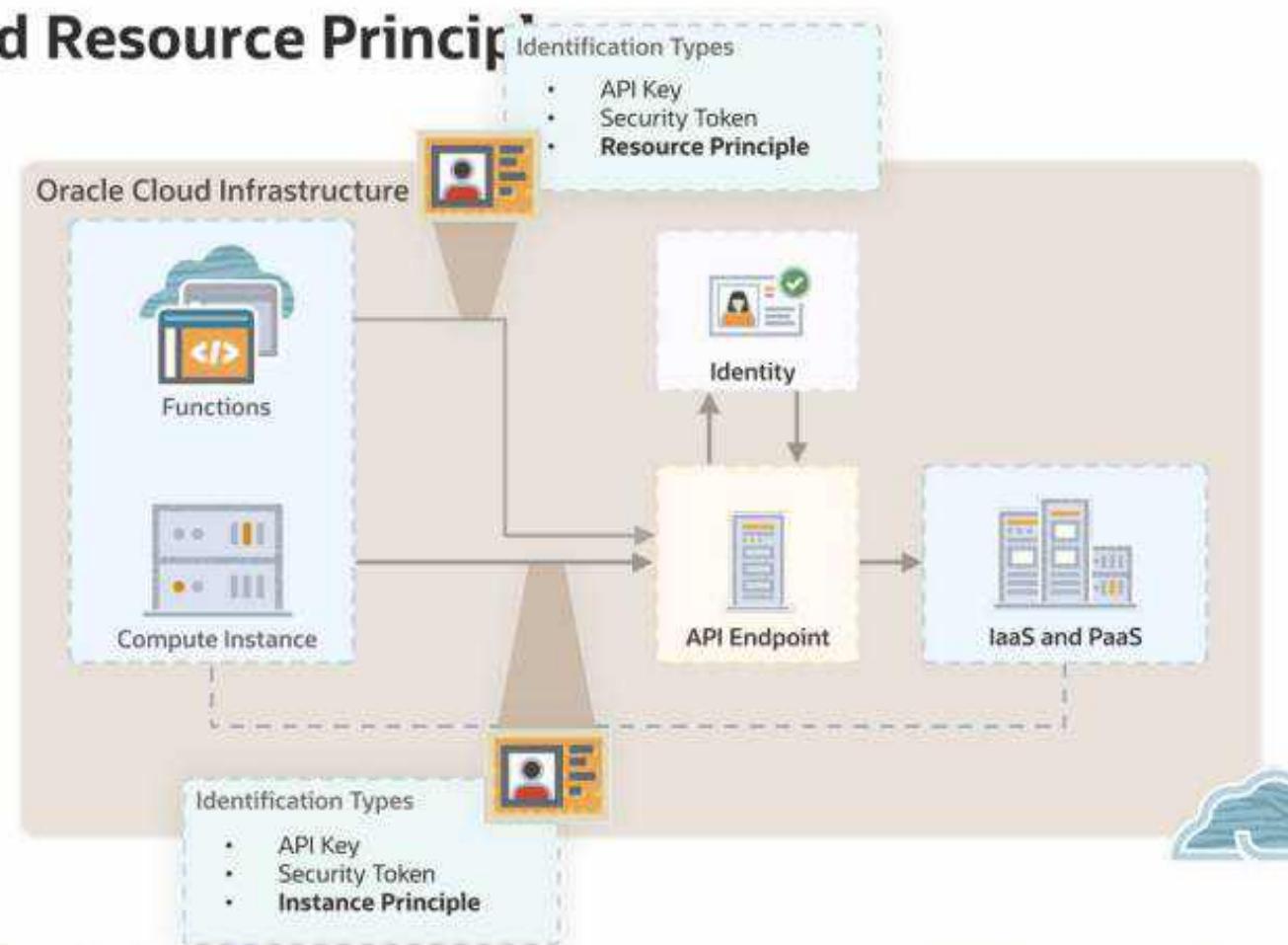
# Security Token



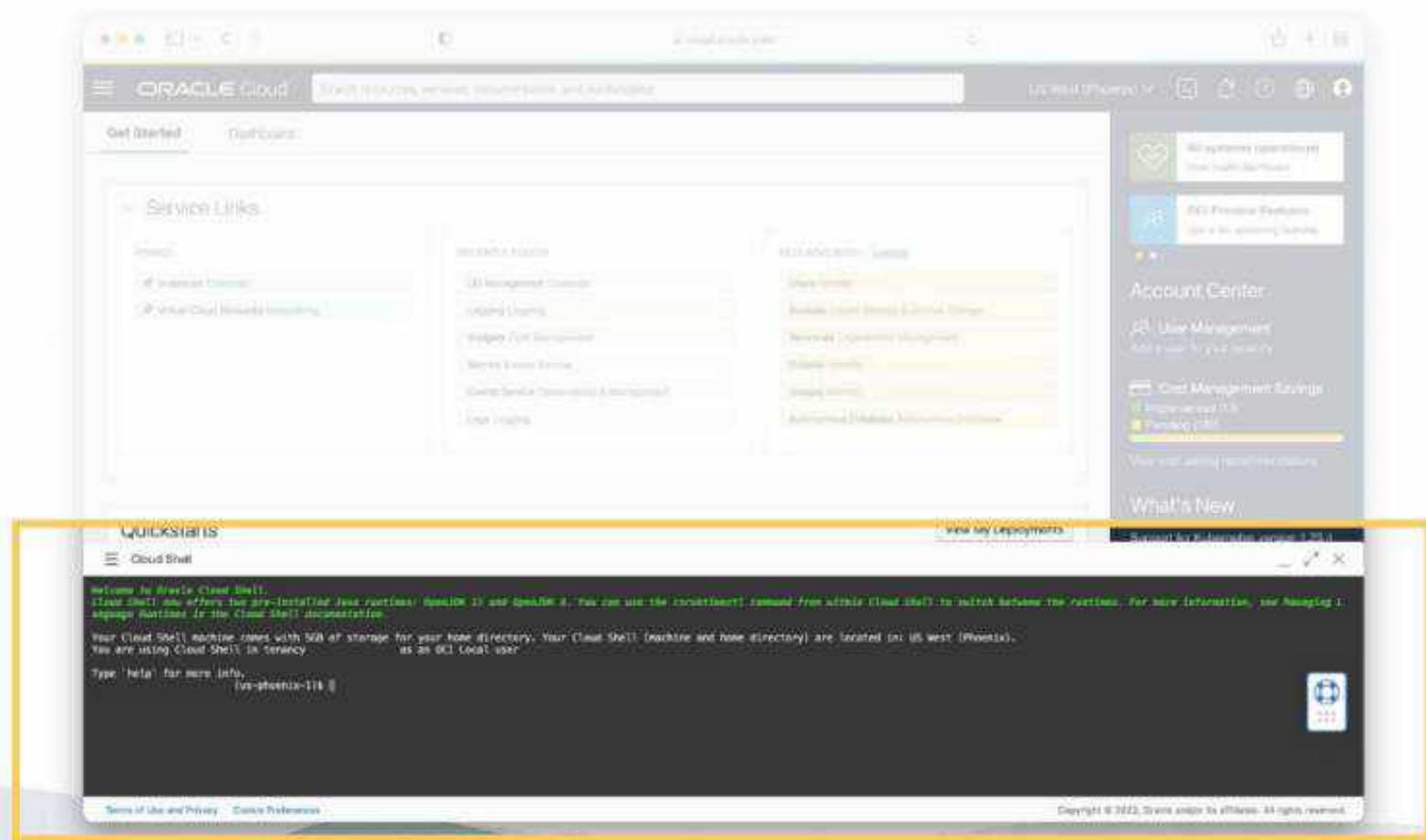
# Security Token



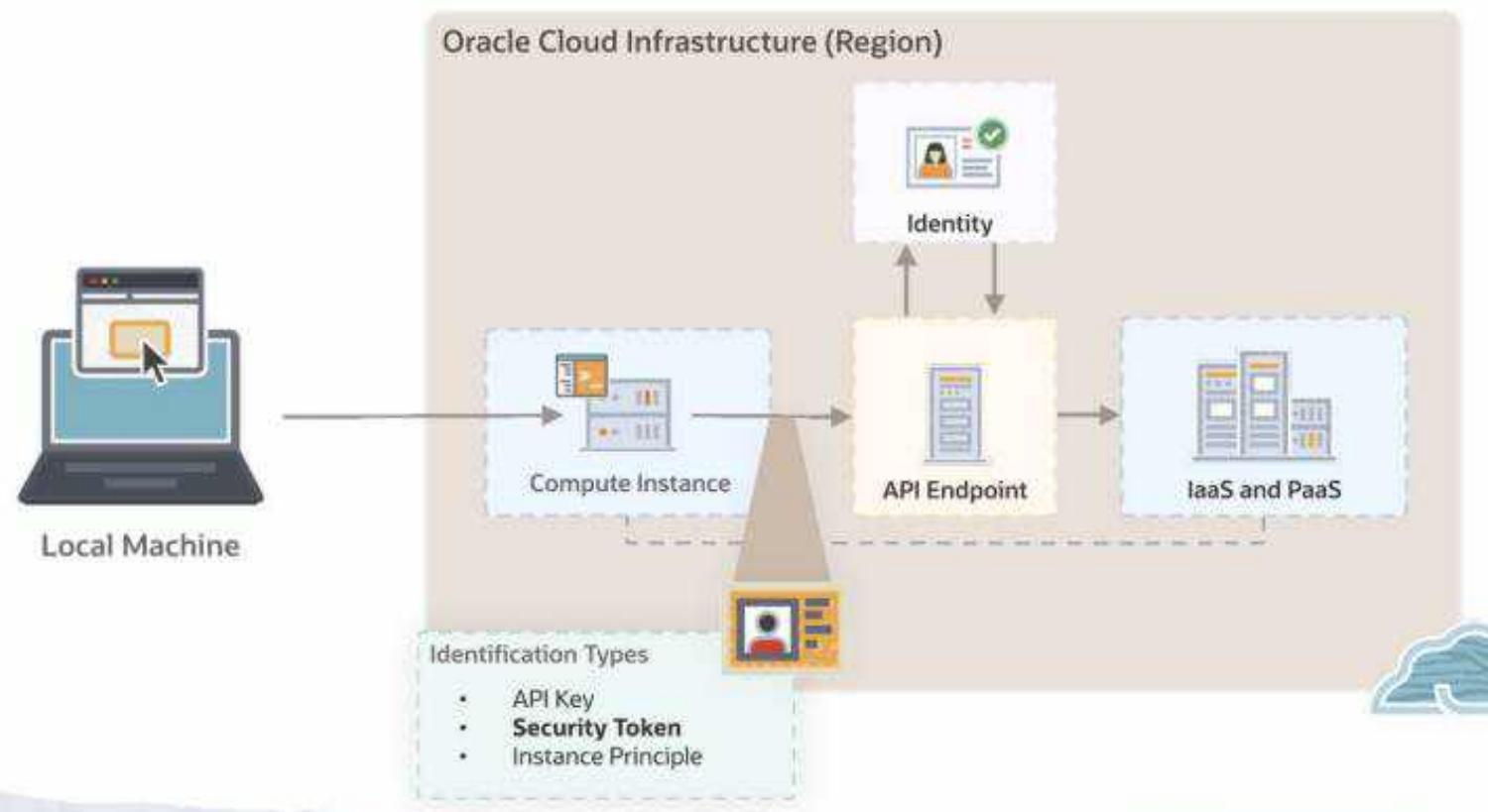
# Instance and Resource Principle



# Cloud Shell



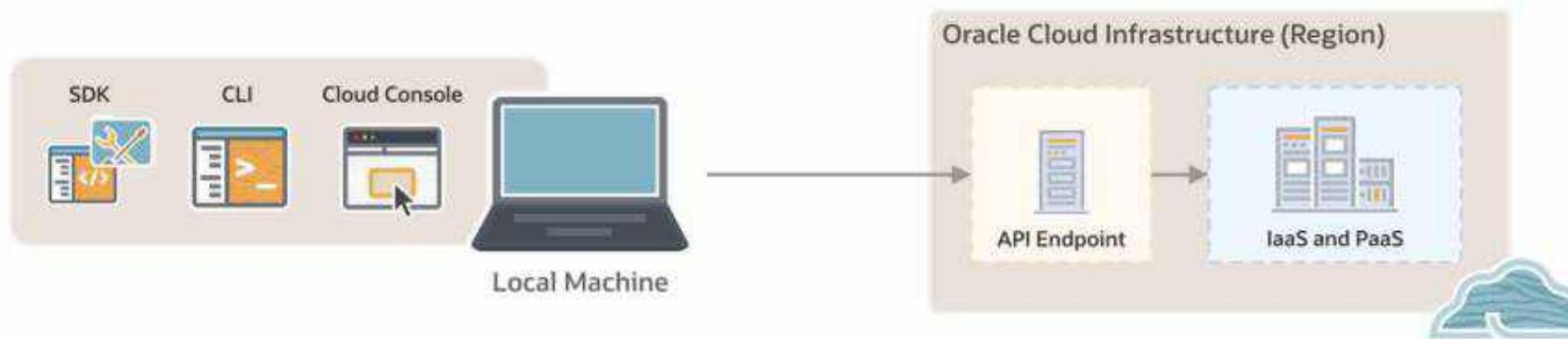
# Cloud Shell



# OCI CLI Syntax

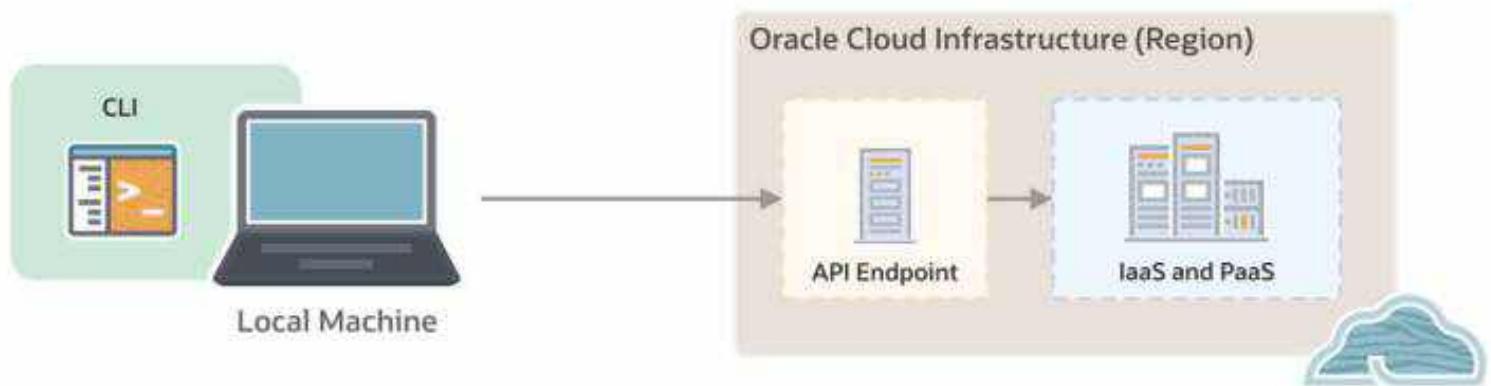
## Recall

---



## Recall

---



## Syntax

---

```
oci <service> <resource> <action> <options>
```

## Syntax

---

```
oci <service> <resource> <action> <options>
    compute
    network
    db
    ...
```

## Syntax

---

```
oci <service> <resource> <action> <options>
      instance
      vcn
      database
      ...
```

## Syntax

---

```
oci <service> <resource> <action> <options>
      create
      delete
      list
      ...
```

## Syntax

---

```
oci <service> <resource> <action> <options>
```

## Example

---

```
oci os bucket create --namespace ExampleNamespace --name ExampleBucketName --compartment-id ocid1.compartment.oc1..exampleuniqueID
```

Base  
Command

## Example

---

```
oci os bucket create --namespace ExampleNamespace --name ExampleBucketName --compartment-id ocid1.compartment.oc1..exampleuniqueID
```

Service:  
Object Storage

## Example

---

```
oci os bucket create --namespace ExampleNamespace --name ExampleBucketName --compartment-id ocid1.compartment.oc1..exampleuniqueID
```



Resource

## Example

---

```
oci os bucket create --namespace ExampleNamespace --name ExampleBucketName --compartment-id ocid1.compartment.oc1..exampleuniqueID
```

Action:

## Example

---

```
oci os bucket create --namespace ExampleNamespace --name ExampleBucketName --compartment-id ocid1.compartment.oc1..exampleuniqueID
```

Text Option

Text Option

Text Option

## Option Types

```
oci <service> <resource> <action> <options>
```

[text]

Use quotes if there are spaces.  
Escape special characters based on shell.

[integer]

[boolean]

[complex type]

JSON string.  
Use --generate-param-json-input  
for an example.

## Generating Examples

Example for single option:

```
oci <service> <resource> <action> --generate-param-json-input  
<parameter-name>
```

Example for full command:

```
oci <service> <resource> <action> --generate-full-command-json-input
```

## Advanced Examples

---

```
oci network vcn create \
--compartment-id ocid.compartment.oc1..exampleuniqueID \
--cidr-blocks "[\"10.0.0.0/24\" , \"172.16.0.0/24\"]" \
--display-name "CLI VCN"
```

```
oci os object put
-bn MyBucket \
--name myfile.txt \
--file /Users/me/myfile.txt \
--metadata '{"key1":"value1","key2":"value2"}'
```