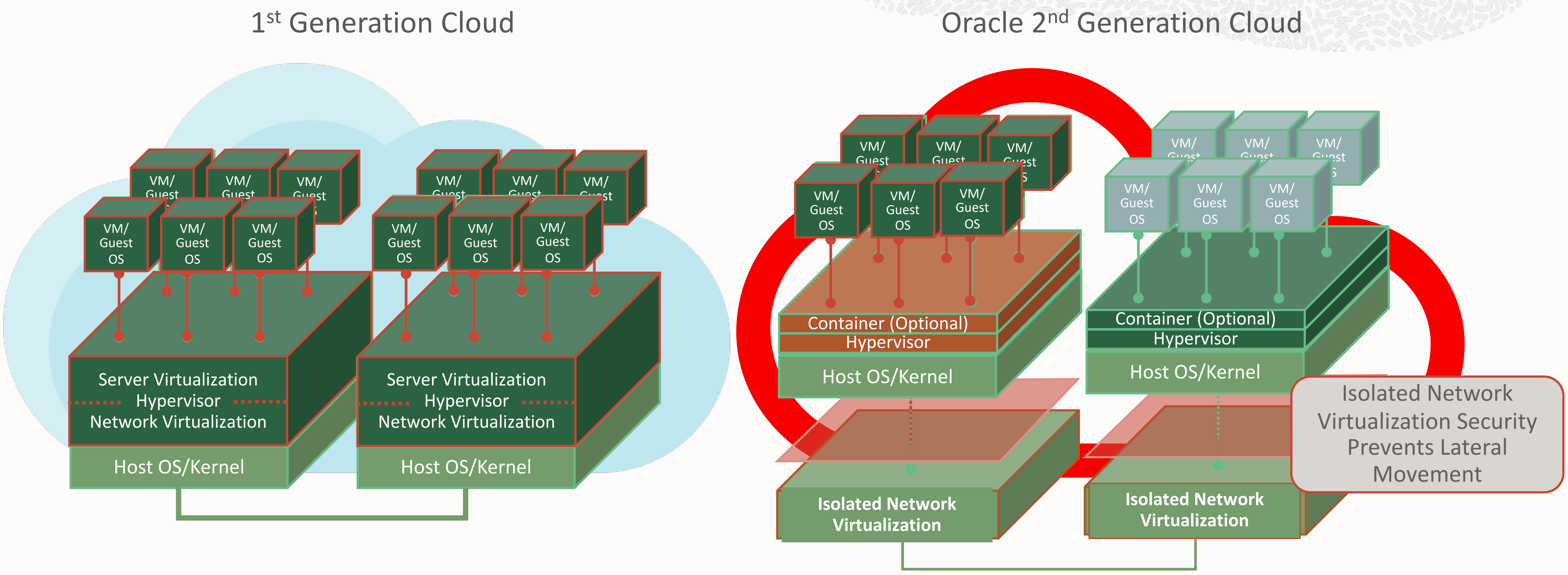
Oracle Cloud Infrastructure

101 Tech presentation

andrej.casny@oracle.com
vladimir.straka@oracle.com

Isolation: Threat Containment & Reduced Risk Built Into the Architecture

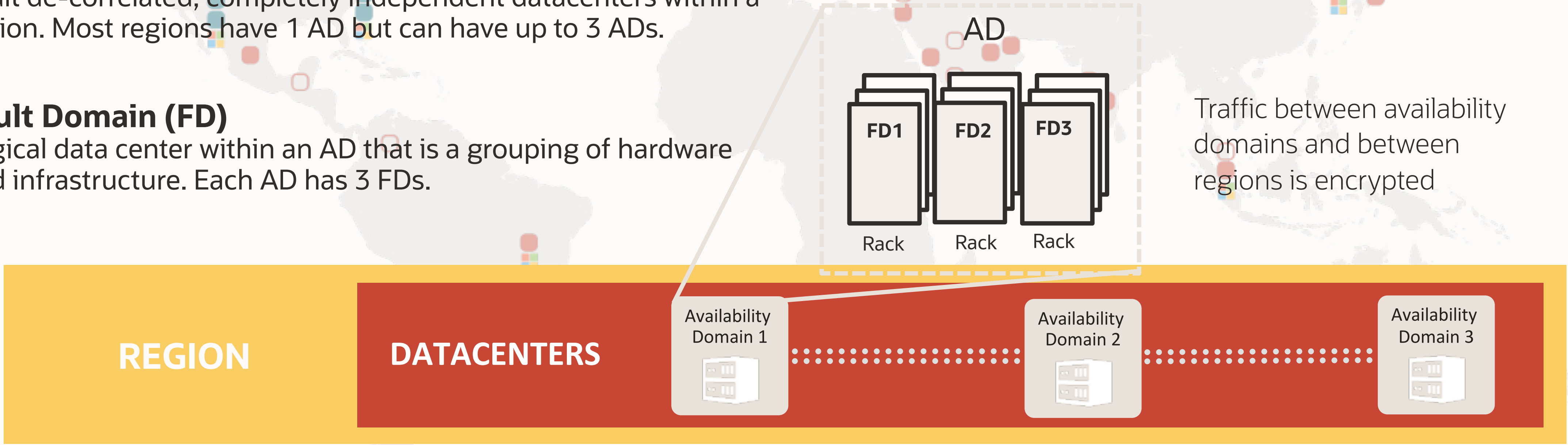


Physical Architecture Concepts

Region
Localized geographic area.
Regions are independent of other regions and can be separated by vast distances—across countries or even continents.

Availability Domain (AD)
Fault de-correlated, completely independent datacenters within a region. Most regions have 1 AD but can have up to 3 ADs.

Fault Domain (FD)
Logical data center within an AD that is a grouping of hardware and infrastructure. Each AD has 3 FDs.

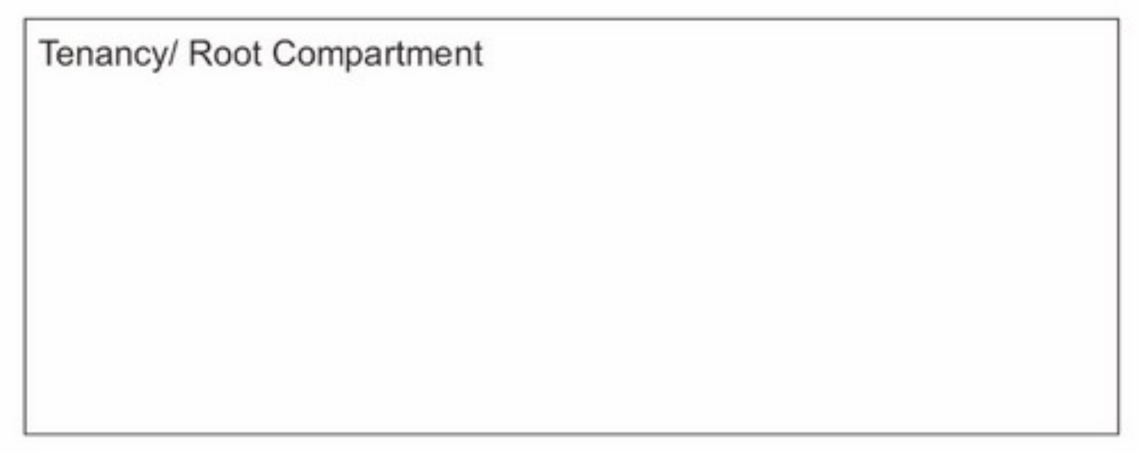


Traffic between availability domains and between regions is encrypted

Account and Access Concepts

Tenancy

Secure and isolated partition within OCI where you can create, organize, and administer your cloud resources.
You can think of the tenancy as your account.



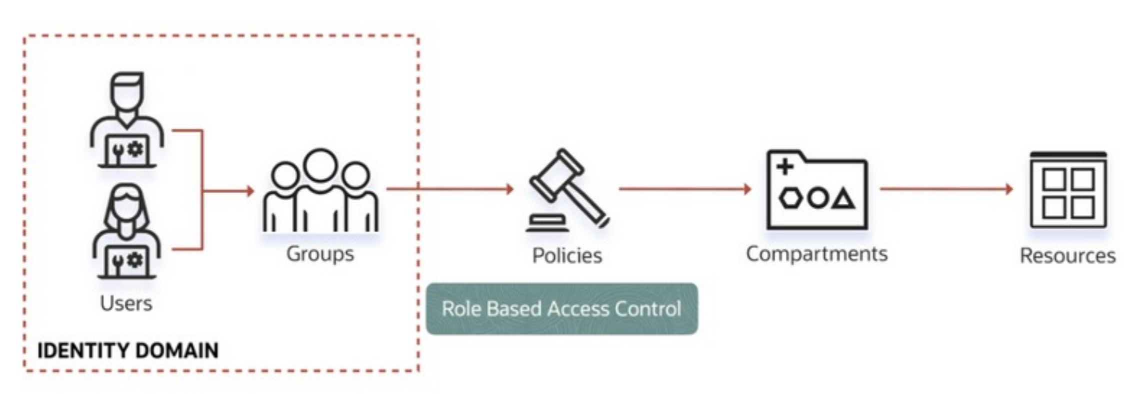
Compartment

Collection of related resources (such as instances, virtual cloud networks, block volumes) that can be accessed only by certain groups that have been given permission.
A compartment should be thought of as a logical group and not a physical container.

Identity Domains and Policies

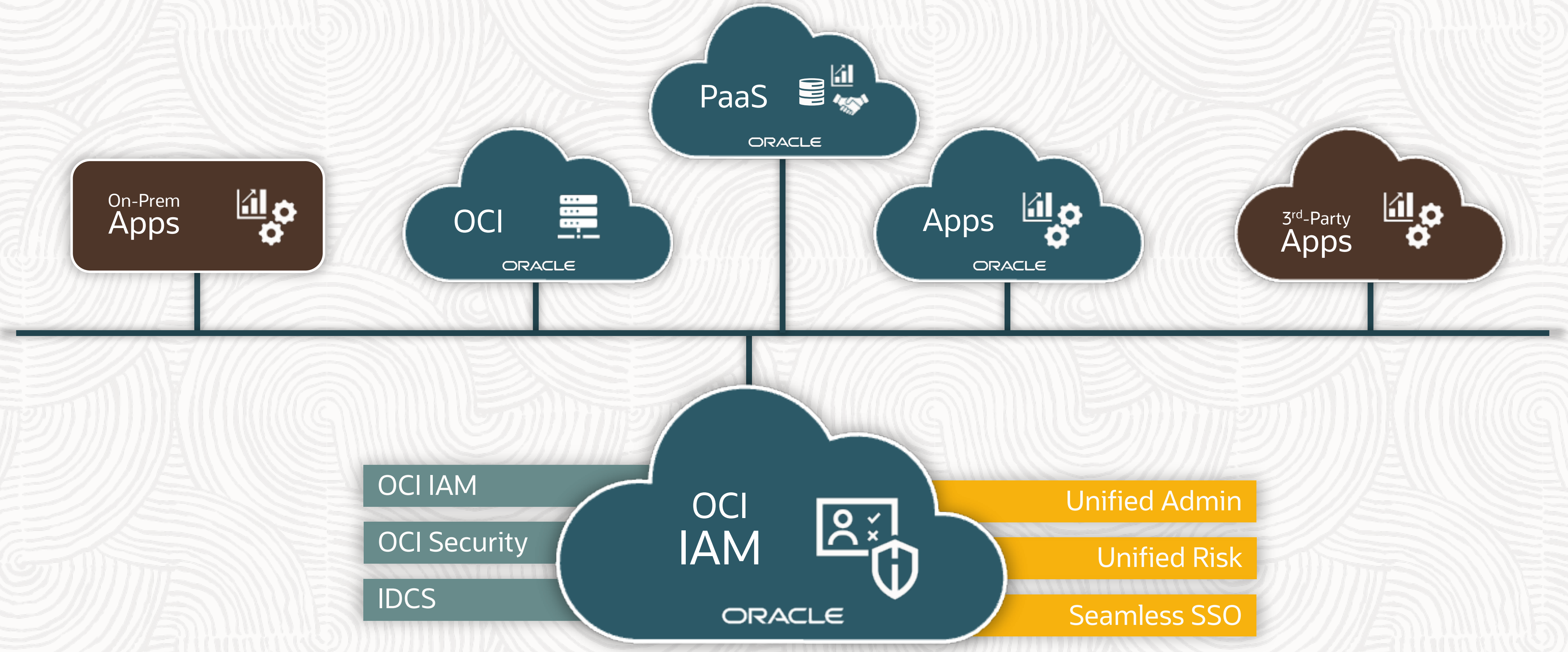
Identity domain is a container for managing users and roles, federating and provisioning of users, secure application integration through Oracle Single Sign-On (SSO) configuration, and OAuth administration.

Policy is a document that specifies who can access which resources, and how.



OCI IAM - Identity Domains

Unified Cloud IAM



Adds New Value:
Unified IAM for Oracle Cloud and SaaS
Identity Domains Admin Experience
Cross-Regions DR

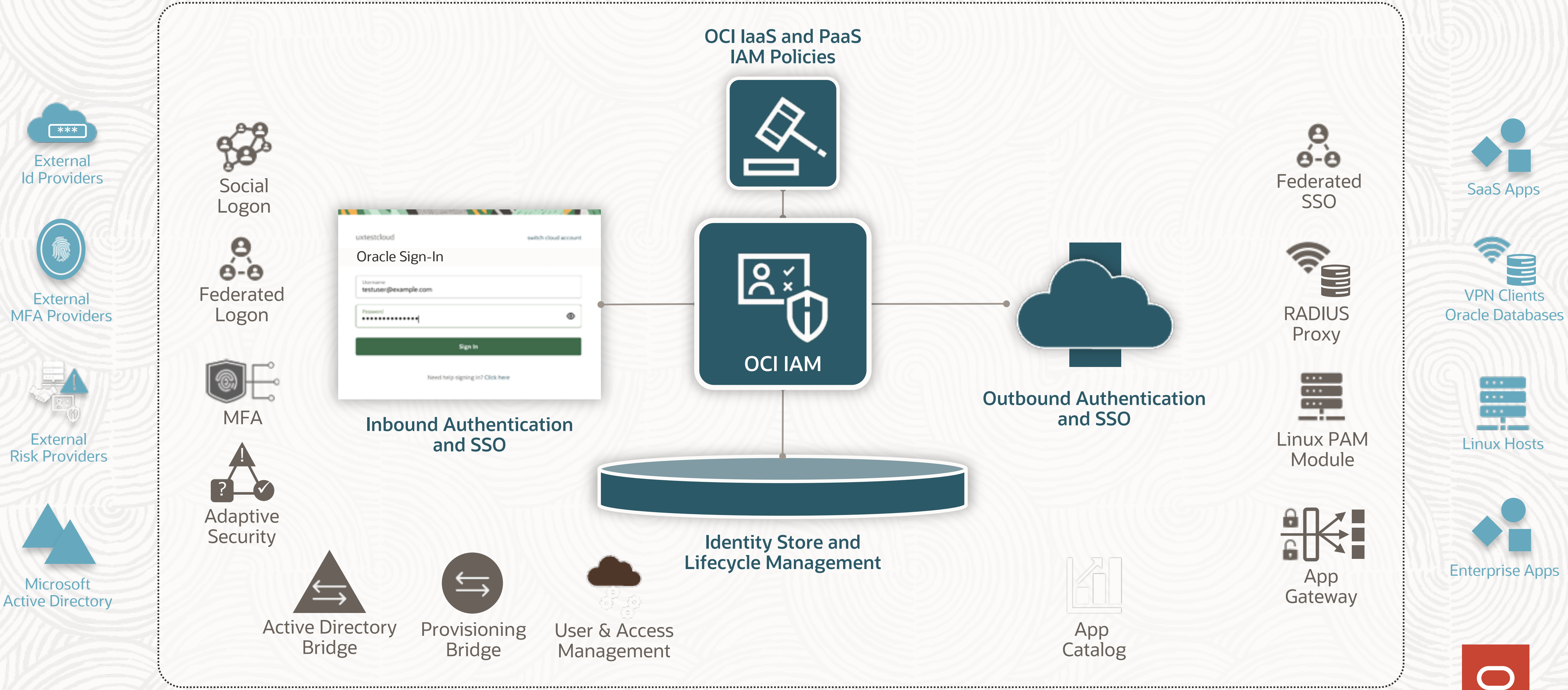
OCI IAM Identity Domain Types

Free (Included)	Oracle Apps (Included)	Oracle Apps Premium ($0.25/user/mo.)	External ($0.016/user/mo.)	Premium ($3.20/user/mo.)
Manage access to OCI resources.	*Provisioned by Oracle services to manage access to subscribed Oracle services.*	*Adds hybrid IAM (proxies, gateways, bridges) for use with on-prem or OCI-hosted Oracle applications.*	*Full IAM feature set for non-employee use-cases, CIAM, and custom app developers.*	*Full IAM feature set for workforce use-cases; manage access across hybrid IT.*
Key Limit: 2000 users	**Key Limit:** Must be provisioned by an Oracle service.	**Key Limit:** Supports only six (6) non-Oracle Apps	**Key Limit:** For non-employees. No hybrid IAM support.	**Key Limit:** None
Included features ▪ Basic authentication, federation, and SSO ▪ MFA and adaptive sec. ▪ User and group mgmt. ▪ User self-service ▪ All security policies: IdP, passwords, sign-on, etc. ▪ Dynamic groups ▪ Schema extensions ▪ Delegated admin ▪ AD bridge inbound sync ▪ PIV/CAC support ▪ Basic branding ▪ OCI IAM policies ▪ Audit and reporting	**Feature restrictions** ▪ No bridges, proxies, gateways (except AD) ▪ No AD bidirectional ▪ No delegated AuthN ▪ No self-registration ▪ No hosted screens ▪ Limit (2) external apps - SSO and LCM ▪ Limit (3) external IdPs	**Additional features** ▪ All bridges, proxies, gateways (limited to Oracle targets): ○ App Gateway ○ Provisioning Bridge ○ EBS Asserter ○ RADIUS Proxy for Oracle Database ○ Linux PAM ▪ AD bidirectional ▪ Delegated AuthN ▪ Self-registration ▪ Hosted screens ▪ Limit (6) external apps - SSO and LCM ▪ Unlimited external IdPs	**Feature restrictions** ▪ No bridges, proxies, gateways ▪ No AD bridge ▪ No identity lifecycle management or provisioning ▪ No OCI IAM policies Note: *These are typically not required in CIAM scenarios.*	**All features** **No restrictions**

Types: https://docs.oracle.com/en-us/iaas/Content/Identity/sku/overview.htm#overview
Pricing: https://www.oracle.com/security/cloud-security/pricing/#iam

OCI Identity & Access Management (OCI IAM)

Enterprise Identity & Access Management



uxtestcloud

switch cloud account

Oracle Sign-In

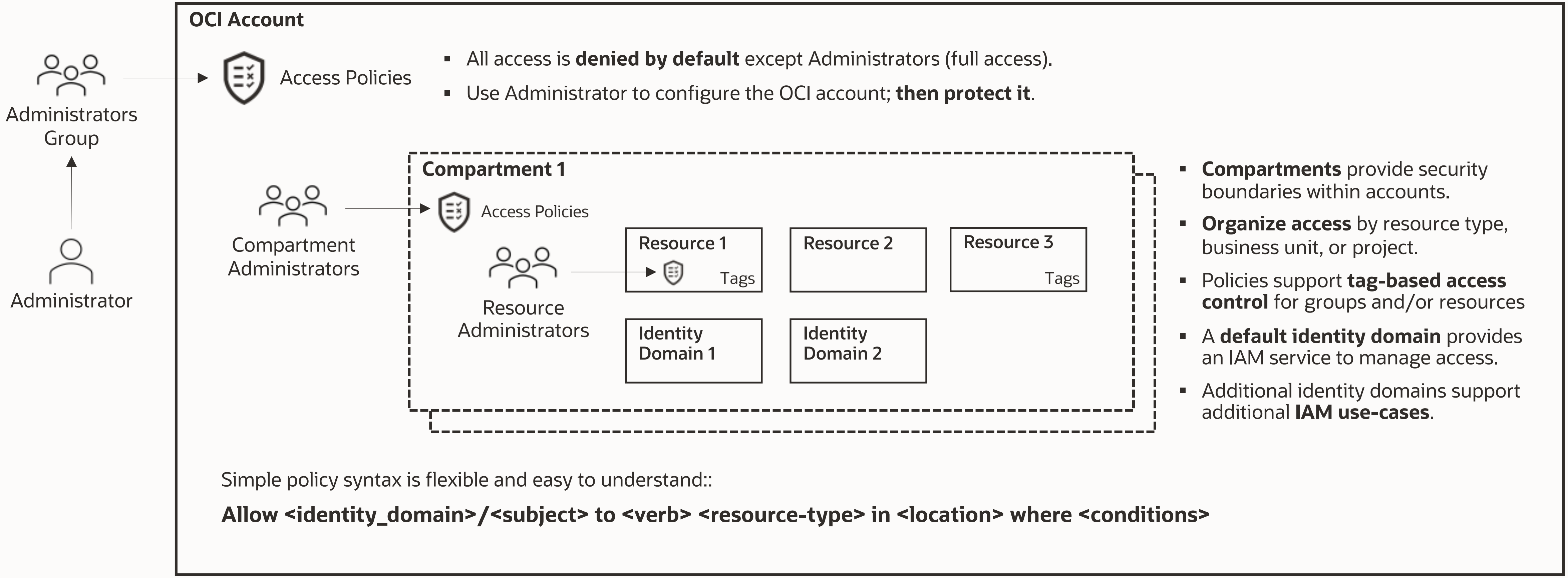
Username: testuser@example.com

Password: ••••••••••••••

Sign In

Need help signing in? Click here

OCI IaaS and PaaS IAM Policies



- All access is **denied by default** except Administrators (full access).
- Use Administrator to configure the OCI account; **then protect it**.

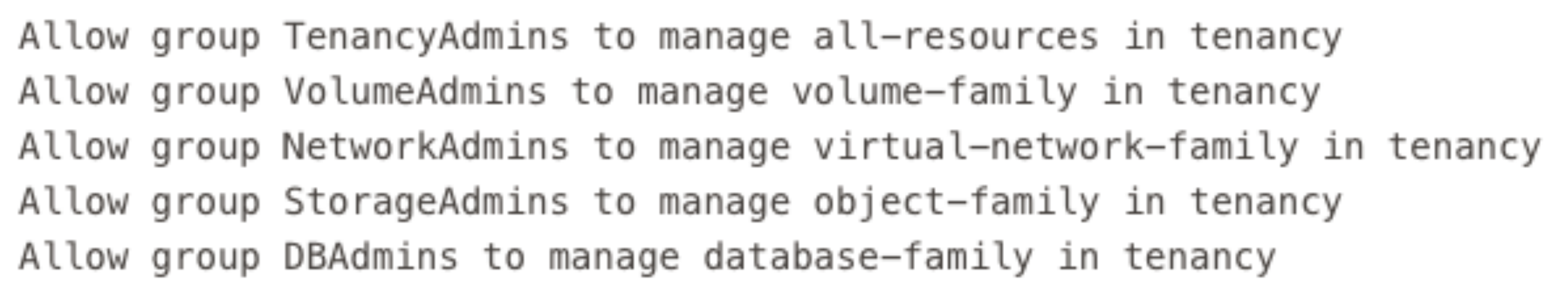
- **Compartments** provide security boundaries within accounts.
- **Organize access** by resource type, business unit, or project.
- Policies support **tag-based access control** for groups and/or resources
- A **default identity domain** provides an IAM service to manage access.
- Additional identity domains support additional **IAM use-cases**.

Simple policy syntax is flexible and easy to understand::

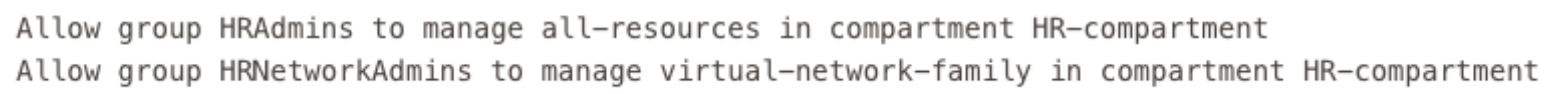
Allow <identity_domain>/<subject> to <verb> <resource-type> in <location> where <conditions>

Security policies - examples

Service-level admins

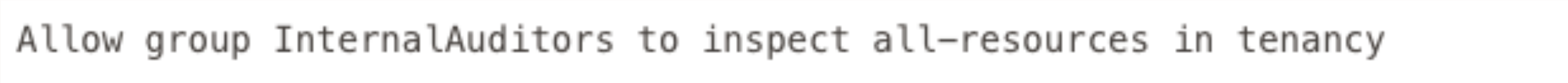


```
Allow group TenancyAdmins to manage all-resources in tenancy
Allow group VolumeAdmins to manage volume-family in tenancy
Allow group NetworkAdmins to manage virtual-network-family in tenancy
Allow group StorageAdmins to manage object-family in tenancy
Allow group DBAdmins to manage database-family in tenancy
```



```
Allow group HRAdmins to manage all-resources in compartment HR-compartment
Allow group HRNetworkAdmins to manage virtual-network-family in compartment HR-compartment
```

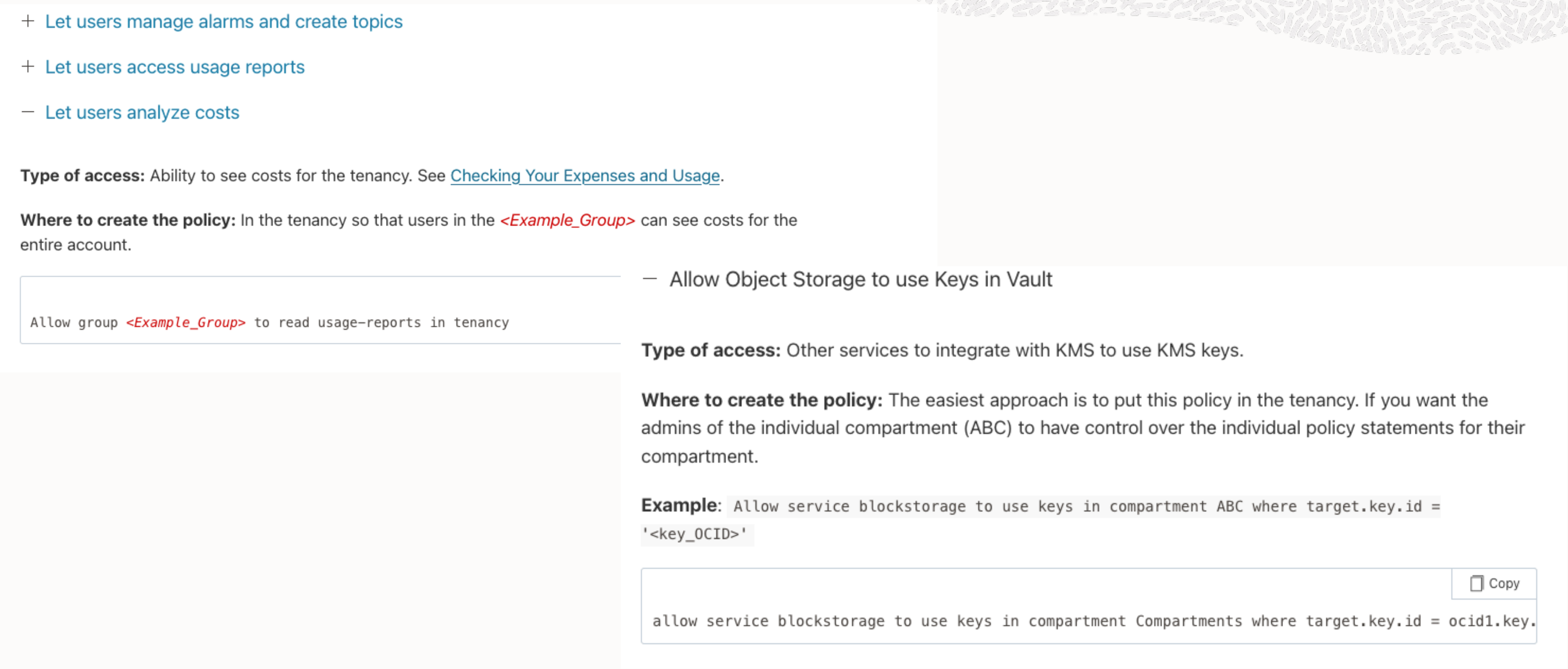
Auditors



```
Allow group InternalAuditors to inspect all-resources in tenancy
```

https://docs.oracle.com/en-us/iaas/Content/Security/Reference/iam_security_topic-Security_Policy_Examples.htm

Common policies – sample



+ Let users manage alarms and create topics

+ Let users access usage reports

— Let users analyze costs

Type of access: Ability to see costs for the tenancy. See Checking Your Expenses and Usage.

Where to create the policy: In the tenancy so that users in the *<Example_Group>* can see costs for the entire account.

```
Allow group <Example_Group> to read usage-reports in tenancy
```

— Allow Object Storage to use Keys in Vault

Type of access: Other services to integrate with KMS to use KMS keys.

Where to create the policy: The easiest approach is to put this policy in the tenancy. If you want the admins of the individual compartment (ABC) to have control over the individual policy statements for their compartment.

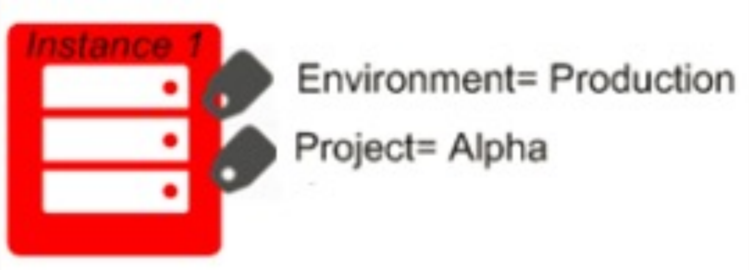
Example: `Allow service blockstorage to use keys in compartment ABC where target.key.id = '<key_OCID>'`

```
allow service blockstorage to use keys in compartment Compartments where target.key.id = ocid1.key.
```

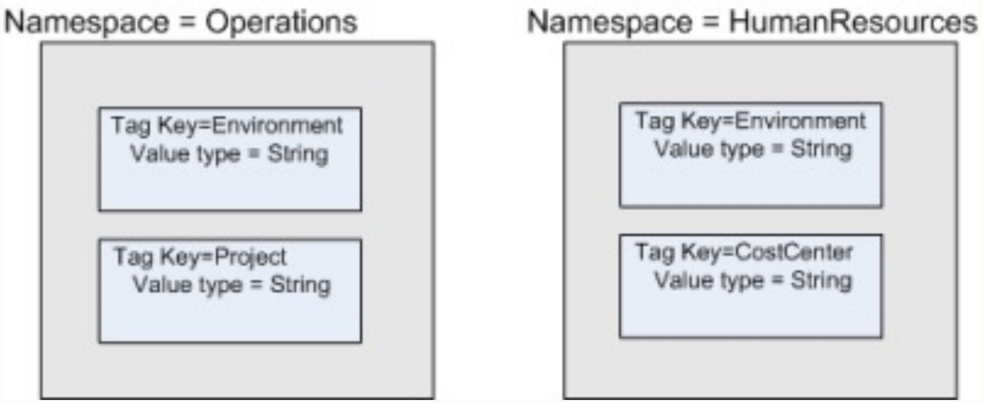
https://docs.oracle.com/en-us/iaas/Content/Identity/Concepts/commonpolicies.htm#top

Tagging

- Free-form Tags – basic implementation
  - Consist simply of a key and a value



- Defined Tags – more features and control
  - Are contained in tag Namespaces
  - Defined schema, secured with Policy



Namespace = Operations

Tag Key=Environment
Value type = String

Tag Key=Project
Value type = String

Namespace = HumanResources

Tag Key=Environment
Value type = String

Tag Key=CostCenter
Value type = String

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 request.principal.group.tag.Operations.Project= ‘Prod’ 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 InstancesA to manage object-family in compartment HR where request.principal.group.tag.Operations.Project= ‘Prod’ Instances in dynamic group InstancesA that has been tagged with Operations.Project=‘Prod’ can manage objects in the compartment HR
Compartment	request.principal.compartment.tag.*{tagNamespace}*.*{tagKeyDefinition}*= '*<value>*	allow dynamic-group InstancesA to manage object-family in compartment HR where request.principal.compartment.tag.Operations.Project= 'Prod' 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.

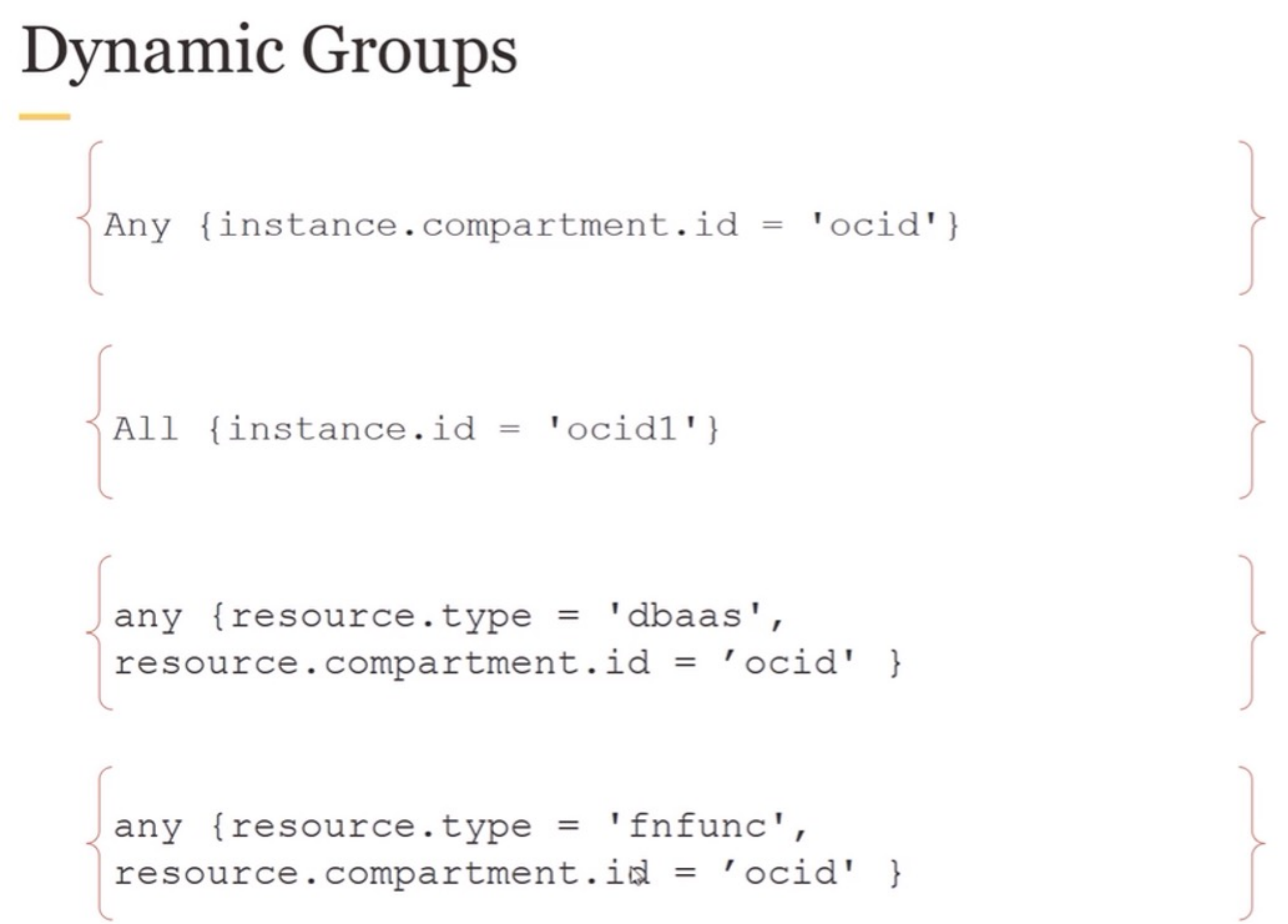
Dynamic Groups

- 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.



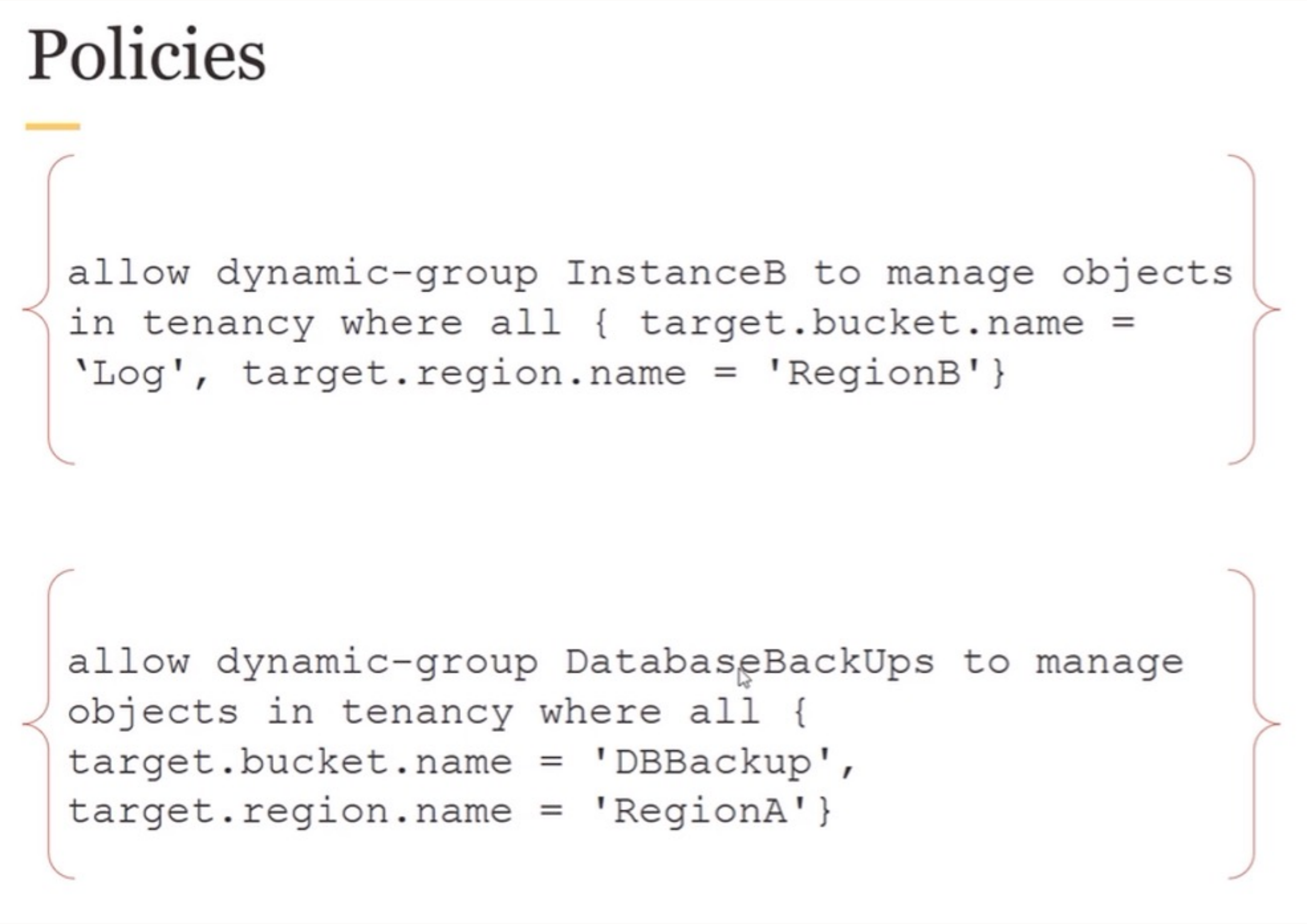
Dynamic Groups

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

```
All {instance.id = 'ocid1'}
```

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

```
any {resource.type = 'fnfunc',
resource.compartment.id = ’ocid' }
```



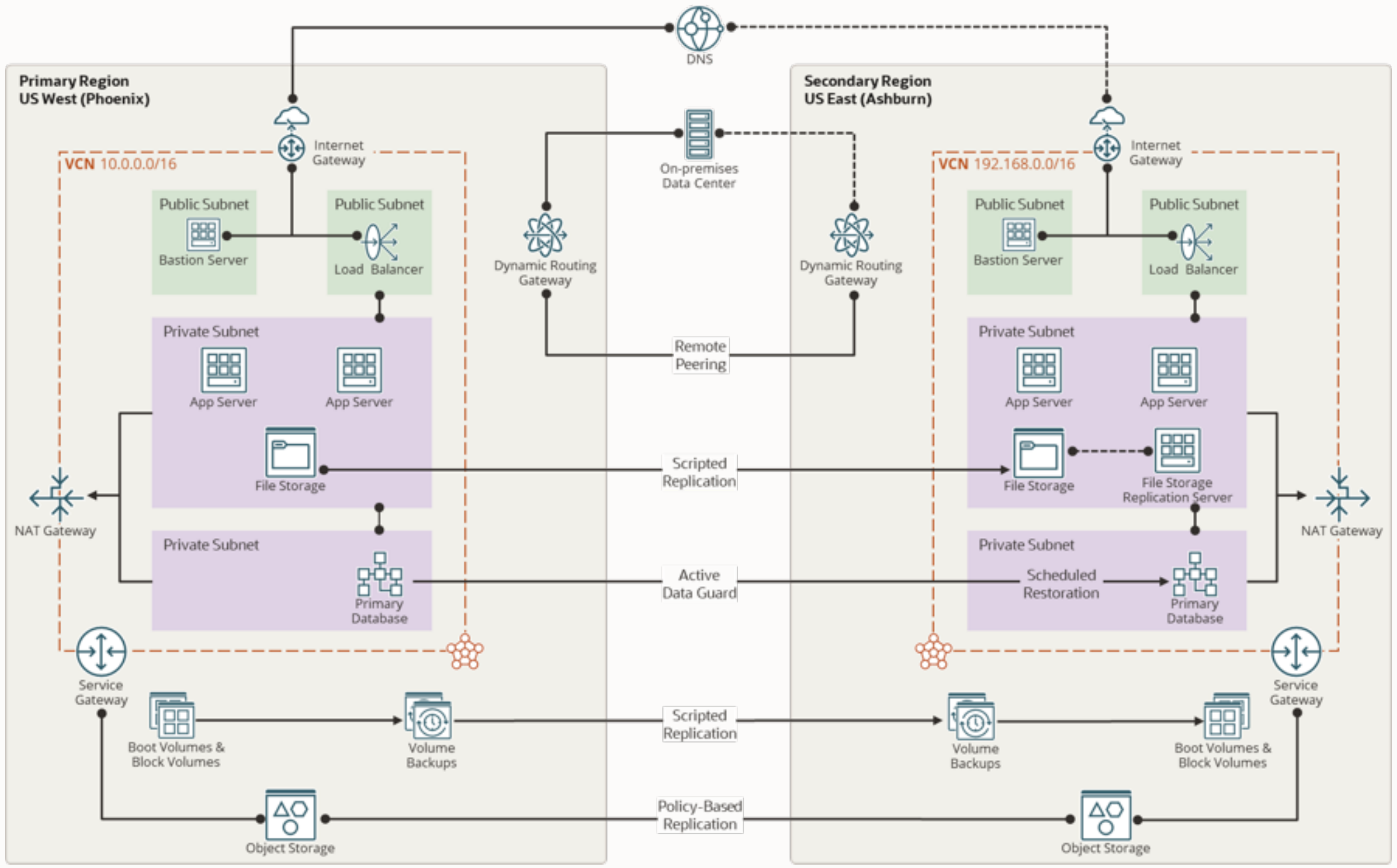
Policies

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

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

Architecting Cloud Networking for Workloads in OCI

Creating a Final Picture for your Networking & Connectivity



Virtual Cloud Network(s)

- Network Topology – Single VCN vs. Hub-Spoke
- Communication – Internet, Oracle Services

Security

- Network Security Groups & Security Lists

Connectivity

- Hybrid Cloud & Multi-cloud Architecture

DNS

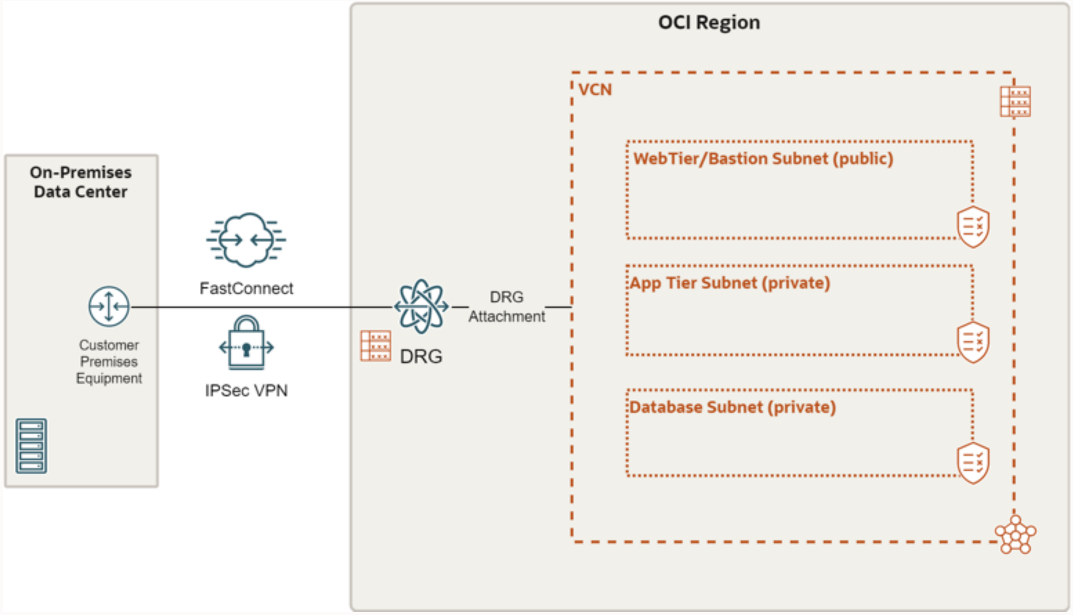
- Private DNS
- Traffic Management

Monitoring

- Metrics
- Logging

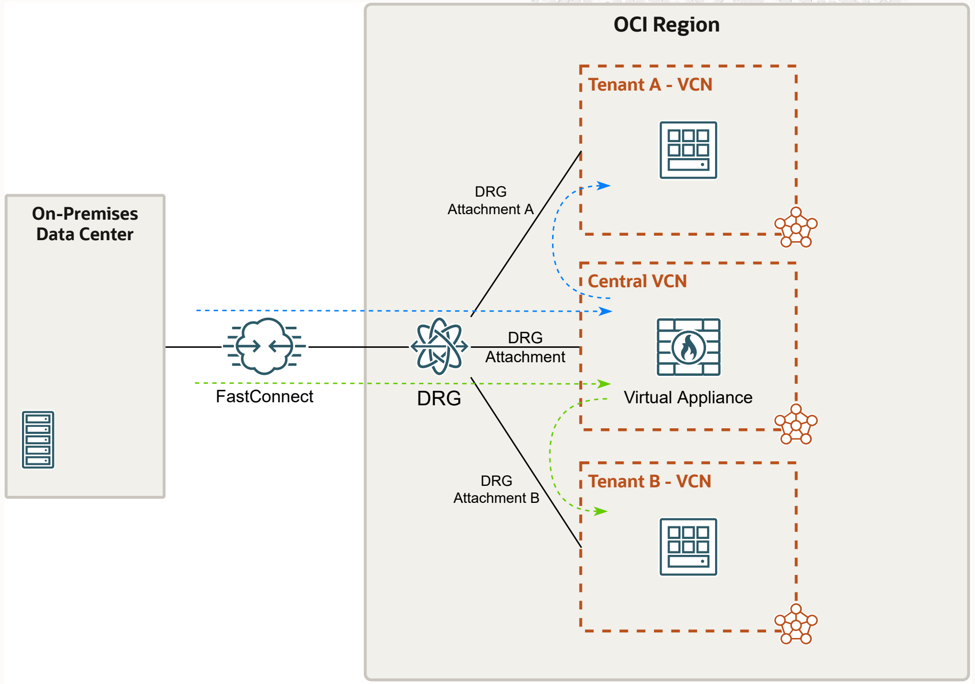
Cloud Network Architecture

Single VCN vs. Hub-Spoke Topology


OCI Region
VCN
WebTier/Bastion Subnet (public)
App Tier Subnet (private)
Database Subnet (private)
On-Premises Data Center
Customer Premises Equipment
FastConnect
IPSec VPN
DRG
DRG Attachment

Single network topology

- Quick deployment



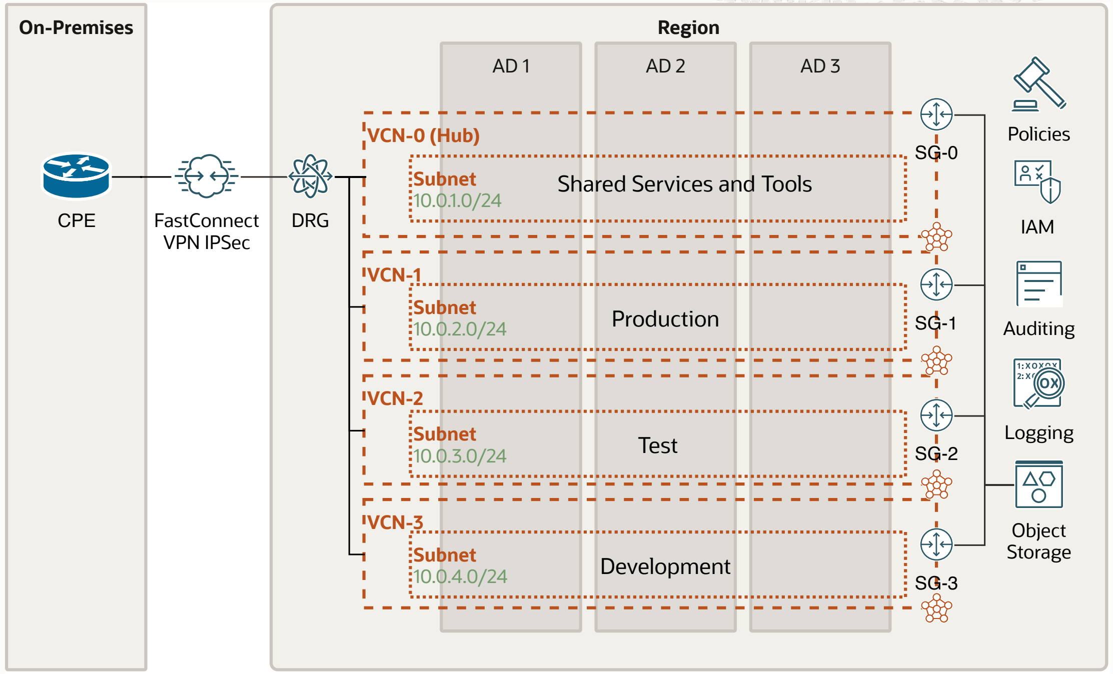
Hub & Spoke network topology

- Flexible solution
- Transit routing capable with firewall in hub VCN
- Recommended as standard deployments

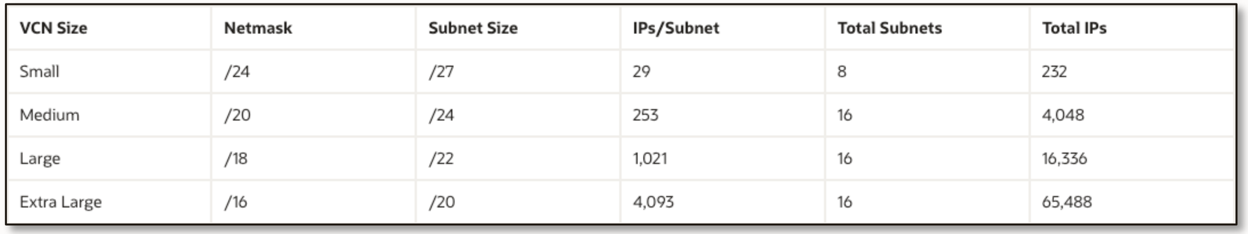
Virtual Cloud Network Specifications

Design Decision: IP Addressing & Workload Accessibility

- Maximize the use of Availability Domains for HA design
- In a region with one AD, use Fault Domains
- Use regional subnets which spans all Availability Domains in a region
- Separate VCNs for different workloads



- Size your VCNs/subnets so expansion can happen
- Choose IP address range that don't overlap with on-premise or other networks customer might connect to
- Maximum 65000 IP within a VCN



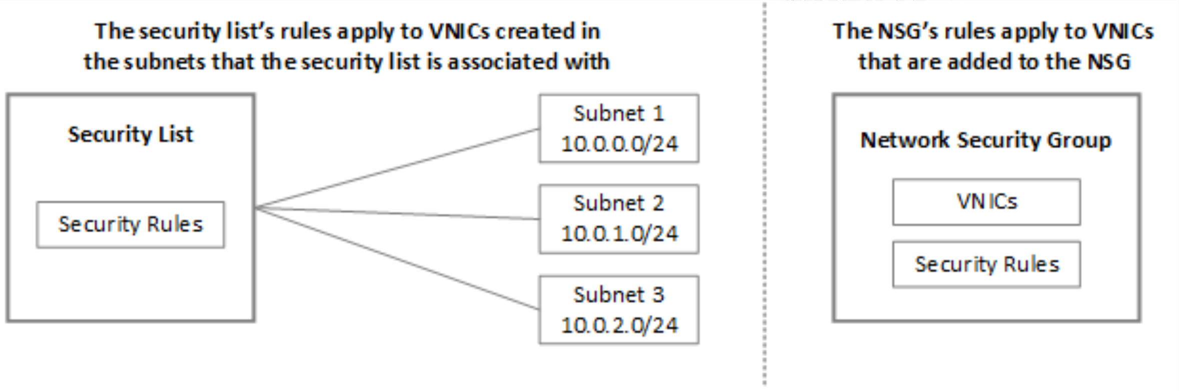
VCN Size	Netmask	Subnet Size	IPs/Subnet	Total Subnets	Total IPs
Small	/24	/27	29	8	232
Medium	/20	/24	253	16	4,048
Large	/18	/22	1,021	16	16,336
Extra Large	/16	/20	4,093	16	65,488

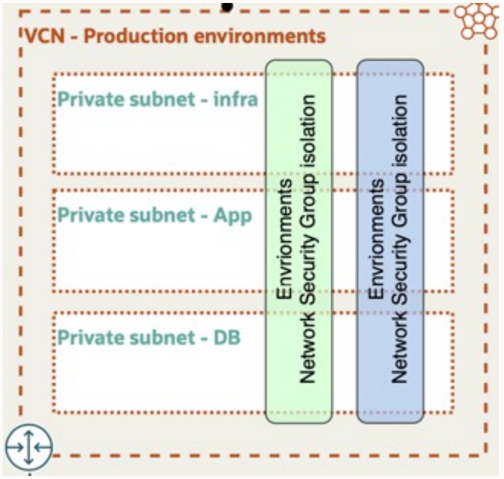
Example of combinations of VCN size, subnet size and usable IPs

Virtual Cloud Network Specifications

Design Decision: IP Addressing & Workload Accessibility

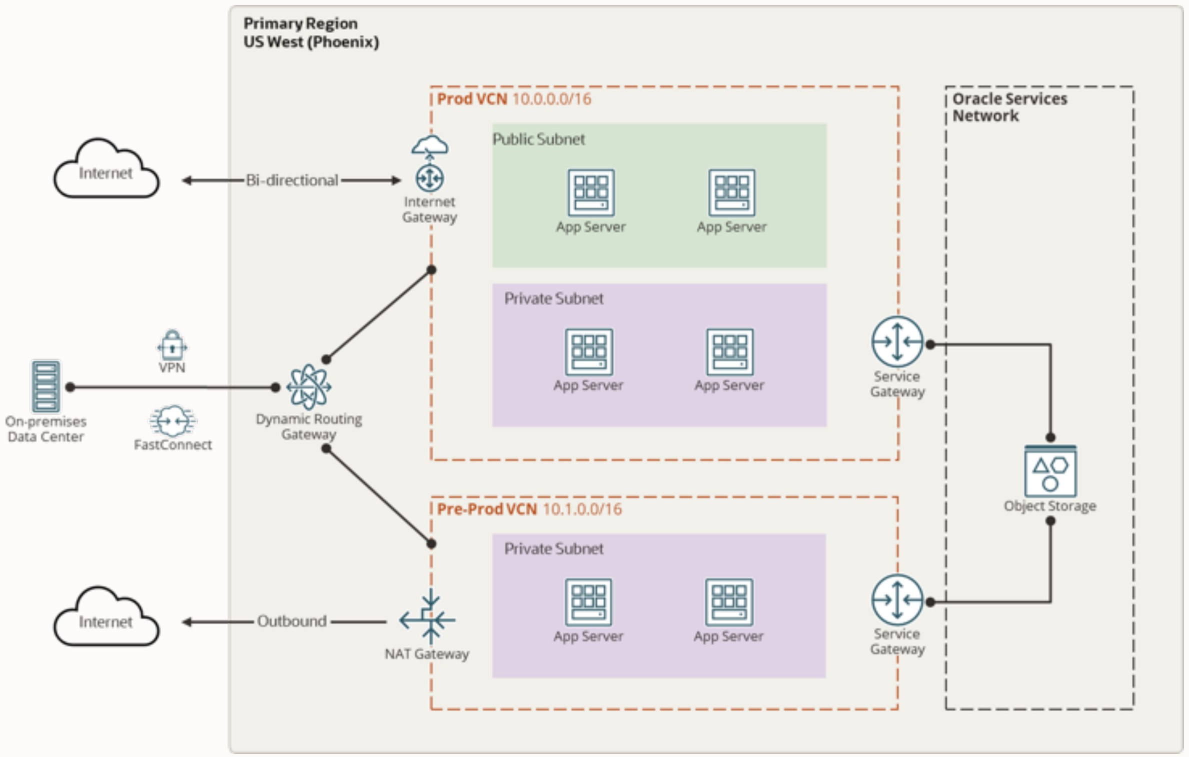
- Use **Security Lists** and/or **Network Security Groups** to control access to your resources in both private and public subnets.
- Security Lists are applied at subnet level
- You can use NSGs to define a set of ingress and egress rules that apply to specific VNICs.
- Oracle recommend using NSGs rather than security lists because NSGs enable you to separate VCN's subnet architecture from the security requirements of your application
- Private subnets are recommended to have individual route tables to control the flow of traffic to other VCNs or on-premises


The security list's rules apply to VNICs created in the subnets that the security list is associated with
Security List
Security Rules
Subnet 1 10.0.0.0/24
Subnet 2 10.0.1.0/24
Subnet 3 10.0.2.0/24
The NSG's rules apply to VNICs that are added to the NSG
Network Security Group
VNICs
Security Rules


VCN - Production environments
Private subnet - infra
Private subnet - App
Private subnet - DB
Envrionments Network Security Group isolation
Envrionments Network Security Group isolation

Workload Communication Requirements

Design Decision: OCI Communication Gateways



Feature	Gateway to use	Comments
Traffic in and out of OCI. Can be initiated from OCI or internet	**Internet Gateway**	Need to have a public subnet and a resource with public IP
Resources in OCI access internet securely	**NAT Gateway**	Use private subnet, cannot receive internet traffic initiated from internet
Access to Object Storage or other Service in Oracle Service Network (OS management Service, Oracle Linux Yum Service etc…)	**Service Gateway**	List of services is long https://www.oracle.com/cloud/networking/service-gateway/service-gateway-supported-services
Connection between OCI and on-premise and between VCNs.	**Dynamic Routing Gateway**	This is a virtual router that connect VCNs and on-premise locations together. Central connection point. Also between regions and different tenancies

OCI Compute Provides Services for Any Workload

Compute Options

Bare Metal

- Instance isolation
- High throughput
- Low latency

Virtual Machines (VMs)

- Flexible sizing
- Security-hardened hypervisor
- Burstable and preemptible instances
- Dense IO and dedicated hosts

Containers

- Managed Kubernetes with bare metal option
- Container instance
- Self-healing clusters

Functions

- Serverless; container-native
- Open source

Processor Platforms

- AMD EPYC
- Intel Xeon
- Arm (Ampere)
- NVIDIA GPUs

Storage Options

Local Attached Storage

- NVMe SSDs
- Up to 51.2 TB
- Supports millions of IOPS

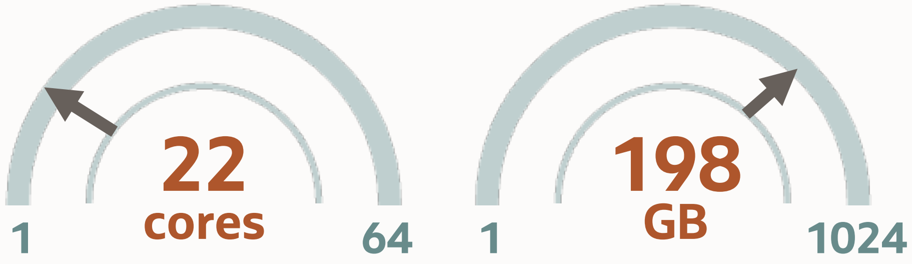
Remote Attached Storage

- NVMe Block Volumes up to 1 PB
- 32 TB / volume
- Up to 300k IOPS per volume

OCI Compute Flexible Instances—*Less Is More*

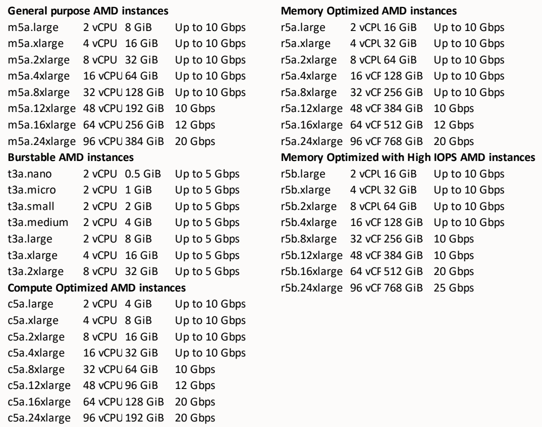
One Oracle Shape for Your Projects

One flexible instance type allows you to allocate cores & memory exactly as needed



Versus The Other Clouds

Fixed instance shapes dictate what you get, limit what you choose, cost more due to extra cores or memories than needed

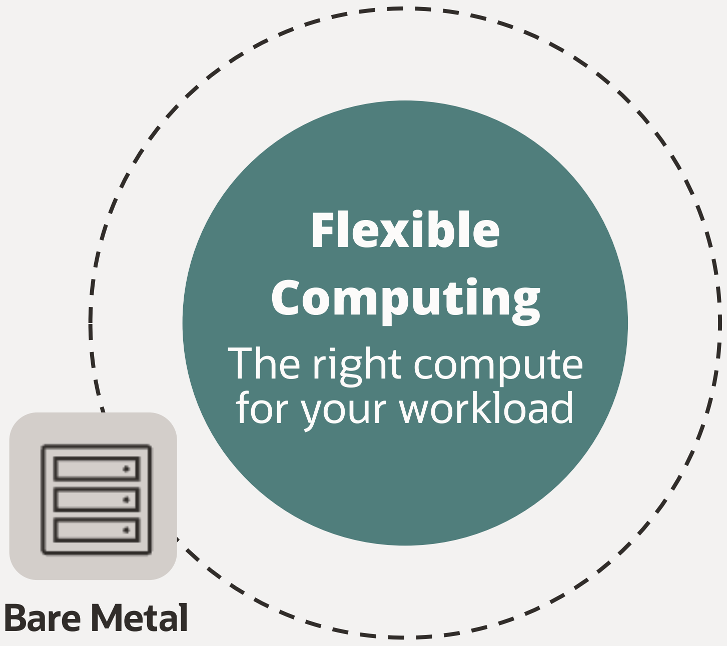


General purpose AMD instances			
m5a.large	2 vCPU	8 GiB	Up to 10 Gbps
m5a.xlarge	4 vCPU	16 GiB	Up to 10 Gbps
m5a.2xlarge	8 vCPU	32 GiB	Up to 10 Gbps
m5a.4xlarge	16 vCPU	64 GiB	Up to 10 Gbps
m5a.8xlarge	32 vCPU	128 GiB	Up to 10 Gbps
m5a.12xlarge	48 vCPU	192 GiB	10 Gbps
m5a.16xlarge	64 vCPU	256 GiB	12 Gbps
m5a.24xlarge	96 vCPU	384 GiB	20 Gbps
Burstable AMD instances			
t3a.nano	2 vCPU	0.5 GiB	Up to 5 Gbps
t3a.micro	2 vCPU	1 GiB	Up to 5 Gbps
t3a.small	2 vCPU	2 GiB	Up to 5 Gbps
t3a.medium	2 vCPU	4 GiB	Up to 5 Gbps
t3a.large	2 vCPU	8 GiB	Up to 5 Gbps
t3a.xlarge	4 vCPU	16 GiB	Up to 5 Gbps
t3a.2xlarge	8 vCPU	32 GiB	Up to 5 Gbps
Compute Optimized AMD instances			
c5a.large	2 vCPU	4 GiB	Up to 10 Gbps
c5a.xlarge	4 vCPU	8 GiB	Up to 10 Gbps
c5a.2xlarge	8 vCPU	16 GiB	Up to 10 Gbps
c5a.4xlarge	16 vCPU	32 GiB	Up to 10 Gbps
c5a.8xlarge	32 vCPU	64 GiB	10 Gbps
c5a.12xlarge	48 vCPU	96 GiB	12 Gbps
c5a.16xlarge	64 vCPU	128 GiB	20 Gbps
c5a.24xlarge	96 vCPU	192 GiB	20 Gbps

Memory Optimized AMD instances			
r5a.large	2 vCPL	16 GiB	Up to 10 Gbps
r5a.xlarge	4 vCPL	32 GiB	Up to 10 Gbps
r5a.2xlarge	8 vCPL	64 GiB	Up to 10 Gbps
r5a.4xlarge	16 vCF	128 GiB	Up to 10 Gbps
r5a.8xlarge	32 vCF	256 GiB	Up to 10 Gbps
r5a.12xlarge	48 vCF	384 GiB	10 Gbps
r5a.16xlarge	64 vCF	512 GiB	12 Gbps
r5a.24xlarge	96 vCF	768 GiB	20 Gbps
Memory Optimized with High IOPS AMD instances			
r5b.large	2 vCPL	16 GiB	Up to 10 Gbps
r5b.xlarge	4 vCPL	32 GiB	Up to 10 Gbps
r5b.2xlarge	8 vCPL	64 GiB	Up to 10 Gbps
r5b.4xlarge	16 vCF	128 GiB	Up to 10 Gbps
r5b.8xlarge	32 vCF	256 GiB	10 Gbps
r5b.12xlarge	48 vCF	384 GiB	10 Gbps
r5b.16xlarge	64 vCF	512 GiB	20 Gbps
r5b.24xlarge	96 vCF	768 GiB	25 Gbps

One simple global pricing model with everyday low pricing make it easy to predict spend

Your cloud should be flexible…

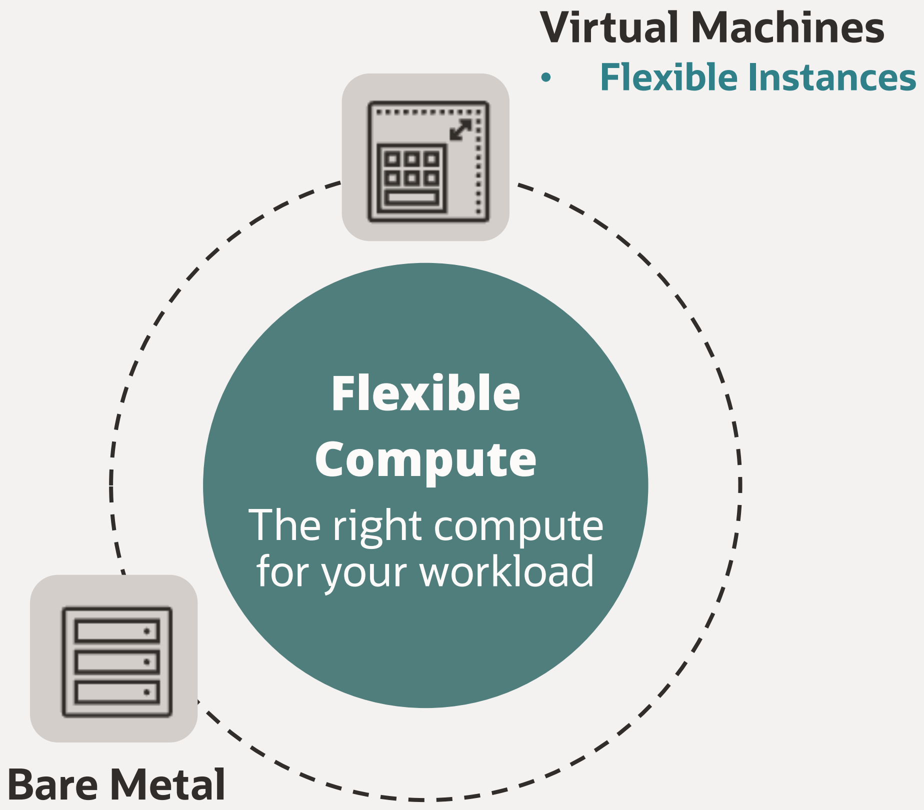


Bare Metal

Dedicated servers that perform better at a lower total cost

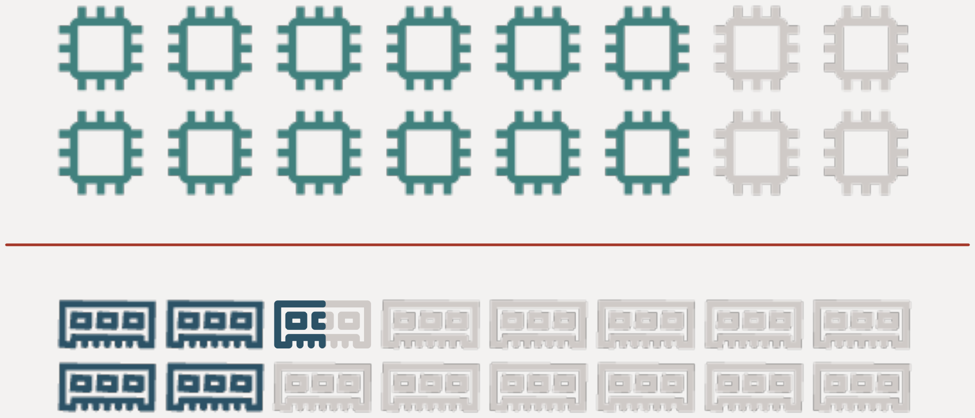
- Control the entire stack with dedicated and secure cloud computing
- Performance and scale without “noisy neighbors”
- Wide range of performance and price flexibility
- Freedom to choose OS platforms that match your existing workloads

Your cloud should be flexible…



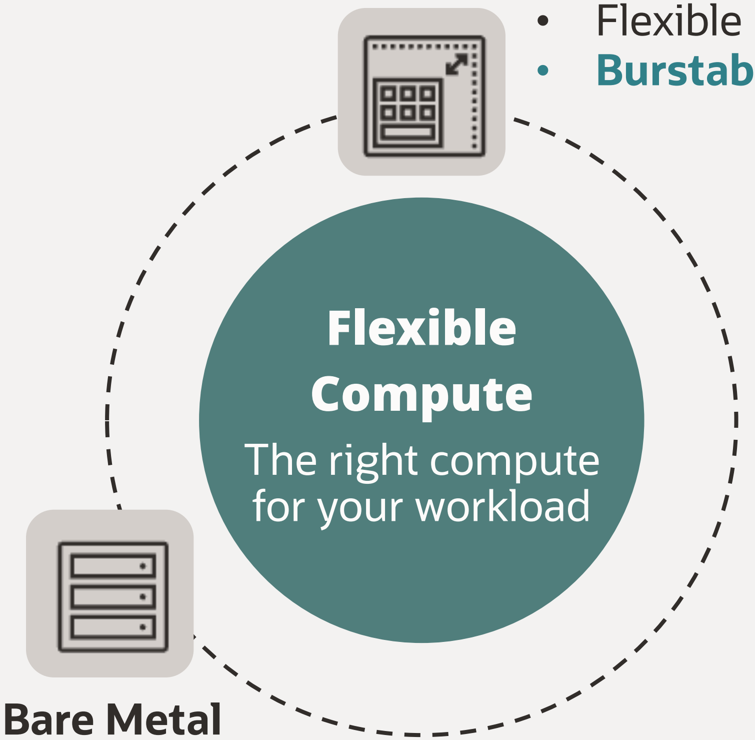
OCI Flexible VM instances

Pay for what you need, not more



12 core x 36 GB mem

Your cloud should be flexible…



Virtual Machines

- Flexible Instances
- **Burstable Instances**

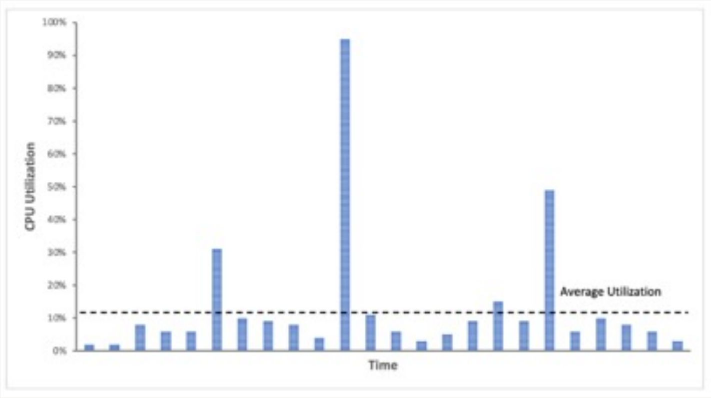
Flexible Compute

The right compute for your workload

Bare Metal

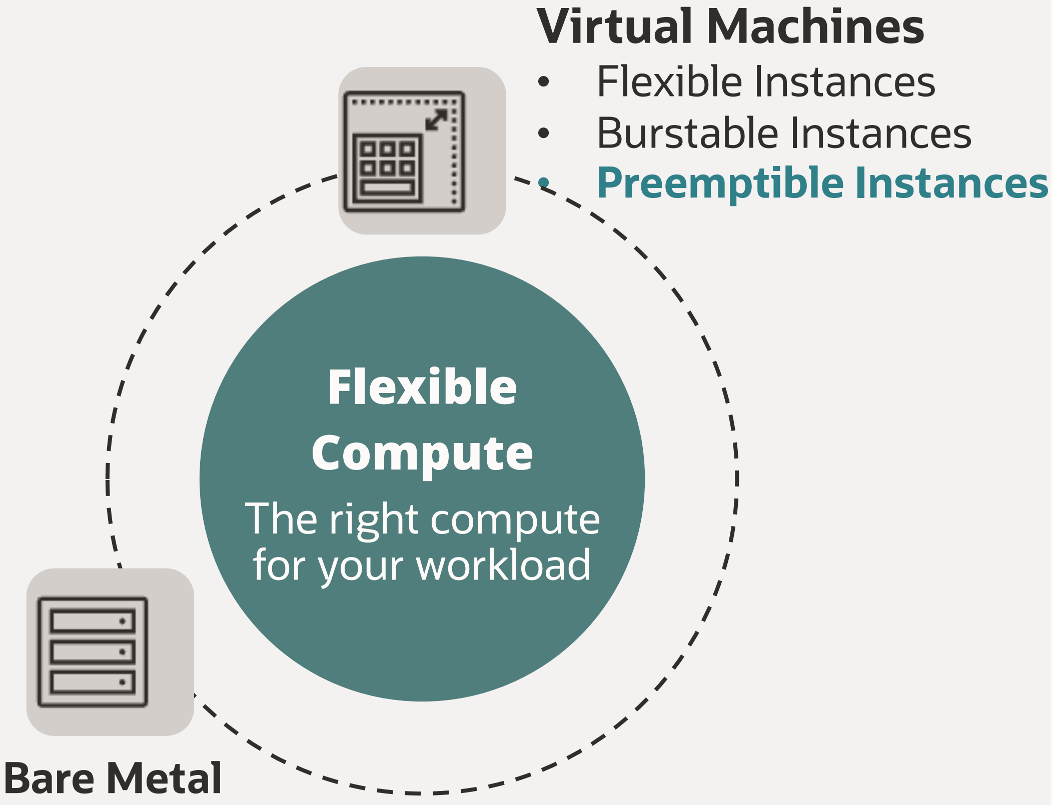
OCI **Burstable** VM Instances

Pay for what you need, burst to get more power



- **Optimized for low CPU workloads** that don't need full cores continuously
- **Easy to configure** with flexible VMs
- **Automatic CPU burst** requiring no customer action
- **Simple pricing** to easily predict spend
- **Choice** Available in all tenancies & regions

Your cloud should be flexible…



Virtual Machines

- Flexible Instances
- Burstable Instances
- **Preemptible Instances**

Flexible Compute

The right compute for your workload

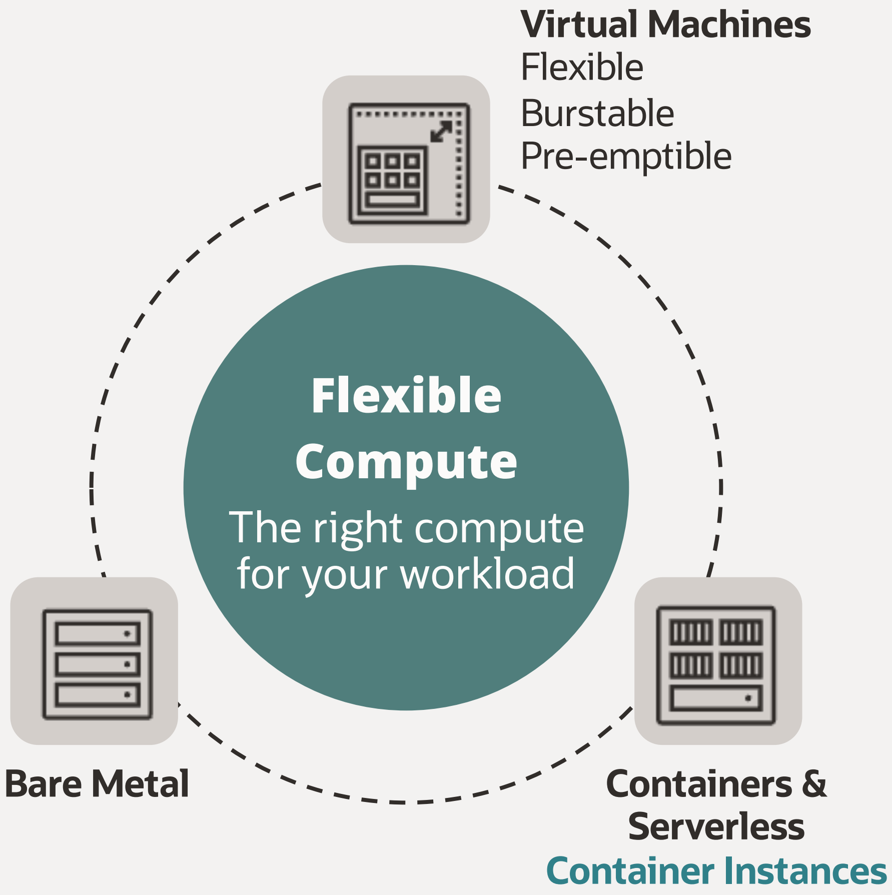
Bare Metal

OCI **Preemptible** VM Instances

Cost effective computing for fault-tolerant and interruptible workloads

- Ideal for batch jobs, rolling builds, big data analytics
- **Less Expensive**: Half the cost of on-demand compute
- **Same performance** and HW as on-demand instances
- **Easy to manage** same as on-demand instances
- **Choice** Available in all tenancies and regions

Your cloud should be flexible…



Virtual Machines
Flexible
Burstable
Pre-emptible

Flexible Compute
The right compute for your workload

Bare Metal

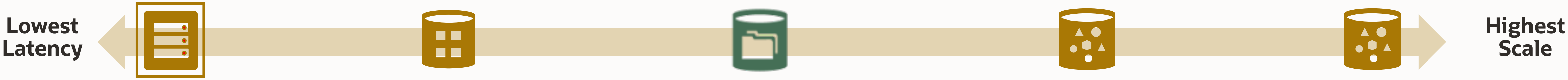
Containers & Serverless
Container Instances

OCI Container Instances

Deploy containers in seconds with less management overhead

- More efficient to operate than self-managed container environments
- Fast, 30-second startup
- Simple lifecycle and billing
- Reduced license costs and overhead
- For bursty or discrete workloads

High performance, flexible, scalable, and low-cost storage



Local NVMe

- Highest performance flash-based storage
- HPC and other demanding IO workloads

Block Storage

- Auto-tuned, high performance remote storage
- OS, application data, and large OLTP workloads

File Storage

- Managed and elastic shared file system

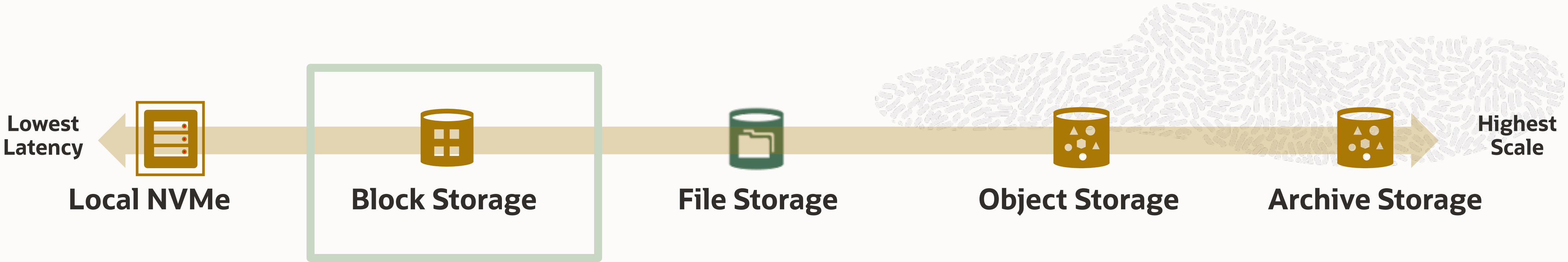
Object Storage

- Elastic unstructured data
- Big data, rich media, backups

Archive Storage

- Long-term archival and backup
- Cost-effective, cold data storage

↓	↑	↑	↑
Cost	Simplicity	Performance	Flexibility



Lowest Latency

Local NVMe

Block Storage

File Storage

Object Storage

Archive Storage

Highest Scale

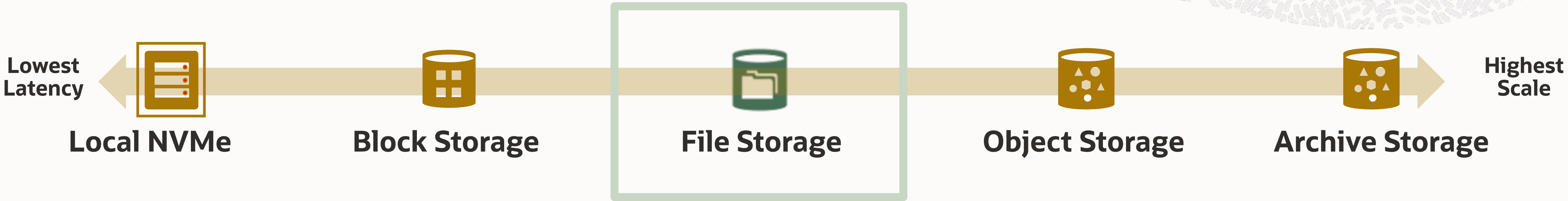
Overview

- **Fast, replicated** virtualized block storage for use with OCI Compute
- Best choice for your OS, application data and large, demanding OLTP workloads

Key Capabilities

- **Industry-leading** price-performance
- **SAN-like** management capabilities
- Scalable to **1 PB and 700,000 IOPS** per Compute instance
- **SLA backed** performance guarantees

File Storage Overview



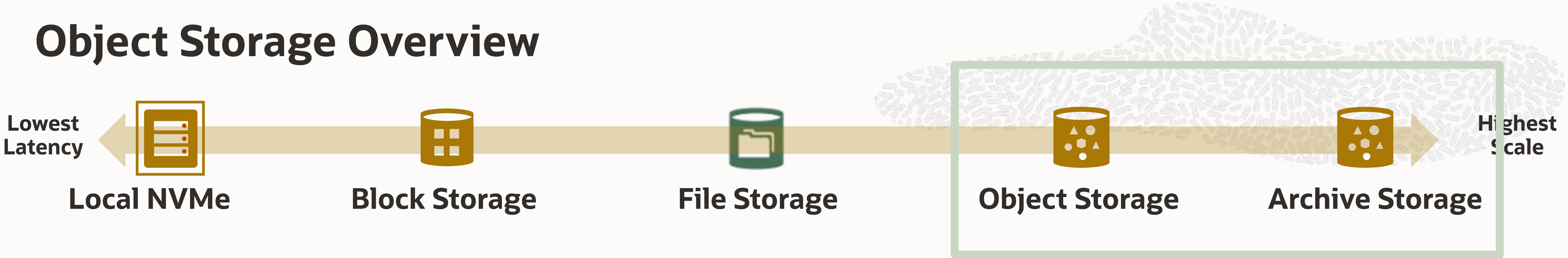
Overview

- Enterprise-grade **shared file system** for business applications
- Provides **network-attached storage (NAS)** in the Cloud that is management-free
- Optimized for parallel workloads

Key Capabilities

- Exabyte scale
- No need to provision, pay and scale as you go
- Easy snapshotting
- NFSv3 Support with Linux and Windows Compatibility
- Replication for Disaster Recovery
- Filesystem Cloning
- VMware certified storage solution

Object Storage Overview



Overview

- Ideal for **massive amounts** of unstructured data
- **Cost-effective** storage for logs, rich media, backup
- Highly **parallelizable**, ideal for big data

Key Capabilities

- **Infinitely** scalable
- Easy, well-established integration with leading solutions via **compatible APIs**
- Connectivity to **Hadoop and Spark** via HDFS connector

ORACLE