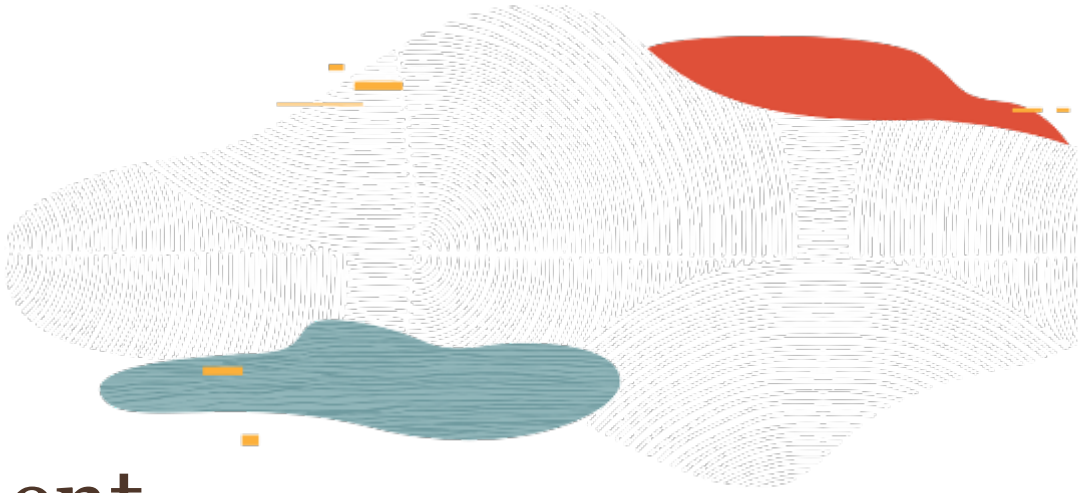
ORACLE



Identity and Access Management

L100

Safe Harbor Statement

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle’s products remains at the sole discretion of Oracle.

Identity and Access Management

- Identity and Access Management (IAM) service enables you to control what type of access a group of users have and to which specific resources
- Resource is a cloud object that you create and use in OCI (e.g. compute instances, block storage volumes, Virtual Cloud Networks)
- Each OCI resource has a unique, Oracle-assigned identifier called an Oracle Cloud ID (OCID)
- IAM uses traditional identity concepts such as Principals, Users, Groups, Policies and introduces a new feature called Compartments

Principals

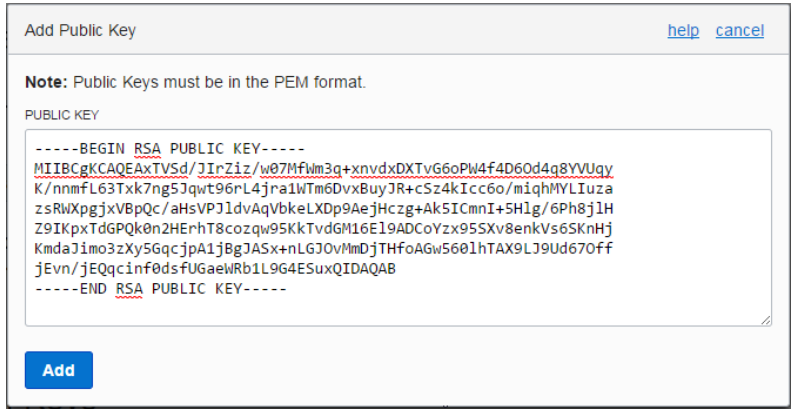
- A principal is an IAM entity that is allowed to interact with OCI resources
- Principals – IAM users and Instance Principals
- **IAM Users**
  - Users are persistent identities setup through IAM service to represent individual people or applications
  - When customers sign-up for an OCI account, the first IAM user is the default administrator
  - Default administrator sets up other IAM users and groups
  - Users enforce security principle of least privilege
    1. User has no permissions until placed in one (or more) groups and
    2. Group having at least one policy with permission to tenancy or a compartment
- A Group is a collection of users who all need the same type of access to a particular set of resources
- Same user can be member of multiple groups
- **Instance Principals**
  - Instance Principals lets instances (and applications) to make API calls against other OCI services removing the need to configure user credentials or a configuration file

Authentication

IAM service authenticates a Principal by –

- User name, Password
  - You use the password to sign in to the web console
  - An administrator will provide you with a one-time password when setting up your account
  - At your first log in, you are prompted to reset the password

- **API Signing Key**
  - Required when using the OCI API in conjunction with the SDK/CLI
  - Key is an RSA key pair in the PEM format (min 2048 bits)
  - In the interfaces, you can copy and paste the PEM public key
- **Auth Tokens**
  - Oracle-generated token strings to authenticate with 3rd party APIs that do no support OCI signature-based authentication (e.g. ADW)




```
begin
 DBMS_CLOUD.create_credential (
     credential_name => 'OBJ_STORE_CRED',
     username => '<userXX>',
     password => '<your Auth Token>'
  ) ;
end;
/
```

Authorization

- Authorization specifies various actions an authenticated Principal can perform
- OCI Authorization - define specific privileges in policies and associating them with principals
- Supports security principle of least privilege; by default, users are not allowed to perform any actions (policies cannot be attached to users, but only groups)
- Policies are comprised of one or more statements which specify what groups can access what resources and at what level of access
- Policies are written in human-readable format:
  - Allow group <group_name> to <verb> <resource-type> in tenancy
  - Allow group <group_name> to <verb> <resource-type> in compartment <compartment_name> [where <conditions>]

- Policy Attachment: Policies can be attached to a compartment or the tenancy. Where you attach it controls who can then modify it or delete it

Policy Syntax

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

Verb	Type of access
inspect	Ability to list resources
read	Includes inspect + ability to get user-specified metadata/actual resource
use	Includes read + ability to work with existing resources (the actions vary by resource type)*
manage	Includes all permissions for the resource

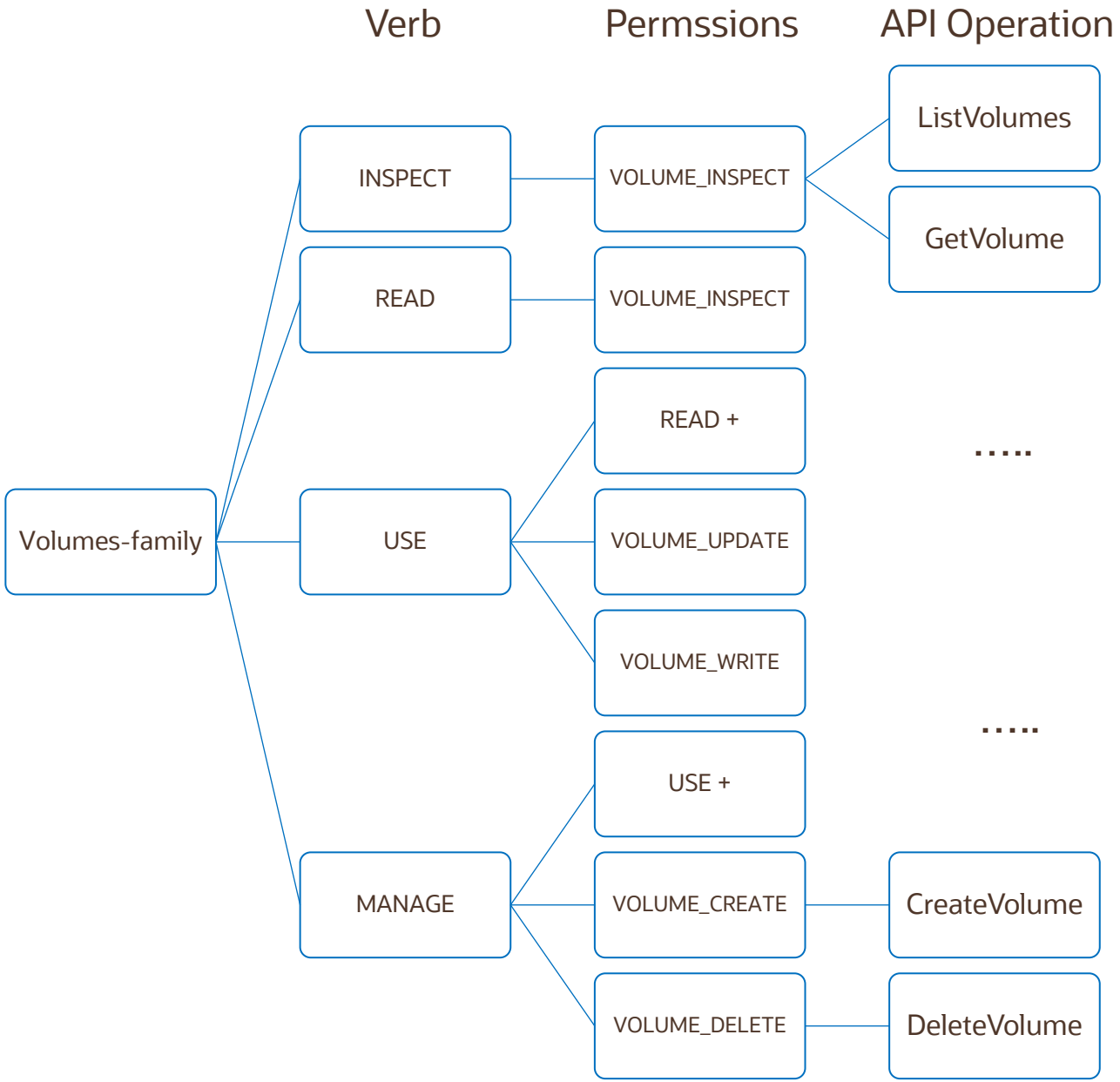
* In general, this verb does not include the ability to create or delete that type of resource

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

The IAM Service has no family resource-type, only individual ones; Audit and Load Balancer have individual resources (load-balancer, audit-events)

Verbs & Permissions

- When you write a policy giving a group access to a particular verb and resource-type, you're actually giving that group access to one or more predefined permissions
- Permissions are the atomic units of authorization that control a user's ability to perform operations on resources
- As you go from inspect > read > use > manage, the level of access generally increases, and the permissions granted are cumulative
- Each API operation requires the caller to have access to one or more permissions. E.g., to use ListVolumes or GetVolume, you must have access to a single permission: VOLUME_INSPECT



Common Policies

1. Network Admins manage a cloud network
    - Allow group NetworkAdmins to manage virtual-network-family in tenancy

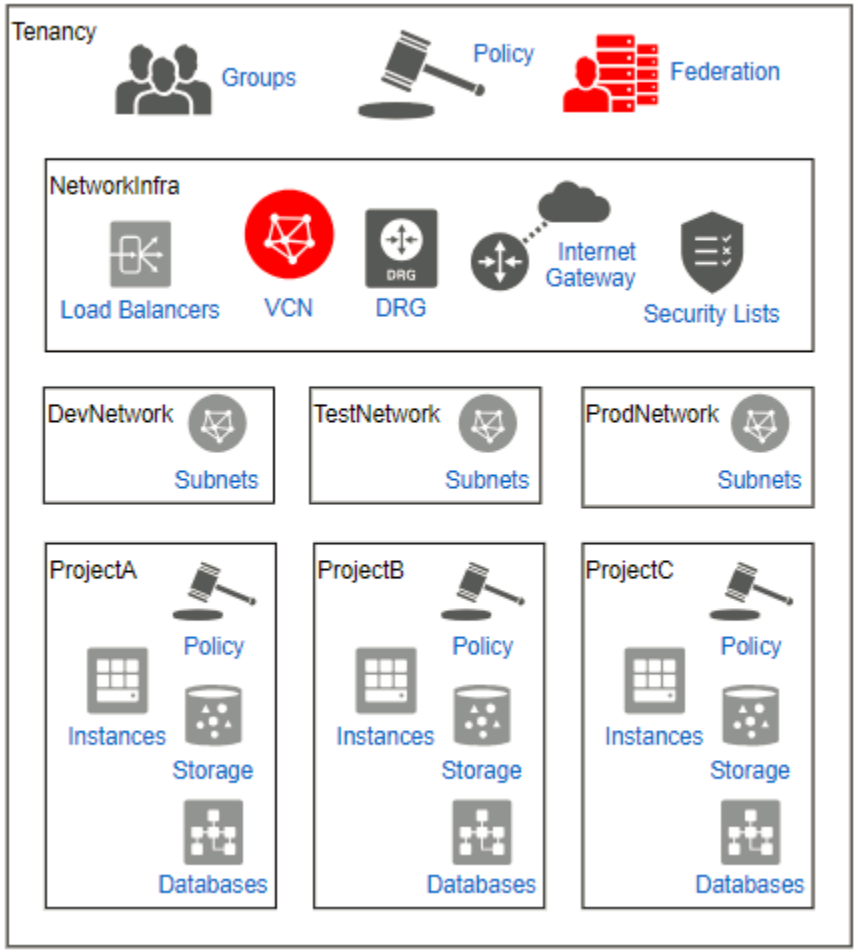
2. Object writers write to Object Storage
    - Allow group ObjectWriters to manage objects in compartment ABC where any {request.permission='OBJECT_CREATE', request.permission='OBJECT_INSPECT'}
    - Allow group ObjectWriters to manage objects in compartment ABC where any {request.operation='CreateObject', request.operation='ListObjects'}

3. Block Storage and Object Storage encrypt and decrypt volumes and buckets
    - Allow service blockstorage, objectstorage-<region_name> to use keys in compartment ABC

Compartment

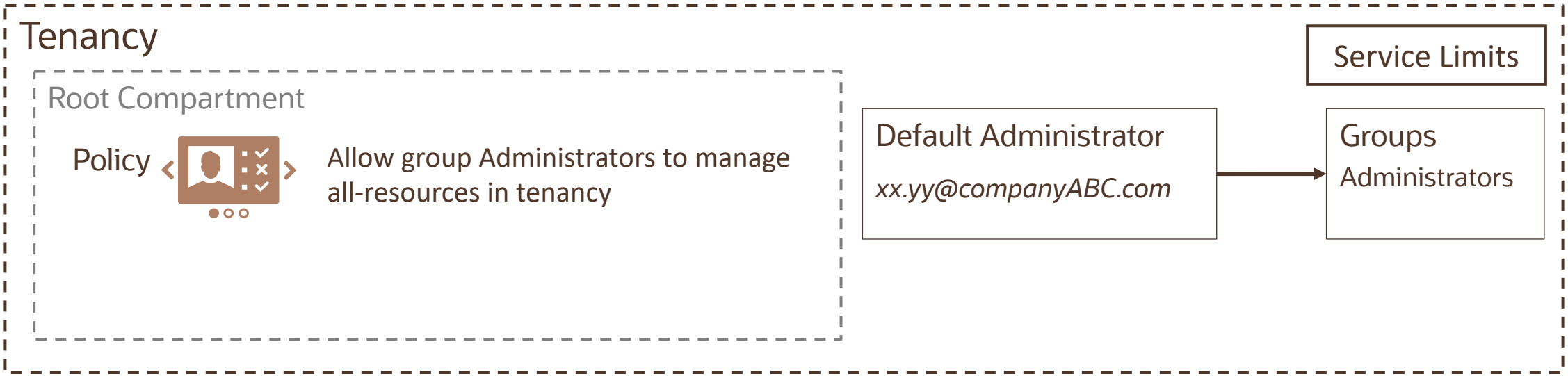
- A compartment is a collection of related resources (VCN, instances,..) that can be accessed only by groups that have been given permission (by an administrator in your organization)
- Compartments help you organize and control access to your resources
- Design considerations:
  - Each resource belongs to a single compartment but resources can be connected/shared across compartments (VCN and its subnets can live in different compartments)
  - A compartment can be deleted after creation or renamed
  - A compartment can have sub compartments that can be up to six levels deep
  - A resource can't be reassigned to a different compartment after creation (exception: Buckets)
  - After creating a compartment, you need to write at least one policy for it, otherwise it cannot be accessed (except by administrators or users who have permission to the tenancy)
  - Sub compartment inherits access permissions from compartments higher up its hierarchy
  - When you create a policy, you need to specify which compartment to attach it to

Reference Model: Compartments



- Compartment: NetworkInfra
  - Critical network infrastructure centrally managed by network admins
  - Resources: top level VCN, Security Lists, Internet Gateways, DRGs
- Compartment: Dev, Test, Prod Networks
  - Modeled as a separate compartment to easily write policy about who can use the network
  - Resources: Subnets, Databases, Storage(if shared)
- Compartment: Projects
  - The resources used by a particular team or project; separated for the purposes of distributed management
  - Resources: Compute Instances, Databases, Block Volumes, etc.
  - There will be multiple of these, one per team that needs it's own DevOps environment

When you sign up for OCI



- Oracle sets up a default administrator for the account
- Default Group Administrators
  - Cannot be deleted and there must always be at least one user in it
  - Any other users placed in the Administrators group will have full access to all of resources
  - Tenancy Policy gives Administrators group access to all resources – this policy can't be deleted/changed

- Root Compartment can hold all the cloud resources
- Best practice is to create dedicated Compartments when you need to isolate resources

Resource Locations

- Global:
  - IAM
  - Key Vaults, Keys
  - DNS

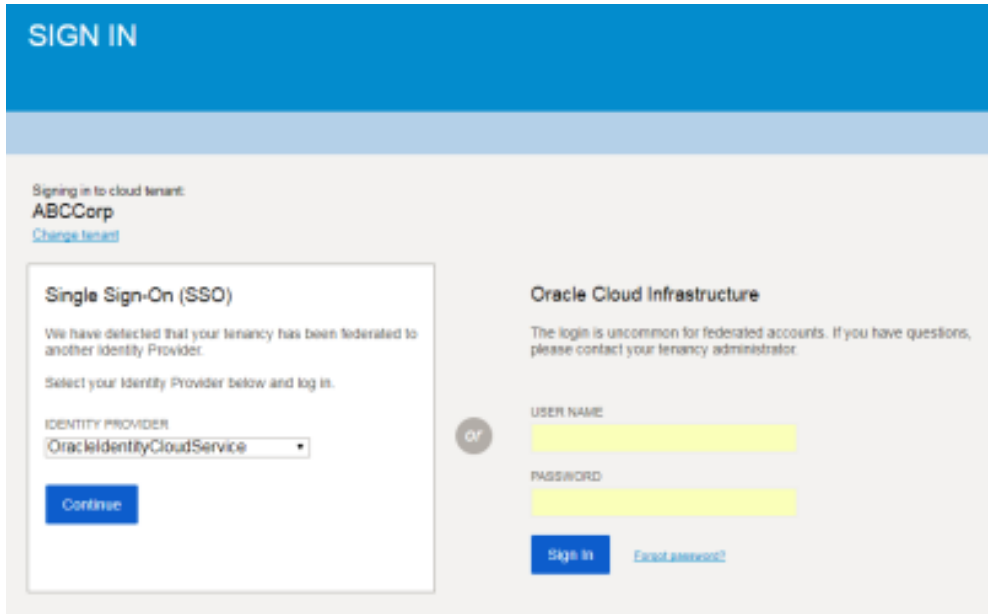
- Availability Domain:
  - Subnet
  - Compute instances
  - Block Volume
  - DB Systems
  - File System (& Mount Target)
  - Ephemeral Public IPs

- Regional:
  - Everything else!

Federation

- OCI provides federation with Oracle IDCS, Microsoft Active Directory and any identity provider that supports the Security Assertion Markup Language (SAML) 2.0 protocol

- Federation
  - First, a federation trust is setup between the Identity Provider (IdP) and OCI
  - Any person in your company who goes to OCI Console is prompted with a SSO experience provided by the IdP
  - The user signs in with the login/password that they've already set up with the IdP and use elsewhere
  - The IdP authenticates the user, and then that user can access OCI resources



Identity and Access Management Demo

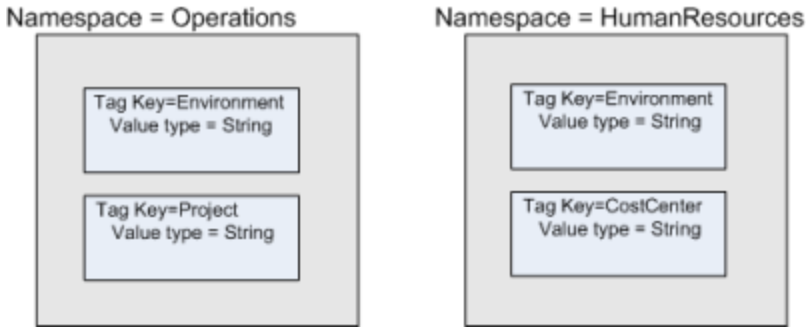
Tagging

- If you've ever added PHX-Project42-RCK21-FED to a title of a compute instance to remind yourself of its purpose, then you'll understand the value of tagging

- OCI Tagging allows you to:
  - Customize the organization of your resources
  - Control tag spam
  - Script bulk actions based on Tags

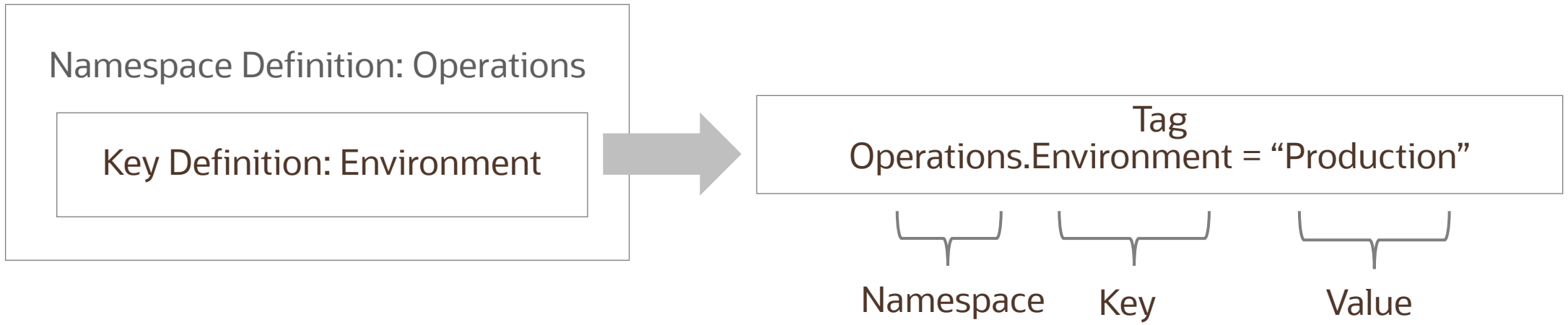
- Free-form Tags – basic implementation
  - Comprises key and value only
  - No defined schema or access restriction

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



Tag Namespace

- A Tag Namespace is a container for tag keys with tag key definitions
- Tag key definition specifies its key (environment) and what types of values are allowed (string, number, text, date, enumerations, etc.)



- Tag key definition or a tag namespace cannot be deleted, but retired. Retired tag namespaces and key definitions can no longer be applied to resources
- You can reactivate a tag namespace or tag key definition that has been retired to reinstate its usage in your tenancy

Audit Service

- Automatically records calls to OCI services API endpoints as log events
- Log Information shows time of API activity, source and target of the activity, action and response
- All OCI Services support Audit Logs
- Perform diagnostics, track resource usage, monitor compliance, and collect security-related events using Audit Logs
- By default, Audit logs are retained for 90 days. You can configure log retention for up to 365 days

Summary

- Identity and Access Management (IAM) service enables you to control what type of access a group of users have and to which specific resources
- IAM Principals – IAM users and Instance Principals
- Authentication – username/password, API Signing keys, Auth Tokens
- Authorization – Policies and associating them with Principals
- Policies syntax and examples of advanced policies
- Compartment, a unique OCI feature, can be used to organize and isolate related cloud resources
- OCI supports both free form tags and defined tags with a schema and secured by policies
- OCI Audit service automatically records calls to OCI services API endpoints as log events

ORACLE

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

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

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

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

Thank you