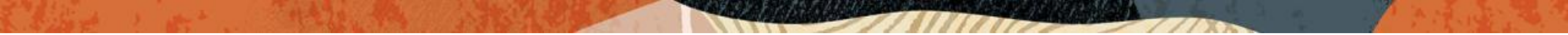
OCI Identity and Access Management

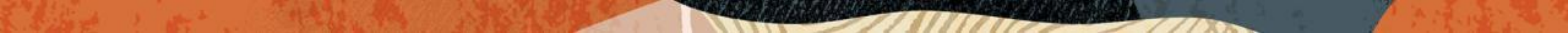
Rohit Rahi
Oracle Cloud Infrastructure

Feb 2020



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.



Agenda

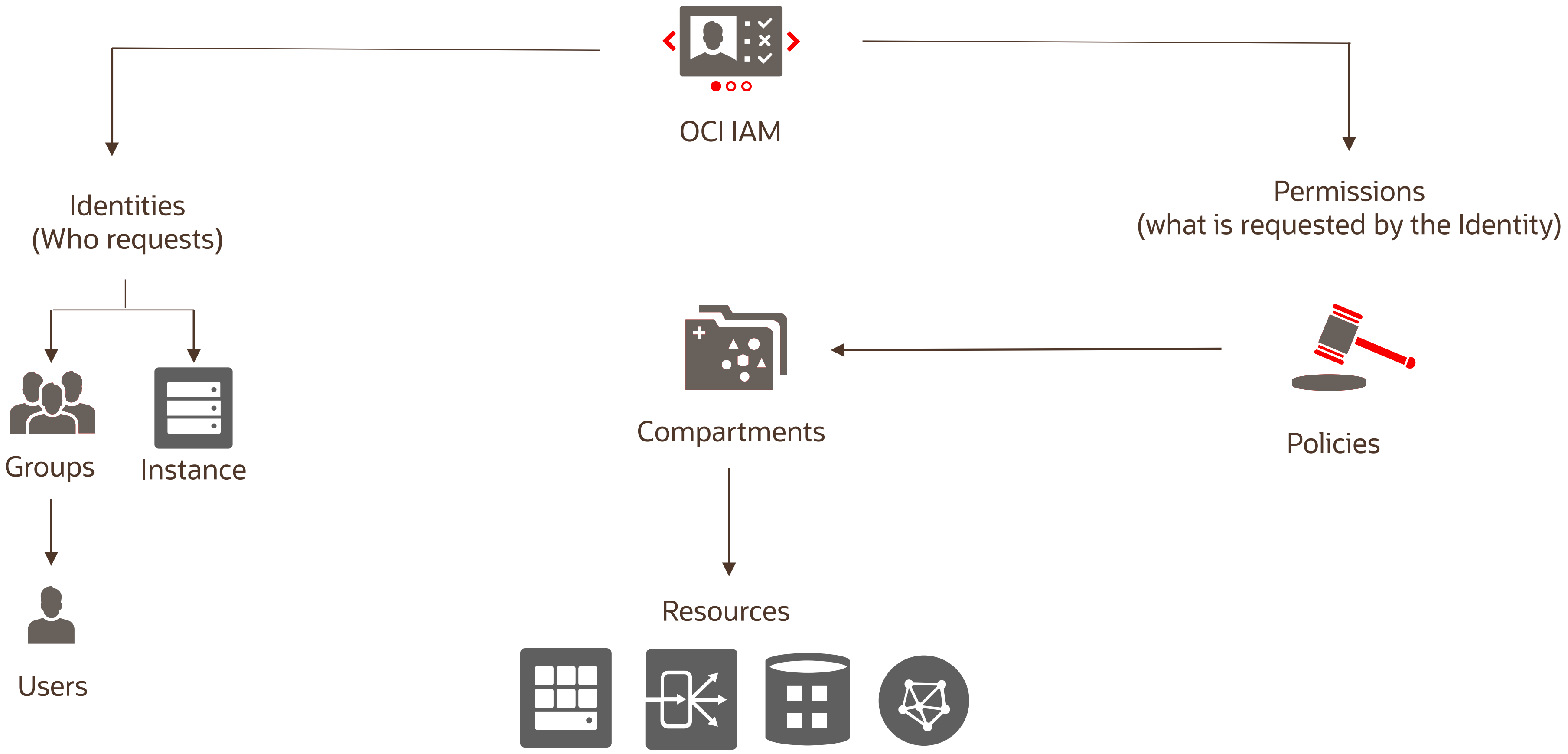
IAM

Authentication

Authorization

Policies

Identity and Access Management



OCI IAM

Identities
(Who requests)

Groups

Instance

Users

Permissions
(what is requested by the Identity)

Compartments

Policies

Resources

Principals

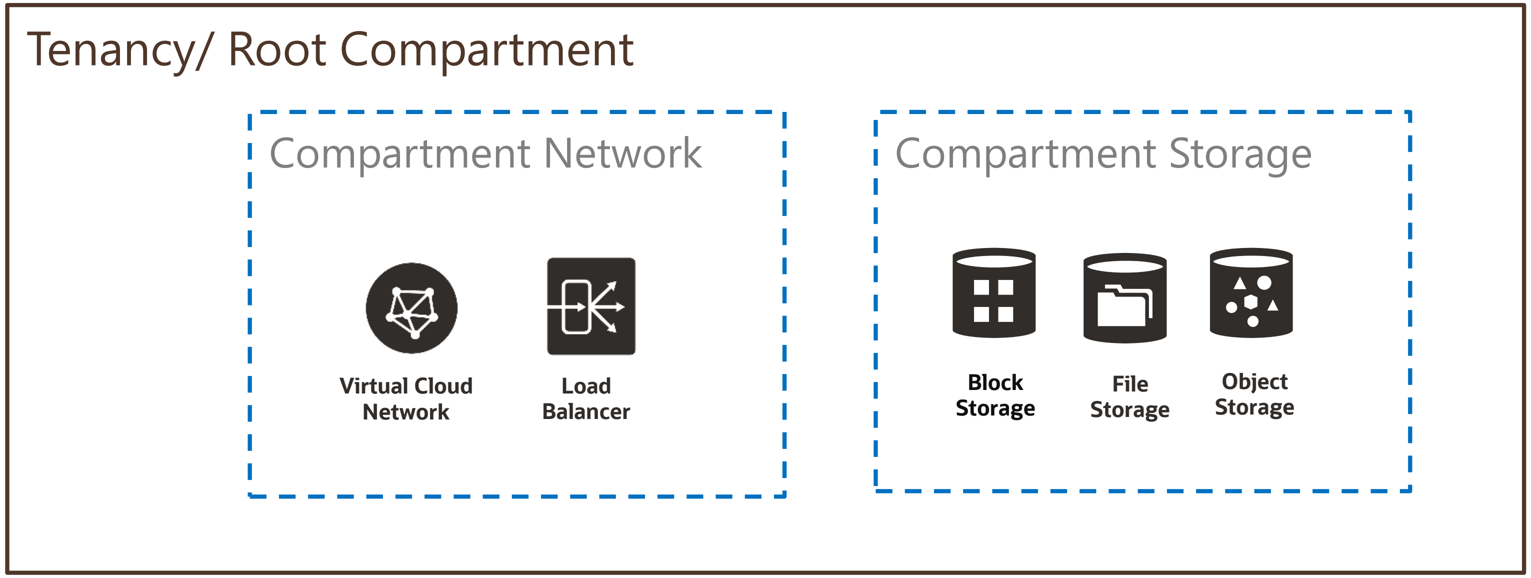
- A principal is an IAM entity that is allowed to interact with OCI resources
- Principals – IAM users and Instance Principals

- **IAM Users and Groups**
  - Users = individual people or applications
  - First IAM user = default administrator; admin sets up other IAM users and groups
  - Users enforce security principle of least privilege
    1. Users → Groups
    2. Group → at least one policy with permission to tenancy or a compartment

- **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

Compartment

A compartment is a collection of related resources. It helps you isolate and control access to your resources

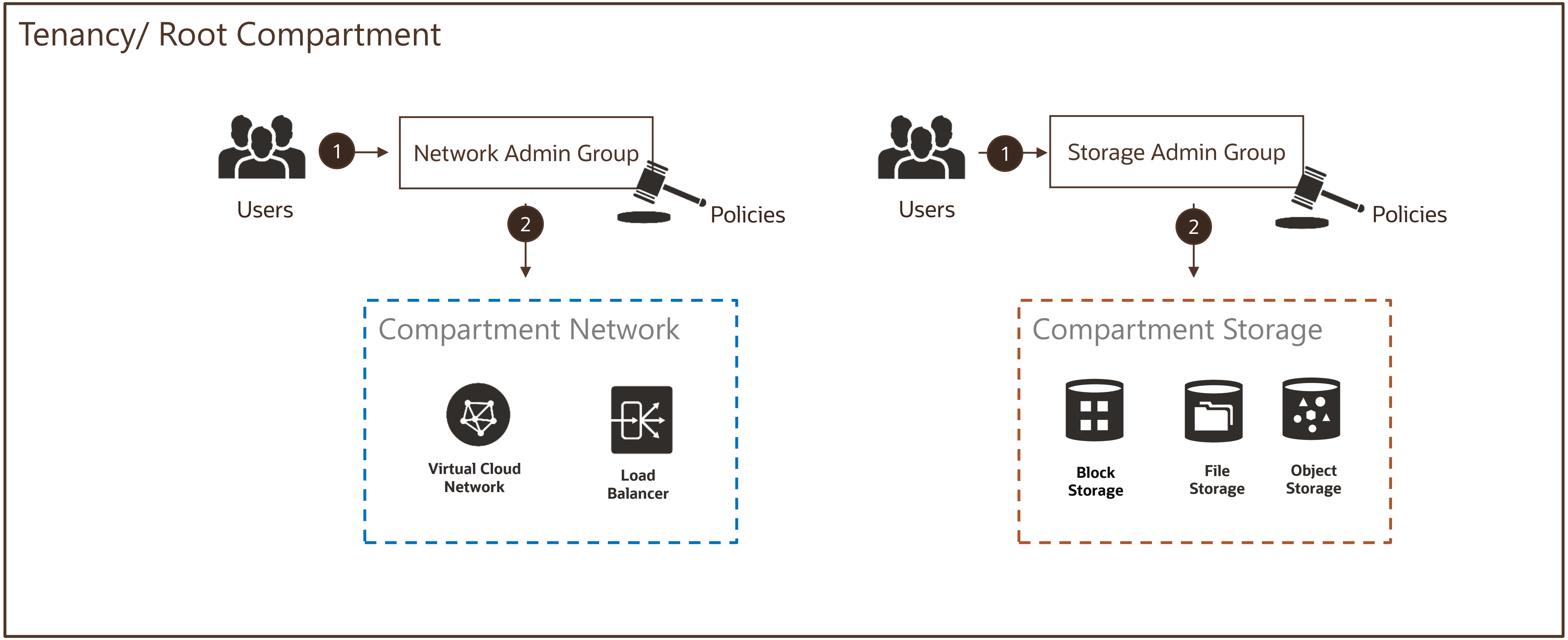


Root Compartment can hold all the cloud resources. Best practice is to create dedicated compartments when you need to isolate resources

Each resource belongs to a single compartment

Resources can interact with other resources in different compartments

You can give group of users access to compartments by writing Policies



Tenancy/ Root Compartment

Users

1

Network Admin Group

Policies

2

Compartment Network

Virtual Cloud Network

Load Balancer

Users

1

Storage Admin Group

Policies

2

Compartment Storage

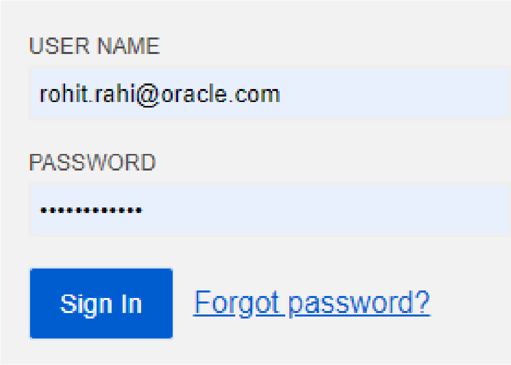
Block Storage

File Storage

Object Storage

Authentication

- Authentication deals with user identity: who is this person? Is this who he says he is?
- OCI IAM service authenticates a Principal by –
    - User name, Password
    - API Signing Key
        - Required when using the OCI API in conjunction with the SDK/CLI
    - Auth Tokens
        - Oracle-generated token strings to authenticate with 3rd party APIs that do no support OCI signature-based authentication (e.g. ADW)

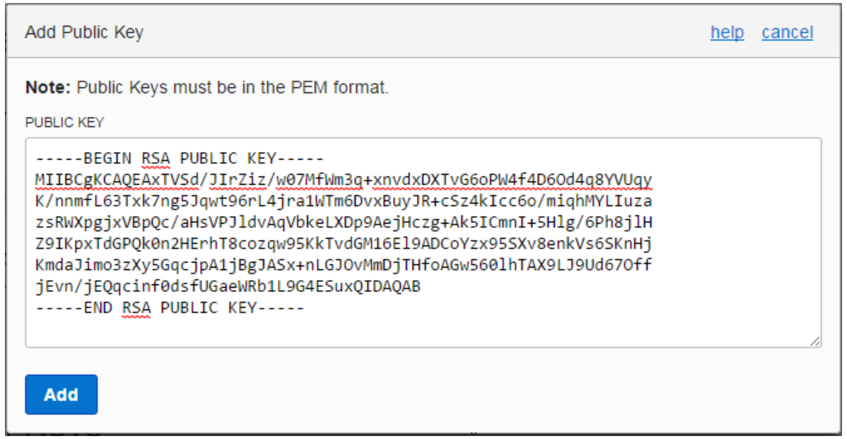


USER NAME

rohit.rahi@oracle.com

PASSWORD

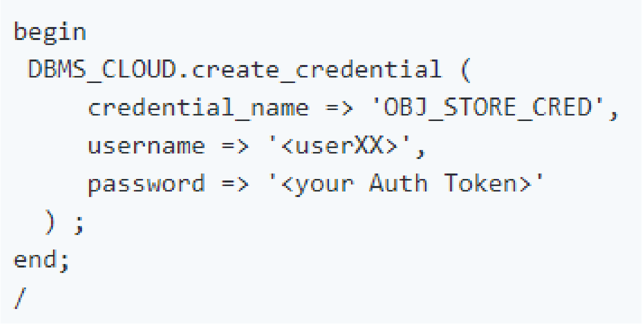
•••••••••••••



Note: Public Keys must be in the PEM format.

PUBLIC KEY

```
-----BEGIN RSA PUBLIC KEY-----
MIIBCgKCAQEAxTVSd/JIrZiz/w07MfWm3q+xnvdxDXTvG6oPW4f4D6Od4q8YVUqy
K/nnmfL63Txk7ng5Jqwt96rL4jra1WTm6DvxBuyJR+cSz4kIcc6o/miqhMYLIuza
zsRWXpgjxVBpQc/aHsVPJldvAqVbkeLXDp9AejHczg+Ak5ICmnI+5Hlg/6Ph8jlH
Z9IKpxTdGPQk0n2HErhT8cozqw95KkTvdGM16El9ADCoYzx95SXv8enkVs6SKnHj
KmdaJimo3zXy5GqcjpA1jBgJASx+nLGJOvMmDjTHfoAGw560lhTAX9LJ9Ud67Off
jEvn/jEQqcinf0dsfUGaeWRb1L9G4ESuxQIDAQAB
-----END RSA PUBLIC KEY-----
```



```
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 = Policies
- 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

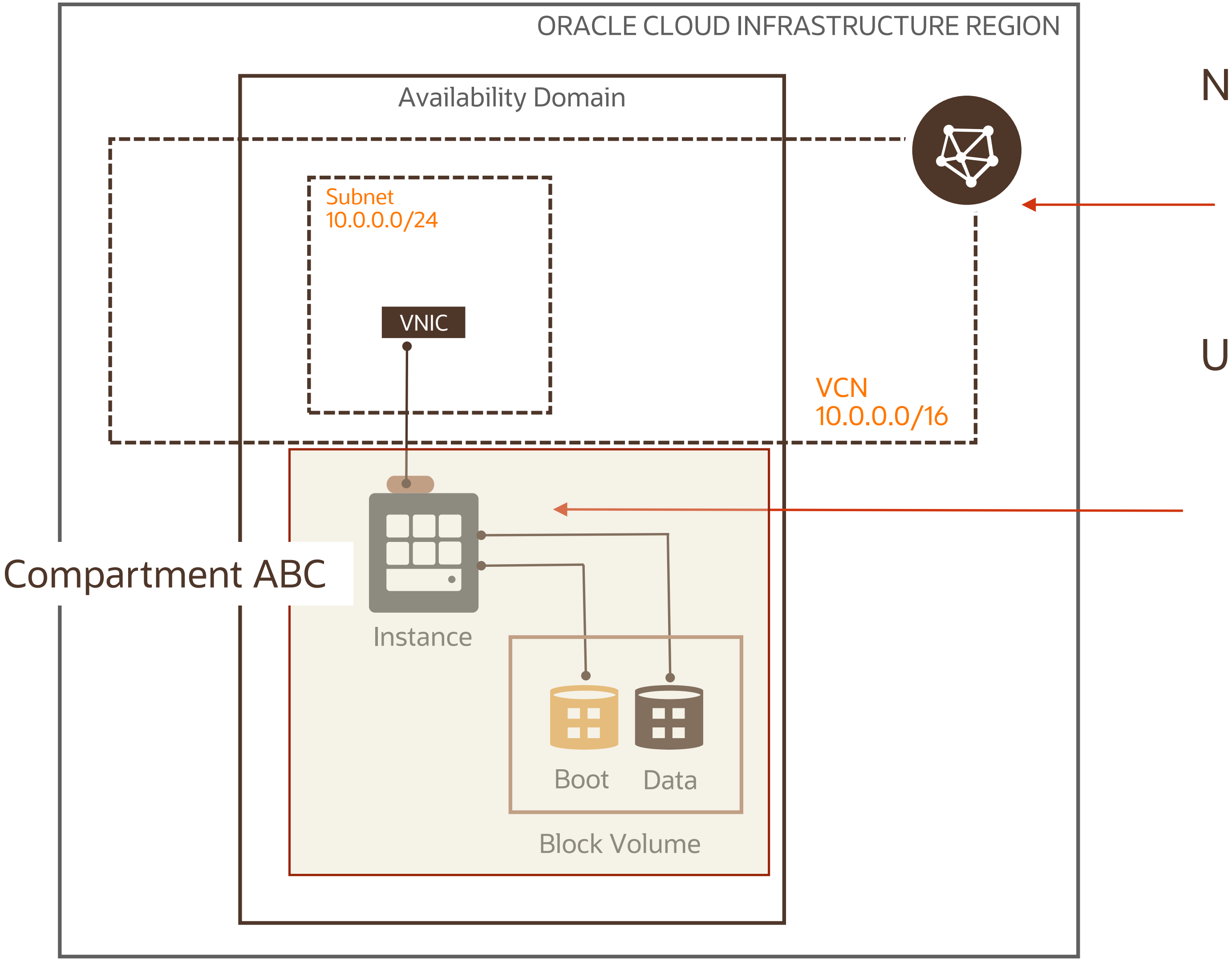
Allow <subject> to <verb> <resource-type> in <location> where <conditions>

Verb	**Type of access**
inspect	List resources
read	Inspect + user-specified metadata
use	Read + Update (the actions vary by resource type)*
manage	All permissions

* 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..
object-family	buckets, objects..
virtual-network-family	vcn, subnet, route-tables, security-lists, …
volume-family	volumes, volume-attachments, volume-backups
Cluster-family	clusters, cluster-node-pool, cluster-work-requests
File-family	file-systems, mount-targets, export-sets…
dns	dns-zones, dns-records, dns-traffic,..

Common Policies



Network Admins manage a cloud network

Allow group NetworkAdmins to manage virtual-network-family in tenancy

Users launch compute instances

Allow group InstanceLaunchers to manage instance-family in compartment ABC

Allow group InstanceLaunchers to use volume-family in compartment ABC

Allow group InstanceLaunchers to use virtual-network-family in compartment XYZ

https://docs.cloud.oracle.com/iaas/Content/Identity/Concepts/commonpolicies.htm

Summary

IAM

Authentication

Authorization

Policies

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