Cloud Engineering

Week 8 Intro

Typical Week

Watch Lecture Videos for the week before your first class

Attend every Q&A session – useful assessment tips

Attend every Lab

- Read Entire Instructions before Class
- Can get ahead on labs using Lab Reports to free up time

Start working on assignments and preparing for tests early

Typical Week

Consultation

- Every Teaching Week
- Underutilised

Discussion Board on Swinburne Canvas

- General questions

Lectures to watch

Swinburne Lectures

- High Level Overview
- Needed to pass

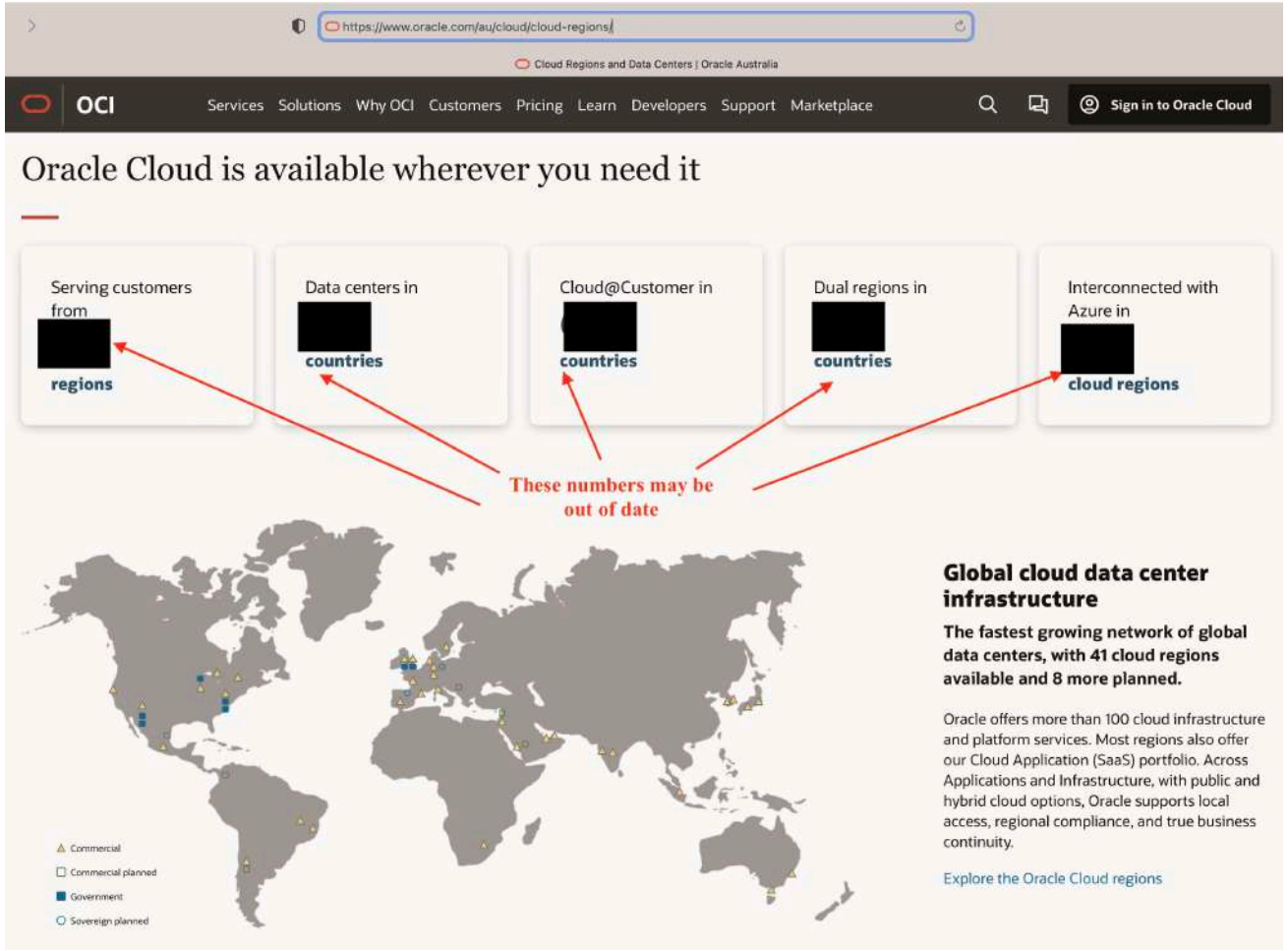
Oracle Lecture Videos

- Deep Dive
- More Topics and More Depth
- Aiming for high marks
- Prepare for certification

Oracle Academy Lecture Videos

- Deep Dive using Oracle Videos
- Prepared by OCI experts
- Cover more than needed for this course
- Some Technical Information in slides may be outdated
- Up to date information on the Web

https://www.oracle.com/au/cloud/cloud-regions/

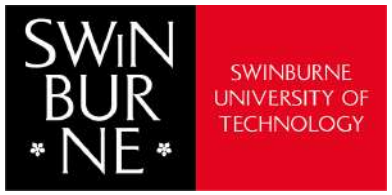


Week 8 Intro

This week:

- Compute services
  - OCI Compute Services
  - VM Images
- OCI Functions – Serverless platforms
- Network
  - CIDR
  - IP Addresses
  - Routing and Gateways
  - VPN & FastConnect

Compute Services



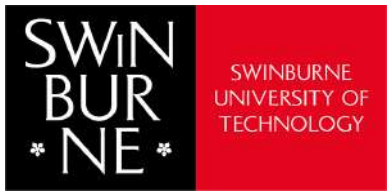
Week 8 Intro Compute Services

OCI Compute

Introduction to OCI Compute

VM Images – Oracle Provided, Custom Images and BYOI

OCI Functions



OCI Functions - Serverless

Background

OCI Functions

Networking

Networking

CIDR

IP Addresses

Routing & Gateways

VPN & Fast Connect

Next week

Next Week

Storage:

- Block Volume
- File storage
- Object Storage

Database:

- Available DB Systems on OCI
- Autonomous DB (ADB)
- Data Guard

Lecture References

Recommend Viewing

Swinburne Lecture – High Level Overview

Oracle Academy – Deeper dive

Cloud Engineering

Compute Services

SWINBURNE UNIVERSITY OF TECHNOLOGY

Compute Services

This presentation:

- OCI Compute Services
- VM Images

Compute

Wide range of compute services for any enterprise use case

Bare Metal

Dedicated physical server access for highest performance and isolation.

When to use:

Applications that require high core counts, large amounts of memory, and high bandwidth

Virtual Machines

An independent computing environment that runs on top of bare metal hardware

When to use:

Applications that do not require the performance and resources of an entire physical machine

Containers

Standard units of software that package code and dependencies for quick and reliable deployments

When to use:

Applications with microservice-based architectures

Functions

Simplify application development with serverless compute.

When to use:

If you just want to focus on the code and not worry about the underlying infrastructure

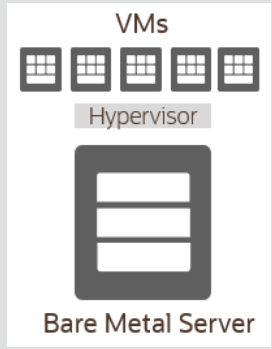
Bare Metal, VM and Dedicated Hosts

Bare Metal (BM)

- Direct Hardware Access – customers get the full Bare Metal server (single-tenant model)

Virtual Machine (VM)

- A hypervisor to virtualize the underlying Bare Metal server into smaller VMs (multi-tenant model)



Dedicated VM Hosts (DVH)

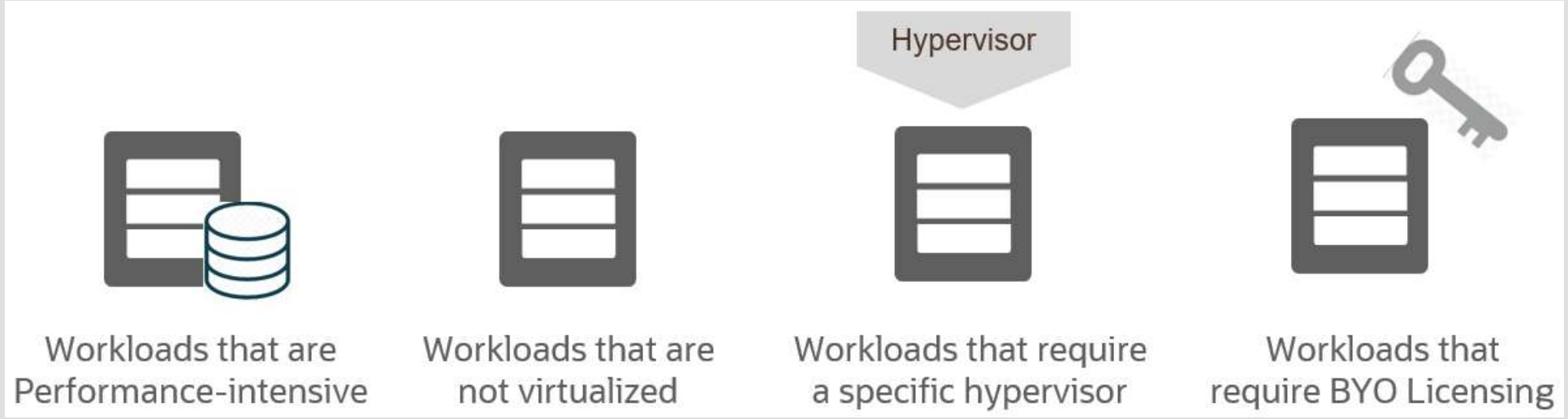
- Run your VMs instances on dedicated servers that are a single tenant and not shared with other customers

VM compute instances runs on the same hardware as a Bare Metal instances, leveraging the same cloud-optimized hardware, firmware, software stack, and networking infrastructure

ORACLE Academy

Bare Metal

Direct Hardware Access with all the Security, Capabilities, Elasticity and Scalability of Oracle Cloud Infrastructure



ORACLE Academy

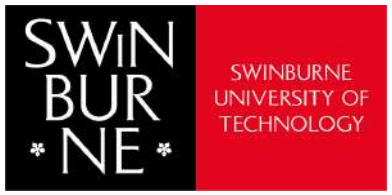
Bare Metal Instances

Shape	Instance type	OCPU	RAM (GB)	Local Disk (TB)	Network Bandwidth	Max vNICs (Linux)	Max vNICs (Win)
BM.Standard2.52	X7 Standard compute	52	768	Block Storage only	2 x 25 Gbps	52	27
BM.DenseIO2.52	X7 Dense I/O compute	52	768	51.2 TB NVMe SSD	2 x 25 Gbps	52	27
BM.Standard.E2.64	E1 AMD Standard compute	64	512	Block Storage only	2 x 25 Gbps	75	76
BM.HPC2.36	X7 High Frequency	36	384	6.7 TB NVMe SSD	1 x 100 Gbps RDMA	50	1
BM.GPU2.2	2xP100 NVIDIA GPUs	28	192	Block Storage only	2 x 25 Gbps	28	15
BM.GPU3.8	8xV100 NVIDIA GPUs	52	768	Block Storage only	2 x 25 Gbps	52	27
BM.Standard1.36	X5 Standard compute	36	256	Block Storage only	10 Gbps	36	1
BM.DenseIO1.36	X5 Dense I/O compute	36	512	28.8 TB NVMe SSD	10 Gbps	36	1
BM.Standard.B1.44	X6 standard compute	44	512	Block Storage only	25 Gbps	44	NA

- Compute Standard E2 is based of AMD EPYC™ processor
- 2 x 25 Gbps implies two NIC cards with 25 Gbps bandwidth
- Network bandwidth is based on expected bandwidth for traffic within a VCN

ORACLE Academy

VM Images



OCI Compute Services

VM Images

Installing OS from scratch takes time

Want to spin up new host quickly

Use images

OCI Compute Services

VM Images

Choose OS

Oracle Linux

RHEL

CentOS

Ubuntu

Windows Server

OCI Compute Services – VM Images

Oracle Provided Images

OS Pre-installed

Username created

Linux – firewall rules

Linux - Startup script using cloud-init

Windows – OTP

Windows – Windows Update

Custom Images

Custom image of instance
Boot disk

Preinstalled software
Other customisations

No data from attached block volume

Max 300GB

Windows - Can't export/download

BYO Image

Bring Own image to Cloud

If underlying hardware supports

Cloud Migration

Old and New OS support

Experimentation/Flexibility

Image Import/Export

- Compute service enables you to share custom images across tenancies and regions using image import/export
- Image import/export uses OCI Object Storage service
- You can import Linux and Windows Operating System
- Supports:
  - **Emulation Mode**:
    - Virtual machines I/O devices (disk, network), CPU, and memory are implemented in software
    - Emulated VM can support almost any x86 operating system. These VMs are slow
  - **Paravirtualized**:
    - Virtual Machine includes a driver specifically designed to enable virtualization
  - **Native Mode**: same as Hardware Virtualized Machine (HVM), offers maximum performance with modern OS's
- You can also find more information about custom images here: https://cloud.oracle.com/iaas/whitepapers/deploying_custom_os_images.pdf

Custom Image v/s Boot Volume Backup

- Custom Images

Pros	Cons
You can export a custom image across regions and tenancies	Instance shuts down and remains unavailable for several minutes until the process finished
No cost associated to store your custom images	Limit of 25 custom images per compartment

- Boot volume Backup

Pros	Cons
It doesn't require a downtime	Cost associated with the amount of Object Storage used to store your backup
Preserve the entire state of your running operating system as a backup	Creating a boot volume backup while instance is running creates a crash-consistent backup

ORACLE Academy

References

References

Oracle Cloud Academy Foundations I Section 4

Day One and Beyond - Season 4 - Oracle Cloud Technical Quick Start:
https://www.youtube.com/watch?v=8kYEYNMK4zg

Cloud Engineering

OCI Functions – Serverless Platforms

SWINBURNE UNIVERSITY OF TECHNOLOGY

OCI Functions – Serverless Platforms

This presentation:

- Background
- OCI Functions

OCI Functions – Serverless Functions

Serverless

Very popular for new architectures

Offers advantages over Compute and Container

OCI Functions – Serverless Functions

Infrastructure as Code

Principles for good software development = Principles for good cloud architecture design

Automate deployment - Terraform

OCI Functions – Serverless Functions

Infrastructure as Code

Decoupling applications

Want loose coupling

OCI Functions – Serverless Functions

Microservice

Perform one task and one task only

May receive some input

May output something

Loosely coupled

Add/Remove microservices without breaking the architecture

Very modular

Extensible

OCI Functions – Serverless Functions

Compute Instance is not a Microservice

Compute Instance running full operating system

Idle CPU, Memory, Storage

Paying for what not using

Expensive to scale

OCI Functions – Serverless Functions

Containers

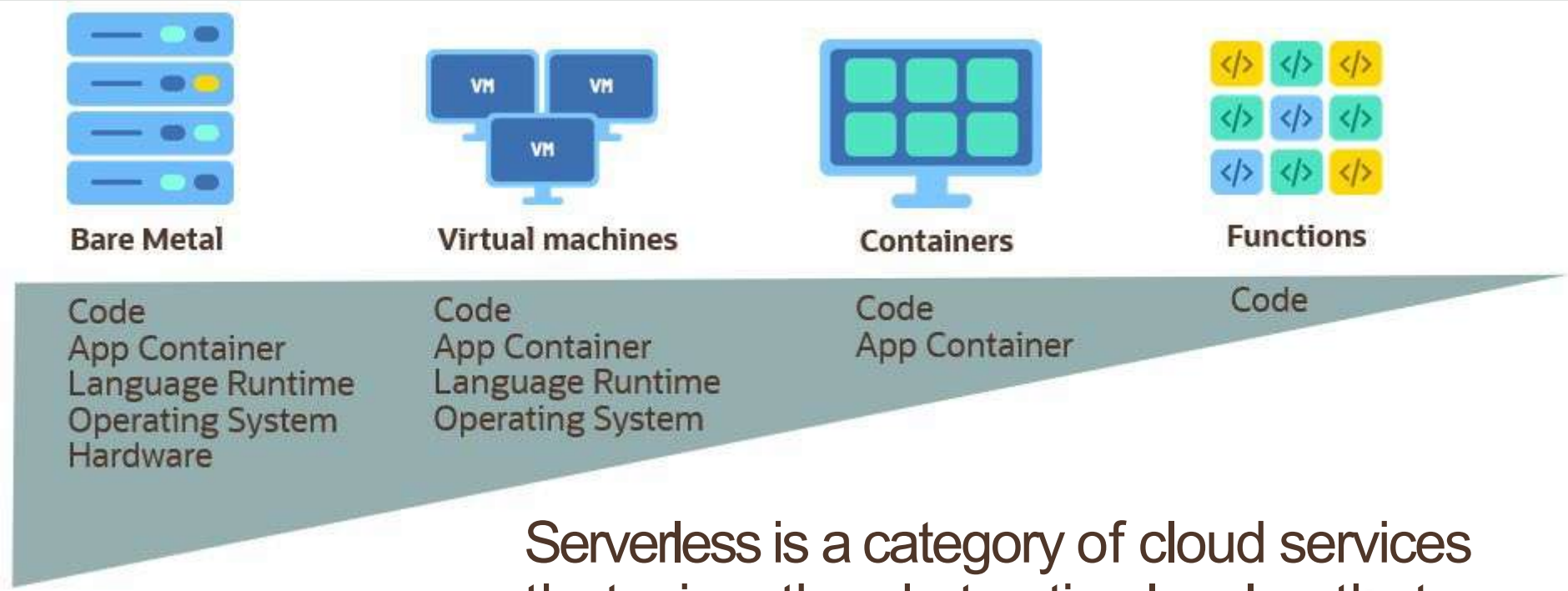
Start faster than Compute Instance

More lightweight

May be a microservice

May still be overprovisioning

Serverless Compute – Functions-as-a-service (FaaS)



Serverless is a category of cloud services that raises the abstraction level so that developers don't need to think about servers, VMs or other IaaS components

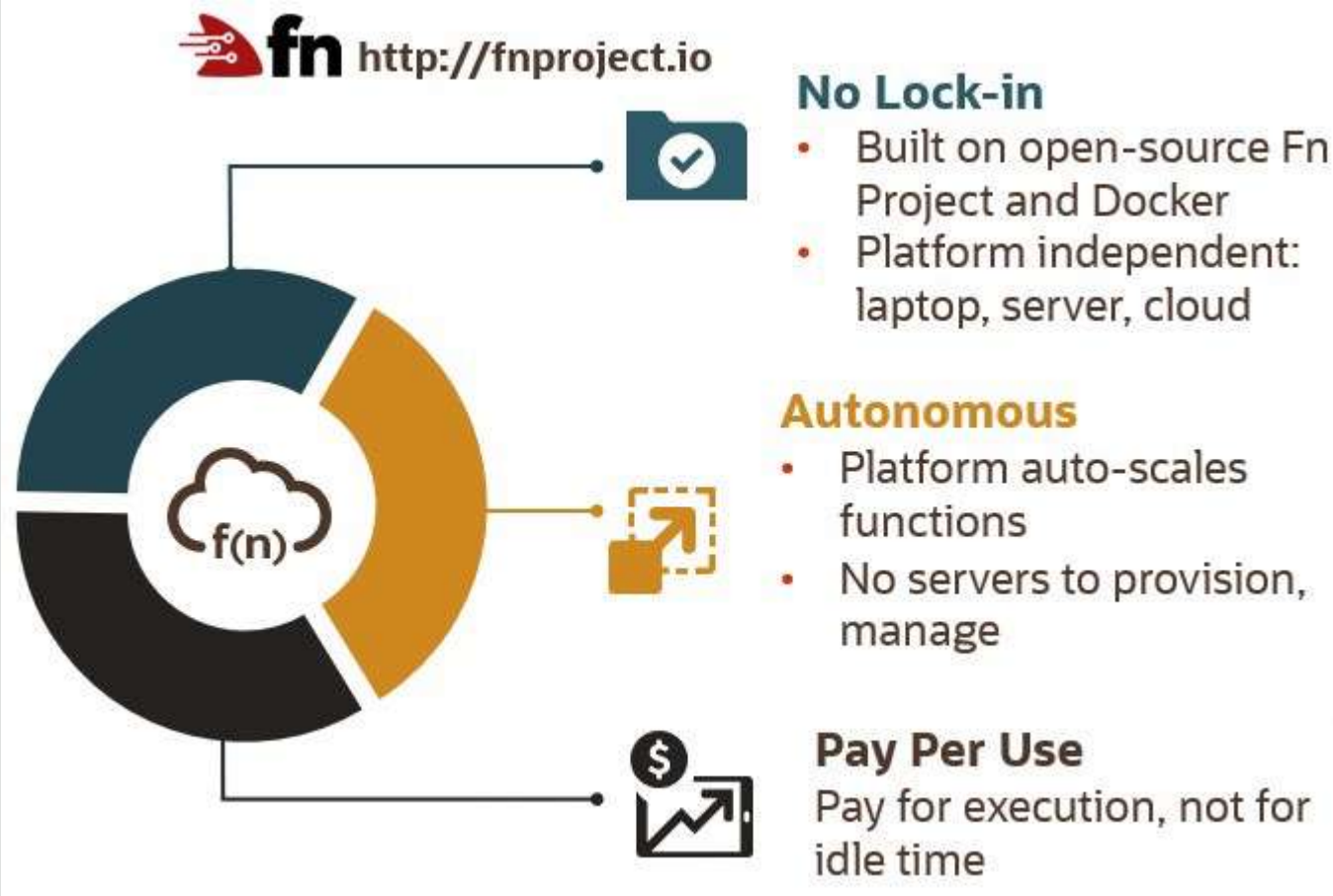
OCI Functions – Serverless Functions

Automation – Serverless vs Container vs Compute Instance

Code vs Software and Code vs Full OS

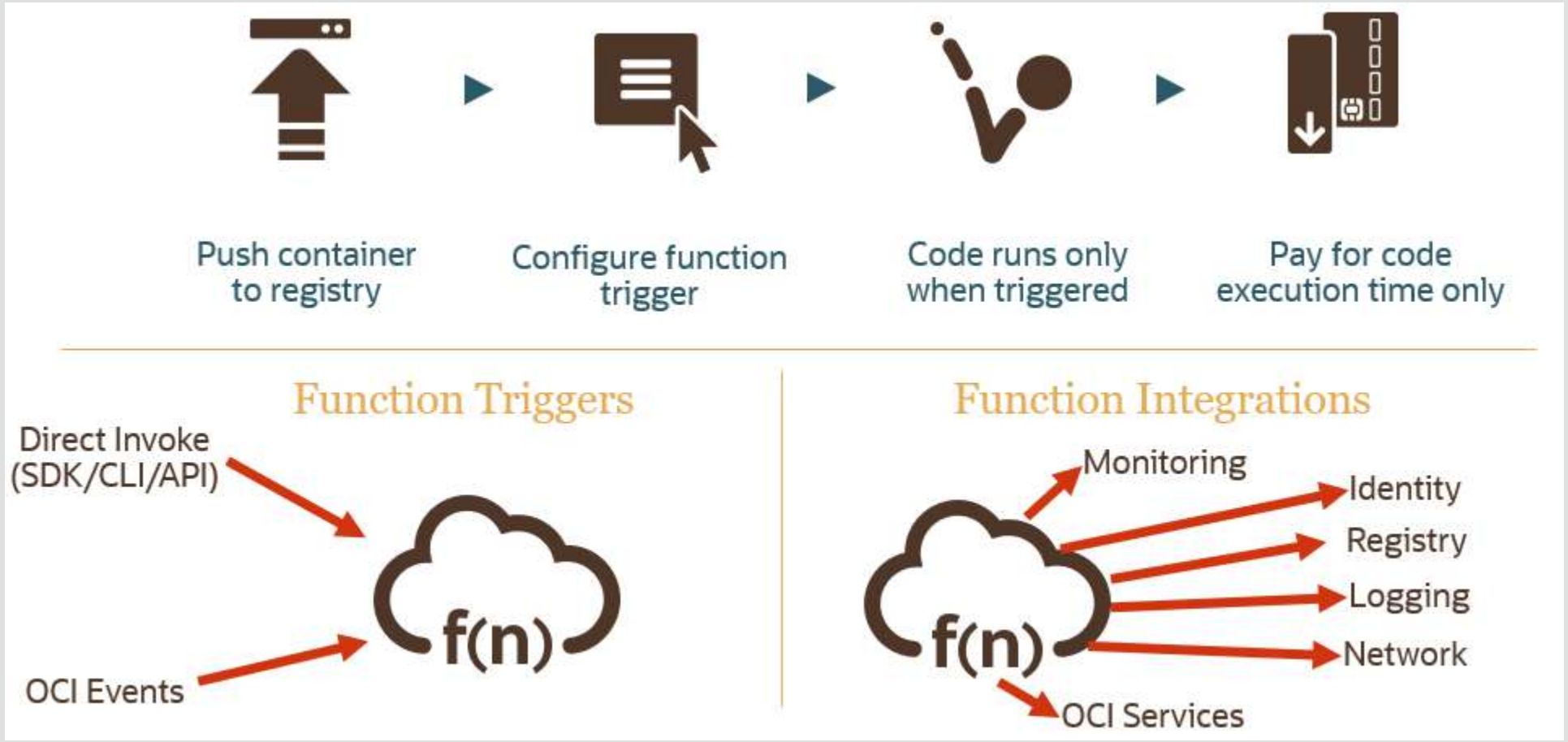
Oracle Functions

- Functions-as-a-Service
- Oracle Cloud Integrated
- Container Native
- Open Source Engine
- Multi-tenant
- Secure



ORACLE Academy

Functions Overview



ORACLE Academy

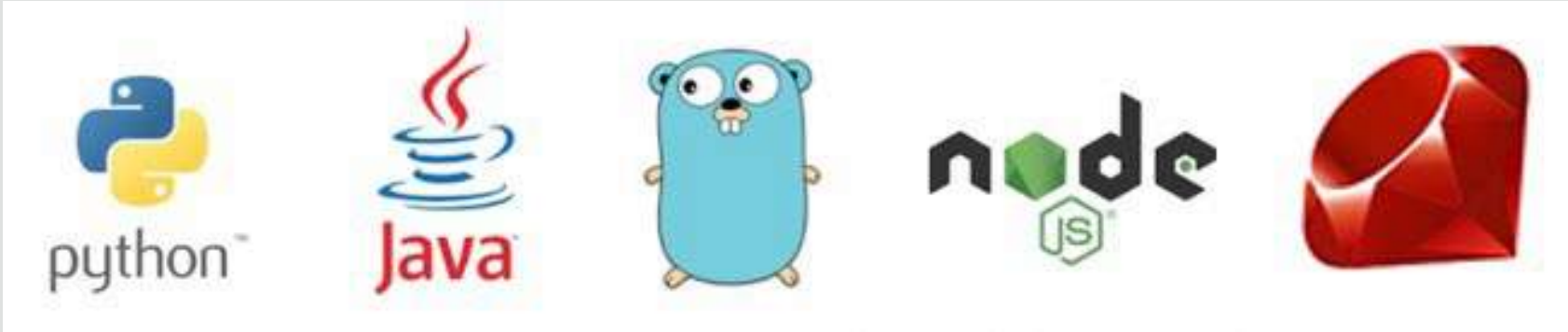
Example Java Function

```java
package com.example.fn;

public class HelloFunction {

    public String handleRequest(String input) {
        String name = (input == null || input.isEmpty()) ? "world" : input;

        return "Hello, " + name + "!";
    }

}
```

ORACLE Academy

Function Development Kits (FDKs)

- Simply write a `handler` function that adheres to the FDK's interface and the FDK will provide the input to your function, as well as deal with returning the proper output format.
- FDKs make it easy to write functions



ORACLE Academy

Oracle Functions Concepts - Applications

- In Oracle Functions, an application is:
  - a logical grouping of functions
  - a common context to store configuration variables that are available to all functions in the application
- When you define an application in Oracle Functions, you specify the subnets in which to run the functions in the application
- Oracle Functions shows applications and their functions in the Console

Oracle Functions Concepts - Functions

- In Oracle Functions, functions are:
  - small but powerful blocks of code that generally do one simple thing
  - grouped into applications
  - stored as Docker images in a specified Docker registry
  - invoked in response to a CLI command or signed HTTP request
- When you deploy a function to Oracle Functions using the Fn Project CLI, the function is built as a Docker image and pushed to a specified Docker registry

Oracle Functions Concepts - Invocations

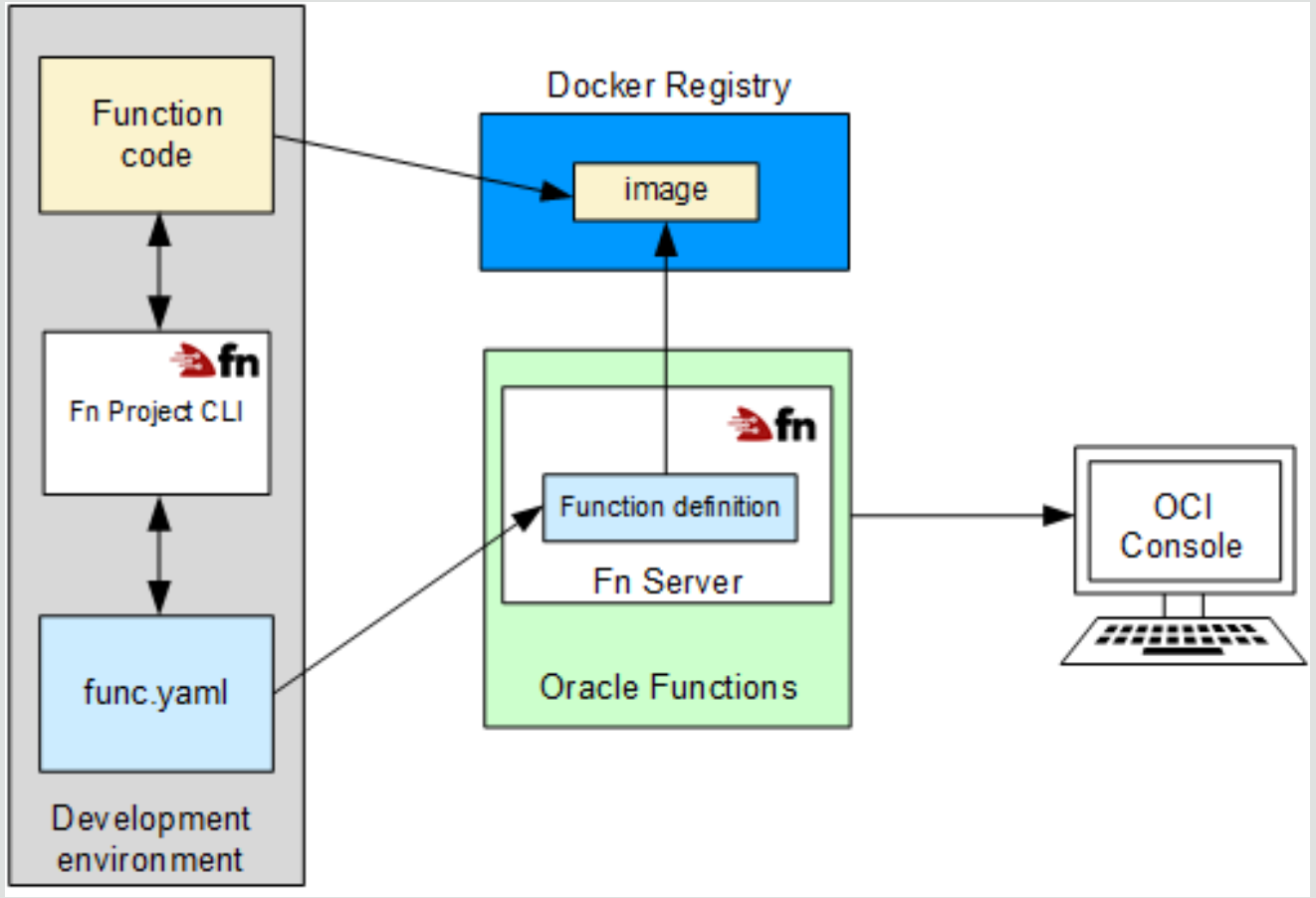
- In Oracle Functions, a function's code is run (or executed) when the function is called (or invoked). You can invoke a function that you've deployed to Oracle Functions from:
  - The Fn Project CLI.
  - The Oracle Cloud Infrastructure SDKs.
  - Signed HTTP requests to the function's invoke endpoint. Every function has an invoke endpoint.
  - Other Oracle Cloud services (for example, triggered by an event in the Events service) or from external services.
- When a function is invoked for the first time, Oracle Functions pulls the function's Docker image from the specified Docker registry, runs it as a Docker container, and executes the function.
- If there are subsequent requests to the same function, Oracle Functions directs those requests to the same container. After a period being idle, the Docker container is removed.

IAM Policies required to work with Oracle Functions

- Select the tenancy's root compartment, and create a new policy with the following two policy statements for the Oracle Functions service:
  - Allow service FaaS to read repos in tenancy
  - Allow service FaaS to use virtual-network-family in compartment <compartment-name>
- If one or more Oracle Functions users is not a tenancy administrator, add the following policy statements to the new policy:
  - Allow group <group-name> to manage repos in tenancy
  - Allow group <group-name> to use virtual-network-family in compartment <compartment-name>
  - Allow group <group-name> to manage functions-family in compartment <compartment-name>
  - Allow group <group-name> to read metrics in compartment <compartment-name>

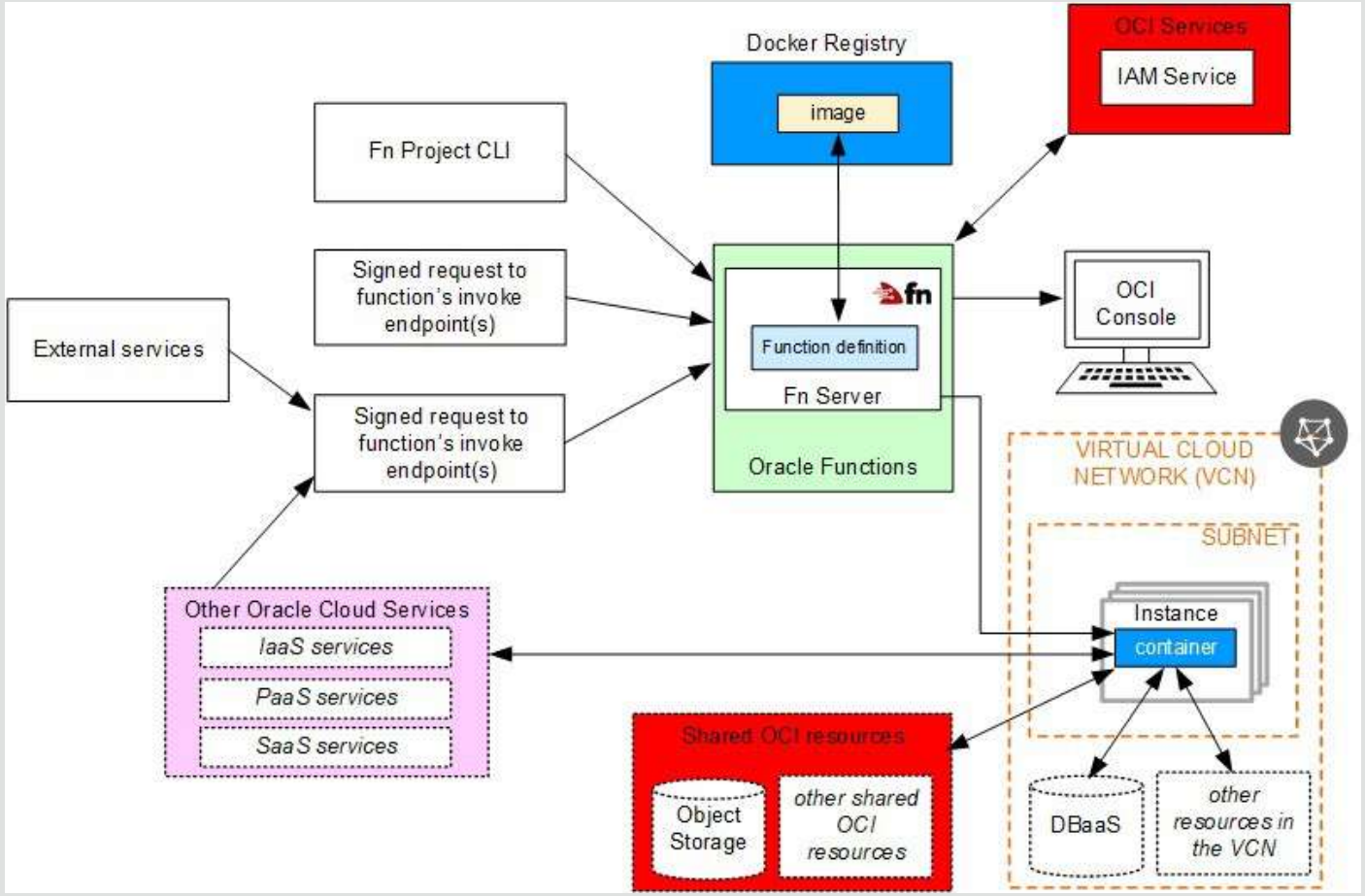
How Oracle Functions works?

Deploying a Function



How Oracle Functions works?

Invoking a Function



ORACLE Academy

Functions Metrics

- FunctionExecutionDuration: Total function execution duration in milliseconds
- FunctionInvocationCount: Total number of function invocations
- FunctionResponseCount: Total number of function responses
  - Errors: The number of times a function failed
  - Throttles: The number of requests to invoke a function that returned a '429 Too Many Requests' error in the response

Use Cases – "Run Code in Response to Events"

ORACLE Academy

References

References

Oracle Cloud Academy Foundations I Section 19

Cloud Engineering

CIDR Basics

SWINBURNE UNIVERSITY OF TECHNOLOGY

CIDR Basics

This presentation:

CIDR Basics

- Network and host addresses
- Subnet mask
- Classful subnetting
- Usable hosts

CIDR (Classless inter-domain routing)

CIDR Basics

CIDR

IPv4 IP address – 32 bits in length

We divide this address into four octets, each 8 bits long

Network address/portion

Host address/portion

10.10.10.3 / 16

CIDR Basics

CIDR

Each bit in an IP address can either be a 1 or a 0

Each bit in an octet has a corresponding decimal value.

- If the bit is set to 0, the decimal value is 0.
- If the bit is set to 1, the decimal value depends on its position in the octet

128 64 32 16 8 4 2 1 -> 2^7 2^6 2^5 2^4 2^3 2^2 2^1 2^0

1 1 0 0 0 0 0 0 -> 128 + 64 = 192

CIDR Basics

192.168.1.0/24 would equate to IP range:

192.168.1.0 – 192.168.1.255

- 128 64 32 16 8 4 2 1 → 2^7 2^6 2^5 2^4 2^3 2^2 2^1 2^0
- 192 is represented as: 1 1 0 0 0 0 0 0

192.168.1.0	1 1 0 0 0 0 0 0	1 0 1 0 1 0 0 0	0 0 0 0 0 0 0 1	0 0 0 0 0 0 0 0
/24 subnet mask	1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	0 0 0 0 0 0 0 0
Logical AND	1 1 0 0 0 0 0 0	1 0 1 0 1 0 0 0	0 0 0 0 0 0 0 1	0 0 0 0 0 0 0 0

ORACLE Academy

CIDR Basics

Classful subnet masks

Class A (8-bits)

Class B (16-Bits)

Class C (24-Bits)

CIDR Basics

Number of hosts

10.10.0.0 / 16

10.10.0.0 – 10.10.255.255

256^2 = 65536 (Class B)

Class A, 256^3 = 1,677,216

CIDR Basics

Problem with Classful subnetting

IPv4 addresses: 2 ^ 32 > 4 billion

Running out

Classful subnetting can be wasteful

CIDR Basics

- Subnets
  - 2 x 2 x 2 = 8. Hosts – 2 x 2 x 2 x 2 x 2 = 32
- Subnetworks
  - 192.168.1.0/27, 192.168.1.32/27, 192.168.1.64/27…

CIDR Basics

Network and Broadcast Address

192.168.1.0 / 24

192.168.1.0 - 192.168.1.255

192.168.1.0 – network address

192.168.1.255 – broadcast address

256 addresses

254 usable hosts

References

References

Oracle Cloud Academy Foundations I Section 2

Cloud Engineering

IP Addresses in Your VCN

SWINBURNE UNIVERSITY OF TECHNOLOGY

IP Addresses in Your VCN

This presentation:

- IPv4
- Public Addresses
- Private Addresses

IP addresses in your VCN

Before watching this Lecture

- CIDR Basics

IP addresesss in Your VCN

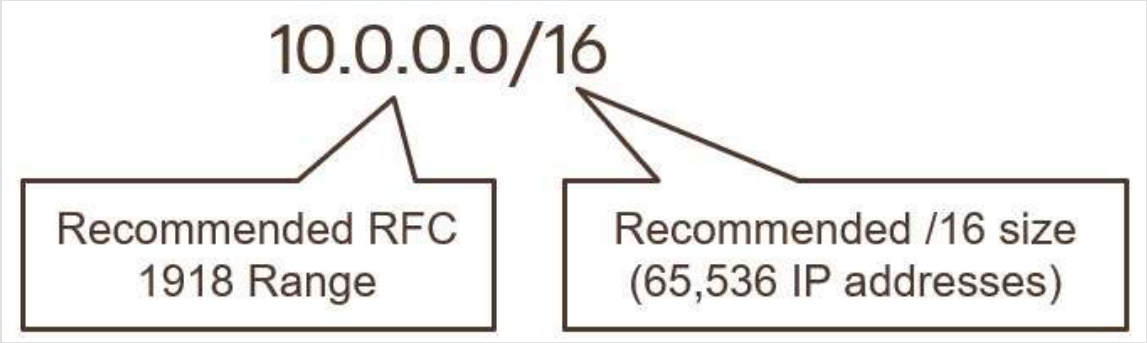
IPv4 and IPv6

Both IPv4 and IPv6 are available

We will cover IPv4

IP Address Range For Your VCN

- Avoid IP ranges that overlap with other on-premises or other cloud networks



- Use private IP address ranges specified in RFC 1918 (10.0.0.0/8, 172.16/12, 192.168/16)
- Allowable OCI VCN size range is from /16 to /30
- VCN reserves the first two IP addresses and the last one in each subnet's CIDR

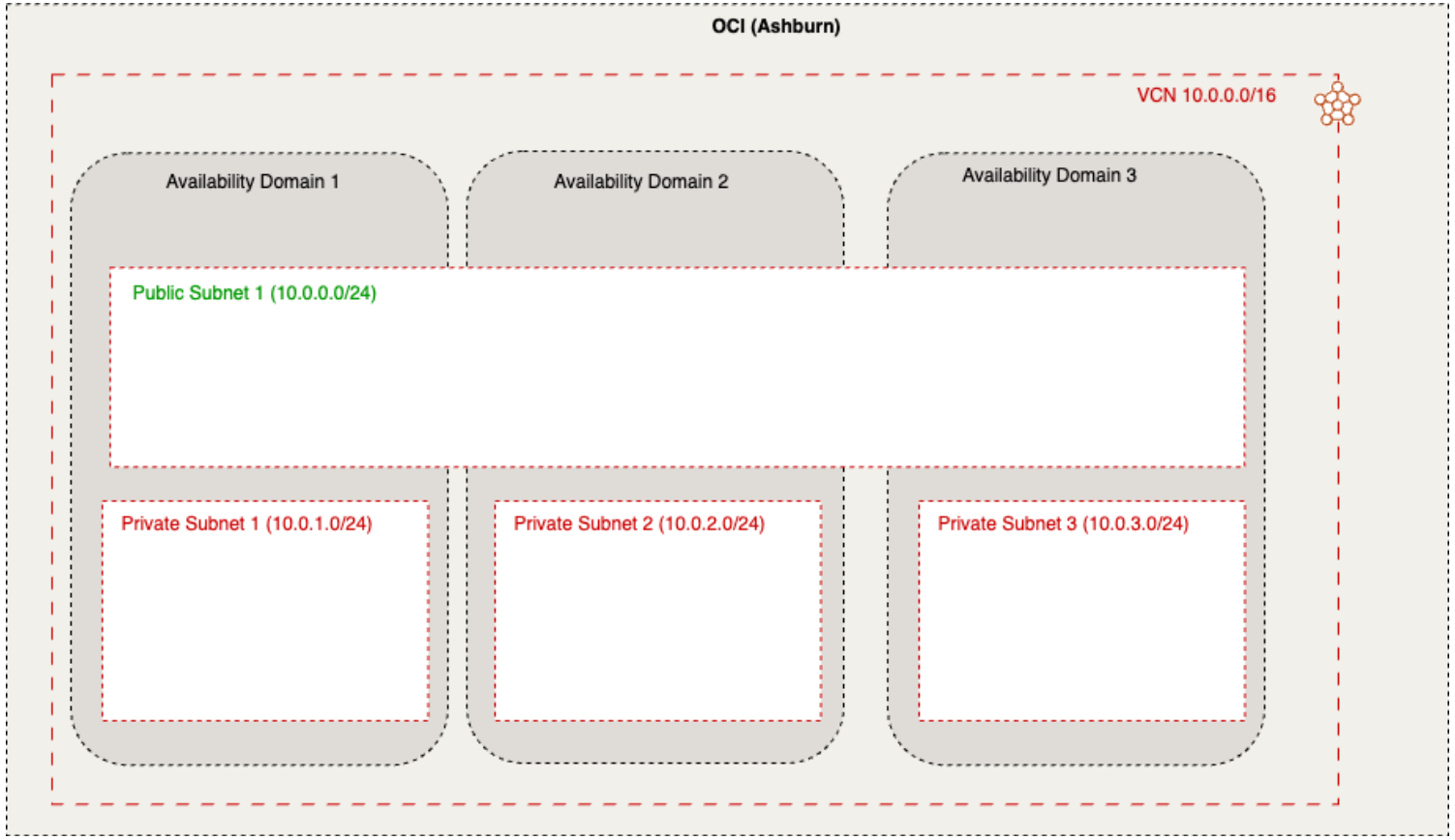
ORACLE Academy

IP addresses in your VCN

VCN Diagram

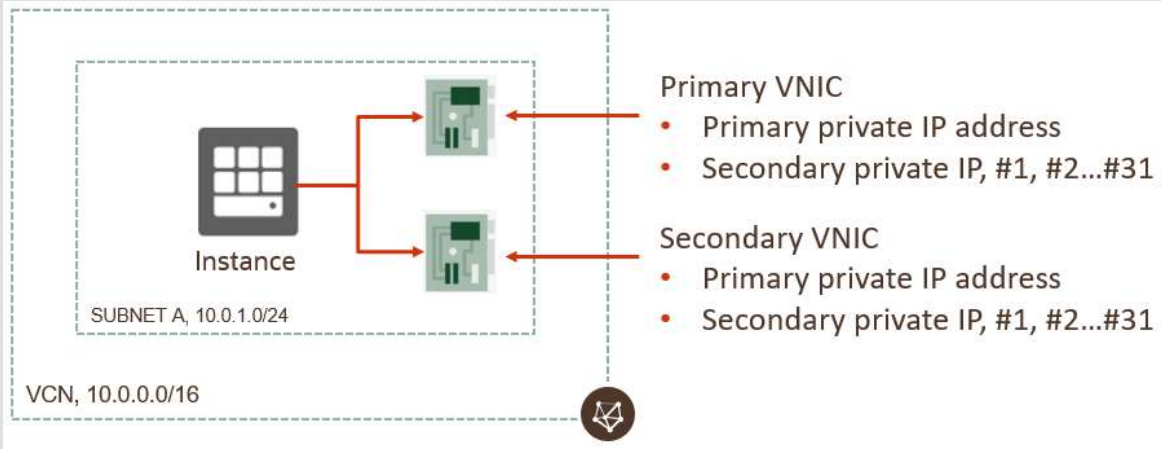
IP addresses in your VCN

VCN Diagram



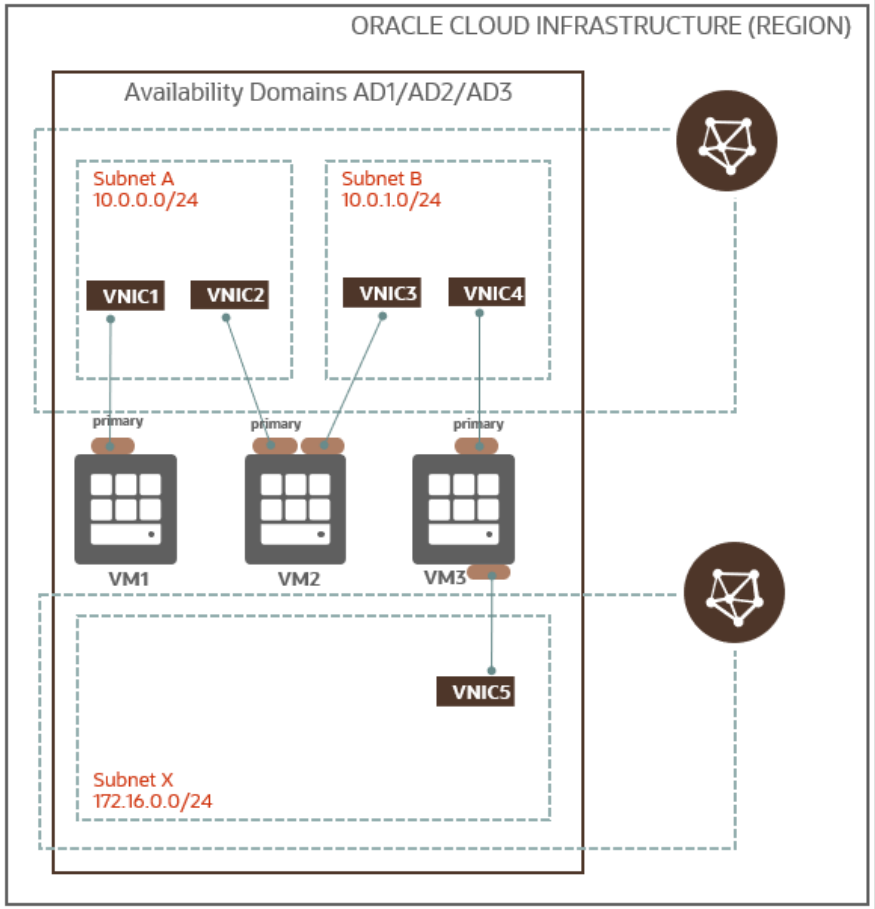
Private IP Addresses

- Each instance in a subnet has at least one primary private IP address
- Instances ≥ 2 VNICs (additional VNICs called secondary VNICs)
- Each VNIC has one primary private IP; can have additional private IPs called secondary private IPs
- A private IP can have an optional public IP assigned to it



ORACLE Academy

Multiple VNICs On Virtual Machines

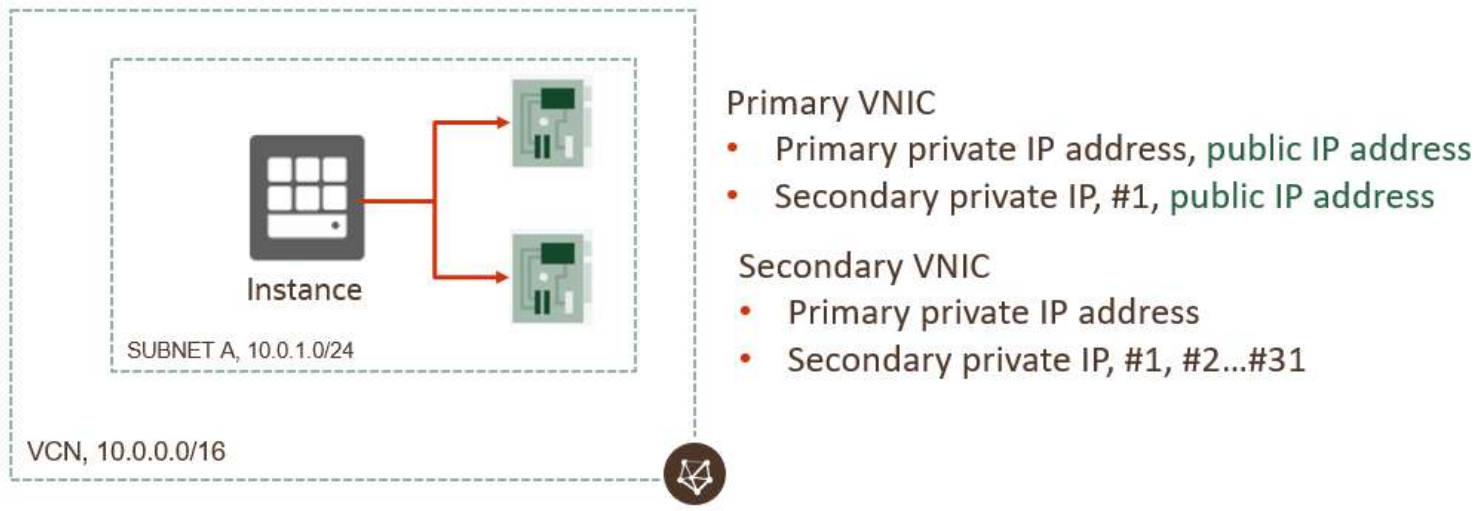


- Every VM has one primary VNIC created at launch, and a corresponding Ethernet device on the instance with the IP address configuration of the primary VNIC
- When a secondary VNIC is added, new Ethernet device is added and is recognized by the instance OS
  - VM1 - single VNIC instance
  - VM2 - connected to two VNICs from two subnets within the same VCN. Used for virtual appliance scenarios
  - VM3 - connected to two VNICs from two subnets from separate VCNs. Used to connect instances to a separate management network for isolated access

ORACLE Academy

Public IP

- Public IP address is an IPv4 address that is reachable from the internet; assigned to a private IP object on the resource (Instance, load balancer)
- Possible to assign a given resource multiple public IPs across one or more VNICs



Public IP Addresses

- Public IP types: Ephemeral and Reserved
  - Ephemeral: temporary and existing for the lifetime of the instance
  - Reserved: Persistent and existing beyond the lifetime of the instance it's assigned to (can be unassigned and then reassigned to another instance)
  - Ephemeral IP can be assigned to primary private IP only (hence, only 1 per VNIC v/s a max 32 for Reserved IP)
- No charge for using Public IP, including when the Reserved public IP addresses are unassociated

Public IP Addresses

- Public IP assigned to
  - Instance (not recommended in most cases)
  - Oracle provided; cannot choose/edit, but can view
    - OCI Public Load Balancer, NAT Gateway, DRG - IPSec tunnels, OKE master/worker
  - Oracle provided; cannot choose/edit/view
    - Internet Gateway, Autonomous Database

References

References

Oracle Cloud Academy Foundations I Section 2

Networking in The Cloud EP.01 Virtual Cloud Networks: https://youtu.be/mIYSgeX5FkM

Oracle Cloud Infrastructure Networking: Overview: https://www.youtube.com/watch?v=DIjGGhidUrI

draw.io starter template for OCI: https://maximilian.tech/2020/11/27/draw-io-starter-template-for-oci-oracle-cloud-infrastructure/

Cloud Engineering

Routing and Gateways

SWINBURNE UNIVERSITY OF TECHNOLOGY

Routing and Gateways

This presentation:

- Gateways
  - Internet Gateway
  - NAT Gateway
  - Service Gateway
  - DRG
- Routing
  - Routes and Route Tables

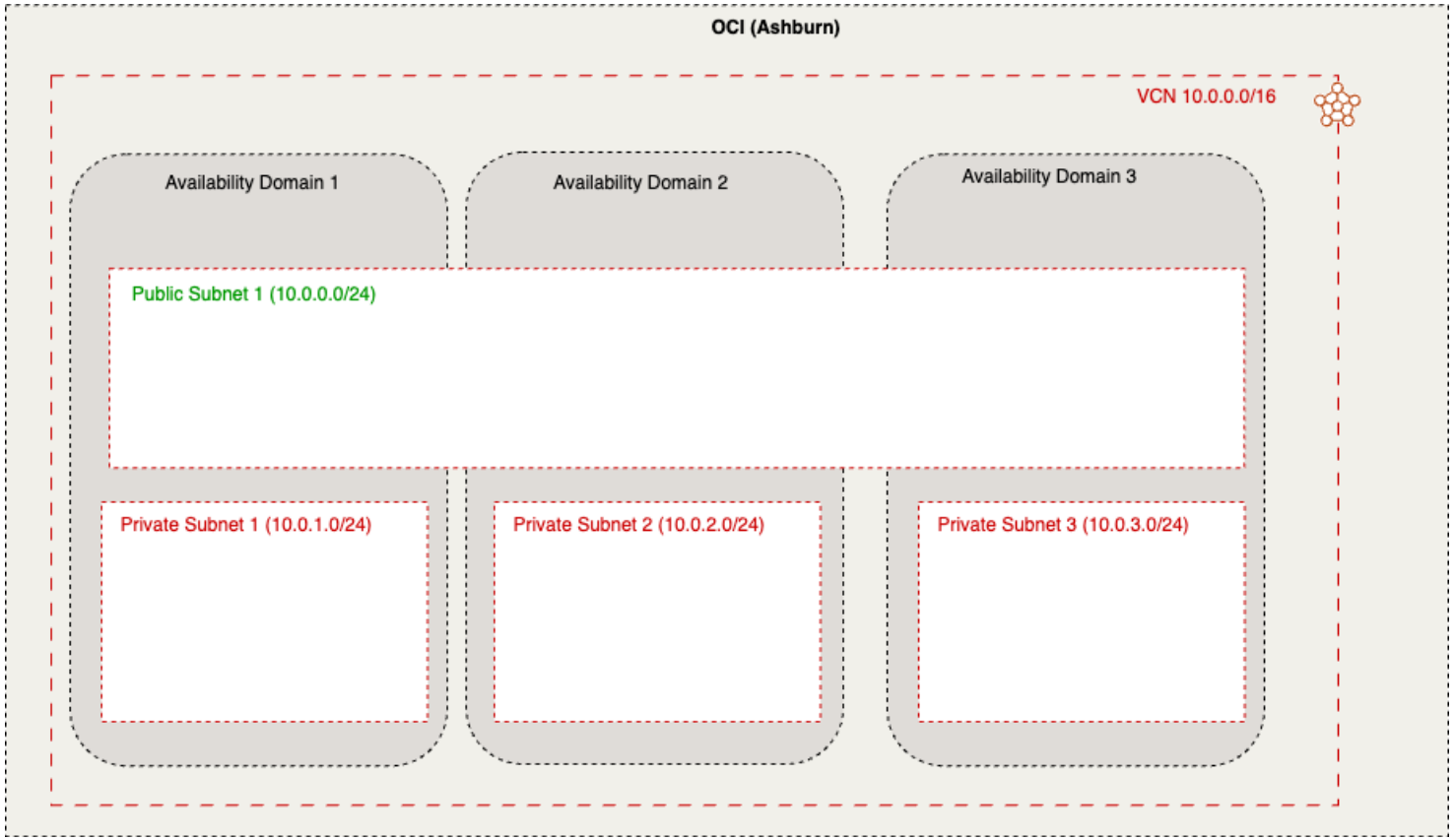
Routing and Gateways

Gateways

When do we need to use them?

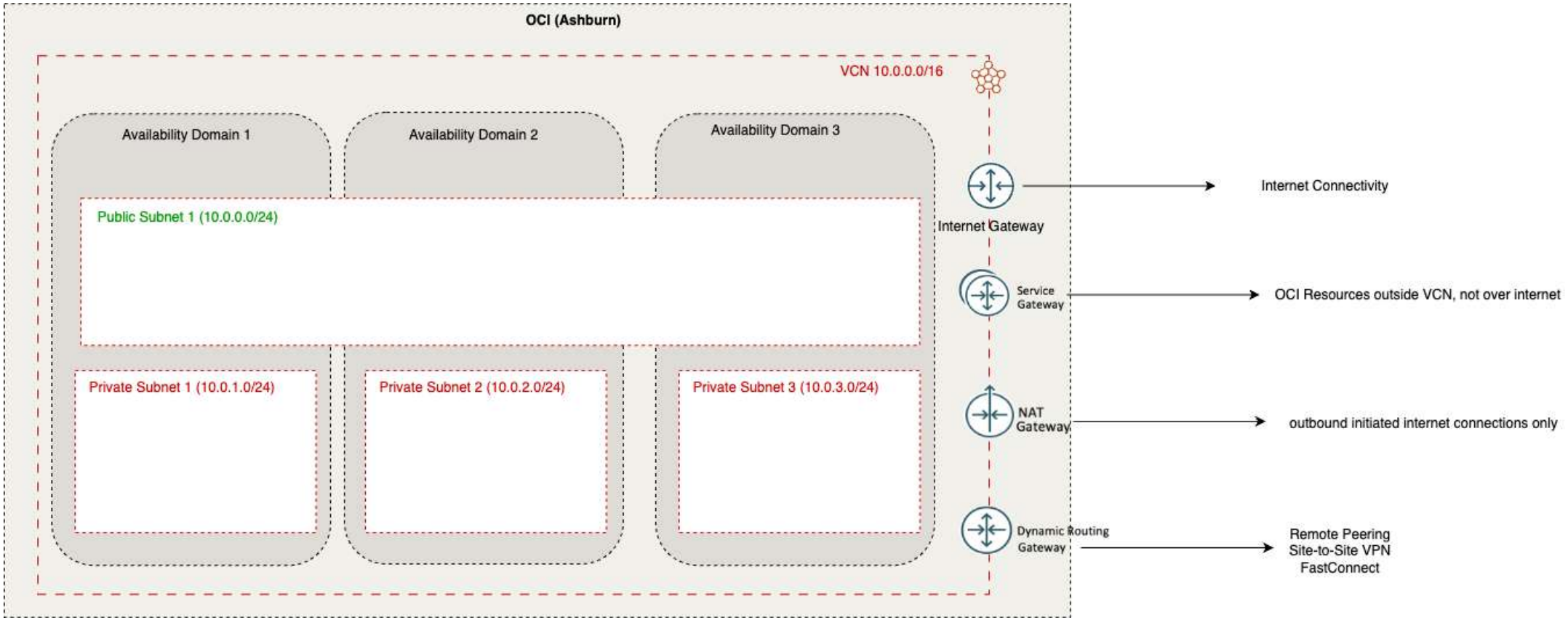
Routing and Gateways

VCN Diagram

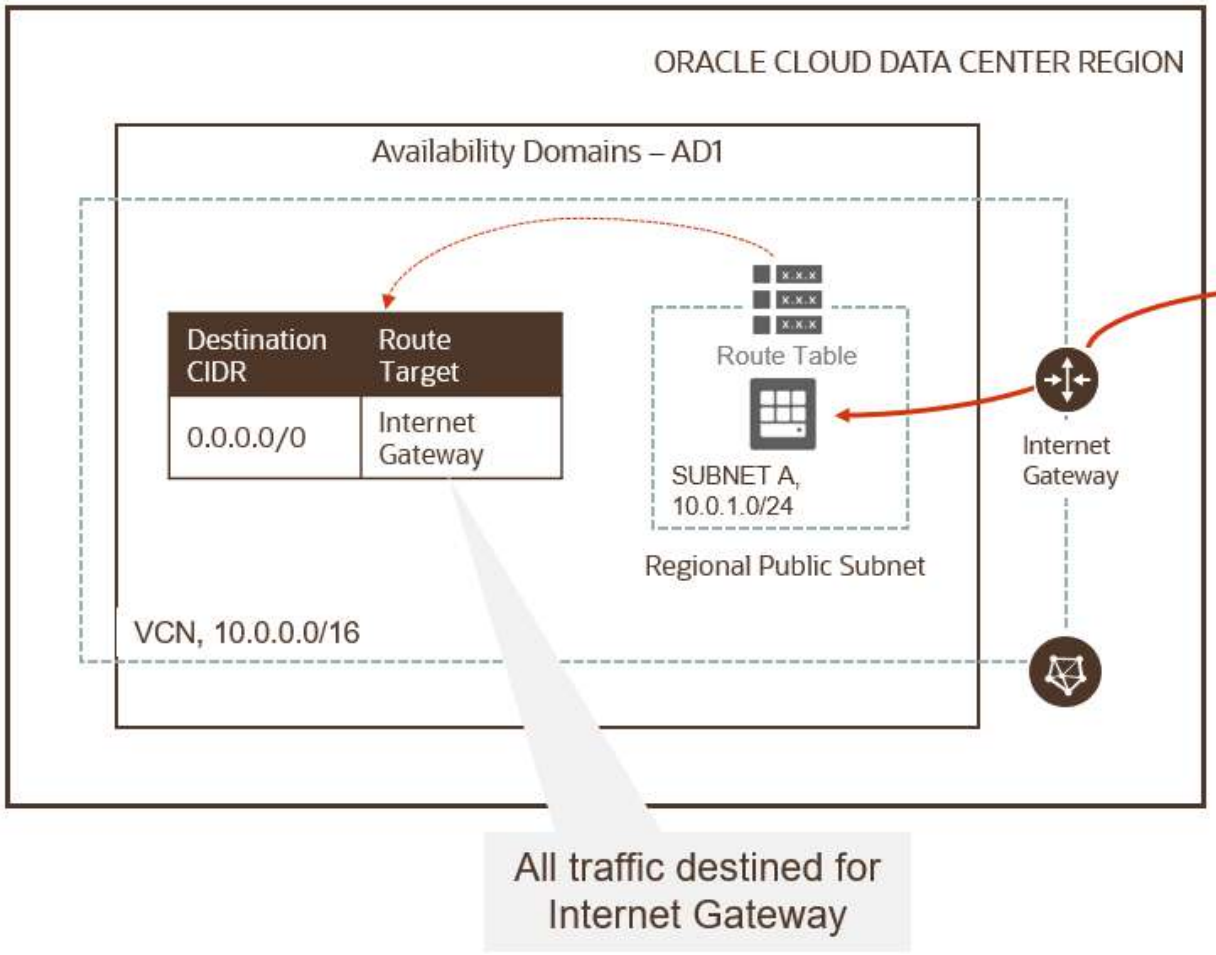


Routing and Gateways

VCN Diagram

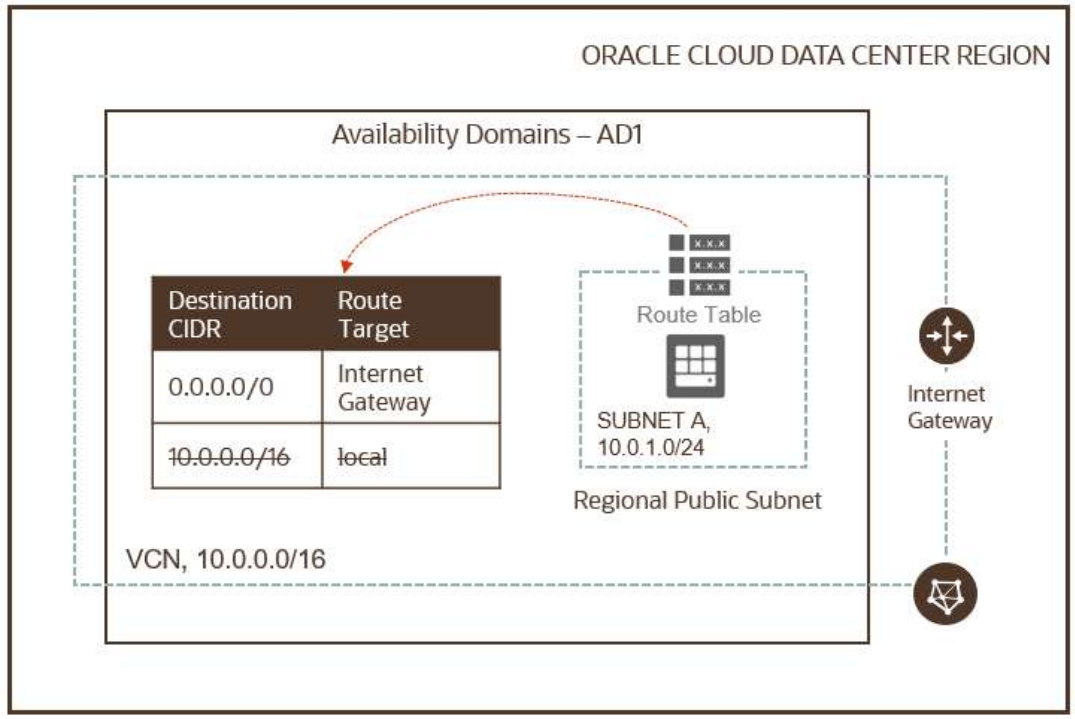


Route Table



- Route Table is used to send traffic out of the VCN
- Consists of a set of route rules; each rule specifies
  - Destination CIDR block
  - Route Target (the next hop) for the traffic that matches that CIDR

Route Table



- Each subnet uses a single route table specified at time of subnet creation, but can be edited later
- Route table is used only if the destination IP address is not within the VCN's CIDR block
- No route rules are required in order to enable traffic within the VCN itself
- When you add an internet gateway, NAT gateway, service gateway, dynamic routing gateway or a peering connection, you must update the route table for any subnet that uses these gateways or connections

ORACLE Academy

References

References

Oracle Cloud Academy Foundations I Section 2

Networking In The Cloud EP.02 VCN Gateways: https://www.youtube.com/watch?v=as2jUtvximY

Networking in the Cloud EP.03 Routing Traffic: https://www.youtube.com/watch?v=BHapvirrS5g

Oracle Cloud Infrastructure Networking: Overview: https://www.youtube.com/watch?v=DIjGGhidUrI

draw.io starter template for OCI: https://maximilian.tech/2020/11/27/draw-io-starter-template-for-oci-oracle-cloud-infrastructure/

Cloud Engineering

Securing Traffic

SWINBURNE UNIVERSITY OF TECHNOLOGY

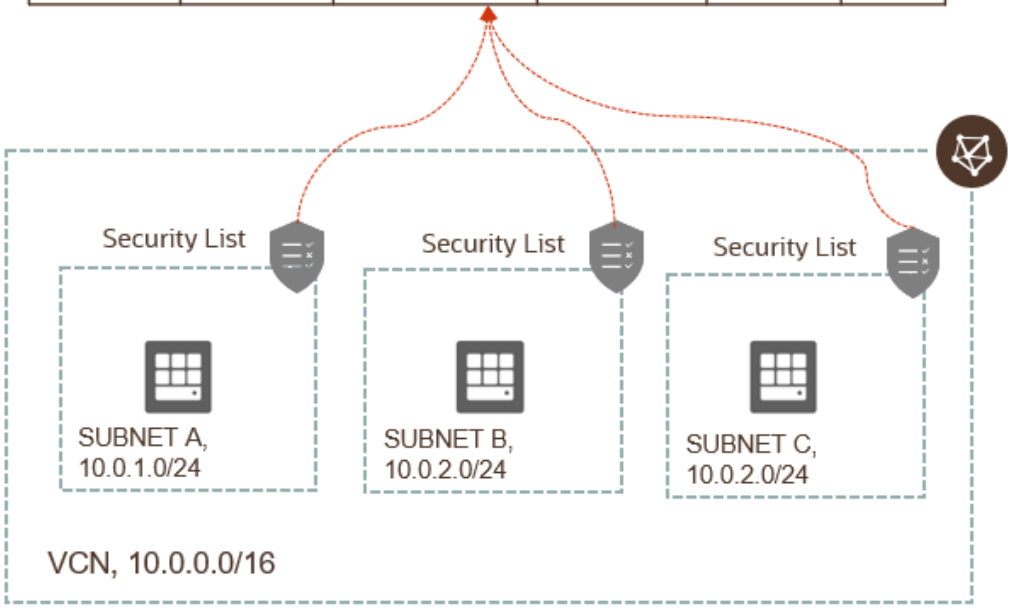
Securing Traffic

This presentation:

- Security List (SL)
- Network Security Group (NSG)
- Stateful Security Rules
- Stateless Security Rules

Security List (SL)

	Direction	CIDR	Protocol	Source Port	Dest Port
Stateful	Ingress	0.0.0.0/0	TCP	All	80
Stateful	Egress	10.0.2.0/24	TCP	All	1521



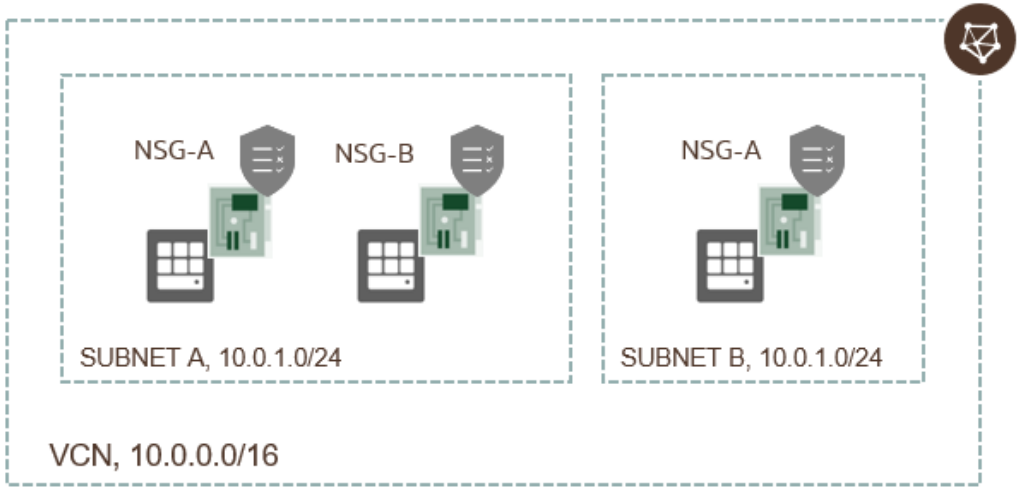
A common set of firewall rules associated with a subnet and applied to all instances launched inside the subnet

- Security list consists of rules that specify the types of traffic allowed in and out of the subnet
- To use a given security list with a particular subnet, you associate the security list with the subnet either during subnet creation or later.
- Security list apply to a given instance whether it's talking with another instance in the VCN or a host outside the VCN
- You can choose whether a given rule is stateful or stateless

ORACLE Academy

Network Security Group (NSG)

		Direction	CIDR	Protocol	Source Port	Dest Port
NSG-A	Stateful	Ingress	0.0.0.0/0	TCP	All	80
NSG-B	Stateful	Ingress	0.0.0.0/0	TCP	All	22

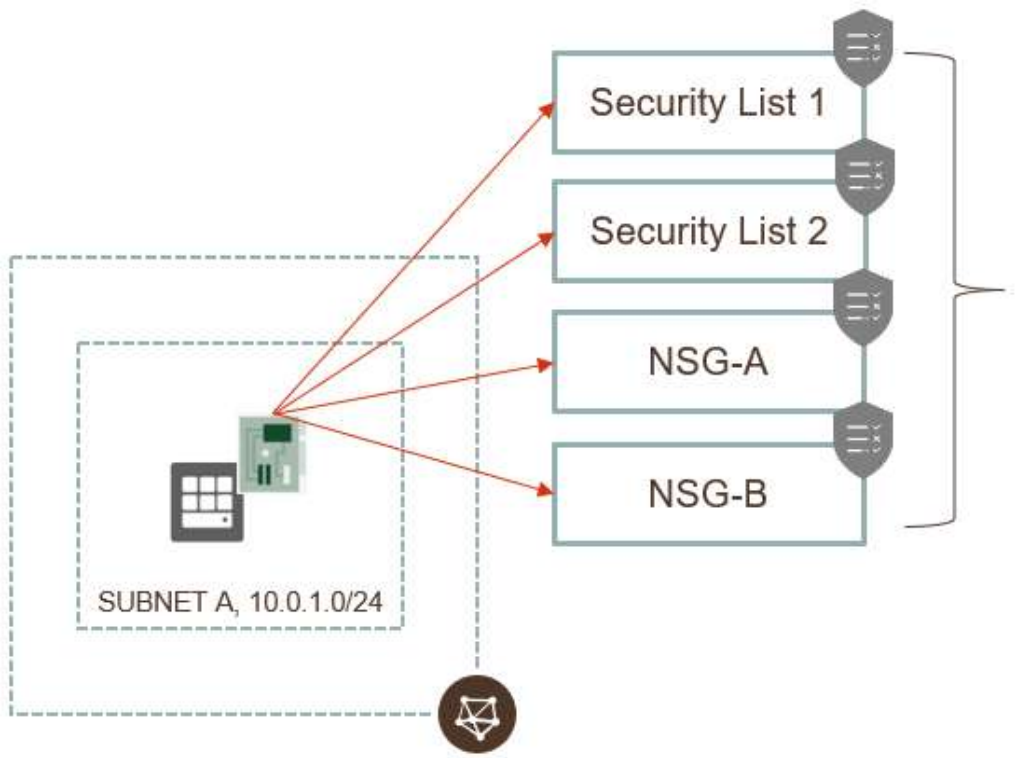


A network security group (NSG) provides a virtual firewall for a set of cloud resources that all have the same security posture

- NSG consists of set of rules that apply only to a set of VNICs of your choice in a single VCN
- Currently, compute instances, load balancers and DB instances support NSG
- When writing rules for an NSG, you can specify an NSG as the source or destination. Contrast this with SL rules, where you specify a CIDR as the source or destination
- Oracle recommends using NSGs instead of SLs because NSGs let you separate the VCN's subnet architecture from your application security requirements

ORACLE Academy

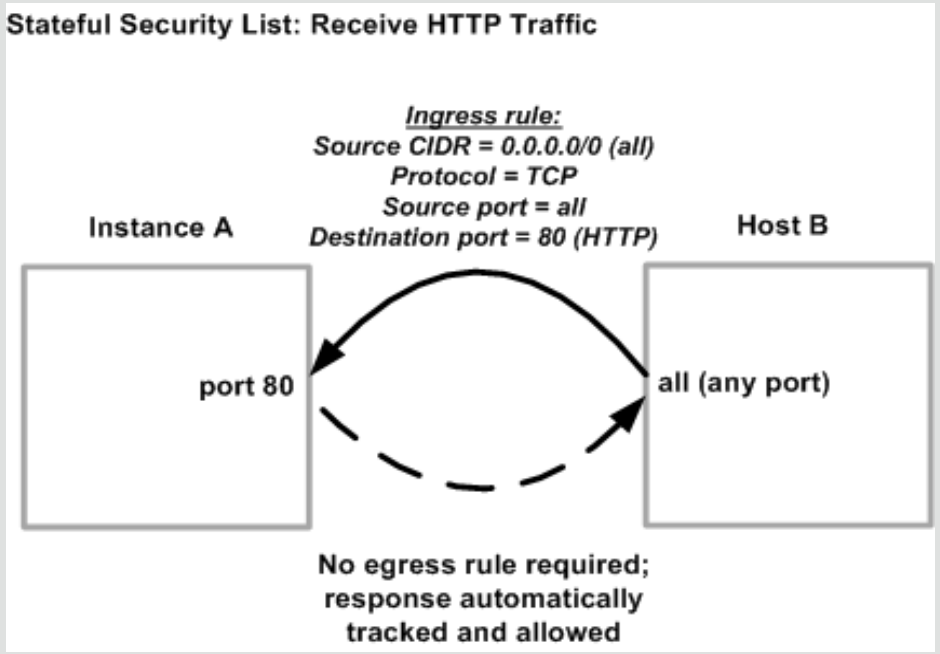
SL + NSG



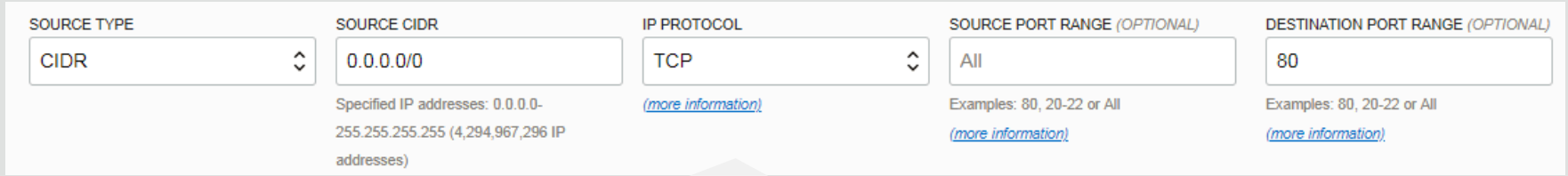
- You can use security lists alone, network security groups alone, or both together
- If you have security rules that you want to enforce for all VNICs in a VCN: the easiest solution is to put the rules in one security list, and then associate that security list with all subnets in the VCN
- If you choose to use both SLs and NSGs, the set of rules that applies to a given VNIC is the union of these items:
  - The security rules in the SLs associated with the VNIC's subnet
  - The security rules in all NSGs that the VNIC is in
  - A packet in question is allowed if any rule in any of the relevant lists and groups allows the traffic

ORACLE Academy

Stateful Security Rules



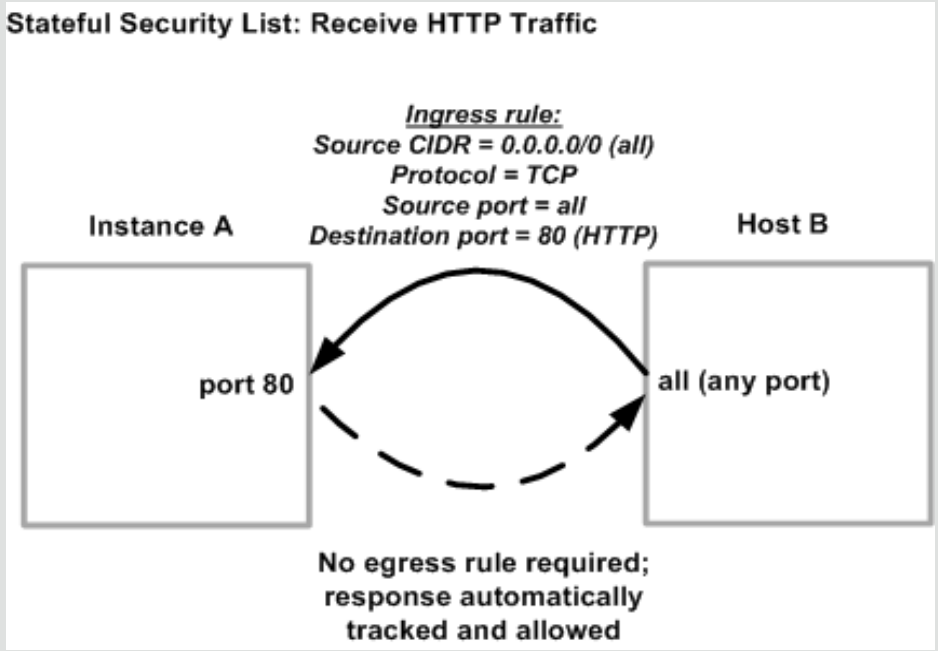
- Connection Tracking: when an instance receives traffic matching the stateful ingress rule, the response is tracked and automatically allowed regardless of any egress rules; similarly for sending traffic from the host
- Default Security List rules are stateful



Hosts in this group are reachable from the internet on Port 80

ORACLE Academy

Stateless Security Rules



- With stateless rules, response traffic is not automatically allowed
- To allow the response traffic for a stateless ingress rule, you must create a corresponding stateless egress rule
- If you add a stateless rule to a security list, that indicates that you do NOT want to use connection tracking for any traffic that matches that rule
- Stateless rules are better for scenarios with large numbers of connections (Load Balancing, Big Data)

ORACLE Academy

Securing Traffic

Final thoughts

May seem a bit abstract

Labs & Assignments

References

References

Oracle Cloud Academy Foundations I Section 2

Networking in the Cloud EP.04 Securing Traffic: https://www.youtube.com/watch?v=rTcT3lK69Ng

Cloud Engineering

VPN & FastConnect

SWINBURNE UNIVERSITY OF TECHNOLOGY

VPN & FastConnect

This presentation:

VPN

FastConnect

VPN & FastConnect

Recap

Public Cloud

Private Cloud

Hybrid Cloud

Multi Cloud

VPN & FastConnect

Advanced Networking Concepts

Cloud	VPN	FastConnect
Public Cloud	Yes*	Yes*+
Private Cloud	Yes	No
Hybrid Cloud	Yes**	Yes**+
Multi Cloud	Yes**	Yes**+

* Optional

+ When using Oracle

** Must use at least one of these

VPN & Fast Connect are key services that make Multi Cloud with OCI possible

VPN & FastConnect

Local Area Network (LAN)

Network at local site

VPN & FastConnect

Internet

Inherently not secure

Most LANs not fully isolated from internet

Cybersecurity threats

VPN & FastConnect

Virtual Private Network

Connect to remote site as if it were on same LAN

VPN & FastConnect

Internet Protocol Security (IPsec)

Authenticate and Secure VPN Connection

VPN & FastConnect

Traditional VPN

Client-Site

Site-Site

VPN & FastConnect

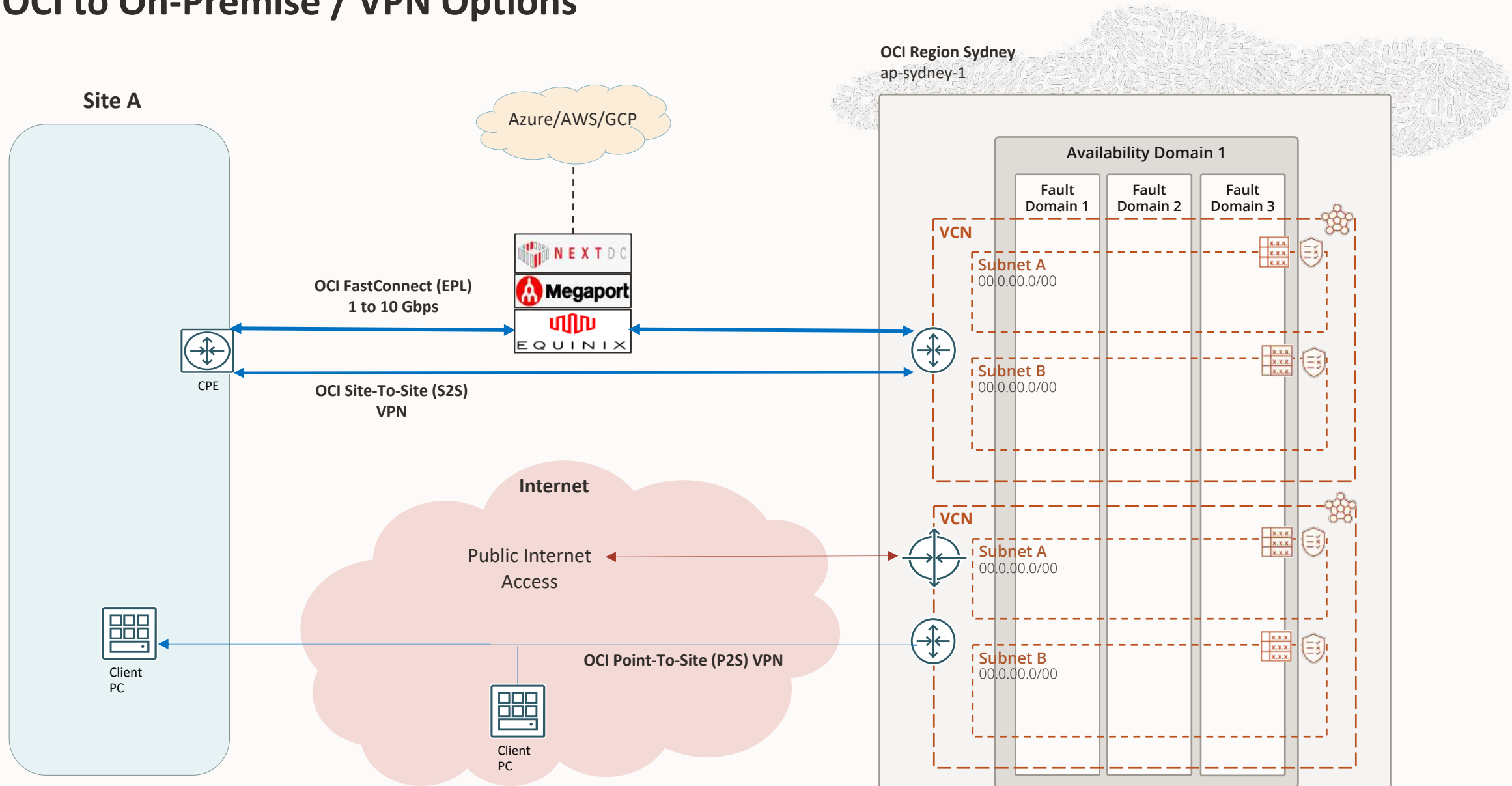
VPN with the Cloud

Client to Cloud (uses Client-Site)

Hybrid Cloud (uses Site-Site)

Multi Cloud (uses Site-Site)

OCI to On-Premise / VPN Options



Connectivity options

Public Internet

- Internet Gateway/ NAT Gateway
- Reserved and Ephemeral IPs
- Internet Data out Pricing (first 10TB free)

VPN

- IPsec authentication and encryption
- Two main options
  - OCI managed VPN Service (free)
  - Software VPN (running on OCI Compute)

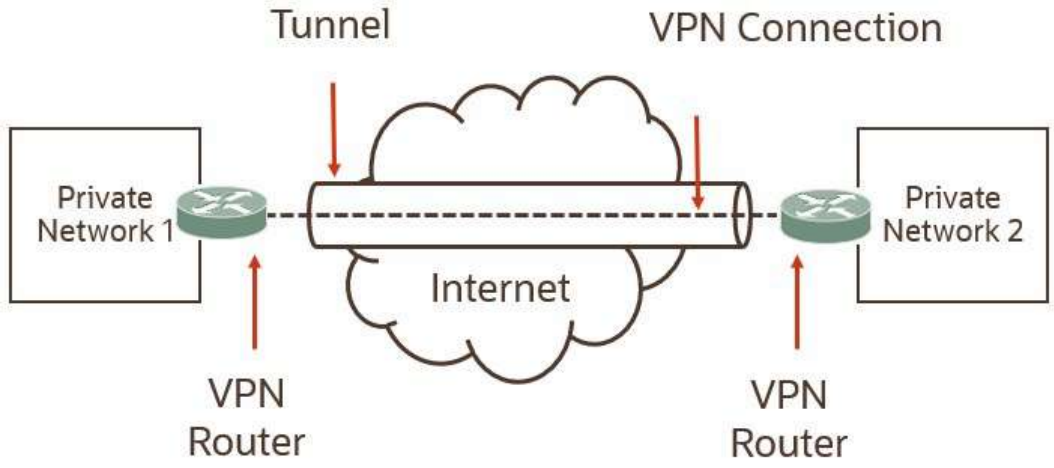
FastConnect

- Private Connection
- Separate from the internet
- Consistent network experience
- Port speeds of 1 Gbps and10 Gbps
- SLA

ORACLE Academy

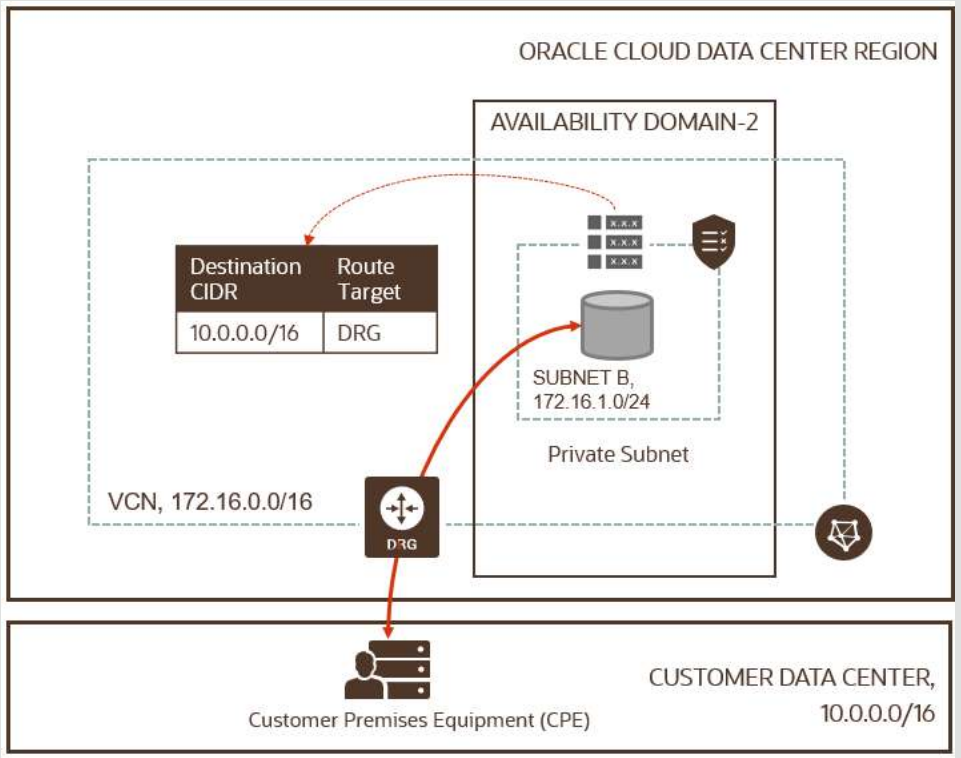
VPN Basics

VPN – using a public network to make end to end connection between two private networks in a secure fashion



- **Tunnel** – a way to deliver packets through the internet to private RFC 1918 addresses
- **Authentication** – provides a mechanism to authenticate who you are
- **Encryption** – packets need to be encrypted, so they cannot be sniffed over the public internet
- **Static routing** – configure a router to send traffic for particular destinations in preconfigured directions
- **Dynamic routing** – use a routing protocol such as BGP to figure out what paths traffic should take

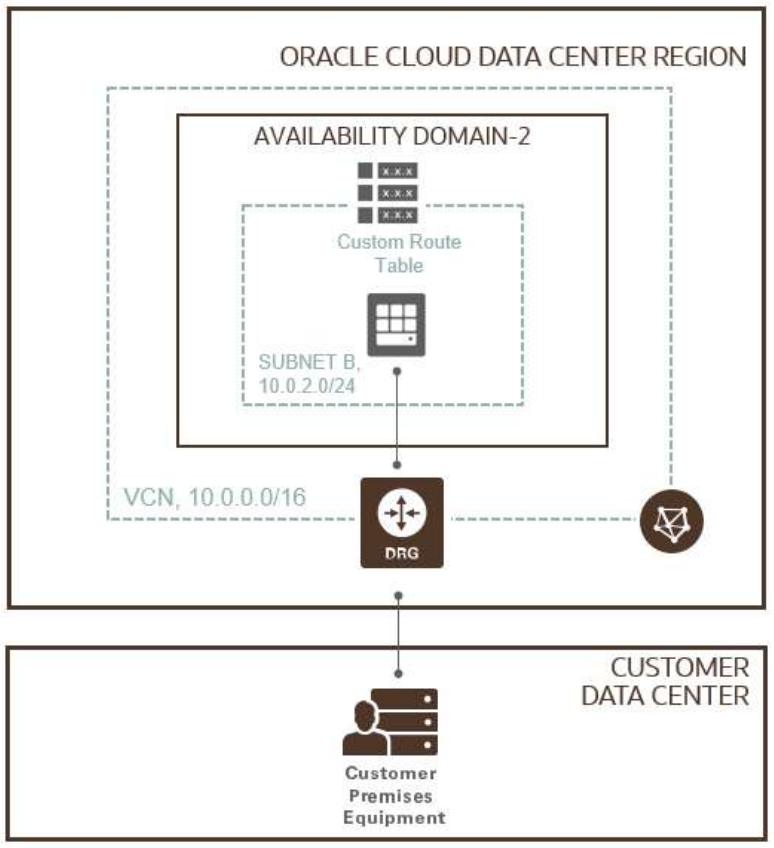
Dynamic Routing Gateway



- A virtual router that provides a path for private traffic between your VCN and destinations other than the internet
- You can use it to establish a connection with your on-premises network via IPsec VPN or FastConnect (private, dedicated connectivity)
- After attaching a DRG, you must add a route for the DRG in the VCN's route table to enable traffic flow
- DRG is a standalone object. You must attach it to a VCN. VCN and DRG have a 1:1 relationship

ORACLE Academy

VPN Connect (IPSec)



- VPN Connect is a managed VPN service which securely connects on-premises network to OCI VCN through an **IPSec VPN connection**
- VPN Connect ensures secure remote connectivity via industry standard IPSec encryption
- Bandwidth is dependent on the customer's access to the Internet and general Internet congestion (Typically less than 250 Mbps – but your mileage may vary)
- **VPN Connect is offered for free**
- Customer Proof of Concepts usually start as a VPN and then morph into FastConnect designs
- OCI provisions redundant VPN tunnels located on physically and logically isolate tunnel endpoints

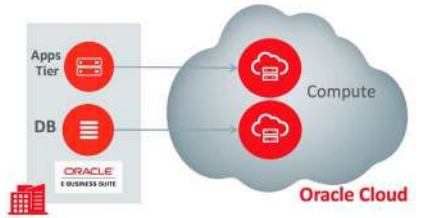
ORACLE Academy

FastConnect

FastConnect provides a dedicated and private connection with higher bandwidth options, and a more reliable and consistent networking experience when compared to internet-based connections

- Connect to OCI directly or via pre-integrated Network Partners
- Port speeds of 1 Gbps and 10 Gbps increments
- Extend remote datacenters into Oracle (“**Private peering**”) or connect to Public resources **(“Public peering”)**
- No charges for inbound/outbound data transfer
- Uses BGP protocol

Why Do You Need Dedicated Connectivity into Cloud?

ORACLE Applications, ORACLE E-Business Suite, ORACLE JD Edwards, ORACLE PeopleSoft, ORACLE Siebel, ORACLE Hyperion	HPC, hadoop, Altair, slurm, Apache Spark		
Latency sensitive enterprise applications	Big Data & High Performance Computing with data-transfer needs	Sensitive data that cannot traverse the public internet	Lift-and-shift to Cloud
Applications with relational database especially vulnerable to latency and require predictable performance including backup, replication use cases	Large data transfer (for example batch jobs or real-time queries) require high performance and low latency	Applications that contain sensitive data benefit from an extra level of privacy and isolation	Moving Web-App-DB tiers to Oracle Cloud needs dedicated network connectivity

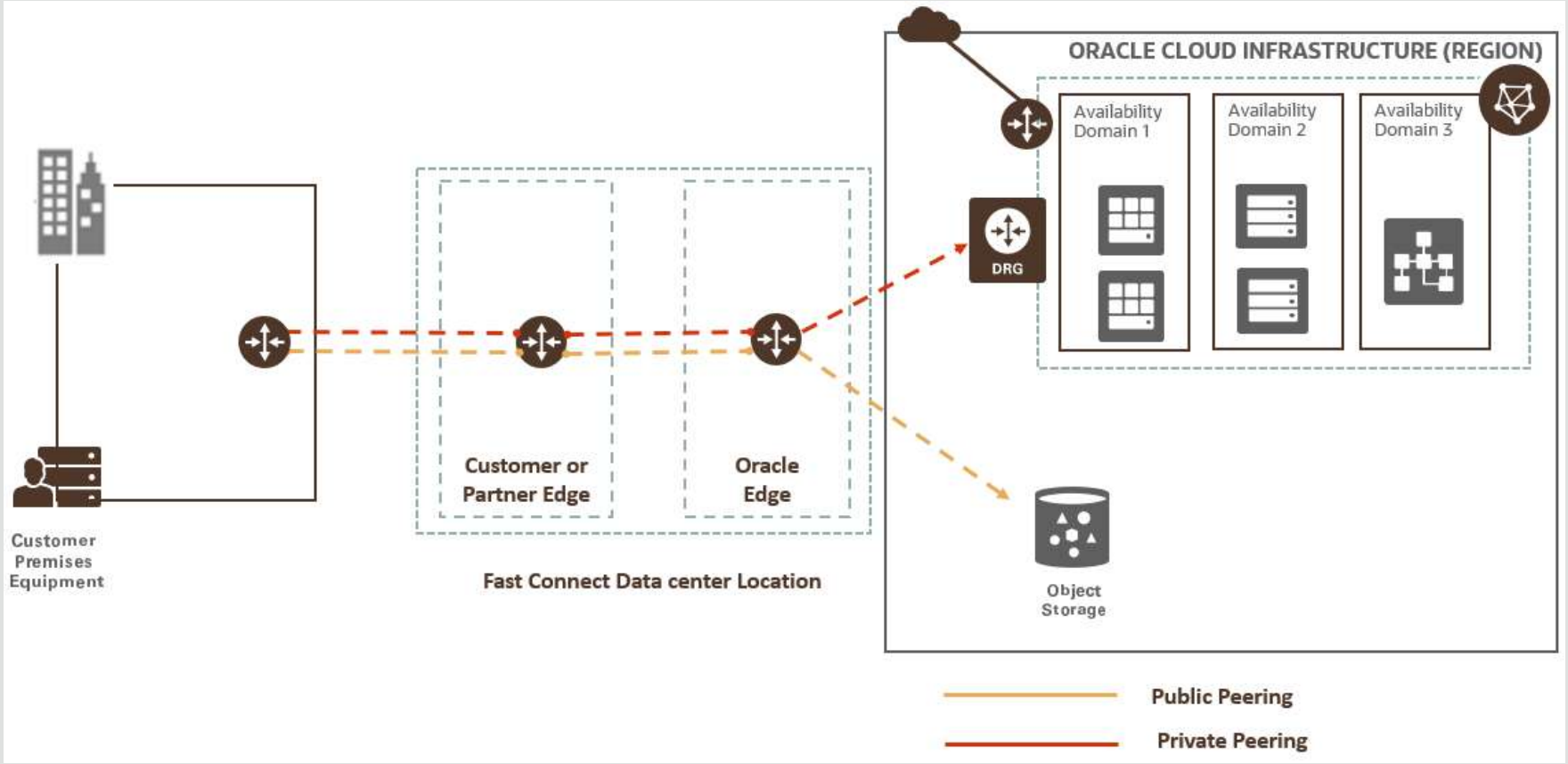
Virtual Circuit

- Virtual circuit - isolated network path that runs over one or more physical network connections to provide a single, logical connection between customer's edge router and their DRG
- Each virtual circuit is made up of information shared between the customer, Oracle, and a provider
- Possible to have multiple virtual circuits to isolate traffic from different parts of organization (e.g. one virtual circuit for 10.0.1.0/24; another for 172.16.0.0/16), or to provide redundancy
- FastConnect uses BGP to exchange routing information

FastConnect Use Scenarios

- Private Peering
  - Extension of the on premise network to the OCI VCN
  - Communication across connection with private IP addresses
- Public Peering
  - To access public OCI services such as Object storage, OCI Console or APIs over dedicated FastConnect connection
  - Doesn't use DRG

FastConnect Use Cases



IPsec VPN and FastConnect

	IPsec VPN	FastConnect
Use case	Dev/test and small scale production workloads	Enterprise-class and mission critical workloads, Oracle Apps, Backup, DR
Supported Services	All OCI Services within VCN	All OCI Services within VCN
Typical bandwidth	Typically < 250 Mbps aggregate	Higher bandwidth; increments of 1 Gbps, and 10 Gbps ports
Protocols	IPsec	BGP
Routing	Static Routing, Dynamic Routing	Dynamic Routing
Connection Resiliency	active-active	active-active
Encryption	Yes, by default	No * (can be achieved using virtual firewall)
Pricing	Free for the managed service	• Billable port hours • No data transfer charge between ADs
SLA	No SLA	99.9% Availability SLA

ORACLE Academy

Online Transport

It's important to consider bandwidth and security when transporting data over the wire. Data should always be encrypted at rest and in transit:

- **VPN over Internet**: Relatively small datasets—up to approximately 2 terabytes (TBs)—can typically be transported over the public internet without problems
- **FastConnect**: It's the right choice for organizations that need to transport large datasets
- **Storage Gateway**: Once a secure connection has been established, organizations can use the Oracle Cloud Infrastructure Storage Gateway to securely create copies of on-premises files and place them into Oracle object storage without the need to modify applications

References

References

Oracle Cloud Academy Foundations I Section 3

Oracle Cloud Academy Foundations I Section 9

Oracle Cloud Academy Foundations II Section 2

Oracle Cloud Academy Foundations II Section 3