NCOAUG

NORTH CENTRAL ORACLE APPS USER GROUP

TRAINING DAY

AUGUST 1, 2019

# OCI Identity and Access Management & Virtual Cloud Network

Best Practices, presented by:

Amrita Mukherjee

Syntax

# Content Overview

- IAM Resources
  - Tenancy name and administrator
  - Compartments
  - Users, Groups, and Policies
- VCN Resources
  - Regions and Availability Domains
  - Subnets and Subnet Access
  - Route Tables and Security Lists
  - DHCP Options
  - Dynamic Routing Gateways and Customer Premises Equipment
  - Load Balancers
  - Internet Gateway, NAT Gateway, and Service Gateways
- Requirements Template
- Demo

# Identity & Access Management

Overview & Resources

NCOAUG
NORTH CENTRAL ORACLE APPS USER GROUP
TRAINING DAY
AUGUST 1, 2019

# IAM Overview

Control who has access to your cloud resources

Control what type of access

Control access to specific resources

**Components of IAM**

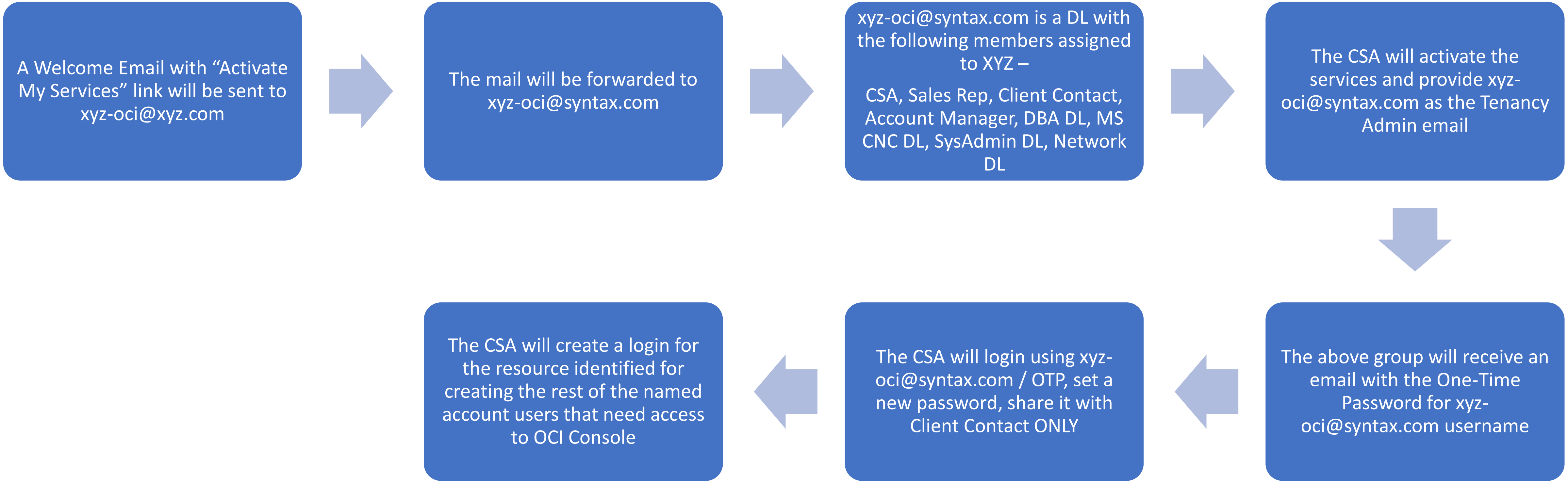
- Resource
- Home Region
- Federation
- User
- Group, Dynamic Group
- Compartment, Tenancy
- Policy

# IAM – Tenancy Name and Administrator

- OCI Provisioning and Activation
- Tenancy Name
- Default Administrator
- Tenancy Administrator E-mail
  - E.g. *xyz-oci@xyz.com*
- Administrators Group
- Tenancy Administrators Policy

Allow group Administrators to manage all-resources in tenancy

# IAM – OCI Provisioning & Activation



A Welcome Email with “Activate My Services” link will be sent to xyz-oci@xyz.com

The mail will be forwarded to xyz-oci@syntax.com

xyz-oci@syntax.com is a DL with the following members assigned to XYZ –

CSA, Sales Rep, Client Contact, Account Manager, DBA DL, MS CNC DL, SysAdmin DL, Network DL

The CSA will activate the services and provide xyz-oci@syntax.com as the Tenancy Admin email

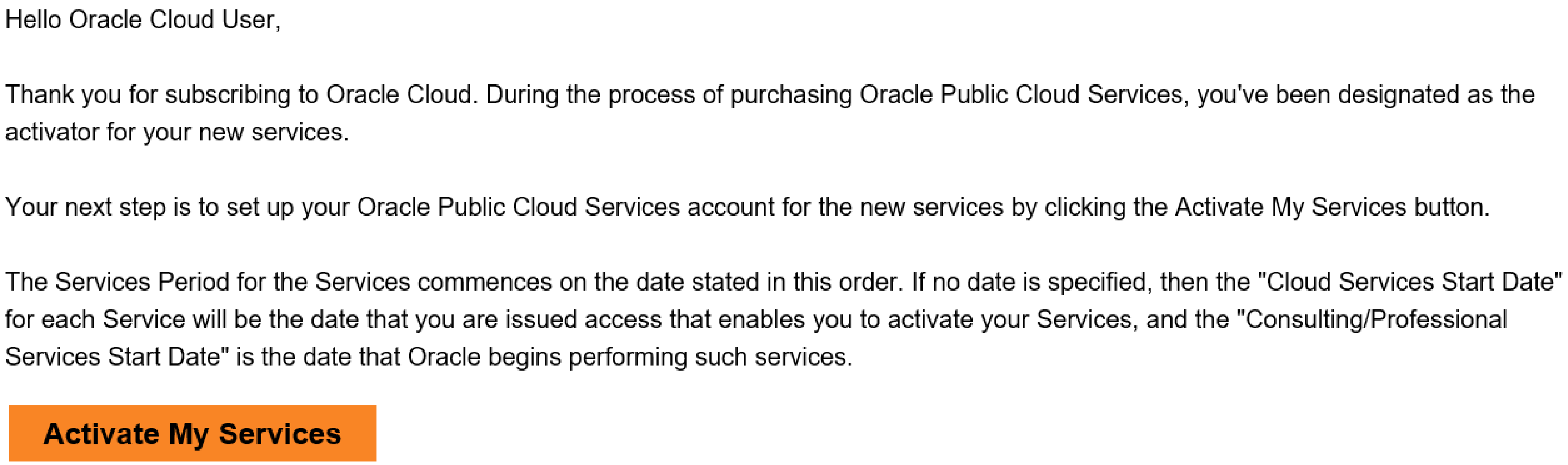
The above group will receive an email with the One-Time Password for xyz-oci@syntax.com username

The CSA will login using xyz-oci@syntax.com / OTP, set a new password, share it with Client Contact ONLY

The CSA will create a login for the resource identified for creating the rest of the named account users that need access to OCI Console

# IAM – OCI Provisioning & Activation

## Activation Email



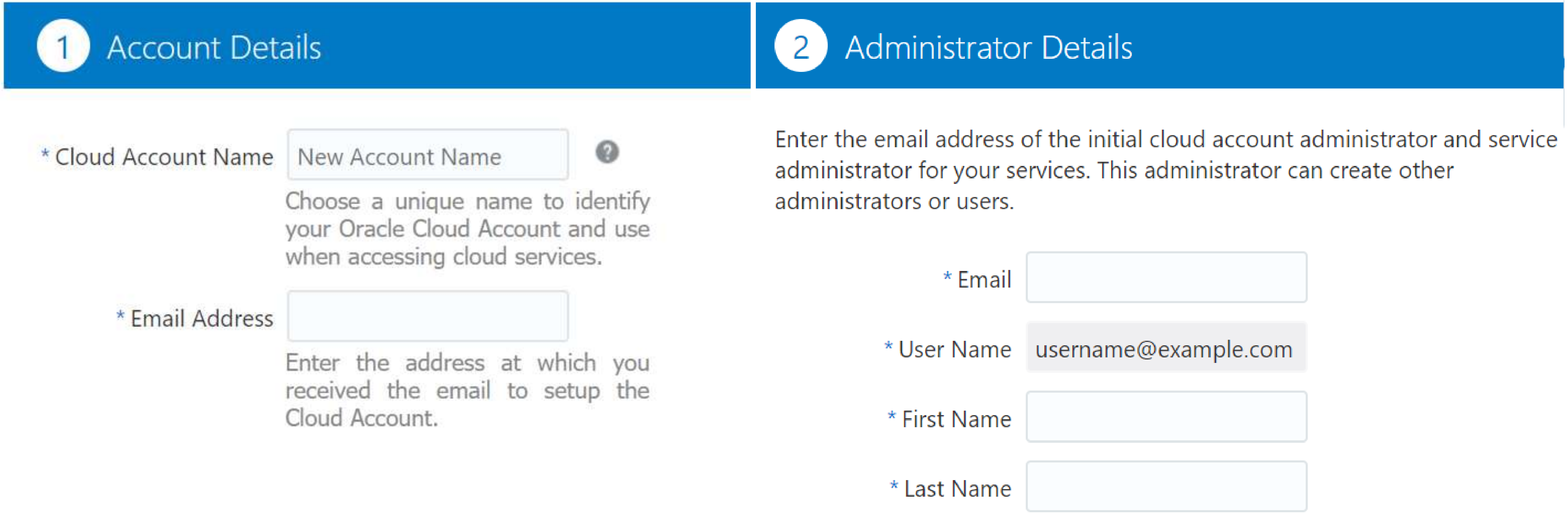
Hello Oracle Cloud User,

Thank you for subscribing to Oracle Cloud. During the process of purchasing Oracle Public Cloud Services, you've been designated as the activator for your new services.

Your next step is to set up your Oracle Public Cloud Services account for the new services by clicking the Activate My Services button.

The Services Period for the Services commences on the date stated in this order. If no date is specified, then the "Cloud Services Start Date" for each Service will be the date that you are issued access that enables you to activate your Services, and the "Consulting/Professional Services Start Date" is the date that Oracle begins performing such services.

# IAM – OCI Provisioning & Activation



## 1 Account Details

* Cloud Account Name: New Account Name ?

Choose a unique name to identify your Oracle Cloud Account and use when accessing cloud services.

* Email Address:

Enter the address at which you received the email to setup the Cloud Account.

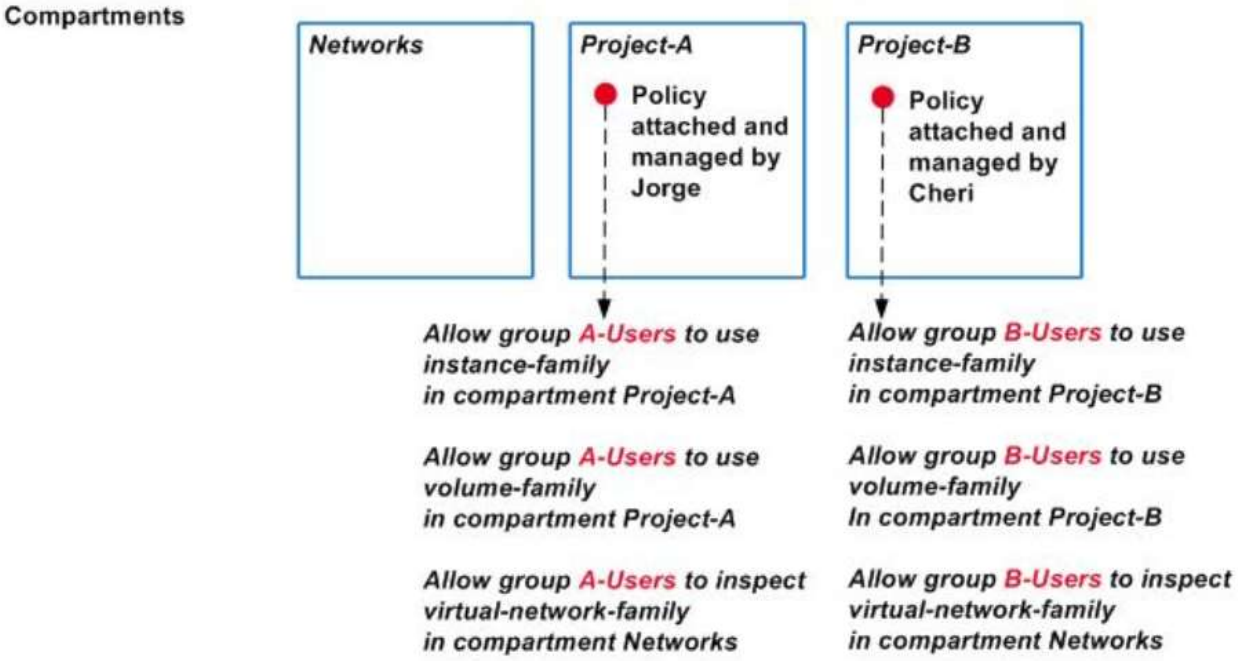
## 2 Administrator Details

Enter the email address of the initial cloud account administrator and service administrator for your services. This administrator can create other administrators or users.

|   |   |
|---|---|
| * Email | |
| * User Name | username@example.com |
| * First Name | |
| * Last Name | |

# IAM - Compartments

- A collection of related resources that can be accessed only by certain groups that have been given permission by an administrator in your organization



Compartments

Networks

Project-A

Policy attached and managed by Jorge

Project-B

Policy attached and managed by Cheri

*Allow group A-Users to use instance-family in compartment Project-A*

*Allow group A-Users to use volume-family in compartment Project-A*

*Allow group A-Users to inspect virtual-network-family in compartment Networks*

*Allow group B-Users to use instance-family in compartment Project-B*

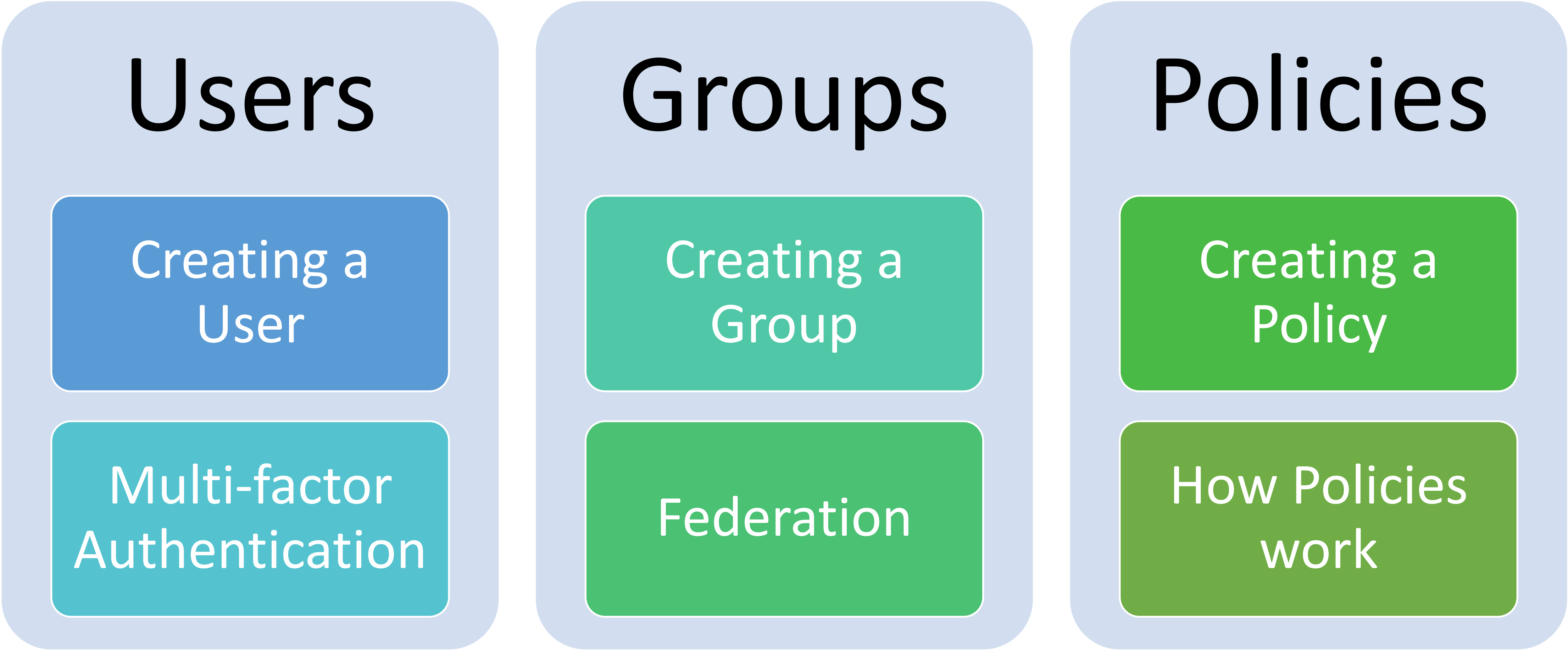
*Allow group B-Users to use volume-family In compartment Project-B*

*Allow group B-Users to inspect virtual-network-family in compartment Networks*

# IAM - Compartments

- Organize and isolate your cloud resources
- Global, across regions
- Creating Compartments
- Access Control for Compartments
- Deleting Compartments
- Default Compartments – root, ManagedCompartmentForPaaS
- Example Compartments – Historical, Management, Production

# IAM – Users, Groups, and Policies



## Users

Creating a User

Multi-factor Authentication

## Groups

Creating a Group

Federation

## Policies

Creating a Policy

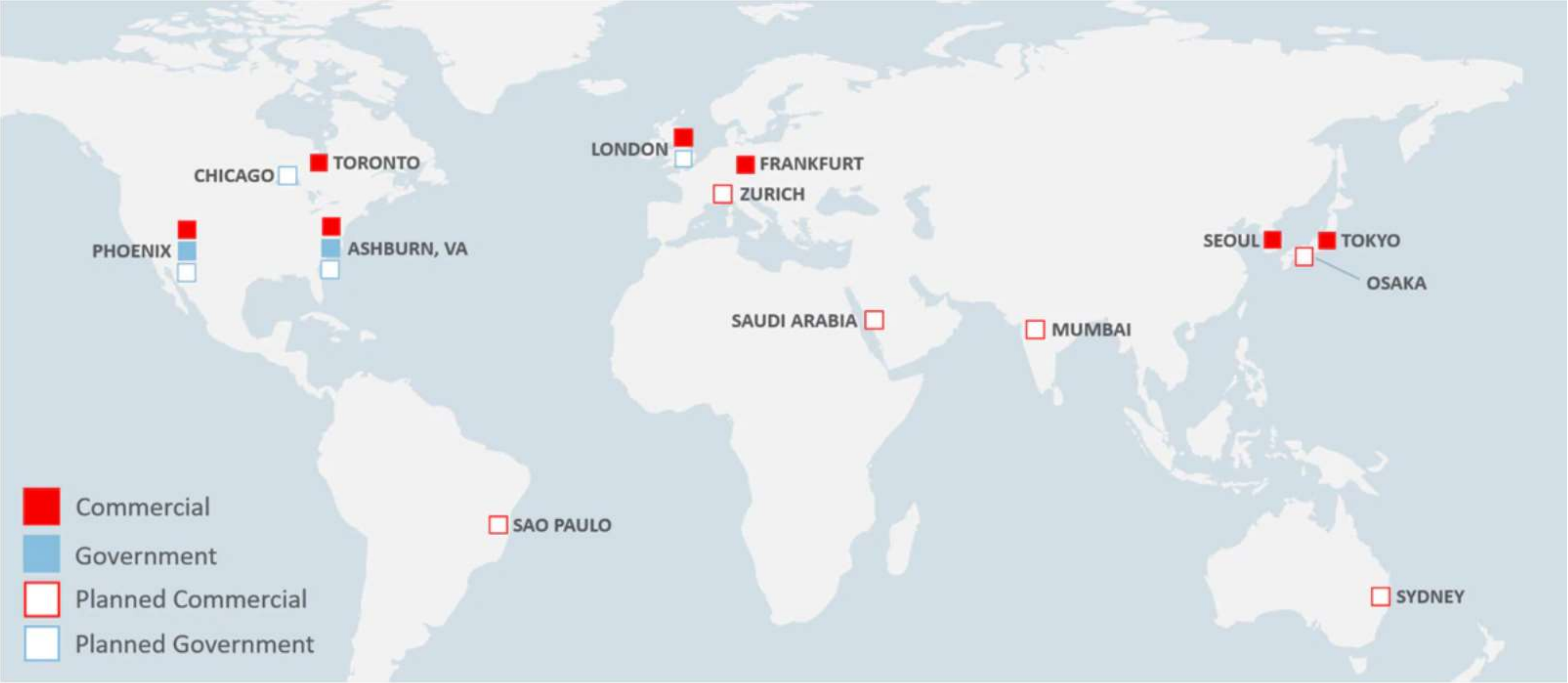
How Policies work

# Virtual Cloud Network

Overview & Resources

NCOAUG
NORTH CENTRAL ORACLE APPS USER GROUP
TRAINING DAY
AUGUST 1, 2019

# OCI Regions & Availability Domains

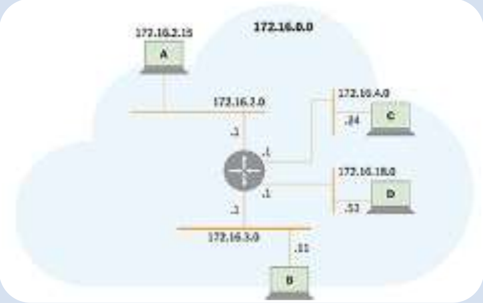


# VCN – Subnets and Subnet Access

Virtual Cloud Network

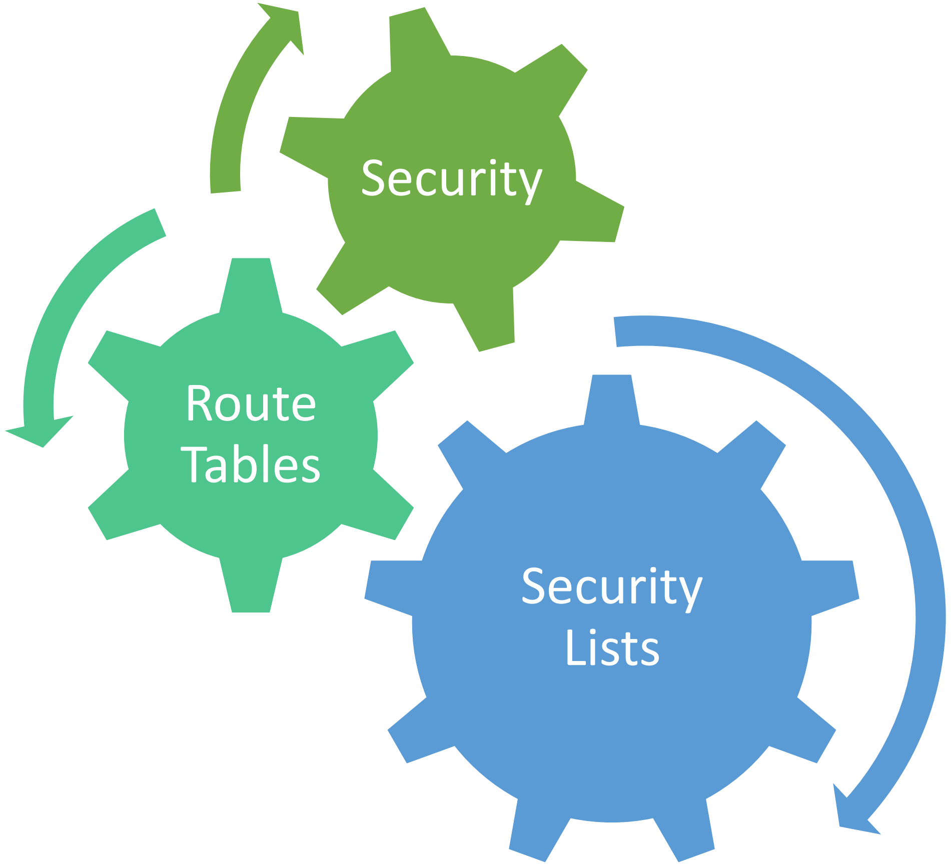
Public Subnet

Private Subnet



CIDR Block

# VCN – Route Tables & Security Lists



# VCN – DHCP Options

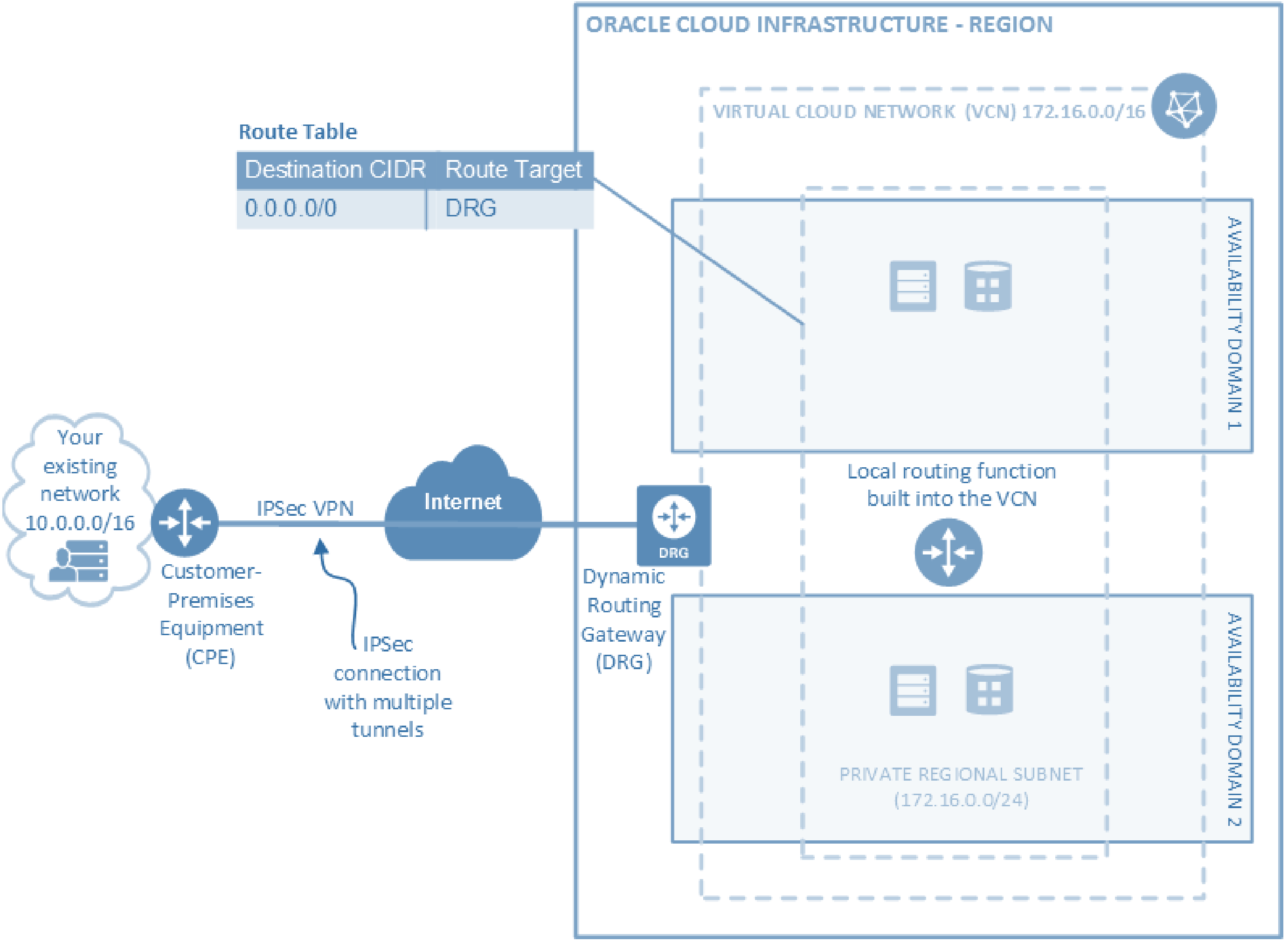
## Dynamic Host Configuration Protocol (DHCP) options in a VCN

- Internet and VCN Resolver
- Custom Resolver

## Search Domain

- *<VCN DNS label>*.oraclevcn.com

# VCN – Customer Premises Equipment



**Route Table**

| Destination CIDR | Route Target |
|---|---|
| 0.0.0.0/0 | DRG |

ORACLE CLOUD INFRASTRUCTURE - REGION
VIRTUAL CLOUD NETWORK (VCN) 172.16.0.0/16
AVAILABILITY DOMAIN 1
AVAILABILITY DOMAIN 2
Local routing function built into the VCN
PRIVATE REGIONAL SUBNET (172.16.0.0/24)
DRG
Dynamic Routing Gateway (DRG)
Internet
IPSec VPN
IPSec connection with multiple tunnels
Customer-Premises Equipment (CPE)
Your existing network 10.0.0.0/16

# VCN – Dynamic Routing Gateways

## DRG

- Virtual Router
- Private Network Traffic

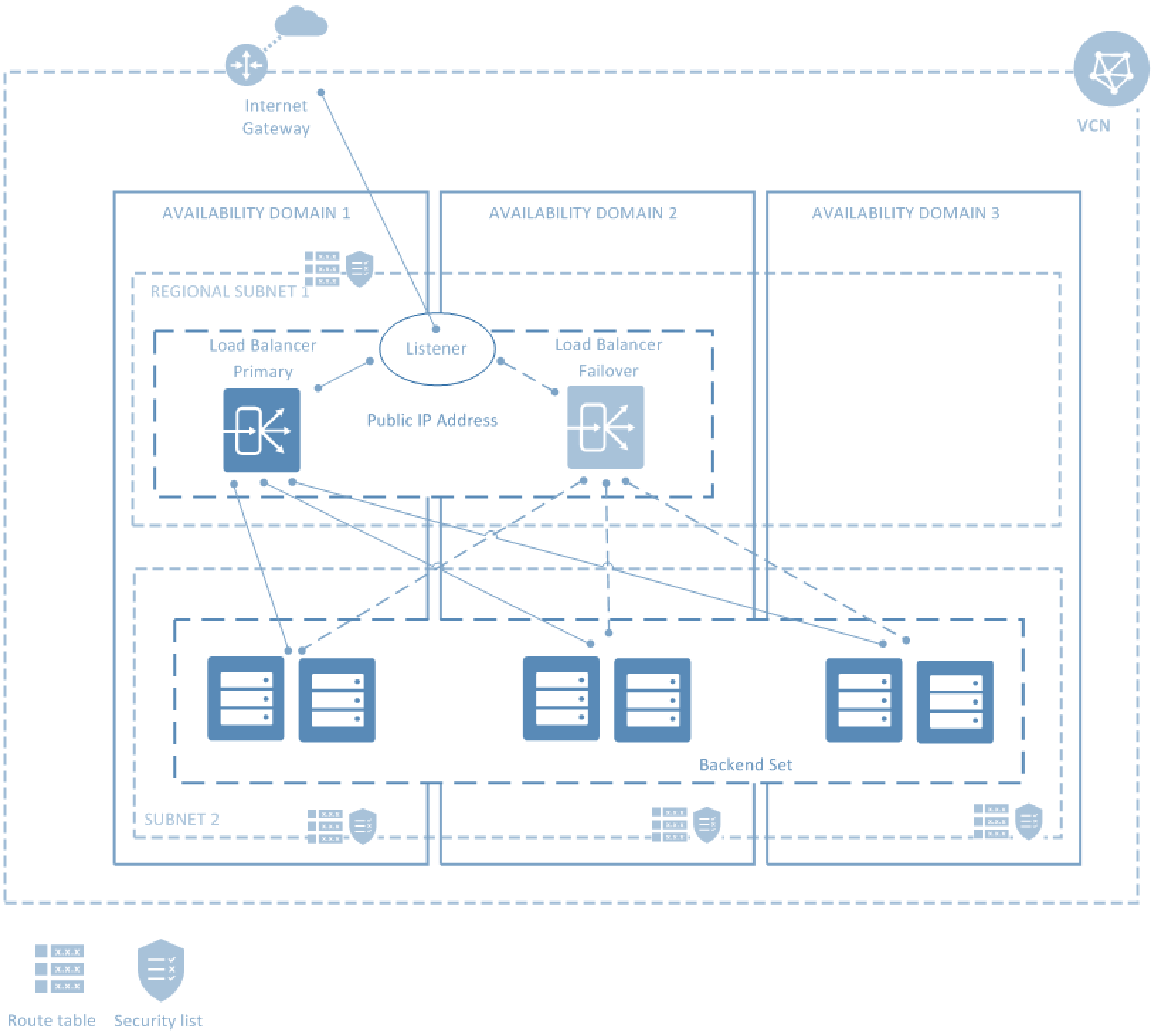
## IPSec VPN

- VPN Connect
- Connect on-prem to VCN

## FastConnect

- Dedicated, private connection
- Higher bandwidth

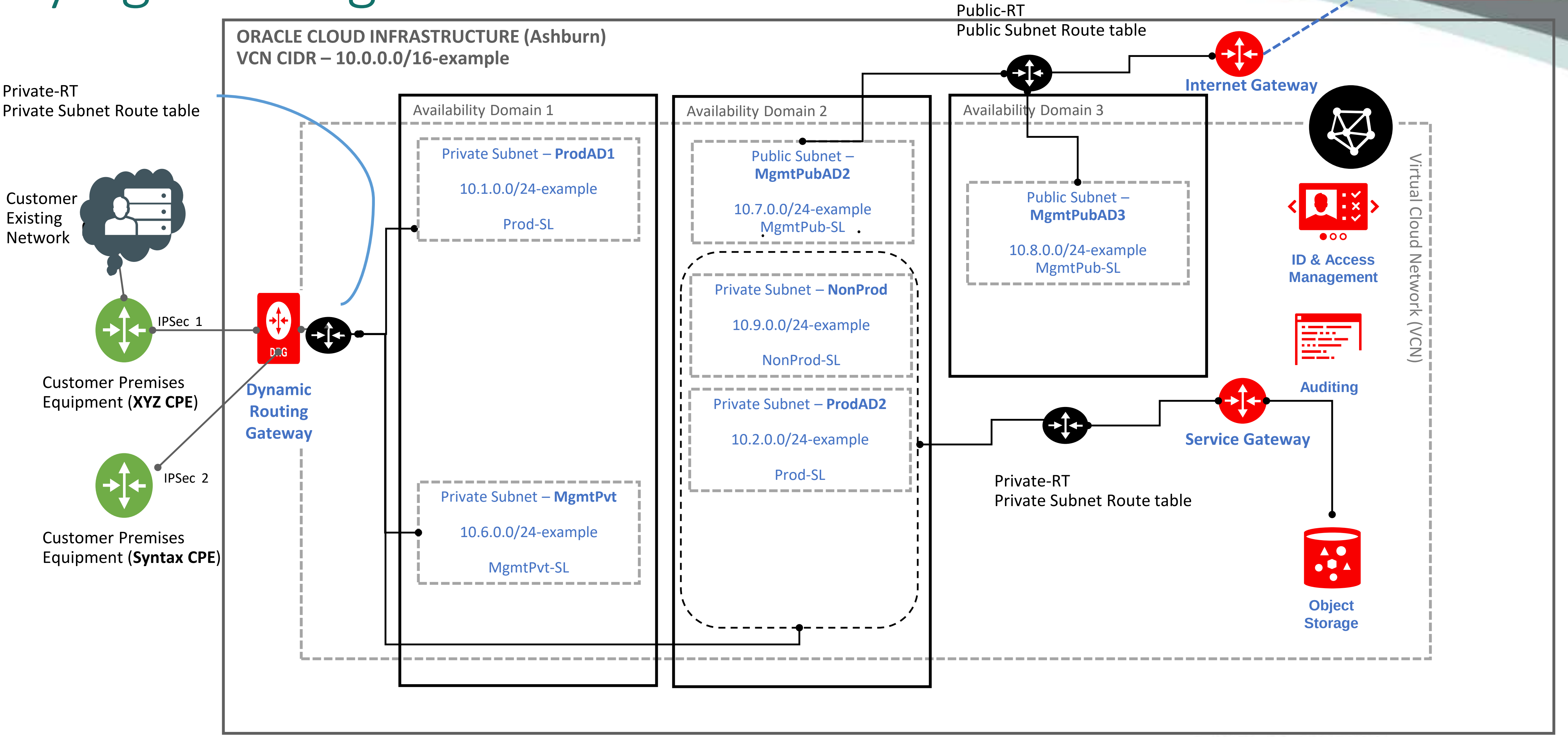
# VCN – Load Balancers



# VCN - Gateways

- Internet Gateway
- NAT Gateway
- Service Gateway

# Tying it all together…



ORACLE CLOUD INFRASTRUCTURE (Ashburn)
VCN CIDR – 10.0.0.0/16-example

Public-RT
Public Subnet Route table

Private-RT
Private Subnet Route table

Customer Existing Network

IPSec 1

IPSec 2

Customer Premises Equipment (**XYZ CPE**)

Customer Premises Equipment (**Syntax CPE**)

DRG

Dynamic Routing Gateway

Availability Domain 1

Private Subnet – **ProdAD1**
10.1.0.0/24-example
Prod-SL

Private Subnet – **MgmtPvt**
10.6.0.0/24-example
MgmtPvt-SL

Availability Domain 2

Public Subnet – **MgmtPubAD2**
10.7.0.0/24-example
MgmtPub-SL

Private Subnet – **NonProd**
10.9.0.0/24-example
NonProd-SL

Private Subnet – **ProdAD2**
10.2.0.0/24-example
Prod-SL

Availability Domain 3

Public Subnet – **MgmtPubAD3**
10.8.0.0/24-example
MgmtPub-SL

Internet Gateway

ID & Access Management

Auditing

Service Gateway

Private-RT
Private Subnet Route table

Object Storage

Virtual Cloud Network (VCN)

# Requirements Gathering

Templates

NCOAUG
NORTH CENTRAL ORACLE APPS USER GROUP
TRAINING DAY
AUGUST 1, 2019

# Requirements Template - Tenancy

| | |
|---|---|
| **Version:** | 1 |
| **Prepared By:** | Solution Architect |
| **Prepared For:** | XYZ Company |
| **CSM:** | Oracle CSM |
| **AM/PM:** | Account Manager / Project Manager |
| **Approved By:** | Client Approver |
| **Date:** | 5-Jul-19 |
| | |
| **Tenancy Name** | xyz |
| **Tenancy Admin** | xyz-oci@xyz.com |
| **DL Members** | CSA |
| | Sales Rep |
| | Client Contact |
| | Account Manager |
| | DBA DL |
| | MS CNC DL |
| | SysAdmin DL |
| | Network DL |

# Requirements Template - IAM

| OCI Compartment Details | | | |
|---|---|---|---|
| | | | |
| Compartment 1: | root | Default | |
| Compartment 2: | ManagedCompartmentForPaaS | Default | |
| Compartment 3: | Historical | | |
| Compartment 4: | Management | | |
| Compartment 5: | JDEProd | | |
| Compartment 6: | JDENonProd | | |
| | | | |

| OCI Group Details | | | |
|---|---|---|---|
| | | | |
| Group Name | Members | Policy | Statement |
| Administrators | oci-xyz@xyz.com | Tenant Admin Policy | ALLOW GROUP Administrators to manage all-resources IN TENANCY |
| SyntaxServiceDesk | techdesk@syntax.com | SSDPolicy | Allow group SyntaxServiceDesk to manage users in tenancy |
| SyntaxNetAdmins | netadmins@syntax.com | SNAPolicy | Allow group SyntaxNetAdmins to manage virtual-network-family in tenancy<br>Allow group SyntaxNetAdmins to read audit-events in tenancy |
| SyntaxSysAdmins | sysadmins@syntax.com | SSAPolicy | Allow group SyntaxSysAdmins to manage volume-family in tenancy<br>Allow group SyntaxSysAdmins to manage instance-family in tenancy<br>Allow group SyntaxSysAdmins to read audit-events in tenancy |
| SyntaxDBAdmins | dbadmins@syntax.com | SDAPolicy | Allow group SyntaxDBAdmins to inspect all-resources in tenancy<br>Allow group SyntaxDBAdmins to read audit-events in tenancy |
| SyntaxCNCAdmins | cncadmins@syntax.com | SCAPolicy | Allow group SyntaxCNCAdmins to inspect all-resources in tenancy<br>Allow group SyntaxCNCAdmins to read audit-events in tenancy |
| ClientNetAdmins | xyznetadmins@xyz.com | CNAPolicy | Allow group ClientNetAdmins to manage virtual-network-family in tenancy<br>Allow group ClientNetAdmins to read audit-events in tenancy |
| Auditors | auditors@xyz.com<br>auditors@syntax.com | AuditorsPolicy | Allow group Auditors to inspect all-resources in tenancy<br>Allow group Auditors to read audit-events in tenancy |

# Requirements Template - Subnets

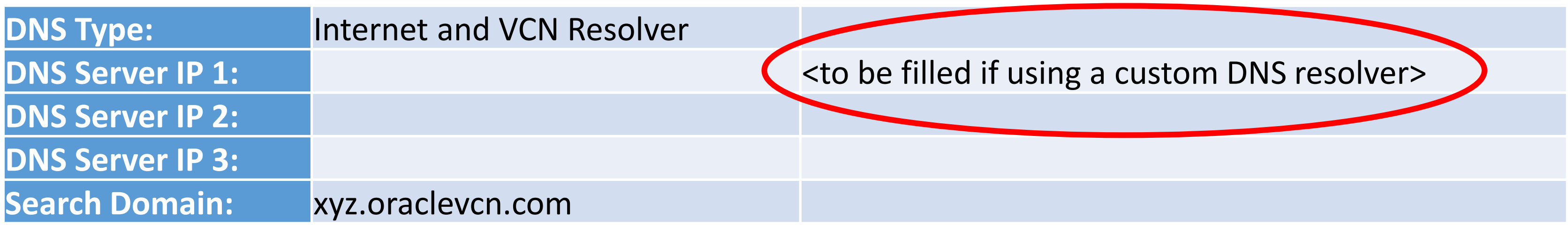
| | | | | | | |
|---|---|---|---|---|---|---|
| **Region:** | Ashburn, VA | | | | | |
| | | | | | | |
| **Virtual Cloud Network Name:** | XYZ-VCN | | | | | |
| **CIDR Block:** | 10.0.0.0/16-example | | | | | |
| **Compartment:** | root | | | | | |
| | | | | | | |
| **Subnet Name** | CIDR Block | Availability Domain | Subnet Access | Security List | Route Table | DHCP |
| **ProdAD1** | 10.1.0.0/24-example | AD1 | Private | Prod-SL | Private-RT | Default |
| **ProdAD2** | 10.2.0.0/24-example | AD2 | Private | Prod-SL | Private-RT | Default |
| **SNProd** | N/A | AD1 | Private | SNProd-SL | Private-RT | Default |
| **DBProd** | N/A | AD1 | Private | DBProd-SL | Private-RT | Default |
| **AppProd** | N/A | AD1 | Private | AppProd-SL | Private-RT | Default |
| **MgmtPvt** | 10.6.0.0/24-example | AD1 | Private | MgmtPvt-SL | Private-RT | Default |
| **MgmtPubAD2** | 10.7.0.0/24-example | AD2 | Public | MgmtPub-SL | Public-RT | Default |
| **MgmtPubAD3** | 10.8.0.0/24-example | AD3 | Public | MgmtPub-SL | Public-RT | Default |
| **NonProd** | 10.9.0.0/24-example | AD2 | Private | NonProd-SL | Private-RT | Default |
| **SNNonProd** | N/A | AD2 | Private | SNNonProd-SL | Private-RT | Default |
| **DBNonProd** | N/A | AD2 | Private | DBNonProd-SL | Private-RT | Default |
| **AppNonProd** | N/A | AD2 | Private | AppNonProd-SL | Private-RT | Default |

# Requirements Template – Route Table & Security List

| Private Route Table Rules | | | |
|---|---|---|---|
| Target Type: | Destination CIDR Block | Target Name | |
| Dynamic Routing Gateway | | XYZ-DRG | <add lines for multiple destination CIDRs> |
| NAT Gateway | | XYZ-NG | <add lines for multiple destination CIDRs> |
| Service Gateway | OCI IAD Object Storage | XYZ-SG | |
| | | | |
| Public Route Table Rules | | | |
| Target Type: | Destination CIDR Block | Target Name | |
| Internet Gateway | 0.0.0.0/0 | XYZ-IG | <restrict access if needed> |

| Prod-SL | | | | | | | |
|---|---|---|---|---|---|---|---|
| Ingress Rules | | | | Egress Rules | | | |
| Source | IP Protocol | Source Port Range / Code | Destination Port Range / Code | Destination | IP Protocol | Source Port Range / Code | Destination Port Range / Code |
| 0.0.0.0/0 | ICMP | 3,4 | - | 0.0.0.0/0 | All Protocols | All | All |
| 10.0.0.0/16-example | ICMP | 3 | - | | | | |
| 10.0.0.0/16-example | TCP | All | 22 | | | | |

# Requirements Template – DHCP Options



| | | |
|---|---|---|
| **DNS Type:** | Internet and VCN Resolver | |
| **DNS Server IP 1:** | | <to be filled if using a custom DNS resolver> |
| **DNS Server IP 2:** | | |
| **DNS Server IP 3:** | | |
| **Search Domain:** | xyz.oraclevcn.com | |

# Requirements Template – CPE & DRG

| | | |
|---|---|---|
| **Customer Premises Equipment Name:** | XYZ-CPE1 | |
| **IP Address 1:** | | <Public IP of XYZ Firewall> |
| | | |
| **Customer Premises Equipment Name:** | Syntax-CPE1 | |
| **IP Address 1:** | | <Public IP of Syntax Firewall> |

| | | |
|---|---|---|
| **Dynamic Routing Gateway Name:** | XYZ-DRG | |
| | | |
| **IPsec Connection Name 1:** | XYZToOCI | |
| **Static Routes:** | | <CIDR blocks that should be accessible over VPN from OCI> |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| **IPsec Connection Name 2:** | SyntaxToOCI | |
| **Static Routes:** | | <CIDR blocks that should be accessible over VPN from OCI> |
| | | |
| | | |
| | | |
| | | |
| | | |

# Requirements Template – LB

| | |
|---|---|
| **Load Balancer Name:** | XYZ-pvt-LB |
| **Shape:** | 100Mbps |
| **VCN:** | XYZ-VCN |
| **Visibility:** | Private |
| **Subnet:** | MgmtPvt |
| | |
| **Load Balancer Name:** | XYZ-pub-LB |
| **Shape:** | 100Mbps |
| **VCN:** | XYZ-VCN |
| **Visibility:** | Public |
| **Subnet 1:** | MgmtPubAD2 |
| **Subnet 2:** | MgmtPubAD3 |

# Requirements Template - Gateways

| | |
|---|---|
| **Service Gateway Name:** | XYZ-SG |
| **Compartment:** | root |
| **Services:** | OCI IAD Object Storage |

| | |
|---|---|
| **Internet Gateway Name:** | XYZ-IG |
| **NAT Gateway Name:** | XYZ-NG |

# Demo

NCOAUG

NORTH CENTRAL ORACLE APPS USER GROUP

TRAINING DAY
AUGUST 1, 2019

# Q & A

NCOAUG

NORTH CENTRAL ORACLE APPS USER GROUP

TRAINING DAY

AUGUST 1, 2019

# Thank you!

amukherjee@syntax.com

NCOAUG

North Central Oracle Apps User Group

TRAINING DAY

AUGUST 1, 2019