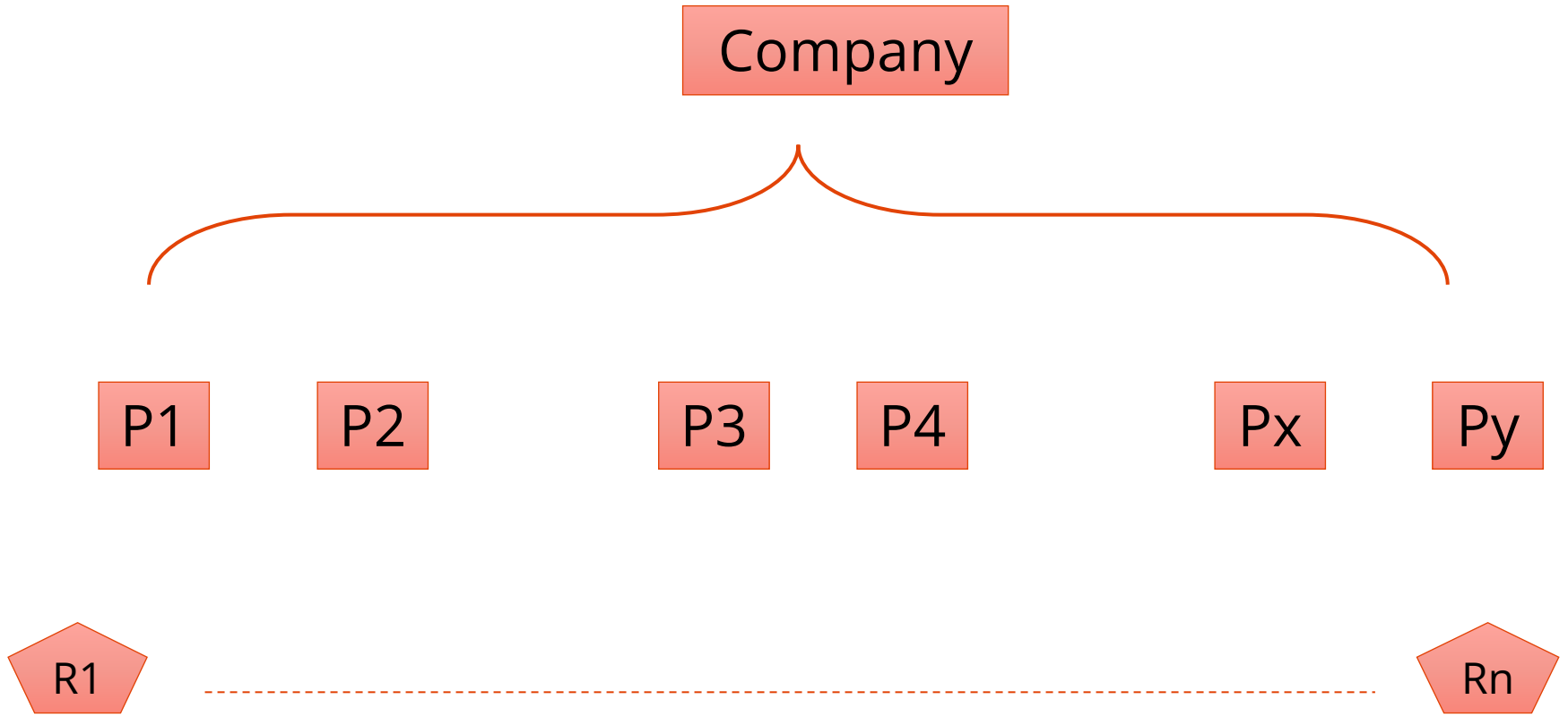
OCI Networking 101

ACE Solutions Architecture Team

OCI Hierarchy



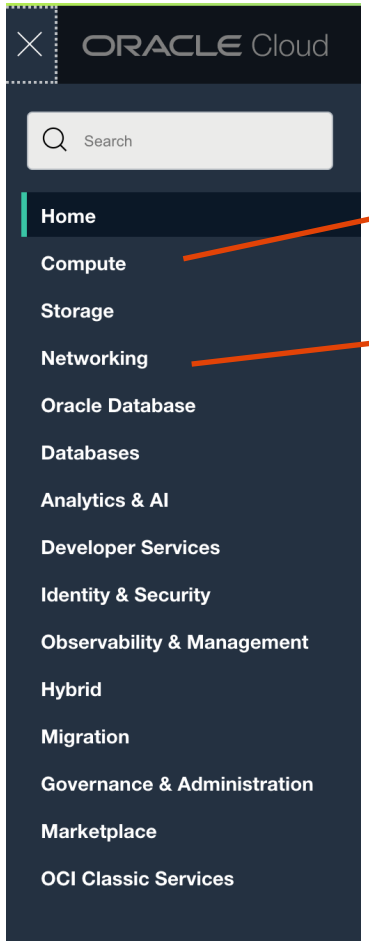
Tenancy (root compartment)

Compartments

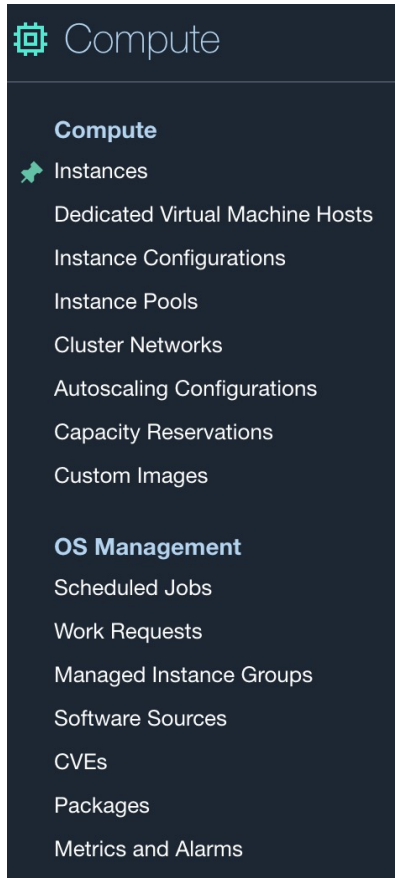
Resources

Oracle Services and Resources

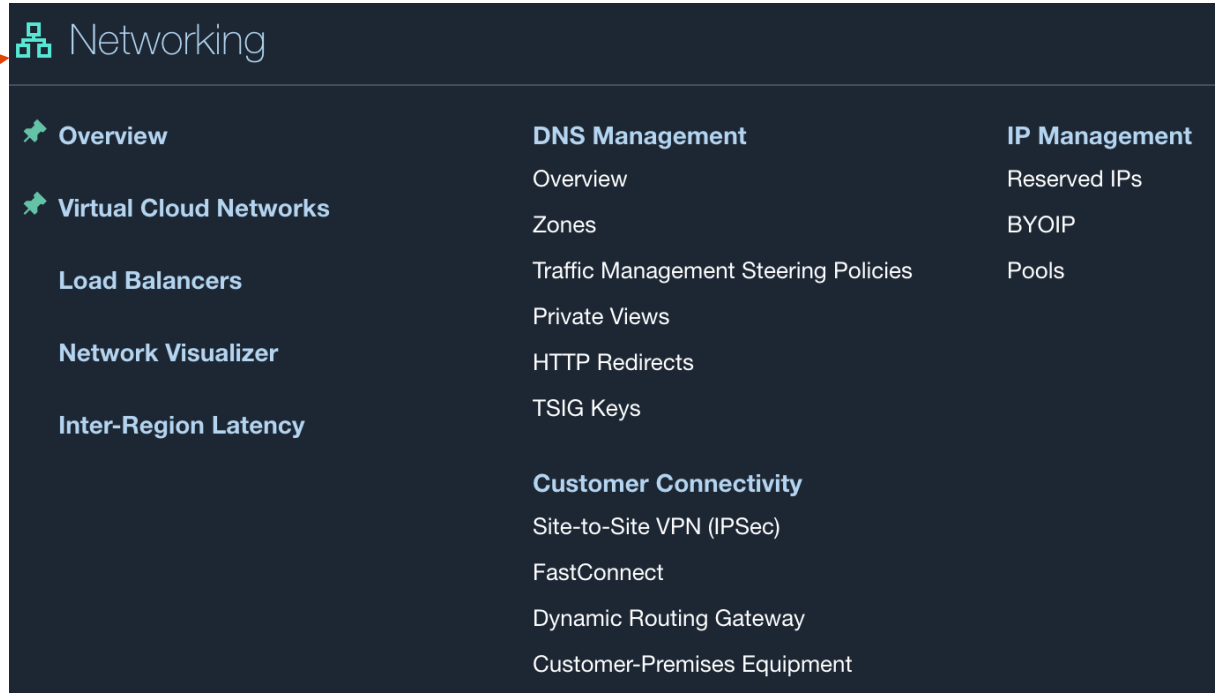
Console Snapshot
IaaS (Core) + Database



Compute Resources



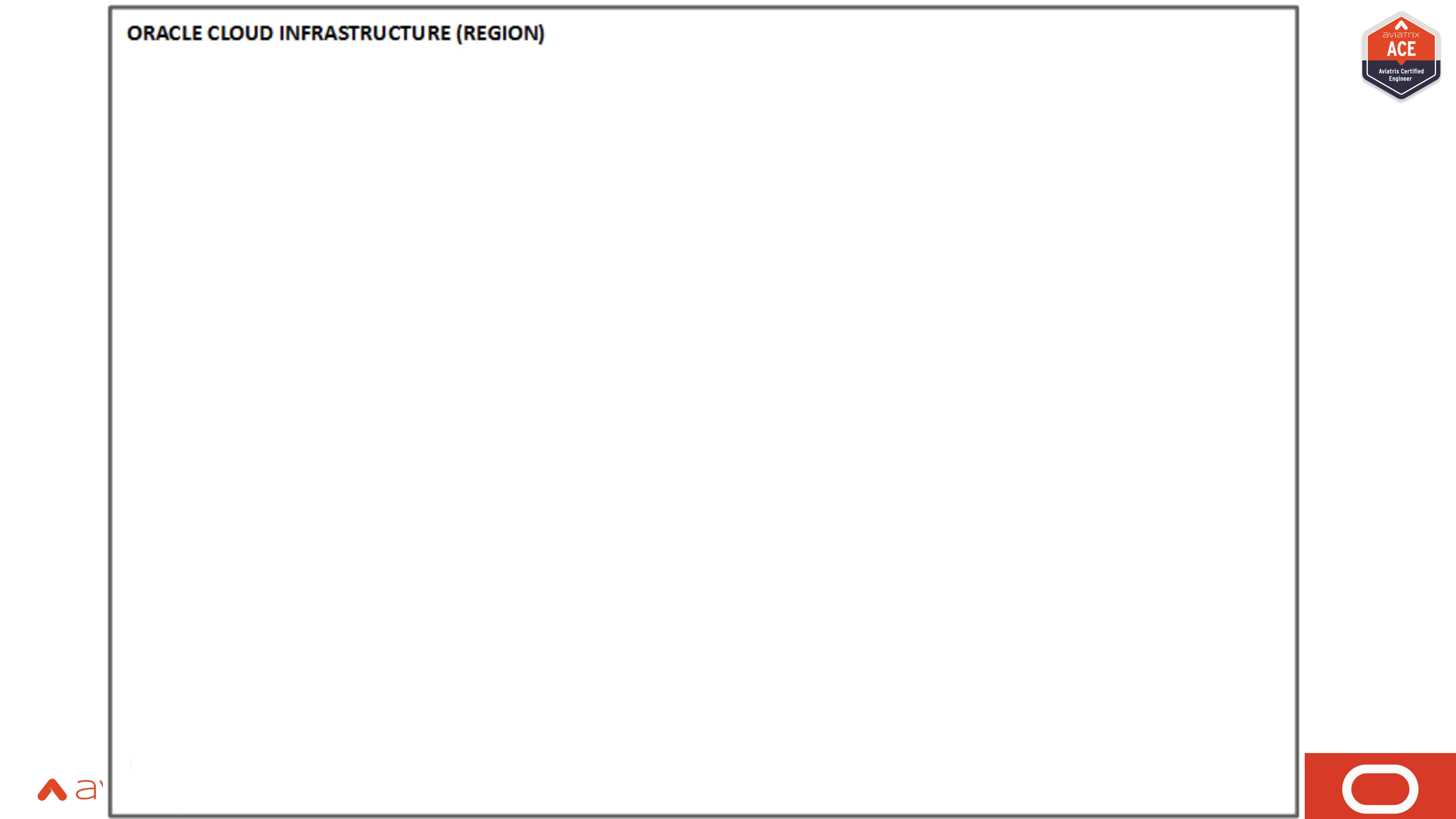
Networking Resources

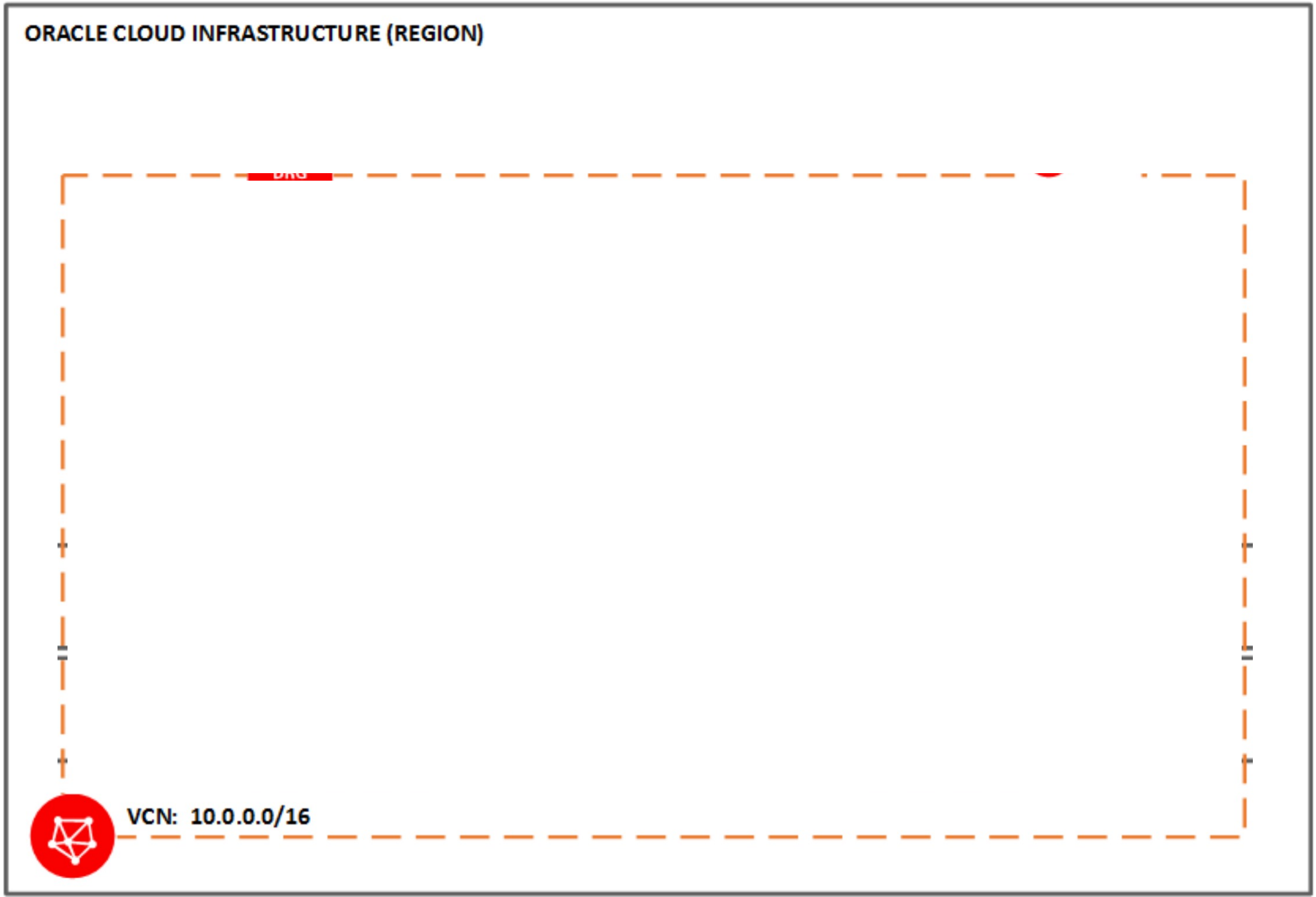


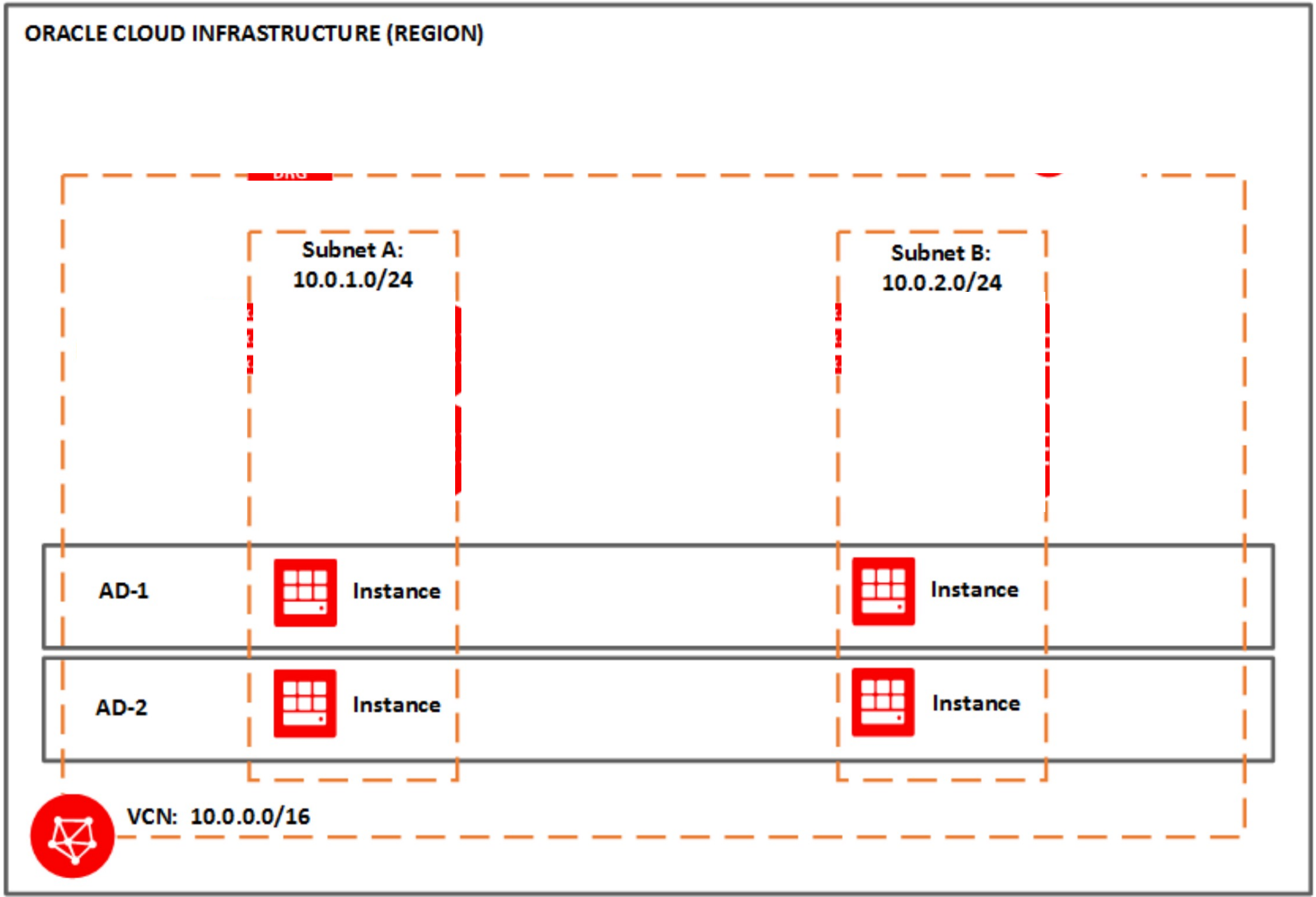
Oracle Important Services

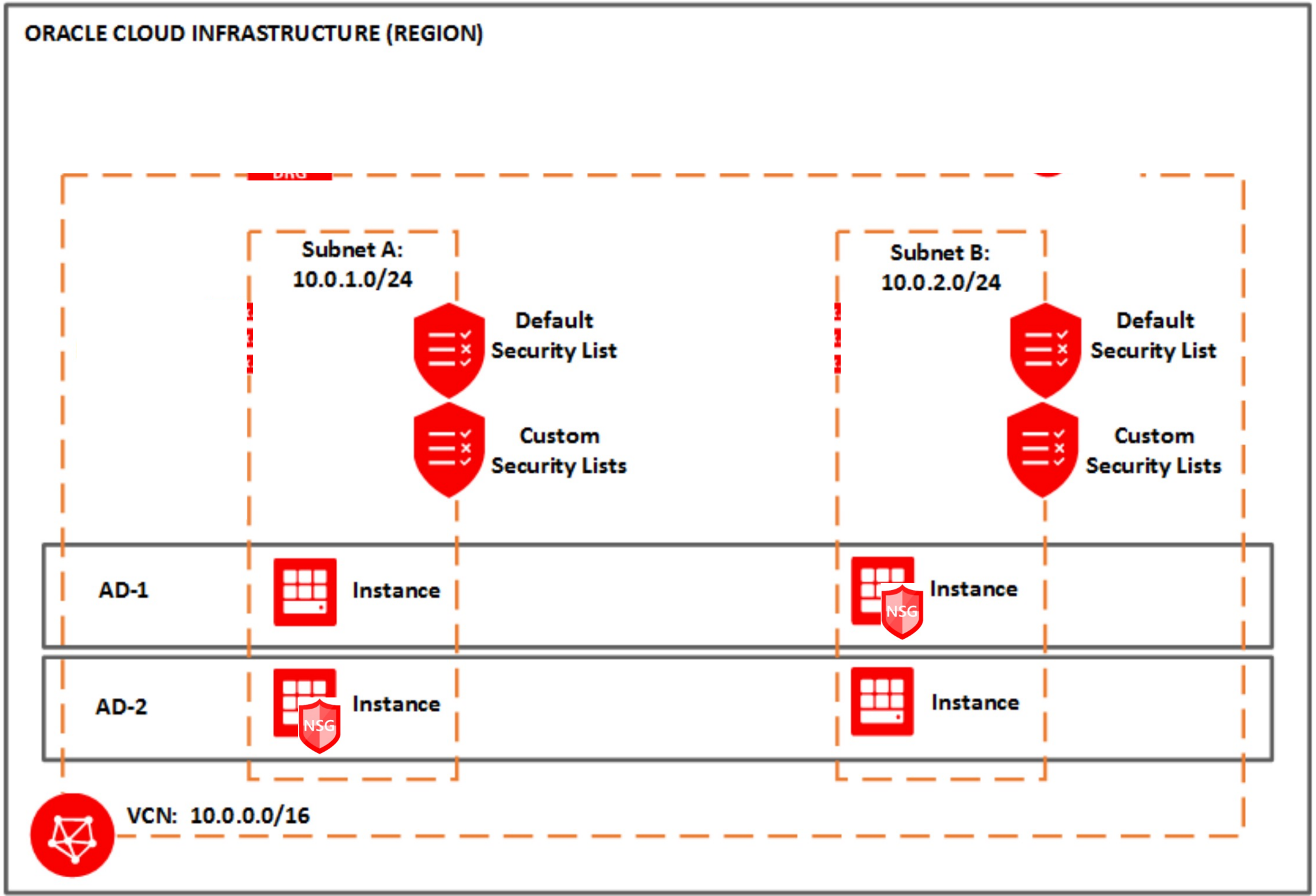
Service Name	Purpose
Compute	Run instances (virtual machine or bare-metal)
IAM	Identity and Access Management
VCN	Virtual Cloud Network
Block Volume	Storage
FastConnect	Connecting On-Prem
DNS Zone Management	DNS

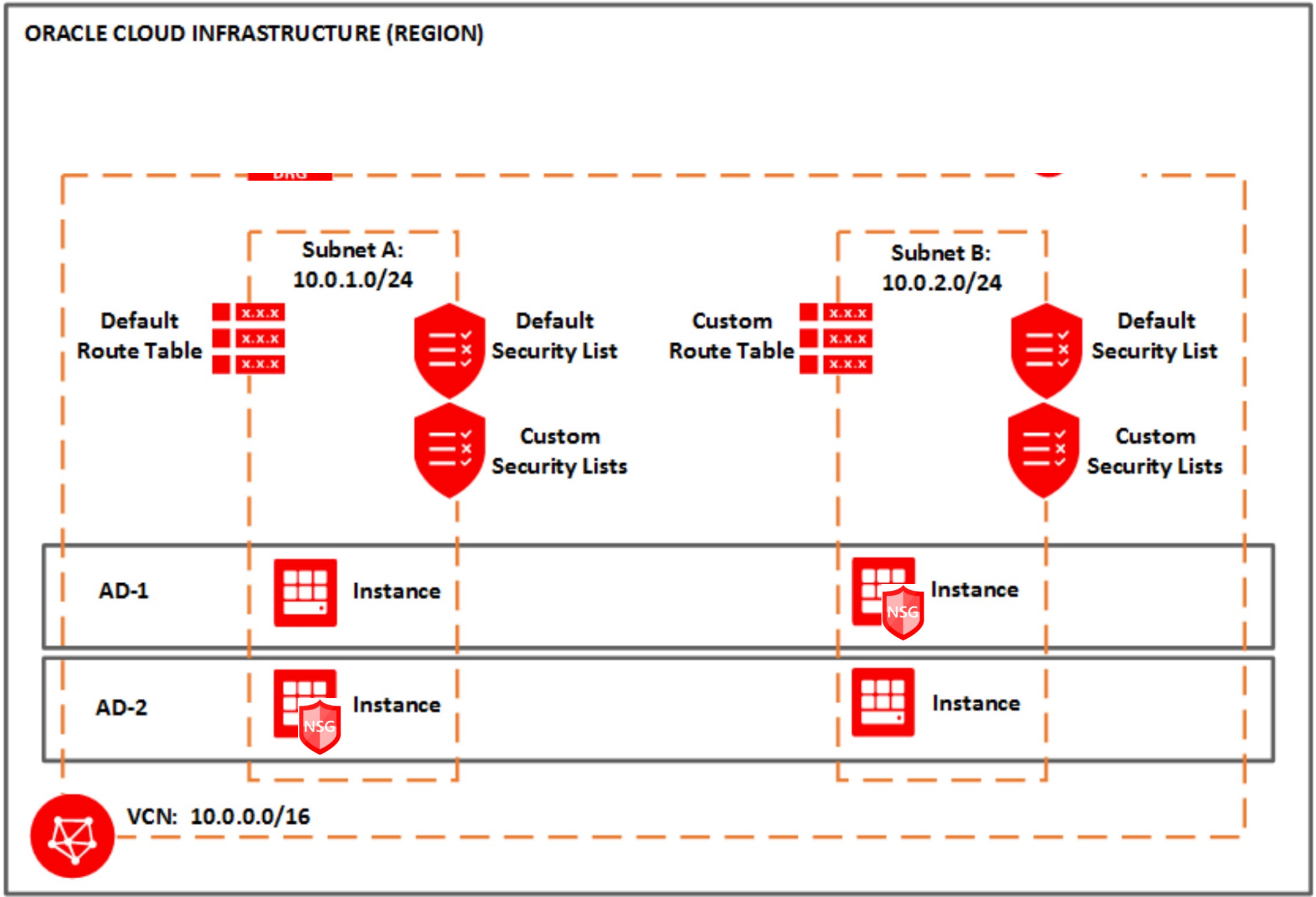
ORACLE CLOUD INFRASTRUCTURE (REGION)

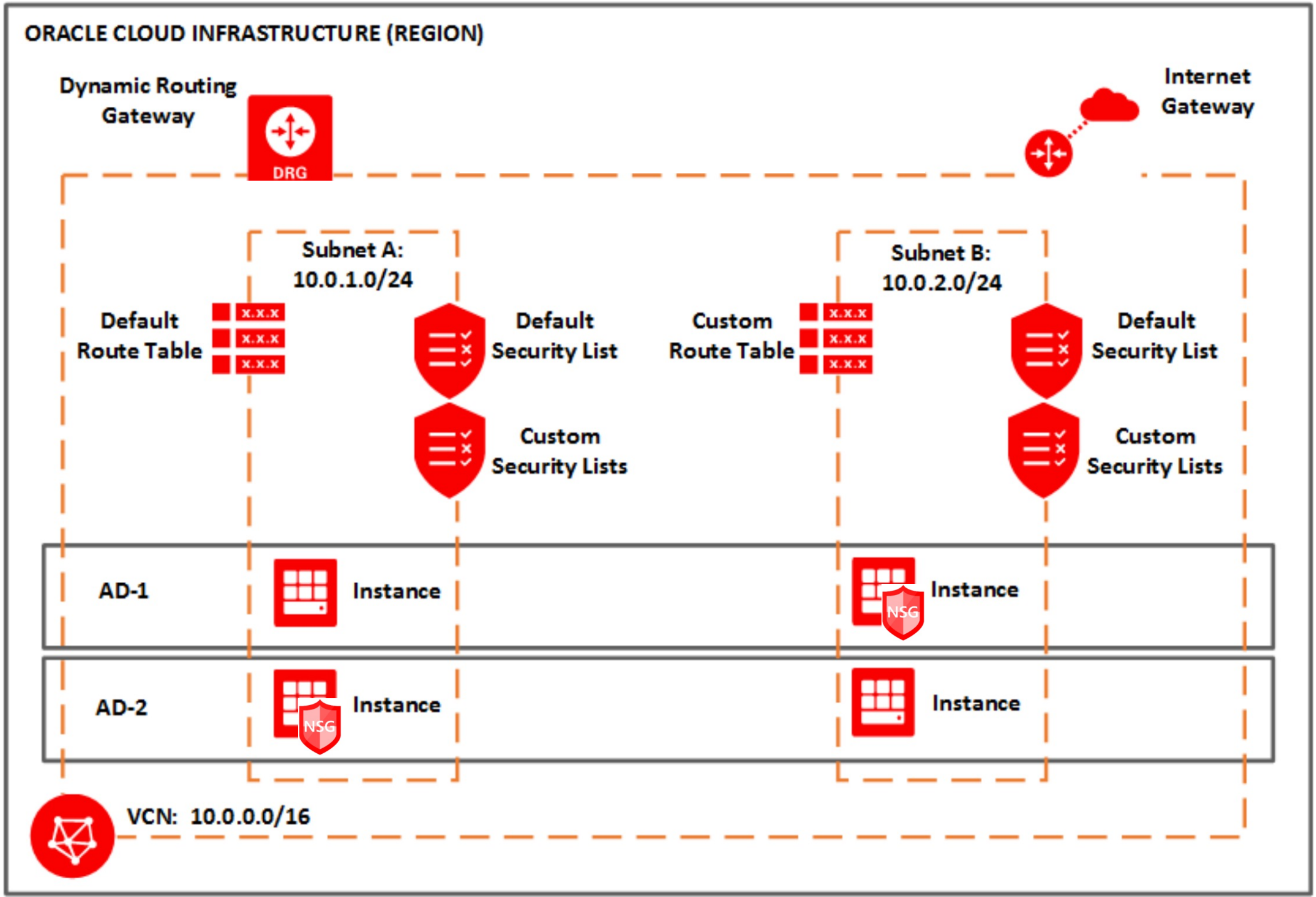



ORACLE CLOUD INFRASTRUCTURE (REGION)
VCN: 10.0.0.0/16


ORACLE CLOUD INFRASTRUCTURE (REGION)
Subnet A:
10.0.1.0/24
Subnet B:
10.0.2.0/24
AD-1
Instance
Instance
AD-2
Instance
Instance
VCN: 10.0.0.0/16


ORACLE CLOUD INFRASTRUCTURE (REGION)
Subnet A:
10.0.1.0/24
Default
Security List
Custom
Security Lists
Subnet B:
10.0.2.0/24
Default
Security List
Custom
Security Lists
AD-1
Instance
NSG
Instance
AD-2
NSG
Instance
Instance
VCN: 10.0.0.0/16


ORACLE CLOUD INFRASTRUCTURE (REGION)
Subnet A:
10.0.1.0/24
Subnet B:
10.0.2.0/24
Default
Route Table
X.X.X
X.X.X
X.X.X
Default
Security List
Custom
Security Lists
Custom
Route Table
X.X.X
X.X.X
X.X.X
Default
Security List
Custom
Security Lists
AD-1
Instance
NSG
Instance
AD-2
NSG
Instance
Instance
VCN: 10.0.0.0/16

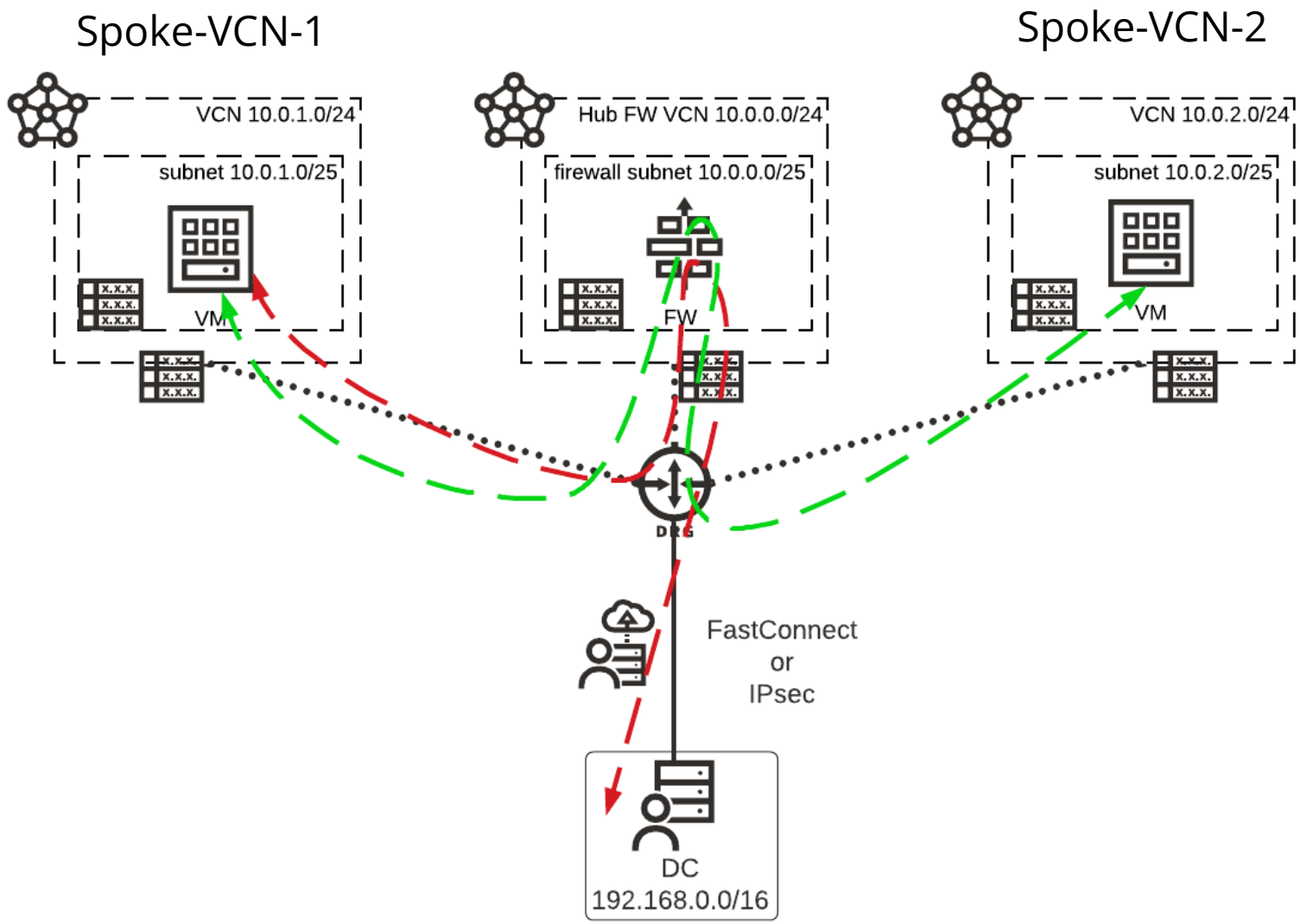

ORACLE CLOUD INFRASTRUCTURE (REGION)
Dynamic Routing Gateway
DRG
Internet Gateway
Subnet A: 10.0.1.0/24
Subnet B: 10.0.2.0/24
Default Route Table
X.X.X
X.X.X
X.X.X
Default Security List
Custom Security Lists
Custom Route Table
X.X.X
X.X.X
X.X.X
Default Security List
Custom Security Lists
AD-1
Instance
NSG
Instance
AD-2
NSG
Instance
Instance
VCN: 10.0.0.0/16

Oracle Native Network Constructs

Construct	Purpose
Dynamic Routing Gateway (DRG)	Transit hub entity. Used for interconnecting VCNs inside a region. Capable of establishing intra- and inter-region connections. Termination point for IPsec VPN and FastConnect circuits.
Service Gateway (SG)	Service gateway is regional and enables access only to supported Oracle services in the same region as the VCN.
Internet Gateway (IG)	Internet Gateway provides a path for network traffic between VCN and the internet
NAT Gateway (NG)	NAT Gateway provides an option for the private resources to access the public internet.
~~Local Peering Gateway (LPG)~~ *Effectively obsolete*	~~Entity required to build a Local "VCN Peering" (within the same region)~~
Subnet	Subnets can be regional in OCI spanning Availability Domains
Route Table	Route Table consists of a set of route rules that provide mapping for the traffic from subnets via gateways to destinations outside the VCN

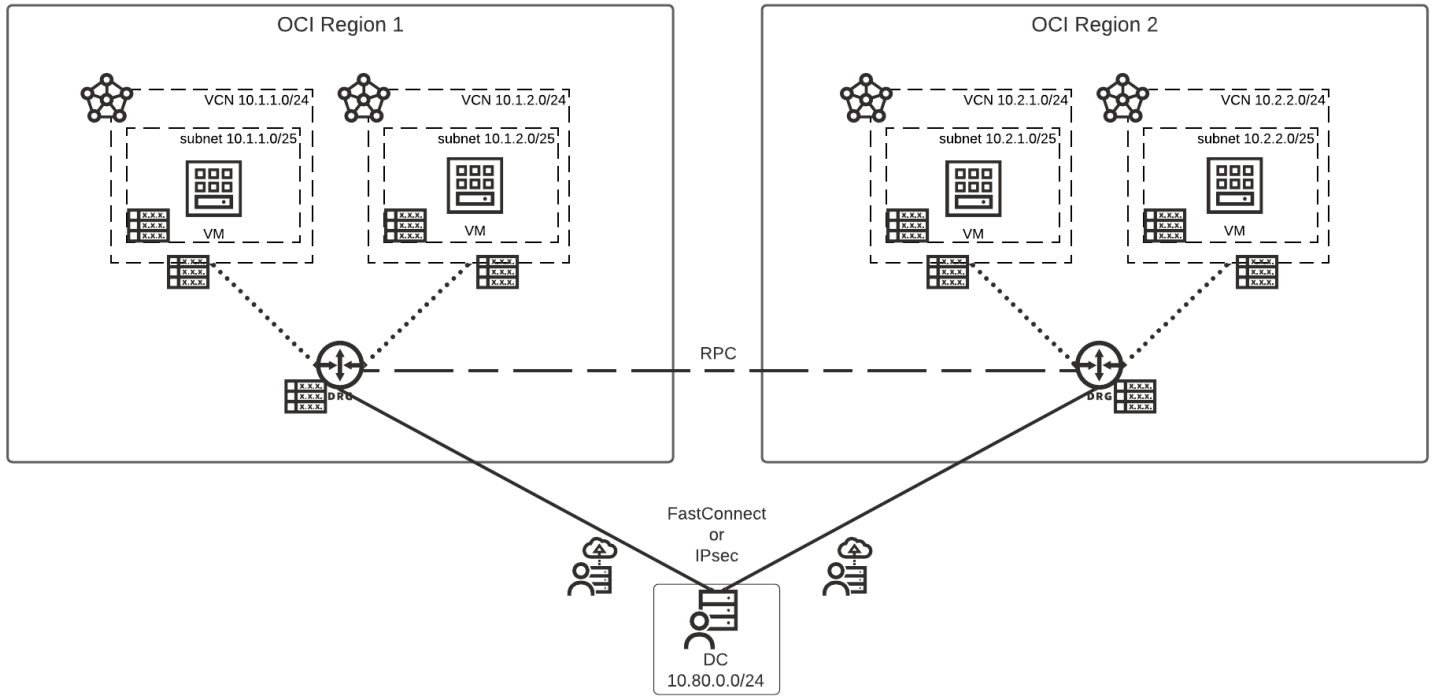
OCI DRG “2.0”

- DRG “2.0” becomes transitive
- DRG becomes the hub gateway supporting 300 attachments
- Improvements for East-West traffic routing options
- Design patterns allowing for FW insertion for traffic between VCNs or to on-prem (in the diagram)
- Still requiring complex route table management, not supporting overlap, lacking visibility into the traffic flows, no traffic encryption controlled by the customer



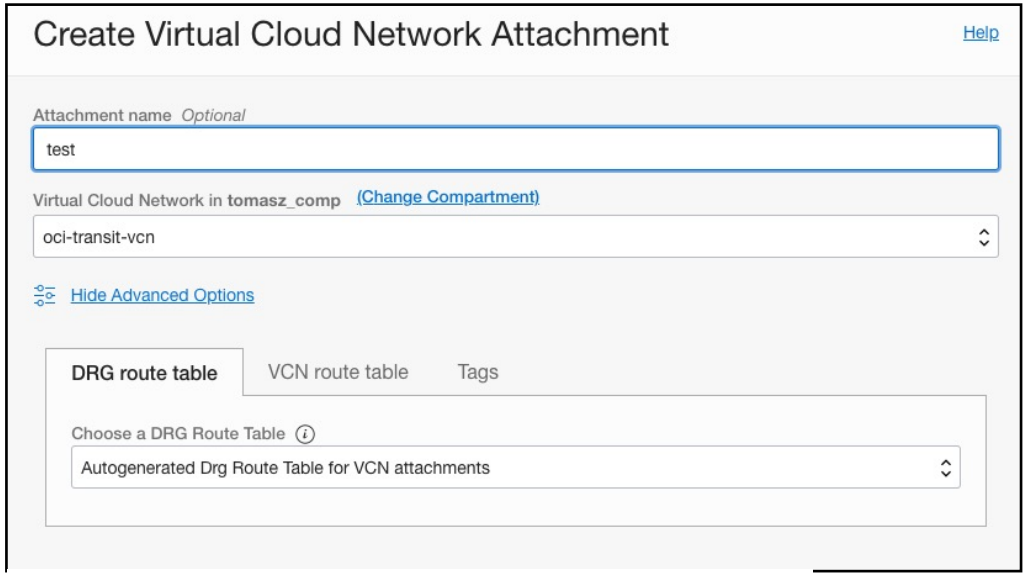
DRG Attachment Types and Route Tables

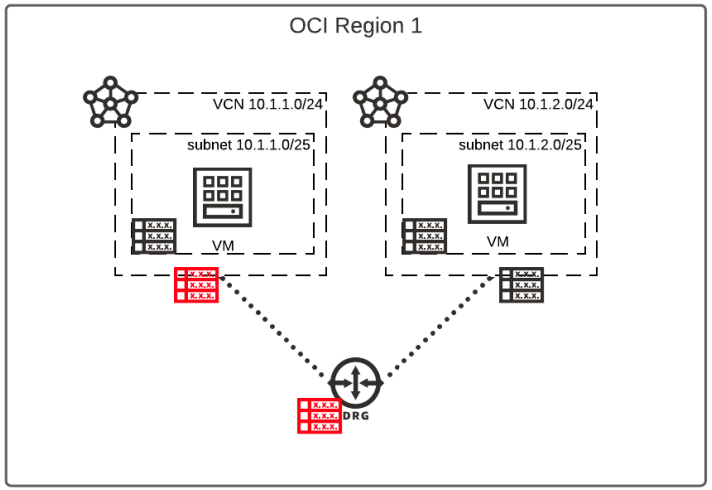
- VCN Attachments
- RPC Attachments (effectively “DRG peering”)
- IPsec Attachments
- FastConnect Attachments



DRG Attachment Types and Route Tables

- Each DRG attachment has an associated Route Table
  - Is used to route packets entering the DRG to their next hop
- DRG supports multiple Route Tables
- DRG route tables support automated Route Import and Export





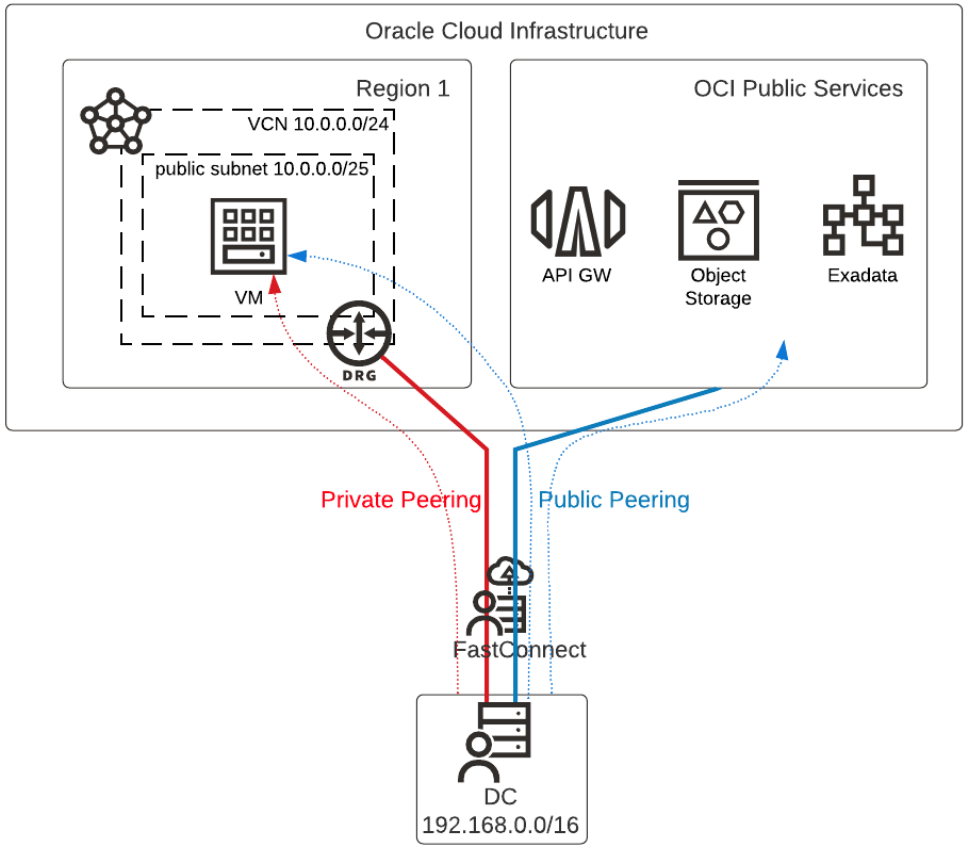
OCI DC to Cloud Access – Oracle FastConnect

Oracle Fast Connect is the private circuit you can build between your DC and OCI for high-throughput, low-latency, stable link.

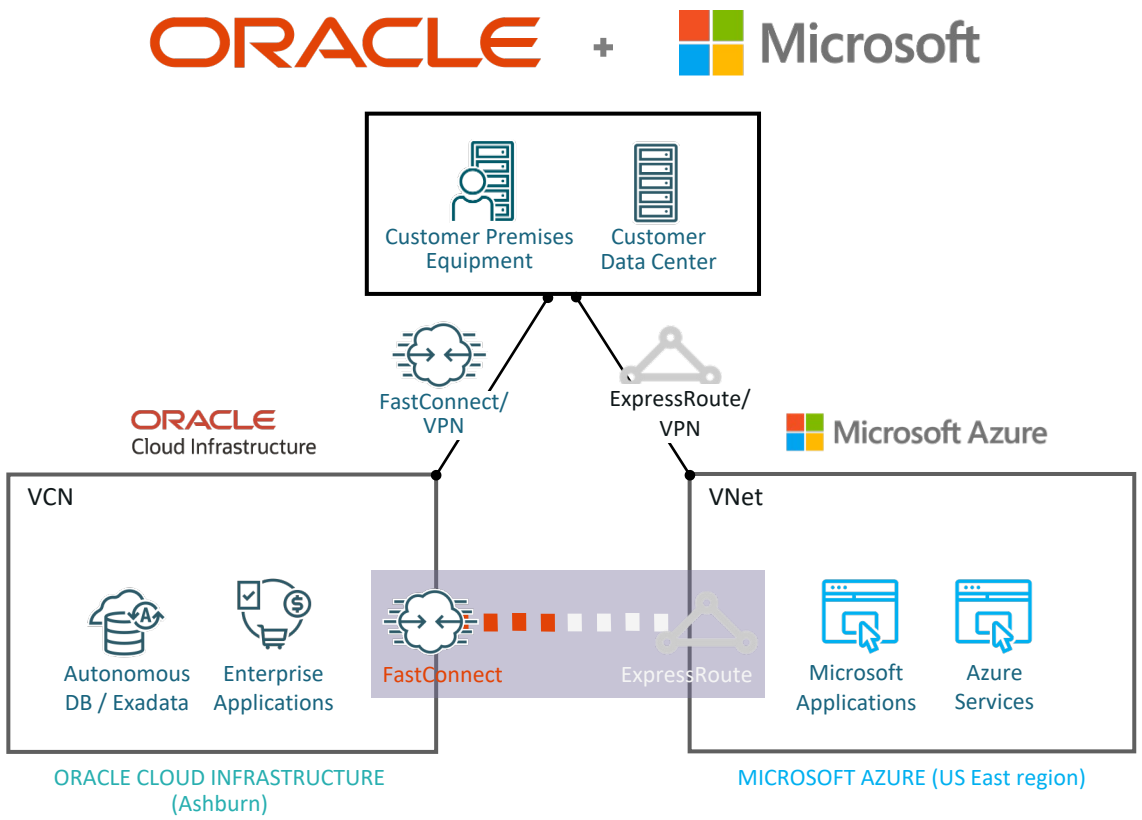
It supports two types of peerings:

- Private Peering – access to your VCN resources using Private IPs, over DRG

- Public Peering – access to OCI Public Services (e.g., Object Storage) or Public IPs in your OCI public subnets (e.g., a public VM)



Connectivity – OCI/Azure Interconnect



- ✓ Microsoft Azure and Oracle Cloud are **interconnected today**, so you can migrate and run mission-critical enterprise workloads across clouds
- ✓ **FastConnect and ExpressRoute** direct connection with 2 millisecond latency and no intermediate service provider required
- ✓ **Unified identity and access** management via single sign-on with automated user provisioning to easily manage resources across clouds
- ✓ **Collaborative support** of workloads across clouds, for example, custom and Oracle Applications on Azure with Oracle Database cloud services – connect best-in-class services across clouds
- ✓ **Available Now:** Ashburn, San Jose, Vinhedo, Toronto, London, Frankfurt, Amsterdam, Tokyo

OCI Networking Summary

Positives

- DRG 2.0 is significantly better than DRG 1.0
- It is mostly free
  - Egress data charges to the internet only after 10 TB monthly
  - FastConnect data is free in/out

Core Challenges

- It is not a multi-cloud solution
- Choice of Encryption (important for financial institutions etc.) – MACsec only on RPCs, not controlled by the customer

Other Challenges

- Limited visibility
  - You don't know exactly why the best route in DRG becomes the selected one
  - No traffic-level visibility
- No way to control AS path length when advertising CIDRs from DRG to external
- Configuration of the RTs in VCNs does not happen automatically (route export not supported for VCN)
  - Prone to errors
  - Difficult to troubleshoot
- Management at scale, even with route import/export, can be challenging

Next: MCNA