ORACLE
Cloud Infrastructure

Virtual Cloud Network Best Practices

Level 201

Jamal Arif

November 2018

ORACLE

Copyright © 2018, Oracle and/or its affiliates. All rights reserved.

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.

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. |

Objectives

- Best Practices VCN Design
- VCN and Subnet Sizing

- **Pre-requisites: Virtual Cloud Network Level 100**
- **Pre-requisites: Virtual Cloud Network Level 200**

Copyright © 2018, Oracle and/or its affiliates. All rights reserved.

Review: Virtual Cloud Network

- VCN network range once created can’t be modified and it is a contiguous IPv4 CIDR block
- VCN is a regional construct and currently subnets are specific to an AD (regional subnets are in roadmap)
- Subnets can have ONE Route Table and MULTIPLE (5*) Security Lists associated to it
- Security Lists support stateful and stateless rules
- All hosts within a VCN can route to all other hosts in a VCN, the route table defines what can be routed into and out of the VCN
- Allowable VCN size range is from /16 to /30 (VCN reserves the first two IP addresses and the last one in each subnet's CIDR)

Copyright © 2018, Oracle and/or its affiliates. All rights reserved.

VCN Best Practices

- Architect your networking infrastructure in a way to maximize use of Availability Domains for High Availability (ADs are fault tolerant and geographically distributed to sustain a natural disaster)
- For single AD applications, make use of Fault Domains
- Ensure VCN CIDR block does not overlap with other VCNs in Oracle Cloud Infrastructure (same/different regions) and with your organizations private IP network ranges
- Ensure not all IP addresses are allocated at once within a VCN or Subnet, instead plan to reserve some IP addresses for future use
- Divide your VCN network range across all ADs evenly
- Hosts that have similar routing requirements can use same routing tables across multiple availability domains for e.g. public hosts, private hosts, NAT instances etc.

Copyright © 2018, Oracle and/or its affiliates. All rights reserved.

VCN Best Practices (2)

- Ensure security lists are used as Firewalls to manage connectivity North-South (incoming/outgoing VCN traffic) and East-West (internal VCN traffic between multiple subnets), and is applied at a Subnet Level. All instances with in that subnet inherit all security rules in that SL.
- Private subnets are recommended to have individual route tables to control the flow of traffic within and outside of VCN.
- OCI recommends to use OCI IAM policies to restrict unauthorized users from managing virtual cloud network resources in your tenancy/compartment. Only network admins are allowed to ‘manage’ VCN resources, and other users can have least privilege policies (use, inspect, read)
- Use OCI tags to tag VCN resources (Route Tables, Security Lists, Subnets etc.) so that all resources are following organizational tagging/naming conventions

Copyright © 2018, Oracle and/or its affiliates. All rights reserved.

Example: VCN and Subnet Sizing

VCN CIDR Block – 10.0.0.0/16 – Extra Large IPv4 CIDR Block

- Divide in Four equal blocks – three for ADs and one spare
  - 10.0.0.0/18 → AD1
  - 10.0.64.0/18 → AD2
  - 10.0.128.0/18 → AD3
  - 10.0.192.0/18 → Extra
- With in each AD, we can have Public and Private Subnets
- Private instances are more prevalent than public instances so we should reserve a greater range for the private subnets.
  - 10.0.0.0/18 → AD1
    - 10.0.0.0/19 → AD1 Private Subnet
    - 10.0.32.0/19 → AD1 Public/spare
      - 10.0.32.0/20 → AD1 Public Subnet
      - 10.0.48.0/20 → AD1 Extra
  - Follow the same design pattern for all 3 Availability Domains.

Copyright © 2018, Oracle and/or its affiliates. All rights reserved.

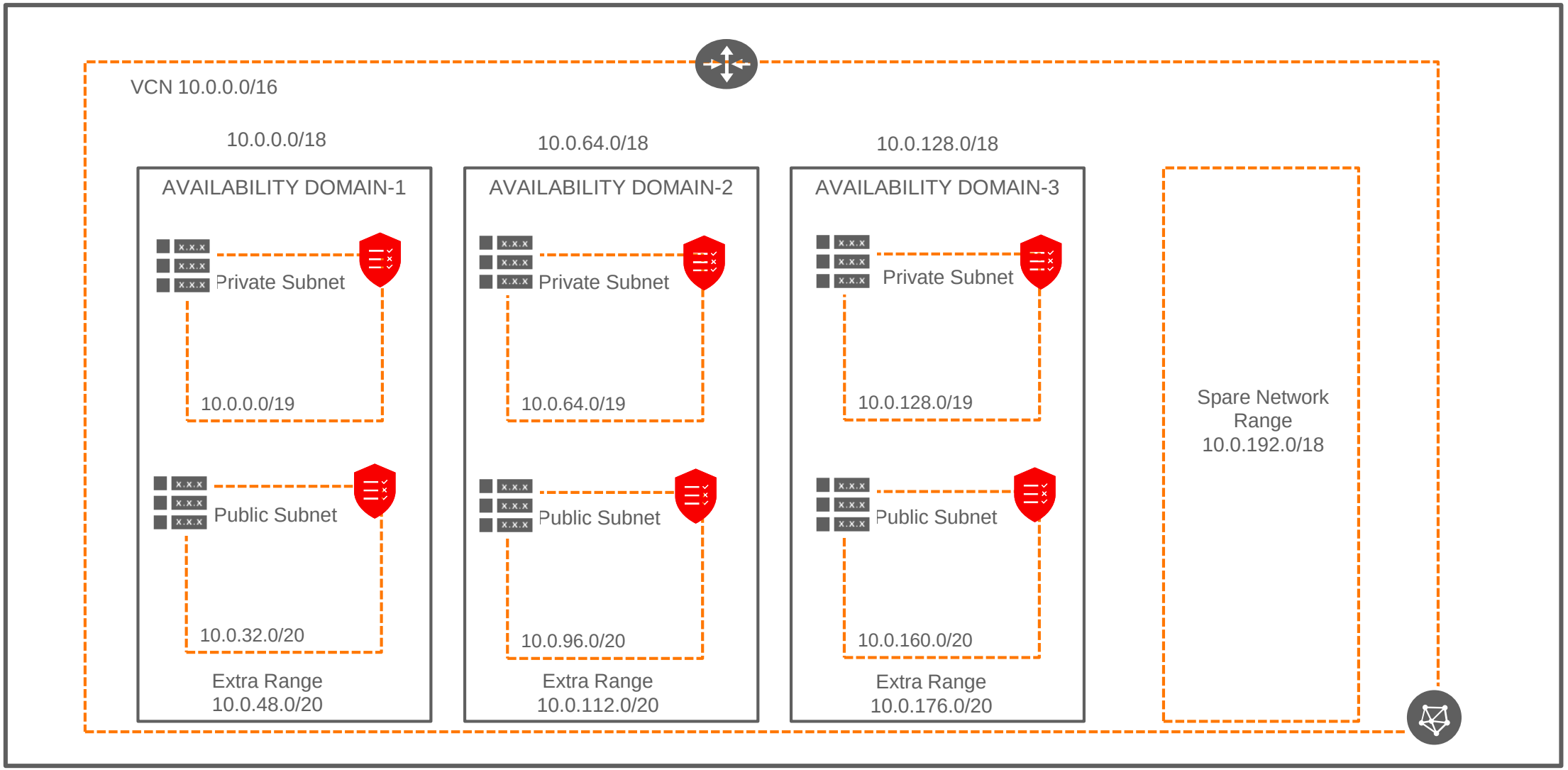
Example: VCN and Subnet Sizing

VCN Size	Netmask	Subnet Size	IPs/Subnet	Total Subnets	Total IPs
Small	/24	/27	29*	8	232
Medium	/20	/24	253*	16	4,048
Large	/18	/22	1021*	16	16,336
Extra Large	/16	/20	4093*	16	65,488

The first two IP addresses and the last one in each subnet's CIDR are reserved.

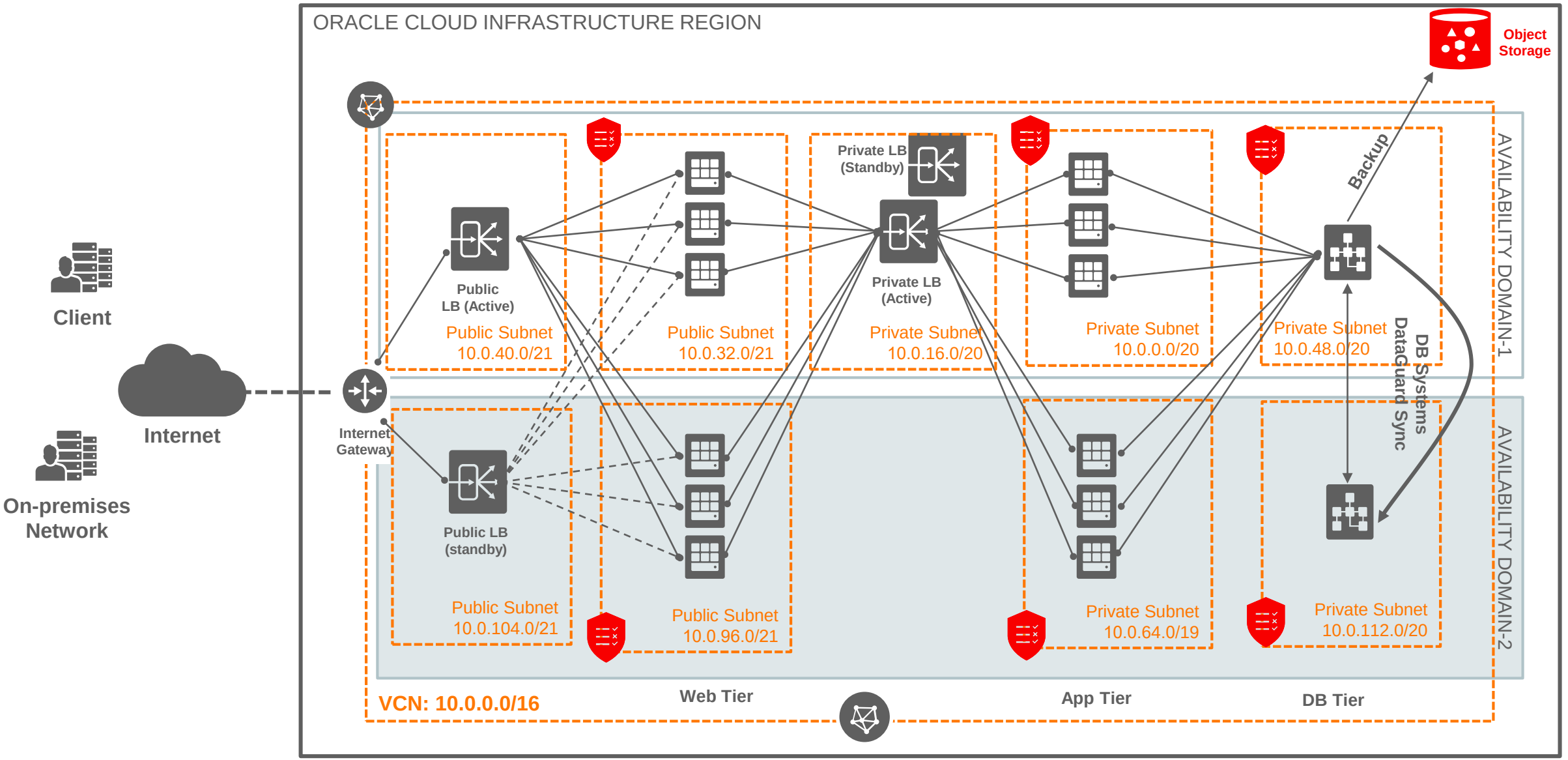
Copyright © 2018, Oracle and/or its affiliates. All rights reserved.

Example: VCN and Subnet Sizing



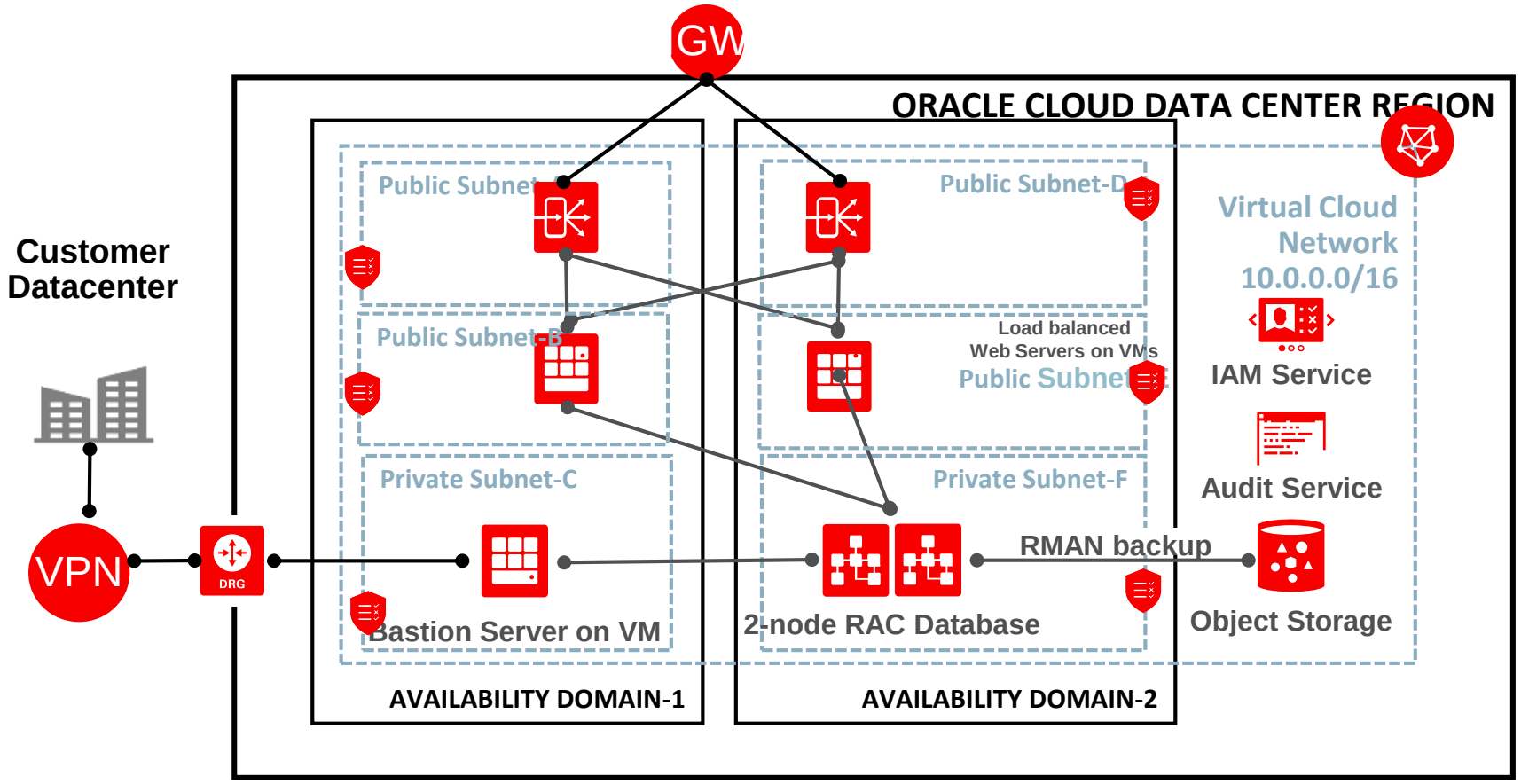
Copyright © 2018, Oracle and/or its affiliates. All rights reserved.

Example: Three Tier Application Architecture (Extra Large VCN size)



Copyright © 2018, Oracle and/or its affiliates. All rights reserved.

Example: Oracle Customer Architecture (1)



Copyright © 2018, Oracle and/or its affiliates. All rights reserved.

Summary

- Best Practices VCN Design
- VCN and Subnet Sizing

Copyright © 2018, Oracle and/or its affiliates. All rights reserved.

ORACLE®
Cloud Infrastructure

cloud.oracle.com/iaas

cloud.oracle.com/tryit