
Oracle Cloud Infrastructure Labs

Oracle Virtual Cloud Network Configuration

V2.0

ORACLE LAB BOOK | APRIL 2018



By
Oracle Sales Consulting Norway
Inge Os

ORACLE®



1. Disclaimer

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.



2. Overview

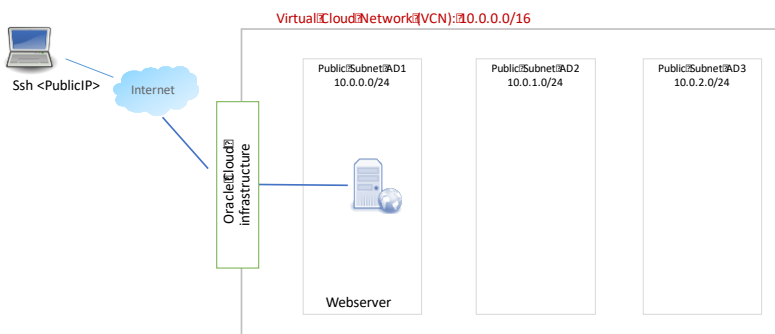
Lab Overview

The lab exercises are designed to complement your training, reinforcing the key concepts by applying and demonstrating what you learned in the presentation sessions. This lab book is comprised of individual exercises. These exercises allow you to get first hands-on exposure working with the Oracle Cloud infrastructure Services (OCI) product using a demo environment, where you will see how key features and functionality are deployed in the software. Using what you learn in the presentations and individual exercises working with the software, you will collaborate as a team in developing and delivering practice presentations.

Create a Virtual Cloud Network (VCN)

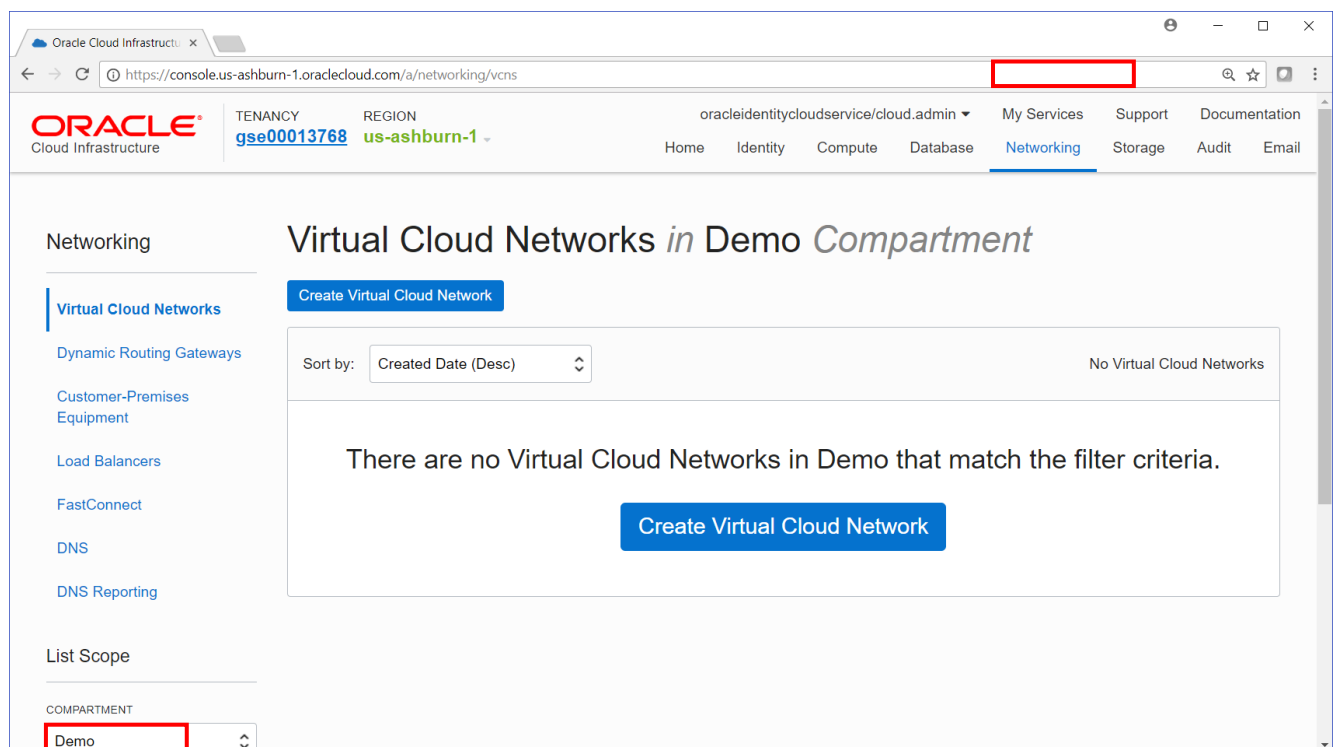
A Virtual Cloud Network (VCN) is a virtual version of a traditional network—including subnets, route tables, and gateways—on which your compute instances run. Customers can bring their network topology to the cloud with VCN. Creating a VCN involves a few key aspects such as:

- Allocate a private IP block for the cloud (CIDR range for the VCN). Customers can bring their own RFC1918 IP addresses.
- Create Subnets by partitioning the CIDR range into smaller networks (sub networks for front end, back end, database)
- Create an optional Internet Gateway to connect VCN subnet with Internet. Instances created in this subnet will have a public IP address.
- Create Route table with route rules for Internet access
- Create Security Group to allow relevant ports for ingress and egress access



Creating a VCN involves allocating a CIDR range (IP address block) for the network, creating a Route Table with custom route rules and path to Internet, carving out a subnet from the IP address block allocated to the VCN.

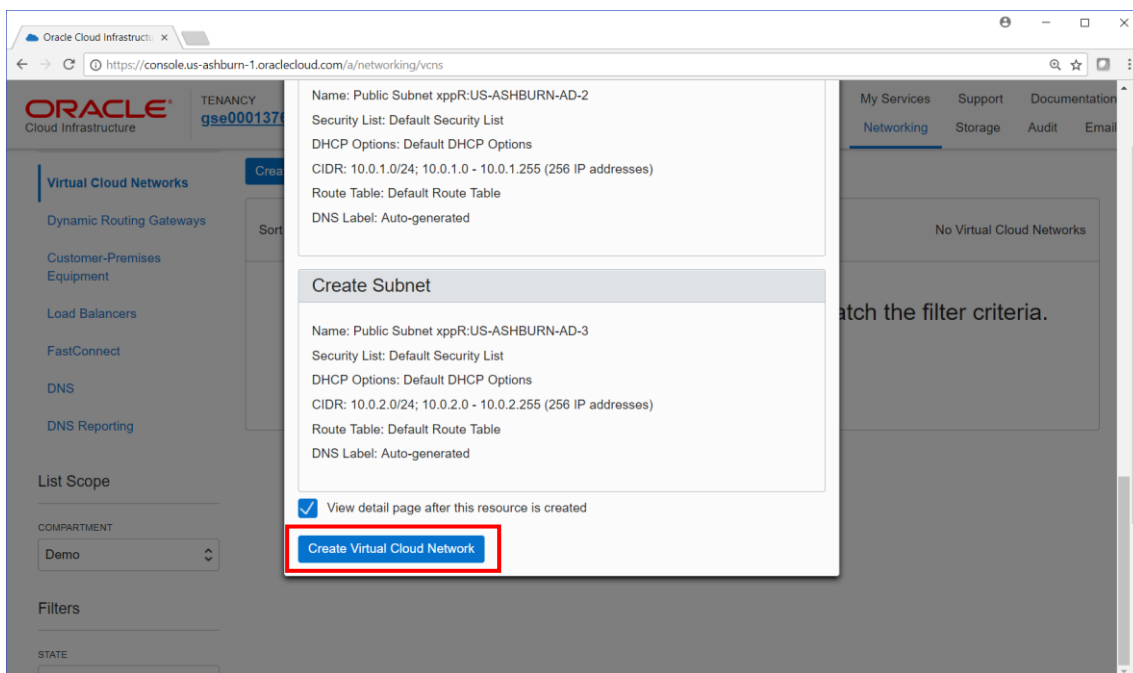
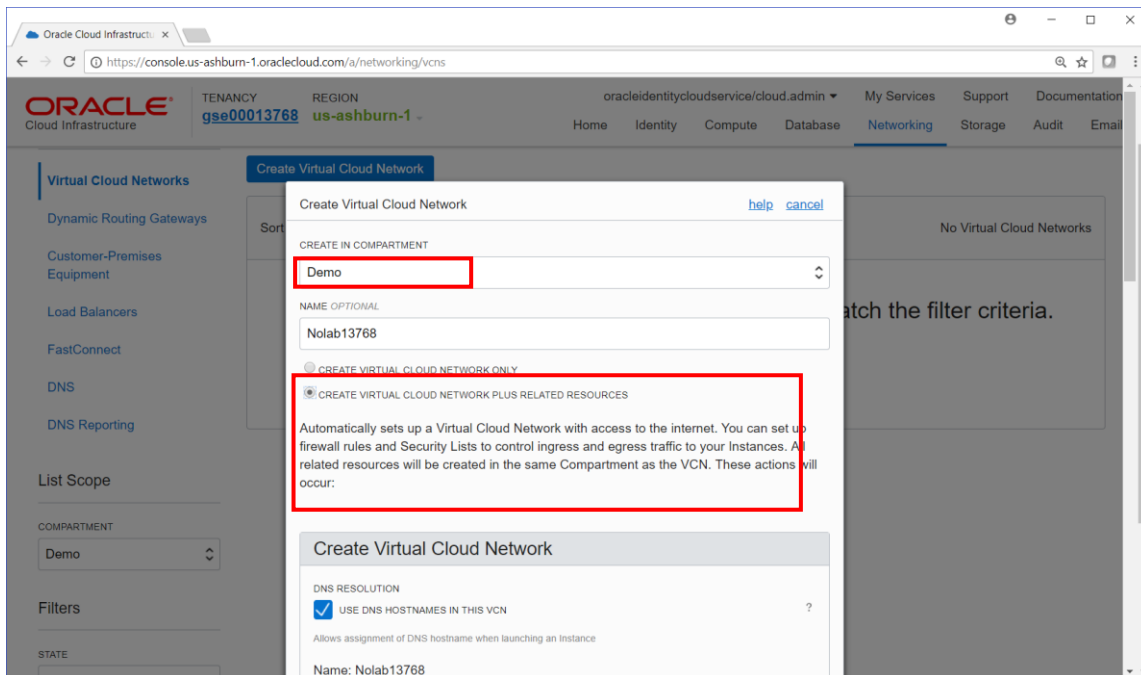
1. After you login, navigate to the networking tab and select Virtual Cloud Networks.




Lab performed with allocated Oracle Demo Account, STOP and make sure you're in the correct compartment.

Any oracle supplied demo accounts uses the demo compartment.


2. Click on the create Virtual Cloud Network button, assuming you're in the correct compartment number. The steps below shows the demo compartment, but you should select your specific compartment as per above.
3. Create a Cloud Network by specifying a name for your VCN and selecting the "Create VIRTUAL CLOUD NETWORK PLUS RELATED RESOURCES" option. This will create a VCN, Subnets, Routing Table, Security Groups and Internet Gateway using a 10.0.0.0/16 CIDR range. Scroll to the bottom of the screen and click "create Virtual Cloud Network" button.
4. Name your VNC with your compartment number ie. NOLABCxx



- Once the VCN is created, navigating to list of VCN's, you can see the "NOLABCxx", which you just created in the step above.

Sort by: Created Date (Desc)		Displaying 1 Virtual Cloud Networks			
 AVAILABLE	Nolab13768 OCID: ...p3yp5a Show Copy	CIDR Block: 10.0.0.0/16	Default Route Table: Default Route Table for Nolab13768	DNS Domain Name: nolab13768... Show Copy	Created: Tue, 17 Apr 2018 08:51:59 GMT




6. Click on the NOLABCxx link above and it displays the three subnets within this network.



Nolab13768
[Terminate](#) [Apply Tag\(s\)](#)
 VCN Information [Tags](#)
 CIDR Block: 10.0.0.0/16
 Compartment: Demo
 Created: Tue, 17 Apr 2018 08:51:59 GMT
 OCID: ...p3yp5a [Show](#) [Copy](#)
 Default Route Table: [Default Route Table for Nolab13768](#)
 DNS Domain Name: nolab13768... [Show](#) [Copy](#)

Resources
 Subnets (3)
 Route Tables (1)
 Internet Gateways (1)
 Dynamic Routing Gateways (0)
 Security Lists (1)
 DHCP Options (1)
 Local Peering Gateways (0)
 List Scope
 COMPARTMENT
 Demo


Subnets in Demo Compartment
[Create Subnet](#)
 Sort by: Created Date (Desc) Displaying 3 Subnets

 AVAILABLE	Public Subnet xppR-US-ASHBURN-AD-3 OCID: ...qyma Show Copy	CIDR Block: 10.0.2.0/24 Virtual Router MAC Address: 00:00:17:EE:B3:FD	Availability Domain: xppR-US-ASHBURN-AD-3 DNS Domain Name: sub6417085... Show Copy Subnet Access: Public Subnet	Route Table: Default Route Table for Nolab13768 Security Lists: Default Security List for Nolab13768	DHCP Options: Default DHCP Options for Nolab13768	...
 AVAILABLE	Public Subnet xppR-US-ASHBURN-AD-2 OCID: ...vockdq Show Copy	CIDR Block: 10.0.1.0/24 Virtual Router MAC Address: 00:00:17:EE:B3:FD	Availability Domain: xppR-US-ASHBURN-AD-2 DNS Domain Name: sub6417085... Show Copy Subnet Access: Public Subnet	Route Table: Default Route Table for Nolab13768 Security Lists: Default Security List for Nolab13768	DHCP Options: Default DHCP Options for Nolab13768	...
 AVAILABLE	Public Subnet xppR-US-ASHBURN-AD-1 OCID: ...vockdq Show Copy	CIDR Block: 10.0.0.0/24 Virtual Router MAC Address: 00:00:17:EE:B3:FD	Availability Domain: xppR-US-ASHBURN-AD-1 DNS Domain Name: sub6417085... Show Copy Subnet Access: Public Subnet	Route Table: Default Route Table for Nolab13768 Security Lists: Default Security List for Nolab13768	DHCP Options: Default DHCP Options for Nolab13768	...

7. Next step is to configure the security lists (aka virtual firewall).

Configure the Next, we are going to edit the security Lists in this VCN, since the Apache server will need access to port 80 (port 443 is optional) for ingress traffic. Click on the Security Lists tab on left.

Other traffic needed for the VM will be tunneled through ssh. Click on the Default Security List for NOLABCxx and it displays the default security rules for this VCN.



Nolab13768

[Terminate](#)
[Apply Tag\(s\)](#)

VCN Information

Tags

CIDR Block: 10.0.0.0/16
 Compartment: Demo
 Created: Tue, 17 Apr 2018 08:51:59 GMT

OCID: ...p3yp5a [Show](#) [Copy](#)
 Default Route Table: [Default Route Table for Nolab13768](#)
 DNS Domain Name: nolab13768... [Show](#) [Copy](#)


Resources

- Subnets (3)
- Route Tables (1)
- Internet Gateways (1)
- Dynamic Routing Gateways (0)
- Security Lists (1)**
- DHCP Options (1)


Security Lists *in Demo Compartment*

Displaying 1 Security Lists

[Create Security List](#)

 <p>Default Security List for Nolab13768</p> <p>OCID: ...npu7q Show Copy</p> <p>Created: Tue, 17 Apr 2018 08:51:59 GMT</p>	...
--	-----

8. Add port 80 and 443 as shown below by clicking on “Edit All Rules”.



Default Security List for Nolab13768

[Edit All Rules](#)
[Terminate](#)
[Apply Tag\(s\)](#)

Security List Information

Tags

OCID: ...npu7q [Show](#) [Copy](#)
 Created: Tue, 17 Apr 2018 08:51:59 GMT

Instance traffic is controlled by firewall rules on each Instance in addition to this Security List

Resources

- Ingress Rules (3)**
- Egress Rules (1)

Ingress Rules

Stateless Rules

No Ingress Rules

There are no stateless Ingress Rules for this Security List.

Stateful Rules				
Source: 0.0.0.0/0	IP Protocol: TCP	Source Port Range: All	Destination Port Range: 22	Allows: TCP traffic for ports: 22 SSH Remote Login Protocol
Source: 0.0.0.0/0	IP Protocol: ICMP	Type and Code: 3, 4		Allows: ICMP traffic for: 3, 4 Destination Unreachable: Fragmentation Needed and Don't Fragment was Set
Source: 10.0.0.0/16	IP Protocol: ICMP	Type and Code: 3		Allows: ICMP traffic for: 3 Destination Unreachable

9. Click add rules

Edit Security List Rules [help](#) [cancel](#)

SECURITY LIST NAME
Default Security List for NOLAB13768

Allow Rules for Ingress

<input checked="" type="checkbox"/>	<input type="checkbox"/>	SOURCE CIDR 0.0.0.0/0	IP PROTOCOL TCP	SOURCE PORT RANGE (OPTIONAL) All	DESTINATION PORT RANGE (OPTIONAL) 22
STATELESS (more information) Allows TCP traffic for ports: 22 SSH Remote Login Protocol					
<input checked="" type="checkbox"/>	<input type="checkbox"/>	SOURCE CIDR 0.0.0.0/0	IP PROTOCOL ICMP	TYPE AND CODE (OPTIONAL) 3, 4	
STATELESS (more information) Allows ICMP traffic for: 3, 4 Destination Unreachable: Fragmentation Needed and Don't Fragment was Set					
<input checked="" type="checkbox"/>	<input type="checkbox"/>	SOURCE CIDR 10.0.0.0/16	IP PROTOCOL ICMP	TYPE AND CODE (OPTIONAL) 3	
STATELESS (more information) Allows ICMP traffic for: 3 Destination Unreachable					

[+ Add Rule](#)

Allow Rules for Egress

<input checked="" type="checkbox"/>	<input type="checkbox"/>	DESTINATION CIDR 0.0.0.0/0	IP PROTOCOL All Protocols		
-------------------------------------	--------------------------	-------------------------------	------------------------------	--	--

10. Add the CIDR ranges 0.0.0.0/0 (port 80, 443).

<input checked="" type="checkbox"/>	<input type="checkbox"/>	SOURCE CIDR 0.0.0.0/0	IP PROTOCOL TCP	SOURCE PORT RANGE (OPTIONAL) All	DESTINATION PORT RANGE (OPTIONAL) 80
STATELESS (more information) Specified IP addresses: 0.0.0.0-255.255.255.255 (4,294,967,296 IP addresses) Allows TCP traffic for ports: 80 HTTP					
<input checked="" type="checkbox"/>	<input type="checkbox"/>	SOURCE CIDR 0.0.0.0/0	IP PROTOCOL TCP	SOURCE PORT RANGE (OPTIONAL) All	DESTINATION PORT RANGE (OPTIONAL) 443
STATELESS (more information) Specified IP addresses: 0.0.0.0-255.255.255.255 (4,294,967,296 IP addresses) Allows TCP traffic for ports: 443 HTTPS					

[+ Add Rule](#)

11. Click on Save Security List Rules.

The screenshot displays the Oracle Cloud console interface for configuring security list rules. It shows two rules: one for Ingress (allowing TCP traffic on port 443) and one for Egress (allowing all protocols to 0.0.0.0/0). The 'Save Security List Rules' button at the bottom is highlighted with a red rectangular box.

Key Takeaway:

- ✓ Customers can bring their Private IP address block from on-premises datacenter. This is very valuable as the customer can preserve their network topology.'

You have now configured the VCN to accept incoming SSH, HTTP and HTTPS traffic on port 22, 80 and 443