Oracle Cloud Infrastructure Practice Load Balancer Service

V1.2

ORACLE LAB BOOK | APRIL 2018

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.

Table of Contents

Overview

The Load Balancing Service provides automated traffic distribution from one entry point to multiple servers within your Virtual Cloud Network (VCN). The service offers a Public load balancer with a public IP address, provisioned bandwidth, and high availability. The Load Balancing Service provisions the public IP address across two subnets within a VCN to ensure accessibility even during an Availability Domain outage.

In this practice, you create a simple public load balancer and verify it with a basic web server application.

Pre-Requisites

- Oracle Cloud Infrastructure account credentials (User, Password, and Tenant)

Practice 6-1: Signing in to the Console

Overview

In this practice, you sign in to the Oracle Cloud Infrastructure console using your credentials.

Assumptions

Note: Some of the UIs might look a little different than the screenshots included in the instructions, but students can still use the instructions to complete the hands-on labs.

Before You Begin

To sign in to the Console, you need the following:

- Tenant, User name and Password
- URL for the Console: https://console.us-ashburn-1.oraclecloud.com/
- Any browser from the supported browsers list (Recommended)

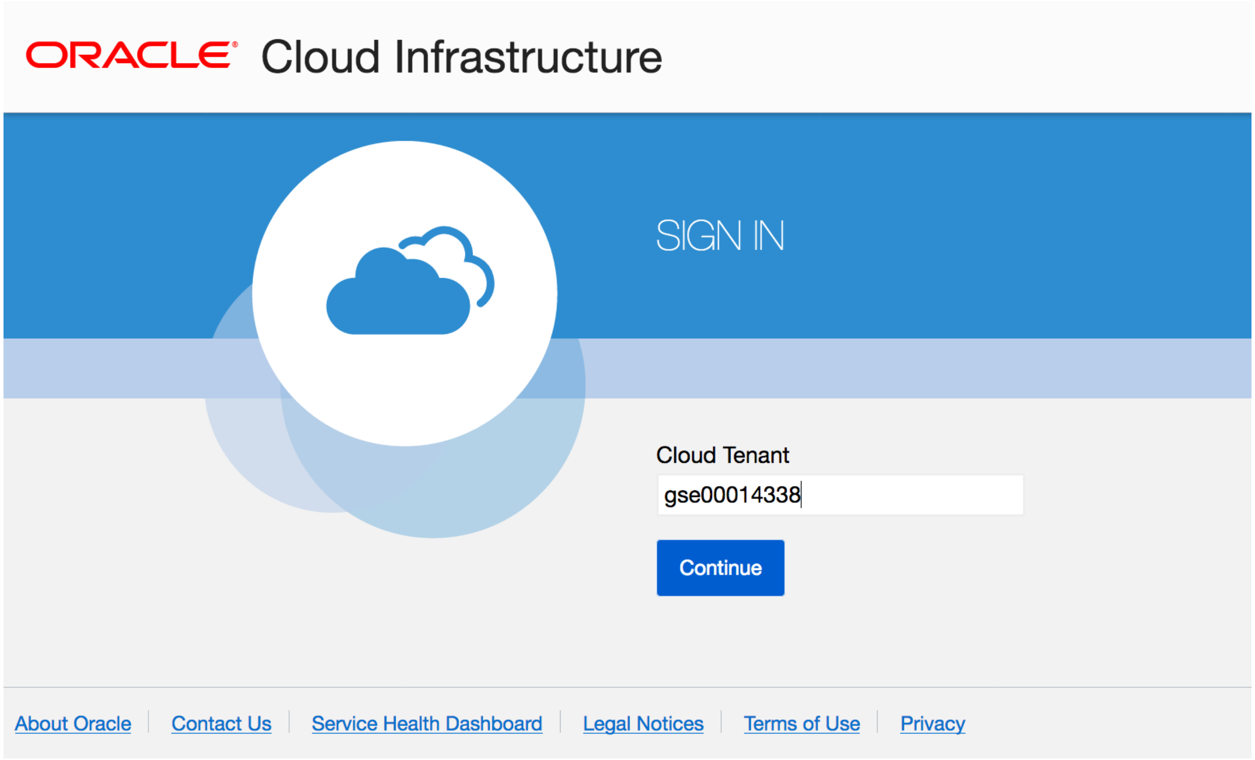
Note:

- **For this lab we use *cloud.admin* and <your-name@oracle.com> as the user name to demonstrate the scenarios. You must use your cloud.admin when you perform these tasks.**
- Oracle Cloud Infrastructure supports the latest versions of Google Chrome, Firefox and Internet Explorer 11.
- When you are provisioned, you will receive a customized URL for your organization. For example, https://console.us-ashburn-1.oraclecloud.com*?tenant=<your-tenant-id>*
- If you omit the tenant argument, the system will ask you to input your tenancy before you can log in.

Duration: 5 minutes

Tasks

1. Sign In
    a. Open a supported browser and go to the Console URL. For example, https://console.us-ashburn-1.oraclecloud.com.
    b. Enter your tenant name: <Tenant> and click Continue.



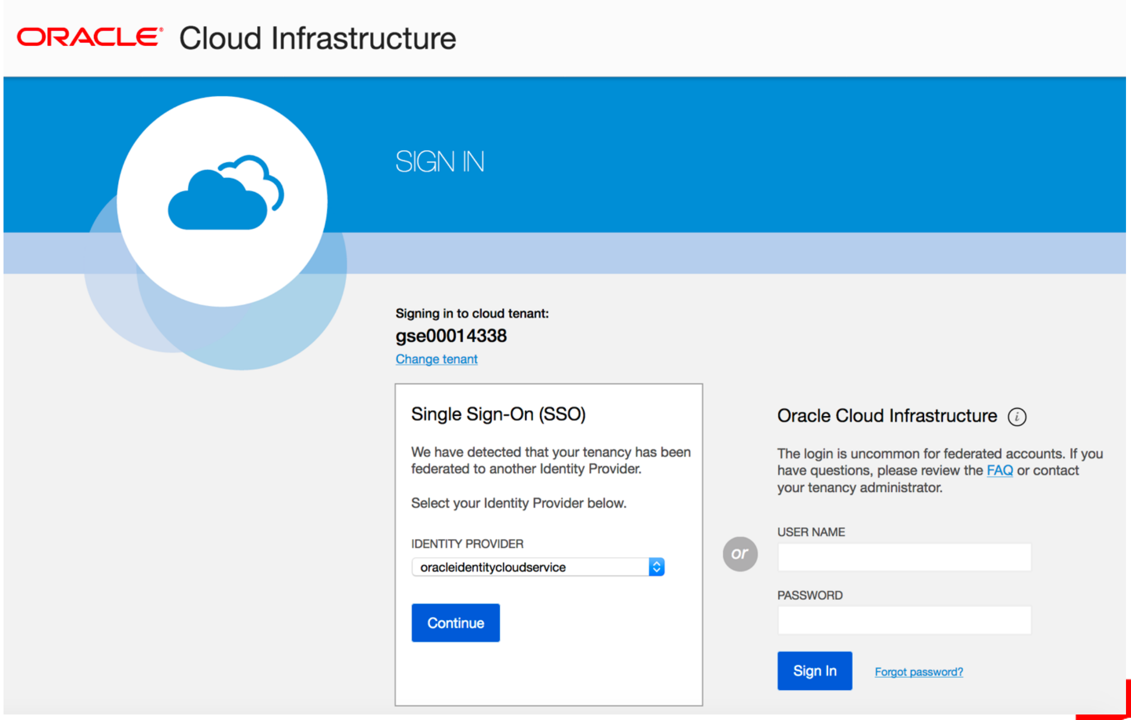
ORACLE Cloud Infrastructure

SIGN IN

Cloud Tenant

gse00014338

c. Oracle Cloud Infrastructure is integrated with Identity Cloud Services, you will see a screen validating your Identity Provider. You can just click **Continue**.



ORACLE Cloud Infrastructure

SIGN IN

Signing in to cloud tenant:

gse00014338

Change tenant

Single Sign-On (SSO)

We have detected that your tenancy has been federated to another Identity Provider.

Select your Identity Provider below.

IDENTITY PROVIDER

oracleidentitycloudservice

Oracle Cloud Infrastructure

The login is uncommon for federated accounts. If you have questions, please review the FAQ or contact your tenancy administrator.

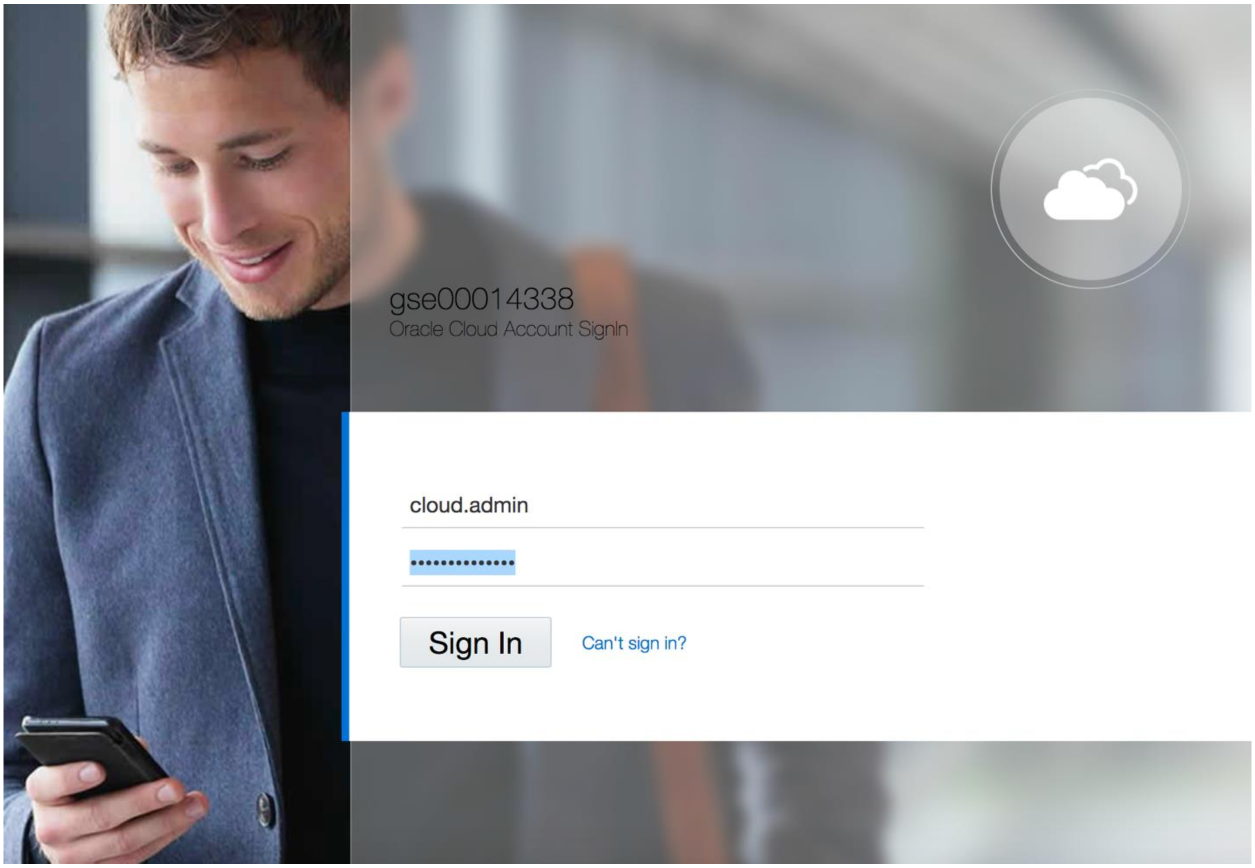
USER NAME

PASSWORD

d. Enter your user name and password

Username: cloud.admin

Password: <instructor will provide password>



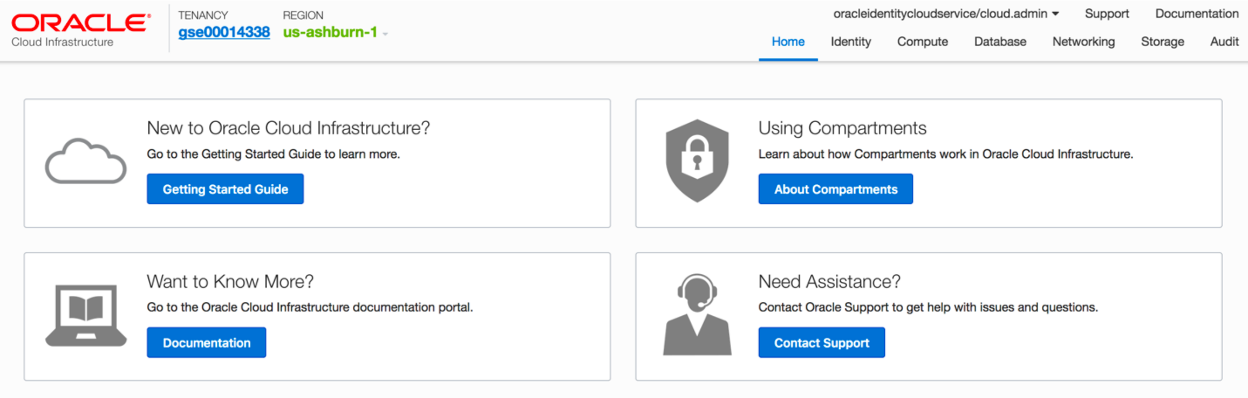
gse00014338

Oracle Cloud Account SignIn

cloud.admin

••••••••••••••

When you sign in to the Console, the home page is displayed.



New to Oracle Cloud Infrastructure?

Go to the Getting Started Guide to learn more.

Using Compartments

Learn about how Compartments work in Oracle Cloud Infrastructure.

Want to Know More?

Go to the Oracle Cloud Infrastructure documentation portal.

Need Assistance?

Contact Oracle Support to get help with issues and questions.

The home page gives you quick links to the documentation and to Oracle Support.

Practice 6-2: Create Virtual Cloud Network (VCN)

Overview

When you work with Oracle Cloud Infrastructure, one of the first steps is to set up a Virtual Cloud Network (VCN) for your cloud resources. This practice gives you an overview of Network Service components and a typical scenario for using a VCN.

For an instance in a given subnet to have direct access to the Internet, it must have the following networking components:

- The VCN must have an Internet Gateway that is enabled
- The subnet must have a route rule that directs traffic to the gateway and must be a Public Subnet
- The subnet must have security list rules that allow the traffic (and each instance's firewall must allow the traffic)
- Each instance must have a public IP address

Before You Begin

You need the following:

- User name, password and compartment
- URL previously used for signing into the Console: (https://console.us-ashburn-1.oraclecloud.com/)

Note: Some of the UIs might look a little different than the screenshots included in the instructions, but students can still use the instructions to complete the hands-on labs.

Duration: 10 minutes

Tasks

2. Create a Cloud Network - **Public Subnets**

   Create a VCN for Load Balancer with the following components:

   – One public subnet per Availability Domain

   – The default security list

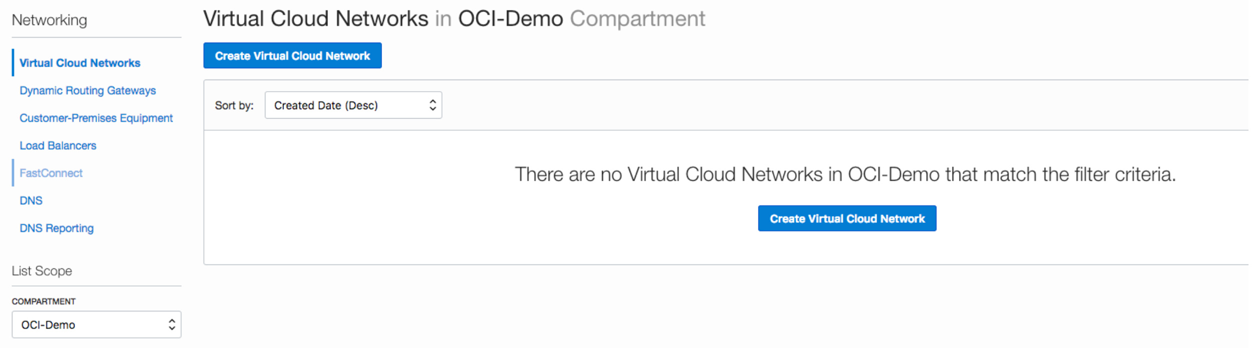
   – The default set of DHCP options

   Note: You can launch one or more compute instances in a subnet. Each instance gets both a public and private IP address. The launch instance dialog now has a check box for choosing whether the instance has a public IP address.

   You can communicate with the instances over the Internet via the public IP address from your on-premises network.

   a. Open the Console, click **Networking**.

   b. Select a compartment on the left that you have permission to work in.



Virtual Cloud Networks in OCI-Demo Compartment

Sort by: Created Date (Desc)

There are no Virtual Cloud Networks in OCI-Demo that match the filter criteria.

COMPARTMENT: OCI-Demo

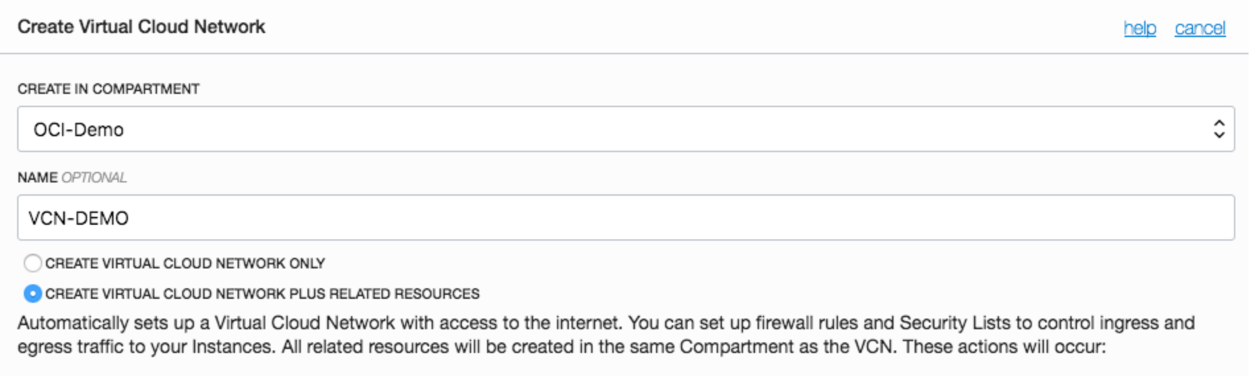
c. Click **Create Virtual Cloud Network**.

d. Enter the following details:

1) **Create in Compartment:** This field defaults to the currently selected compartment. Select the compartment you want to create the VCN in, if not already selected.

2) **Name:** Enter a name for your cloud network (for example, LB-DEMO).

Note: Enter a friendly name for the cloud network. It doesn't have to be unique, and it cannot be changed later in the Console (but you can change it with the API).



Create Virtual Cloud Network

CREATE IN COMPARTMENT: OCI-Demo

NAME *OPTIONAL*: VCN-DEMO

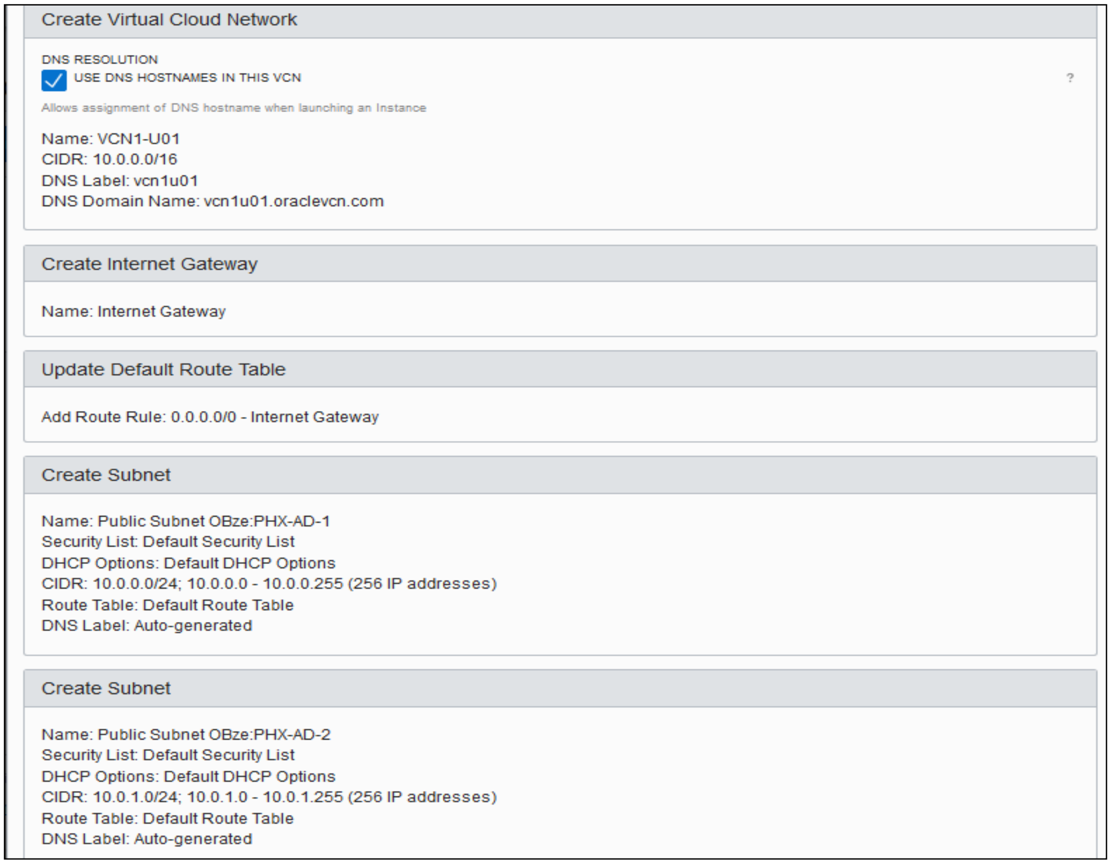
○ CREATE VIRTUAL CLOUD NETWORK ONLY

● CREATE VIRTUAL CLOUD NETWORK PLUS RELATED RESOURCES

Automatically sets up a Virtual Cloud Network with access to the internet. You can set up firewall rules and Security Lists to control ingress and egress traffic to your Instances. All related resources will be created in the same Compartment as the VCN. These actions will occur:

e. Select **Create Virtual Cloud Network plus related resources**. The dialog box expands to list the items that will be created with your cloud network.

Note: This option is the quickest way to get a working cloud network in the fewest steps.



Create Virtual Cloud Network

DNS RESOLUTION

☑ USE DNS HOSTNAMES IN THIS VCN

Allows assignment of DNS hostname when launching an Instance

Name: VCN1-U01
CIDR: 10.0.0.0/16
DNS Label: vcn1u01
DNS Domain Name: vcn1u01.oraclevcn.com

Create Internet Gateway

Name: Internet Gateway

Update Default Route Table

Add Route Rule: 0.0.0.0/0 - Internet Gateway

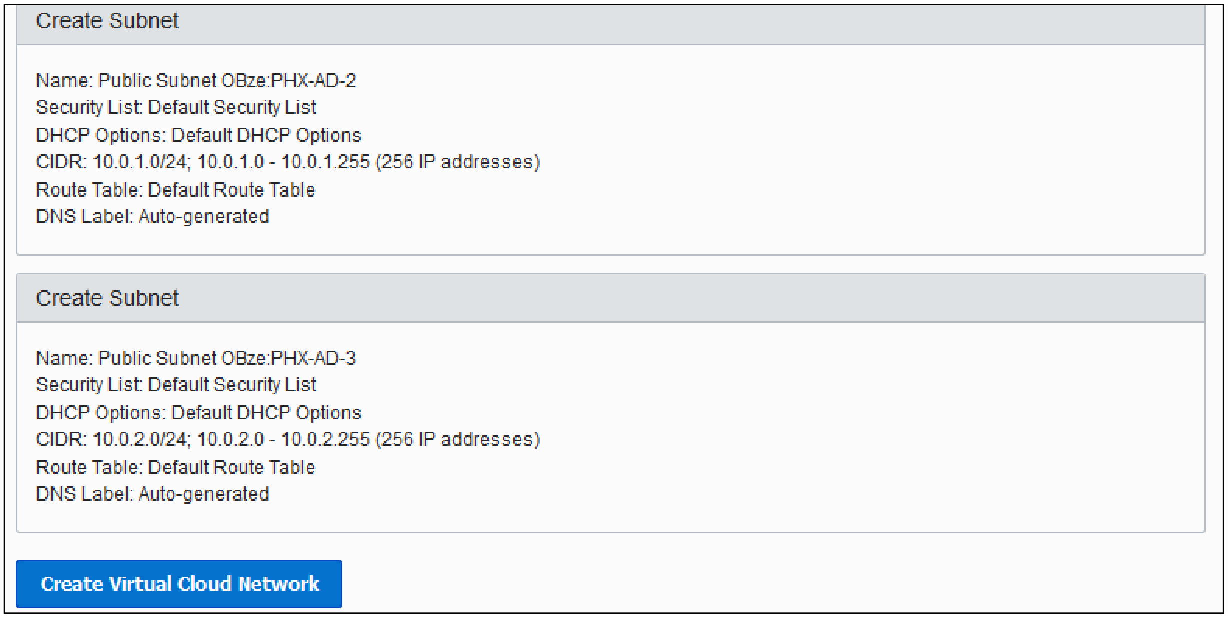
Create Subnet

Name: Public Subnet OBze:PHX-AD-1
Security List: Default Security List
DHCP Options: Default DHCP Options
CIDR: 10.0.0.0/24; 10.0.0.0 - 10.0.0.255 (256 IP addresses)
Route Table: Default Route Table
DNS Label: Auto-generated

Create Subnet

Name: Public Subnet OBze:PHX-AD-2
Security List: Default Security List
DHCP Options: Default DHCP Options
CIDR: 10.0.1.0/24; 10.0.1.0 - 10.0.1.255 (256 IP addresses)
Route Table: Default Route Table
DNS Label: Auto-generated

f. Scroll to the bottom of the dialog box and click **Create Virtual Cloud Network**.



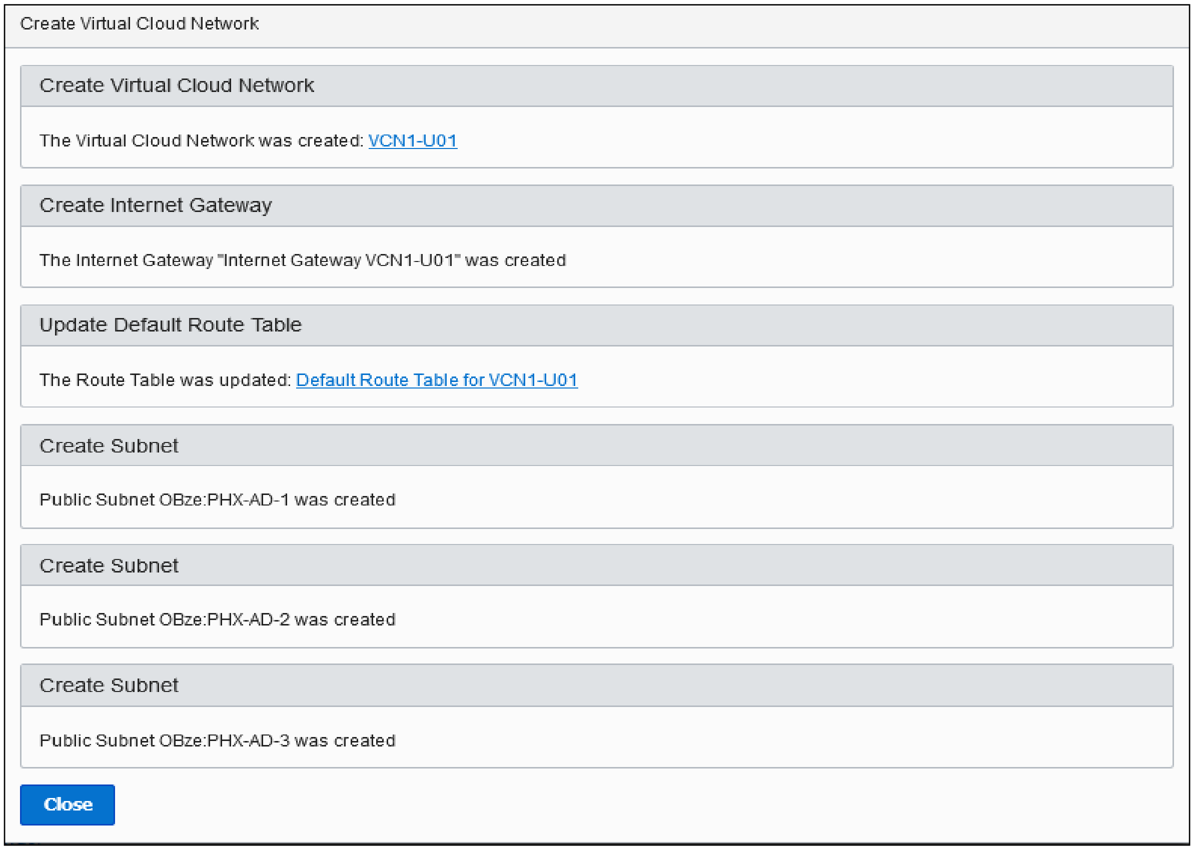
Create Subnet

Name: Public Subnet OBze:PHX-AD-2
Security List: Default Security List
DHCP Options: Default DHCP Options
CIDR: 10.0.1.0/24; 10.0.1.0 - 10.0.1.255 (256 IP addresses)
Route Table: Default Route Table
DNS Label: Auto-generated

Create Subnet

Name: Public Subnet OBze:PHX-AD-3
Security List: Default Security List
DHCP Options: Default DHCP Options
CIDR: 10.0.2.0/24; 10.0.2.0 - 10.0.2.255 (256 IP addresses)
Route Table: Default Route Table
DNS Label: Auto-generated

g. A confirmation page displays the details of the cloud network that you just created.



Create Virtual Cloud Network

Create Virtual Cloud Network

The Virtual Cloud Network was created: VCN1-U01

Create Internet Gateway

The Internet Gateway "Internet Gateway VCN1-U01" was created

Update Default Route Table

The Route Table was updated: Default Route Table for VCN1-U01

Create Subnet

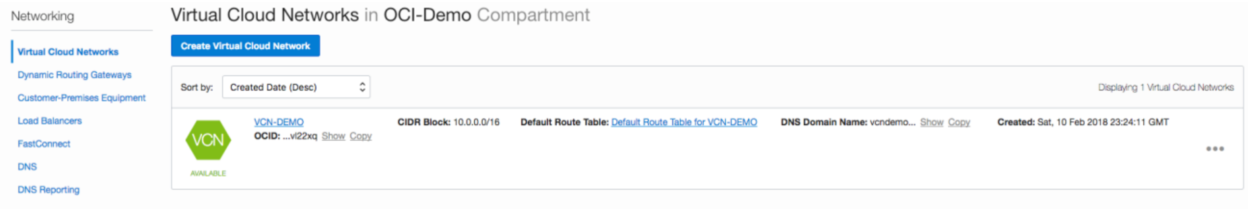
Public Subnet OBze:PHX-AD-1 was created

Create Subnet

Public Subnet OBze:PHX-AD-2 was created

Create Subnet

Public Subnet OBze:PHX-AD-3 was created



Virtual Cloud Networks in OCI-Demo Compartment

Sort by: Created Date (Desc)

Displaying 1 Virtual Cloud Networks

VCN-DEMO
OCID: ...vi22xq Show Copy
CIDR Block: 10.0.0.0/16
Default Route Table: Default Route Table for VCN-DEMO
DNS Domain Name: vcndemo... Show Copy
Created: Sat, 10 Feb 2018 23:24:11 GMT

For example, the cloud network above has the following resources and characteristics:

- CIDR block range of 10.0.0.0/16
- An Internet Gateway
- A route table with a default route rule to enable traffic between VCN and the Internet Gateway
- A default security list that allows specific ingress traffic to and all egress traffic from the instance
- A public subnet in each Availability Domain
- The VCN will automatically use the Internet and VCN Resolver for DNS

Practice 6-3: Creating Two Web Servers

Overview

You will create two web servers that will work as backend servers for your Public Load Balancer.

Duration: 10 minutes

Tasks

1. Launch Two Instances

   This example uses a VM.Standard2.1 shape.

   a. In the Console, click **Compute**.

   b. Click **Launch Instance**.

   c. In the **Launch Instance** dialog box, enter the following:

      1) **Name:** Enter a name (for example: **Webserver1**).

      2) **Availability Domain:** Select the first Availability Domain in the list, AD-1.

      3) **Image:** Select the Oracle-Linux-7.x image. (The image name has the latest patch date appended to it.)

      4) **Shape:** Select VM Standard2.1.

      5) **Virtual Cloud Network:** Select the cloud network that you created (**LB_Network**).

      6) **Subnet:** Select the public subnet LB Subnet 1 in Availability Domain 1.

      7) **DNS name:** Leave blank.

      8) **SSH Keys:** Use the pub key generated to create this instance. NOTE: Make sure to use the keys that you have access too as you will use this key to ssh into the instances in next steps.

   d. Click **Launch Instance**.

   e. Repeat the previous steps, but this time enter the name **Webserver2**, select **Availability Domain AD-2, LB_Network** for the VCN, and **LB Subnet 2 for the subnet**.

2. Start a Web Application on Each Instance. Use ssh to access the instances and start the web server by executing the following commands on each instance:

   Note: You can use two separate ssh sessions to execute these commands on both instances in parallel to save time.

   a.
   ```
   ssh -i </path/privateKey>  opc@<PublicIP_Address>
   ```

   b. Run yum update:
   ```
   $> sudo yum -y update
   ```

   c. Install the Apache HTTP Server:
   ```
   $> sudo yum -y install httpd
   ```

   d. Open port 80 on the firewall to allow http and https traffic through:
   ```
   $> sudo firewall-cmd --permanent --add-port=80/tcp
   ```

   e. Reload the firewall:
   ```
   $> sudo firewall-cmd --reload
   ```

   f. Start the web server:
   ```
   $> sudo systemctl start httpd
   ```

   g. Add an index.htm file on each instance to indicate which server it is.

      On the first instance enter:
   ```
   $> sudo su
   $> echo 'WebServer1' >>/var/www/html/index.html
   $> exit
   ```

   h. On the second instance enter:
   ```
   $> sudo su
   $> echo 'WebServer2' >>/var/www/html/index.html
   $> exit
   ```

Practice 6-4: Creating and Testing Load Balancer

Note: Your load balancer should always reside in different subnets than your application instances. This allows you to keep your application instances secured in private subnets, while allowing public Internet traffic to the load balancer in the public subnets.

Duration: 26 minutes Tasks

1. Add Two Subnets to Your VCN to Host Your Load Balancer

a. Add a Security List.

1) In the **Console**, click **Networking**, and then click **Virtual Cloud Networks**. This displays the list of VCNs in the current compartment.

2) Click the name of the VCN that includes your Web Instances.

3) Under **Resources**, click **Security Lists**.

4) Click **Create Security List**

a) **Create in Compartment:** This field defaults to the current compartment

b) Enter a **Name** (for example, **LB Security List**).

c) Delete the entry for the ingress rule and the entry for the egress rule by clicking on the red X icon.

Note: The security list should have no rules. The correct rules are automatically added during the load balancer workflow.

d) Click **Create Security List**.

e) Return to your Virtual Cloud Network Details page.

b. Add a Route Table.

1) Under **Resources**, click **Route Tables**.

2) Click **Create Route Table**. Enter the following:

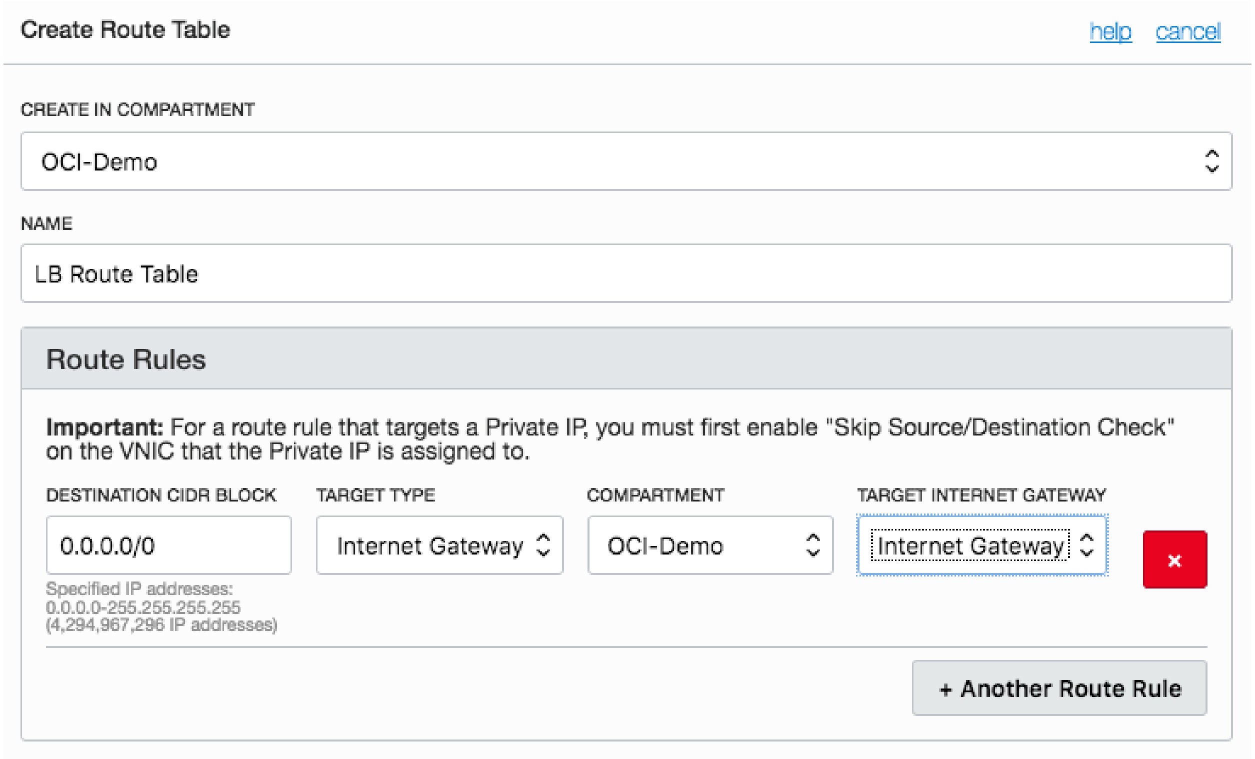
a) **Create in Compartment**: This field defaults to your current compartment. Select the compartment you want to create the route table in, if not already selected.

b) **Name**: Enter a name (for example, LB Route Table)

c) **Destination CIDR Block**: Enter 0.0.0.0/0

d) **Target**: Select the Internet Gateway for your VCN.

e) Click **Create Route Table**.



Create Route Table

CREATE IN COMPARTMENT: OCI-Demo

NAME: LB Route Table

Route Rules

Important: For a route rule that targets a Private IP, you must first enable "Skip Source/Destination Check" on the VNIC that the Private IP is assigned to.

DESTINATION CIDR BLOCK	TARGET TYPE	COMPARTMENT	TARGET INTERNET GATEWAY
0.0.0.0/0	Internet Gateway	OCI-Demo	Internet Gateway

Specified IP addresses: 0.0.0.0-255.255.255.255 (4,294,967,296 IP addresses)

2. Create the first subnet.

a) Under **Resources**, click **Subnets**.

b) Click **Create Subnet**.

c) Enter the following:

Name: Enter a name (for example, LB Subnet 1).

Availability Domain: Choose the first Availability Domain (AD-1).

CIDR Block: Enter 10.0.4.0/24.

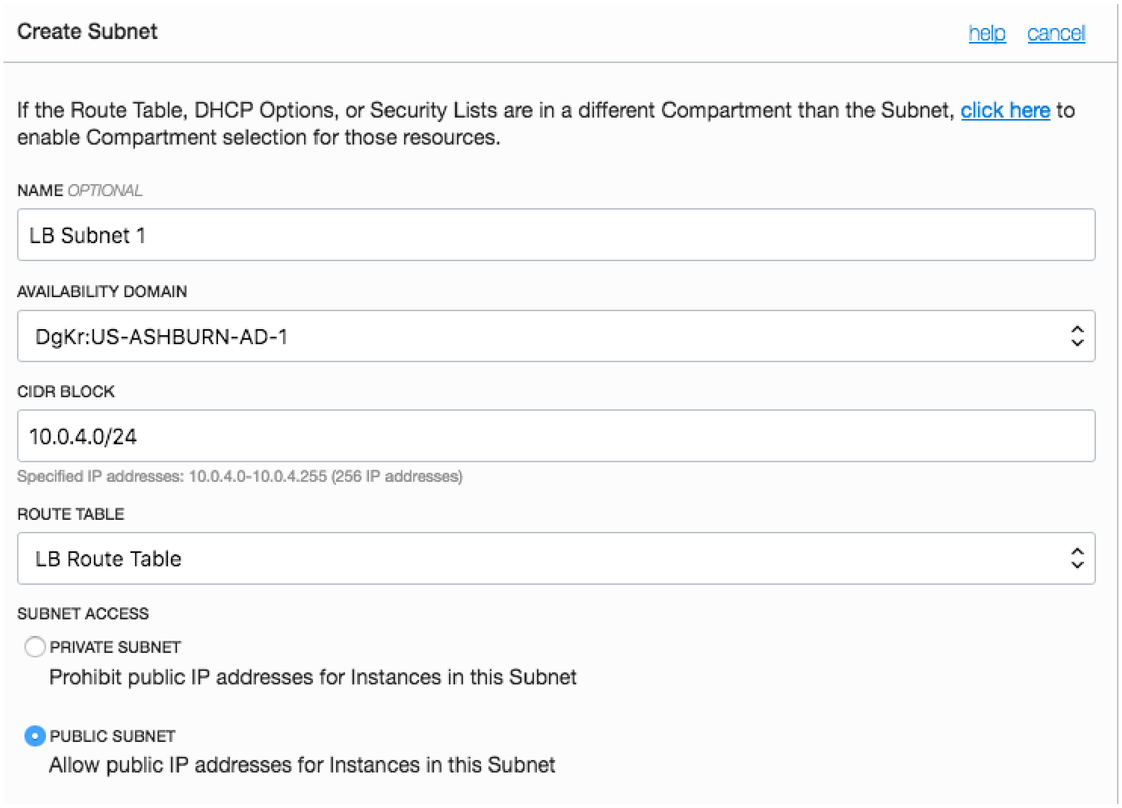
Route Table: Select the **LB Route Table** you created.

Subnet Access: Make sure you have Public selected.

DHCP Options: Leave blank.

Security Lists: Select the **LB Security List** you created.

d. Click **Create**.



Create Subnet

If the Route Table, DHCP Options, or Security Lists are in a different Compartment than the Subnet, click here to enable Compartment selection for those resources.

NAME *OPTIONAL*

LB Subnet 1

AVAILABILITY DOMAIN

DgKr:US-ASHBURN-AD-1

CIDR BLOCK

10.0.4.0/24

Specified IP addresses: 10.0.4.0-10.0.4.255 (256 IP addresses)

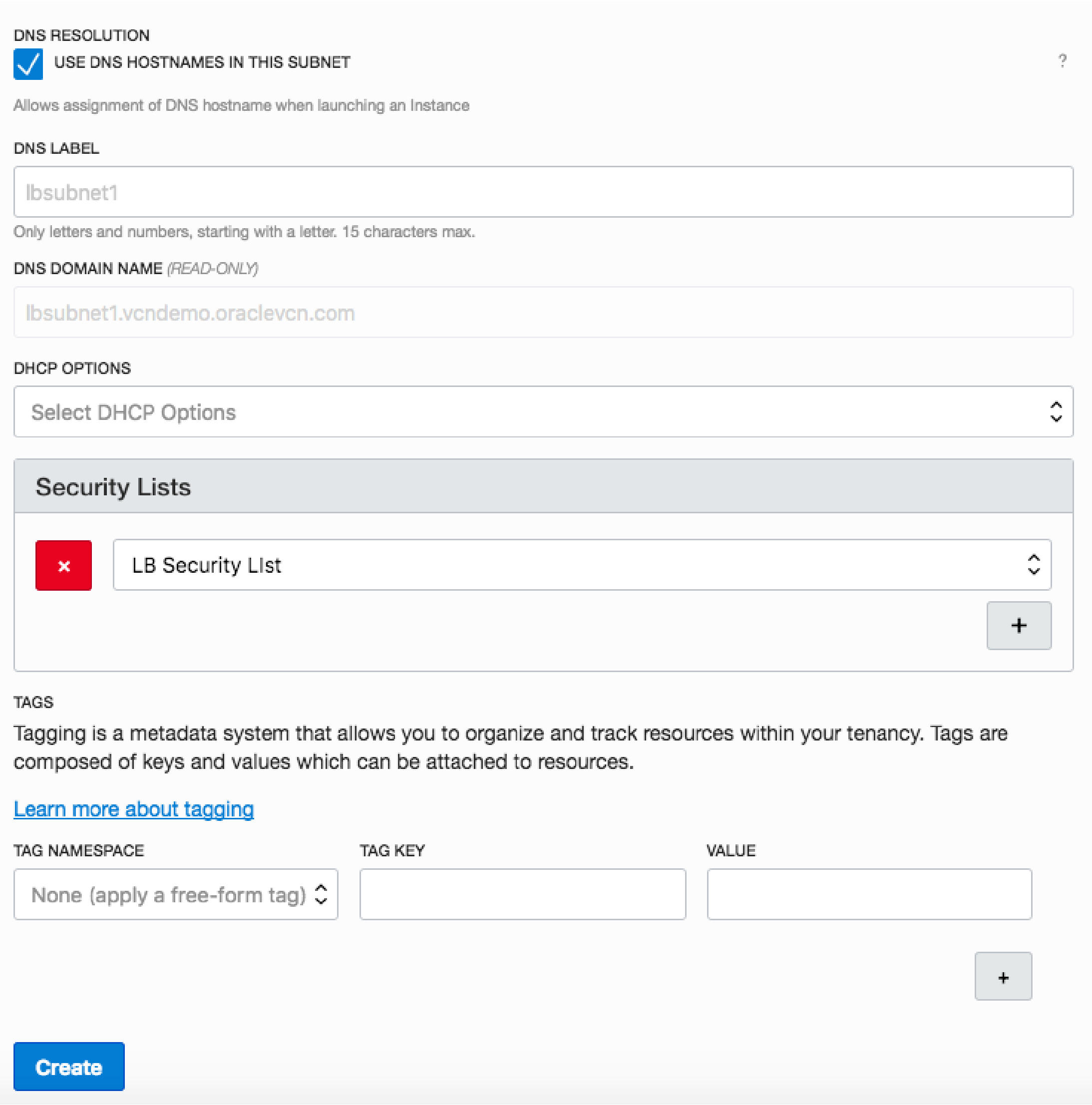
ROUTE TABLE

LB Route Table

SUBNET ACCESS

○ PRIVATE SUBNET
Prohibit public IP addresses for Instances in this Subnet

● PUBLIC SUBNET
Allow public IP addresses for Instances in this Subnet



DNS RESOLUTION

☑ USE DNS HOSTNAMES IN THIS SUBNET ?

Allows assignment of DNS hostname when launching an Instance

DNS LABEL

lbsubnet1

Only letters and numbers, starting with a letter. 15 characters max.

DNS DOMAIN NAME *(READ-ONLY)*

lbsubnet1.vcndemo.oraclevcn.com

DHCP OPTIONS

Select DHCP Options

Security Lists

× LB Security LIst

+

TAGS

Tagging is a metadata system that allows you to organize and track resources within your tenancy. Tags are composed of keys and values which can be attached to resources.

Learn more about tagging

TAG NAMESPACE	TAG KEY	VALUE
None (apply a free-form tag)		

+

Create

3. Create the second subnet.

Create a second load balancer subnet in a different Availability Domain from the subnet you previously created.

1) In the details page of your VCN, click **Create Subnet**.

2) Enter the following:

a) **Name:** Enter a name (for example, LB Subnet 2).

b) **Availability Domain:** Choose the second Availability Domain (AD-2).

c) **CIDR Block:** Enter 10.0.5.0/24.

d) **Route Table:** Select the **LB Route Table** you created.

e) **Subnet Access**: Make sure you have Public selected

f) **DHCP Options:** Leave blank.

g) **Security Lists:** Select the **LB Security List** you created.

h) Click **Create**.

4. Create a Load Balancer

When you create a load balancer, you choose its shape (size) and you specify two subnets from different Availability Domains. This ensures that the load balancer is highly available and is only active in one subnet at a time.

a. In the Console, click **Networking**, and then click **Load Balancers**. Ensure that the compartment designated for you is selected on the left.

b. Click **Create Load Balancer**.

c. Enter the following:

1) **Name:** Enter a name for your load balancer.

2) **Shape:** Select 100Mbps. This specifies the bandwidth of the load balancer. For this tutorial, use the smallest shape. Note that the shape cannot be changed later.

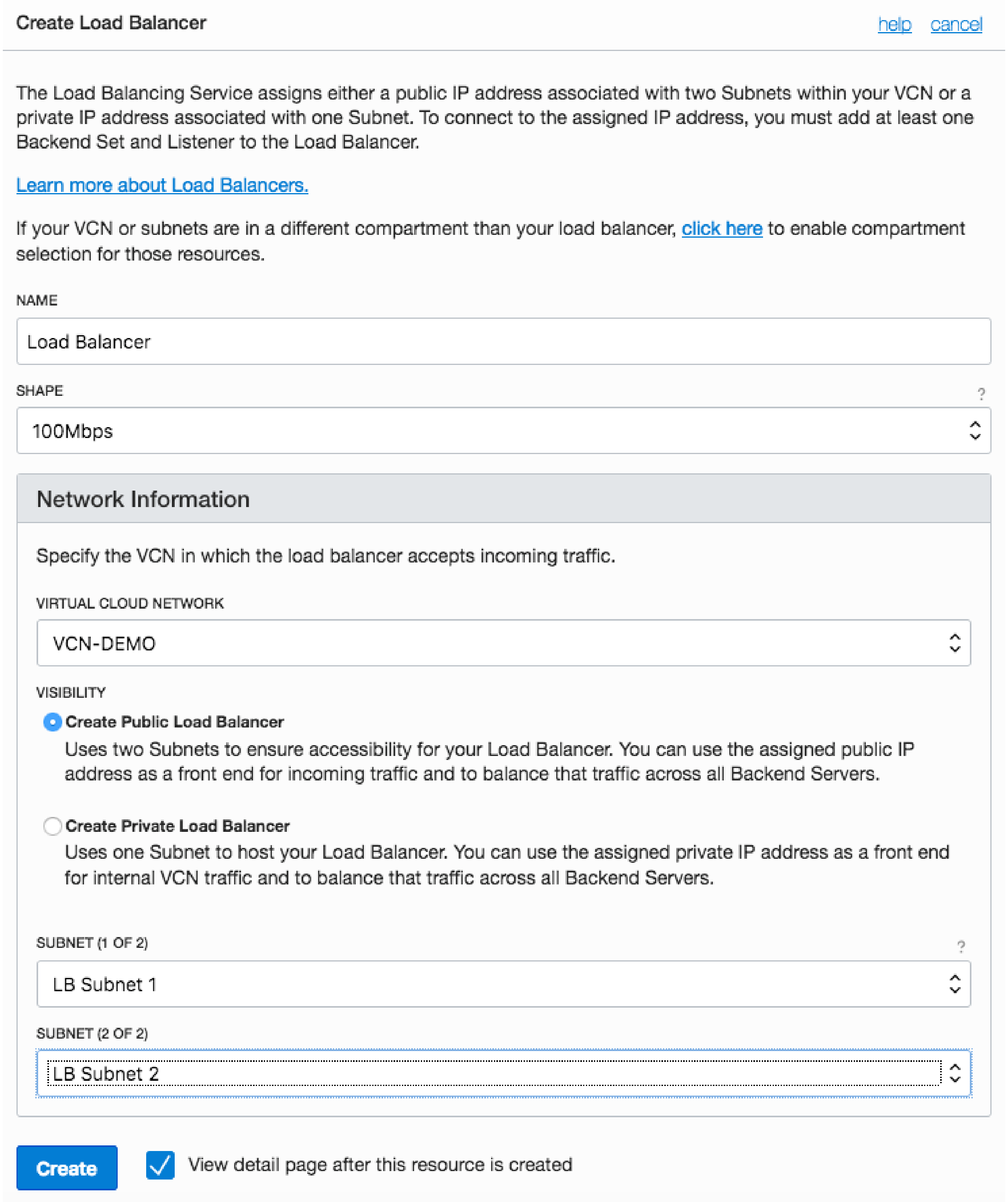
3) **Virtual Cloud Network:** Select the Virtual Cloud Network for your load balancer.

4) **Visibility**: Create Public Load Balancer

4) **Subnet (1 of 2):** Select LB Subnet 1.

5) **Subnet (2 of 2):** Select LB Subnet 2. Note that the second subnet must reside in a different Availability Domain from the first.

d. Click **Create**.



Create Load Balancer

The Load Balancing Service assigns either a public IP address associated with two Subnets within your VCN or a private IP address associated with one Subnet. To connect to the assigned IP address, you must add at least one Backend Set and Listener to the Load Balancer.

Learn more about Load Balancers.

If your VCN or subnets are in a different compartment than your load balancer, click here to enable compartment selection for those resources.

NAME: Load Balancer

SHAPE: 100Mbps

Network Information

Specify the VCN in which the load balancer accepts incoming traffic.

VIRTUAL CLOUD NETWORK: VCN-DEMO

VISIBILITY

● **Create Public Load Balancer**
Uses two Subnets to ensure accessibility for your Load Balancer. You can use the assigned public IP address as a front end for incoming traffic and to balance that traffic across all Backend Servers.

○ **Create Private Load Balancer**
Uses one Subnet to host your Load Balancer. You can use the assigned private IP address as a front end for internal VCN traffic and to balance that traffic across all Backend Servers.

SUBNET (1 OF 2): LB Subnet 1

SUBNET (2 OF 2): LB Subnet 2

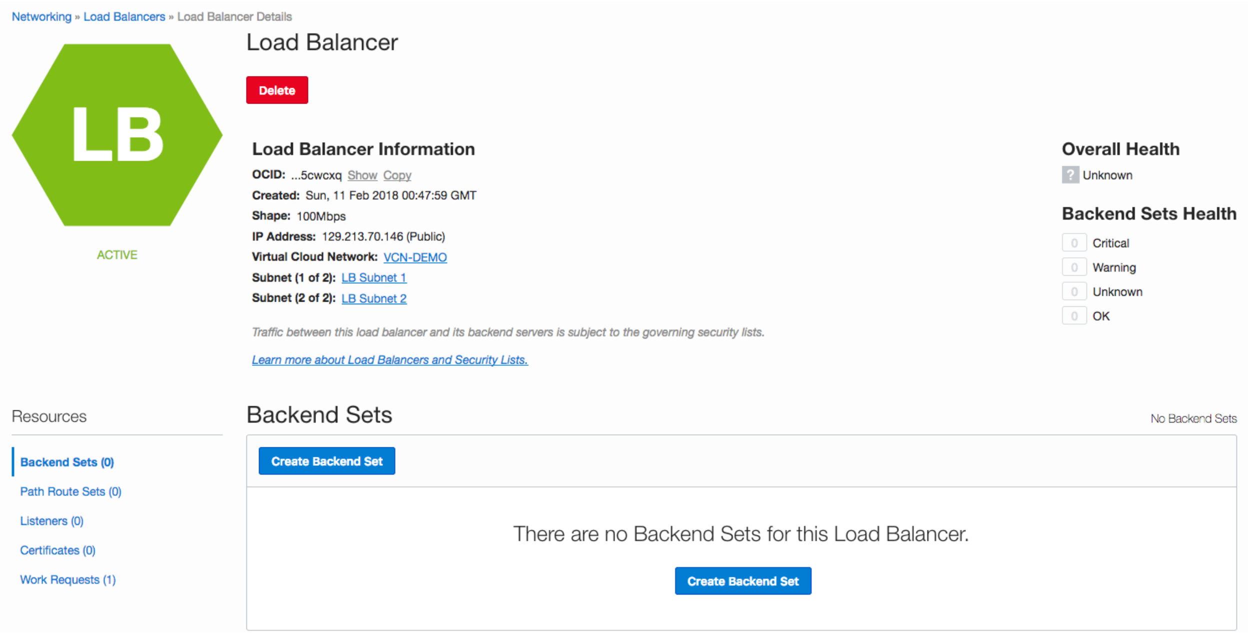
☑ View detail page after this resource is created

When a load balancer is created, you're assigned a public IP address to which you route all incoming traffic. The IP address is highly available, meaning it is available from both subnets that you specified. Note that it is only active in one subnet at a time.

5. Create a Backend Set with Health Check

A backend set is a collection of backend servers to which your load balancer directs traffic. Define the backend set policy and health check.

a. Click the name of your load balancer to view its details.



Load Balancer

Load Balancer Information

OCID: ...5cwcxq Show Copy
Created: Sun, 11 Feb 2018 00:47:59 GMT
Shape: 100Mbps
IP Address: 129.213.70.146 (Public)
Virtual Cloud Network: VCN-DEMO
Subnet (1 of 2): LB Subnet 1
Subnet (2 of 2): LB Subnet 2

Traffic between this load balancer and its backend servers is subject to the governing security lists.

Learn more about Load Balancers and Security Lists.

Overall Health

? Unknown

Backend Sets Health

0	Critical
0	Warning
0	Unknown
0	OK

Backend Sets

No Backend Sets

There are no Backend Sets for this Load Balancer.

b. **Click Create** Backend Set.

c. In the dialog box, enter:

1) **Name:** Give your load balancer backend set a name. The name cannot contain spaces.

2) **Policy:** Choose Weighted Round Robin.

d. Enter the Health Check details.

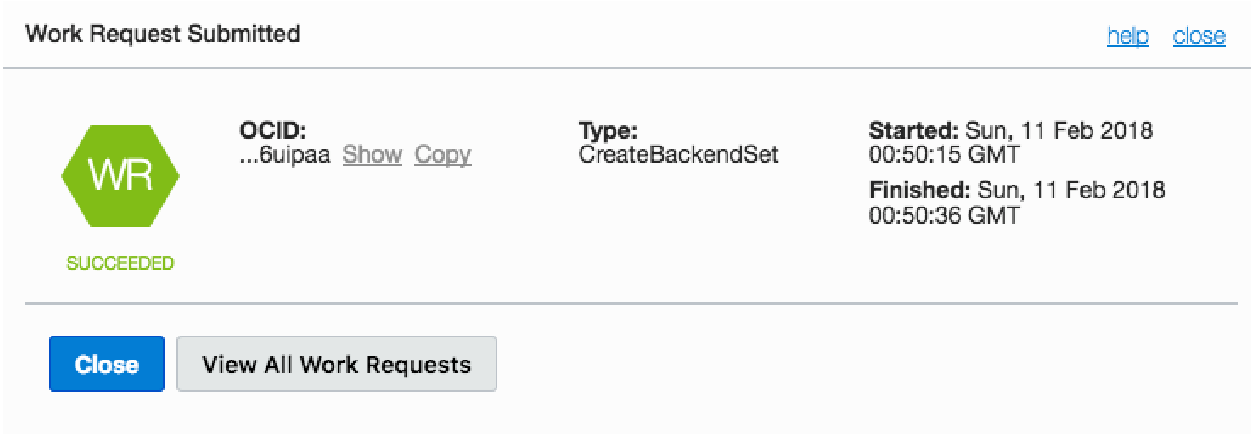
1) **Protocol:** Select HTTP

2) **Port:** Enter 80

3) **URL Path** (URI)**:** Enter "/"   The rest of the fields are optional and can be left blank for this practice.

e. Click **Create**.

When the Backend Set is created, the Work Request status changes to Succeeded. Close the Work Request dialog box.



Work Request Submitted

OCID: ...6uipaa Show Copy

Type: CreateBackendSet

Started: Sun, 11 Feb 2018 00:50:15 GMT

Finished: Sun, 11 Feb 2018 00:50:36 GMT

4. Add Backend Servers to Your Backend Set

a. On the details page of your load balancer, click **Backend Sets**. The backend set you created is displayed.

b. Click the name of the backend set to view its details.

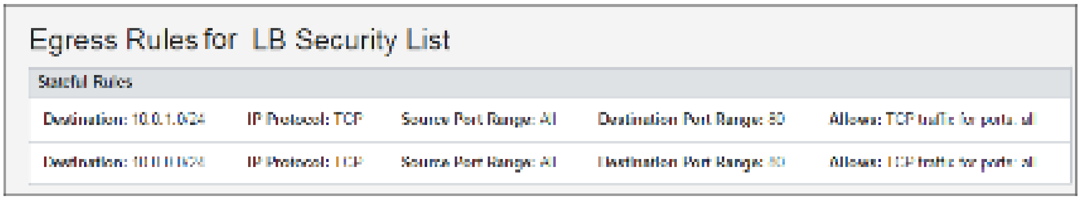
c. Click **Edit Backends** In the dialog box, do the following:

1) Ensure that **Help me create proper security list rules** is selected.

a) Updates to the security list for your load balancer subnets are as follows:

(i) Allow egress traffic to the backend server 1 subnet (for example, Public-Subnet-AD1)

(ii) Allow egress traffic to the backend server 2 subnet (for example, Public-Subnet-AD2)



Egress Rules for LB Security List

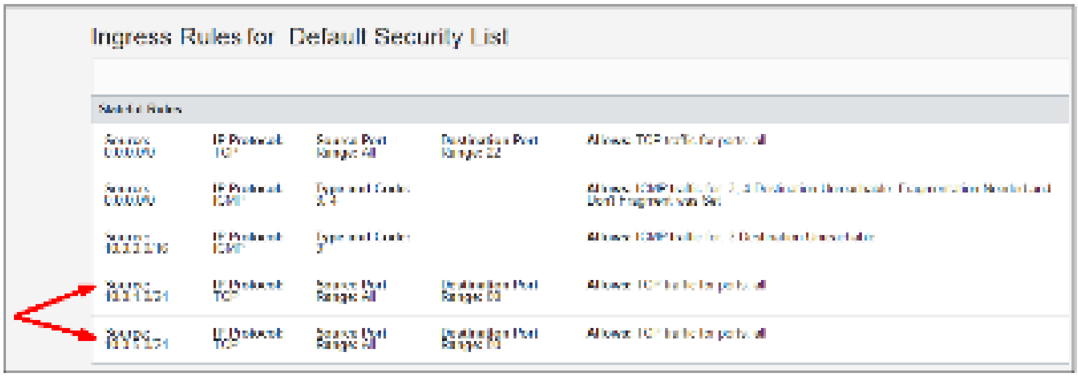
Stateful Rules

Destination: 10.0.1.0/24	IP Protocol: TCP	Source Port Range: All	Destination Port Range: 80	Allows: TCP traffic for ports: all
Destination: 10.0.0.0/24	IP Protocol: TCP	Source Port Range: All	Destination Port Range: 80	Allows: TCP traffic for ports: all

b) Updates to the security list for your backend server subnets are as follows:

(i) Allow ingress traffic from load balancer subnet 1

(ii) Allow ingress traffic from load balancer subnet 2



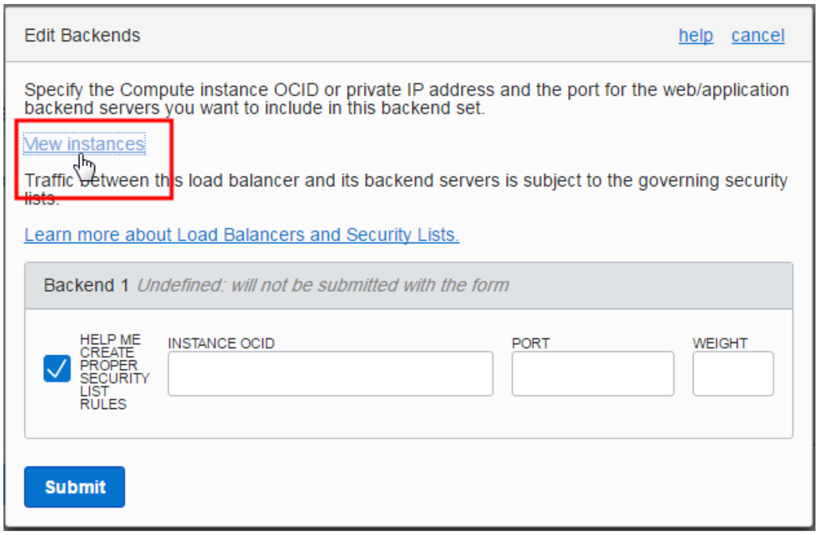
Ingress Rules for Default Security List

Stateful Rules

Source: 0.0.0.0/0	IP Protocol: TCP	Source Port Range: All	Destination Port Range: 22	Allows: TCP traffic for ports: all
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
Source: 10.0.1.0/24	IP Protocol: TCP	Source Port Range: All	Destination Port Range: 80	Allows: TCP traffic for ports: all
Source: 10.0.2.0/24	IP Protocol: TCP	Source Port Range: All	Destination Port Range: 80	Allows: TCP traffic for ports: all

2) **OCID:** Paste the OCID of the first instance (Webserver1).

a) In the dialog box, click **View Instances**.



Edit Backends

Specify the Compute instance OCID or private IP address and the port for the web/application backend servers you want to include in this backend set.

Traffic between this load balancer and its backend servers is subject to the governing security lists.

Backend 1 *Undefined: will not be submitted with the form*

☑ HELP ME CREATE PROPER SECURITY LIST RULES	INSTANCE OCID	PORT	WEIGHT

This opens a new browser tab that displays the instances in the current compartment.

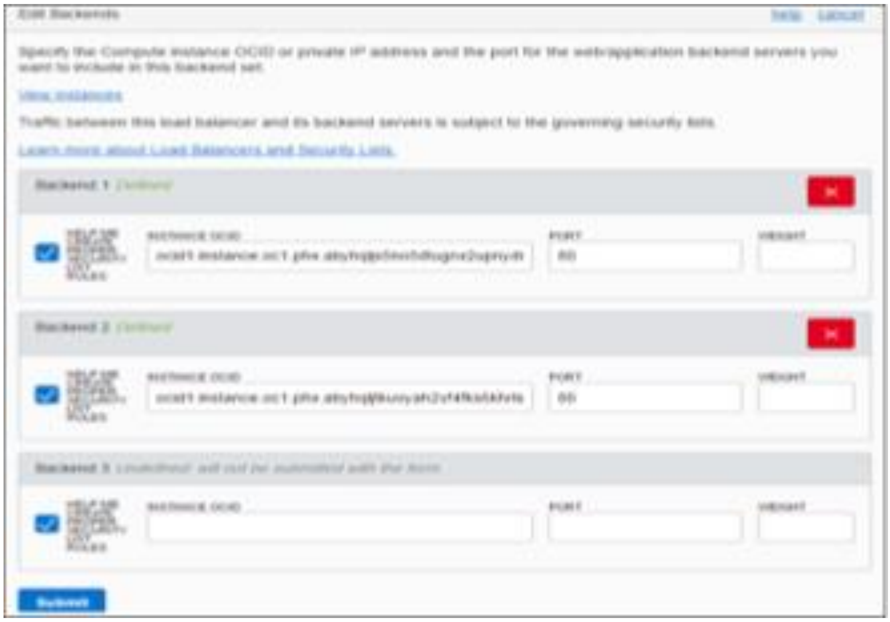
b) If your instances are not in the current compartment, select the compartment to which the instance belongs (select from the list on the left side of the page). A shortened version of the instance's OCID is displayed next to each instance.

c) Click **Copy** to copy the OCID. You can then paste it into the Instance ID field.

3) **Port:** Enter 80.

4) **Weight:** Leave blank to weight the servers evenly.

5) Repeat Steps 2 through 4, pasting in the OCID for the second instance (Webserver2).



Edit Backends

Help Cancel

Specify the Compute instance OCID or private IP address and the port for the web/application backend servers you want to include in this backend set.

View instances

Traffic between this load balancer and its backend servers is subject to the governing security lists.

Learn more about Load Balancers and Security Lists.

Backend 1 (Defined)

☑ HELP ME CREATE PROPER SECURITY LIST RULES

INSTANCE OCID	PORT	WEIGHT
ocid1.instance.oc1.phx.[illegible]	80	

Backend 2 (Defined)

☑ HELP ME CREATE PROPER SECURITY LIST RULES

INSTANCE OCID	PORT	WEIGHT
ocid1.instance.oc1.phx.[illegible]	80	

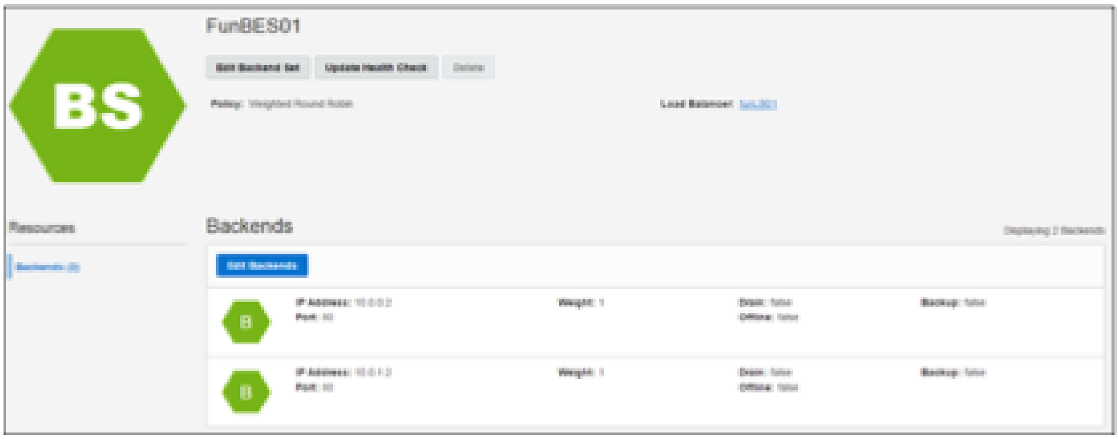
Backend 3 (Undefined: will not be submitted with the form)

☑ HELP ME CREATE PROPER SECURITY LIST RULES

INSTANCE OCID	PORT	WEIGHT

6) Click **Submit.**

7) Scroll down and click **Create Rules** once it turns green.



FunBES01

Policy: Weighted Round Robin

Load Balancer: funLB01

Backends

Displaying 2 Backends

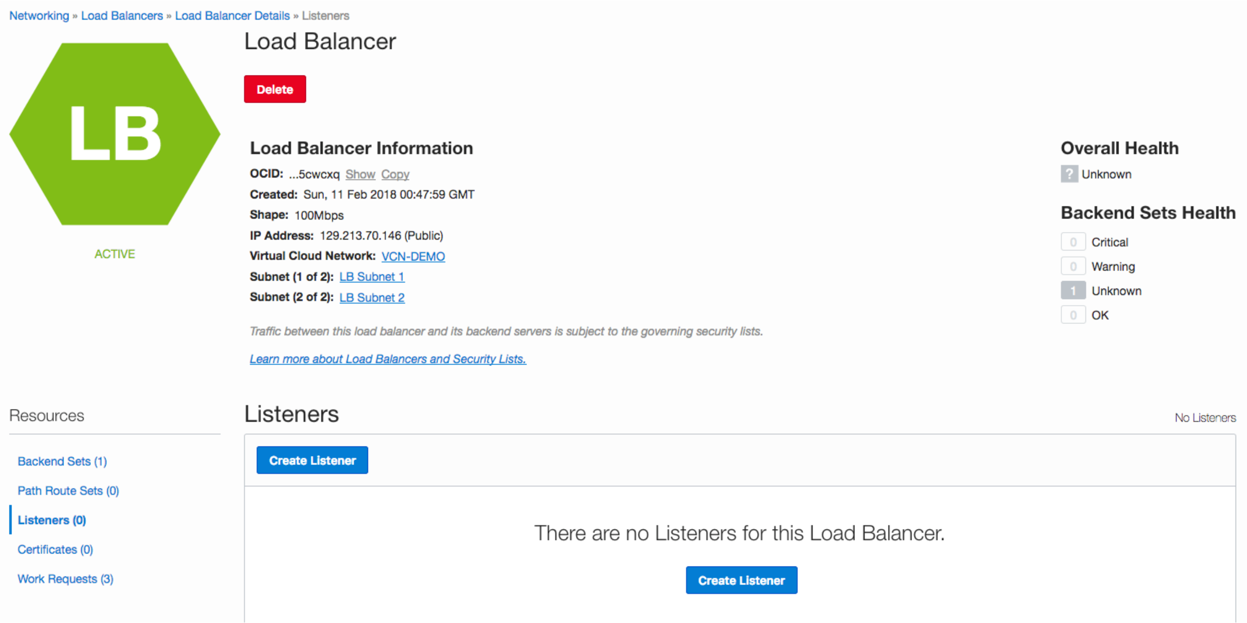
IP Address: 10.0.0.2 **Port:** 80 **Weight:** 1 **Drain:** false **Offline:** false **Backup:** false

IP Address: 10.0.1.2 **Port:** 80 **Weight:** 1 **Drain:** false **Offline:** false **Backup:** false

5. Create a Listener

A listener is an entity that checks for connection requests. The load balancer listener listens for ingress client traffic using the port you specify within the listener and the load balancer's public IP. In this practice, you define a listener that accepts HTTP requests on port 80.

a. On your Load Balancer Details page, click **Listeners**.



Load Balancer Information

OCID: ...5cwcxq Show Copy
Created: Sun, 11 Feb 2018 00:47:59 GMT
Shape: 100Mbps
IP Address: 129.213.70.146 (Public)
Virtual Cloud Network: VCN-DEMO
Subnet (1 of 2): LB Subnet 1
Subnet (2 of 2): LB Subnet 2

Traffic between this load balancer and its backend servers is subject to the governing security lists.

Learn more about Load Balancers and Security Lists.

Overall Health

? Unknown

Backend Sets Health

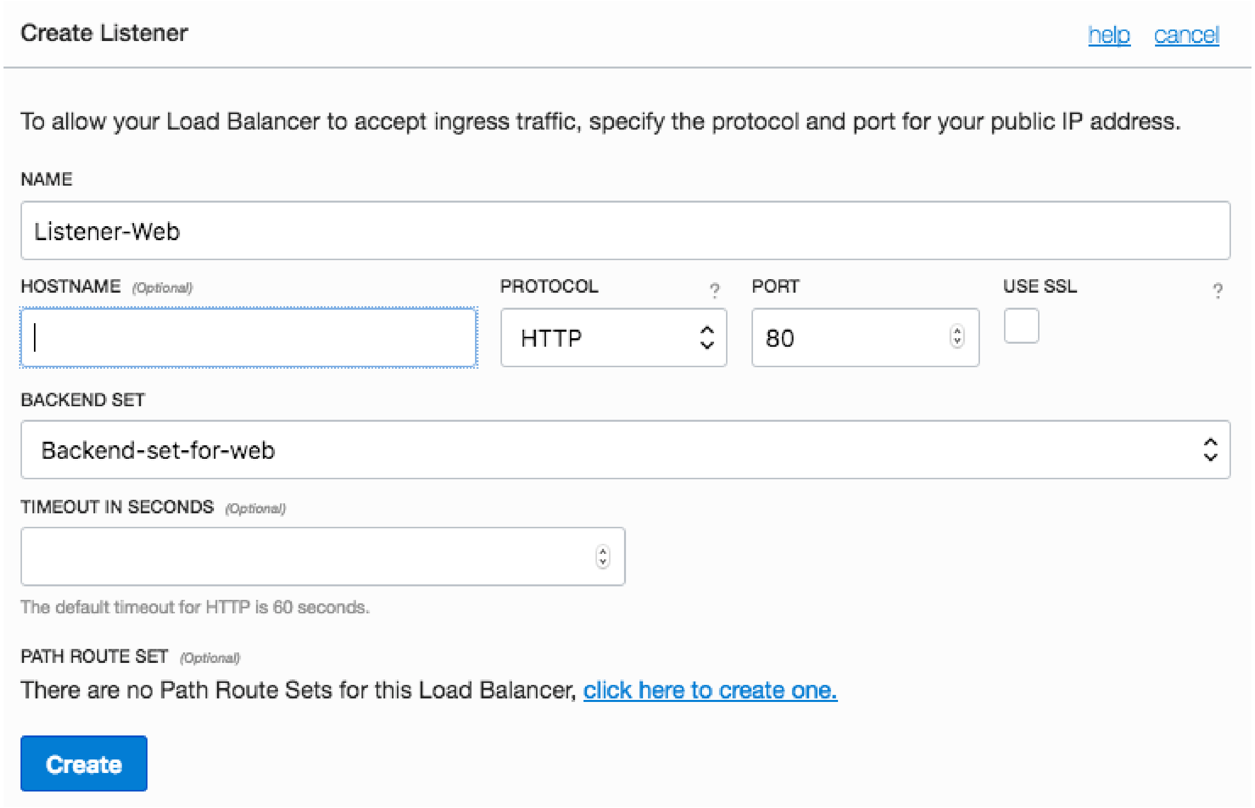
0	Critical
0	Warning
1	Unknown
0	OK

There are no Listeners for this Load Balancer.

b. Click **Create Listener**.

c. Enter the following:

1) **Name:** Enter a friendly name.
2) **Hostname**: Leave it blank.
3) **Protocol:** Select HTTP.
4) **Port:** Enter 80 as the port on which to listen for incoming traffic.
5) **Backend Set:** Select the backend set you created.



Create Listener

To allow your Load Balancer to accept ingress traffic, specify the protocol and port for your public IP address.

NAME: Listener-Web

HOSTNAME (Optional):

PROTOCOL: HTTP

PORT: 80

USE SSL: □

BACKEND SET: Backend-set-for-web

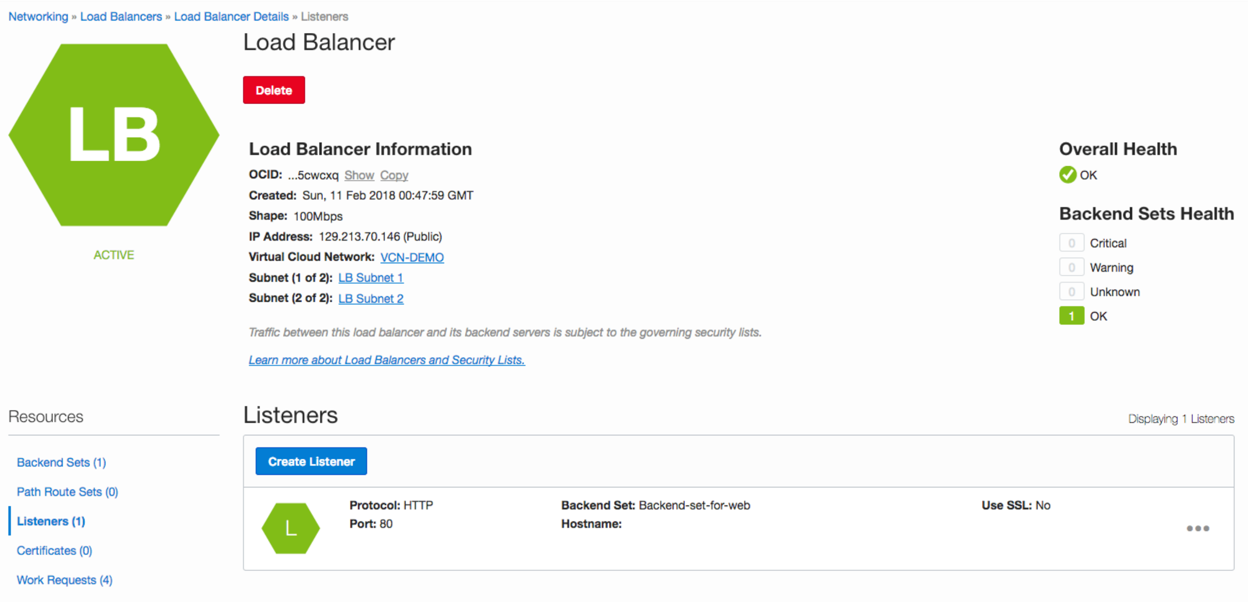
TIMEOUT IN SECONDS (Optional):

The default timeout for HTTP is 60 seconds.

PATH ROUTE SET (Optional)

There are no Path Route Sets for this Load Balancer, click here to create one.

d. Click **Create**.



Networking » Load Balancers » Load Balancer Details » Listeners

Load Balancer

Load Balancer Information

OCID: ...5cwcxq Show Copy
Created: Sun, 11 Feb 2018 00:47:59 GMT
Shape: 100Mbps
IP Address: 129.213.70.146 (Public)
Virtual Cloud Network: VCN-DEMO
Subnet (1 of 2): LB Subnet 1
Subnet (2 of 2): LB Subnet 2

Traffic between this load balancer and its backend servers is subject to the governing security lists.

Learn more about Load Balancers and Security Lists.

Overall Health

✓ OK

Backend Sets Health

0	Critical
0	Warning
0	Unknown
1	OK

Resources

Listeners

Displaying 1 Listeners

Protocol: HTTP
Port: 80
Backend Set: Backend-set-for-web
Hostname:
Use SSL: No

1. Update the **Load Balancer Subnet Security List** to Allow Internet Traffic to the Listener. To enable the traffic to get to the listener, update the load balancer subnet's security list.

   a. Go to your VCN details page.

   b. Click **Security Lists**. A list of the security lists in the cloud network is displayed.

   c. Click the **LB Security List**. This displays the details of the LB Security List.

   d. Click **Edit All Rules**.

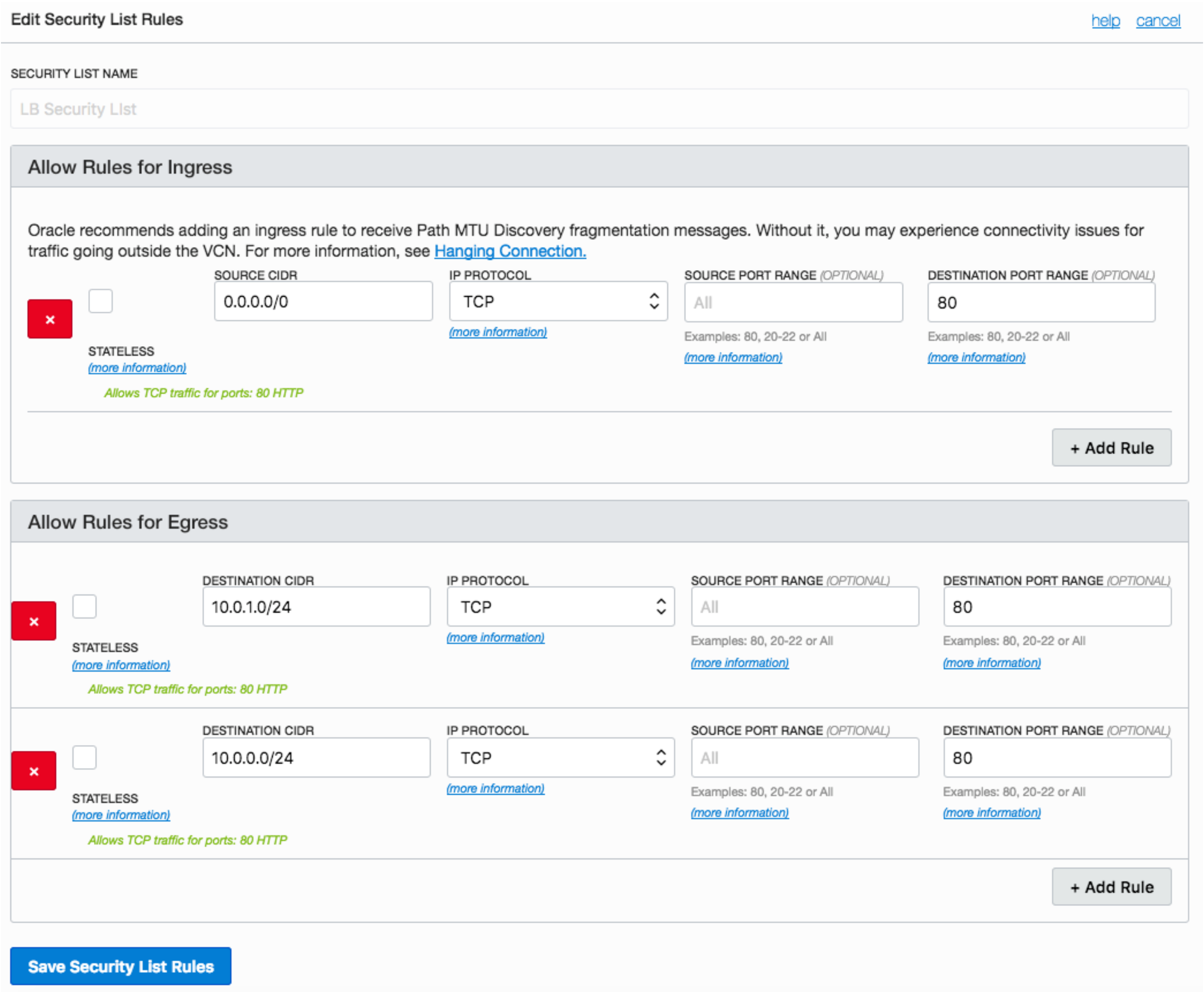
   e. Under **Allow Rules for Ingress**, click **Add Rule**.

   f. Enter the following ingress rule:

      Source CIDR: Enter 0.0.0.0/0

      IP Protocol: Select TCP

      Destination Port Range: Enter 80 (the listener port).



Edit Security List Rules

help cancel

SECURITY LIST NAME

LB Security List

Allow Rules for Ingress

Oracle recommends adding an ingress rule to receive Path MTU Discovery fragmentation messages. Without it, you may experience connectivity issues for traffic going outside the VCN. For more information, see Hanging Connection.

	SOURCE CIDR	IP PROTOCOL	SOURCE PORT RANGE *(OPTIONAL)*	DESTINATION PORT RANGE *(OPTIONAL)*
□ STATELESS *(more information)*	0.0.0.0/0	TCP *(more information)*	All Examples: 80, 20-22 or All *(more information)*	80 Examples: 80, 20-22 or All *(more information)*

Allows TCP traffic for ports: 80 HTTP

+ Add Rule

Allow Rules for Egress

	DESTINATION CIDR	IP PROTOCOL	SOURCE PORT RANGE *(OPTIONAL)*	DESTINATION PORT RANGE *(OPTIONAL)*
□ STATELESS *(more information)*	10.0.1.0/24	TCP *(more information)*	All Examples: 80, 20-22 or All *(more information)*	80 Examples: 80, 20-22 or All *(more information)*

Allows TCP traffic for ports: 80 HTTP

	DESTINATION CIDR	IP PROTOCOL	SOURCE PORT RANGE *(OPTIONAL)*	DESTINATION PORT RANGE *(OPTIONAL)*
□ STATELESS *(more information)*	10.0.0.0/24	TCP *(more information)*	All Examples: 80, 20-22 or All *(more information)*	80 Examples: 80, 20-22 or All *(more information)*

Allows TCP traffic for ports: 80 HTTP

+ Add Rule

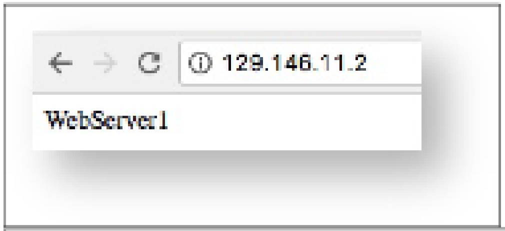
Save Security List Rules

g. Click **Save Security List Rules**.

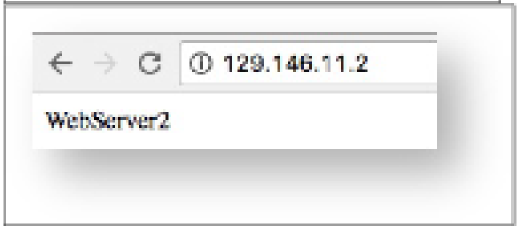
7. Verify Your Load Balancer

Test the functionality of the load balancer by navigating to its public IP address on a web browser.

a) Open a web browser.
b) Enter the load balancer's public IP address. The index.htm page from one of your web servers is displayed.
c) Refresh the web page. The index.htm page from the other web server should now be displayed. This demonstrates that the load of the web server is being shared between both instances.



WebServer1



WebServer2