Solution Engineer Assisted Workshop Day

Lab 03 – Networking Basics and Advanced

V1.1

ORACLE LAB BOOK | JANURARY 2019

ORACLE

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.

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

Definitions:

ACLs - collection of security rules that can be applied to a vNICset. ACLs determine whether a packet can be forwarded to or from a vNIC, based on the criteria specified in its security rules.

- An interface on an IP network is not, by default, reachable from any source that is not on the same IP network or on the same IP network exchange.

Security Lists – is a group of Compute Classic instances that you can specify as the source or destination in one of more security rules.

- The instances in a security list can communicate fully, on all ports, with other instances in the same security list using their private IP addresses.
- The inbound policy is always set to deny, so by default traffic from any source outside the security list can't access the instances that are part of the security list.
- The outbound policy controls the flow of traffic out of the security list. For example, if the outbound policy is set to deny, packets can't flow out of the security list. To allow instances in a security list to communicate with hosts outside the security list, set the outbound policy to permit.

Security Rules – Essentially firewall rules, which you can use to permit traffic between Compute Classic instances in different security lists as well as between instances and external hosts.

- The source and destination specified in a security rule can be either a security IP list (that is, a list of external hosts) or a security list.
- A firewall rule that you can define to control network access to Compute Classic instances over a specified security application.

Shared Network (VCN) – each instance is assigned a private IP address from a common pool.

IP Network (subnet) – Private network in a public cloud. For ExaCC it is called IP Network. Able to bring your own IP addresses and subnets, and used to isolate instances by creating multiple IP networks. Uses IP from the IP Network pool different from the shared network.

IP Exchange – Enables access between IP networks that have non-overlapping addresses, so that instances on these networks can exchange packets with each other without NAT.

Port – Network term referring to a virtual endpoint

vNIC - (Virtual Network Interface Card) The emulation of a physical network adapter (NIC)

vNICset - is a collection of one or more vNICs. For example, you use vNICsets to specify multiple vNICs as a source or a destination in a security rule.

of Oracle-provided IP addresses an IP network allows define an IP subnet in your account.

- In the shared network, access to your instances is determined by security lists and security rules, while in the IP network you create security rules and access control lists (ACLs) enable access to instances.

Pre-Requisites

1. Oracle Cloud Infrastructure account credentials (User, Password, and Tenant)
2. SSH Keys generated for compute SSH access.
3. User access to you must have the Compute_Operations role.

Sign into tenancy:

Access the Tenancy Welcome Email using this link:
http://10.136.208.135/shares/export/nas/pcm/ocm15/t1Welcome.html

Pre-Requisite 3-0: Requirements for Load Balancing

Overview

What you need for a public load balancer:

- Two existing instances (WEBHOST1 and WEBHOST2), each running a webserver (ex Apache Web server or Oracle HTTP server
- Custom domain name, defined and managed by a DNS provider. Example: http://www.myCompany.example.com
- On each Web server host, the main page of your Web site or application is available at the following URL:

  host:80/

- Before you begin, it is important that you are able to successfully connect to this URL on each origin server in the server pool. This step confirms that you have configured the required security list, security rules, and security applications to allow HTTP access to the Compute instances over port 80. For more information about configuring access to a Compute instance, see Configuring the Shared Network in Using Oracle Compute Cloud Service (IaaS).

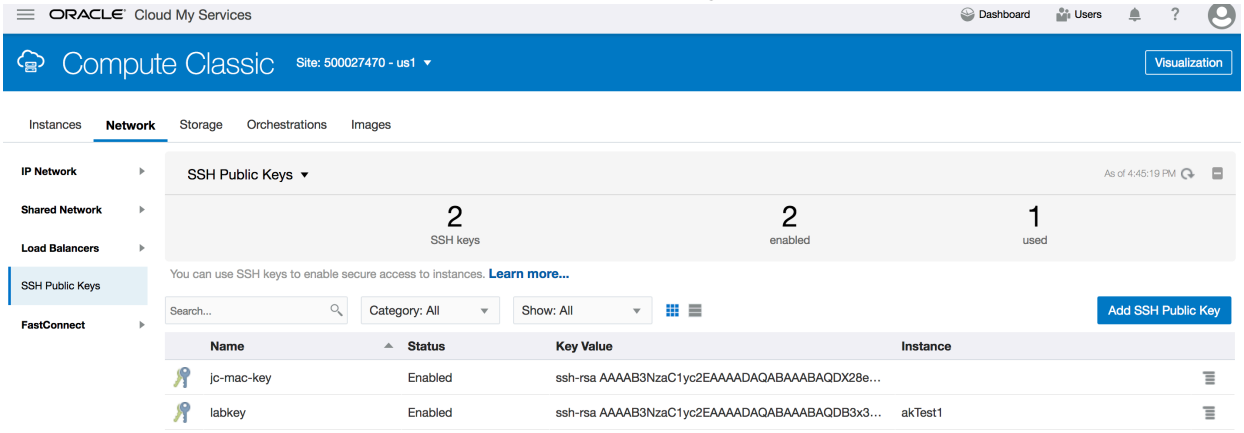
Assumptions

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.

Quick Creation of Both Web Servers

Upload SSH key

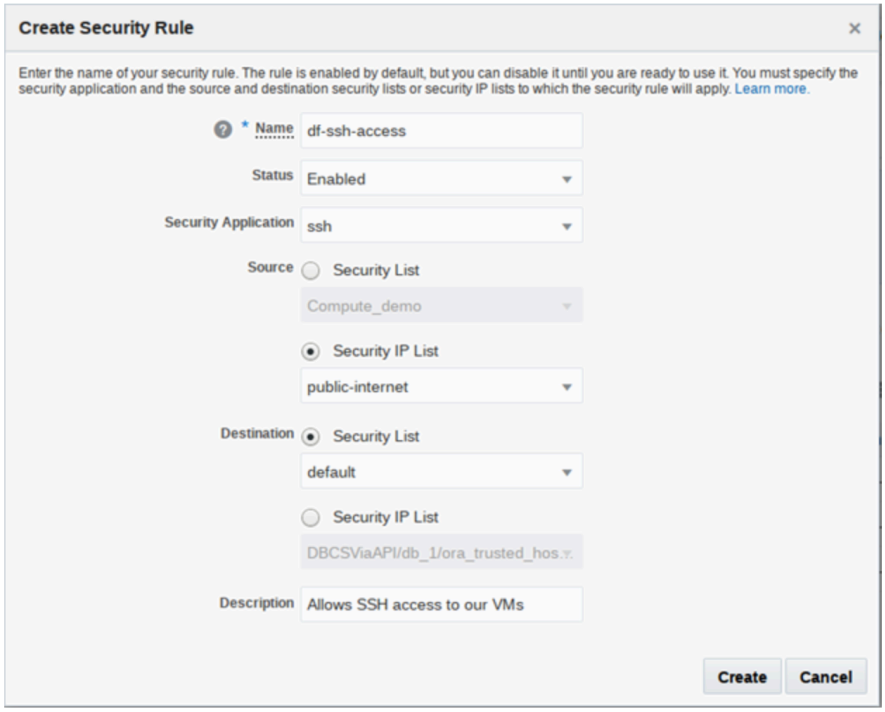
1. Clicked in the **Network** tab. Click **Add SSH Public Key.**



Name	Status	Key Value	Instance
jc-mac-key	Enabled	ssh-rsa AAAAB3NzaC1yc2EAAAADAQ...	
labkey	Enabled	ssh-rsa AAAAB3NzaC1yc2EAAAADAQ...	akTest1
Rocio_pubkey	Enabled	ssh-rsa AAAAB3NzaC1yc2EAAAADAQ...	

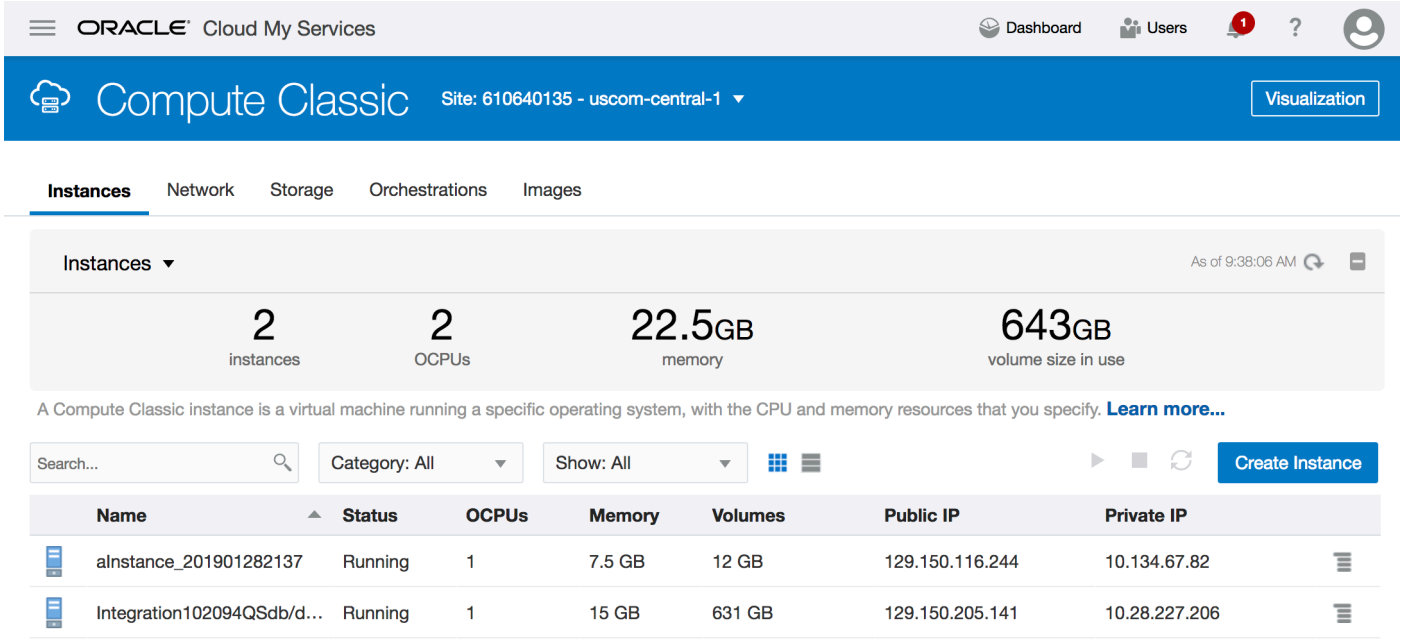
Create Instances

1. [View only] Under the "Shared Network" click on "Security Applications"
    - There are a number of applications already defined. For this exercise we will use the ssh application as this is how we will authenticate to the VM.
2. [View Only] Under the "Shared Network" click on "Security IP Lists"
    - Security can be applied either by IP address or by linking VMs into a security List. We will use both approaches for this VM. The source identified as coming from the "public-internet". i.e. Anyone can log onto this VM from any IP address.
3. [View Only] Under the "Shared Network" click on "Security Lists"
    - A VM can be linked to one or more security list and then access restrictions applied to all VMs in the list at once. In our scenario we will simply use the default list for our VMs.
4. Under the "Shared Network" click on the "Security Rules" and then click on "Create Security Rule" Fill in the details as follows:
    a. **Name**: <YOUR INITIALS>-ssh-access
    b. **Status** : Enabled
    c. **Security Application** : ssh
    d. **Source:** Select Security IP List and from the drop list choose public-internet
    e. **Destination**: Select Security List and from the drop list choose default.

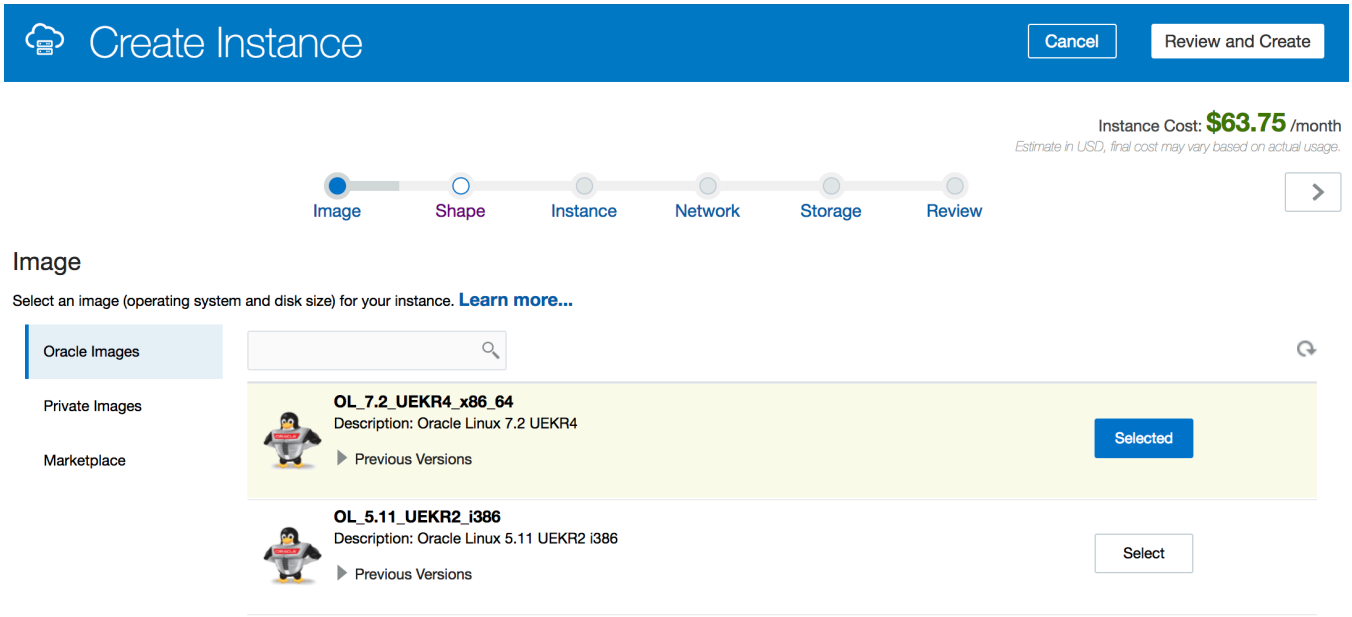


Initial Creation of VM

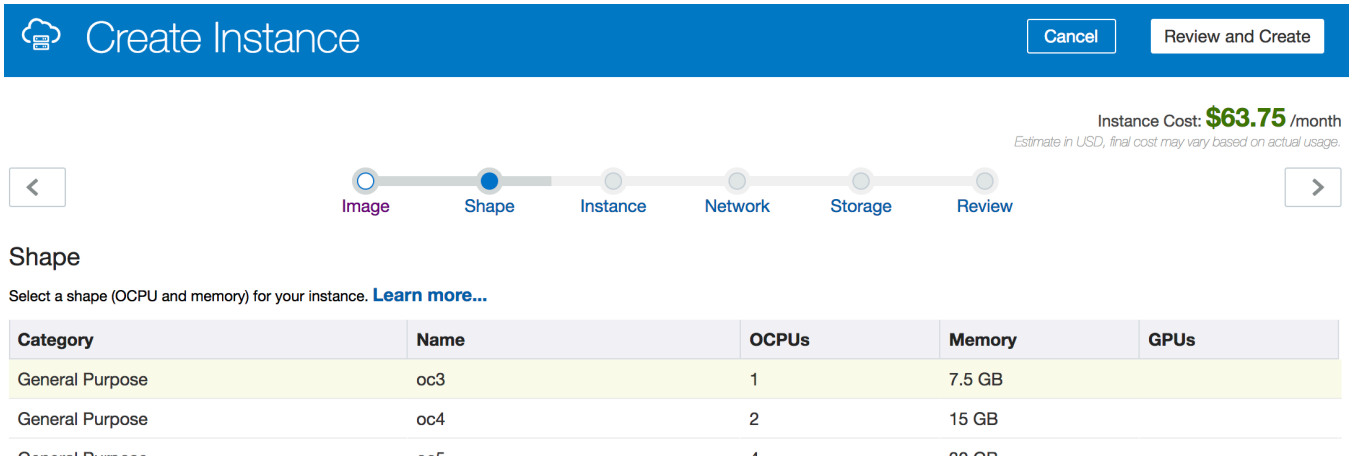
1. Click on the **Instances** tab. Click on create instance button. Click **Customize**



2. Under Images choose Oracle Linux 7.2 UEKR4 (OL_7.2_UEKR4_x86_64). Click next



3. Under shape choose oc3 – General Purpose 1 OCPU. Click Next



4. Under Instance.
    a. Name: <you initials>-workshop
    b. Label: <your initials>-workshop
    c. SSH keys: <pick the key you created earlier

Instance

Enter the required details to create your instance. **Learn more...**

Placement: Auto

Name*: rs-workshop

Label*: rs-workshop

Description: Compute workshop website

Tags: website ×

SSH Keys: rs-workshop × [Add SSH Public Key]

Custom Attributes:

5. Under Network. Provide theses information. Click next:
    a. **DNS Hostname Prefix**: <your initials>-workshop
    b. **Network Options**: Deselect IP network to leave only Shared Network
    c. **Security Lists**: default (Select by clicking the cursor into the box and then select the default from the dropdown list).

Instance Cost: **$63.75** /month

Estimate in USD, final cost may vary based on actual usage.

Image | Shape | Instance | Network | Storage | Review

Network

Configure network settings. **Learn more...**

DNS Hostname Prefix:

Network Options: ☐ IP Network ☑ Shared Network

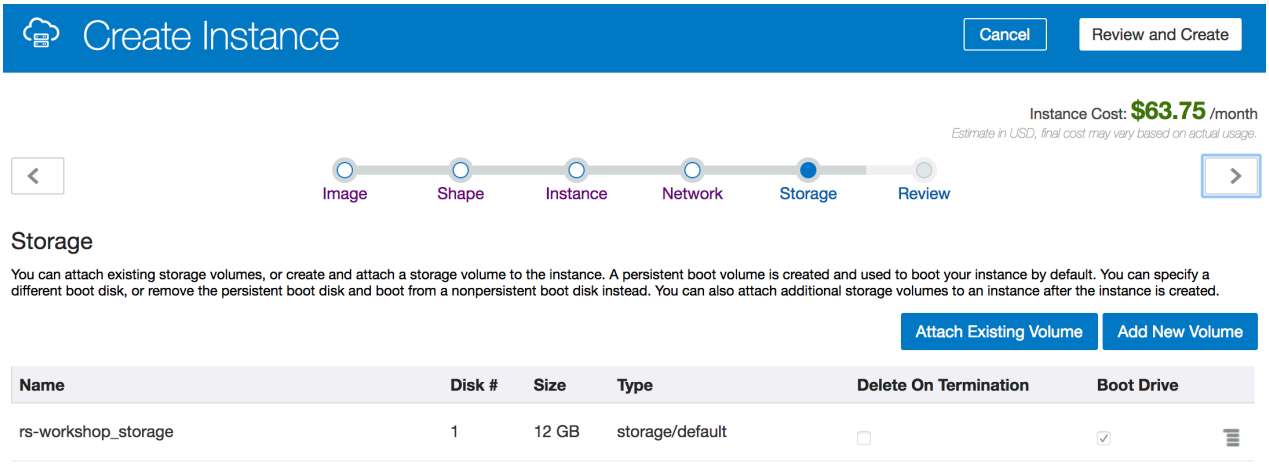
Shared Network Options

Public IP Address: Auto Generated

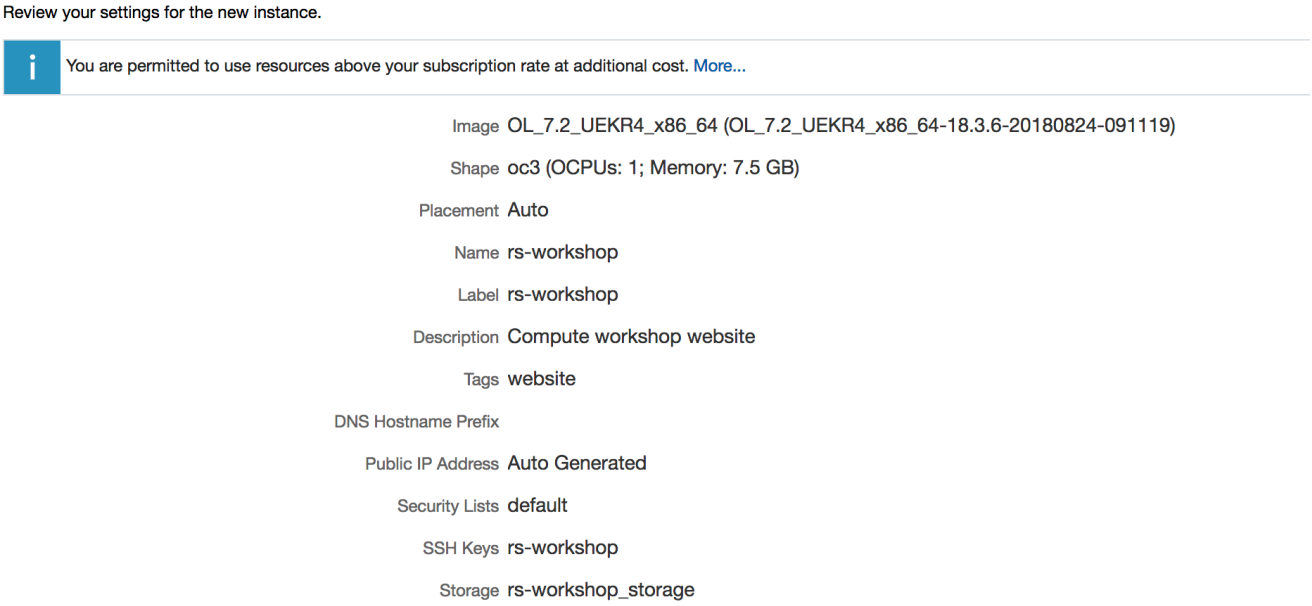
Security Lists*: default × [Create Security List]

6. Storage. No Changes here.

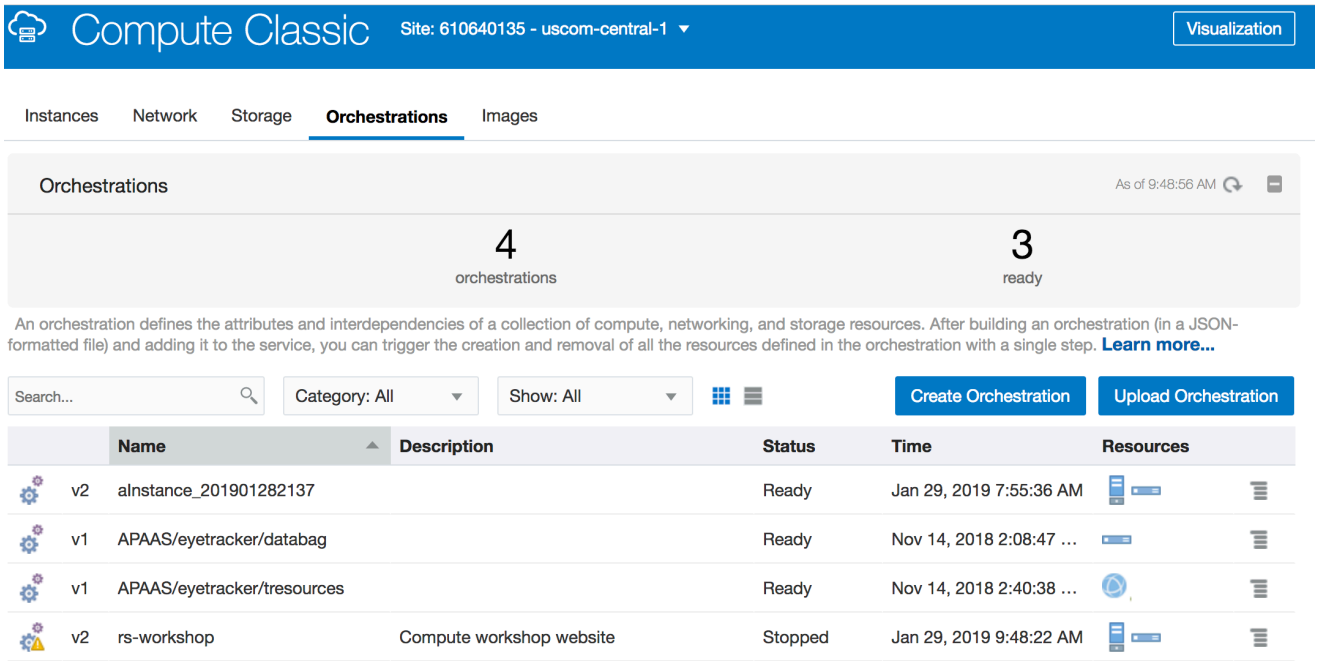
- Note: If you want to turn this instance into a template, you need to select the hamburger menu and remove the persistent disk otherwise, you cannot take snapshot on it.



7. Review the instance creation then click Create.



8. You can see the progress by clicking on the Orchestrations tab and then clicking on the refresh icon (beside the "Upload Orchestration" button) or by clicking on refresh on the Instances tab to see the VM being created.



9. From the instances page the "public" ip address of the VM is shown. Use this to ssh onto the VM as the OPC user.

Linux/Mac users

- **ssh -i <path to private key> opc@<Public IP address>**

Windows users

- setup putty config for ssh key access.

Install Webserver Apache and create a simple html page

1. 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
   $> sudo firewall-cmd –permanent --add-port=7777/tcp
   ```

   Should say success

   e. Reload the firewall:

   ```
   $> sudo firewall-cmd --reload
   ```

   Should say success

   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
   ```

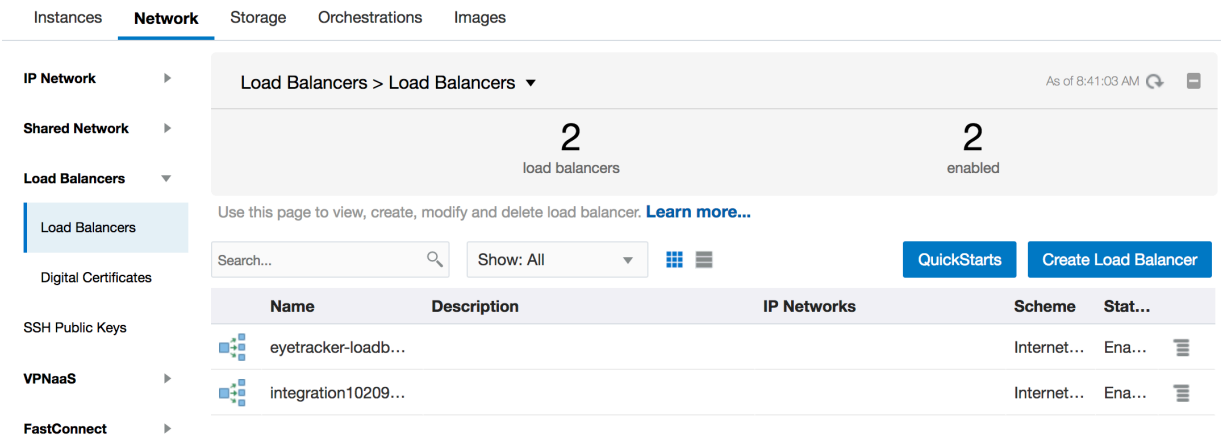
   h. On the second instance enter:

   ```
   $> sudo su
   $> echo 'WebServer2' >>/var/www/html/index.html
   $> exit
   ```

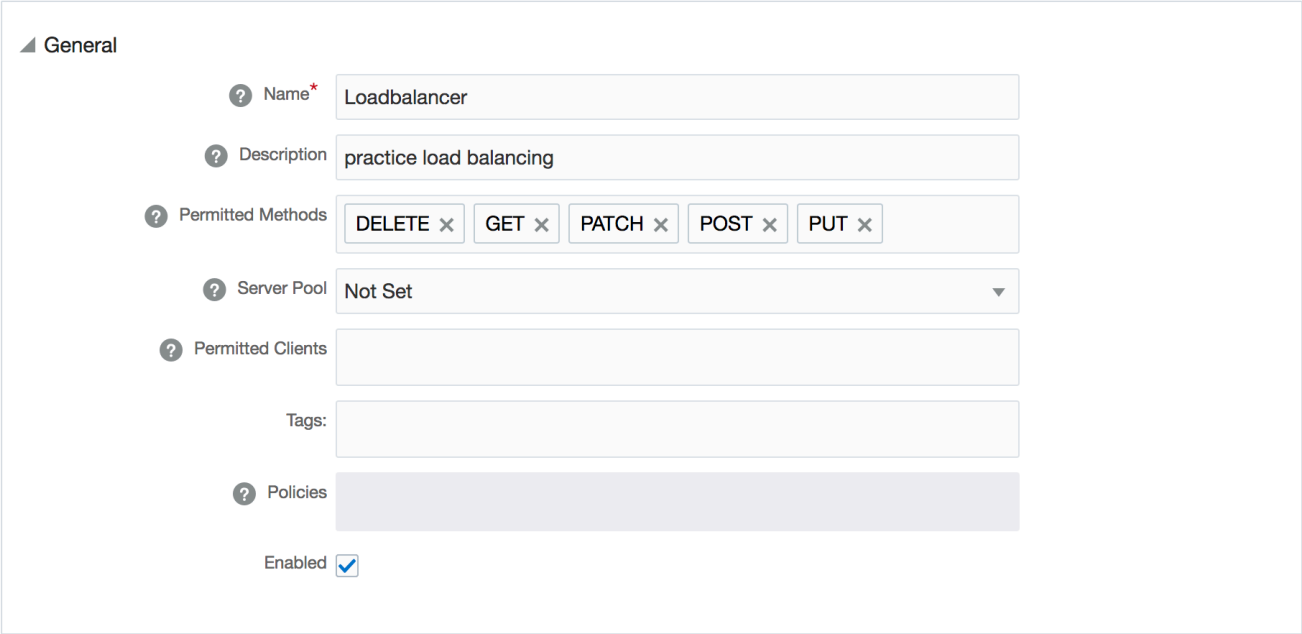
Practice 3-1: Creating Load Balancer

Creating a Load Balancer

1. On the Network page, expand Load Balancers in the left navigation pane and select **Load Balancers.**



2. Click Create Load Balancer. The Create Load Balancer dialog box appears.

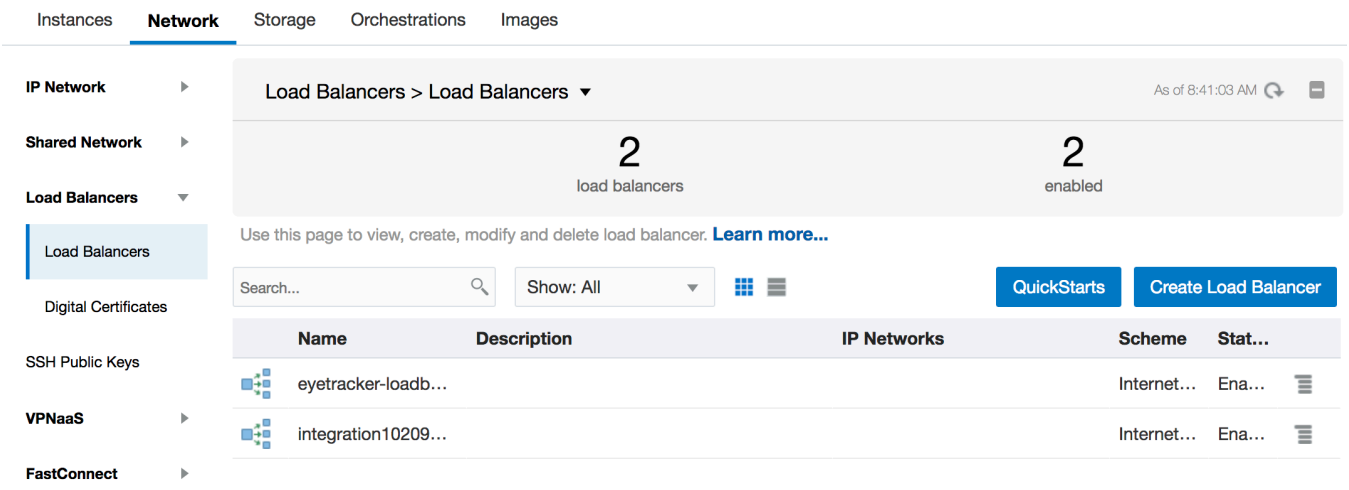


   - This image shows the Create Load Balancer dialog box.
3. In the Name field, enter **LoadBalancer1**, and accept the default values for the other fields.
   - The name you enter here is used to identify the load balancer in the Compute console.
4. Click **Create**.

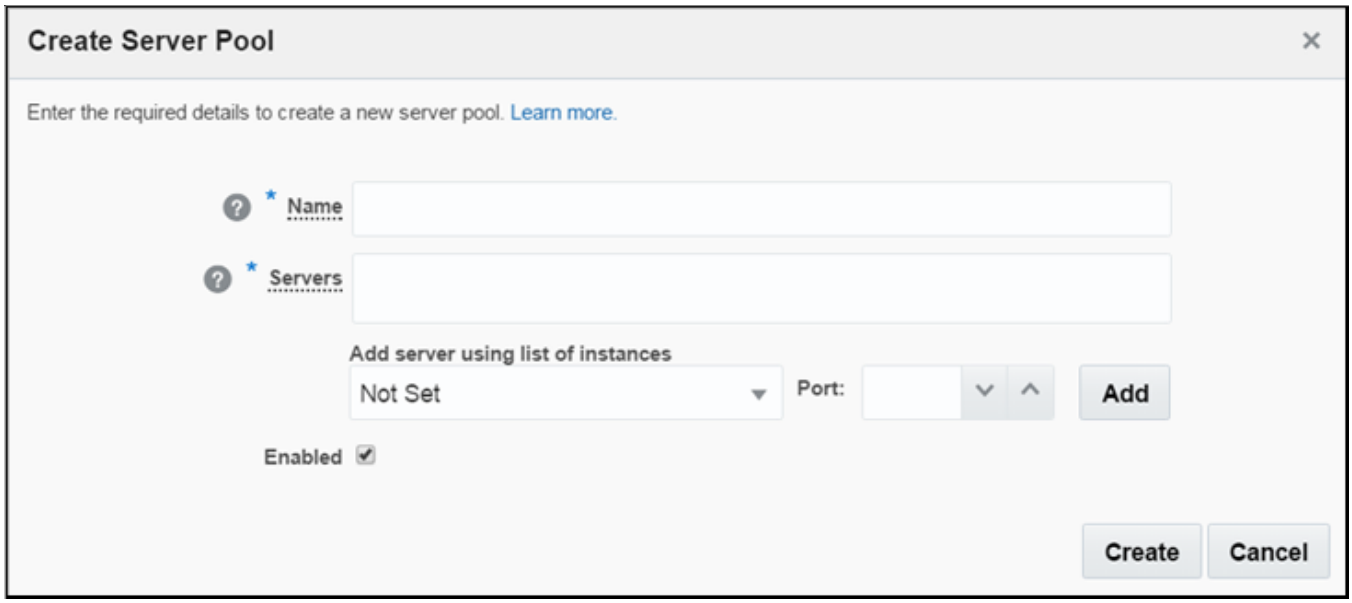
Practice 3-2: Creating the Server Pool for the Load Balancer

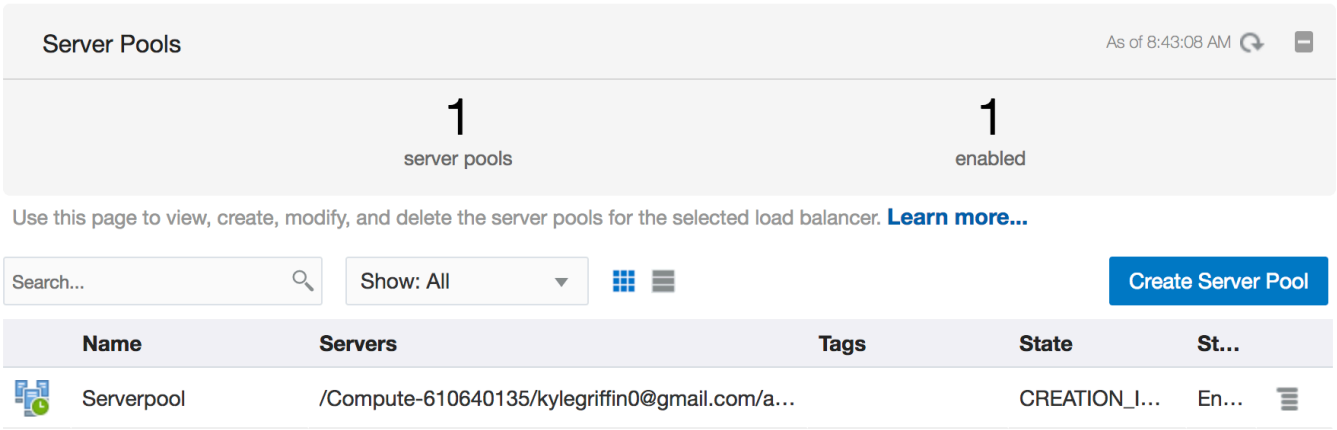
Create the Server Pool

1. Click the update icon This image shows the update icon for updating a load balancer. Next to the load balancer you just created, and select Update. The **Overview** page of the load balancer appears.



2. Click **Server Pools** in the left pane, and then click Create Server Pool. The Create Server Pool dialog box appears.



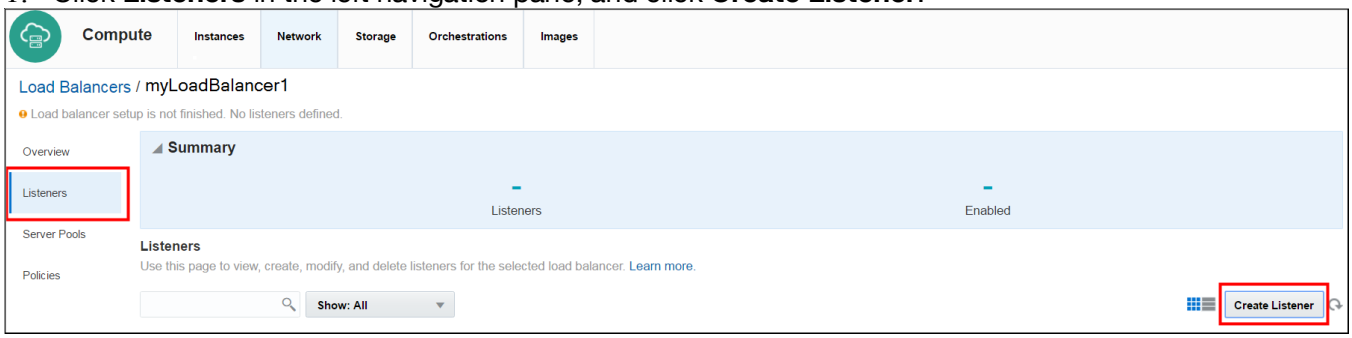


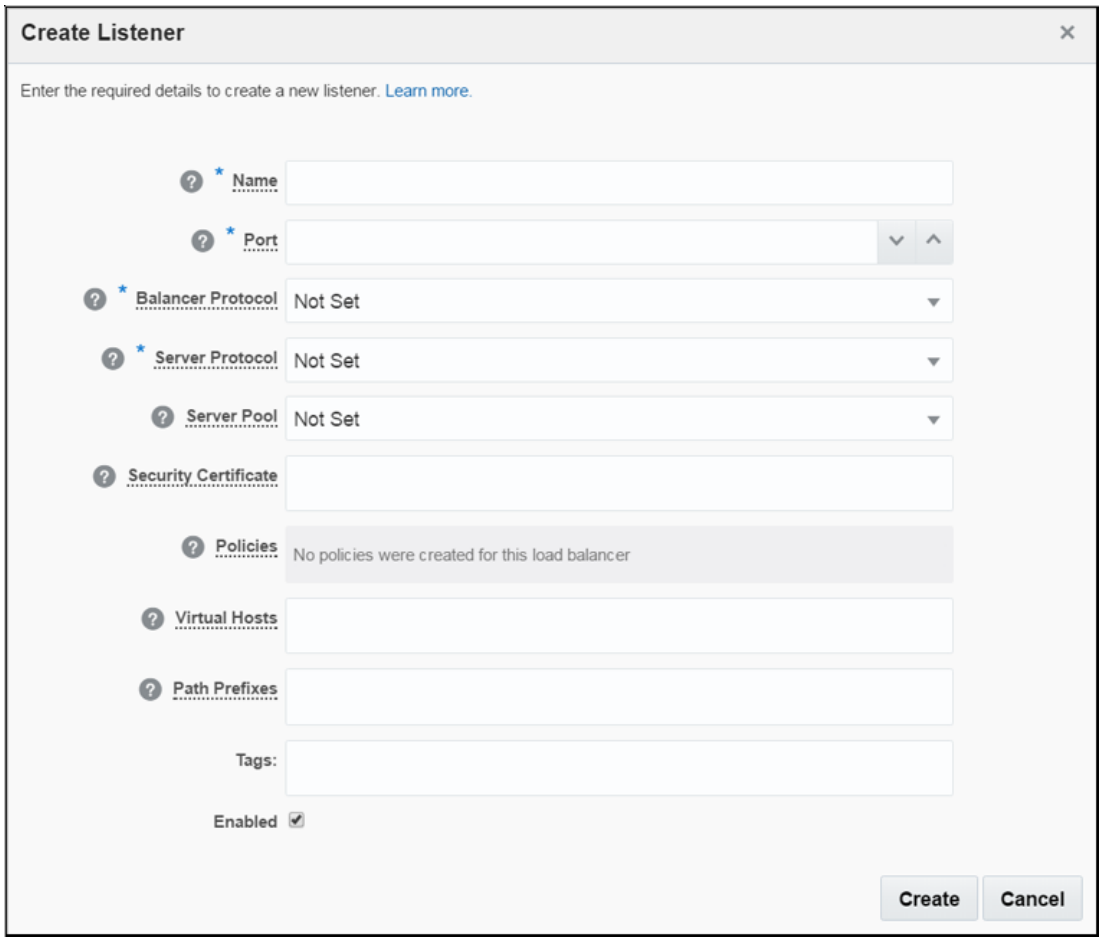
3. In the **Name** field, enter ServerPool1.

   This name is used to identify the server pool in the Compute console.
4. From the Add server using list of instances drop-down menu, select the first compute instance (WEBHOST1), and enter 80 in the Port field. Click **Add** to add <WEBHOST1 ip>:80 to the Servers field.
5. Use the same procedure to add WEBHOST2:80 to the Servers field.
6. Verify that the Enabled check box is selected, and click Create to create the server pool.

Practice 3-3: Creating a Listener for the Load Balancer

1. Click **Listeners** in the left navigation pane, and click **Create Listener**.





2. For the following fields in the Create Listener dialog box, do the following:

   Name: Enter myListener1
   Port: Enter 80
   Balancer Protocol: Select HTTP
   Server Protocol: Select HTTP
   Server Pool: Select serverPool1
   Virtual Hosts: Enter the canonical host name of the server. (optional)
   Enabled: Select this check box
   Click **Create** to create the listener.

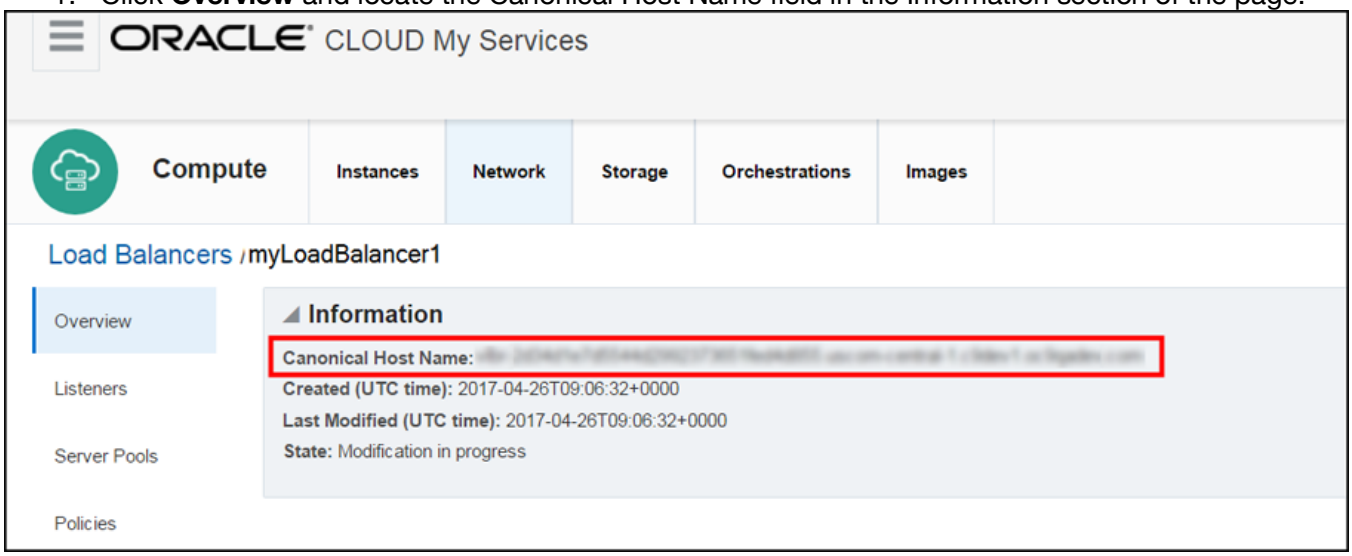
Adding IP Address of Load Balancer to Security List

Add the IP addresses of the load balancer to the Security IP list you created for the Compute instances in the server pool.

The security IP list identifies the IP addresses that can access the Compute instances. You should have already configured your IP network so HTTP requests can be received by the Compute instances, but this step ensures the load balancer IP is recognized by the Compute instances. See Managing Security IP Lists in Using Oracle Compute Cloud Service (IaaS)

Practice 3-4: Verifying the Load balancer

1. Click **Overview** and locate the Canonical Host Name field in the Information section of the page.



2. Use the value in the Canonical Host Name field to determine the URL you can use to access the load balancer. The URL is in the following form (**optional**):

   http://canonical_host_name/

3. Open a new browser window, and enter the URL of the load balancer.

4. Verify that the URL resolves successfully. If the URL resolves successfully, you have verified that the load balancer is up and running and sending requests to at least one server in the server pool.

5. Reload the page to see the load balancer change from WebServer1 and WebServer2