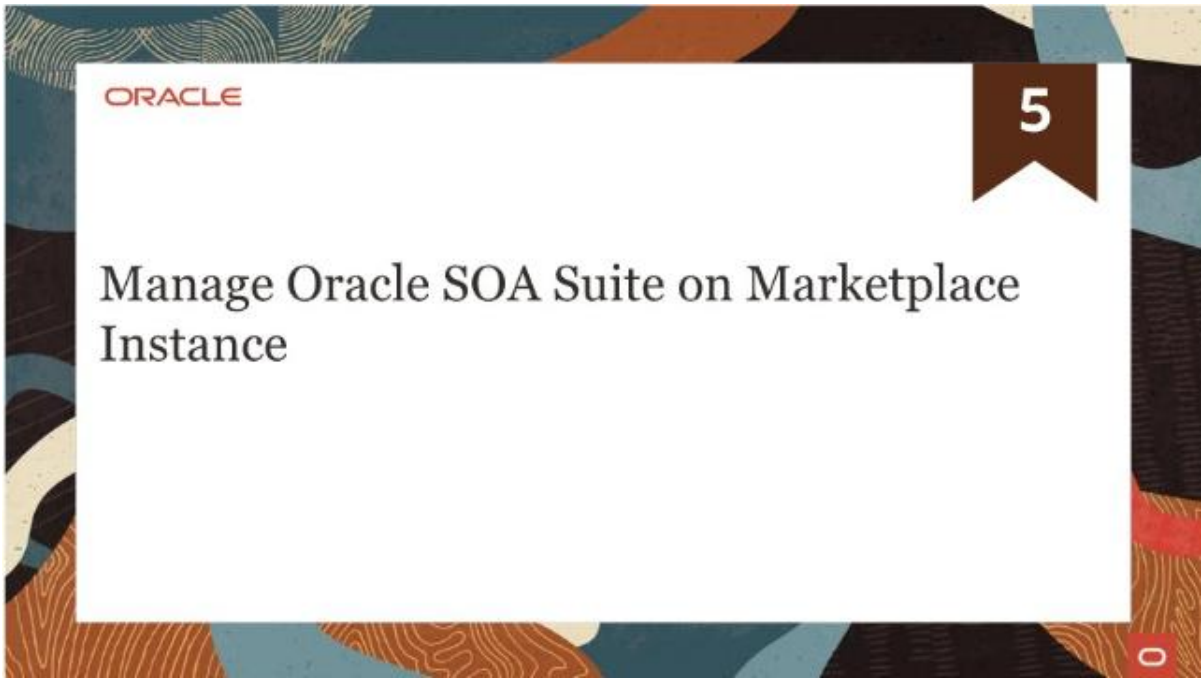

ORACLE
5
Manage Oracle SOA Suite on Marketplace Instance

Objectives

After completing this lesson, you should be able to:

- Know how to manage the Oracle SOA Suite on Marketplace Instance
- Know how to edit an Oracle SOA Suite on Marketplace Instance
- Understand how to add or delete a load balancer post-provisioning
- Access a VM through a secure shell

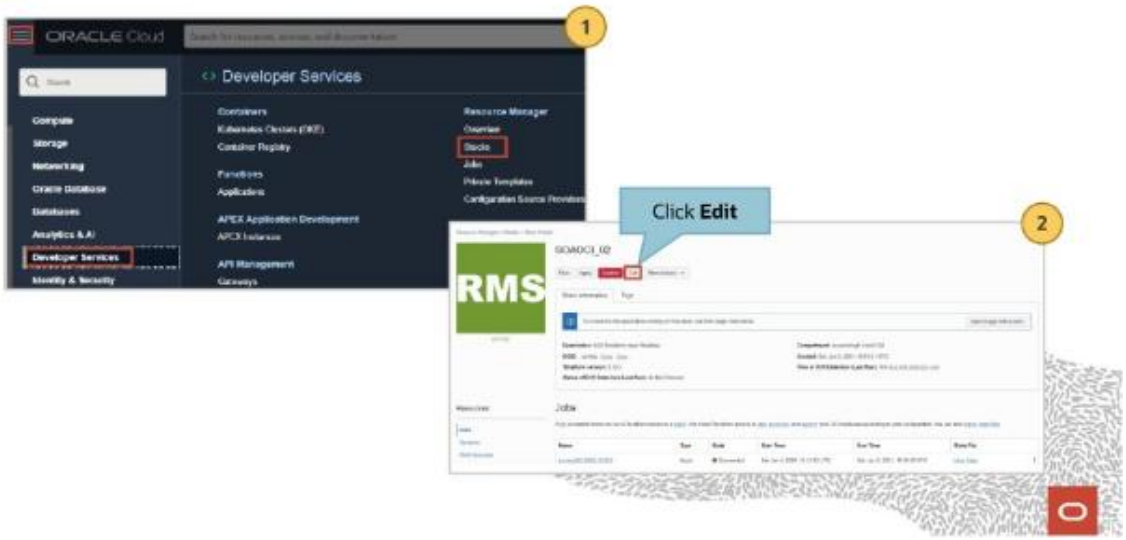
Manage Oracle SOA Suite on Marketplace Instance: Overview

Manage Oracle SOA Suite on Marketplace Instance

Oracle SOA Suite on Marketplace in Oracle Cloud Infrastructure is customer-managed, not Oracle-managed. This means that you are responsible for managing instances, including performing database management, completing backups, and installing patches. You can perform several management tasks from the Oracle Cloud Infrastructure Console.

- Edit an Oracle SOA Suite on Marketplace Instance
- Add or Delete a Load Balancer Post-Provisioning
- Access a VM Through a Secure Shell (SSH)
- Create an SSH Tunnel
- Change VM Users
- Run WLST Commands on a VM

Edit an Oracle SOA Suite on Marketplace Instance

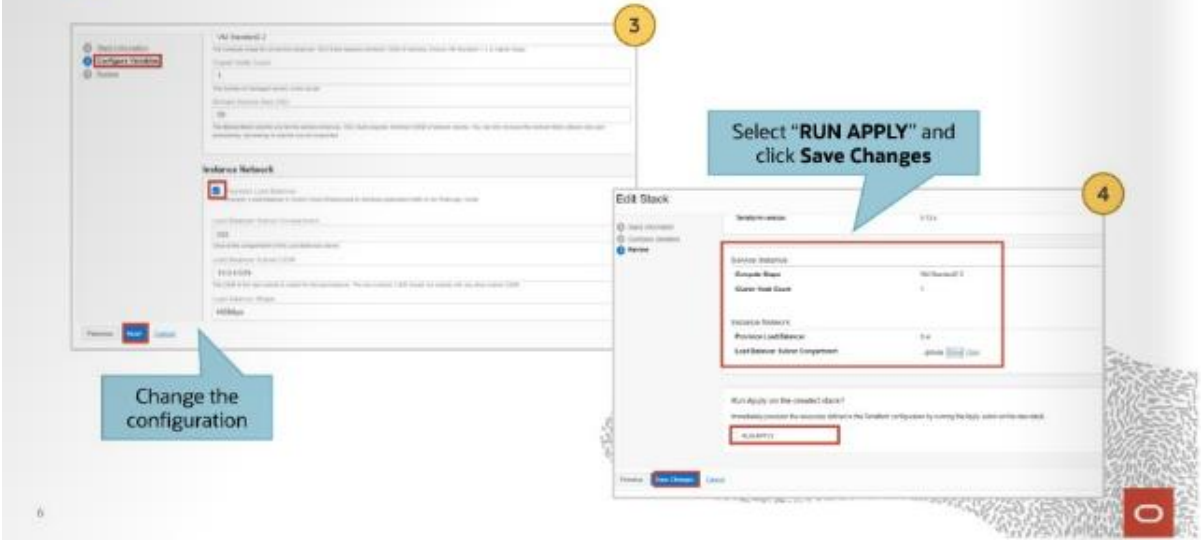


You can edit an Oracle SOA Suite on Marketplace instance from Resource Manager or the Details page.

To edit an Oracle SOA Suite on Marketplace instance:

1. From OCI console, expand Menu and click Developer Services→ Stacks
2. Go to the Stack Details page of the instance you want to edit.
3. On the Stack Details page, click **Edit Stack**.

Edit an Oracle SOA Suite on Marketplace Instance

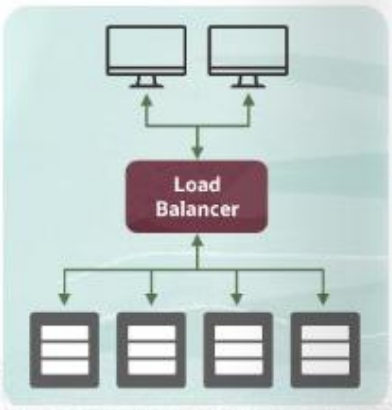


4. In the Edit Stack wizard, click **Next** to go to **Configure Variables** and edit any of the following editable fields as required: **Compute Shape**, Cluster Node Count
5. Domain Volume Size (GB) Load Balancer Subnet Compartment
6. Existing Subnet for Load Balancer
7. Load Balancer Shape for field descriptions.
8. Click **Next** to navigate to the Review page; select RUN APPLY and then click **Save Changes**.

Add a Load Balancer

Load Balancer

- Provides automated traffic distribution from one entry point into multiple backend servers in VCN.
- Includes a backend set to route incoming traffic to your Compute instances.
- Improves resource utilization, facilitates scaling, and helps ensure high availability



So, Oracle Cloud infrastructure Load Balancing Service provides an automated traffic distribution from one entry point into multiple backend servers in your Virtual Cloud Network.

A logical entity is defined by a list of backend servers, a load balancing policy, and a health check policy. SSL configuration is optional. The backend set determines how the load balancer directs traffic to the collection of backend servers.

This helps to load-balance large amounts of traffic, which could overwhelm a single server; it gives a mechanism to scale out an application tier by adding more servers and also provides the application higher availability, so even if one availability domain has an issue, you can still be up and running in other availability domains.

Load balancer is a regional service – load balancers come in pairs, active and passive, and public load balancers live in two separate availability domains providing HA, with no single point of failure.

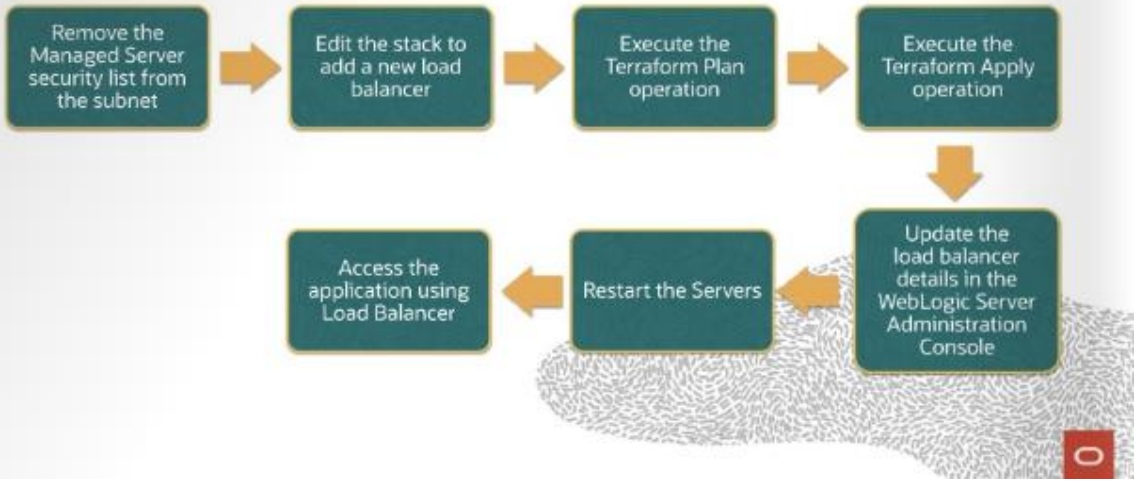
The OCI load balancer supports TCP and the usual http protocols, as well as HTTP/2 and websocket, supporting things like Data Compression, Server Push, Multiplexing of requests . . . all of these features are supported.

For security purposes, it supports SSL offloading, SSL termination, SSL end to end, and SSL tunneling.

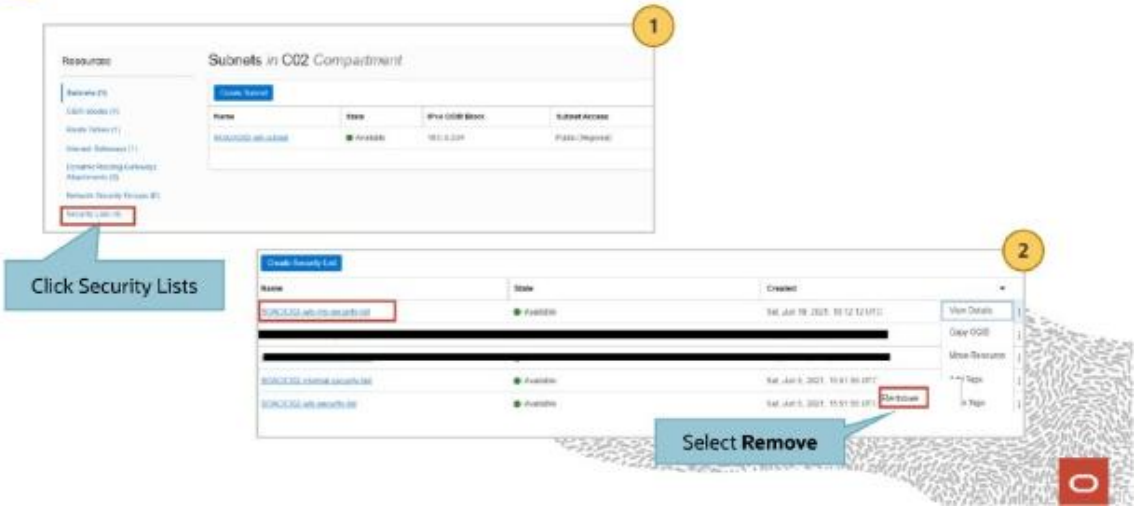
Load Balancer

- Existing or a new load balancer can be configured, post provisioning.
- Adding or deleting load balancer can be performed using OCI Console Resource Manager.
- Need to ensure that the SOA server is in running state.
- When you add a new load balancer, the following changes will affect the load balancer configuration
  - Any subsequent scale out or scale in operations to the SOA instance
  - Any changes to the stack such as de-provisioning

Add a New Load Balancer in a New Subnet



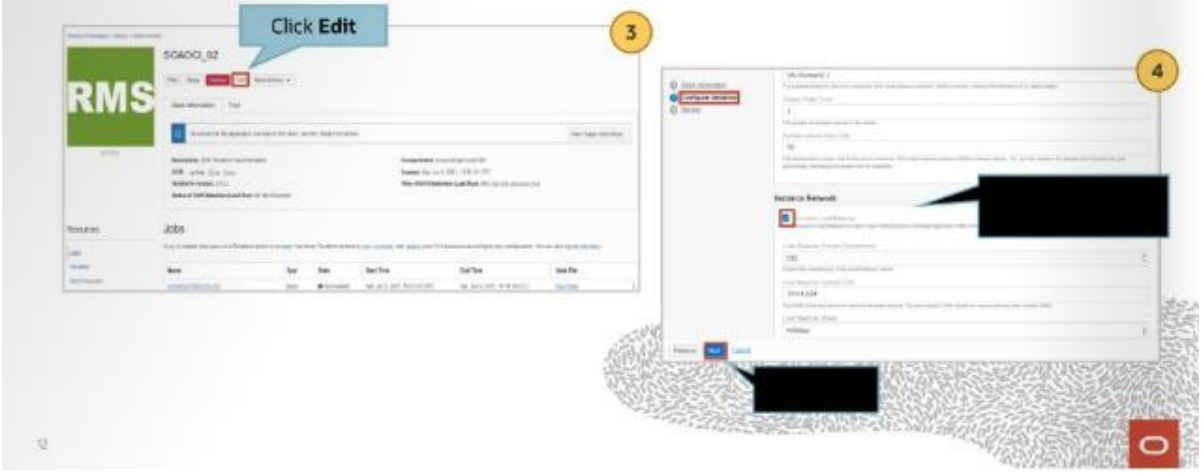
Remove the Managed Server Security List from Subnet



Remove the Managed Server security list from the subnet:

1. Sign in to the Oracle Cloud Infrastructure Console.
2. Open the navigation menu, click Networking, and then click Virtual Cloud Networks.
3. Select the VCN for the instance.
4. On the Virtual Cloud Network Details page, select the subnet for the instance.
5. On the Subnet Details page, locate the security list for the instance.
6. At the far right of the row for the security list, click and select Remove; then click Remove in the Remove Security List From Subnet dialog box.

Edit the Stack to Add a New Load Balancer in New Subnet



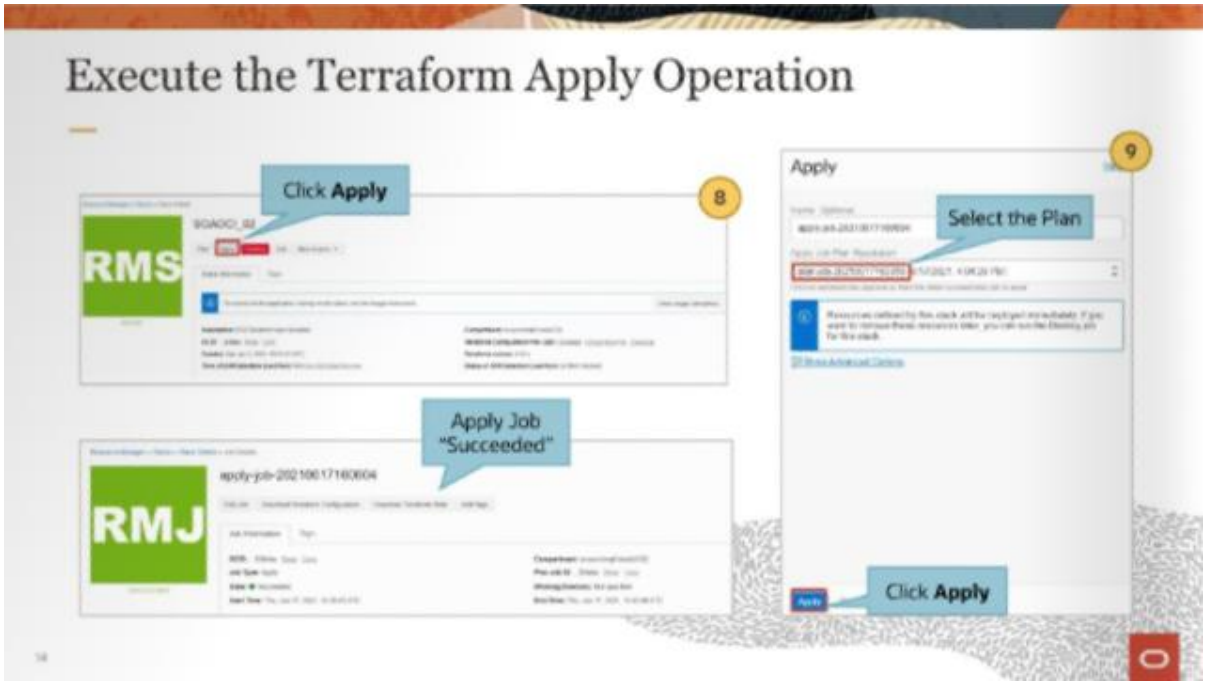
Edit the stack to add a new load balancer:

1. Go to the Stack Details page of the instance to which you want to add a load balancer.
2. On the Stack Details page, click Edit Stack.
3. In the Edit Stack wizard, click Next to go to Configure Variables and select the Provision Load Balancer check box; then select the required Load Balancer Shape.
4. Click Next to navigate to the Review page and then click Save Changes.

Execute the Terraform Plan Operation

Execute the Terraform Plan operation:

1. Go to the Stack Details page of the instance.
2. On the Stack Details page, click Terraform Actions and select Plan.
3. In the Plan dialog box, click Plan.



Execute the Terraform Apply operation:

1. The Terraform Apply operation creates a new load balancer, along with the associated resources such as a listener, backend sets, and so on.
2. When the Terraform Plan job completes successfully, click Terraform Actions and select Apply.
3. In the Apply dialog box, click Apply.

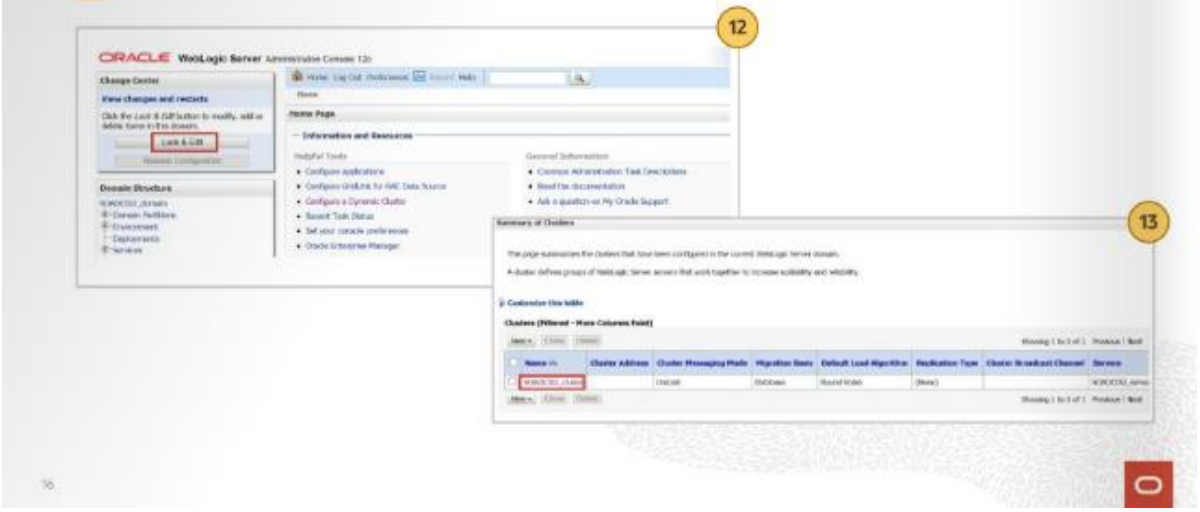
Get the Load Balancer Details and Validate Results

Get the load balancer details and validate results:

After the Terraform Apply operation completes successfully, view the log:

1. Go to the Stack Details page of the instance to which you want to add a load balancer.
2. In the Jobs section, click the job name to display the Job Details page.
3. Under Resources in the left pane, click Outputs to view the log.
4. Make a note of the load balancer URL and newly updated service console URLs at the end of the log.

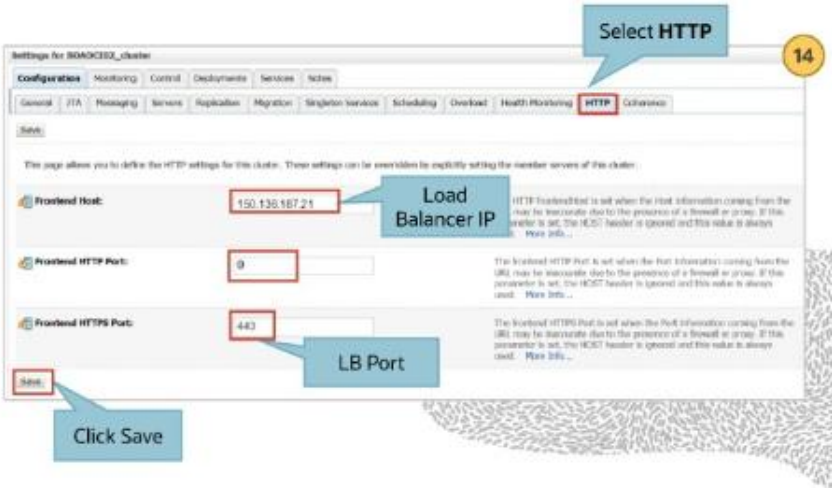
Update the Load Balancer Details in the WebLogic Server Administration Console



Update the load balancer console URL in the WebLogic Server Administration Console:

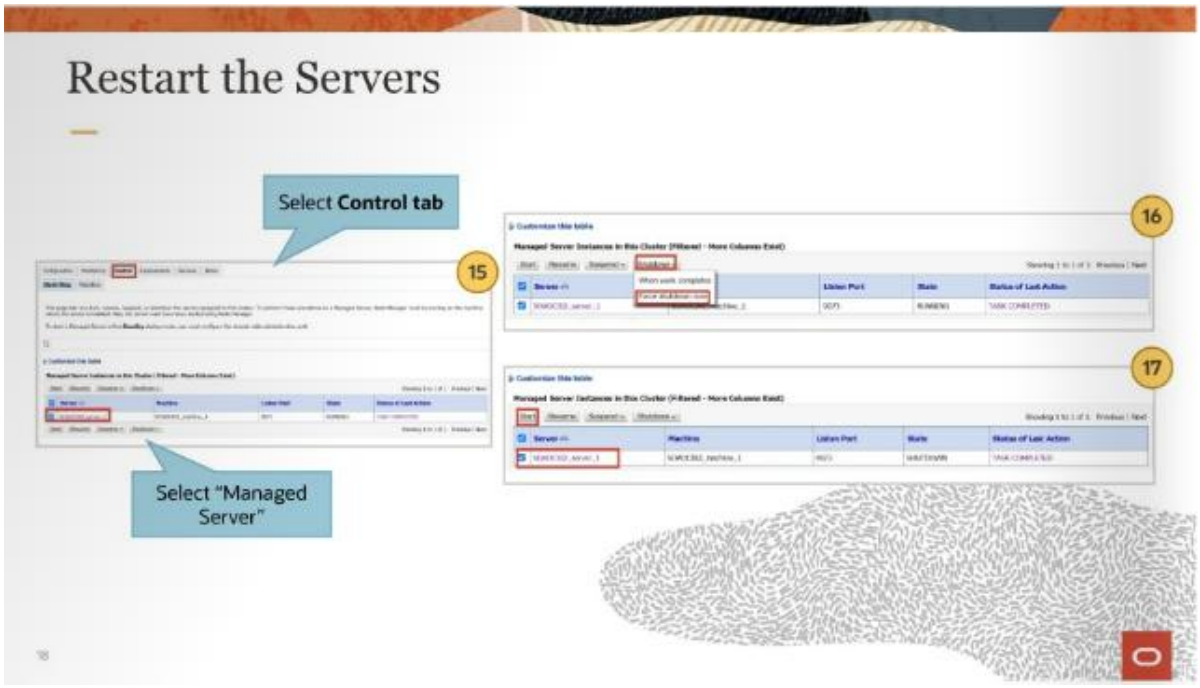
1. Log in to the WebLogic Server Administration Console, and under Domain Structure, expand Environment, select Clusters, and select your SOA cluster.

Update the Load Balancer Details in the WebLogic Server Administration Console



Update the load balancer console URL in the WebLogic Server Administration Console:

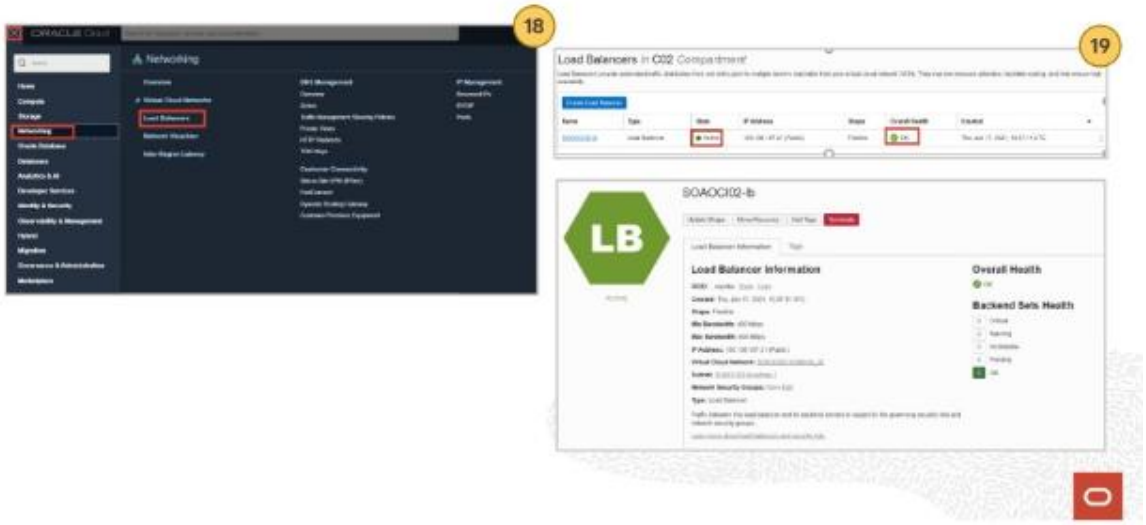
2. On the Configuration page, select the HTTP tab.
3. Update the Frontend Host value to the load balancer public IP address (from the log) and set the Frontend HTTPS Port to 443.
4. Click Save.



Restart the servers:

1. In the WebLogic Server Administration Console, select the Control tab and then the Start/Stop tab.
2. Select all Managed Servers and then click Shutdown and select Force shutdown now.
3. After shutdown completes, select all Managed Servers and click Start.

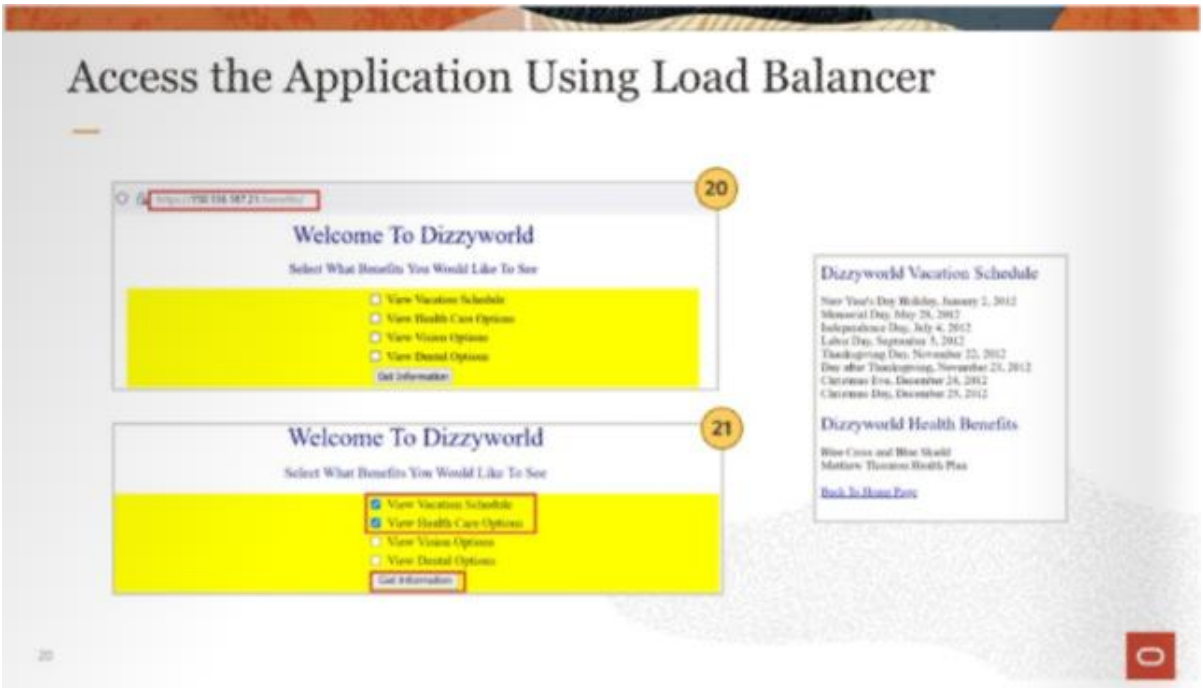
Verify the Load Balancer Health



Verify the Load Balancer Health:

From the OCI console, open the navigation menu and click Networking. Under Networking, click Load Balancers. You can see Load Balancer Overall Health is **OK.**

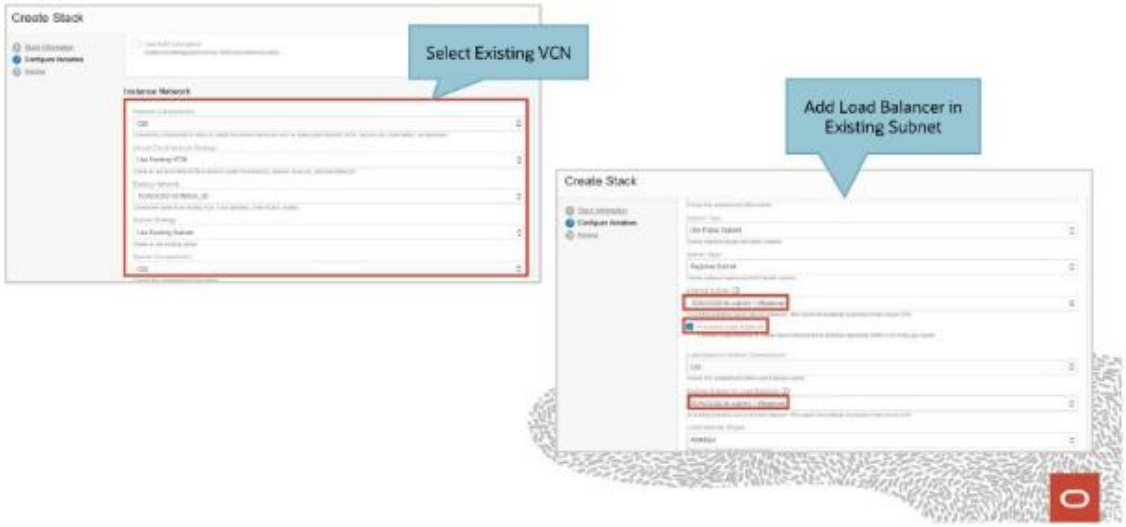
Access the Application Using Load Balancer



1. To access the application using Load Balancer, in your browser, enter the Load Balancer URL followed by context root, i.e., /benefits.
2. https://<Load Balancer IP>:<Load Balancer Port>/benefits

   Example : https://150.136.187.21:443/benefits

Add a New Load Balancer in an Existing Subnet

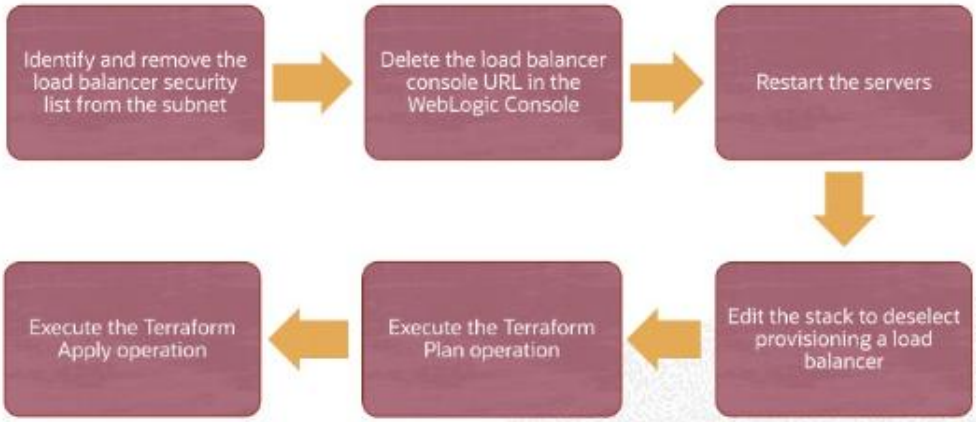


If you use an existing subnet, note that the provisioning process will not create any security lists to open ports in the subnets. You must open the ports explicitly before provisioning. To add a load balancer in an existing subnet:

1. Go to the Stack Details page of the instance to which you want to add a load balancer.
2. On the Stack Details page, click **Edit Stack**.
3. In the Edit Stack wizard, click **Next** to go to **Configure Variables** and select the PROVISION LOAD BALANCER check box; then select the required LOAD BALANCER SHAPE.
4. Click **Next** to navigate to the Review page and then click **Save Changes**.

Delete a Load Balancer

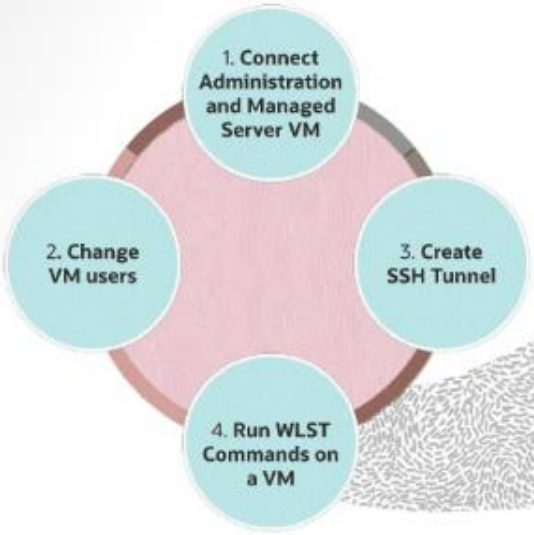
Delete a Load Balancer When Added in a New Subnet



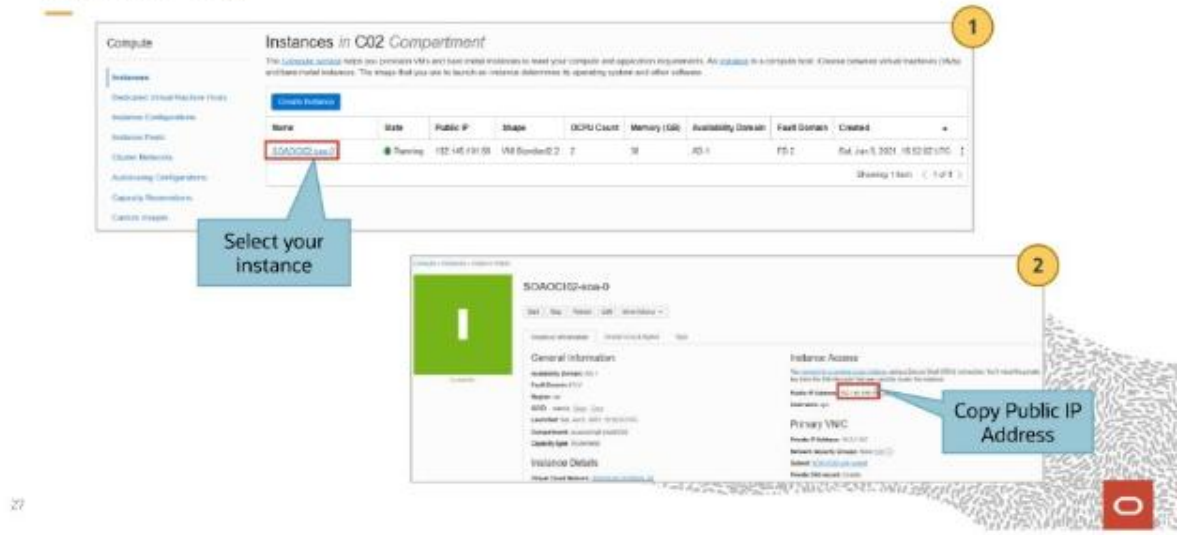
Delete a Load Balancer When Added in an Existing Subnet

Access a VM Through a Secure Shell (SSH)

Access a VM Through a Secure Shell (SSH)



Connect to the Administration and Managed Server VM

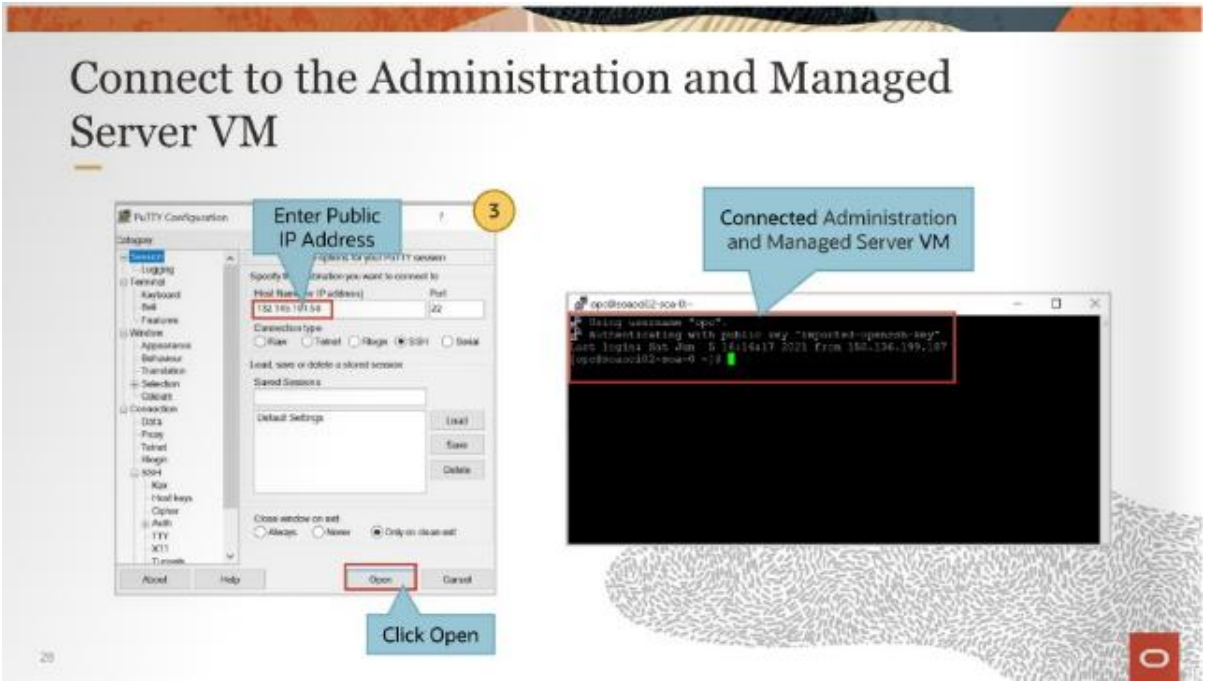


- You can access the Administration and Managed Server VM through a secure shell (SSH) utility.

To access the Administration Server VM through SSH:

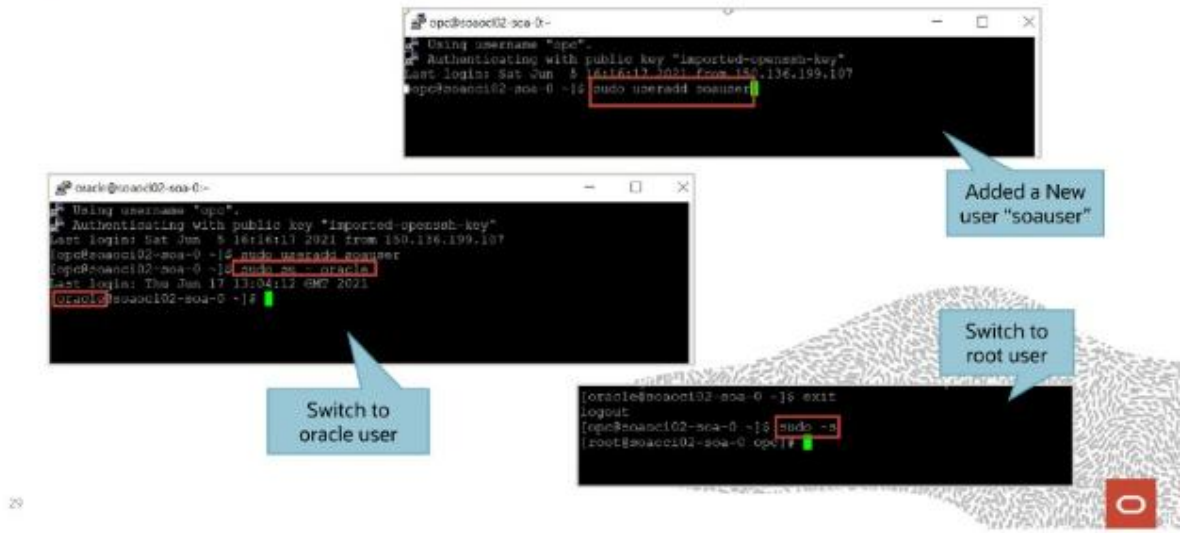
1. Sign in to the Oracle Cloud Infrastructure Console.
2. Open the navigation menu and click Compute. Under Compute, click Instances.
3. Click the instance associated with the VM you want to access.
4. Note the public IP address of the Administration Server VM.

The .ppk file extension indicates that the private key is in PuTTY's proprietary format. You must use a key of this format when using PuTTY. If you have to use a key saved in a different format, see the PuTTY documentation.



5. On Windows, you can use PuTTY, an open-source networking client for the Windows platform, to connect to the VM as the opc user.
   a. Launch PuTTY.
      - The PuTTY Configuration window is displayed, showing the Session panel.
   b. In the **Host Name (or IP address)** field, enter the public IP address of the VM.
   c. In the Category tree, expand Connection if necessary and then click **Data**.
   d. In the **Auto-login username** field, enter opc.
   e. Confirm that the **When username is not specified** option is set to **Prompt**.
   f. In the Category tree, expand **Connection > SSH** and then click **Auth**.
   g. Under **Private key file for authentication**, click **Browse**.
   h. Navigate to and select your private key file. Then click **Open**.
   i. Click **Open** to open the connection to the VM.
6. If the private key was defined with a passphrase, enter this value when prompted.

Change VM Users



- You can change users on a VM in order to perform specific administration tasks.
- You must SSH to a VM only as the opc user. This user has root privileges on the operating system (OS) running in the VM. For example, opc can be used to create other OS users on a VM. Simply prefix root operations with the sudo command.

Changing to the oracle user

The oracle user has regular OS user permissions. It is intended to be used to start and stop Oracle products that have been installed on the VM or to run other Oracle applications and utilities on the VM.

Changing to the root user

An alternative to using the sudo command to perform root OS operations as the opc user is to change to the root user.

Create an SSH Tunnel

To set up an SSH tunnel to an Administration Server VM:

1. Sign in to the Oracle Cloud Infrastructure Console.
2. Open the navigation menu and click Compute. Under Compute, click Instances.
3. Click the instance associated with the VM you want to access.
4. Note the public IP address of the Administration Server VM.
5. **On Windows, you can use PuTTY, an open-source networking client for the Windows platform, to create an SSH tunnel to the VM.**
   - To download PuTTY, go to http://www.putty.org/ and click the link to download PuTTY.
     a. Launch PuTTY. The PuTTY Configuration window is displayed, showing the Session panel.
     b. In the **Host Name (or IP address)** field, enter the public IP address of the VM.
     c. In the Category tree, expand **Connection** if necessary and then click **Data**.
     d. In the **Auto-login username** field, enter opc.
     e. Confirm that the **When username is not specified** option is set to **Prompt**.

f. In the Category tree, click **Connection > SSH**.

g. Under **Protocol options**, select the **Don't start a shell command at all** check box.

h. In the Category tree, expand **Connection > SSH** and then click **Auth**.

i. Under **Private key file for authentication**, click **Browse**.

j. Navigate to and select your private key file. Then click **Open**.

k. In the Category tree, click **Connection > SSH > Tunnels**.

l. In the **Destination** field, enter *IP*:*port*, where *IP* is the IP address of the VM and *port* is the port number on the VM to which you want to connect.

m. In the **Source Port** field, enter the same port number.

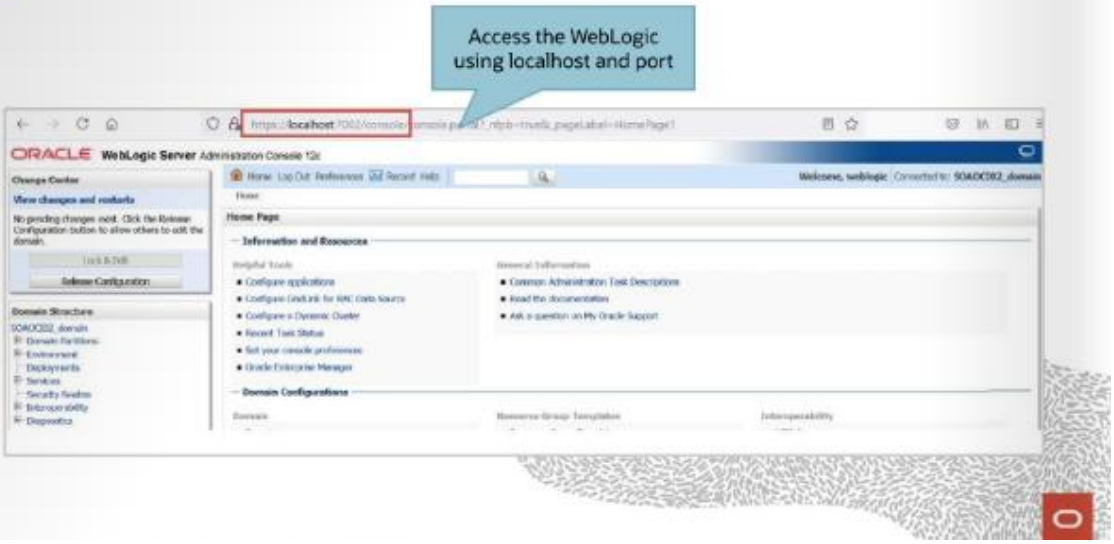
n. Click the **Add** button.

o. Click **Open** to create the SSH tunnel to the VM.

6. **If the private key was defined with a passphrase, enter this value when prompted.**

- **Applications running on your local machine can now communicate with the VM by using localhost:*port*, where *port* is the local port number.**
- **For example, after creating an SSH tunnel to port 7002 on the Administration Server VM, launch a web browser and connect to http://localhost:7002/console.**
  - The .ppk file extension indicates that the private key is in PuTTY's proprietary format. You must use a key of this format when using PuTTY. If you have to use a key saved in a different format, see the PuTTY documentation.
  - You can optionally save this session configuration by navigating to the Session panel and clicking Save. When you open PuTTY the next time, you can load this configuration by selecting it and clicking Load.
  - After your work with the SSH tunnel is complete, press Ctrl+C to shut down the SSH tunnel.

Accessing the WebLogic Administration Console



Once you create the SSH tunnel, it's time to access the WebLogic administration console using localhost.

Open the web browser and enter the url https://localhost:7002/console. After providing the user credentials, you will be able to see the home page of WebLogic.

So, you have successfully accessed the WebLogic administration console using localhost.

Run WLST Commands on a VM

Steps to run WLST commands on a VM:

1. Connect to the Administration Server VM.
2. Change to the **oracle** user.
3. Change the directory to the bin folder in **DOMAIN_HOME :cd $DOMAIN_HOME/bin**.
4. Set up the environment: . ./setDomainEnv.sh.
5. Start WLST : /u01/app/oracle/middleware/oracle_common/common/bin/wlst.sh.
6. Connect to the Admin Server: "connect('username', 'password', 'admin-server-host:admin-server-port')".

Example: connect('weblogic','Wwelcome#123','soaoci02soa0.subpubsoaoci02.soaoci02vcn.oraclevcn.com:9071')

You can run WLST commands from within any Oracle SOA Suite VM that includes an Oracle WebLogic Server installation.

You can refer to the documentation link for more information about WLST commands:
https://docs.oracle.com/middleware/12213/wls/WLSTC/reference.htm#WLSTC119

Summary

In this lesson, you should have learned how to:

- Manage the Oracle SOA Suite on Marketplace Instance
- Edit an Oracle SOA Suite on Marketplace Instance
- Add or delete a load balancer post-provisioning
- Access a VM through a secure Shell

Practice 5: Manage Oracle SOA Suite on Marketplace Instance

- Practice 5-1: Add a New Load Balancer in a New Subnet
- Practice 5-2: Connect to Administration and Managed Server VM
- Practice 5-3: Create an SSH Tunnel