

Practices for Lesson 5:
Manage Oracle SOA Suite on
Marketplace Instance

Overview

In these practices, you will learn how to:

- Add a new load balancer in a new subnet.
- Access a VM through a Secure Shell (SSH).
- Connect to the Administration Server VM.
- Change VM users.
- Create an SSH tunnel to the VM.

Practice 5-1: Add a New Load Balancer in a New Subnet

Overview

If you did not enable a load balancer when provisioning your Oracle SOA Suite on Marketplace instance, you can add a new load balancer at any time after provisioning.

In this practice, you will add a new load balancer in a new subnet and access an application using Load Balancer IP and port.

Assumptions

- You have completed the previous practices successfully.

Tasks

Here are the steps to be followed in order to add a load balancer in a new subnet:

1. Identify and remove the Managed Server security list from the subnet
2. Edit the stack to add a new load balancer
3. Execute the Terraform Plan operation
4. Execute the Terraform Apply operation
5. Get the load balancer details and validate results
6. Update the load balancer console URL in the WebLogic Server Administration Console
7. Restart the servers

Step 1 - Identify and remove the Managed Server security list from the subnet

1. Log in to your assigned Cloud account.
2. Open the navigation menu, click **Networking**, and then click **Virtual Cloud Networks**.
3. Navigate to Virtual Cloud Networks page; select your VCN (example: SOAOCI02-VCNSOA_02) from the list of VCNs.



The screenshot shows the Oracle Cloud console interface for Virtual Cloud Networks. On the left is a navigation menu with 'Networking' selected. The main area is titled 'Virtual Cloud Networks in C02 Compartment'. Below the title is a table listing VCNs. The first row, 'SOAOCI02-VCNSOA_02', is highlighted with a red box. The table columns are Name, State, IPv4 CIDR Block, IPv6 CIDR Block, Default Route Table, DNS Search Name, and Created. The 'SOAOCI02-VCNSOA_02' row shows a state of 'Available', an IPv4 CIDR block of '10.0.0.0/16', and a default route table of 'DEFAULT_ROUTE_TABLE_FOR_SOAOCI02_VCN_02002'. The DNS search name is 'soaoci02vcns02vcns02-001' and it was created on 'Thu, Apr 1, 2021, 17:39:29 UTC'.

Name	State	IPv4 CIDR Block	IPv6 CIDR Block	Default Route Table	DNS Search Name	Created
SOAOCI02-VCNSOA_02	Available	10.0.0.0/16	—	DEFAULT_ROUTE_TABLE_FOR_SOAOCI02_VCN_02002	soaoci02vcns02vcns02-001	Thu, Apr 1, 2021, 17:39:29 UTC

- Click **Subnets** in the left pane. In the subnet list, click **SOAOCI02-wls-subnet** to open the security list entries.



- Choose the security list "SOAOCI02-wls-ms-security-list." At the far right of the row for the security list, select **Remove** and then click **Remove** in the Remove Security List from Subnet dialog box.



Step 2 - Edit the stack to add a new load balancer

- Next, from navigation menu click **Developer Services**. Under Resource Manager, click **Stacks**.
- Click the name of your stack. (In our example, it is **SOAOCI_02**.)

8. On the Stack Details page, click **Edit** and **Select Edit Stack**.

Resource Manager > Stacks > Stack Details

SOAOCI_02

Plan Apply **Edit** More Actions

Stack Information Tags

To connect to the application running on this stack, see the Usage Instructions. [View Usage Instructions](#)

Description: SOA Terraform Input Variables
OCID: oqaqje-330x-c5v
Terraform version: 0.12.x
Status of Drift Detection (Last Run): @ Not Checked

Compartment: ocuocmgpl-ocyp-000
Created: Sat, Jun 5, 2021, 15:51:21 UTC
Time of Drift Detection (Last Run): N/A (see [OCID: SOAOCI_02](#))

Resources

Jobs

A job is created when you run a Terraform action on a stack. Use these Terraform actions to [apply](#), [destroy](#), and [delete](#) your OC resources according to your configuration. You can also [create state files](#).

Name	Type	Status	Start Time	End Time	State File
terraform-2021-06-05-15-51-21	Apply	Succeeded	Sat, Jun 5, 2021, 15:51:23 UTC	Sat, Jun 5, 2021, 16:10:26 UTC	View State

9. In the Edit Stack wizard, click **Next** to go to **Configure Variables** page.

Edit Stack

1 Stack Information
2 Configure Variables
3 Review

Terraform configuration source [?](#)

☐ Folder ☒ Zip file

Optional

Drop a zip file [Browse](#)

Working Directory

Use Terraform configuration files in the root folder

The file path to the directory from which to run Terraform

Name: Optional

SOAOCI_02

Description: Optional

SOA Terraform Input Variables

Terraform version

0.12.x

Support for Terraform version 0.11.x ends in May 2021.

Next Cancel

10. Select the **Provision Load Balancer** check box under **Instance Network**

Instance Network

☒ **Provision Load Balancer**
Provision a load balancer in Oracle Cloud Infrastructure to distribute application traffic to the WebLogic cluster.

Load Balancer Subnet Compartment
C02
Choose the compartment of the Load Balancer subnet.

Load Balancer Subnet CIDR
10.0.4.0/24
The CIDR of the new subnet is used for the load balancer. The new subnet's CIDR should not overlap with any other subnet CIDRs.

Load Balancer Shape
400Mbps

[Previous](#) [Next](#) [Cancel](#)

11. Click **Next** to navigate to the **Review** page; then click **Save Changes**.

Step 3 - Execute the Terraform Plan operation

12. To complete the addition of the load balancer, follow the below steps.
 - a. Click **Plan** on the Stack Details page.

Resource Manager > Stacks > Stack Details

RMS SOAOCI_02

[Plan](#) [Apply](#) [Destroy](#) [Edit](#) [More Actions](#)

Stack Information Tags

To connect to the application running on this stack, see the Usage Instructions. [View Usage Instructions](#)

Description: SOA Terraform input variables
OCID: oc4wps Stack: UCI-00
Created: Sat, Jun 5, 2021, 15:51:21 UTC
View of Stack Details (Last Run): N/A: Stack is in a failed state


Compartment: oc4wpsrgt/oc4wps/C02
Terraform Configuration File (.tf): [Upload New File](#) [Download](#)
Terraform version: 0.12.x
Status of Stack Details (Last Run): [Not Checked](#)

- # Plan

Help

Name: *Optional*

plan-job-20210617160316

 [Show Advanced Options](#)

Plan

Cancel

- Resource Manager > Theory > Stack Outputs > Job Outputs



While this job is running, only parameters are available. You can get a complete log when the job is finished.

plan-job-20210617160316

[Run job](#)
[Download Teradata Configuration](#)
[Cancel job](#)
[Add Tags](#)

Job information Tags

OID: [View](#) [Show logs](#)

Job type: Plan

Working directory: Not specified

Run time: N/A

Compartment: [messaging-mgmt-CO](#)

State: ● In progress

Start time: Thu, Jan 17, 2021, 10:14:20 UTC

- d. Go back to **Stacks Details** page; you can see Terraform Plan job with **Succeeded** state.

[illegible]

Step 4 - Execute the Terraform Apply operation

- e. From the Stack Details page, click **Apply**.

Resource Manager > Stacks > Stack Details



SOAOCI_02

[Plan](#)
[Apply](#)
[Loading](#)
[Edit](#)
[More Actions](#)

Stack Information

Tags



To connect to the application running on this stack, see the [Usage Instructions](#).

[View Usage Instructions](#)

Description: SOA Termination Input Variables

UUID: [js-nhja](#) [View](#) [Edit](#)

Created: Sat, Jun 8, 2024 10:57:31 UTC

Time of Drift Detection (Last Run): N/A [View drift detection logs](#)

Compartment: ocwocntrng-cvwy002

Termination Configuration File: [jargp](#) [Uploaded](#) [Download New File](#) [Download](#)

Termination version: 0.12.0

Status of Drift Detection (Last Run): @ Not Checked

- f. In the Apply dialog box, choose the Plan job that you have created, click Apply.

Apply [Help](#)

Name: *Optional*
apply-job-20210617160604

Apply Job Plan Resolution
plan-job-20210617160316 (6/17/2021, 4:04:26 PM)

Choose automatically approve or from the latest succeed plan job to apply

i Resources defined by this stack will be deployed immediately. If you want to remove these resources later, you can run the Destroy job for this stack.

[Show Advanced Options](#)

Apply [Cancel](#)

- g. Allow sufficient time for the apply job to complete. Initially, the status of the job will be **In Progress**.

Resource Manager > Stacks > Stack Details > Job Details

RMJ Resource Manager Jobs

i While this job is running, only partial logs are available. You can get a complete log when the job is finished.

apply-job-20210617160604

[Edit Job](#) [Download Transform Configuration](#) [Cancel Job](#) [Add Tags](#)

Job Information **Tags**

Job ID: `apply-job-20210617160604` **Job Type:** Apply **Status:** In Progress **Start Time:** Thu, Jun 17, 2021, 15:36:49 UTC **Compartment:** `aws-logs-2017-07-01-us-east-1` **Plan Job ID:** `plan-job-20210617160316` **Working Directory:** Not specified **End Time:** N/A

- h. Go back to Stack Details page; you can view the **Apply** job with **Succeeded** state.



SOAOCI_02

Plan: Apply **Succeeded** 0.00 Work History

Stack Information | **Tags**

To connect to the application running on this stack, see the [usage instructions](#).

Description: SOA for plan-type/variables
OOD: [view](#) [edit](#) [copy](#)
Created: Sat, Jun 17, 2023, 10:17:11 CDT
Name of SOA Detection Last Run: Not Successful detection run

Component: [view](#) [edit](#) [copy](#)
Service Configuration File (API): [view](#) [edit](#) [copy](#)
Service Version: 1.0.0
Name of SOA Detection Last Run: Not Successful

Resources

Jobs

A job is created when you create a service instance on a stack. Use the [Jobs](#) section to view, [download](#), and [delete](#) jobs. To download a job, click the [Download](#) link.

Name	Type	Status	Start Time	End Time	Stack File
apply-job-20210617160604	Apply	Succeeded	Fri, Jun 17, 2023, 10:30:45 CDT	Fri, Jun 17, 2023, 10:40:45 CDT	Download
stack-20210617160604	Plan	Succeeded	Fri, Jun 17, 2023, 10:30:45 CDT	Fri, Jun 17, 2023, 10:40:45 CDT	

13. Click the **apply job** name, and it displays the Job Details page as shown below.



apply-job-20210617160604

Download Job | Download Service Configuration | Download Service File | Add Tags

Job Information | **Tags**

OOD: [view](#) [edit](#) [copy](#)
Job Type: Apply
Status: **Succeeded**
Start Time: Fri, Jun 17, 2023, 10:30:45 CDT

Component: [view](#) [edit](#) [copy](#)
Plan Job ID: [view](#) [edit](#) [copy](#)
Working Directory: Not specified
End Time: Fri, Jun 17, 2023, 10:40:45 CDT

Resources

Logs

[Download logs](#) | [Show Threadlogs](#)

Initializing...

- Start time: 2023-06-17 10:30:45 CDT
- End time: 2023-06-17 10:40:45 CDT
- Job type: Apply
- Job ID: apply-job-20210617160604
- Stack ID: stack-20210617160604
- Stack name: SOA for plan-type/variables
- Stack version: 1.0.0
- Stack file: [download](#)
- Stack file path: [download](#)
- Stack file size: [download](#)
- Stack file type: [download](#)
- Stack file content: [download](#)

Step 5 - Get the load balancer details and validate results

- Under **Resources** in the left pane, click **Outputs** to view the load balancer URL and newly updated service console URLs.

Resources

Logs

Metrics

Associated Resources

Outputs

View State

Outputs

Key	Value
EMR_Container	https://132.145.181.58/7032wem
Instance_Schedule_Id	ip4k9w6: 0:00: 0:00
LoadBalancer_Public_Ip	150.133.167.21
LoadBalancer_Subnet_Id	ip4k9w6: 0:00: 0:00
Service_Consoles	ip4k9w6: 0:00: 0:00
Service_Instances	181.181.1.0:00: 0:00
Version	12.2.1.4 (RF with ATP D0)
Virtual_Cloud_Network_Id	ip4k9w6: 0:00: 0:00
Waiting_Address_Route_Console	https://132.145.181.58/7032wem

- Alternatively, click **Logs** and scroll through the log file till the end and identify load balancer IP address and updated service console URLs that you can use to access the instance. Here you can make a note of **Load Balancer** public IP address.

[illegible]

Add Ingress Rules to access WebLogic Server Administration Console and other consoles:

Add the following ingress rule in security list **SOAOCI02-wls-security-list**, which is under **"SOAOCI02-wls-subnet"** of your VCN. Detailed steps are listed in the practices for Lesson 3.

Rule 1:

- a. **SOURCE TYPE:** Select **CIDR**.
- b. **SOURCE CIDR:** Enter the public IP address of the machine where the Administration Server URL is opened from a browser (for example, if the public IP address is 123.123.456.456 then enter 123.123.456.456/32).
- c. **IP PROTOCOL:** Select **TCP**.
- d. **DESTINATION PORT RANGE:** 7002
- e. **Description:** To access WebLogic and Enterprise Manager
- f. Click **Add Ingress Rules**.

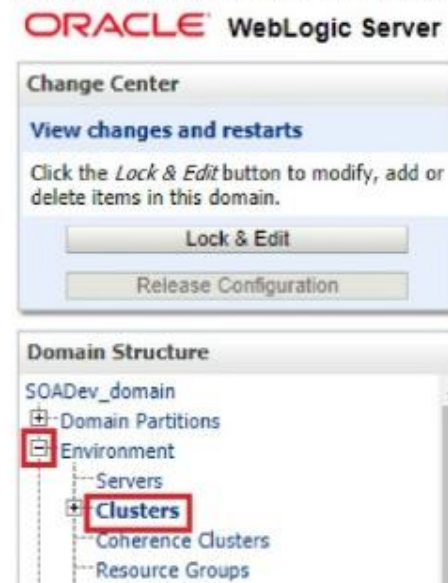
Step 6 - Update the load balancer console URL in the WebLogic Server Administration Console:

1. Access the WebLogic Administration Console using the URL <https://132.145.191.58:7002/console> (this is an example URL in our case and it will be different for you) and provide the username as "weblogic" and password as "Wwelcome#123" and then click "Login".
2. It displays the WebLogic Server Administration console home page.

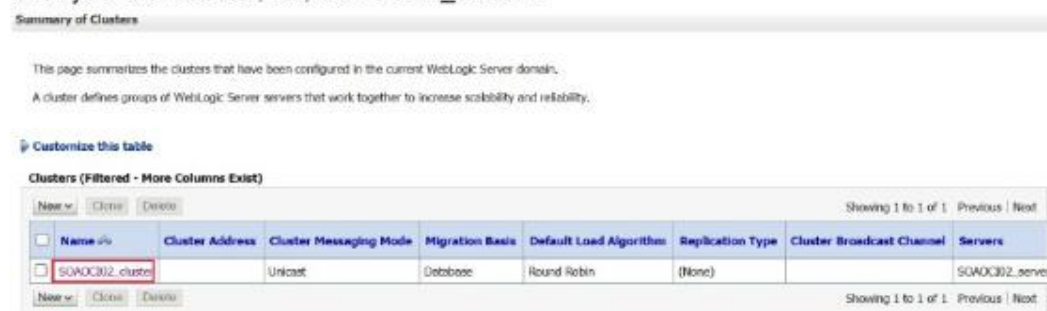
- Click "Lock & Edit."



- Under Domain Structure, expand **Environment** and select **Clusters**.



- Click your SOA cluster, i.e., **SOAOC102_cluster**.



6. On the Configuration page, select the **HTTP** tab.
 - a. Update the **Frontend Host** value to the **Load Balancer public IP address**.
 - b. Set the **Frontend HTTPS Port** to 443.
 - c. Click **Save**.

Settings for SOAOCIO2_cluster

Configuration Monitoring Control Deployments Services Notes

General JTA Messaging Servers Replication Migration Singleton Services Scheduling Overload Health Monitoring **HTTP** Cofession

Save

This page allows you to define the HTTP settings for this cluster. These settings can be overridden by explicitly setting the member servers of this cluster.

Frontend Host: 150.136.167.21

Frontend HTTP Port: 0

Frontend HTTPS Port: 443

Save

- d. Ensure that the settings are updated successfully.

Step 7 – Restart the servers

7. Next, select the **Control** tab; select the Managed Server, i.e., SOAOCIO2_server_1.

Configuration Monitoring **Control** Deployments Services Notes

Start/Stop Migration

This page lets you start, resume, suspend, or shutdown the servers assigned to this cluster. To perform these operations on a Managed Server, Node Manager must be running on the machine where the server is installed. Also, the server must have been started using Node Manager.

To start a Managed Server in the **Standby** startup mode, you must configure the domain-wide administration port.

Customize this table

Managed Server Instances in this Cluster (Filtered - More Columns Exist)

Start Resume Suspend Shutdown Showing 1 to 1 of 1 Previous Next

Server	Machine	Listen Port	State	Status of Last Action
SOAOCIO2_server_1	SOAOCIO2_machine_1	9073	RUNNING	TASK COMPLETED

Start Resume Suspend Shutdown Showing 1 to 1 of 1 Previous Next

8. Click **Shutdown** and select **Force shutdown now** from the drop-down list.

Customize this table

Managed Server Instances in this Cluster (Filtered - More Columns Exist)

Start Resume Suspend **Shutdown** Showing 1 to 1 of 1 Previous Next

Server	Machine	Listen Port	State	Status of Last Action
SOAOCIO2_server_1	SOAOCIO2_machine_1	9073	RUNNING	TASK COMPLETED

When work completes
force shutdown now

9. Click **Yes** to continue.
10. Allow sufficient time to shut down the server, and you can see the server state as "SHUTDOWN."

11. After shutdown completes, select the Managed Servers and click **Start**.

Customize this table

Managed Server Instances in this Cluster (Filtered - More Columns Exist)

Start Resume Suspend Shutdown Showing 1 to 1 of 1 Previous Next

Server	Machine	Listen Port	State	Status of Last Action
SOAOC02_server_1	SOAOC02_machine_1	9073	SHUTDOWN	TASK COMPLETED

12. Click **Yes** to continue.

13. Allow sufficient time (3 to 4 mins) to **start** the server, and you can see the state as **"RUNNING."**

Customize this table

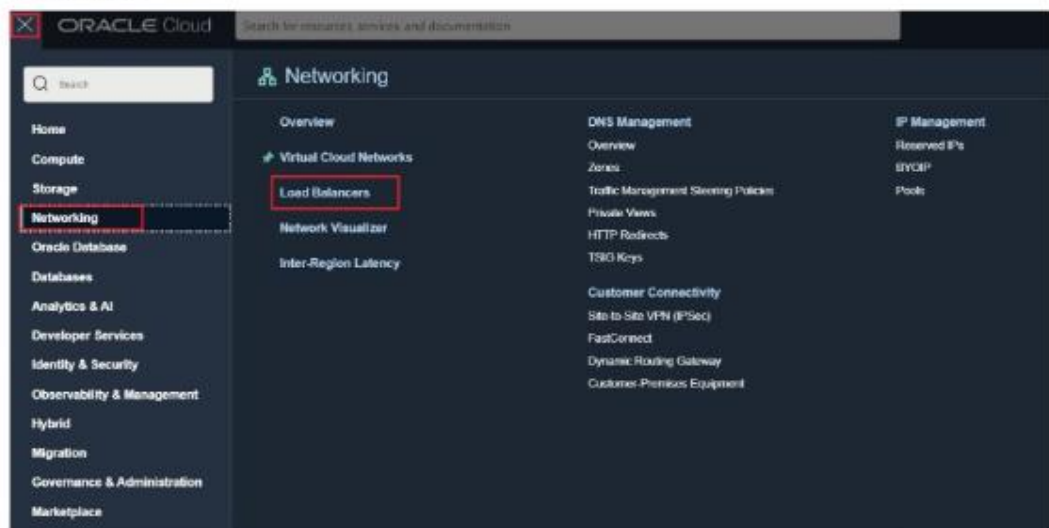
Managed Server Instances in this Cluster (Filtered - More Columns Exist)

Start Resume Suspend Shutdown Showing 1 to 1 of 1 Previous Next

Server	Machine	Listen Port	State	Status of Last Action
SOAOC02_server_1	SOAOC02_machine_1	9073	RUNNING	TASK COMPLETED

Verify the health of the Oracle Cloud Infrastructure load balancer:

1. From the OCI console, open the navigation menu and click **Networking**. Now click **Load Balancers**.



2. Select the **compartment** that is assigned to you.

List Scope

Compartment

C02

ocucictmg6 (root)/C02

3. You can see a load balancer, i.e., **SOAOCI02_lb** with active state, and Overall Health is **OK**.

Load Balancers in C02 Compartment

Load Balancers provide automated traffic distribution from one entry point to multiple servers reachable from your virtual cloud network (VCN). They improve resource utilization, facilitate scaling, and help ensure high availability.

Create Load Balancer						
Name	Type	State	IP Address	Shape	Overall Health	Created
SOAOCI02-lb	Load Balancer	Active	150.136.167.21 (Public)	Flexible	OK	Thu, Jun 17, 2021, 10:37:11 UTC

4. In case your Load Balancer Overall Health is **Critical** or **Warning** or **Unknown**, follow the below steps to update the Load Balancer Overall Health as **OK**.

- a. Select the Load Balancer name, and it displays the details page.



ACTIVE

SOAOCI02-lb

Update Shape Move Resource Add Tags Terminate

Load Balancer Information Tags

Load Balancer Information

OCID: ovcnka-2lam-02m
Created: Thu, Jun 17, 2021, 10:37:11 UTC
Shape: Flexible
Min Bandwidth: 400 Mbps
Max Bandwidth: 400 Mbps
IP Address: 150.136.167.21 (Public)
Virtual Cloud Network: SOAOCI02-VCN
Subnet: SOAOCI02-subnet-1
Network Security Groups: None (0)
Type: Load Balancer
Traffic between this load balancer and its backend servers is subject to the governing security rule and network security groups.
[Learn more about load balancers and security rules.](#)

Overall Health

OK

Backend Sets Health

OK

- b. Select **Backend Sets** under Resources and click **SOAOCI02-lb-backendset**.

Resources

Link

Backend Sets (1)

Backend Pools (0)

Rule Sets (0)

Listeners (1)

Backend Sets

Create Backend Set

Name	Other Suite	Traffic Distribution Policy	Number of Backends	Health
SOAOCI02-lb-backendset		Weighted Round Robin	1	OK

Showing 1 item 1 of 1

- c. Select **Backends**.

- d. Next, select the check box and click **Add Backends**.

<input checked="" type="checkbox"/>	IP Address	Port	Weight	Drain	Offline	Backup
<input checked="" type="checkbox"/>	10.0.3.107	9073	1	False	False	False

- e. Choose your Compute Instance; change the port as "9073". Click **Add**.

Choose how to add backend servers by selecting Compute instances or by entering IP addresses.

☒ Compute Instances ☐ IP Addresses

Specify the Compute instances to include in your set of backend servers.

Instances in C02 [\(Choose Compartment\)](#)

<input type="checkbox"/>	Name	IP Address	OCID	Availability Domain	Port	Weight
<input type="checkbox"/>	CohRN144-coh-0	10.0.3.201	...3ootnq Show Copy	yQUJ-US-ASHBURN-AD-1	80	1
<input type="checkbox"/>	CohRN26a-bastion-instance	10.0.6.221	...ola5pa Show Copy	yQUJ-US-ASHBURN-AD-1	80	1
<input type="checkbox"/>	CohRN26a-coh-0	10.0.3.200	...lpwq Show Copy	yQUJ-US-ASHBURN-AD-1	80	1
<input checked="" type="checkbox"/>	SOAOC102-soa-0	10.0.3.107	...naesq Show Copy	yQUJ-US-ASHBURN-AD-1	9073	1

1 Selected Showing 4 items < 1 of 1 >

To enable load balancer traffic, add ingress and egress security list rules to the corresponding subnets.

☐ Manually configure security list rules after the backend servers are added

☒ Automatically add security list rules

Add Cancel

- f. Click **Close** and allow sufficient time for the work request to complete.
- g. You will see the Load Balancer Health changed from previous state to **OK** state.

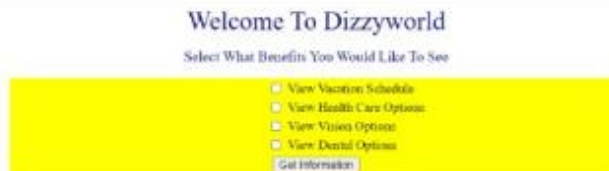
5. To access the newly deployed web application using Load Balancer, perform the following steps:

- a. In another tab of your browser, enter the Load Balancer URL followed by **context-root**, i.e., /benefits.

https://<Load Balancer IP>:<Load Balancer Port>/benefits

Example : <https://150.136.187.21:443/benefits>

- b. It displays the home page of **dizzy** managed server.



- c. Select "View Vacation Schedule" and "View Health Care Options" and click **Get Information** button.



- d. It displays the output as shown below.

Dizzyworld Vacation Schedule

New Year's Day Holiday, January 2, 2012
Memorial Day, May 28, 2012
Independence Day, July 4, 2012
Labor Day, September 3, 2012
Thanksgiving Day, November 22, 2012
Day after Thanksgiving, November 23, 2012
Christmas Eve, December 24, 2012
Christmas Day, December 25, 2012

Dizzyworld Health Benefits

Blue Cross and Blue Shield
Matthew Thornton Health Plan

[Back To Home Page](#)

- e. Click the **Back To Home Page** link to go back to the Home page.

This completes the task of creating a load balancer and accessing the deployed application with load balancer IP and port.

Practice 5-2: Connect to Administration and Managed Server VM

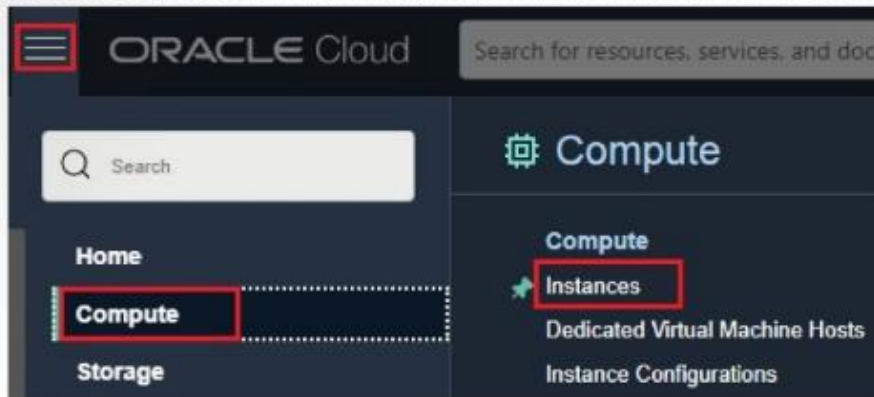
Overview

You can change users on a VM in order to perform specific administration tasks.

In this practice, you will learn how to connect to Administration and Managed Server VM and change the users in VM.

Tasks

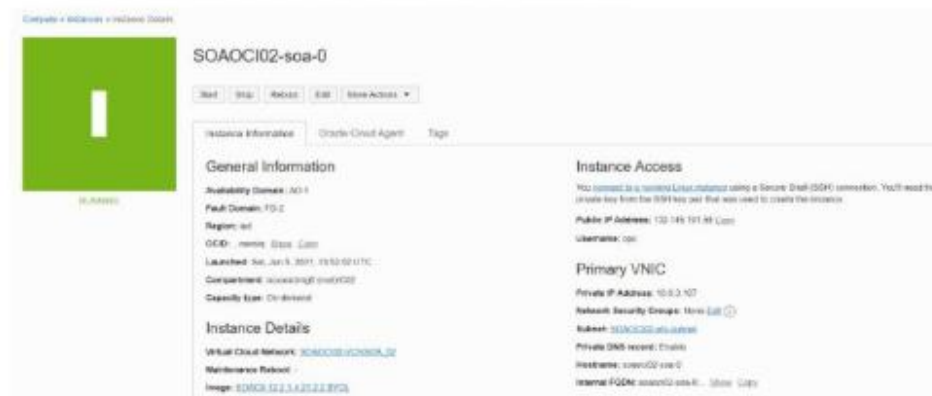
1. From the OCI console, open the navigation menu and click **Compute** → **Instances**.



2. Select the compartment that is assigned to you and click the instance name (example: in our case, it is **SOAOCI02-soa-0**).

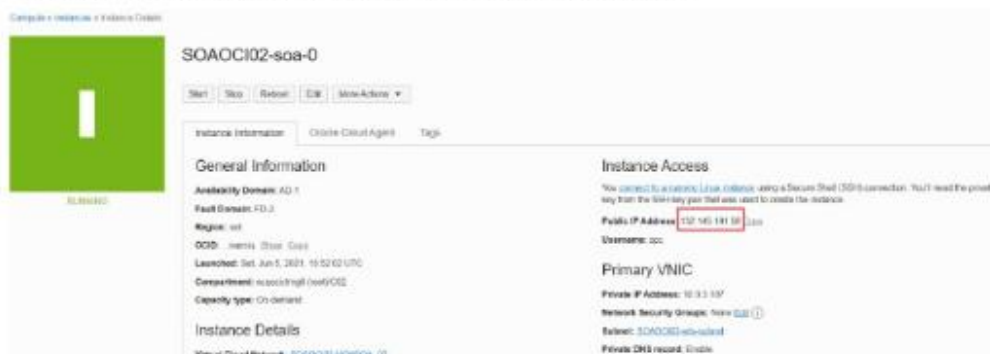


3. You can see the Instance Information as shown below.



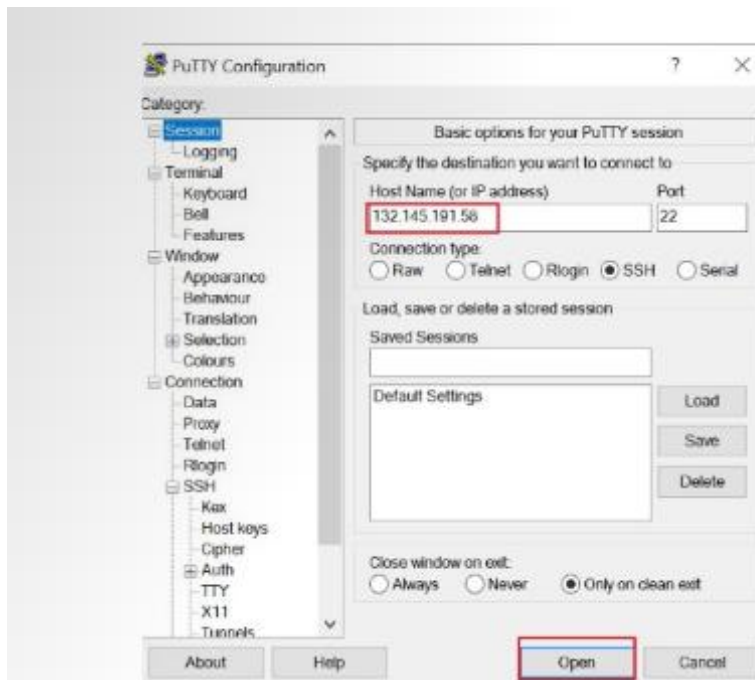
The screenshot displays the Oracle Cloud console interface for an instance named "SOACI02-soa-0". The instance is in the "RUNNING" state, indicated by a green square icon. The "General Information" tab is selected, showing details such as Availability Domain (AD-1), Fault Domain (FD-2), Region (us), OCID, Launch Time, Compartment, Capacity Type, and Instance Details (Virtual Cloud Network, Maintenance Reboot, Image). The "Instance Access" section provides instructions on connecting via SSH and lists the Public IP Address (132.145.191.88), Username (opc), Primary VNIC, Private IP Address (10.0.3.107), Network Security Group, Subnet, Private DNS record, Hostname, and Internal FQDN.

4. Note the public IP address of the Administration Server VM.

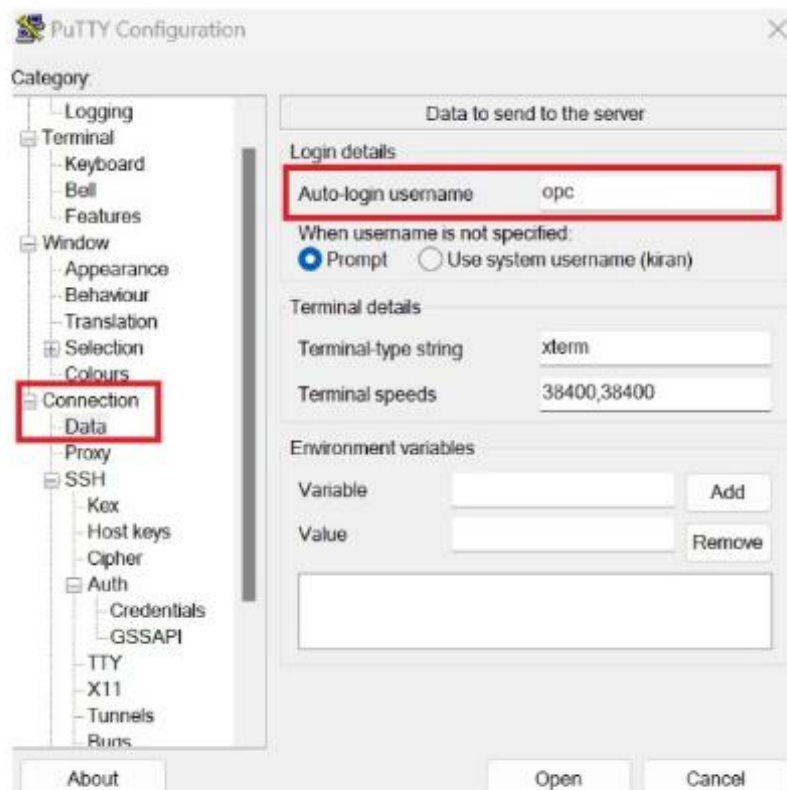


This screenshot is identical to the previous one, showing the Oracle Cloud console for instance "SOACI02-soa-0". In this view, the "Public IP Address" (132.145.191.88) in the "Instance Access" section is highlighted with a red box to draw attention to it.

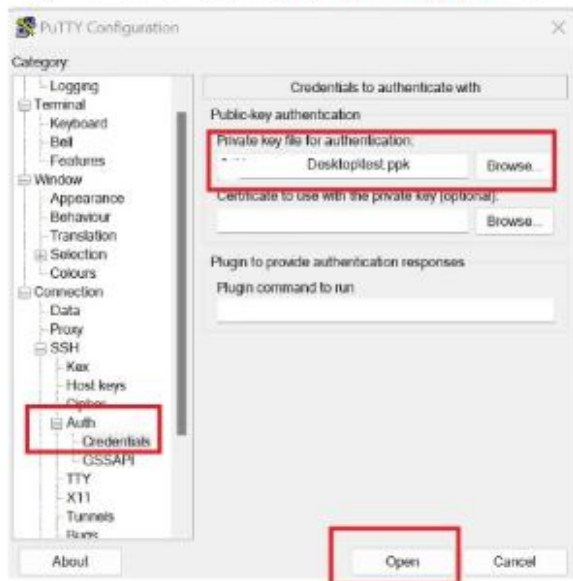
5. Open **Putty** application from your local Windows system and perform the following steps to establish a command-line connection to your VM:
- Enter public IP address in the **Host Name** field.



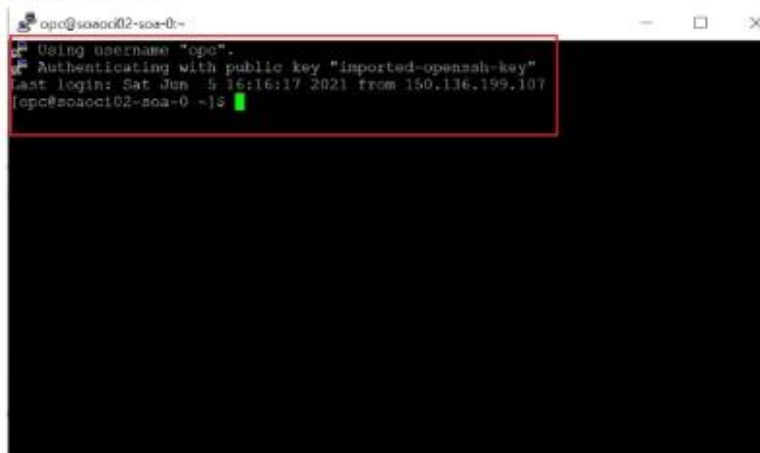
- b. From the left-side menu, navigate to **Connection** → **Data**. Enter **opc** in the Auto-login username field.



- c. From the left-side menu, navigate to **Connections→SSH→Auth→ Credentials**. Under **Private Key file for authentication**, click **browse** to select and upload your private key. In this example, it is **my-OCI-key.ppk** file.



- d. Click **Open** to open the connection to the VM.
6. You will be prompted to Administration Server or Managed Server VM (based on the Host IP provided). When the VM command line appears, you can use any resource accessible from the VM.



You must SSH to a VM only as the `opc` user. This user has root privileges on the OS running in the VM. For example, `opc` can be used to create other OS users on a VM. Prefix root operations with the `sudo` command.

7. Enter the following command to add **users** on a VM.

```
[opc@soaoci02-soa-0 ~] sudo useradd soauser
```

```
opc@soaoci02-soa-0:~  
Using username "opc".  
Authenticating with public key "imported-openssh-key"  
Last login: Sat Jun 5 16:16:17 2021 from 150.136.199.107  
[opc@soaoci02-soa-0 ~]$ sudo useradd soauser
```

8. The **oracle** user has regular OS user permissions. Use the below command to change to the **oracle** user.

```
[opc@soaoci02-soa-0 ~] sudo su - oracle
```

```
oracle@soaoci02-soa-0:~  
Using username "opc".  
Authenticating with public key "imported-openssh-key"  
Last login: Sat Jun 5 16:16:17 2021 from 150.136.199.107  
[opc@soaoci02-soa-0 ~]$ sudo useradd soauser  
[opc@soaoci02-soa-0 ~]$ sudo su - oracle  
Last login: Thu Jun 17 13:04:12 GMT 2021  
oracle@soaoci02-soa-0 ~]$
```

9. An alternative to using the **sudo** command to perform root OS operations as the **opc** user is to change to the **root** user. To change to the **root** user, enter the following command:

```
[oracle@soaoci02-soa-0 ~] exit  
[oracle@soaoci02-soa-0 ~] sudo -s
```

```
[oracle@soaoci02-soa-0 ~]$ exit  
logout  
[opc@soaoci02-soa-0 ~]$ sudo -s  
[root@soaoci02-soa-0 opc]#
```


Practice 5-3: Create an SSH Tunnel

Overview

An SSH tunnel to an Oracle SOA Suite on Marketplace VM enables you to connect to other non-public ports on the VM through a port on your local machine.

If a resource provided by a VM uses a port that is not directly accessible through the Internet, you can access that resource by creating an SSH tunnel to the port.

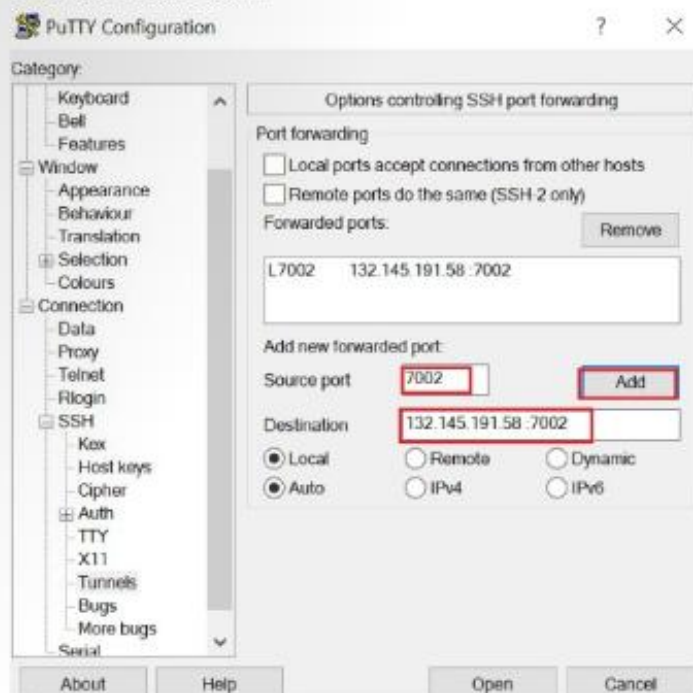
In this practice, you will create an SSH tunnel to an Administration Server VM and access the VM using localhost and port.

Tasks

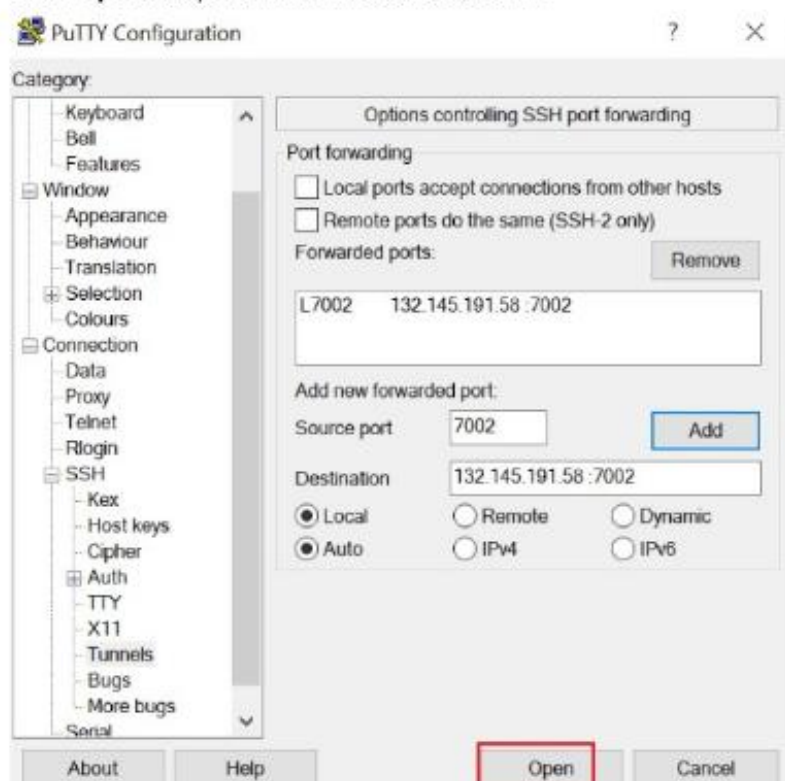
To set up an SSH tunnel to an Administration Server VM:

1. Open **Putty** application from your local Windows system and perform the following steps to establish a command-line connection to your VM:
 - a. Enter public IP address in the **Host Name** field.
 - b. From the left-side menu, navigate to **Connection** → **Data**. Enter **opc** in the Auto-login username field.
 - c. From the left-side menu, navigate to **Connections** → **SSH** → **Auth** → **Credentials**. Under **Private Key file for authentication**, click **browse** to select and upload your private key. In this example, it is **my-OCI-key.ppk** file.
 - d. In the Category tree, click **Connection > SSH > Tunnels**.
 - e. In the Destination field, enter IP: port:
 - 1) Where IP is the public IP address of the VM and port is the port number on the VM to which you want to connect (**Example: 132.145.191.58 :7002**).
 - f. In the Source Port field, enter the same port number.

- g. Click the **Add** button.



- h. Click **Open** to open the connection to the VM.



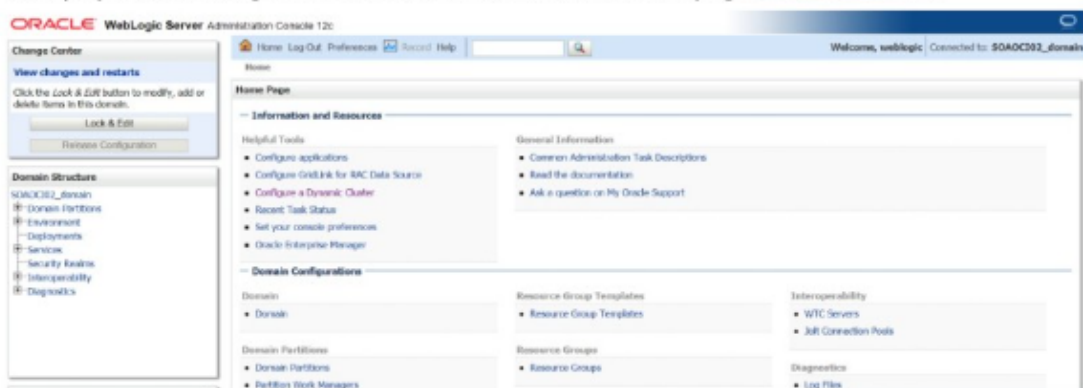
- i. It will connect to **Administration Server VM** as shown below.



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 9001 on the Administration Server VM, launch a web browser and connect to <http://localhost:9001/console>.

2. Now access the WebLogic Administration Console using the URL <https://localhost:7002/console> (this is an example URL in our case and it may be different for you) and provide the username as "weblogic" and password as "Wwelcome#123" and then click "Login".
3. It displays the WebLogic Server Administration console home page as shown below.



This completes the task of setting up an SSH tunnel to an Administration Server VM and accessing the WebLogic administration console using localhost.

