

Lab Guide

A Practical Guide to

Oracle Cloud for Infrastructure

Version 1.1

© 2020 TechTipsOnDemand.com

Table of Contents

DISCLAIMER.....	3
Cost Saving Best Practices	3
Lab Guide Overview	3
Lab #1: Signing up for OCI	5
Lab #2: Core OCI Compute	9
Lab #3: Core OCI Networking	26
Lab #4: Core OCI Block Storage	53
Lab #5: Core OCI Object Storage	77
Lab #7: Core OCI Load Balancer	102
Lab #8: Core Identity and Access Management	117
References	152
Appendix A : How to Access Private OCI Compute Instances using a Jump Server	152

DISCLAIMER

The student performing the steps in this lab guide is solely responsible for any charges incurred. The Author of this course and TechTipsOnDemand are not liable for any charges you may incur while performing any of the labs or exercises associated with this course and lab guide.

While the Author makes every attempt to leverage OCI services that are part of the Oracle Free Tier Trial Period, the availability of such services as part of a free trial period are subject to change by Oracle and may convert to a paid service.

Any service that is part of the Free Trial period becomes a paid service after the trial period expires, and as such is the financial responsibility of the student and the organization which owns the OCI Tenancy where the costs are incurred.

Cost Saving Best Practices

The following tips are recommended for minimizing any costs you may incur during the course of this lab:

1. Stop compute instances when you are not using them. Running compute instances cost money. Stopped instances do not cost money.
2. Delete block and boot volumes when you are done with them. Persistent storage such as block storage costs money.
3. Delete object storage objects when you are done with them. Persistent objects cost money.

Lab Guide Overview

This lab guide will teach you how to create, manage, and secure infrastructure in OCI, using a variety of methods and tools. Each lab builds upon the previous, so it is highly recommended you perform all the labs in sequence.

The References section of this document contains links to the software needed for this lab, as well as links to online documentation for reference.

System Requirements

There are very few system requirements for this course. Since everything we are doing is in the cloud, we simply need a computer with one of the common operating systems and an internet connection.

- Operating System: Windows, Linux or OSX
- Internet connection
- Ability to sign up for an OCI account using a credit card or an existing account with sufficient privileges to execute the labs.

Organization

Each lab is organized into the following structure:

- **Skills Learned** describes what you will get out of the lab
- **Overview** describes the overall details of the lab
- **Configuration Parameters** defines parameters and values you will need to perform the lab
- **Instructions** provide the details steps needed to perform the lab

Links to required software can be found in the References section of this lab guide.

Need Help?

If you need help with the labs or have questions please write us at support@techtipsondemand.com

Lab #1: Signing up for OCI

Duration 30 minutes

Skills Learned

At the end of this exercise, you will be able to:

- Sign up for a free-tier OCI account
- Log into your OCI account

Overview

In this first lab you will sign up for the free-tier version of OCI. This lab will get you familiar with navigating the OCI console, viewing account details, changing your password, and view billing information including creating a budget.

Instructions

1	Sign up for a Free-Tier OCI account
1.1	Visit http://www.oracle.com/cloud/free and click the sign-up button to create a new Oracle Cloud account.
1.2	Fill out the signup form and go through the email verification process.
1.3	As part of the signup, you will be asked to specify a Default Geographic Region for your account. The region you pick will serve as your home region. I suggest you pick a region that is geographically close to where you or your company resides. You can always subscribe to other regions.
1.4	You will be asked to specify a Tenancy name. The tenancy name must be globally unique within Oracle. Organizations can have multiple tenancies and tend to name their tenancies after their department names or computing environments (dev, test, production). The tenancy name will be used when logging into the OCI console.
1.5	For individual users of OCI, select the Pay-as-you-Go model (PAYGO).
1.6	After you complete the registration process, you will receive a welcome email from Oracle containing information on how to log into your account.

1.7	Use the link in the welcome email to access the OCI Console. Log in using your email address and the credentials you specified when signing up for OCI.
2	Preparing your Tenancy for this Lab Guide
2.1	<p>Whether you are working in a brand new tenancy that is entirely yours alone or you are sharing one with your organization or group, we are going to carve out an area within the tenancy where we are going to perform all the lab exercises.</p> <p>As you will learn in lectures on OCI IAM and Compartments, OCI has a feature concept called Compartments. A compartment is a way to organize and group OCI resources in a tenancy. A compartment structure can be flat or it can be hierarchical. Compartments are also used with OCI's authorization policies so that types of resources can be managed by one group in a compartment while permitting users of another group to use those resources.</p> <p>It is fairly common to see large organizations set up a compartment structure that aligns with their corporate structure or IT and development departments.</p> <p>For this lab guide, you will do all your work under one top level compartment that we will call <code>OCI_Labs</code>.</p>
2.2	<p>To create a compartment, log into the OCI Console and navigate to Identity > Compartments from the stacked navigation menu in the upper left-hand corner of the Console.</p> <p>You will see at least two compartments already, possibly more. By default, every tenancy comes with at least a root compartment. All other compartments will hang off the root compartment.</p>
2.3	Create a new compartment by clicking on the Create Compartment button.
2.4	In the dialog that appears, enter the name of the compartment <code>OCI_Labs</code> and a description. Make sure the Parent compartment is the root compartment.

Create Compartment [Help](#)

Name:

Description:

Parent Compartment:

Tagging is a metadata system that allows you to organize and track resources within your tenancy. Tags are composed of keys and values that can be attached to resources.
[Learn more about tagging](#)

TAG NAMESPACE: TAG KEY: VALUE:

[+ Additional Tag](#)

[Create Compartment](#) [Cancel](#)

2.5 Click Create Compartment after filling in the information. Your compartment will be created. You may have to refresh your browser window if the compartment does not immediately appear in the list.

3 Setting a Budget and Monitoring Usage

3.1 The first thing you should do after you create your account is to set up a budget in OCI. By defining a budget, OCI will notify you when you approach, reach, and exceed the budget.

In this section you will define a monthly budget and then specify when to get alerted based on forecasted or actual usage.

3.2 Log into the OCI Console and click on the three stacked bars in the upper left to pop out the main navigation menu.

3.3 Navigate to Account Management > Budgets

3.4 Click Create Budget and provide the following details:

	<p>Budget Scope: <i>Compartment</i> Name: <i>Provide any name for your budget</i> Description: <i>Leave blank</i> Target Compartment: <i>OCI_Labs</i> Monthly Budget Amount: Enter a value that you are comfortable with. Remember, this is the figure OCI will use to alert you.</p> <p>Under Budget Rules, specify whether you want to be notified based on actual spend or forecasted spend. For this course, I would suggest actual spend.</p> <p>Under Threshold Type, select whether you want to be notified if you come within a certain percentage of your budget or an actual dollar amount. For example, if your budget was \$100 and you specify a threshold of 80%, you will get notified when you use \$80 worth of OCI services. Likewise, if you specify an absolute amount, you will get notified when you consume that absolute amount.</p> <p>Under Email Addresses, be sure to include your email address and an email message to remind you why you are getting an email from Oracle.</p> <p>Once done, click Create.</p>
3.5	<p>You can use OCI's Cost Analysis tool to determine what services are costing you money. This is useful if your free trial expires and your account converts to a normal paid account.</p> <p>Access the Cost Analysis tool by going to Account Management > Cost Analysis.</p>
3.6	<p>You will be presented with a fairly typical reporting page. You can specify a date range and what type of report you want to run. If you have created a new account, then this page will not be very excited since we have not used any services yet.</p>

Conclusion

In this lab you should have signed up for an OCI Account and with that received a free trial period. We also set up a budget so that we can be alerted if we are using services that cost money and exceed our budget. Lastly, you got to see the Cost Analysis Tool which can be used to generate real-time cost usage reports.

Lab #2: Core OCI Compute

Duration 1 hour

Skills Learned

At the end of this exercise, you will be able to:

- Create a compute instance
- Generate SSH keypairs for logging into OCI compute instances
- Create a second VNIC
- Use PuTTY to log into a compute instance
- Stop, Start, and Terminate compute instance
- Monitor health

Overview

We are going to dive right into creating our first compute instance in OCI just to get our feet wet very quickly. In this lab we are going to keep things simple by starting with how to create a compute instance and how to log into it, and of course how to stop and terminate the instance.

We start here because 1) Creating compute instances is why we are here so let's just cut to the chase and 2) we need to know how to deploy compute instances in order to demonstrate how all the other OCI IaaS features work.

Estimated Costs

You may incur costs associated with running compute instances that are not part of the Always Free Eligible tier. Oracle charges for how long a compute instance is running and the OCPU/hour rate is based upon the compute shape being used, so it is recommended that you use the smallest shape possible and stop all instances when you are done working with them to reduce your costs.

Oracle provides an online cost estimator which you can use to estimate your costs based on expected usage.

<https://www.oracle.com/cloud/cost-estimator.html>

A word of caution! A running compute instance costs money and requires that you have a paid account or are in the free trial period to provision. While there is an Always Free Tier available, it limits you to two compute instances. To save on costs, always STOP your compute instances when you are done using them. A stopped instance does not incur any costs associated with compute, however any persistent storage will indeed incur some costs.

Instructions

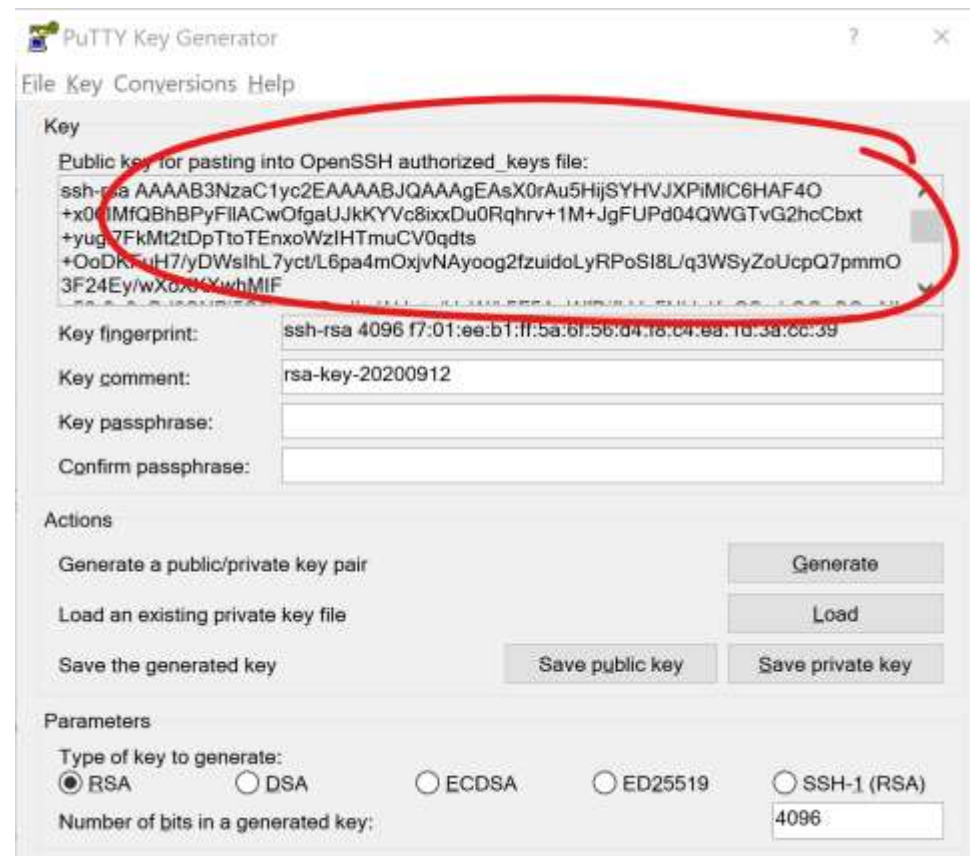
1	Generating SSH Keys
1.1	<p>Linux compute instances in OCI use SSH keys for authentication. In this lab you will create an SSH keypair first, then create a new compute instance with the public half of the keypair which will allow you to log in using ssh and the private half of the keypair.</p> <p>Instructions for generating ssh keys on Linux and Windows machines will be provided below.</p>
1.2	<p>Generating SSH Keys on Linux machines</p> <p>In a Linux terminal window run the following command to generate an RSA-based key with a size of 4096 bits.</p> <p>Leave the password blank when prompted.</p> <pre>\$ ssh-keygen -t rsa -b 4096 -f oci_lab.id_rsa</pre> <p>The command will generate the private key oci_lab.id_rsa and the public key oci_lab.id_rsa.pub.</p> <p>You can find more information on generating and managing SSH keys here:</p> <p>https://www.ssh.com/ssh/keygen/</p>
1.3	<p>Generating SSH Keys on Windows machines using PuTTY</p> <p>If you are on Windows, one of the more common SSH clients is PuTTY, a free SSH client and toolset that supports SSH key creation and management.</p> <p>You can download PuTTY at https://www.putty.org/.</p> <p>Step 1. Download and install PuTTY from www.putty.org</p>

Step 2. Start the PuTTYgen application from the Start menu.

Step 3. Generate a private key by first selecting RSA as the key type and the number of bits as 4096.

Then click the Generate button and move your mouse cursor around the PuTTYgen window. This is used to generate some randomness that's used in creating the private key.

Step 4. Once the generating is complete, select all the text in the 'Public key for pasting ...' window shown below. Save the text in a text file (using notepad or something similar) using the filename **oci_lab.id_rsa.pub**.



Step 5. Save the private key by clicking the Save private key button. Do not set a passphrase. Save the file using the name **oci_lab.ppk**.

	Be sure to save the ppk (private putty key) in a safe location.
1.4	<p>Generating SSH Keys in Windows using Powershell</p> <p>Power users can also use powershell and openSSH tools instead of using PuTTY.</p> <p>Open a Powershell window (Press Win + R and type powershell) and follow the instructions for Generating SSH Keys on Linux.</p>
2	Creating a Virtual Cloud Network
2.1	<p>In order to create a compute instance, we need a place to deploy it. When you deploy a server in a data center, you physically mount it in a rack and then connect it to the network. In the cloud case, you will create a virtual network called a VCN and subnets within that VCN.</p> <p>There is an entire lab that focused on OCI Networking and VCNs in detail, however for this lab you will use a default configuration from OCI that will give us a basic VCN to work with.</p>
2.2	Log into the OCI console and navigate to Networking > Virtual Cloud Networks
2.3	Under List Scope, select the OCI_Labs compartment. Recall from Lab 1 that we created the OCI_Labs compartment. All OCI resources we create will be created in this compartment.
2.4	Select Start VCN Wizard.
2.5	Select VCN with Internet Connectivity, then click Start VCN Wizard.
2.6	<p>Under Basic Information, specify vcn1 for the VCN name.</p> <p>Verify the compartment is set to OCI_Labs.</p> <p>Leave all the other values alone as they are sufficient for this lab.</p>
2.7	<p>Click Next to move to the Summary screen. This screen shows us how the VCN will be created and with what OCI resources.</p> <p>The VCN wizard gives us a rather functional network which includes both a public and private subnet, and various network gateways for accessing the internet and OCI services.</p>
2.8	Click Create.
2.9	Once OCI creates the VCN and all its resources, you may click on the View Virtual Cloud Network button at the bottom of the screen.

3	Creating a Compute Instance
3.1	In this section you will launch a Linux compute instance in one of the public subnets you created earlier and connect to it using ssh.
3.2	Log into the OCI console and navigate to Compute > Instances.
3.3	Under List Scope, select the OCI_Labs compartment if not already selected.
3.4	Click the Create Instance button.
3.5	<p>The Create Compute instance screen provides a wide variety of parameters for configuring a compute instance.</p> <p>Specify the following configuration parameters.</p> <p>Name: Leave the system generated name Create in compartment: OCI_Labs</p>
3.6	<p>Select Change Image and browse all the available images. Images that are tagged Always Free Eligible incur no additional cost to use.</p> <p>Platform images are maintained by Oracle and are your typical general purpose OS images. Oracle Images are also maintained by Oracle but are purpose built for specific workloads or configurations. Partner Images are developed and maintained by trusted Oracle third parties.</p> <p>Under Image, use the image – Oracle Linux 7.9</p>

Browse All Images

<input type="checkbox"/>	CentOS 6.10
<input type="checkbox"/>	CentOS 7
<input type="checkbox"/>	CentOS 7.9
<input type="checkbox"/>	CentOS 8
<input type="checkbox"/>	CentOS 8.3
<input type="checkbox"/>	Oracle Autonomous Linux 7.9
<input type="checkbox"/>	Oracle Linux 6.10
<input type="checkbox"/>	Oracle Linux 7.8
<input checked="" type="checkbox"/>	Oracle Linux 7.9
<input type="checkbox"/>	Oracle Linux 8
<input type="checkbox"/>	Windows Server 2012 R2 Datacenter
<input type="checkbox"/>	Windows Server 2012 R2 Standard
<input type="checkbox"/>	Windows Server 2016 Datacenter
<input type="checkbox"/>	Windows Server 2016 Standard
<input type="checkbox"/>	Windows Server 2019 Datacenter

3.7 **Select** Show Shape, Network, and Storage options to reveal additional parameters.

3.8 If your region has more than one availability domain, you have the option of specifying which AD to launch the compute instance in. It is a best practice to spread your compute instances across availability domains within a region to provide

some level of fault tolerance and high availability in the event one AD goes offline.

In the Networking lab, we created regional subnets which span all ADs within a region, whereas a regular subnet only exists in one AD. Regional subnets eliminate the need to set up additional subnets in each region, create route rules and configure security lists to permit compute instances to talk to one another.

For this lab we will leave it in AD 1.

3.9

Select Change Shape to select the type and size of compute instance we want to create. The selection of shapes will be restricted depending on whether you have a paid account or a free tier account.

For this lab we are going to use one of the Always Free Eligible shapes.

**** Keep in mind that you are limited to the number of Always Free Eligible compute instances you can create in a tenancy. If there are no free compute instances available, then you would need to register a form of payment with your OCI account in order to provision additional compute instances. ****

Select Virtual Machine for Instance Type.

Select one of the Always Free Eligible shapes under Specialty and Legacy shapes.

Then click the Select Shape button to return to the compute instance screen.

Browse All Shapes

To access all shapes, [upgrade](#). You'll pay only for what you use, no minimum terms and no prepayments.


[Upgrade](#)


Instance type

Virtual Machine Always Free Eligible
 A virtual machine is an independent computing environment that runs on top of physical bare metal hardware. ✓

Bare Metal Machine
 A bare metal compute instance gives you dedicated physical server access for highest performance and strong isolation.

Shape series

AMD Rome
 Customizable OCPU count. For general purpose workloads.

Intel Skylake
 Fixed OCPU count. Latest generation Intel Standard shapes.

Specialty and Legacy
 Earlier generation AMD and Intel Standard shapes. Always Free, Dense I/O, GPU, and HPC shapes. ✓

Shape Name	OCPU	Memory (GB)	Local Disk	Network Bandwidth (Gbps)	Max. Total V
<input checked="" type="checkbox"/> VM.Standard.E2.1.Micro <small>Always Free Eligible</small>	1	1	Block Storage Only	0.48	1

1 Selected Showing 1 Item

3.10 Next we want to configure the networking for this compute instance by specifying which network and subnet to launch the compute instance in, and whether we want to assign a public IP address.

For this lab, we want to launch the compute instance in the bastion subnet we created earlier and assign a public IP address so we can ssh into it.

Specify the following details:

	<p>Virtual Cloud Network Compartment: <i>OCI_Labs</i> Select a Virtual Cloud Network: <i>vcn1</i> Subnet Compartment: <i>root</i> Subnet: <i>Public Subnet-vcn1(regional)</i></p> <p>Select <i>Assign a Public IP Address</i></p>
3.11	<p>Under Add SSH Keys, you can upload a private SSH key or you can have Oracle generate one for you, or not specify one at all.</p> <p>For this lab we are going to use the SSH keys we generated earlier by specifying the public key. Oracle will take the public key and bootstrap the compute instance with it. You hold on to the private key.</p> <p>Select Choose Public Key Files to load the oci_lab.id_rsa.pub (public key) that was created in the first part of the lab.</p>
3.12	<p>Click Create to launch the instance.</p> <p>It will take a little bit of time to provision the instance. After you launch the instance, you will be taken to the instance details page which has important information about the compute instance. The work request status will change from Provisioning to Running (if all goes well).</p>
3.13	<p>Once the instance is running, you will see various details that are specific to the instance, such as networking details.</p> <p>Note the public IP and private IP addresses that have been assigned to the instance. The public IP address is generated by Oracle from their pool of public IPs. You will connect to this compute instance using its public IP.</p> <p>The private IP address is assigned out of the subnet that the instance resides in.</p>

The screenshot displays the Oracle Cloud console interface for a compute instance. The 'Instance Information' tab is active, showing various details. Red circles are drawn around specific fields: 'Availability Domain: AD-1', 'Fault Domain: FD-2', 'Region: phx' under the 'General Information' section; and 'Public IP Address: 129.146.44.55' and 'Username: ubuntu' under the 'Instance Access' section. Other visible details include OCID, launch time, compartment, agent management status, virtual cloud network, maintenance reboot status, image, launch mode, maintenance recovery action, shape configuration, primary VNIC details, and launch options.

3.14 Copy the public IP address of the instance.

4 Connect to the Compute Instance

4.1 This section provides instructions for connecting to the compute instance using SSH from Linux and Windows desktops.

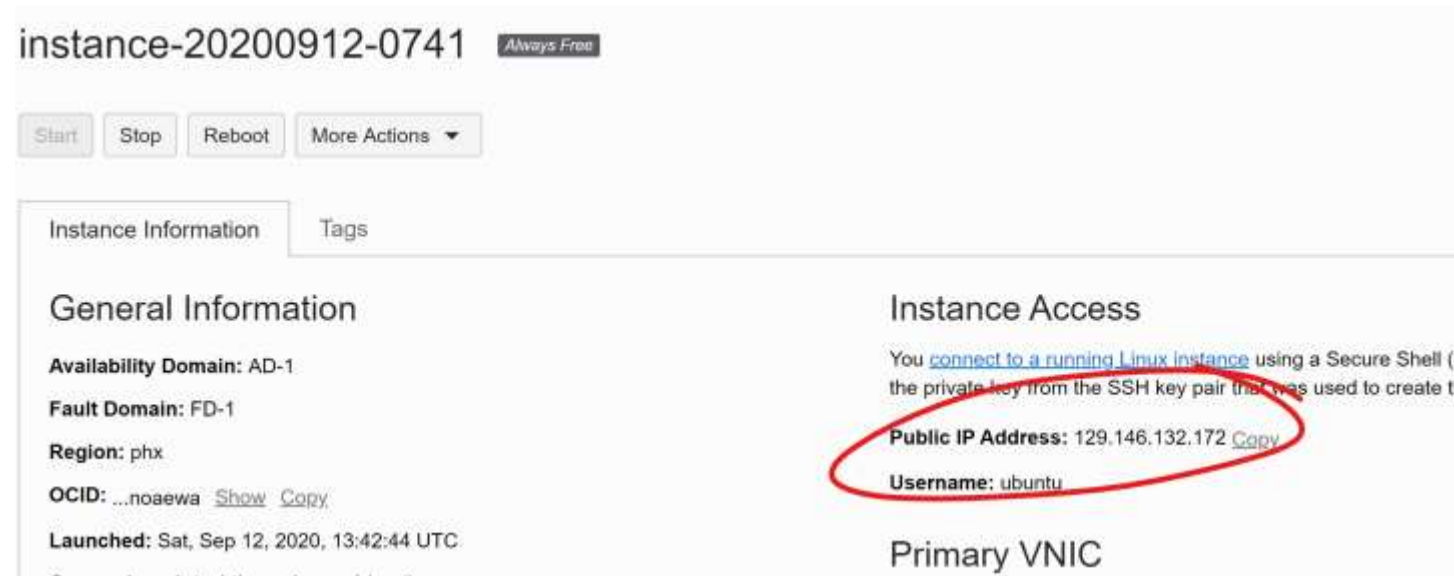
4.2 Connecting to a Compute Instance from Linux

Open a terminal window in linux and run the following command to connect to the compute instance:

```
$> ssh -i /path/to/oci_lab.id_rsa ubuntu@public_IP_of_compute_instance
```

Be sure to specify the location of the private key you created earlier and the public IP address of the compute instance

you created. You can find the public IP address in the OCI console on the details page for the compute instance.



Let's break this command down.

`-i` specifies what private key (identity file) to use. In this case you must specify the location of the private key you created earlier.

`opc@public_IP_of_compute_instance` specifies what user and what host to connect to. For example,

```
$> ssh -i ~/.ssh/oci_lab.id_rsa opc@129.146.132.172
```

This command will connect to the public IP address of a compute instance (129.146.132.172) as username `opc` (default OCI username for Oracle Linux images) using the identity file `oci_lab.id_rsa`.

4.3

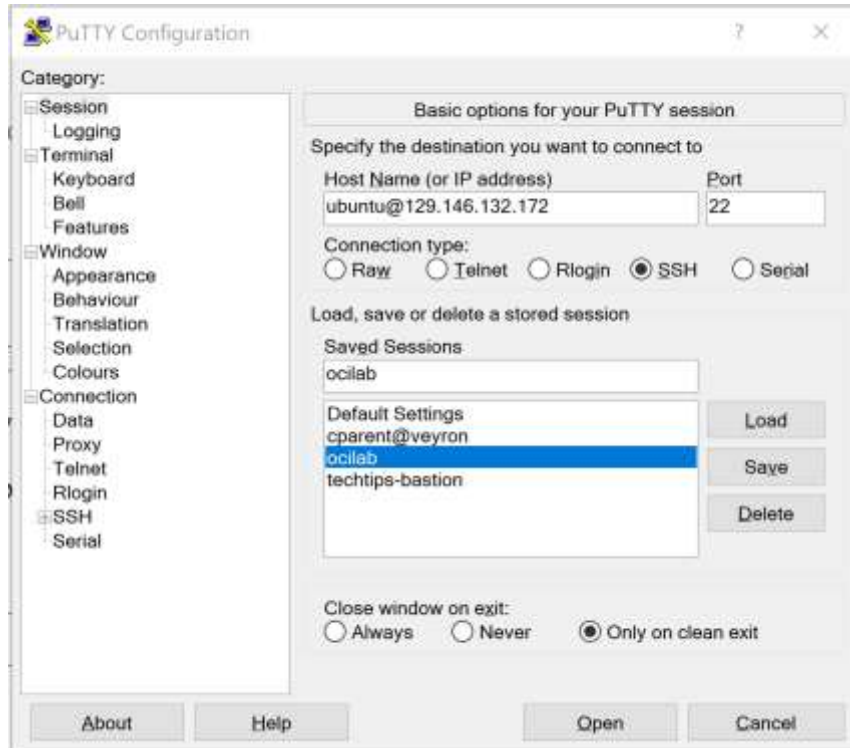
Connecting to a Compute Instance from Windows using PuTTY

Launch PuTTY from the Windows Start Menu.

Enter `opc@public_IP_of_compute_instance` in the Hostname (or IP address) field.

Under SSH > Auth, specify the private key you created earlier by clicking the Browse button.

Go back to Session, enter a name for this session (ocilab) and click Save.




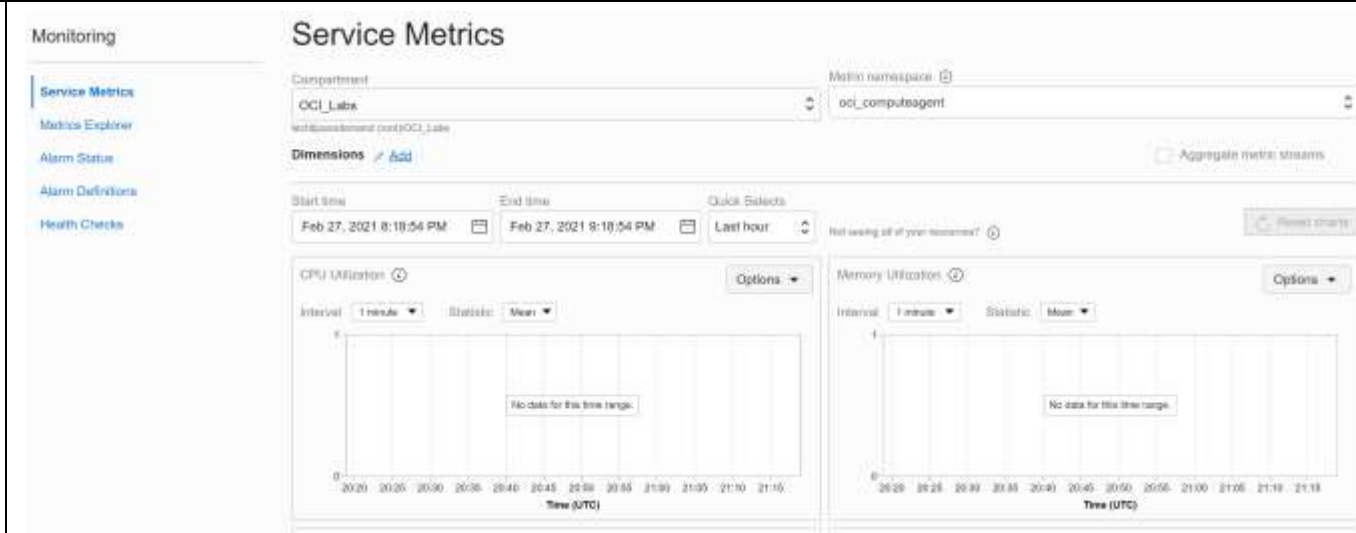
Click Open to open a connection to the compute instance. If you have any issues connecting to the new instance, be sure to double-check:

1. You have specified the correct private key that goes with the public key on the compute instance
2. You are connecting as user *opc*.
3. You are connecting to the correct public IP address for the compute instance. You can find the public IP address in the OCI console under Compute > Instances.

4.4 Once you are connected to your compute instance, feel free to poke around the server.

Using the wizard to create a VCN automatically generated some basic network security rules that only allow us to SSH into the network from the internet. We will learn more about securing VCNs in the OCI Networking lab.

5	Monitoring Health
5.1	<p>Each OCI compute instance emits health and performance metrics to the OCI Monitoring service under the namespace <code>oci_computeagent</code>.</p> <p>The <code>oci_computeagent</code> namespace contains a variety of information specific to a compute instance, including CPU and memory utilization, disk I/O, and network I/O.</p>
5.2	<p>You can quickly view the health of a particular compute instance by navigating to the compute instance (Compute > Instances > bastion1 for example) and selecting Metrics as show in the screenshot below.</p> <p>OCI provides an interactive report that allows you to look at metrics over a period of time. I</p> 
5.3	<p>You can also access compute metrics from OCI Monitoring directly.</p> <p>Navigate to Monitoring > Service Metrics from the main navigation menu. Under Metric Namespace, select <code>oci_computeagent</code> Select the OCI_Labs compartment.</p> <p>This screen will display metrics for all compute instances in the OCI Labs compartment.</p>



6 Create a Secondary vNIC

6.1 Creating additional nVNICS is akin to adding additional network cards to a server chassis. OCI supports creating additional vNICs to support a variety of networking use cases, such as building your own NAT router for example.

The specific shape of a compute instance determines the number of vNICs that can be created. In this lab we will create a new compute instance that supports additional vNICs. The compute instance will be created in a public subnet but the secondary vNIC will be deployed in a private subnet. In essence this compute instance will have a 'leg' in each subnet.

6.2 Create a new compute instance using the method above, by placing it the public subnet for vcn1.

Use a compute shape that supports more than 1 vNIC. For example, under Specialty and Previous Generation shapes, select the VM.Standard.E2.1 shape, which supports max of 2 vNICs.

Configure the instance to use the same SSH key you created earlier.

6.3 Once the instance has booted and is running, select Attached VNICS from the compute instance's resources menu.

6.4 Click the Create vNIC button and specify the following details:

Name: secondvnic

	<p>Network: Normal setup Subnet: <i>Use the private subnet in the vcn1 VCN. Be sure to select the OCI_Labs compartment.</i></p> <p>Accept all other default values and save changes.</p>
6.5	<p>Once the secondary vnic is created, you must run a special Oracle script for the VNIC and local route table to be configured on the compute instance.</p> <p>SSH into the compute instance using your SSH key.</p>
6.6	<p>Run the following commands to download and execute the script as root.</p> <pre>\$ sudo su \$ wget https://docs.oracle.com/en-us/iaas/Content/Resources/Assets/secondary_vnic_all_configure.sh \$ chmod u+x secondary_vnic_all_configure.sh \$./secondary_vnic_all_configure.sh -c</pre>
6.7	<p>Run the following ifconfig command to confirm that a second interface has been created. Take note of the IP address assign to the second VNIC – in this example it is ens5. This IP address comes out of the CIDR block for the private subnet in VCN1.</p> <p>The primary VNIC, ens3, is assigned an IP address from the CIDR block for the public subnet.</p> <pre>\$ ifconfig -a ens3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 9000 inet 10.0.0.12 netmask 255.255.255.0 broadcast 10.0.0.255 ether 00:00:17:02:03:be txqueuelen 1000 (Ethernet) RX packets 88007 bytes 143391102 (136.7 MiB) RX errors 0 dropped 0 overruns 0 frame 0 TX packets 78519 bytes 71557388 (68.2 MiB) TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0 ens5: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 9000 inet 10.0.1.2 netmask 255.255.255.0 broadcast 0.0.0.0 ether 02:00:17:05:d2:12 txqueuelen 1000 (Ethernet) RX packets 0 bytes 0 (0.0 B) RX errors 0 dropped 0 overruns 0 frame 0 TX packets 0 bytes 0 (0.0 B)</pre>

```
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    loop txqueuelen 1000 (Local Loopback)
    RX packets 11144 bytes 620808 (606.2 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 11144 bytes 620808 (606.2 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

7 Managing Compute Instance Lifecycle

7.1

Compute instances go through several phases:

Stopped: Instance is powered off. No compute cost is incurred for a stopped instance.

Running: Instance is up and running. Compute costs are being incurred on an hourly basis.

Terminated: Instance has been deleted. No compute cost is incurred for a terminated instance.

Instances that are running incur cost since compute is charged on an hourly basis. Instances that are not running, either stopped or terminated, do not incur compute costs.

7.2

When you create a compute instance using the OCI console, OCI will automatically launch the instance into a running state.

You can use the console to stop, reboot, terminate or start an instance.

7.3

Let's stop our running compute instance by navigating to Compute > Instances.

You will see a list of compute instances. Select the 3 dots (ellipsis) next to the instance we created earlier as shown in the screenshot below.

Select Stop to shutdown the instance. You will be presented with a warning about shutting down the instance. Go ahead and confirm the shutdown.

Instances in techtipsondemand (root) Compartment

The [Compute service](#) helps you provision VMs and bare metal instances to meet your compute and application requirements. An [instance](#) is a compute host. Choose between virtual machines (VMs) and bare metal instances. The image that you use to launch an instance determines its operating system and other software.

[Create Instance](#)

Name	State	Public IP	Shape	OCPU Count	Memory (GB)	Availability Domain	Fault Domain	Created
instance-20200912-0741	Always Free Running	129.146.132.172	VM.Standard.E2.1.Micro	1	1	AD-1	FD-1	Sat, Sep 12, 2020, 13:42:44 UTC

Showing 1 item < 1 of 1 >

- 7.4 The compute instance's state will change from Running to Stopping. Eventually the state will transition to Stopped.
- 7.5 To restart the instance, click on the ellipsis again and select Start. The state will change from Stopped to Starting, then Running.
- 7.6 You can terminate an instance while it is either stopped or running. A terminated instance is effectively deleted.
- Select Terminate from the ellipsis menu. You will be asked whether to preserve the boot volume. Go ahead and check the box to delete the boot volume.
- Boot volumes normally cost money since they are persistent storage, so be sure to delete your boot volumes when terminating compute instances. We will cover boot volumes in a later lab.

Conclusion

This lab showed you how to quickly provision a compute instance in a virtual cloud network and access it using SSH.

Lab #3: Core OCI Networking

Duration 60 minutes

Skills Learned

At the end of this exercise, you will be able to:

- Create a Virtual Cloud Network
- Create public and private subnets
- Route network traffic using OCI Internet, NAT, and Service Gateways
- Control network access using network security rules
- Understand the difference between a network security group and a network security list

Overview

In this lab you will begin creating a virtual cloud network from scratch using a variety of OCI networking features. A VCN or virtual cloud network is the foundation for building any network in OCI. Think of a VCN as your own virtual data center that is defined by a range of IP addresses known as a CIDR block.

Subnets can be created to segment a VCN into smaller networks. Subnets are typically used to provide network isolation for different workloads, such as application servers and databases. In a traditional environment, application servers would be deployed into a subnet separate from the database. Firewall rules would then be implemented to permit network traffic to flow from the application server subnet to the database subnet. In OCI we implement this sort of network security using network security lists. A security list is attached to a subnet and defines what traffic is allowed in and out. You can specify what port, protocol, and even where the traffic is coming from or headed to. While security lists are used to control network access, routing of network traffic in and out of a VCN is handled using a variety of routing gateways and the route table. A routing gateway is a networking gateway similar to your router at home, directing traffic from your home network to the internet and vice versa. In OCI there are gateways that route traffic to and from the Internet such as the Internet and NAT gateways.

A Service Gateway is a special gateway that allows you to call OCI services privately. In plain speak this means when you call an OCI service such as autonomous database or functions, OCI keeps the traffic inside the Oracle Service Network which remains private. The traffic never flows over the internet.

A route table in a VCN contains route rules that determine how network traffic in a VCN is directed. No explicit route rules are needed to route traffic within a VCN, such as between subnets. However, if you have a compute instance in a private subnet that needs to talk to the internet, then a route rule must exist to send traffic from that compute instance to an OCI NAT Gateway.

A more modern method of providing network isolation rather than using subnets is a network security group. An NSG is a logical grouping that associates compute instances with a set of security rules. NSGs are completely decoupled from the actual networking layout. In fact, you could have a completely flat network with no subnetting, and still mimic secure network isolation through the creation and application of various network security groups.

This is what you are going to build.

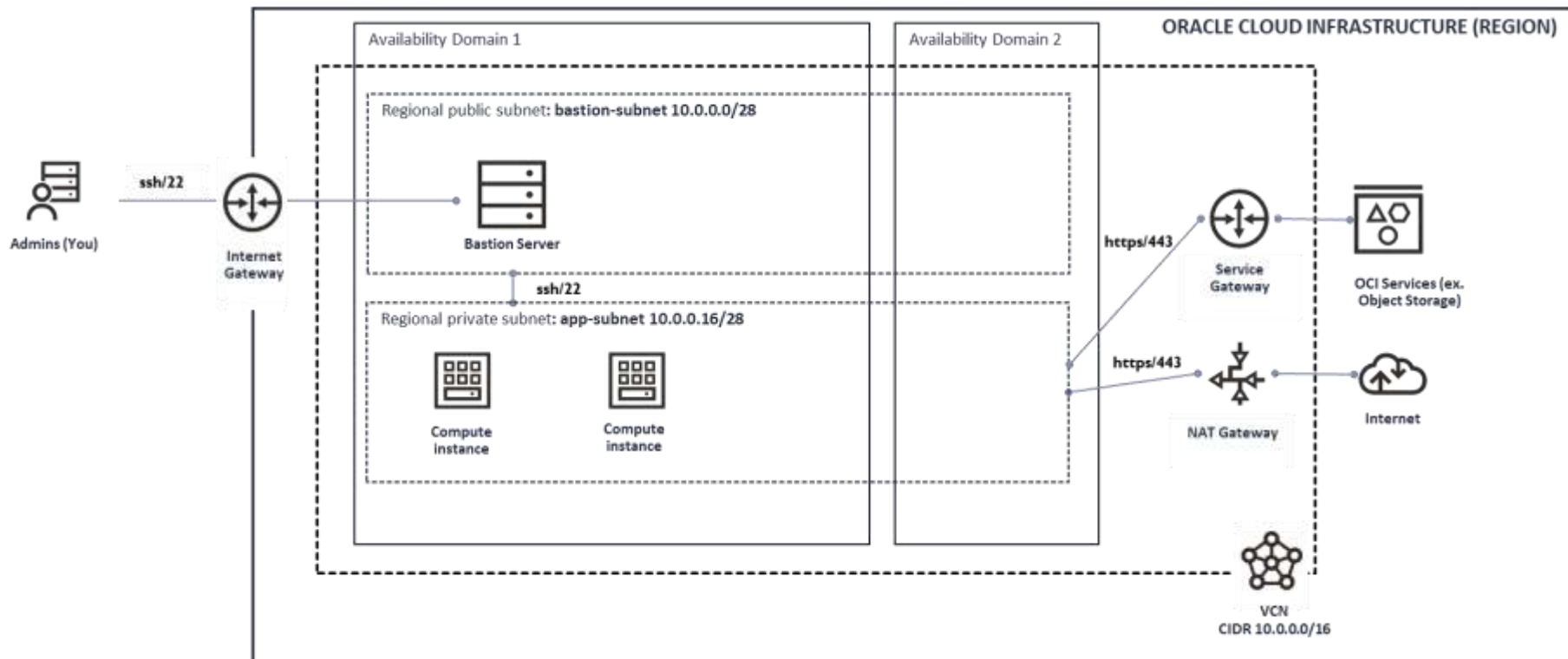
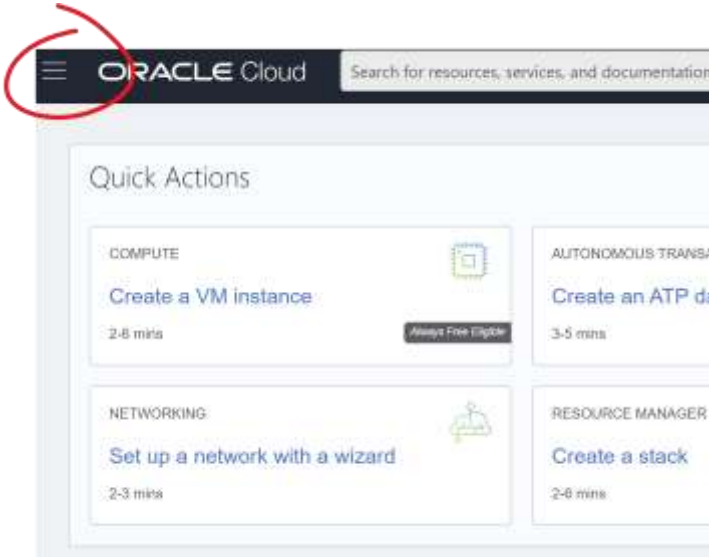


Figure 1 Core Network Lab Diagram

Instructions

1.	Creating a Virtual Cloud Network
1.1.	In this section you will be creating the network shown in the figure above to support an eventual 3-tiered web application deployment. For now we are going to start with creating a VCN and subnets for hosting a public bastion server and private application servers.
1.2.	Log into the OCI console using your web browser using the login URL that was in the welcome email from Oracle or go to cloud.oracle.com and click on sign in.
1.3.	<p>Once logged into the OCI console, navigate to Networking > Virtual Cloud Networks by clicking on the stacked bars in the upper left hand part of the OCI console.</p> 
1.4.	Under List Scope, select OCI_Labs.
1.5.	Create a new VCN by clicking on the Create VCN button.

Virtual Cloud Networks *in techtipsondemand (root) Compartment*

Virtual Cloud Networks are virtual, private networks that you set up in Oracle data centers. It closely resembles a traditional network, with firewall rules and specific types of communication gateways that you can choose to use.

[Create VCN](#)
[Start VCN Wizard](#)

Name	State	CIDR Block	Default Route Table	DNS Domain Name	Created
No items found.					

Showing 0 Items < 1 of 1 >

1.6. Use the information below to create the VCN:

Name: vcn_oci_labs

Create in Compartment: OCI_Labs

CIDR Block: 10.0.0.0/16

Keep the remaining default values.

Your VCN configuration should look similar to the screenshot below.

The screenshot shows the 'Create a Virtual Cloud Network' form. At the top, there's a title 'Create a Virtual Cloud Network' and a 'Help' link. Below the title, there are two input fields: 'NAME' with the value 'vcn_oci_labs' and 'CREATE IN COMPARTMENT' with a dropdown menu showing 'OCI_Labs'. Below the dropdown, the text 'techtipsondemand (root)/OCI_Labs' is visible. The next section is 'CIDR Blocks', which contains a warning message: 'The IP ranges of the CIDR blocks must not overlap. [Learn more.](#)'. Below the warning, there's a 'CIDR BLOCK' input field with the value '10.0.0.0/16'. Below this field, the text 'Specified IP addresses: 10.0.0.0-10.0.255.255 (65,536 IP addresses)' is displayed. To the right of the input field is a close button (X). Below the CIDR block section, there's a 'DNS RESOLUTION' section with a checked checkbox 'USE DNS HOSTNAMES IN THIS VCN'. Below the checkbox, the text 'Required for instance hostname assignment if you plan to use VCN DNS or a third-party DNS. This choice cannot be changed after the VCN is created. [Learn more.](#)' is shown. At the bottom, there are two buttons: 'Create VCN' and 'Cancel'.

1.7. Click the Create VCN button.

You will be taken to a page that shows the details of the VCN that you just created, including any resources that are part of a VCN (Subnets, Route Tables, Internet Gateways, etc). When you create a VCN using the OCI console, OCI automatically creates a few networking resources including:

- A default route table with no route rules.
- A default security list that allows SSH/22 and ICMP ingress, and allows any port/protocol to go out.

The default route table and security list are used as default values when you create a subnet in the OCI console. For

	this lab we will be created our own security lists and route tables.
2.	Creating Public and Private Subnets
2.1.	<p>With our VCN created, let's create some subnets. A subnet is a way to carve up a large network into smaller networks. Subnets are typically used to isolate application functions from one another in a multi-tier architecture. For example, in a three-tier application, you would have one subnet for a public facing load balancer, another for the application servers, and yet another subnet for the database.</p> <p>A public subnet allows OCI resources such as compute to have a public IP address assigned to them, allowing them to be reachable from the internet.</p> <p>A private subnet does not allow resources to have a public IP, therefore these resources are not directly accessible from the internet.</p> <p>In this lab you will create both public and a private subnets to host a bastion server and application servers respectively.</p>
2.2.	<p>In this section you will create a public subnet for hosting a bastion server. The bastion server will have a public IP address, which will allow us to access it from the internet. We will then use the bastion server to access compute instances in our VCN that have private IP addresses.</p> <p>In the VCN details page of the VCN we created earlier, click on Subnets on the left-hand side of the console.</p> <p>Create a public subnet by clicking the Create button and specify the following details for the public subnet.</p> <p>Name: <i>bastion-subnet</i> Subnet type: <i>Regional</i> CIDR block: <i>10.0.0.0/28</i> Route table: <i>Default Route Table for vcn_oci_labs</i> Subnet Access: <i>Public – MAKE SURE THIS IS SELECTED!</i> DNS Resolution: <i>Checked</i> DNS Label: <i>Blank</i> DHCP Options: <i>Default DHCP Options for vcn_oci_labs</i> Security Lists: <i>Default Security List for vcn_oci_labs</i></p> <p>The Public Subnet Access option is what enables public IP addresses to be assigned. Private subnets do not permit public IP addresses to be defined.</p>

Create Subnet

NAME

bastion-subnet



CREATE IN COMPARTMENT

OCI_Labs



techtipsondemand (root)/OCI_Labs

SUBNET TYPE

Regional (Recommended)

Instances in the subnet can be created in any availability domain in the region. Useful for high availability.



Availability Domain-specific

Instances in the subnet can only be created in one availability domain in the region.

CIDR Block

CIDR BLOCK

10.0.0.0/28

Specified IP addresses: 10.0.0.0-10.0.0.15 (16 IP addresses)

ROUTE TABLE COMPARTMENT IN **OCI_LABS** [\(CHANGE COMPARTMENT\)](#)

Default Route Table for vcn_oci_labs



Create Subnet

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

bastionsubnet

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

DNS DOMAIN NAME READ-ONLY

<dns-label>.vcnoci4abs.oraclevcn.com

DHCP OPTIONS COMPARTMENT IN OCI_LABS [\(CHANGE COMPARTMENT\)](#)

Select DHCP options



Security Lists

You can associate up to 5 network security lists with the subnet.

SECURITY LIST COMPARTMENT IN OCI_LABS [\(CHANGE COMPARTMENT\)](#)

Create Subnet

[Cancel](#)

- 2.3. Repeat the previous steps to create a **private** regional subnet named *app-subnet* with a CIDR block of 10.0.0.16/28. To make the subnet private, be sure to select Private Subnet under Subnet Access.

3. Security Lists

- 3.1. Even though we get a default security list when a VCN is created, we are going to create our own security list so you can learn how to do this for yourself.

	<p>Each subnet will have its own security list controlling network traffic in and out. This is because the public subnet needs to be treated differently than the private subnet. The bastion subnet will only allow SSH traffic in so that we can connect to the bastion server using SSH. This will be the only protocol allowed.</p> <p>The app subnet will have a security list that will only allow SSH traffic from the bastion subnet and no where else. For now, it will be the only protocol that we allow in.</p> <p>Both subnets will have a security rule that will allow any network traffic to leave the subnet for the internet.</p> <p>Let's create a security list to allow ssh into the public subnet, and allow ssh out of the public subnet to other subnets in our VCN. The intent here is to create a subnet for a bastion server that we will deploy later on. A bastion server is a compute instance that typically sits in a DMZ and is used to access all other servers that are deployed in private subnets.</p> <p>It is a best practice to minimize the number of resources exposed to the internet as much as possible. You can achieve this by deploying all your compute instances and resources in private subnets, and then allowing access to these servers through limited known access points such as a bastion server or a public load balancer.</p> <p>Navigate to the VCN details page (Networking > Virtual Cloud Networks > vcn_oci_labs) and click on Security Lists.</p>
3.2.	<p>Click Create Security List and specify the following details:</p> <p>Name: <i>Default Bastion SecList</i> Create in compartment: <i>OCI_Labs</i></p> <p>Add an ingress rule to allow ssh traffic over port 22 into the subnet.</p> <p>Stateless: Unchecked Source Type: CIDR Source CIDR: 0.0.0.0/0 IP Protocol: SSH (TCP/22)</p> <p>This rule will allow ssh traffic coming from anywhere into the subnet since the source CIDR is set to 0.0.0.0/0, which is shorthand for any address.</p> <p>*** For additional security, you should whitelist your own network address as the source CIDR so that OCI only permits ssh coming from a trusted location.</p> <p>For example, if you want to ssh into the bastion from your home, you could use the public IP address that is assigned</p>

by your Internet Service Provider.

Create Security List [Help](#) [Cancel](#)

A security list contains ingress and egress rules that specify the types of traffic allowed in and out of instances. [Learn more about Security Lists](#)

NAME

Default Bastion Security List

CREATE IN COMPARTMENT

techtipsondemand (root)

Allow Rules for Ingress

Ingress Rule 1

Allows TCP traffic for ports: 22 SSH Remote Login Protocol

☐ STATELESS ⓘ

SOURCE TYPE SOURCE CIDR IP PROTOCOL ⓘ

CIDR 0.0.0.0/0 SSH (TCP/22)

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

SOURCE PORT RANGE OPTIONAL ⓘ DESTINATION PORT RANGE OPTIONAL ⓘ

All 22

Example: 80, 90, 99

- 3.3. **Add an egress rule to the same bastion security list** to allow SSH traffic out of the public subnet to any location within the VCN. This will allow us to SSH into any private compute instance.

Click the Additional Egress Rule button and specify the following rules:

Stateless: Unchecked

Destination Type: CIDR

Destination CIDR: 10.0.0.0/16 (This is the CIDR block for the entire VCN)

IP Protocol: SSH (TCP/22)

Click Create Security List once you are done.


3.4. Security lists must be explicitly assigned to subnets. To assign the bastion security list to the bastion subnet, select Subnets under Resources on the vcn_oci_labs details page (Networking > Virtual Cloud Networks > vcn_oci_labs > Subnets).

Click on bastion-subnet in the Subnets table.

You will see the default security list assigned to the subnet on the Subnet details page.

3.5. Assign a security list by clicking the Add Security List button, then select the Default Bastion Security List.

3.6. Once the bastion security list is assigned, we can remove the default security list from the bastion subnet. Select the ellipsis (3 vertical dots) next to the Default Security List for vcn1 and then select Remove.



Security Lists

[Add Security List](#)

Name	State	Compartment	Created
Default Bastion Security List	● Available	techtipsondemand (root)	Thu, Aug 27, 2020, 01:02
Default Security List for wp-vcn	● Available	techtipsondemand (root)	Wed, Aug 19, 2020, 01:2

Showing 2 items

- View Details
- Edit
- Move Resource
- Copy OCID
- View Tags
- Add Tags
- Remove

3.7.

Repeat the previous steps to:

- 1) Create a new security list named Default Private Security List that allows ssh/22 into the app subnet from the bastion subnet. Be sure to use the bastion subnet's CIDR (10.0.0.0/28) as the source CIDR in the new list.
- 2) Assign the security list to the app subnet.
- 3) Remove the default security list from the app subnet.

The new rule should look like the following:

Default Private Security List

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

Move Resource Add Tags Terminate

Security List Information Tags

OCID: ...fwxbjq [Show](#) [Copy](#) Compartment: OCI_Labs

Created: Mon, Feb 15, 2021, 20:29:46 UTC

Ingress Rules

Add Ingress Rules Edit Remove

<input type="checkbox"/>	Stateless ▾	Source	IP Protocol	Source Port Range	Destination Port Range	Type and Code	Allows	Description
<input type="checkbox"/>	No	10.0.0.0/28	TCP	All	22		TCP traffic for ports: 22 SSH Remote Login Protocol	⋮

0 Selected Showing 1 Item < 1 of 1 >

3.8.

Up to this point, you have created a virtual cloud network and two subnets. You have also implemented virtual firewalls for each of the subnets using security lists. These security lists define what network traffic is allowed to flow in and out.

The next step is to define network routes to allow traffic to flow into and out of our VCN using OCI network gateways.

4.	Routing Internet Traffic using Route Tables and an Internet Gateway
4.1.	<p>In OCI route tables and gateways are used to send traffic out of a VCN.</p> <p>The OCI Internet Gateway is the first one you will create. An Internet Gateway is a virtual router that directs traffic to flow from the internet into a VCN, and conversely allows traffic to flow out of a VCN to the internet. This is different than a security list which is a firewall essentially that determines what protocols and ports are allowed.</p> <p>Only public subnets can use an IGW to send traffic to the internet since public subnets allow for public IP addresses. Resources with only private IP addresses cannot directly send traffic to the Internet. They need to use a NAT Gateway which we will cover shortly.</p> <p>To create an Internet Gateway, navigate to the vcn_oci_labs details page (Networking > Virtual Cloud Networks > vcn_oci_labs), and select Internet Gateways under Resources.</p>
4.2.	Click Create Internet Gateway button. Specify igw as the name of the gateway and place it in the OCI_Labs compartment.
4.3.	<p>With the internet gateway created, we need to create a route rule to tell the VCN how to route internet bound traffic.</p> <p>Under Resources, select Route Tables.</p>
4.4.	Add a new route rule to the Default Route Table by clicking on the name of the route table then click on Add Route Rules.

Default Route Table for vcn_oci_labs

Move Resource Add Tags Terminate

Route Table Information

Tags

OCID: ...72znfa [Show](#) [Copy](#)

Compartment: OCI_Labs

Created: Mon, Feb 15, 2021, 19:48:17 UTC

Route Rules

Add Route Rules

Edit

Remove



Destination

Target Type

Target

No items found.

0 Selected

4.5. Specify the following details for the route rule:

Target Type: *Internet Gateway*

Destination CIDR Block: 0.0.0.0/0

Target Internet Gateway: igw

The route rule will direct traffic to the internet (0.0.0.0/0) through the internet gateway.

Hit the Create button to create the rule.

Add Route Rules

[Help](#)


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.

Route Rule

TARGET TYPE

Internet Gateway

DESTINATION CIDR BLOCK

0.0.0.0/0

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

TARGET INTERNET GATEWAY IN **OCI_LAB5** [\(CHANGE COMPARTMENT\)](#)

igw

DESCRIPTION OPTIONAL

Maximum 255 characters

5. Create the Bastion Server

- 5.1. In this section we will create some compute instances to demonstrate how the routing and network security lists work.
- Start by creating a public compute instance called bastion1 in the bastion subnet using the same procedures in the previous lab. Be sure to check the box for assigning a public IP address. Use the same SSH key you generated earlier.
- 5.2. Verify you can access the bastion server using the public SSH key you provided.
- If you can connect, then you successfully configured your VCN to allow ssh traffic to the bastion server.
- If you cannot connect, verify the following:

	<ol style="list-style-type: none"> 1) The bastion server is assigned a public IP address (must be placed in a public subnet). 2) The bastion subnet has the correct security list and rules assigned to it to allow SSH/22 in (ingress). 3) The bastion subnet has a default route table with a route rule to use the internet gateway. 4) You are attempting to connect using the public IP address of the bastion server. 5) You are using the correct SSH key
6.	Create a Private Compute Instance
6.1.	<p>After the public instance is created and started, create another compute instance in the private subnet called app1. This time you will NOT assign a public IP address since this compute instance is private.</p> <p>Use the same SSH key as before.</p> <p>Start the instance and verify it is running in the OCI Console.</p> <p>Take note of its private IP address. We will need this to connect to it from the bastion server.</p>
6.2.	<p>Next let's verify the security rules for allowing ssh into the private subnet are working properly.</p> <p>SSH into the bastion server then ssh into the app server using its private IP address.</p> <p>If you get challenged for a login, then the networking is working, however you will not be able to login because you are not yet able to present your private SSH key to the app server. More on this in a moment.</p> <p>If your attempt to connect times out or you get another error trying to connect, then there may be issue with the security lists. If this is the case, verify the following:</p> <ol style="list-style-type: none"> 1) The Default Bastion Security List has an egress rule that allows ssh/22 to the VCN CIDR (10.0.0.0/16). 2) The Default Private Security List has an ingress rule that allows ssh/22 from the bastion subnet 10.0.0.0/28. 3) The Default Private Security List is assigned to the app subnet.
6.3.	<p>Next you will use the bastion server to connect to the private compute instance. Since the private compute instance does not have a public IP address, we cannot connect to it directly, however we can connect to it from the bastion server because the bastion server has a private IP address in the same VCN as the app server.</p> <p>You will 'jump' through the bastion server to private app server. To do this, you need to configure your SSH client to proxy or forward our SSH connection to the app server.</p>

	<p>Follow the instructions in the Appendix A : How to securely connect to private OCI instances over the Internet. This appendix covers both Windows and Linux/OSX SSH clients.</p>
6.4.	<p>Once you have completed the instructions for setting up SSH agent-forwarding, verify you can connect to the private compute instance by first connecting to the public server using its public IP address.</p> <p>Once connected to the public server, ssh to the private server using its private IP address. If you properly set up your SSH client to use agent forwarding, you should not be prompted for any authentication credentials when connecting to the private instance.</p>
6.5.	<p>Try accessing the public internet from the private compute instance.</p> <p>\$ curl -L https://www.google.com</p> <p>Curl should not work for two reasons:</p> <ol style="list-style-type: none"> 1) We have not told OCI how to handle internet-bound traffic. We need a route rule defined to solve this problem. 2) We have not created a network security rule to allow http traffic to leave the subnet for the internet. We need a security rule to permit HTTP/HTTPS. <p>In the next section you will create routing gateways to allow access to the internet.</p>
7.	Routing Traffic to the Internet using OCI NAT Gateway
7.1.	<p>Compute instances need a public IP in order to send requests to the Internet. The Internet Gateway allows instances in public subnets with public IP addresses direct access to the Internet.</p> <p>Compute instances in a private subnet do not have a public IP address, so they cannot directly access the internet. For this situation, OCI provides a NAT Gateway virtual router. The NAT Gateway (NATGW) is a virtual router that gets provisioned in a public subnet and assigned a public IP. Private subnet traffic headed to the internet is routed through the NATGW. NATGW allows responses from the internet back into the VCN. NATGW is only used for egress out of the VCN, not for ingress.</p> <p>In this section you will provision and configured a NAT Gateway to allow compute instances in a private subnet to access the internet.</p>
7.2.	Navigate again to the VCN details page and select NAT Gateways under Resources.
7.3.	Create a NAT Gateway by clicking the button and specifying the following details:

Name: natgw
Compartment: OCI_Labs

Create NAT Gateway [Help](#) [Cancel](#)

A NAT gateway lets instances that don't have public IP addresses access the Internet.

NAME
wp-natgw

CREATE IN COMPARTMENT
techtipsondemand (root)

Tagging is a metadata system that allows you to organize and track resources within your tenancy. Tags are composed of keys and values that can be attached to resources.
[Learn more about tagging](#)

TAG NAMESPACE	TAG KEY	VALUE
None (add a free-for...)		

+ Additional Tag

Note: A public IP will be automatically created for this NAT gateway.

Create NAT Gateway Cancel

OCI will automatically assign a public IP address to the gateway. You can see the assigned public IP address for the NAT gateway listed under NAT Gateways.

7.4. Next we need to define a route rule that will send internet bound traffic through the NAT Gateway. Since this route is only for private compute instances, we need to separate this route from the other route we created using the Internet Gateway. To do this, we will create a new route table.

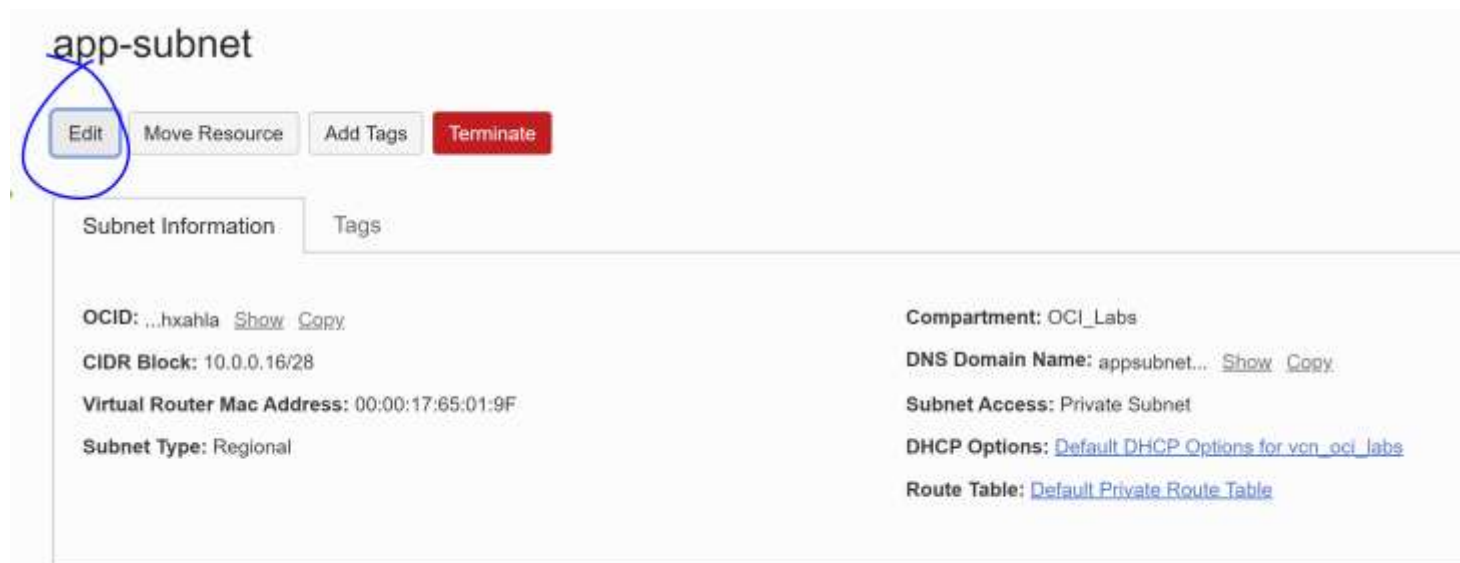
Under Route Tables for the VCN, click the Create Route Table button to create a new table named Default Private Route Table.

- 7.5. Next add a new route rule that will send traffic from the private subnet to the internet by clicking on the new route table then clicking on the Add Route Rules button.

Here is the route rule that will send internet-bound traffic to the NAT Gateway.

Target Type: NAT Gateway
Destination CIDR block: 0.0.0.0/0
Target NAT Gateway: natgw

- 7.6. Assign the Default Private Route Table to the app-subnet by editing the subnet and changing the route table to Default Private Route Table.



- 7.7. With our route defined, we now need to create a security rule to allow traffic to flow out of the app-subnet.
- Create an **egress** rule in the Default Private Security List to allow TCP from the private subnet to the internet.

Stateless: Unchecked
Destination Type: CIDR
Destination CIDR: 0.0.0.0/0
IP Protocol: TCP

Edit Egress Rule

Egress Rule 1

TCP traffic for ports: All

☐ STATELESS ⓘ

DESTINATION TYPE: CIDR

DESTINATION CIDR: 0.0.0.0/0
Specified IP addresses: 0.0.0.0-255.255.255.255 (4,294,967,296 IP addresses)

IP PROTOCOL ⓘ: TCP

SOURCE PORT RANGE OPTIONAL ⓘ: All
Examples: 80, 20-22

DESTINATION PORT RANGE OPTIONAL ⓘ: All
Examples: 80, 20-22

DESCRIPTION OPTIONAL
Maximum 255 characters

Save Changes Cancel

- 7.8. Verify the private compute instance app1 can now access the internet by connecting to it using SSH through the bastion server as we did earlier in the lab, then run the following curl command.
- ```
$ curl https://www.google.com
```
- curl should return HTML from Google. If you receive a connection time out or any other connection error, verify that you have
- 1) Routed traffic from the app-subnet to the NAT Gateway using a route rule.

|           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|           | 2) Allowed TCP traffic to leave the app-subnet for the Internet using a security rule.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>8.</b> | <b>Routing Traffic to OCI Services using Service Gateway</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| 8.1.      | <p>OCI Service Gateway is yet another virtual router that is used to access regional OCI services such as Object Storage privately without sending the traffic over the public internet. OCI services are hosted on a special network known as the Oracle Services Network.</p> <p>The OCI Service Gateway allows compute instances in your VCN to access OCI services using public endpoints but keeps the network flow from going over the internet. Using a Service Gateway is an alternative to configuring a NAT Gateway. With a NAT Gateway, network traffic is routed out to the internet, ev</p> <p>In this section you will create the Service Gateway in your VCN, then write a route rule to send traffic destined for OCI services through the Service Gateway.</p> |
| 8.2.      | Navigate to Service Gateways under Resources on the VCN details page.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

## vcn\_oci\_labs

Move Resource

Add Tags

Terminate

VCN Information

Tags

**Compartment:** OCI\_Labs

**Created:** Mon, Feb 15, 2021, 19:48:17 UTC

**CIDR Block:** 10.0.0.0/16

**OCID:** ...ylryzq [Show](#) [Copy](#)
**DNS Resolver:** [vcn\\_oci\\_labs](#)
**Default Route Table:** [Default Route Table for vcn\\_oci\\_labs](#)
**DNS Domain Name:** vcnocilabs.oraclevcn.com

## Service Gateways *in OCI\_Labs Compartment*

Create Service Gateway

| Name | State | Services | Route Table ⓘ | Created |
|------|-------|----------|---------------|---------|
|------|-------|----------|---------------|---------|

No items found.

Show

- 8.3. Click Create Service Gateway and specify the following details:
- Name:** sgw  
**Compartment:** OCI\_Labs  
**Services:** All <Region> Services in Oracle Services Network
- The value for Services in the dropdown will vary depending on what region you are working in.

**Create Service Gateway** [Help](#)

**Information** Make sure to set up route rules and security rules to enable the desired access to the service gateway. [Learn more about service gateways.](#)

**Warning** Your workloads may need access to public endpoints not supported by the service gateway (for example, to get updates or patches). Ensure you have a NAT gateway or other access to the internet if necessary. [Learn more.](#)

NAME  
wp-sgw

CREATE IN COMPARTMENT  
techtipsondemand (root)

SERVICES  
All PHX Services In Oracle Services Network

[Show Advanced Options](#)

- 8.4. Next create a route rule to send network requests for OCI services (like object storage) to the service gateway.
- In this exercise, only the private subnets will be accessing OCI services privately, so create the rule in the Default Private Route Table.
- Add the following route rule to the Default Private Route Table:
- Target Type:** Service Gateway  
**Destination Service:** All <Region> Services in Oracle Service Network  
**Target Service Gateway:** sgw



Networking » Virtual Cloud Networks » wp-vcn » Route Table Details

## Default Private Route Table

Move Resource
Add Tags
Terminate

Route-Table Information
Tags

OCID: [oh5lcaq](#) [Show](#) [Copy](#)

Created: Thu, Aug 27, 2020, 12:56:27 UTC

AVAILABLE

Resources

Route Rules (1)

| Destination | Target Type | Target                   |
|-------------|-------------|--------------------------|
| 0.0.0.0/0   | NAT Gateway | <a href="#">wp-natgw</a> |

0 Selected

## Add 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.

### Route Rule

TARGET TYPE

Service Gateway

DESTINATION SERVICE ⓘ

All PHX Services In Oracle Services Network

TARGET SERVICE GATEWAY IN TECHTIPSONDEMAND (ROOT)

[/CHANGE COMPARTMENT/](#)

wp-sgw

DESCRIPTION (OPTIONAL)

Maximum 255 characters

+ Additional Route Rule

Add Route Rules
Cancel

- 8.5. The Default Private Route Table should now look like the screenshot below. This route table contains two rules: one for sending traffic for Oracle Services through the service gateway, and all other traffic intended for the internet through the NAT gateway.

## Route Rules

| <a href="#">Add Route Rules</a> <a href="#">Edit</a> <a href="#">Remove</a> |                                                                  |                 |                       |
|-----------------------------------------------------------------------------|------------------------------------------------------------------|-----------------|-----------------------|
| <input type="checkbox"/>                                                    | Destination                                                      | Target Type     | Target                |
| <input type="checkbox"/>                                                    | 0.0.0.0/0                                                        | NAT Gateway     | <a href="#">natgw</a> |
| <input type="checkbox"/>                                                    | <a href="#">All PHX Services In Oracle Services Netw<br/>ork</a> | Service Gateway | <a href="#">sgw</a>   |
| 0 Selected                                                                  |                                                                  |                 |                       |

- 8.6. Now that we have our routes set up, we need to modify our security lists to allow compute instances in the private subnet to talk to OCI services.
- Add a new egress rule to the Default Private Security List:
- Destination Type:** Service  
**Destination Service:** All <Region> Services in Oracle Services Network  
**IP Protocol:** TCP
- You can leave destination port blank for now. This egress rule will permit any TCP traffic to the Oracle Service Network.

The screenshot shows the 'Add Egress Rules' window in the Oracle Cloud console. It is titled 'Egress Rule 1'. Below the title, it says 'Allows TCP traffic'. There is a 'STATELESS' checkbox which is currently unchecked. The 'DESTINATION TYPE' is set to 'Service'. The 'DESTINATION SERVICE' is set to 'All PHX Services In Oracle Service...'. The 'IP PROTOCOL' is set to 'TCP'. Both the 'SOURCE PORT RANGE' and 'DESTINATION PORT RANGE' are set to 'All'. Below these fields, there are examples: 'Examples: 80, 20-22'. The 'DESCRIPTION' field contains the text 'Allow app subnet to talk to OSN'. At the bottom of the window, there are three buttons: 'Add Egress Rules' (in blue), 'Cancel', and '+ Additional Egress Rule'.

Once the rule is created, requests for OCI services from our private subnet will be routed through the OSN and not out to the public internet. This keeps the traffic more secure since it does not expose it publicly.

**9. Shutdown all Compute Instances**

9.1. Be sure to stop any running compute instances when you are finished with the lab. A stopped instance does not incur any charges.

Do not terminate the instances as that will delete them. We will be reusing bastion1 and app1 in later labs.

**Conclusion**

In this lab you learned how to:

- 1) Create VCNs and subnets

- 2) Implement virtual firewalls using Network Security Lists
- 3) Route traffic in and out of the VCN using Internet and NAT Gateways
- 4) Route Oracle Services traffic privately to the Service Gateway

## Lab #4: Core OCI Block Storage

*Duration 60 minutes*

### Skills Learned

At the end of this exercise, you will be able to:

- Provision and attach block storage volumes to compute instances
- Backup and restore volumes
- Clone volumes
- Monitor storage usage

### Overview

The OCI Block Volume Service provides raw high performance durable block volume storage for compute instances. If you need to install and run software on your compute instances, you would do so on a block volume attached to the compute instance. In fact, the boot volume on any OCI compute instance is just a special type of block volume.

In this lab you will learn how to provision, attach, and manage block volumes through backups and cloning.

Block volume storage, like all other storage services in OCI, costs money and the limits to the number of volumes and size of those volumes in the Oracle Free Trial Period and Free Tier is quite limited. Block volume storage is billed based on total provisioned capacity per month. If you provision a 1 TB volume but are only using 50 GB of it, you will be charged for the full 1 TB per month. This is different than object storage where you pay for only what you consume.

To keep any potential costs down, it is highly recommended that students delete all volumes and volume backups at the end of each exercise.

### Instructions

|      |                                                                                                                      |
|------|----------------------------------------------------------------------------------------------------------------------|
| 1.   | <b>Adding Storage to a Compute Instance using a Block Volume</b>                                                     |
| 1.1. | Block volumes provide a compute instance with durable storage which allows the data on the volume to persist between |

reboots of a compute instance. The process for provisioning a volume and using it with a compute instance is as follows:

- 1) Create a block volume of a certain size with certain performance characteristics.
- 2) Attach the volume to the compute instance. This is the process of associating the volume with a compute instance.
- 3) Format and mount the volume as a file system on the compute instance.

In this lab you will attach a 50 GB block volume to the private compute instance, app1, that you created in the Core Compute lab.

- 1.2. First we need to find out what Availability Domain our app1 instance is in so we know where to create the block volume. The block volume must live in the same AD as our compute instance. A block volume resource, much like a compute resource cannot span different data centers or ADs. It is an AD-local resource.

- 1.3. In the OCI Console, navigate to Compute > Instance. Make sure to select the OCI Labs compartment.

Take note of the Availability Domain for app1.

### Instances in OCI\_Labs Compartment

The [Compute service](#) helps you provision VMs and bare metal instances to meet your compute and application requirements. An [instance](#) is a compute host. Choose between virtual machines (VMs) and bare metal instances. The image that you use to launch an instance determines its operating system and other software.

Create Instance

| Name                                | State   | Public IP     | Shape                  | OCPU Count | Memory (GB) | Availability domain | Fault domain | Created        |
|-------------------------------------|---------|---------------|------------------------|------------|-------------|---------------------|--------------|----------------|
| app1 <small>Always Free</small>     | Running | -             | VM.Standard.E2.1.Micro | 1          | 1           | AD-1                | FD-2         | Tue, Feb 16, 2 |
| bastion1 <small>Always Free</small> | Running | 158.101.9.198 | VM.Standard.E2.1.Micro | 1          | 1           | AD-1                | FD-2         | Mon, Feb 15, 1 |

Showing 2 Items

- 1.4. Now create the block volume by navigating to Block Storage > Block Volumes from the navigation menu.

- 1.5. Click the Create Block Volume button and specify the following parameters:

**Name:** app1\_datavol

**Create in Compartment:** OCI\_Labs

**Availability Domain:** *Select same as app1*

OCI allows us to define performance characteristics for block volumes. Performance is typically linear, meaning the larger the volume, the more IOPS or throughput is provided.

To keep costs to a minimum, **select Custom under Volume Size and Performance.**

**Volume Size (In GB):** 50 GB

**Default Volume Performance:** Lower Cost

Keep the default values for the rest of the parameters.

Click Create Block Volume.

---

## Create Block Volume

Name

app1\_datavol

Create In Compartment

OCI\_Labs

techtipsondemand (root)/OCI\_Labs

Availability Domain

wHOZ:PHX-AD-1

### Volume Size and Performance

☐ DEFAULT ☒ CUSTOM

VOLUME SIZE (IN GB)

50

Size must be between 50 GB and 32,768 GB (32 TB). Volume performance varies with volume size.

DEFAULT VOLUME PERFORMANCE

Lower Cost      Balanced      Higher Performance

Recommended for workloads that are throughput intensive with large sequential I/O, such as big data and streaming, log processing and data warehouses. [Learn more](#)

#### Default Volume Performance

IOPS: Up to 100 IOPS (2 IOPS/GB)

Throughput: Up to 12 MB/s (240 KB/s/GB)

Create Block Volume

[Cancel](#)

- 1.6. Once the volume is provisioned and available, you can attach it to a compute instance.
- Click on the block volume you just created, then click on Attached Instances then Attach to Instance.
- 1.7. The Attach to Instance dialog will present several different options for configuring the attachment. There are two attachment types available – Paravirtualized and iSCSI. Paravirtualized is far simpler to configure, however, iscsi provides much better performance.



Let's start with Paravirtualized first.

**Attachment type:** *Paravirtualized*

**Access Type:** *Read/Write*

**Instance:** *app1* (OCI Labs compartment)

**Device name:** */dev/oracleoci/oraclevd*

The device name is where the volume will exist as a device in Linux.

Attach the volume by clicking the Attach button.

1.8. Once the volume is done attaching, your screen should look like the following:

## Attached Block Volumes

[Block volumes](#) provide high-performance network storage to support a broad range of I/O intensive workloads.

Attach Block Volume

| Name                        | State      | Volume Type  | Device path             | Type            | Access     | Size  |
|-----------------------------|------------|--------------|-------------------------|-----------------|------------|-------|
| <a href="#">app_datavol</a> | ● Attached | Block Volume | /dev/oracleoci/oraclevd | paravirtualized | Read/Write | 50 GB |

1.9. The next step is to partition, format, and mount the volume on the host.

SSH into app1 by connecting to the bastion first then hopping over to app1.

1.10. Verify the volume is attached to the host by running fdisk. Look for /dev/sdb in the output.

```
[opc@app1 ~]$ sudo fdisk -l
```

WARNING: fdisk GPT support is currently new, and therefore in an experimental phase. Use

at your own discretion.

Disk /dev/sda: 50.0 GB, 50010783744 bytes, 97677312 sectors  
Units = sectors of 1 \* 512 = 512 bytes  
Sector size (logical/physical): 512 bytes / 4096 bytes  
I/O size (minimum/optimal): 4096 bytes / 1048576 bytes  
Disk label type: gpt  
Disk identifier: 6F25D687-CAE6-428A-8AA0-E618C576A2EB

| # | Start    | End      | Size  | Type            | Name                 |
|---|----------|----------|-------|-----------------|----------------------|
| 1 | 2048     | 411647   | 200M  | EFI System      | EFI System Partition |
| 2 | 411648   | 17188863 | 8G    | Linux swap      |                      |
| 3 | 17188864 | 97675263 | 38.4G | Microsoft basic |                      |

**Disk /dev/sdb: 53.7 GB, 53687091200 bytes, 104857600 sectors**  
Units = sectors of 1 \* 512 = 512 bytes  
Sector size (logical/physical): 512 bytes / 4096 bytes  
I/O size (minimum/optimal): 4096 bytes / 1048576 bytes

---

1.11. Run fdisk to create a new primary partition on the volume.

```
$ sudo fdisk /dev/sdb
```

**Command (m for help): n**

Partition type:

  p  primary (0 primary, 0 extended, 4 free)  
  e  extended

**Select (default p): p**

**Partition number (1-4, default 1): 1**

First sector (2048-104857599, default 2048):

Using default value 2048

Last sector, +sectors or +size{K,M,G} (2048-104857599, default 104857599):

Using default value 104857599

Partition 1 of type Linux and of size 50 GiB is set

**Command (m for help): w**

The partition table has been altered!

Calling ioctl() to re-read partition table.

|                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |            |            |           |                 |      |            |          |      |   |      |    |      |       |      |   |      |    |          |       |      |      |      |    |      |       |      |   |      |    |                |           |     |      |     |    |   |           |      |      |      |    |           |       |     |   |     |    |             |       |     |   |     |    |               |       |     |   |     |    |                |                  |            |            |            |           |                 |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|-----------|-----------------|------|------------|----------|------|---|------|----|------|-------|------|---|------|----|----------|-------|------|------|------|----|------|-------|------|---|------|----|----------------|-----------|-----|------|-----|----|---|-----------|------|------|------|----|-----------|-------|-----|---|-----|----|-------------|-------|-----|---|-----|----|---------------|-------|-----|---|-----|----|----------------|------------------|------------|------------|------------|-----------|-----------------|
|                  | Syncing disks.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |            |            |           |                 |      |            |          |      |   |      |    |      |       |      |   |      |    |          |       |      |      |      |    |      |       |      |   |      |    |                |           |     |      |     |    |   |           |      |      |      |    |           |       |     |   |     |    |             |       |     |   |     |    |               |       |     |   |     |    |                |                  |            |            |            |           |                 |
| 1.12.            | <p>Format the volume once it is partitioned.</p> <pre>[opc@app1 ~]\$ sudo mkfs -t ext4 /dev/sdb1</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |            |            |           |                 |      |            |          |      |   |      |    |      |       |      |   |      |    |          |       |      |      |      |    |      |       |      |   |      |    |                |           |     |      |     |    |   |           |      |      |      |    |           |       |     |   |     |    |             |       |     |   |     |    |               |       |     |   |     |    |                |                  |            |            |            |           |                 |
| 1.13.            | <p>Mount the volume under a new directory named /datavol</p> <pre>[opc@app1 ~]\$ sudo mkdir /datavol</pre> <pre>[opc@app1 ~]\$ sudo mount /dev/sdb1 /datavol</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |            |            |           |                 |      |            |          |      |   |      |    |      |       |      |   |      |    |          |       |      |      |      |    |      |       |      |   |      |    |                |           |     |      |     |    |   |           |      |      |      |    |           |       |     |   |     |    |             |       |     |   |     |    |               |       |     |   |     |    |                |                  |            |            |            |           |                 |
| 1.14.            | <p>Run df to view the mounted volumes.</p> <pre>[opc@app1 ~]\$ df -h</pre> <table><tr><td>Filesystem</td><td>Size</td><td>Used</td><td>Avail</td><td>Use%</td><td>Mounted on</td></tr><tr><td>devtmpfs</td><td>315M</td><td>0</td><td>315M</td><td>0%</td><td>/dev</td></tr><tr><td>tmpfs</td><td>345M</td><td>0</td><td>345M</td><td>0%</td><td>/dev/shm</td></tr><tr><td>tmpfs</td><td>345M</td><td>9.3M</td><td>336M</td><td>3%</td><td>/run</td></tr><tr><td>tmpfs</td><td>345M</td><td>0</td><td>345M</td><td>0%</td><td>/sys/fs/cgroup</td></tr><tr><td>/dev/sda3</td><td>39G</td><td>2.9G</td><td>36G</td><td>8%</td><td>/</td></tr><tr><td>/dev/sda1</td><td>200M</td><td>8.6M</td><td>192M</td><td>5%</td><td>/boot/efi</td></tr><tr><td>tmpfs</td><td>69M</td><td>0</td><td>69M</td><td>0%</td><td>/run/user/0</td></tr><tr><td>tmpfs</td><td>69M</td><td>0</td><td>69M</td><td>0%</td><td>/run/user/994</td></tr><tr><td>tmpfs</td><td>69M</td><td>0</td><td>69M</td><td>0%</td><td>/run/user/1000</td></tr><tr><td><b>/dev/sdb1</b></td><td><b>49G</b></td><td><b>52M</b></td><td><b>47G</b></td><td><b>1%</b></td><td><b>/datavol</b></td></tr></table> | Filesystem | Size       | Used      | Avail           | Use% | Mounted on | devtmpfs | 315M | 0 | 315M | 0% | /dev | tmpfs | 345M | 0 | 345M | 0% | /dev/shm | tmpfs | 345M | 9.3M | 336M | 3% | /run | tmpfs | 345M | 0 | 345M | 0% | /sys/fs/cgroup | /dev/sda3 | 39G | 2.9G | 36G | 8% | / | /dev/sda1 | 200M | 8.6M | 192M | 5% | /boot/efi | tmpfs | 69M | 0 | 69M | 0% | /run/user/0 | tmpfs | 69M | 0 | 69M | 0% | /run/user/994 | tmpfs | 69M | 0 | 69M | 0% | /run/user/1000 | <b>/dev/sdb1</b> | <b>49G</b> | <b>52M</b> | <b>47G</b> | <b>1%</b> | <b>/datavol</b> |
| Filesystem       | Size                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Used       | Avail      | Use%      | Mounted on      |      |            |          |      |   |      |    |      |       |      |   |      |    |          |       |      |      |      |    |      |       |      |   |      |    |                |           |     |      |     |    |   |           |      |      |      |    |           |       |     |   |     |    |             |       |     |   |     |    |               |       |     |   |     |    |                |                  |            |            |            |           |                 |
| devtmpfs         | 315M                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 0          | 315M       | 0%        | /dev            |      |            |          |      |   |      |    |      |       |      |   |      |    |          |       |      |      |      |    |      |       |      |   |      |    |                |           |     |      |     |    |   |           |      |      |      |    |           |       |     |   |     |    |             |       |     |   |     |    |               |       |     |   |     |    |                |                  |            |            |            |           |                 |
| tmpfs            | 345M                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 0          | 345M       | 0%        | /dev/shm        |      |            |          |      |   |      |    |      |       |      |   |      |    |          |       |      |      |      |    |      |       |      |   |      |    |                |           |     |      |     |    |   |           |      |      |      |    |           |       |     |   |     |    |             |       |     |   |     |    |               |       |     |   |     |    |                |                  |            |            |            |           |                 |
| tmpfs            | 345M                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 9.3M       | 336M       | 3%        | /run            |      |            |          |      |   |      |    |      |       |      |   |      |    |          |       |      |      |      |    |      |       |      |   |      |    |                |           |     |      |     |    |   |           |      |      |      |    |           |       |     |   |     |    |             |       |     |   |     |    |               |       |     |   |     |    |                |                  |            |            |            |           |                 |
| tmpfs            | 345M                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 0          | 345M       | 0%        | /sys/fs/cgroup  |      |            |          |      |   |      |    |      |       |      |   |      |    |          |       |      |      |      |    |      |       |      |   |      |    |                |           |     |      |     |    |   |           |      |      |      |    |           |       |     |   |     |    |             |       |     |   |     |    |               |       |     |   |     |    |                |                  |            |            |            |           |                 |
| /dev/sda3        | 39G                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 2.9G       | 36G        | 8%        | /               |      |            |          |      |   |      |    |      |       |      |   |      |    |          |       |      |      |      |    |      |       |      |   |      |    |                |           |     |      |     |    |   |           |      |      |      |    |           |       |     |   |     |    |             |       |     |   |     |    |               |       |     |   |     |    |                |                  |            |            |            |           |                 |
| /dev/sda1        | 200M                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 8.6M       | 192M       | 5%        | /boot/efi       |      |            |          |      |   |      |    |      |       |      |   |      |    |          |       |      |      |      |    |      |       |      |   |      |    |                |           |     |      |     |    |   |           |      |      |      |    |           |       |     |   |     |    |             |       |     |   |     |    |               |       |     |   |     |    |                |                  |            |            |            |           |                 |
| tmpfs            | 69M                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 0          | 69M        | 0%        | /run/user/0     |      |            |          |      |   |      |    |      |       |      |   |      |    |          |       |      |      |      |    |      |       |      |   |      |    |                |           |     |      |     |    |   |           |      |      |      |    |           |       |     |   |     |    |             |       |     |   |     |    |               |       |     |   |     |    |                |                  |            |            |            |           |                 |
| tmpfs            | 69M                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 0          | 69M        | 0%        | /run/user/994   |      |            |          |      |   |      |    |      |       |      |   |      |    |          |       |      |      |      |    |      |       |      |   |      |    |                |           |     |      |     |    |   |           |      |      |      |    |           |       |     |   |     |    |             |       |     |   |     |    |               |       |     |   |     |    |                |                  |            |            |            |           |                 |
| tmpfs            | 69M                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 0          | 69M        | 0%        | /run/user/1000  |      |            |          |      |   |      |    |      |       |      |   |      |    |          |       |      |      |      |    |      |       |      |   |      |    |                |           |     |      |     |    |   |           |      |      |      |    |           |       |     |   |     |    |             |       |     |   |     |    |               |       |     |   |     |    |                |                  |            |            |            |           |                 |
| <b>/dev/sdb1</b> | <b>49G</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | <b>52M</b> | <b>47G</b> | <b>1%</b> | <b>/datavol</b> |      |            |          |      |   |      |    |      |       |      |   |      |    |          |       |      |      |      |    |      |       |      |   |      |    |                |           |     |      |     |    |   |           |      |      |      |    |           |       |     |   |     |    |             |       |     |   |     |    |               |       |     |   |     |    |                |                  |            |            |            |           |                 |
| 2.               | <b>Adding the volume to /etc/fstab</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |            |            |           |                 |      |            |          |      |   |      |    |      |       |      |   |      |    |          |       |      |      |      |    |      |       |      |   |      |    |                |           |     |      |     |    |   |           |      |      |      |    |           |       |     |   |     |    |             |       |     |   |     |    |               |       |     |   |     |    |                |                  |            |            |            |           |                 |
| 2.1.             | <p>If you want the data volume to be permanently mounted on the host, it must be added to /etc/fstab. If you were to reboot the compute instance now, the volume would not appear mounted.</p> <p>Edit /etc/fstab and add the following line at the bottom of the file.</p> <pre>\$ sudo vi /etc/fstab</pre> <p>Append the following line to /etc/fstab</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |            |            |           |                 |      |            |          |      |   |      |    |      |       |      |   |      |    |          |       |      |      |      |    |      |       |      |   |      |    |                |           |     |      |     |    |   |           |      |      |      |    |           |       |     |   |     |    |             |       |     |   |     |    |               |       |     |   |     |    |                |                  |            |            |            |           |                 |

|           |                                                                                                                                                                                                                                                                                                                                                        |
|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|           | <pre>/dev/sdb1    /datavol    ext4    defaults    0    1</pre>                                                                                                                                                                                                                                                                                         |
| 2.2.      | <p>Run the commands to verify our changes work:</p> <p>First unmount /datavol.</p> <pre>\$ sudo umount /datavol</pre> <p>Remount the volumes in /etc/fstab</p> <pre>\$ sudo mount -a</pre>                                                                                                                                                             |
| 2.3.      | <p>Verify /datavol has been remounted.</p> <pre>\$ sudo df -h</pre>                                                                                                                                                                                                                                                                                    |
| 2.4.      | <p>Back in the OCI Console, restart the app1 compute instance.</p> <p>Go to Compute &gt; Instances &gt; app1. Select Reboot from the menu.</p>                                                                                                                                                                                                         |
| 2.5.      | After app1 reboots, ssh into app1 and confirm /datavol is automatically mounted.                                                                                                                                                                                                                                                                       |
| <b>3.</b> | <b>Attaching a Block Volume using ISCSI</b>                                                                                                                                                                                                                                                                                                            |
| 3.1.      | <p>Paravirtualized attachments are a simple and easy way to attach a block volume to a host as we performed in the previous lab. However, there are performance advantages to attaching volumes using ISCSI.</p> <p>In this section you will detach the volume we just mounted and reattach using ISCSI.</p>                                           |
| 3.2.      | <p>On the app1, unmount the volume. You can run df again to see that is no longer mounted.</p> <pre>[opc@app1 ~]\$ sudo umount /datavol [opc@app1 ~]\$ df -h Filesystem      Size  Used Avail Use% Mounted on devtmpfs        315M   0   315M   0% /dev tmpfs           345M   0   345M   0% /dev/shm tmpfs           345M  9.3M  336M   3% /run</pre> |

```
tmpfs 345M 0 345M 0% /sys/fs/cgroup
/dev/sda3 39G 2.9G 36G 8% /
/dev/sda1 200M 8.6M 192M 5% /boot/efi
tmpfs 69M 0 69M 0% /run/user/0
tmpfs 69M 0 69M 0% /run/user/994
tmpfs 69M 0 69M 0% /run/user/1000
```

- 3.3. In the OCI Console, detach the block volume from app1 by going to the app1 compute instance details page > Attached Block Volumes and selecting Detach from the menu for the app\_datavol volume.

### Attached Block Volumes

[Block volumes](#) provide high-performance network storage to support a broad range of I/O intensive workloads.

Attach Block Volume

| Name        | State    | Volume Type  | Device path             | Type            | Access     | Size  | AD   | Created  |                                                                                          |
|-------------|----------|--------------|-------------------------|-----------------|------------|-------|------|----------|------------------------------------------------------------------------------------------|
| app_datavol | Attached | Block Volume | /dev/oracleoci/oraclevd | paravirtualized | Read/Write | 50 GB | AD-1 | Sat, Feb | View Block Volume Details<br>Copy Attachment OCID<br>Copy Resource OCID<br><b>Detach</b> |

- 3.4. Reattach the volume but this time specify ISCSI as the attachment type.

## Attach Block Volume

### Volume attachment type

- ☐ Let Oracle Cloud Infrastructure choose the best attachment type  
☒ ISCSI  
☐ Paravirtualized

☐ Require CHAP Credentials

- ☒ Select volume   ☐ Enter volume OCID

Block Volume in OCI\_Labs [\(Change Compartment\)](#)

app\_datavol



### Caution

This Block Volume is not an Always Free resource and may be lost when your Free Trial expires. We recommend using Always Free block volumes with Always Free instances, or you can [upgrade now](#) and not have to worry about it.

Device path *Optional* ⓘ

/dev/oracleoci/oraclevd

### Access

- ☒ **Read/Write**  
 Configures the volume attachment as read/write, not shared with other instances. This enables attachment to a single instance only and is the default configuration.
- ☐ **Read/Write - Shareable**  
 Configures the volume attachment as read/write, shareable with other instances. This enables read/write attachment to multiple instances.
- ☐ **Read Only - Shareable**

**Attach**

[Cancel](#)

3.5. Once the volume shows as attached in the OCI Console, you will need to run a series of ISCSI commands on the app1 compute instance.

The ISCI commands are specific to the volume and the compute instance. To get the commands, click on the ellipsis next to the attached volume and select iSCSI Commands and Information from the menu.

The screenshot below shows us the commands specific to this particular block volume.

## iSCSI Commands & Information

[Help](#)

Use OS tools to edit your `/etc/fstab` volume to have the `_netdev` and `nofail` options from the OS. Failure to run commands will cause instance boot failure.

Commands for connecting

```
sudo iscsiadm -m node -o new -T iqn.2015-12.com.oracleiaas:91ad9130-640c-4aff-8a11-5977708535
sudo iscsiadm -m node -o update -T iqn.2015-12.com.oracleiaas:91ad9130-640c-4aff-8a11-5977708535
sudo iscsiadm -m node -T iqn.2015-12.com.oracleiaas:91ad9130-640c-4aff-8a11-5977708535
```

[Copy](#)

Commands for disconnecting

```
sudo iscsiadm -m node -T iqn.2015-12.com.oracleiaas:91ad9130-640c-4aff-8a11-5977708535
sudo iscsiadm -m node -o delete -T iqn.2015-12.com.oracleiaas:91ad9130-640c-4aff-8a11-5977708535
```

[Copy](#)

**IP address and port:** 169.254.2.4:3260 [Copy](#)

**Volume IQN:** iqn.2015-12.com.oracleiaas:91ad9130-640c-4aff-8a11-5977708535b6 [Copy](#)

Close

3.6. It is recommended that you copy these commands into a text file or somewhere you can reference them later. You can also come back to the console to retrieve the commands.

3.7. SSH into app1 and run the iSCSI commands for connecting to the volume.

3.8. Run `fdisk -l` to see the disk attached to the host. Notice that the partition you created earlier, `/dev/sdb1`, has been preserved.

```
[opc@app1 ~]$ sudo fdisk -l
```

```
WARNING: fdisk GPT support is currently new, and therefore in an experimental phase. Use
at your own discretion.
```

```

Disk /dev/sda: 50.0 GB, 50010783744 bytes, 97677312 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 4096 bytes
I/O size (minimum/optimal): 4096 bytes / 1048576 bytes
Disk label type: gpt
Disk identifier: 6F25D687-CAE6-428A-8AA0-E618C576A2EB

```

| # | Start    | End      | Size  | Type            | Name                 |
|---|----------|----------|-------|-----------------|----------------------|
| 1 | 2048     | 411647   | 200M  | EFI System      | EFI System Partition |
| 2 | 411648   | 17188863 | 8G    | Linux swap      |                      |
| 3 | 17188864 | 97675263 | 38.4G | Microsoft basic |                      |

```

Disk /dev/sdb: 53.7 GB, 53687091200 bytes, 104857600 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 4096 bytes
I/O size (minimum/optimal): 4096 bytes / 1048576 bytes
Disk label type: dos
Disk identifier: 0xfc457d0f

```

| Device    | Boot | Start | End       | Blocks   | Id | System |
|-----------|------|-------|-----------|----------|----|--------|
| /dev/sdb1 |      | 2048  | 104857599 | 52427776 | 83 | Linux  |

### 3.9. Mount the partition under /datavol as before.

```

[opc@app1 ~]$ sudo mount /dev/sdb1 /datavol
[opc@app1 ~]$ df -h

```

| Filesystem | Size | Used | Avail | Use% | Mounted on     |
|------------|------|------|-------|------|----------------|
| devtmpfs   | 315M | 0    | 315M  | 0%   | /dev           |
| tmpfs      | 345M | 0    | 345M  | 0%   | /dev/shm       |
| tmpfs      | 345M | 9.3M | 336M  | 3%   | /run           |
| tmpfs      | 345M | 0    | 345M  | 0%   | /sys/fs/cgroup |
| /dev/sda3  | 39G  | 2.9G | 36G   | 8%   | /              |
| /dev/sda1  | 200M | 8.6M | 192M  | 5%   | /boot/efi      |
| tmpfs      | 69M  | 0    | 69M   | 0%   | /run/user/0    |
| tmpfs      | 69M  | 0    | 69M   | 0%   | /run/user/994  |
| tmpfs      | 69M  | 0    | 69M   | 0%   | /run/user/1000 |
| /dev/sdb1  | 49G  | 52M  | 47G   | 1%   | /datavol       |



**4. Creating a Backup of a Block Volume**

4.1. OCI allows you to create a backup of a block volume, either scheduled or manual.

4.2. To create a full manual backup of a volume, navigate to Block Storage > Block Volumes > app\_datavol

4.3. Under Block Volume Backups, select Create Block Volume Backup.

Specify the following parameters:

**Name:** *app\_datavol\_backup\_01*

**Backup Type:** *Full*

Click Create.

4.4. The backup request will appear under Block Volume Backups.

### Block Volume Backups *in OCI\_Labs Compartment*

| Create Block Volume Backup   |             |             |                                   |             |            |                                 |
|------------------------------|-------------|-------------|-----------------------------------|-------------|------------|---------------------------------|
| Name                         | State       | Backup Type | Backup Size / Volume Size (in GB) | Source Type | Expiration | Created                         |
| <a href="#">app_backup01</a> | ● Available | Full        | 2 / 50                            | Manual      |            | Sat, Feb 20, 2021, 14:24:16 UTC |
| Showing 1 item < 1 of 1 >    |             |             |                                   |             |            |                                 |

4.5. You can also create an incremental backup as well by going through the same steps as a full backup. Simply select Incremental as the Backup Type.

Here we created an incremental backup volume, however since we did not change anything on disk, the size of the backup is similar to the full back in this case.

## Block Volume Backups in OCI\_Labs Compartment

| Create Block Volume Backup                        |           |             |                                   |             |            |                                 |
|---------------------------------------------------|-----------|-------------|-----------------------------------|-------------|------------|---------------------------------|
| Name                                              | State     | Backup Type | Backup Size / Volume Size (in GB) | Source Type | Expiration | Created                         |
| <a href="#">app_datavol_backup_incremental_01</a> | Available | Incremental | 1 / 50                            | Manual      |            | Sat, Feb 20, 2021, 14:26:34 UTC |
| <a href="#">app_backup01</a>                      | Available | Full        | 2 / 50                            | Manual      |            | Sat, Feb 20, 2021, 14:24:16 UTC |
| Showing 2 items < 1 of 1 >                        |           |             |                                   |             |            |                                 |

## 5. Restoring a Block Volume Backup

5.1. The process for restoring a block volume backup is to :

- 1) Create a new block volume from the backup directly.
- 2) Mount the new block volume on the compute instance where the data needs to be restored.

5.2. To restore from a set of backups, start with the last incremental backup. Select Create Block Volume from the last incremental backup.

## Block Volume Backups in OCI\_Labs Compartment

| Create Block Volume Backup                        |           |             |                                   |             |            |          |
|---------------------------------------------------|-----------|-------------|-----------------------------------|-------------|------------|----------|
| Name                                              | State     | Backup Type | Backup Size / Volume Size (in GB) | Source Type | Expiration | Created  |
| <a href="#">app_datavol_backup_incremental_01</a> | Available | Incremental | 1 / 50                            | Manual      |            | Sat, Feb |
| <a href="#">app_backup01</a>                      | Available | Full        | 2 / 50                            | Manual      |            | Sat, Feb |
| Showing 2 items < 1 of 1 >                        |           |             |                                   |             |            |          |

5.3. The dialog for creating a block volume will appear. Select the same parameters as the original volume, however for the name specify *restored\_app\_datavol*.

5.4. The restored block volume will appear alongside the original as shown in the OCI Console.

## Block Volumes in OCI\_Labs Compartment

Block volumes provide high-performance network storage to support a broad range of I/O intensive workloads. [Learn more](#)

Create Block Volume

| Name                                 | State     | Size  | Default Performance | Auto-tune | Current Performance | Availability Domain | Backup Policy |     |
|--------------------------------------|-----------|-------|---------------------|-----------|---------------------|---------------------|---------------|-----|
| <a href="#">restored_app_datavol</a> | Available | 50 GB | Lower Cost          | Off       | Lower Cost          | wHOZ:PHX-AD-1       | -             | \$1 |
| <a href="#">app_datavol</a>          | Available | 50 GB | Lower Cost          | Off       | Lower Cost          | wHOZ:PHX-AD-1       | -             | \$1 |
|                                      |           |       |                     |           |                     |                     |               | \$  |

### 5.5. [Optional Step]

Once the restored volume is available, you can then go through the process of attaching and mounting the volume as done earlier in the lab.

## 6. Backing up a Block Volume on a Regular Basis

6.1. OCI allows you to define a backup policy so that a block volume can be backed up on a regular basis.

To create a backup policy, navigate to Block Volumes > Block Storage > Backup Policies.

6.2. Notice Oracle provides some out-of-the-box backup policies for you to use: Gold, Silver, and Bronze. Each policy has a different set of backup schedules.

Feel free to click on any policy to view the different schedules and retention periods for each backup.

6.3. For this lab, you will create your own backup policy with two schedules to supply a daily incremental backup and one full backup per week.

Click the Create Backup Policy button and specify a name for the backup policy. Click Create.

6.4. On the backup policy page, you can define backup schedules that tell OCI when to take a backup and how long to keep it.

Click Add Schedule to define a schedule for a daily incremental backup. This schedule will retain the daily backups for 7 days.

Set the following parameters:

**Add Schedule**

Schedule Type  
☒ Daily ☐ Weekly ☐ Monthly ☐ Yearly

Hour of the day  
00:00

Retention Time In Days  
7

Backup Type  
☐ Full ☒ Incremental

Timezone  
☒ UTC ☐ Regional Data Center Time

**Add Schedule** [Cancel](#)

Click Add Schedule when finished.

6.5. Define another schedule for a weekly full backup with a retention period of 4 weeks.

**Add Schedule**

Schedule Type  
☐ Daily ☒ Weekly ☐ Monthly ☐ Yearly

Day of the week  
Monday

Hour of the day  
00:00

Retention Time In Weeks  
4

Backup Type  
☒ Full ☐ Incremental

Timezone  
☒ UTC ☐ Regional Data Center Time

**Add Schedule** [Cancel](#)

6.6. Once complete, your screen should look like this:

## Schedules

| <a href="#">Add Schedule</a> |             |                      |                |
|------------------------------|-------------|----------------------|----------------|
| Schedule Type ▲              | Backup Type | Start Time           | Retention Time |
| Daily                        | Incremental | 00:00, UTC ⓘ         | A week ⋮       |
| Weekly                       | Full        | Monday, 00:00, UTC ⓘ | 4 weeks ⋮      |
| Showing 2 Items < 1 of 1 >   |             |                      |                |

- 6.7. For the policy to work, it needs to be attached to a block volume.
- Go back to the app\_datavol details page (Block Storage > Block Volumes > app\_datavol) and click the Edit button.
- Scroll down to the bottom of the Edit page and select the backup policy you just defined.

## Edit Volume

Recommended for workloads that are throughput intensive with large sequential I/O, such as big data and streaming, log processing and data warehouses. [Learn more](#)

### AUTO-TUNE PERFORMANCE

☐ Off

Auto-tune performance changes the volume performance to lower cost when the volume is detached. When the volume is reattached, the volume performance is automatically adjusted to the previous setting. [Learn more](#)

### Backup Policies

Select Backup Policy in **OCI\_Labs** [\(Change Compartment\)](#)

app\_datavol\_backup\_policy

OCID: ...qsufca [Show](#) [Copy](#)

Number of Schedules: 2

Created: Sat, 20 Feb 2021 14:40:40 GMT

Cross Region Copy Target: None ⓘ

[Save Changes](#)

[Cancel](#)

Save changes when you are done.

The backup policy is now in effect for the block volume. This can be seen on the app\_datavol's details page.

## app\_datavol

Edit

Move Resource

Add Tags

Terminate

Block Volume Information

Tags

Availability Domain: whoz:PHX-AD-1

Compartment: techtipsondemand (root)/OCI\_Labs

OCID: ...4vaw2q [Show](#) [Copy](#)

Created: Sat, Feb 20, 2021, 13:12:36 UTC

Default Performance: Lower Cost ⓘ

Auto-tune Performance: Off ⓘ

Current Performance: Lower Cost ⓘ

Size: 50 GB ⓘ

Hydrated: true

Encryption Key: Oracle-managed key

Volume Group: None

## Scheduled Backups

Managed By: volume ⓘ

Backup Policy: [app\\_datavol\\_backup\\_policy](#) ⓘ

Cross Region Copy Target: None ⓘ

**7. Cloning a Block Volume**

- 7.1. You can clone a block volume to create an exact copy of it instantaneously. A cloned block volume is different than a backup for several reasons.
- 1) A clone is a point in time copy of a block volume.
  - 2) Cloning creates another block volume of the same size and characteristics and data. A backup takes time to perform and contains only data on the volume and is stored in object storage.
  - 3) Cloning allows you to quickly duplicate an environment to support a variety of use cases, such as troubleshooting production issues in a development environment for example.
- 7.2. To create a clone in the OCI Console, go back to the list of block volumes in the OCI Labs compartment (Navigate to Block Storage > Block Volumes).
- 7.3. Select Create Clone from the ellipsis menu for app\_datavol.
- In the clone dialog, specify cloned\_app\_datavol as the name then click Create Clone.



7.4. The cloned volume will appear in the list of volumes.

### Block Volumes in OCI\_Labs Compartment

Block volumes provide high-performance network storage to support a broad range of I/O intensive workloads. [Learn more](#)

Create Block Volume

| Name                                 | State     | Size  | Default Performance | Auto-tune | Current Performance | Availability Domain | Backup Policy                             | Created                         |   |
|--------------------------------------|-----------|-------|---------------------|-----------|---------------------|---------------------|-------------------------------------------|---------------------------------|---|
| <a href="#">cloned_app_datavol</a>   | Available | 50 GB | Lower Cost          | Off       | Lower Cost          | WHOZ:PHX-AD-1       | -                                         | Sat, Feb 20, 2021, 14:56:57 UTC | ⋮ |
| <a href="#">restored_app_datavol</a> | Available | 50 GB | Lower Cost          | Off       | Lower Cost          | WHOZ:PHX-AD-1       | -                                         | Sat, Feb 20, 2021, 14:33:08 UTC | ⋮ |
| <a href="#">app_datavol</a>          | Available | 50 GB | Lower Cost          | Off       | Lower Cost          | WHOZ:PHX-AD-1       | <a href="#">app_datavol_backup_policy</a> | Sat, Feb 20, 2021, 13:12:36 UTC | ⋮ |

Showing 3 items < 1 of 1 >

## 8. Detaching a Block Volume from a Compute Instance

8.1. Detaching a block volume is the process of removing it from a compute instance. Detaching does not delete the volume.

To detach an iSCSI-attached volume, the following steps need to be performed.

- 1) Unmount the filesystem on the OS
- 2) Run the iSCSI detach commands as provided by OCI
- 3) Detach the volume from the instance in the OCI Console

8.2. On the app1 host, unmount the file system.

```
[opc@app1 ~]$ sudo umount /datavol
[opc@app1 ~]$ df -h
Filesystem Size Used Avail Use% Mounted on
devtmpfs 315M 0 315M 0% /dev
tmpfs 345M 0 345M 0% /dev/shm
tmpfs 345M 9.3M 336M 3% /run
tmpfs 345M 0 345M 0% /sys/fs/cgroup
/dev/sda3 39G 2.9G 36G 8% /
/dev/sda1 200M 8.6M 192M 5% /boot/efi
```

|             | <pre>tmpfs          69M    0   69M    0% /run/user/0 tmpfs          69M    0   69M    0% /run/user/994 tmpfs          69M    0   69M    0% /run/user/1000</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |              |                          |             |             |       |        |         |                                                                                                                                                                  |         |  |             |          |              |                          |       |            |       |      |         |                                                                                                                                                                  |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|--------------------------|-------------|-------------|-------|--------|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|--|-------------|----------|--------------|--------------------------|-------|------------|-------|------|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 8.3.        | <p>Run the iSCSI detach commands that you saved earlier.</p> <p>If you need to get the commands again, navigate to the app1 compute instance in the OCI Console. Under Attached Block Volumes, select iSCSI Commands and Information next to app_datavol.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |              |                          |             |             |       |        |         |                                                                                                                                                                  |         |  |             |          |              |                          |       |            |       |      |         |                                                                                                                                                                  |
| 8.4.        | <p>After you have run the detach iSCSI commands on the host, go back to the OCI Console and select detach from the app_datavol menu.</p> <p><b>Attached Block Volumes</b></p> <p>Block volumes provide high-performance network storage to support a broad range of I/O intensive workloads.</p> <div><div>Attach Block Volume</div><table><thead><tr><th>Name</th><th>State</th><th>Volume Type</th><th>Device path</th><th>Type</th><th>Access</th><th>Size</th><th>AD</th><th>Created</th><th></th></tr></thead><tbody><tr><td>app_datavol</td><td>Attached</td><td>Block Volume</td><td>/dev/oracleoci/oraclevdb</td><td>iscsi</td><td>Read/Write</td><td>50 GB</td><td>AD-1</td><td>Sat, Fe</td><td><div>View Block Volume Details</div><div>iSCSI Commands &amp; Information</div><div>Copy Attachment OCID</div><div>Copy Resource OCID</div><div>Detach</div></td></tr></tbody></table></div> | Name         | State                    | Volume Type | Device path | Type  | Access | Size    | AD                                                                                                                                                               | Created |  | app_datavol | Attached | Block Volume | /dev/oracleoci/oraclevdb | iscsi | Read/Write | 50 GB | AD-1 | Sat, Fe | <div>View Block Volume Details</div> <div>iSCSI Commands &amp; Information</div> <div>Copy Attachment OCID</div> <div>Copy Resource OCID</div> <div>Detach</div> |
| Name        | State                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Volume Type  | Device path              | Type        | Access      | Size  | AD     | Created |                                                                                                                                                                  |         |  |             |          |              |                          |       |            |       |      |         |                                                                                                                                                                  |
| app_datavol | Attached                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Block Volume | /dev/oracleoci/oraclevdb | iscsi       | Read/Write  | 50 GB | AD-1   | Sat, Fe | <div>View Block Volume Details</div> <div>iSCSI Commands &amp; Information</div> <div>Copy Attachment OCID</div> <div>Copy Resource OCID</div> <div>Detach</div> |         |  |             |          |              |                          |       |            |       |      |         |                                                                                                                                                                  |
| 8.5.        | <p>Confirm that you want to detach the volume.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |              |                          |             |             |       |        |         |                                                                                                                                                                  |         |  |             |          |              |                          |       |            |       |      |         |                                                                                                                                                                  |
| 8.6.        | <p>Once the volume is detached, it will no longer appear on the list of attached volumes for app1.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |              |                          |             |             |       |        |         |                                                                                                                                                                  |         |  |             |          |              |                          |       |            |       |      |         |                                                                                                                                                                  |

## Attached Block Volumes

[Block volumes](#) provide high-performance network storage to support a broad range of I/O intensive workloads.

Attach Block Volume

| Name | State | Volume Type | Device path | Type | Access | Size |
|------|-------|-------------|-------------|------|--------|------|
|------|-------|-------------|-------------|------|--------|------|

There are no block volumes attached to this instance.

### 9. Deleting a Block Volume

9.1. Volumes can only be deleted after they have been detached from all compute instances.

Navigate to Block Volumes > Block Storage and select Terminate next to the app\_datavol volume. Confirm that you want to terminate the volume.

## Block Volumes in OCI\_Labs Compartment

Block volumes provide high-performance network storage to support a broad range of I/O intensive workloads. [Learn more](#)

Create Block Volume

| Name                                 | State     | Size  | Default Performance | Auto-tune | Current Performance | Availability Domain | Backup Policy                               | Created          |
|--------------------------------------|-----------|-------|---------------------|-----------|---------------------|---------------------|---------------------------------------------|------------------|
| <a href="#">cloned_app_datavol</a>   | Available | 50 GB | Lower Cost          | Off       | Lower Cost          | wHOZ:PHX-AD-1       | -                                           | 2020-08-26 09:04 |
| <a href="#">restored_app_datavol</a> | Available | 50 GB | Lower Cost          | Off       | Lower Cost          | wHOZ:PHX-AD-1       | -                                           | 2020-08-26 09:04 |
| <a href="#">app_datavol</a>          | Available | 50 GB | Lower Cost          | Off       | Lower Cost          | wHOZ:PHX-AD-1       | <a href="#">app_datavol_backup policy</a> ⓘ | 2020-08-26 09:04 |

View Block Volume Details  
Edit  
Create Clone  
Create Manual Backup  
Assign Master Encryption Key  
Move Resource  
Copy OCID  
View Tags  
Add Tags  
Terminate

9.2. Once the volume is terminated, it will appear as terminated in the list of volumes. A terminated volume no longer exists and does not incur any charges.

9.3. Repeat the previous steps to terminate all remaining block volumes.

## 10. Cleaning up Block Volume Backups

10.1. Remove the block volume backups that we created earlier by navigating to Block Volume Backups under Block Storage. Select Terminate next to each backup. Terminated backups are deleted and do not incur any charges.

Block Storage

Block Volumes

Block Volume Backups

Volume Groups

Volume Group Backups

Backup Policies

List Scope

Compartment

OCI\_Labs

techtipsondemand (root)/OCI\_Labs

Block Volume Backups in OCI\_Labs Compartment

| Name                                              | State      | Backup Source | Source Region     | Backup Type | Backup Size / Volume Size (in GB) | Size |
|---------------------------------------------------|------------|---------------|-------------------|-------------|-----------------------------------|------|
| <a href="#">app_datavol_backup_incremental_01</a> | Terminated | app_datavol   | US West (Phoenix) | Incremental | 1 / 50                            | M    |
| <a href="#">app_backup01</a>                      | Terminated | app_datavol   | US West (Phoenix) | Full        | 2 / 50                            | M    |

## 11. Lab Cleanup – IMPORTANT!

- 11.1.
- 1) Shutdown any running compute instances.
  - 2) Confirm all block volumes have been terminated.
  - 3) Confirm all backups have been terminated.

## Lab #5: Core OCI Object Storage

Duration 30 minutes

### Skills Learned

At the end of this exercise, you will be able to:

- Create both public and private buckets
- Store and fetch objects using a variety of tools
- Grant access to objects using PARs
- Managing access with OCI IAM Policy

## Overview

OCI Object Storage is an infinitely scalable cloud native persistent store for unstructured data, such as documents, videos, images, log files, database backups, et cetera. Object storage has many use cases from hosting static content for a website to forming a data lake for data analytics workloads.

In OCI, objects are stored in buckets which can be made either public or private. Public objects and buckets are accessible by anyone on the internet, however access to private objects and buckets requires an OCI credential and an appropriate IAM policy that grants a user or group or thing access. Access can be granted to private objects using a special OCI feature known as pre-authenticated requests, also known as a PAR. A PAR is essentially a URL that contains a one-time generated access token that grants anyone with the URL permission to access an object.

In this lab you will learn how to work with objects and buckets using your browser and the OCI command line interface or CLI.

## Instructions

| 1.   | Working with Public Objects and Buckets                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.1. | <p>In this section you will learn how to store and access public objects in a public bucket.</p> <p>A public object is one that is read-only accessible by anyone on the internet. They do not need to be an authenticated or authorized user. Each public bucket and each public object have a unique HTTP URL associated with them that can be accessed from the internet. A public bucket and a public object only allow read access though, not write.</p> <p>You still need to be logged into OCI in order to write to a bucket, regardless of its visibility.</p> <p>To get started, let's create our first bucket.</p> <p>Log into the OCI Console and navigate to Object Storage from the stacked navigation menu.</p> |
| 1.2. | <p>Under List Scope, select OCI_Labs.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| 1.3. | <p>Click the Create Bucket button and specify public1 as the bucket name. Leave all other values defaulted.</p> <p>Your screen should look similar to the screenshot below. Click Create to create the bucket.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

**Create Bucket**

Bucket Name  
public1

Default Storage Tier  
Storage tier for a bucket can only be specified during creation. Once set, you cannot change the storage tier in which a bucket resides.

☒ Standard  
☐ Archive

Object Events ⓘ  
☐ Emit Object Events

Object Versioning ⓘ  
☐ Enable Object Versioning

Encryption  
☒ Encrypt using Oracle managed keys  
Saves all encryption-related metadata to Oracle  
☐ Encrypt using customer-managed keys  
Requires a valid key from a vault that you have access to. [Learn More](#)

Tags  
Tagging is a metadata system that allows you to organize and track resources within your tenancy. Tags are composed of keys and values that can be attached to resources.  
[Learn more about tagging](#)

| Tag Namespace              | Tag Key | Value |
|----------------------------|---------|-------|
| None (add a free-form tag) |         |       |

1.4. By default, all object storage buckets are created as private. In order to change them to public, you must change their visibility in the OCI Console.

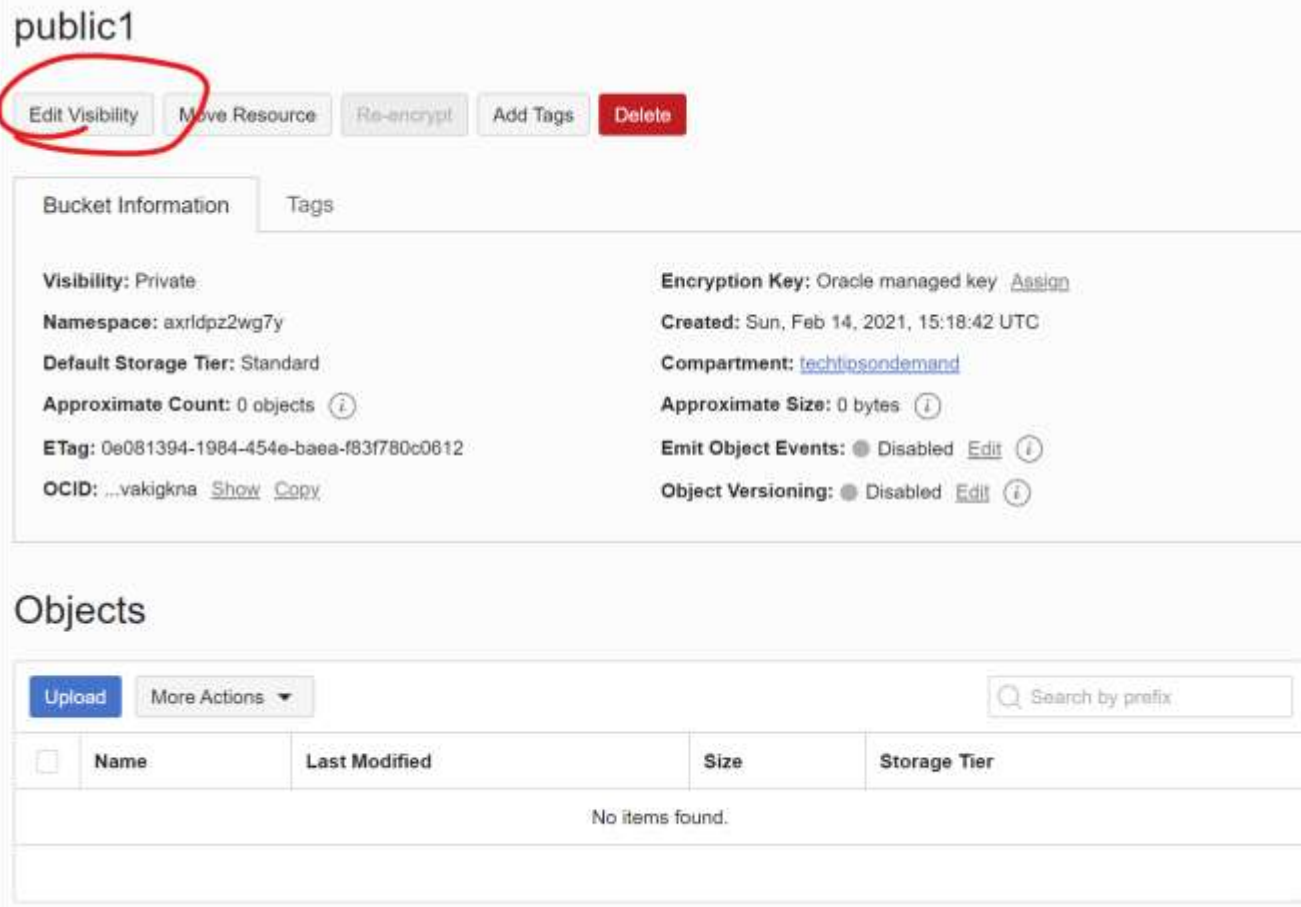
Click on the name of the bucket you just created, public1.

1.5. You will be taken to the bucket details page for public1.

To make the bucket public, click on the Edit Visibility button under the name of the bucket and select Public. This will make any objects in the bucket accessible on the internet.

You also have the option to allow users to list objects in a bucket. This may or may not be desirable depending on the use case, so let's be safe and leave this option unchecked.

Click Save Changes.



**public1**

Edit Visibility Move Resource Re-encrypt Add Tags Delete

Bucket Information Tags

Visibility: Private Encryption Key: Oracle managed key [Assign](#)

Namespace: axrldpz2wg7y Created: Sun, Feb 14, 2021, 15:18:42 UTC

Default Storage Tier: Standard Compartment: [techtipsondemand](#)

Approximate Count: 0 objects [i](#) Approximate Size: 0 bytes [i](#)

ETag: 0e081394-1984-454e-baaa-f83f780c0612 Emit Object Events: ☒ Disabled [Edit](#) [i](#)

OCID: ...vakigkna [Show](#) [Copy](#) Object Versioning: ☒ Disabled [Edit](#) [i](#)

### Objects

Upload More Actions [Search by prefix](#)

| <input type="checkbox"/> | Name | Last Modified | Size | Storage Tier |
|--------------------------|------|---------------|------|--------------|
| No items found.          |      |               |      |              |

- 1.6. You should now see the visibility status has changed from Private to Public on the bucket details page. OCI displays a little warning icon letting you know that the bucket is public.
- 1.7. With the bucket created, you can now upload an object to the bucket right from the OCI Console.
- On the bucket details page, click the Upload button. Select any file you wish to upload to the bucket.



## public1

Edit Visibility
Move Resource
Re-encrypt
Add Tags
Delete

### Bucket Information

### Tags

**Visibility:** Public

**Namespace:** axrldpz2wg7y

**Default Storage Tier:** Standard

**Approximate Count:** 0 objects

**ETag:** edf72e01-89b3-4c96-916c-f4309cbcacb9

**OCID:** ...vakigkna Show Copy

**Encryption Key:** Oracle managed key Assign

**Created:** Sun, Feb 14, 2021, 15:18:42 UTC

**Compartment:** techtipsondemand

**Approximate Size:** 0 bytes

**Emit Object Events:** Disabled Edit

**Object Versioning:** Disabled Edit

## Objects

Upload

More Actions ▼

Search by prefix

| Name           | Last Modified                   | Size       | Storage Tier |  |
|----------------|---------------------------------|------------|--------------|--|
| Split Rail.jpg | Sun, Feb 14, 2021, 15:29:55 UTC | 298.84 KiB | Standard     |  |

1.8. After the file is uploaded, it will appear in the list of objects for the bucket.

## public1

Edit Visibility

Move Resource

Re-encrypt

Add Tags

Delete

## Bucket Information

## Tags

Visibility:  Public

Namespace: axrldpz2wg7y




Default Storage Tier: Standard

Approximate Count: 0 objects 

ETag: edf72e01-89b3-4c96-916c-f4309cbcacb9


OCID: ...vakigkna [Show](#) [Copy](#)Encryption Key: Oracle managed key [Assign](#)


Created: Sun, Feb 14, 2021, 15:18:42 UTC

Compartment: [techtipsondemand](#)Approximate Size: 0 bytes Emit Object Events:  Disabled [Edit](#) Object Versioning:  Disabled [Edit](#) 

## Objects

Upload

More Actions  Search by prefix

| <input type="checkbox"/> | Name                                    | Last Modified                   | Size       | Storage Tier |                                                                                     |
|--------------------------|-----------------------------------------|---------------------------------|------------|--------------|-------------------------------------------------------------------------------------|
| <input type="checkbox"/> | <input type="checkbox"/> Split Rail.jpg | Sun, Feb 14, 2021, 15:29:55 UTC | 298.84 KiB | Standard     |  |

1.9. The file you uploaded now exists on the public internet and is represented by a URL.

To get the URL of the object, click the three dots (ellipsis) next to the object. A menu will appear.

Select View Object Details from the menu. You will see some basic information about the object, including a URL.

Try copying and pasting the URL in another browser window.

Public object storage is a great way to host static website assets such as images and videos. This is just one use case of course.

|           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.10.     | Let's delete the object now by clicking on the ellipsis and selecting Delete. Confirm the object was delete and the URL is no longer valid.                                                                                                                                                                                                                                                                                                                              |
| <b>2.</b> | <b>Working with Private Buckets and Objects</b>                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 2.1.      | <p>Now you will work with a private bucket and objects.</p> <p>Create another bucket by clicking the Create Bucket button.</p> <p>Specify the following information for the bucket:</p> <p><b>Bucket Name:</b> private1<br/> <b>Default Storage Tier:</b> Standard (Default)</p> <p>Click the Create Button to provision the bucket.</p>                                                                                                                                 |
| 2.2.      | <p>On the Objects screen you will see a table listing all the objects in the bucket, which should be empty since you just created the bucket.</p> <p>Click the Upload button and upload any type of file you wish.</p> <p>Since the bucket is private, all objects within the bucket are private by default which means only authenticated OCI users with the proper authorization (you) have access to objects in the bucket.</p>                                       |
| 2.3.      | After the file is uploaded, you will see it appear in the list of objects.                                                                                                                                                                                                                                                                                                                                                                                               |
| 2.4.      | <p>Because the object was uploaded to a private bucket, it is no accessible on the internet. Users will need to be logged into OCI and granted access to bucket or object explicitly.</p> <p>To verify the object is indeed private, get the URL for the object by viewing the object details just like we did with the public object.</p> <p>Try accessing the URL. You should receive an error message that the bucket doesn't exist or you don't have permission.</p> |
| 2.5.      | <p>You can download objects from within the OCI Console using a browser by selecting Download from the ellipsis menu next to the object.</p> <p>Go ahead and give it a try.</p>                                                                                                                                                                                                                                                                                          |
| 2.6.      | <p>Delete the object by going to the ellipsis menu for the object and selecting Delete.</p> <p>The object will be removed from the bucket.</p>                                                                                                                                                                                                                                                                                                                           |

### 3. Using the OCI CLI with Object Storage

3.1. Up to now we have used the OCI Console exclusively to interact with OCI services. While the console is great tool, it is not as powerful nor as flexible as using the OCI tools, APIs, and CLI to manage our cloud infrastructure.

In this section you will use the OCI command line interface to work with OCI object storage.

There are two options for install the CLI. You can go the easy route and use OCI's Cloud Shell, which is a terminal window in the cloud that has all the tools already installed configured to use your OCI credentials. This option is most suitable for a learning or demo environment.

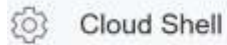
The other option is to install the OCI CLI on your machine, which is a more involved process, requiring you to download and install the tools, along with configuring the tools to use an OCI authentication token; but is the preferred method for supporting development and production environments in OCI.

In this lab guide, we will use Cloud Shell to run the CLI.

3.2. To use the OCI CLI already installed in the Cloud Shell, simply launch the Cloud Shell by selecting the Terminal icon located in the upper right portion of the OCI Console.



A terminal window will appear in your browser window.



```
chris@cloudshell:~ (us-phoenix-1)$
```

3.3. You can verify the OCI CLI is installed by running the oci command with no arguments.

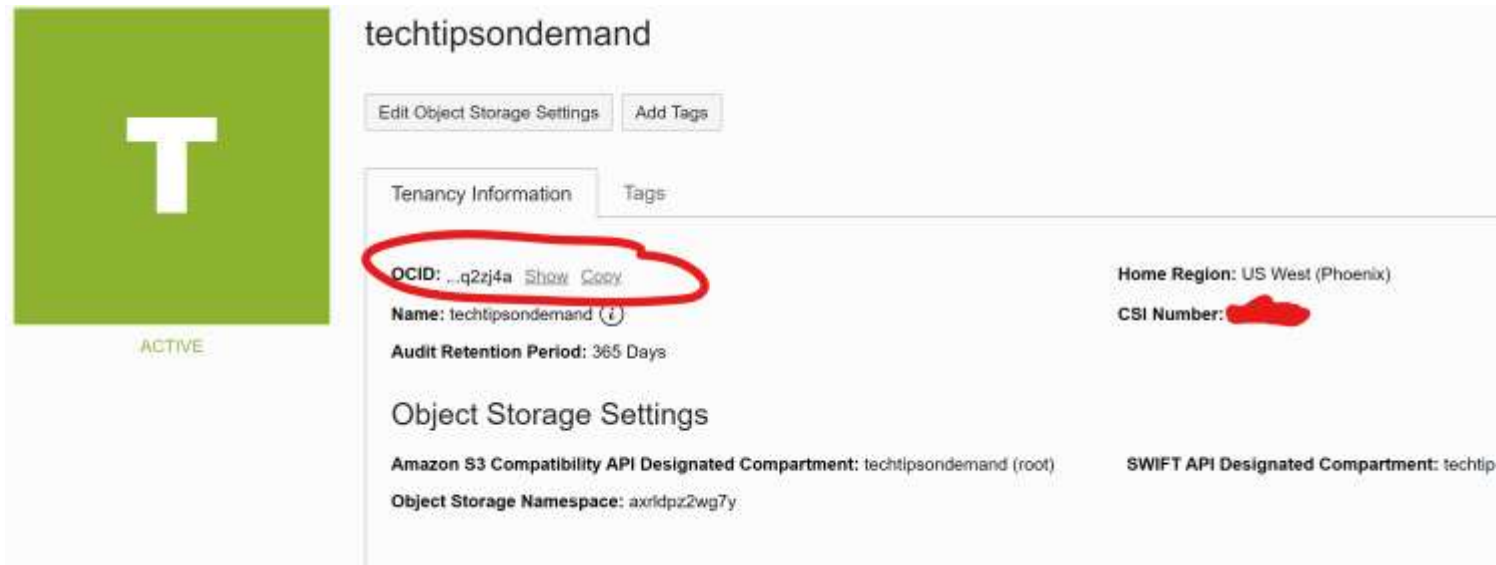
```
$ oci
```

## 4. Managing Buckets with the OCI CLI

4.1. To use the OCI CLI, we first need to get the OCID or identifier for our tenancy. Each tenancy has a globally unique OCID.

To get the OCID for your tenancy, click on the Profile icon in the OCI Console then click on the name of your tenancy.

The OCID for the tenancy will appear on the Tenancy Details page in the Tenancy Information box. Click on either Show or Copy next to the OCID value. Save the OCID somewhere on your computer as we will be using this throughout the rest of this lab guide.



4.2. Run the following command to create a private bucket named bucket2:

```
$ oci os bucket create --name bucket2 --compartment-id <Put your tenancy OCID here>
```

4.3. You can verify the bucket was created by using the OCI CLI to list all buckets in a compartment. The OCI CLI will return json formatted results.

```
$ oci os bucket list --compartment-id <Your Tenancy or Compartment OCID>
```

## 5. Working with Objects using the OCI CLI

5.1. In this section you will store an object in a bucket using the CLI.

If you are using Cloud Shell or any other Linux environment, create a simple text file.

```
$ echo "This is my simple text file" >> object.txt
```

5.2. Upload the text file to object storage using the following command:

```
$ oci os object put --bucket-name bucket2 --file object.txt
```

|           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 5.3.      | <p>You can verify the object was stored in the bucket by listing the contents of the bucket.</p> <pre>\$ oci os object list --bucket-name <i>bucket2</i></pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| 5.4.      | <p>Here is the command to download an object.</p> <pre>\$ oci os object get --bucket-name <i>bucket2</i> --object <i>object.txt</i> --file <i>object2.txt</i></pre> <p>The <code>--file</code> parameter tells OCI where to store the downloaded object on your filesystem.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| 5.5.      | <p>To delete an object:</p> <pre>\$ oci os object delete --bucket-name <i>bucket2</i> --object <i>object.txt</i></pre> <p>The OCI CLI will prompt you to confirm deletion of the object.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>6.</b> | <b>Working with Pre-Authenticated Requests</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| 6.1.      | <p>A PAR is a generated URL that allows anyone with the URL to access a private object. The generated URL serves as a secret access token in a way, so the generation and storage of a PAR should be a protected operation.</p> <p>PARs are commonly used when you want to share protected information with a client or customer that does not have an account in your OCI tenancy. It is a best practice in this case to generate a PAR that has a short lifespan and securely hand that URL to the end user.</p> <p>In this section you will generate a PAR URL for an object. The PAR will grant access to the file to anyone with the URL. You are going to configure the PAR to provide READ-ONLY access and for it to expire after a few minutes.</p> |
| 6.2.      | Use the OCI Console to upload a file to the bucket you created earlier.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| 6.3.      | Create a PAR by selecting the ellipsis next to the file you just uploaded then Create Pre-Authenticated Request.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| 6.4.      | <p>The options for creating a PAR are fairly simple. You can create a PAR for a bucket or a file.</p> <p>In this tutorial, configure the PAR to permit read-only access on the object.</p> <p>Also configure the PAR to expire after 10 minutes. This forces the PAR to be no longer valid after a certain period of time – a best practice for giving external users temporary access to files!</p>                                                                                                                                                                                                                                                                                                                                                        |

**Create Pre-Authenticated Request** [Help](#)

Name  
par-object-Split Rail.jpg-20210210-0621

Pre-Authenticated Request Target

☐ Bucket  
You can only use the pre-authenticated request URL to create objects in this bucket. You cannot read from or list the objects in this bucket.

☒ Object

Object Name  
Split Rail.jpg

Access Type

☒ Permit reads on the object

☐ Permit writes to the object

☐ Permit reads on and writes to the object

Expiration  
Feb 17, 2021 13:21 UTC

[Create Pre-Authenticated Request](#) [Cancel](#)

- 6.5. After you click Create Pre-Authenticated Request, the PAR URL will be displayed on the screen only once. Be sure to copy this URL down somewhere safe since you will not be able to retrieve it from OCI again.

If you lose your PAR URL, you can always generate a new one in the OCI console.

**Pre-Authenticated Request Details**

Name Read-Only  
par-object-Split Rail.jpg-20210210-0621

Pre-Authenticated Request URL Read-Only  
[https://objectstorage.us-phoenix-1.oraclecloud.com/p/rEXC20xu/CqisL-K5EN\\_xuLNF8-Q41r4dUY0rAu1pcccbOSvx94ERyjbVXF\\_vcin/axrldpz2wg7y/b/privatebucket1/o/Split%20Rail.jpg](https://objectstorage.us-phoenix-1.oraclecloud.com/p/rEXC20xu/CqisL-K5EN_xuLNF8-Q41r4dUY0rAu1pcccbOSvx94ERyjbVXF_vcin/axrldpz2wg7y/b/privatebucket1/o/Split%20Rail.jpg)

Copy this URL for your records. It will not be shown again.

[Close](#)

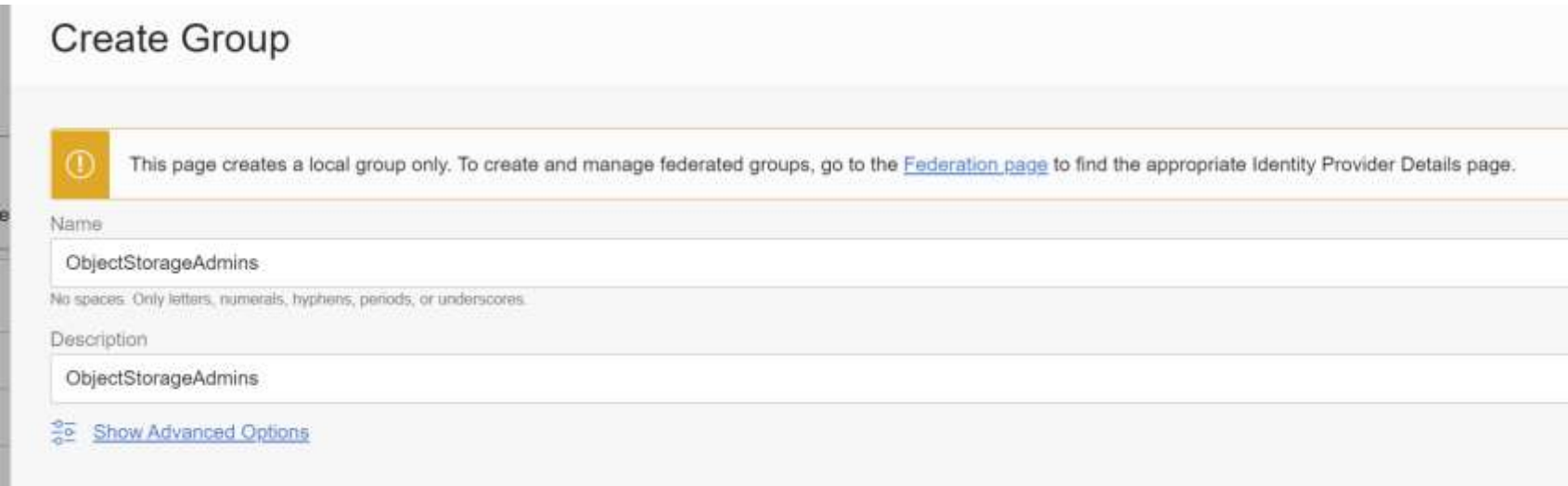
- 6.6. Close the PAR dialog after you have saved your PAR URL.
- Now navigate to the PAR URL using your browser and the object you upload should appear, depending on the type of object.



|           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 6.7.      | <p>Back in the OCI Console, you can see an inventory of PARs by going to Object Storage &gt; bucket2 &gt; Pre-Authenticated Requests.</p> <p>Here in this table you will see a list of PARs and whether they are expired or active. If it has been 10 minutes since you created the PAR, it should show as expired by now.</p>                                                                                                                                                                                                                                            |
| 6.8.      | If the PAR is not expired by now, go ahead and expire it by selecting the ellipsis next to the PAR.                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| 6.9.      | After the PAR is expired, try accessing the PAR URL again from your browser. You should receive an error message that either the bucket does not exist or you are not authorized to access it.                                                                                                                                                                                                                                                                                                                                                                            |
| <b>7.</b> | <b>Working with PARs using curl</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| 7.1.      | <p>Curl is a command line URL utility that allows you to issue different types of HTTP requests such as GET and POST. Think of curl as a very flexible and powerful command line HTTP client that lets you call any HTTP endpoint (Websites,</p> <p>In this section you will use curl to download and upload objects using a PAR url.</p>                                                                                                                                                                                                                                 |
| 7.2.      | <p>Curl is already installed in the Cloud Shell environment, however if you want to install curl in your own environment there are hundreds of articles on the internet that detail the procedure so it will not be covered here in this lab. For most linux systems, it's a simple one line command.</p> <p>Depending on your Linux distribution:</p> <p>For Debian-based distros, including Ubuntu:</p> <pre>\$ apt-get install curl</pre> <p>For RHEL-based distros:</p> <pre>\$ yum install curl</pre> <p>Curl comes with Windows and is available in Powershell.</p> |
| 7.3.      | <p>In the OCI Console, create a PAR for bucket2 – this will allow someone with the URL to upload objects to a bucket. A bucket PAR only allows writes to a bucket, it does not allow read. So someone with the URL will not be able to list objects in a bucket.</p> <p>To create a PAR for a bucket, navigate to Object Storage in the navigation menu and click on the bucket name – in this case bucket2.</p>                                                                                                                                                          |
| 7.4.      | Under Resources click on Pre-Authenticated Requests then click the button Create Pre-Authenticated Request.                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

|      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| 7.5. | <p>In the dialog that appears, make sure Bucket is selected for Pre-Authenticated Request Target. Leave all other values default.</p> <p>Click Create Pre-Authenticated Request and save the generated URL.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| 7.6. | <p>The syntax to upload a file to object storage using a PAR URL is:</p> <pre>\$ curl -X PUT --data-binary '@&lt;local-filename&gt;' &lt;unique-PAR-URL&gt;/&lt;target_objectname&gt;</pre> <p>Take note that you must append the name of the object after the PAR URL. Unlike using the OCI CLI where you explicitly specify the bucket and have to be an authenticated OCI user, a PAR URL combines both bucket and authorization to access the bucket in the URL.</p> <p>Use the curl command above to upload any file to object storage using the PAR you generated.</p> <p>Here is an example uploading the object.txt file created earlier.</p> <pre>\$ curl -X PUT -data-binary '@object.txt' https://objectstorage.us-phoenix-1.oraclecloud.com/p/vt4YH9HZ1BmgMLgHqD7wCCWvOCIJ9-AhHoSIC-UPzBn8Sbte4MtkQYUNjBgBcCY4/n/axrldpz2wg7y/b/bucket2/o/object.txt</pre> |
| 7.7. | <p>The PAR that you generated only permits a user to write objects to the bucket. If you want to share access to the object using a PAR, you must create a PAR just for that object.</p> <p>Back in the OCI Console, navigate to bucket2 to see a list of objects in the bucket. You should see the object that you just uploaded using curl.</p> <p>To create a PAR for the object, select Create Pre-Authenticated Request from the ellipsis menu next to the object.</p>                                                                                                                                                                                                                                                                                                                                                                                            |
| 7.8. | <p>In the PAR dialog, you can choose what type of access to allow on the object, either read, write, or both. Select read and write then create the request. Be sure to save the PAR URL.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 7.9. | <p>Back on the command line, use curl to fetch the object using the PAR for the object. The curl command below is equivalent to putting the URL in your browser address bar.</p> <pre>\$ curl -X GET https://objectstorage.us-phoenix-1.oraclecloud.com/p/7cn6JIHk5RjqEK15iRTxQ51urx5pze2iKyiwYKp8tc6K94xVozm9EoLz4UC5nppy/n/axrldpz2</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

|           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|           | <code>wg7y/b/bucket2/o/object.txt</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| 7.10.     | <p>The PAR for the object also allows writes. Make a change to <code>object.txt</code> on your local file system and upload it back to object storage using the same PAR.</p> <pre>\$ curl -X PUT -data-binary '@object.txt' https://objectstorage.us-phoenix-1.oraclecloud.com/p/7cn6JIHk5RjqEKl5iRTxQ51urx5pze2iKyiwyKp8tc6K94xVozm9EoLz4UC5nppy/n/axrldpz2wg7y/b/bucket2/o/object.txt</pre>                                                                                                                                                                             |
| <b>8.</b> | <b>Granting Users and Groups Access to Object Storage</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 8.1.      | <p>In this section you will be introduced to how OCI handles identity and access management within a tenancy. OCI provides a robust policy-based authorization model that allows an administrator to author policies in natural language that permit users or groups access to OCI resources.</p> <p>In this section you will write an IAM policy that lets a group of users manage an object storage bucket and another group to only read and write objects in the bucket.</p>                                                                                           |
| 8.2.      | <p>For this scenario you are going to create two local OCI Groups: <code>ObjectStorageAdmins</code> and <code>ObjectStorageUsers</code>. The storage admins will be responsible for creating and managing buckets in an OCI compartment. Recall an OCI compartment is a logical construct that is used for organizing and manage OCI resources.</p> <p>The storage users will be able to read and write to the object storage buckets only in the OCI compartment.</p> <p>In the OCI Console, select the stacked navigation bars and navigate to Identity &gt; Groups.</p> |
| 8.3.      | <p>Create a group called <code>ObjectStorageAdmins</code> by selecting the Create Group button.</p> <p>On the Create Group dialog, specify the name of the group and a description (it's required).</p>                                                                                                                                                                                                                                                                                                                                                                    |

|      |                                                                                                                                                                                                                                                           |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      |                                                                                                                                                                         |
| 8.4. | Create another group called ObjectStorageUsers.                                                                                                                                                                                                           |
| 8.5. | <p>In this scenario you are going to only allow the object storage admins and users to work with buckets and objects in a dedicated OCI compartment.</p> <p>Navigate to Identity &gt; Compartments. Select the OCI_Labs compartment under List Scope.</p> |
| 8.6. | Create a new compartment called ObjectStorageLab under the OCI_Labs compartment by clicking on the Create Compartment button.                                                                                                                             |
| 8.7. | <p>Next you are going to write an IAM policy that allows the ObjectStorageAdmins to create and manage buckets and objects in the ObjectStorageLab compartment.</p> <p>Navigate to Identity &gt; Policies.</p>                                             |
| 8.8. | <p>Click Create Policy and fill in the following values:</p> <p><b>Name:</b> <i>ObjectStorageLabPolicy</i></p> <p><b>Description:</b> <i>Same as Name</i></p> <p><b>Compartment:</b> <i>root</i></p>                                                      |

Use the Policy Builder to quickly select from pre-defined commonly used policies.

**Policy Use Cases:** *Storage Management*

**Common Policy Templates:** *Let Object Storage admins manage buckets and objects.*

**Under Groups,** select the *ObjectStorageAdmins* group.

**Under Location,** select the *ObjectStorageLab* compartment.

As you select options, you will see the actual Policy Statement being generated at the bottom of the dialog. Notice the two statements, one that allows the admin group to manage buckets in the compartment, and the another that allows the admin group to manage objects in the compartment. The verb manage is special in that it allows the highest level of access for the resource being secured.

There are other verbs like inspect and use which will see shortly.

Your screen should look similar to the screenshot below. Click the Create button once you are done.

---

## Create Policy

[Help](#)

Name

ObjectStorageLabPolicy



No spaces. Only letters, numerals, hyphens, periods, or underscores.

Description

ObjectStorageLabPolicy

Compartment

techtipsondemand (root)



### Policy Builder

[Customize \(Advanced\)](#)

#### Policy Options

Policy use cases

Storage Management



Common policy templates

Let Object Storage admins manage buckets and objects



#### Let Object Storage admins manage buckets and objects

Ability to do all things with Object Storage buckets and objects in the selected compartments.

Groups

ObjectStorageAdmins



Location

ObjectStorageLab



#### Policy Statements

Allow **ObjectStorageAdmins** to manage buckets in compartment **ObjectStorageLab**Allow **ObjectStorageAdmins** to manage objects in compartment **ObjectStorageLab** [Show Advanced Options](#)

8.9. Next you will author a set of policies to allow users to manage objects in a compartment. The storage users group will not have permission to manage buckets, just objects.

This time you are going to author the policy directly without using the policy builder.

|       |                                                                                                                                                                                                 |
|-------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       | Under Identity > Policies, click on the ObjectStorageLabPolicy you just created.                                                                                                                |
| 8.10. | Select Edit Policy Statements.                                                                                                                                                                  |
| 8.11. | On the Edit Policy Statements screen, click Add Another Statement and enter the following statement:<br><i>Allow group ObjectStorageUsers to manage objects in compartment ObjectStorageLab</i> |
| 8.12. | Add another statement to let the users view buckets in a compartment.<br><i>Allow group ObjectStorageUsers to read buckets in compartment ObjectStorageLab</i>                                  |
| 8.13. | When are you done adding the statements, click the Save Changes button.<br>Your policy should now consist of the four statements:                                                               |

## ObjectStorageLabPolicy

[Edit Policy](#)[Add Tags](#)[Delete](#)[Policy Information](#)[Tags](#)

**OCID:** ...c6zopsdq [Show](#) [Copy](#)

**Compartment:** techtipsondemand (root)

**Description:** ObjectStorageLabPolicy

**Created:** Sun, Feb 14, 2021, 14:02:20 UTC

## Statements

[Edit Policy Statements](#)

Allow group ObjectStorageAdmins to manage buckets in compartment ObjectStorageLab

Allow group ObjectStorageAdmins to manage objects in compartment ObjectStorageLab

Allow group ObjectStorageUsers to manage objects in compartment ObjectStorageLab

Allow group ObjectStorageUsers to read buckets in compartment ObjectStorageLab

8.14. Now in order for us to test to see if our policies work as they should, we need to create some users.

First we will create a storage admin user.

Under Identity > User, click Create User and fill in the following details:



|       |                                                                                                                                                                                                                                                                                       |
|-------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       | <p><b>Name:</b> <i>objectstorage_admin</i></p> <p><b>Description</b> <i>object_storage_admin</i></p> <p>Leave email blank and click the Create button.</p>                                                                                                                            |
| 8.15. | <p>On the User Details page for the admin user, set a password for this user by selecting the Create/Reset Password button.</p> <p>You will be shown a one-time password for the user. Be sure to copy this down somewhere. This OTP will be reset upon first login.</p>              |
| 8.16. | <p>With the user created, you can now add the user to the storage admin group.</p> <p>On the User Details page, click the Add User to Group button and select the ObjectStorageAdminGroup from the list.</p> <p>The User Details page will list what groups this user is part of.</p> |

## objectstorage\_admin

objectstorage\_admin

Edit User

Create/Reset Password

Enable Multi-Factor Authentication

Edit User Capabilities

More Actions ▾

### User Information

### Tags

**OCID:** ...yqb2fa [Show](#) [Copy](#)**Federated:** No**Created:** Sun, Feb 14, 2021, 14:28:27 UTC**My Oracle Support account:** -**Multi-factor authentication:** Disabled**Email:** -

### Capabilities

**Local password:** Yes**SMTP credentials:** Yes**API keys:** Yes**Customer secret keys:** Yes**Auth tokens:** Yes

## Groups

Add User to Group

Remove

| <input type="checkbox"/> | Group Name ▲        | Status                        | Description         |   |
|--------------------------|---------------------|-------------------------------|---------------------|---|
| <input type="checkbox"/> | ObjectStorageAdmins | ● Active                      | ObjectStorageAdmins | ⋮ |
| 0 Selected               |                     | Displaying 1 Group < 1 of 1 > |                     |   |

- 8.17. Repeat the above steps to create another user called objectstorage\_user. Set a password as before and add the user to the objectstorage\_user group.

## objectstorage\_user

objectstorage\_user

Edit User Create/Reset Password Enable Multi-Factor Authentication Edit User Capabilities More Actions ▾

User Information

Tags

**OCID:** ...xhwwxa [Show](#) [Copy](#)

**Created:** Sun, Feb 14, 2021, 14:39:27 UTC

**Multi-factor authentication:** Disabled

**Email:** -

**Federated:** No

**My Oracle Support account:** -

### Capabilities

**Local password:** Yes

**API keys:** Yes

**Auth tokens:** Yes

**SMTP credentials:** Yes

**Customer secret keys:** Yes

## Groups

Add User to Group

Remove


| <input type="checkbox"/> | Group Name         | Status   | Description        |
|--------------------------|--------------------|----------|--------------------|
| <input type="checkbox"/> | ObjectStorageUsers | ● Active | ObjectStorageUsers |

0 Selected

Displaying 1 Group < 1 of 1 >

8.18. With both our users and our policies set up you can now test that everything works. Here are the steps.

1. Log in to the OCI Console as the storage admin user and set a new password.
2. Create an object storage bucket in the new compartment

|       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       | <ol style="list-style-type: none"> <li>Log in as the storage user and set a new password.</li> <li>Read and write objects to the new bucket.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| 8.19. | Log out of the OCI Console and log back in as the objectstorage_admin user using the OCI Direct Sign form (not Single Sign On). You will be asked to set a new password.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| 8.20. | Navigate to Object Storage from the main navigation menu.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| 8.21. | <p>By default you are working in the root compartment. You should see an authorization error since the objectstorage_admin user has not been granted any access in the root compartment.</p> <p>Select the ObjectStorageLab compartment under List Scope to change compartments. The authorization error should disappear.</p>                                                                                                                                                                                                                                                                                                                                                                                                       |
| 8.22. | <p>Create a new object storage bucket, keeping all the default values.</p> <p>After the bucket is created, your screen should look like this:</p>  <p>The screenshot shows the OCI Object Storage console interface. On the left, there's a navigation menu with 'Object Storage' selected. Below it, 'List Scope' is set to 'ObjectStorageLab'. The main area is titled 'Buckets in ObjectStorageLab Compartment' and shows a table with one bucket: 'bucket-20210214-0747'. The table columns are Name, Default Storage Tier, Visibility, and Created. The bucket is Standard, Private, and was created on Sun, Feb 14, 2021, 14:47:57 UTC.</p> |
| 8.23. | <p>Next you will log in as the object storage user and try to write to the bucket.</p> <p>Log back into the OCI Console as objectstoage_user. Again you will have to set a new password since this is the first time logging in as this user.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| 8.24. | Navigate to Object Storage and select the ObjectStorageLab compartment.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

|           |                                                                                                                                                                                                                                                                                                                                          |
|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|           | You should see the bucket that was just created by the admin user.                                                                                                                                                                                                                                                                       |
| 8.25.     | <p>First verify that the storage user is not able to delete the bucket. Recall we only gave the regular user the ability to read buckets in the compartment, not delete.</p> <p>Try deleting the bucket by selecting the ellipsis next to the bucket name. The option will be visible but you should receive an authorization error.</p> |
| 8.26.     | Next verify that this user can upload objects to the bucket by clicking on the bucket name and then the Upload button. Upload any file you wish.                                                                                                                                                                                         |
| 8.27.     | Verify the user can also delete objects in the bucket as well.                                                                                                                                                                                                                                                                           |
| <b>9.</b> | <b>Lab Cleanup</b>                                                                                                                                                                                                                                                                                                                       |
| 9.1.      | <p>Perform the following steps to clean up your lab environment:</p> <ol style="list-style-type: none"><li>1) Delete all objects that were created as part of this lab</li><li>2) Stop any running compute instances.</li></ol>                                                                                                          |

## Conclusion

In this lab you were introduced to core object storage concepts buckets, objects, PARs and IAM policies. You used a variety of tools for working with object storage, including the OCI Console, OCI CLI, and curl to create buckets and objects both public and private. We saw how to grant access to objects using PARs for anonymous users, and how to use IAM policies and groups to grant users of our tenancy access to buckets and objects.

## Lab #6:

## Lab #7: Core OCI Load Balancer

---

*Duration 1 hour*

### Skills Learned

At the end of this exercise, you will be able to:

- Provision different types of load balancers and listeners
- Manage backend sets
- Enable SSL
- Enable and view access and error logs

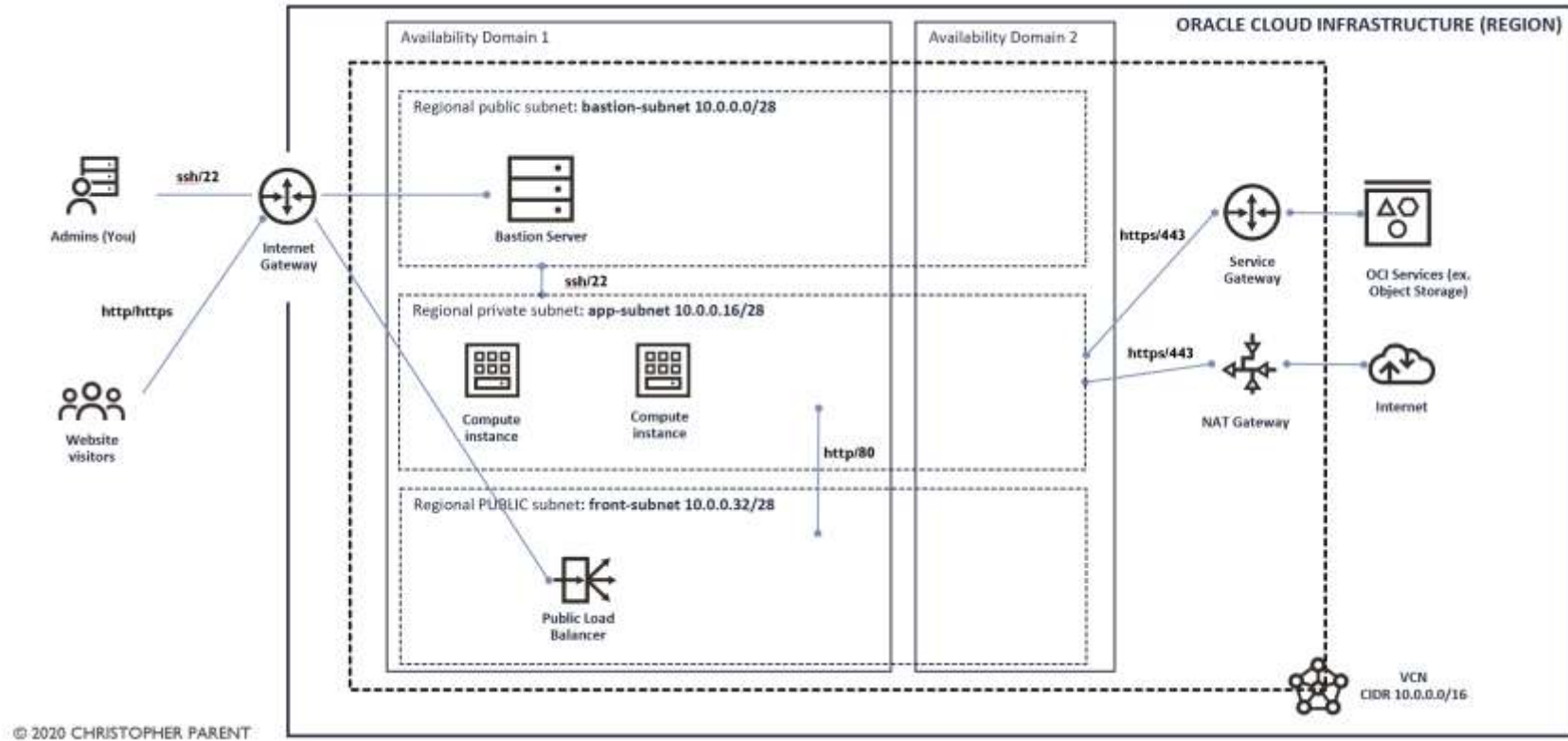
### Overview

A load balancer is typically used to provide high availability for an application or service that is deployed across two or more servers by distributing requests using an algorithm. A load balancer is configured to manage requests for a service across a pool of servers known as a backend set in OCI. The load balancer is intelligent to know which servers are healthy and which are unhealthy using a health check system that involves polling each backend compute instance.

If the load balancer detects one of the servers in a backend set is unhealthy, then it will mark it as such and not forward any requests to it, so the client or user never gets sent to a bad server. When the load balancer detects the server is healthy again, its status is updated and can start receiving requests again.

In this lab you will configure a load balancer to provide high availability and SSL for a simple website running on two compute instances.

Below is a picture showing what our VCN will look like when we are done. We will add an additional compute instance in app-subnet to provide a two-node web server setup. A load balancer will be deployed in a new public subnet and will be configured to handle http and https requests for our website.



## Instructions

|      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.   | <b>Setting up a 2-Node Apache Cluster</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| 1.1. | <p><b>WARNING:</b><br/> <i>Setting up a 2 node cluster requires provisioning another compute instance which is not part of the Always Free Tier. If you proceed with creating another compute instance you will certainly incur charges. You can minimize these charges by only running the instance for the duration of the lab and then immediately stopping it after the lab. In this section we are going to set up a website using Apache running on two compute instances.</i></p> <p>We will use the app1 compute instance we created previously in addition to a new instance we will create right now.</p> |

|      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      | <p><b>Create a new private compute instance called app2 in the same compartment and private subnet as app1.</b></p> <p>Use the same Oracle Linux image as you did with app1.</p> <p>Select the smallest compute shape available to keep costs down. Since you will have reached the service limits for the Always Free tier, pick the smallest compute shape available.</p> <p>For convenience use the same SSH key as you did with app1.</p>                                                                                                                                                             |
| 1.2. | <p>The next step is to install Apache on each server.</p> <p>SSH into app1 through the bastion and run the following commands to install and enable Apache</p> <pre>\$ sudo dnf install httpd \$ sudo systemctl enable --now httpd.service</pre> <p>Run the following commands to open up port 80 on app1.</p> <pre>\$ sudo firewall-cmd --add-service=http --permanent \$ sudo firewall-cmd --reload</pre> <p>It is important to note that every Oracle Linux image comes with a host-based firewall enabled. So in addition to using security lists, you must also enable ports on the host itself.</p> |
| 1.3. | <p>Verify Apache is up and running by executing curl on the host.</p> <pre>\$ curl -L <a href="http://localhost">http://localhost</a></pre> <p>The Apache default page should be returned in the response.</p>                                                                                                                                                                                                                                                                                                                                                                                            |
| 1.4. | <p>For this lab we want to create our own custom web page and not use the default page that comes with Apache. We are going to create a very simple index.html.</p> <pre>\$ sudo su \$ echo "Hello welcome to \$HOSTNAME " &gt; /var/www/html/index.html</pre>                                                                                                                                                                                                                                                                                                                                            |
| 1.5. | <p>Run the curl command again and verify the new html page is returned instead of the default page. The hostname should</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |



|           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|           | also appear on the page.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| 1.6.      | Repeat the previous steps to setup Apache on app2 with the same index.html page and configure the firewall to allow http/80.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>2.</b> | <b>Preparing the Network</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| 2.1.      | <p>In this lab you are going to create a public load balancer – one that has a public IP address and is accessible on the public internet. Visitors will access the website using the LB's public IP address. Before we create a load balancer, we need a place to put it.</p> <p>The diagram at the beginning of this lab shows the public load balancer being provisioned in a new public subnet that is called front-subnet.</p> <p>Log into the OCI Console and create the new public subnet with the following parameters:</p> <p><b>Name:</b> front-subnet<br/><b>Type:</b> regional<br/><b>Compartment:</b> OCI_Labs<br/><b>CIDR:</b> 10.0.0.32/28<br/><b>Route table:</b> Default Route Table for vcn_oci_labs<br/><b>Subnet access:</b> Public<br/><b>Security List:</b> Leave blank – we will create a new one next.</p> |

Networking » Virtual Cloud Networks » vcn\_oci\_labs » Subnet Details

## front-subnet

Edit Move Resource Add Tags Terminate

**Subnet Information** Tags

OCID: ...msylvq [Show](#) [Copy](#) Compartment: OCI\_Labs  
 CIDR Block: 10.0.0.32/28 DNS Domain Name: frontsubnet... [Show](#) [Copy](#)  
 Virtual Router Mac Address: 00:00:17:65:01:6F Subnet Access: Public Subnet  
 Subnet Type: Regional DHCP Options: [Default DHCP Options for vcn\\_oci\\_labs](#)  
 Route Table: [Default Route Table for vcn\\_oci\\_labs](#)

**Resources**

Security Lists (1)

Logs

Tag Filters [add](#) | [clear](#)

no tag filters applied

## Security Lists

Add Security List

| Name                              | State     | Compartment | Created                         |
|-----------------------------------|-----------|-------------|---------------------------------|
| <a href="#">Public_LB_SecList</a> | Available | OCI_Labs    | Mon, Feb 22, 2021, 01:21:45 UTC |

Showing 1 item < 1 of 1 >

2.2. We need some new security rules to allow HTTP into the load balancer on port 80 and another rule to allow HTTP traffic to leave the load balancer and hit the web servers app1 and app2.

The first rule will allow HTTP on port 80 in to the load balancer's subnet. The second rule will allow the load balancer to send http traffic to the web servers running on port 80.

Create a new security list called Public\_LB\_SecList and add the following rules:

### Ingress

Allow TCP from 0.0.0.0/0 to destination port 80


### Egress

Allow TCP to 10.0.0.16/28 on port 80

|           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 2.3.      | Add this new security list to the public load balancer's subnet.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| 2.4.      | <p>Now we must create a corresponding security rule for the app-subnet to allow HTTP traffic in from the load balancer.</p> <p>Create another security list call Private_App_SecList and add the following rule:</p> <p><b>Ingress</b><br/>Allow TCP from 10.0.0.32/28 to destination port 80.</p>                                                                                                                                                                                                                                                                                                                                                               |
| 2.5.      | Add the security list to the app-subnet.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>3.</b> | <b>Creating a Public Load Balancer</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| 3.1.      | <p>With our network prepared, we can now create a public load balancer. This public load balancer will be configured to listen for HTTP traffic on port 80 and load balance requests across a backend set that has both app1 and app2 web servers in it.</p> <p>In the OCI Console, navigate to Networking &gt; Load Balancers.</p>                                                                                                                                                                                                                                                                                                                              |
| 3.2.      | <p>Click the Create Load Balancer button and specify the following parameters.</p> <p><b>Load Balancer Name:</b> website_lb<br/> <b>Choose Visibility Type:</b> Public<br/> <b>Assign a public IP address:</b> Ephemeral<br/> <b>Under shapes,</b> keep the default values for bandwidth.</p> <p>Under <b>Choose Networking</b>, place the load balancer in the front-subnet in the vcn_oci_labs VCN.</p> <p>Click <b>Next</b> to configure the load balancer backend set.</p>                                                                                                                                                                                   |
| 3.3.      | <p>Under <b>Load Balancing Policy</b>, select Weighted Round Robin. This policy will distribute requests evenly across our web servers.</p> <p>Click the <b>Add Backends</b> button and add app1 and app2 to the backend set. A backend is essentially our web server cluster. The load balancer will load balance requests across every compute instance in the backend set.</p> <p>Leave the default values under <b>Health Check policy</b>. The Health Check Policy is used by the load balancer to know if a compute instance in the backend set is healthy or not. If it is not healthy, the load balancer will not forward requests to that instance.</p> |

|      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      | Click <b>Next</b> to configure the Listener.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| 3.4. | <p>The Listener is what listens for incoming requests. You can define what protocol and what port the listener should be listening on, and whether SSL/TLS should be configured.</p> <p>In this lab:</p> <ol style="list-style-type: none"><li>1) Keep the default listener name</li><li>2) Specify HTTP as the traffic type</li><li>3) Specify port 80 as the listen ingress port</li></ol> <p>Click the <b>Submit</b> button to create the load balancer.</p> <p>Oracle will assign a public IP address to the public load balancer, which you can see on the Load Balancer's details page. It is this public IP address that will be used to visit our website.</p> |
| 3.5. | <p>Once the load balancer is provisioned, it will take time for the Overall Health status to update showing healthy.</p> <p><b>Verify the health of your backend set</b> by clicking on the load balancer website_lb &gt; Backend Sets &gt; the backend set &gt; backends.</p> <p>app1 and app2 should appear in the backend set.</p>                                                                                                                                                                                                                                                                                                                                  |

Networking » Load Balancers » Load Balancer Details » Backend Sets » Backend Set Details » Backends



### bs\_lb\_2021-0221-1825

[Edit](#) [Update Health Check](#) [Delete](#)

Backend Set Information

#### Backend Set Information

Policy: Weighted Round Robin

Load Balancer: [lb\\_2021-0221-1825](#)

#### Overall Health

Critical


#### Backends Health

1 Critical

0 Warning

0 Unknown

0 OK



### bs\_lb\_2021-0221-1825

[Edit](#) [Update Health Check](#) [Delete](#)

Backend Set Information

#### Backend Set Information

Policy: Weighted Round Robin

Load Balancer: [lb\\_2021-0221-1825](#)

#### Overall Health

OK

#### Backends Health

0 Critical

0 Warning

0 Unknown

1 OK

3.6. Confirm the health of each backend – app1 and app2 – is healthy.

© 2020 TechTipsOnDemand.com

109

|           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|           | <p>If the health is unknown or critical, verify the following:</p> <ol style="list-style-type: none"> <li>1) Apache is up and running with our custom web page</li> <li>2) The firewall on the web server host allows HTTP in</li> <li>3) Security list for the app-subnet allows TCP/80 in from the load balancer subnet (front-subnet).</li> <li>4) Security list on the public load balancer subnet (front-subnet) allows egress to app-subnet on port 80.</li> </ol>                                                                                                                                                                                                                                                                                                      |
| <b>4.</b> | <b>Verify the Load Balancer is Working</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| 4.1.      | <p>In this section you will confirm that the load balancer is load balancing requests across each web server and that it can detect and handle one of the servers going offline.</p> <p>In order to proceed, the backend set must be healthy as noted in the previous section.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| 4.2.      | <p>When you installed and setup Apache to host our really simply website, you create an index.html page for each server. To demonstrate what server is returning the request, you put the name of the server in the index.htm, such that when you hit the public IP address of the load balancer, you will see a different index.html depending on what server the load balancer is sending the request to.</p> <p>To demonstrate, <b>use your browser</b> to go to the public IP address of the load balancer. You should see the index.html that you created earlier with the name of the server.</p> <p>Refresh your browser to reload the request. The load balancer will round robin your request across each server, returning the index.html page for that server.</p> |
| <b>5.</b> | <b>Testing Server Failure</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| 5.1.      | <p>In this section you will observe what happens when one of the web servers goes offline.</p> <p><b>SSH into app1</b></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| 5.2.      | <p>Shutdown the webserver by running the command:</p> <pre>\$ sudo systemctl stop httpd</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| 5.3.      | <p>Use your browser <b>to revisit the public IP address of the load balancer</b>. Verify that app2 is returning the request by observing the output from the web page. Keep refreshing your browser window to confirm that only app2 is returning the</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

|           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|           | response.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| 5.4.      | <p>In the OCI Console, <b>check the health status</b> of the backend set by going to Networking &gt; Load Balancers &gt; website_lb &gt; Backend Sets.</p> <p>app1 should appear in a critical state.</p> <p>OCI will check the health status of a server on a regular interval that you can configure. By default, the interval is 10000 ms.</p>                                                                                                                                                                                 |
| 5.5.      | <p>Restart apache on app1</p> <pre>\$ sudo systemctl start httpd</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| 5.6.      | <p>Verify the health of the backend set returns to OK. It may take some time for the change to be reflected in the UI, but you should be able to test using your browser to hit the load balancer IP address after a few seconds of restarting apache.</p>                                                                                                                                                                                                                                                                        |
| <b>6.</b> | <b>Enabling SSL</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| 6.1.      | <p>In this section you will enable SSL for your website by loading a certificate bundle into a new load balancer listener that you will create.</p> <p>The certificate bundle is a combination of a signed SSL certificate plus a private key. The load balancer uses this bundle to accept SSL requests from users and to terminate the SSL connection at the load balancer. The request or network traffic then moves from the load balancer to the web server unencrypted.</p>                                                 |
| 6.2.      | <p>First let's generate a certificate bundle to be used with the load balancer. For this exercise you will be created a self-signed certificate using openssl.</p> <p>This step requires the use of openssl, which is available for installation on most operating systems.</p> <p>Run the following commands:</p> <pre>\$ openssl genrsa -aes256 -passout pass:gsahdg -out server.pass.key 4096 \$ openssl rsa -passin pass:gsahdg -in server.pass.key -out server.key \$ openssl req -new -key server.key -out server.csr</pre> |

|      |                                                                                                                                                                                                                                                                                                                                                                                                               |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      | <pre>\$ openssl x509 -req -sha256 -days 365 -in server.csr -signkey server.key -out server.crt</pre> <p>The server.key is the private key for the server, in this case, for the load balancer. It is used to terminate the SSL connection before sending it to the web server.</p> <p>The server.crt is the SSL certificate used to establish an SSL connection with end user.</p>                            |
| 6.3. | <p>Next we need to create a certificate bundle to be used with our load balancer.</p> <p>In the OCI Console, navigate to Networking &gt; Load Balancers &gt; website_lb &gt; Certificates.</p>                                                                                                                                                                                                                |
| 6.4. | <p>Click the Add Certificate button.</p> <p>Name the certificate ocilabs_selfsigned</p> <p>Under SSL certificate, you can either upload the server.crt file or you can paste in its contents.</p> <p>Add the private key by checking the box for Specify Private Key and uploading or pasting in the contents of server.key.</p> <p>Click Add Certificate when done.</p>                                      |
| 6.5. | <p>Once the certificate has been added, we now need to create a new listener to listen for https/443 requests using the certificate we just uploaded.</p> <p>Under Resources heading for the load balancer, select Listeners.</p>                                                                                                                                                                             |
| 6.6. | <p>Click Create Listener.</p> <p>Provide the following information:</p> <p><b>Name:</b> website_secure_listener<br/> <b>Check the box for Use SSL.</b> This should update the Port to 443.</p> <p><b>Certificate name:</b> Select the ocilabs_selfsigned certificate.<br/> <b>Uncheck Verify Peer Certificate</b><br/> <b>Backend set:</b> Select the backend set – there should be only one in the list.</p> |



Click the Create Listener button.

## Create Listener

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

Name

website\_secure\_listener

There are no hostnames for this load balancer. [Create a hostname.](#)

Protocol

HTTP

Port

443

Use SSL



Certificate Name

ocilabs\_selfsigned

Verify Peer Certificate



Backend Set

bs\_lb\_2021-0221-1825

Idle Timeout In Seconds: *Optional*

The default timeout for HTTP is 60 seconds.

There are no path route sets for this load balancer. [Create a path route set.](#)

6.7. It will take OCI a moment to provision the listener with the certificate you specified.

You can check the status and any error messages under the Resources heading > Work Requests.

Typically the listener will fail if the SSL certificate or private key are invalid or malformed. If this is the case, then confirm the certificate bundle was created properly. If not, recreate the bundle and add it to the listener.

6.8. Once the HTTPS listener is up and running, you may access the website using HTTPS instead of HTTP.

Using your browser, go to [https://public IP address of LoadBalancer](https://public_IP_address_of_LoadBalancer)

Since we are using a self-signed certificate, the browser will warn you that you are accessing an unsafe website. In the real world you would use a proper certificate from a trusted Certified Authority rather than a self-signed certificate. However the process for using CA-signed cert and a self-signed cert with OCI is the same.

## 7. Enabling Logs

7.1. The OCI Load Balancer has the ability to write both access and error logs to the OCI Logging Service.

To enable logs, go to Logs under the Resources heading for the load balancer.

7.2. You can enable either the access log or error log or both.

Click on the Enable toggle for the Access Log and specify the following details:

**Compartment:** OCI\_Labs

**Log Group:** Default\_Group

**Log Name:** website\_access\_logs

**Log Retention:** 1 month

Click the button when you are done.

OCI Logging organizes logs into groups called Log Groups. You are free to create your own log groups, however in this section we are using the default log group for simplicity.

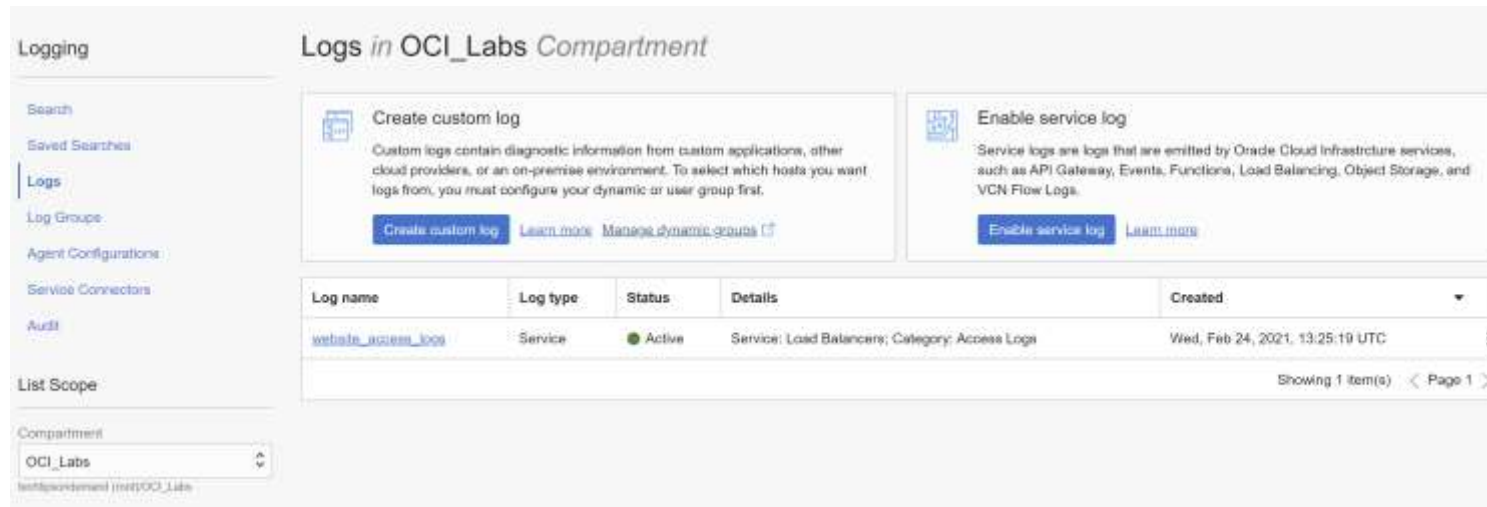
7.3. You can access the log file from the Logs screen by clicking on the name of the log:

Logs

| Category | Status | Log Name                            | Log Group                     | Enable Log                                  |   |
|----------|--------|-------------------------------------|-------------------------------|---------------------------------------------|---|
| access   | Active | <a href="#">website_access_logs</a> | <a href="#">Default_Group</a> | <input checked="" type="checkbox"/> Enabled | ⋮ |
| error    | —      | —                                   | —                             | <input type="checkbox"/> Disabled           | ⋮ |

Showing 2 Items

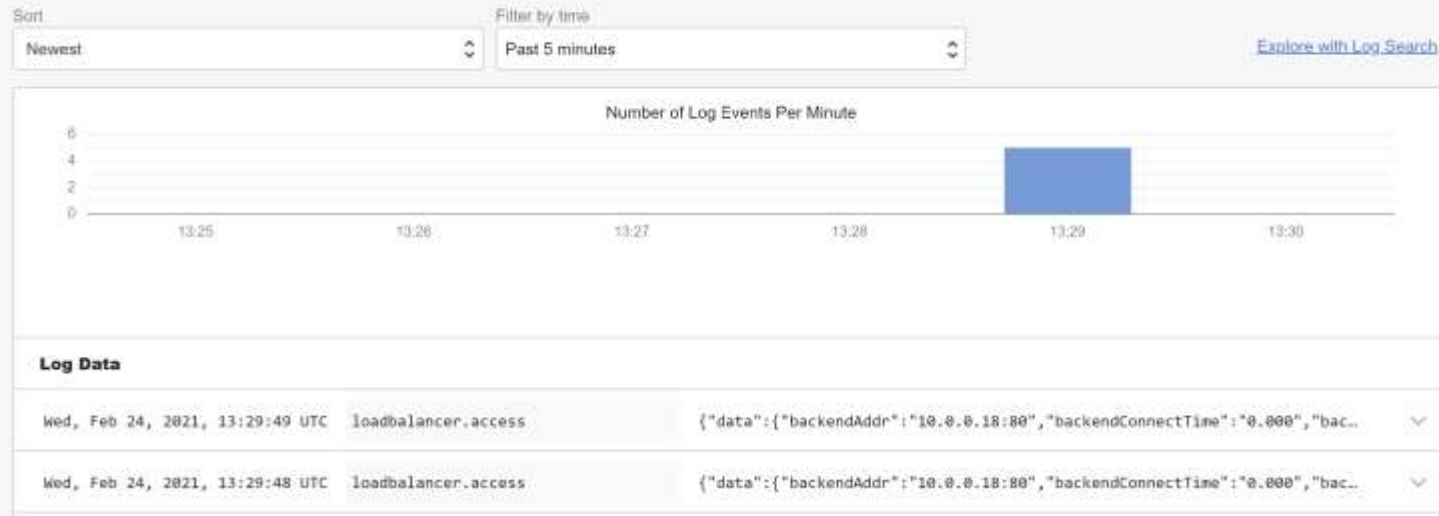
7.4. You can also get to OCI Logging in the OCI Console by navigating to Logging > Logs.



7.5. In another browser window, visit the website again a few times, refreshing the browser window. Doing so will create entries in the access log.

7.6. View the access log by clicking on its name in the OCI Console. You should now see access log entries.

## Explore Log



7.7. Expanding one of the log entries will reveal more details about the request, including which web server handled the request.

## 8. Cleaning Up

- 8.1. Perform the following steps to once you are done with the lab
- 1) Stop all running compute instances
  - 2) Terminate the Load Balancer we created by going to the OCI Console > Networking > Load Balancers. Select the ellipsis for the website-lb, then select Terminate, which will delete the load balancer and its configuration.

## Lab #8: Core Identity and Access Management

---

*Duration 30 minutes*

### Skills Learned

At the end of this exercise, you will be able to:

- Organize resources using Compartments
- Create local OCI users and groups
- Manage access to resources using policies
- Create and manage users and groups using Identity Cloud Service

### Overview

Up to this point in the lab, you have done everything as a tenancy administrator. As a tenancy administrator, you are a member of the administrators group, which automatically grants access to do anything in the tenancy without needing explicit permission to do so. In the real world however, resources need governance – there needs to be a separation of duties to ensure the security, integrity, and availability of the resources in a tenancy. In plain English, this means putting users in groups and granting access to OCI resources using OCI IAM policies.

An IAM policy is a statement or set of statements that let someone or something do something with an OCI resource. The policy syntax is based on natural language so it is easy to read and learn.

In this lab you will learn how to organize resources based on a typical organizational structure into compartments and manage them using IAM policies.

We will also touch on using Identity Cloud Service or IDCS as the preferred method for managing users and groups rather than using local IAM accounts. Every tenancy comes with an instance of IDCS, which allows you to federate with your company's identity provider. This allows you to easily and securely tie into your company's identity management system without needing to maintain a duplicate set of users in OCI. You can use IDCS on its own, even if you do not have a corporate identity management system.

Let us pretend that our organization's IT department has the following teams, members, and responsibilities.

| Team    | Responsibilities                                                           | Members   |
|---------|----------------------------------------------------------------------------|-----------|
| Network | Designing, implementing, and managing all networks in the cloud, including | joe_smith |

|                |                                                                                                                                                                                                      |          |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|
| Admins         | controlling security lists, routes, and gateways.                                                                                                                                                    |          |
| Storage Admins | Creating and managing block volumes, including managing backups, snapshots, and migrations.                                                                                                          | jane_doe |
| Developers     | Developing and deploying applications to compute nodes in the cloud. Team is also responsible for creating and managing compute instances, including attaching storage volumes to compute instances. | han_lee  |

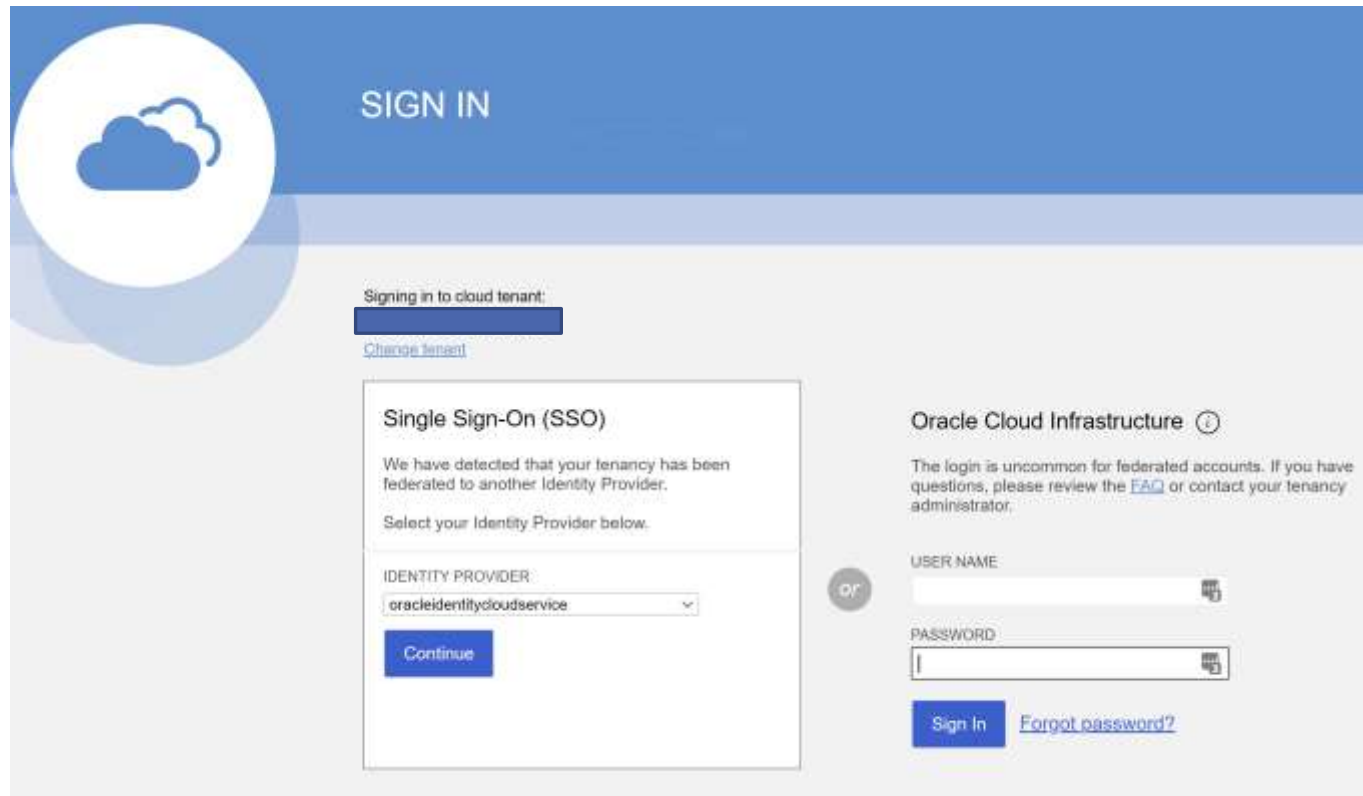
We want to set up our tenancy so that it aligns with our organizational structure. Each team will have its own OCI group and each team member will be given an OCI account.

Compartments will be created to organize and manage OCI resources in alignment with our organizational structure. IAM policies will be written to grant the groups access to resources.

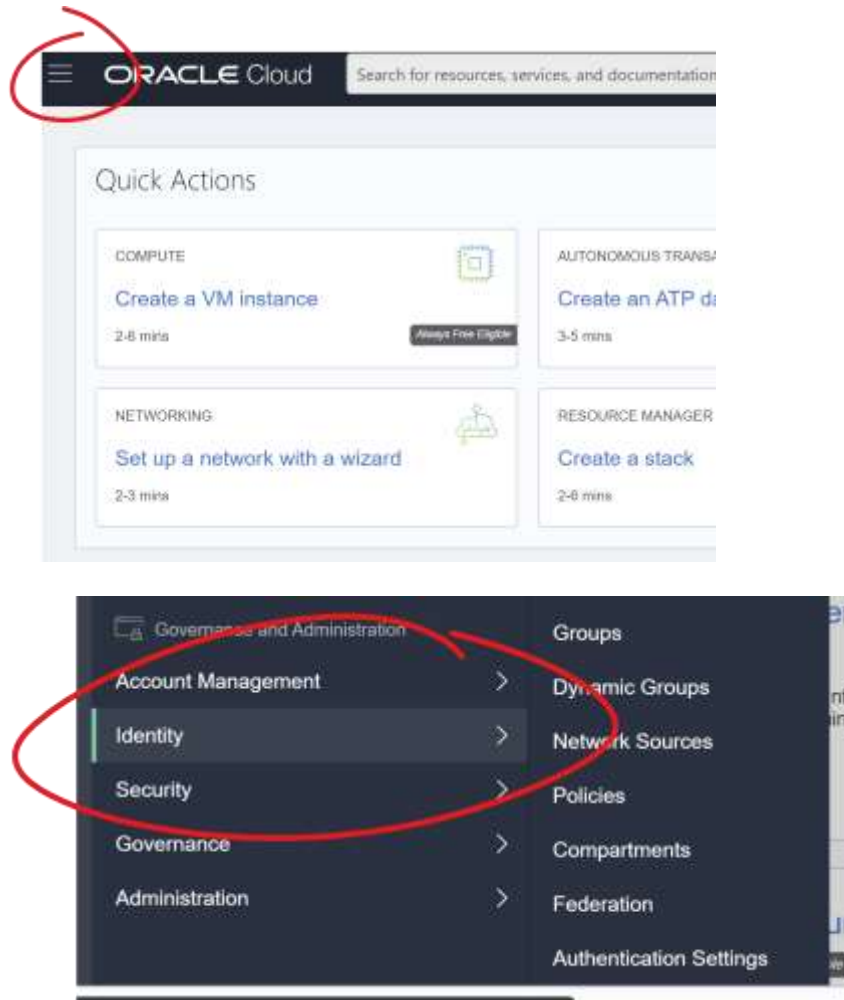
## Instructions

|           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>1.</b> | <b>Creating a Compartment Structure</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| 1.1.      | <p>In this section you will create compartments to support the scenario outlined above. You will create the following compartments:</p> <p>Networks – used to organize certain virtual networking resources<br/> DevTeam – used to organize compute and any other resources the development team is responsible for managing.</p> <p><i>** You need to have the proper permissions in OCI to execute this lab. This lab presumes that you personally created the OCI tenancy and therefore have the necessary permissions to create and manage resources already. **</i></p>                                                                                                  |
| 1.2.      | <p>Log into the OCI console using your web browser using the login URL that was in the welcome email from Oracle or go to <a href="https://cloud.oracle.com">cloud.oracle.com</a> and click on sign in.</p> <p>You should be presented with a login screen that looks similar to the screenshot below. If you have never signed in, you may be presented with a single dialog asking you for a cloud account name first. Enter in the name of the tenancy that you specified when signing up. This will also be in your welcome email.</p> <p>You will then see two options on the login screen. The first option (on the left) allows you to login using SSO. The second</p> |

option (on the right) allows you to login using a local account. Select the second option and use the credentials you specified when signing up for OCI.



- 1.3. Once you have logged in, you will be in the OCI console.
- Click the stacked bars in the upper left and then click on Identity (near the bottom).



1.4. Select Compartments under Identity.



**Identity**

**Compartments**

Create Compartment

| Name                     | Status | OCID   | Authorized | Subcompartments | Created                        |
|--------------------------|--------|--------|------------|-----------------|--------------------------------|
| techondemand.root        | Active | oc214a | Yes        | 1               | -                              |
| MacrosCompartmentForPaas | Active | oc302a | Yes        | 0               | Fri, Aug 7, 2020, 15:42:19 UTC |

Showing 2 items < Page 1 >

Filters

STATE

Active | Deleting

1.5. Create a compartment by clicking the button and specifying the following parameters.

**Name:** Networks

**Description:** Put whatever you want here but it is a required field.

**Parent Compartment:** Select the OCI\_Labs compartment

Your screen should look similar to the screenshot below.

## Create Compartment [Help](#)

Name

Description

Parent Compartment

OCI\_Labs

techtipsondemand (root)OCI\_Labs

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

[Learn more about tagging](#)

| TAG NAMESPACE              | TAG KEY              | VALUE                |
|----------------------------|----------------------|----------------------|
| None (add a free-form tag) | <input type="text"/> | <input type="text"/> |

+ Additional Tag

Create Compartment

[Cancel](#)

Click the button at the bottom of the dialog to create the compartment.

- The Networks compartment should now appear in the list of compartments in the OCI console under the OCI\_Labs compartment.

## Child Compartments

| <a href="#">Create Compartment</a> |          |         |            |                 |                                 |
|------------------------------------|----------|---------|------------|-----------------|---------------------------------|
| Name                               | Status   | OCID    | Authorized | Security Zone ⓘ | Created                         |
| <a href="#">Networks</a>           | ● Active | ocvcl4a | Yes        | Not Enabled     | Sat, Feb 20, 2021, 22:41:19 UTC |
| Showing 1 Item < 1 of 1 >          |          |         |            |                 |                                 |

## Compartments

| <a href="#">Create Compartment</a>        |          |           |            |                 |                                |
|-------------------------------------------|----------|-----------|------------|-----------------|--------------------------------|
| Name                                      | Status   | OCID      | Authorized | Subcompartments | Created                        |
| <a href="#">techtipsondemand (root)</a>   | ● Active | oc2z4a    | Yes        | 2               | -                              |
| <a href="#">ManagedCompartmentForPaaS</a> | ● Active | ocvni6zo  | Yes        | 0               | Fri, Aug 7, 2020, 15:42:19 UTC |
| <a href="#">Networks</a>                  | ● Active | ocbeavaka | Yes        | 0               | Sun, Aug 9, 2020, 21:11:03 UTC |
| Showing 3 Items < Page 1 >                |          |           |            |                 |                                |

1.7. Create the DevTeam compartment following the same steps as the Networks compartment.

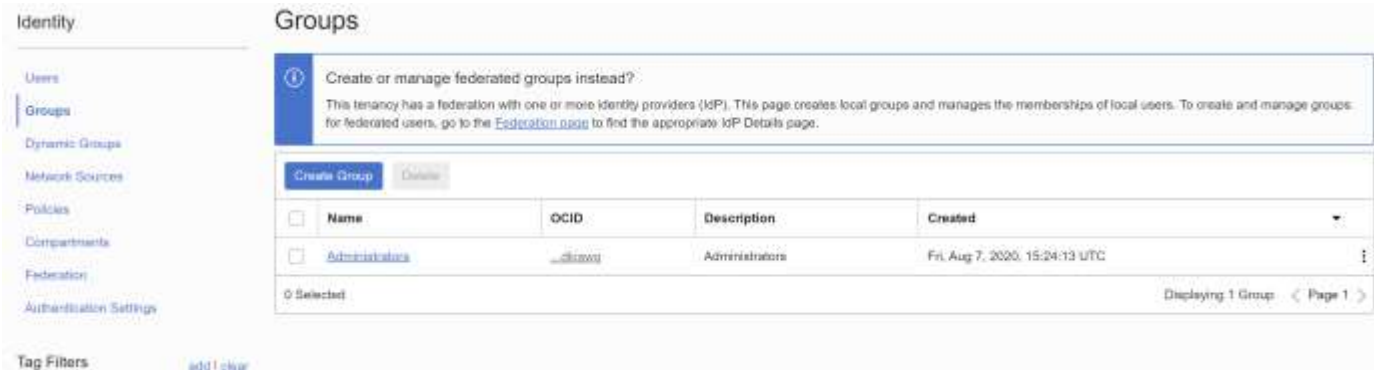
## 2. Creating Local Users and Groups

2.1. In this section you will create local users and groups in OCI for each of the teams:

NetworkAdmins  
StorageAdmins  
DevTeam

You will eventually write IAM policies that grant these groups access to certain OCI resources.

2.2. Access OCI Groups by selecting Groups under Identity. You can also click on the stacked bars in the upper-left, then navigate to Identity then Groups.



Notice there is one group already created: Administrators. This group was created when we created the tenancy and contains at least one user – the person who created the tenancy.

2.3. Click Create Group and specify the following parameters for the Network Admins group.

Name: NetworkAdmins

Description: *Put whatever you want here but it is a required field.*

Once you are done click Create.

Create Group


[Help](#) [Cancel](#)

!

This page creates a local group only. To create and manage federated groups, go to the [Federation page](#) to find the appropriate Identity Provider Details page.

NAME

NetworkAdmins



No spaces. Only letters, numerals, hyphens, periods, or underscores.

DESCRIPTION

Network administrators


TAGS


Tagging is a metadata system that allows you to organize and track resources within your tenancy. Tags are composed of keys and values that can be attached to resources.  
[Learn more about tagging](#)

TAG NAMESPACE

TAG KEY

VALUE

None (add a free-form tag) 



+ Additional Tag

Create

Cancel

2.4. Repeat the process for the StorageAdmins group and the DevTeam group.

Your group list should look like this:

## Groups



## Create or manage federated groups instead?

This tenancy has a federation with one or more identity providers (IdP). This page creates local groups and manages the memberships of local users. To create and manage groups for federated users, go to the [Federation page](#) to find the appropriate IdP Details page.

Create Group

Delete

| <input type="checkbox"/> | Name                           | OCID      | Description            | Created                        |            |
|--------------------------|--------------------------------|-----------|------------------------|--------------------------------|------------|
| <input type="checkbox"/> | <a href="#">DevTeam</a>        | ...f33tkq | The Developers         | Sun, Aug 9, 2020, 21:25:08 UTC | ⋮          |
| <input type="checkbox"/> | <a href="#">StorageAdmins</a>  | ...qvztrg | The storage guys       | Sun, Aug 9, 2020, 21:24:55 UTC | ⋮          |
| <input type="checkbox"/> | <a href="#">NetworkAdmins</a>  | ...csluua | Network administrators | Sun, Aug 9, 2020, 21:24:44 UTC | ⋮          |
| <input type="checkbox"/> | <a href="#">Administrators</a> | ...dkiawq | Administrators         | Fri, Aug 7, 2020, 15:24:13 UTC | ⋮          |
| 0 Selected               |                                |           |                        | Displaying 4 Groups            | < Page 1 > |

2.5. You may have seen various warnings and notices about creating federated groups. What we are doing here in this lab is creating local users and groups, which live and are managed only within OCI. OCI supports federation with an external identity provider (IdP) that allows users to log in using SSO. Federated users and groups are managed by the IdP, not by OCI.

2.6. Now let's create some users. Click on Users on the left side of the screen under Identity.

Identity

Users
Groups
Dynamic Groups
Network Sources
Policies
Compartments
Federation
Authentication Settings
Tag Filters

Create or manage federated users instead?

This tenancy has a federation with one or more identity providers (IdP), which means users typically sign in as federated users. This page creates local users, manages their local capabilities, and lets them sign in to Oracle Cloud Infrastructure if the federated IdP is unavailable. To create and manage federated users, go to the [Federation page](#) to find the appropriate IdP Details page.

Create User
Delete

| <input type="checkbox"/> | Name                                        | Status | Email                      | Description                | Federated | Created                        |   |
|--------------------------|---------------------------------------------|--------|----------------------------|----------------------------|-----------|--------------------------------|---|
| <input type="checkbox"/> | <a href="#">oracle@techtipsondemand.com</a> | Active | -                          | chris@techtipsondemand.com | Yes       | Fri, Aug 7, 2020, 15:30:58 UTC | ⋮ |
| <input type="checkbox"/> | <a href="#">chris@techtipsondemand.com</a>  | Active | chris@techtipsondemand.com | Christopher Parent         | No        | Fri, Aug 7, 2020, 15:24:13 UTC | ⋮ |

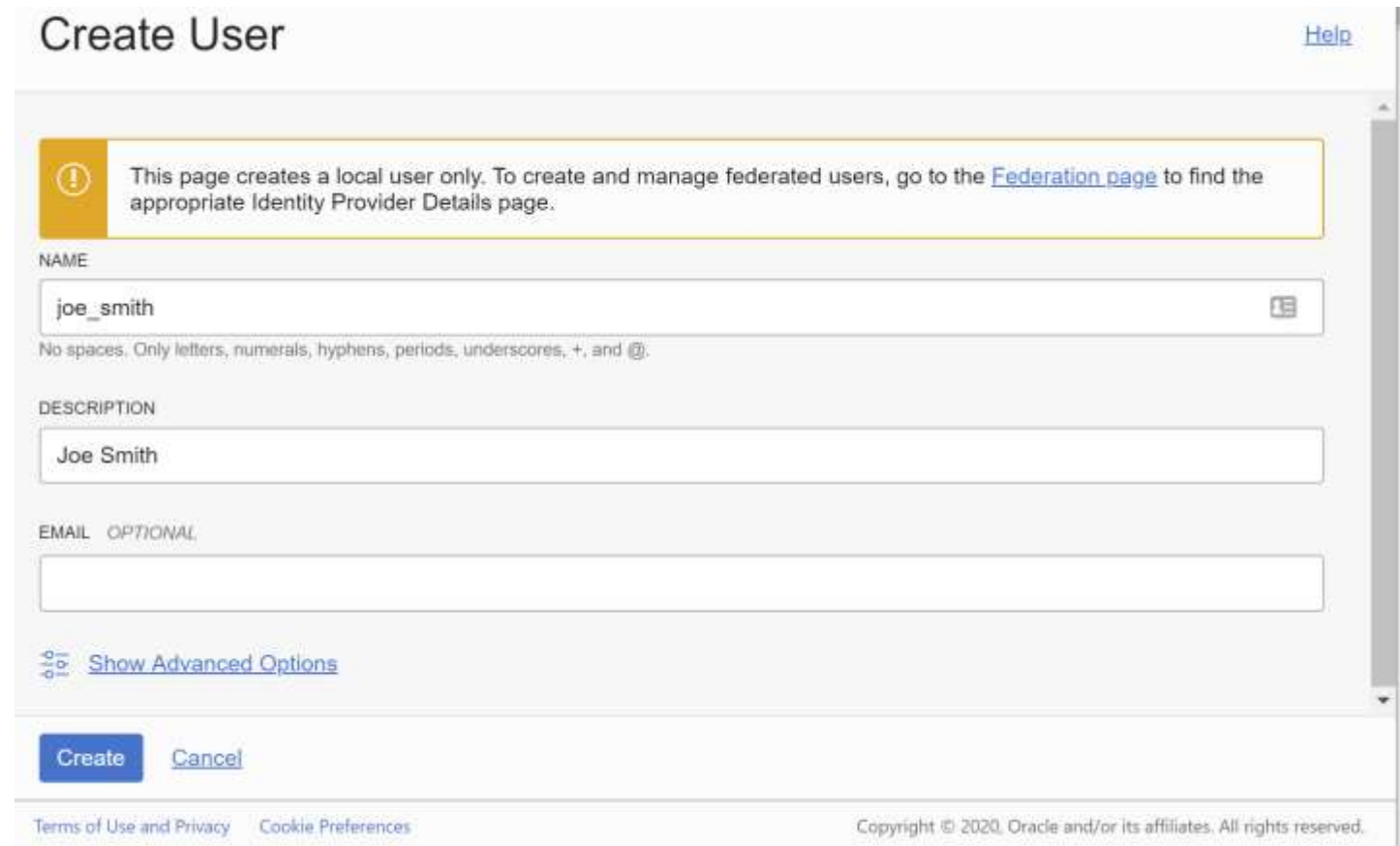
0 Selected
Displaying 2 Users
< Page 1 >

2.7. Use the Create User button to create the following users. You can leave the email addresses blank.


Name: joe\_smith

Name: jane\_doe

Name: han\_lee



Create User [Help](#)

 This page creates a local user only. To create and manage federated users, go to the [Federation page](#) to find the appropriate Identity Provider Details page.

NAME

joe\_smith 

No spaces. Only letters, numerals, hyphens, periods, underscores, +, and @.

DESCRIPTION

Joe Smith

EMAIL OPTIONAL

 [Show Advanced Options](#)

[Create](#) [Cancel](#)

[Terms of Use and Privacy](#) [Cookie Preferences](#) Copyright © 2020, Oracle and/or its affiliates. All rights reserved.

2.8. Your Users screen should look like the following:

## Users



### Create or manage federated users instead?

This tenancy has a federation with one or more identity providers (IdP), which means users typically sign in as federated users. This page creates local users, manages their local capabilities, and lets them sign in to Oracle Cloud Infrastructure if the federated IdP is unavailable. To create and manage federated users, go to the [Federation page](#) to find the appropriate IdP Details page.

[Create User](#)
[Delete](#)

| <input type="checkbox"/> | Name                                                                | Status | Email                      | Description                | Federated | Created                         |            |
|--------------------------|---------------------------------------------------------------------|--------|----------------------------|----------------------------|-----------|---------------------------------|------------|
| <input type="checkbox"/> | <a href="#">han_lee</a>                                             | Active | -                          | Han Lee                    | No        | Tue, Aug 11, 2020, 02:47:53 UTC | ⋮          |
| <input type="checkbox"/> | <a href="#">jane_doe</a>                                            | Active | -                          | Jane Doe                   | No        | Tue, Aug 11, 2020, 02:47:44 UTC | ⋮          |
| <input type="checkbox"/> | <a href="#">joe_smith</a>                                           | Active | -                          | Joe Smith                  | No        | Tue, Aug 11, 2020, 02:46:47 UTC | ⋮          |
| <input type="checkbox"/> | <a href="#">oracleident@cloudservice/chris@techtipsondemand.com</a> | Active | -                          | chris@techtipsondemand.com | Yes       | Fri, Aug 7, 2020, 15:30:56 UTC  | ⋮          |
| <input type="checkbox"/> | <a href="#">chris@techtipsondemand.com</a>                          | Active | chris@techtipsondemand.com | Christopher Parent         | No        | Fri, Aug 7, 2020, 15:24:13 UTC  | ⋮          |
| 1 Selected               |                                                                     |        |                            |                            |           | Displaying 5 Users              | < Page 1 > |

2.9. Next let's assign these users to the right groups. You can either add a user to a group, or a group to a user.

For this tutorial we will be adding users to a group through the Group interface. This is preferred if you are adding users in bulk.


Navigate to Groups and select the NetworkAdmins group.



Identity » Groups » Group Details

## NetworkAdmins

[Edit Group](#) [Add Tags](#) [Delete](#)



ACTIVE

**Group Information** Tags

**OCID:** ...csiuua [Show](#) [Copy](#)

**Created:** Sun, Aug 9, 2020, 21:24:44 UTC

**Description:** Network administrators

**Resources**

- [Group Members](#)
- [IdP Mapped Groups](#)

## Group Members

[Add User to Group](#)

| Name            | OCID | Description | Federated | Created |
|-----------------|------|-------------|-----------|---------|
| No items found. |      |             |           |         |

Showing 0 items < 1 of 1 >

- 2.10. Under Group Members, select Add User to Group. Select joe\_smith from Users list and click Add.

## Group Members

| <a href="#">Add User to Group</a> |           |             |           |                                 |
|-----------------------------------|-----------|-------------|-----------|---------------------------------|
| Name                              | OCID      | Description | Federated | Created                         |
| <a href="#">joe_smith</a>         | ...p7yhcg | Joe Smith   | No        | Tue, Aug 11, 2020, 02:46:47 UTC |
| Showing 1 Item < 1 of 1 >         |           |             |           |                                 |

2.11. Repeat the above steps to add jane\_doe to the StorageAdmins group and han\_lee to the DevTeam group.

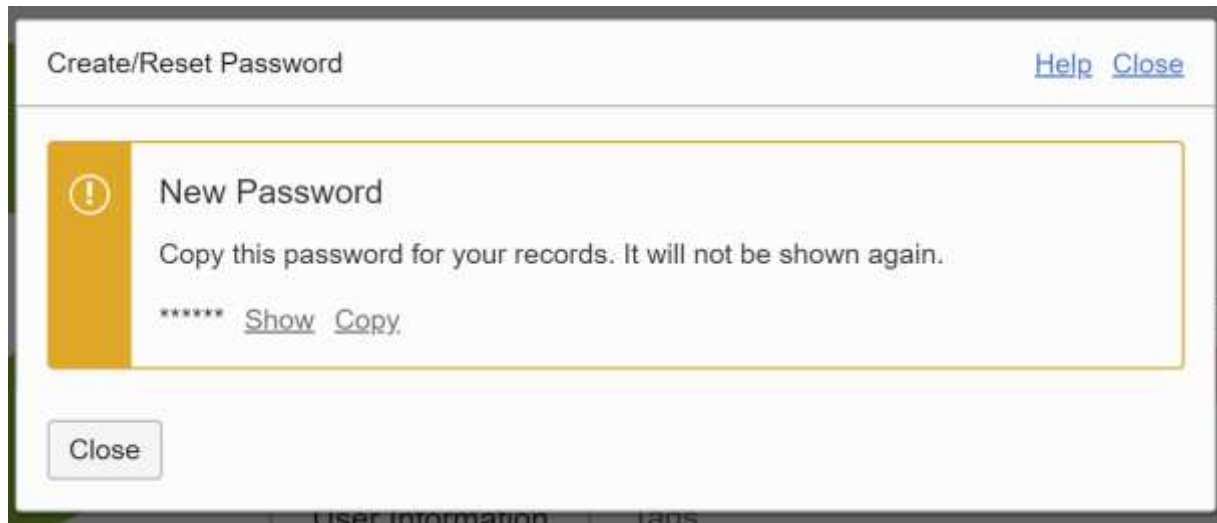
2.12. At this point, users have been created and assigned to groups, but the users do not yet have any credentials to login or access OCI.

You can assign a one-time password to a user in the Console. When the user logs into the console for the first time, they will be asked to change the password.

Navigate to Users under Identity and select joe\_smith.



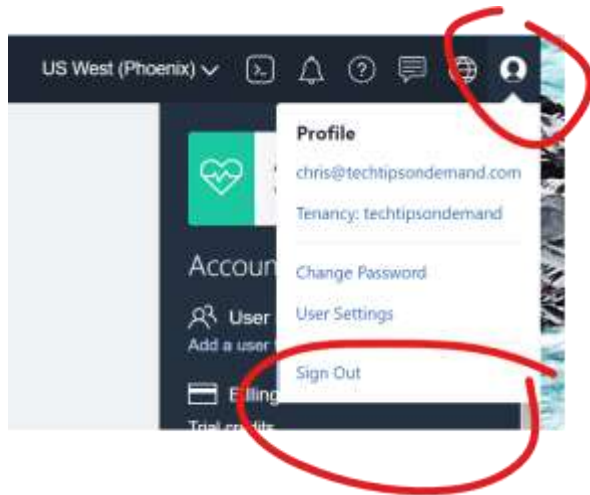
- |       |                                                                                                                                                                                                                 |
|-------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2.13. | Generate a password for joe_smith by clicking the Create/Reset Password button. Then click Create/Reset Password button again to confirm the action.                                                            |
| 2.14. | A new password will be generated for the user. You must save the password somewhere until you log in as this user.<br><br>If you lose the password, you can always repeat the above steps to rest the password. |



2.15. Repeat the above steps to create passwords for jane\_doe and han\_lee. Be sure to save each of the passwords.

2.16. Let's verify that we can log in as one of the users using the new password.

First you need to log out of the OCI Console. Locate the profile icon in the upper right of the screen and select Sign out.



2.17. Log back in using the joe\_smith local user and the password that was generated.

2.18. You will be asked to change the password when you log in for the first time.

2.19. The users we created do not yet have any permissions assigned to them. We did add users to a group, but we have not yet written any IAM policies granting users access to really do anything.

To verify this, try creating a compartment as before.

Go to Identity > Compartments.

2.20. Notice how the user can only see the root compartment and the managed compartment for PaaS. This user cannot see any of the compartments that were created earlier because we have not granted this user any permissions. Users need INSPECT permission at a minimum to see a list of compartments.

## Compartments

| Create Compartment                        |          |           |            |                 |                                |
|-------------------------------------------|----------|-----------|------------|-----------------|--------------------------------|
| Name                                      | Status   | OCID      | Authorized | Subcompartments | Created                        |
| <a href="#">techtipsondemand (root)</a>   | ● Active | ...g2zj4a | Yes        | 1               | -                              |
| <a href="#">ManagedCompartmentForPaaS</a> | ● Active | ...yni6zg | Yes        | 0               | Fri, Aug 7, 2020, 15:42:19 UTC |
| Showing 2 Items < Page 1 >                |          |           |            |                 |                                |

2.21. Try creating a compartment by clicking the Create Compartment button.

The dialog will appear, and you are able to fill it out. However when you click the create button, you will receive an authorization error. This is expected since this user has not been given any permissions.

**Create Compartment** [Help](#) [Cancel](#)

NAME  
MyOwnCompartment

DESCRIPTION  
This is for me

PARENT COMPARTMENT  
techtipsondemand (root)

Tagging is a metadata system that allows you to organize and track resources within your tenancy. Tags are composed of keys and values that can be attached to resources.  
[Learn more about tagging](#)

TAG NAMESPACE TAG KEY VALUE

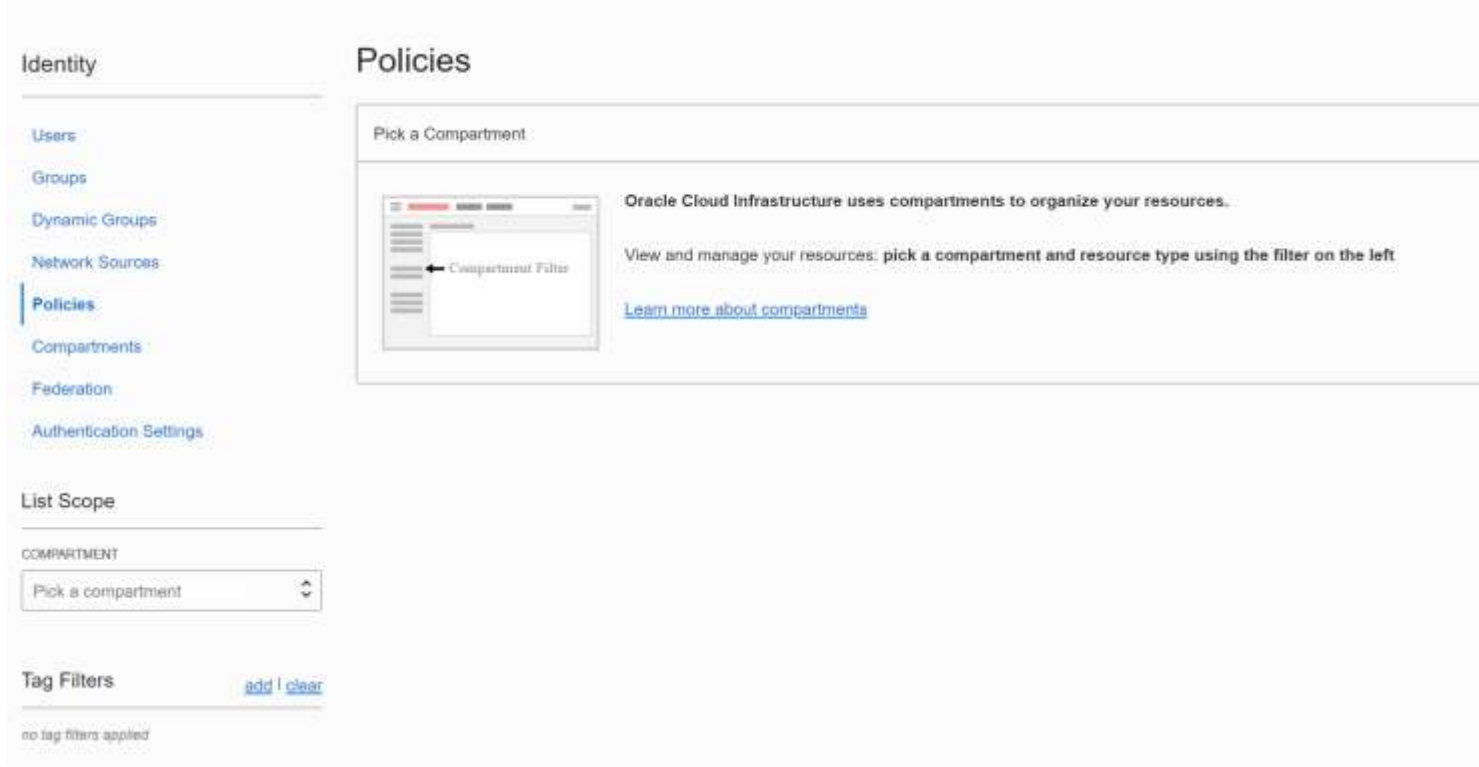
None (add a free-form-form...)

Authorization failed or requested resource not found

### 3. Writing an OCI IAM Policy

3. In this section you will write a couple IAM policies to grant our users access based upon each group's responsibilities that were called out earlier in the lab. We will write the remaining policies in future labs. This section is meant to demonstrate policy writing.

3.2. Log back into the OCI console as a tenancy administrator. (In most cases, this is the account you used to sign up for OCI).

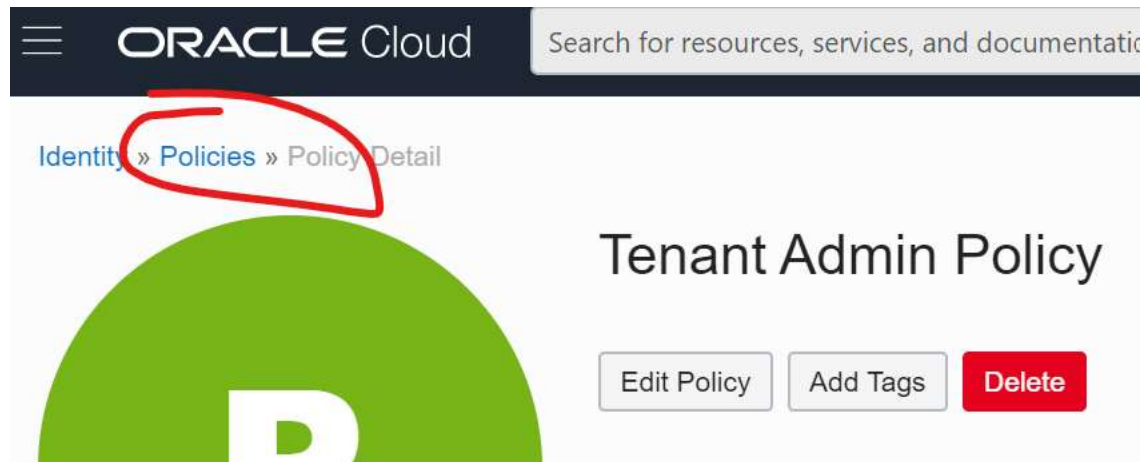
|      |                                                                                                                                                                                                                                                              |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      | Remember only the Tenancy Administrator has access to write IAM policies at this point.                                                                                                                                                                      |
| 3.3. | <p>Navigate to Identity &gt; Policies</p>                                                                                                                                 |
| 3.4. | <p>Policies are created in a compartment, just like most other OCI resources you will create.</p> <p>Under List Scope, select the root compartment.</p> <p>You will see two default policies – one for the Tenancy Admin and one called PSM-root-policy.</p> |
| 3.5. | To see what a policy looks like, click on the Tenancy Admin policy. This policy grants the group Administrators access to manage all resources in the tenancy.                                                                                               |

## Statements

[Edit Policy Statements](#)

ALLOW GROUP Administrators to manage all-resources IN TENANCY

3.6. Click on Policies in the breadcrumbs near the upper left to go back to the list of policies.



3.7. The first policy we want to write is to allow everyone in our tenancy to see the list of compartments. This will allow users to see what compartments are available through the OCI Console or through the OCI API, however it will not allow users to create compartments. Only administrators will be allowed to create compartments.

Under List Scope, select the root compartment so that we are viewing policies for the root compartment.

3.8. **Click Create Policy.** This will launch the create policy dialog.



**Specify the following parameters for the policy:**

Name: Default\_User\_Policy

Description: Default policy that will apply to all users

Keep Policy Current: Enabled

Compartment: (root)

**Policy Statement #1:**

Allow any-user to inspect compartments in tenancy

This policy will let everyone in the tenancy read all compartments. *Any-user* is a special group that automatically refers to every user in the tenancy.

**Save the policy when you are done.**

---

## Create Policy

[Help](#)

**i** A policy simply allows a [group](#) to work in certain ways with specific types of [resources](#) in a particular [compartment](#). Policies may also only apply under certain [conditions](#). [Learn more.](#)

NAME

Default\_User\_Policy



No spaces. Only letters, numerals, hyphens, periods, or underscores.

DESCRIPTION

Policies that apply to every user

☒ KEEP POLICY CURRENT ☐ USE VERSION DATE

COMPARTMENT

techtipsondemand (root)

## Policy Statements

[Advanced Policy Editor](#)

STATEMENT 1



Allow any-user to inspect compartments in tenancy

[+ Another Statement](#)Example: Allow group [\[group\\_name\]](#) to [\[verb\]](#) [\[resource-type\]](#) in compartment [\[compartment\\_name\]](#) where [\[condition\]](#)

- 3.9. Notice that a policy can have more than one statement, which is handy if you wish to group related policy statements into a single policy.

#### 4. Let Network Admins Management Networks

- 4.1. The next policy you are going to create is to allow the network admins to create and manage all network related resources under the OCI\_Labs compartment. This includes virtual cloud networks, security lists, subnets, and network security groups.

**Click on the Customize(Advanced) link and Create a new policy with the following parameters.**

Name: Network\_Management\_Policy

Description: Network management policy

Compartment: root

**Policy Statement #1:**

Allow group NetworkAdmins to manage virtual-network-family in compartment OCI\_Labs

**Save the policy when you are done.**

Let's break down this policy statement.

The subject of this policy statement is the group NetworkAdmins.

The resource that is being granted access to is virtual-network-family, which represents a collection of OCI networking resources, including VCNs, security lists, subnets and network security groups.

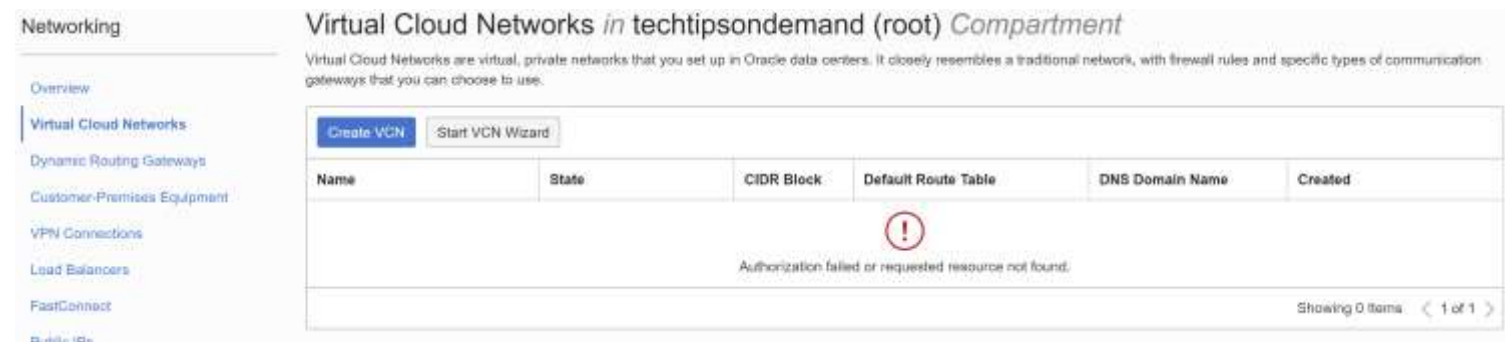
The last portion of the policy statement specifies the location where the access is being granted, in this case the OCI\_Labs compartment, which will include any child compartments as well.

4.2. Let's verify this policy statement actually works by logging in as the network admin and see if we can create a virtual cloud network.

4.3. **Log out of the OCI console and log back in as joe\_smith.** You will be asked to set a password for this user upon first login.

4.4. **Navigate to Networking > Virtual Cloud Networks from the left-hand navigation pane.**

By default you are in the root compartment after logging into the OCI console. You should see an authorization failed error on the Virtual Cloud Networks screen. This is because joe\_smith has not been granted any network-related access in the root compartment.



4.5. On the left-hand side under List Scope, select the OCI\_Labs:Networks compartment. The error should disappear since joe\_smith has manage permissions in this compartment, which gives Joe the ability to create a virtual network.

Let's verify that right now by creating a virtual cloud network using the VCN Wizard.

- a. Start the VCN Wizard.
- b. Create a VCN with Internet Connectivity and name it test-vcn.
- c. Select the Networks compartment.
- d. Accept all other default values and finish creating the VCN.

The Wizard will create the VCN and all supporting networking services in the Networks compartment.

---

4.6. Let's see if Joe can create any compute instances in the private subnet.

Navigate to Compute Instances and try provisioning a compute instance in the OCI Labs, Networks, or DevTeam compartments.

You can tell immediately that the Joe, who is a network admin, cannot even see a list of available compute instances in any compartment as the OCI Console displays an authorization error when trying to render the page.

A Network Admin should be able to at least see what compute instances are deployed in a VCN.

You will have to log back into the OCI Console as yourself to create the policy.

Add this statement to the Network Management Policy.

Allow group NetworkAdmins to read instances in OCI\_Labs

---

4.7. Log back into the OCI Console as Joe Smith and review the list of compute instances in the OCI Labs compartment by going to Compute > Instances.

Joe should now be able to see the two compute instances that were created earlier in this lab: bastion1 and app1.

If you try to create an instance as Joe, you will be met with an authorization error since the NetworkAdmins only have READ permission on compute instances.

---

|           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>5.</b> | <b>Let Storage Admins manage Block Volumes</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| 5.1.      | <p>Log back into the OCI Console as yourself again since we are about to create some additional IAM policies.</p> <p>The next policy you will write will allow the storage team the ability to create block volumes and take backups.</p> <p>Create the following policy named <code>Storage_Admin_Policy</code> in the root compartment:</p> <p>Allow group <code>StorageAdmins</code> to manage volume-family in compartment <code>OCI_Labs</code><br/> Allow group <code>StorageAdmins</code> to use instance-family in compartment <code>OCI_Labs</code></p> <p>The first statement lets the storage admins manage volumes in the OCI Labs compartment, while the second policy allows the storage admins to attach volumes to compute instances that are deployed in any compartment under OCI Labs.</p> <p>The verb <code>USE</code> includes the ability for the storage admins to read compute instances but also attach volumes as well.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| 5.2.      | <p>Log into the OCI Console as Jane Doe and verify the following actions:</p> <ol style="list-style-type: none"> <li>Create a block volume in the DevTeam compartment called <code>app_datavol2</code>.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>6.</b> | <b>Let the Dev Team create Compute Instances</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| 6.1.      | <p>The development team has the ability to provision compute instances in VCNs and attach block volumes, but it does not have the authority to create networks or block volumes. Create the following policy statements in a single policy named <code>DevTeam_Policy</code>.</p> <ol style="list-style-type: none"> <li>Allow group <code>DevTeam</code> to manage instance-family in compartment <code>OCI_Labs:DevTeam</code></li> <li>Allow group <code>DevTeam</code> to use volumes in compartment <code>OCI_Labs:DevTeam</code></li> <li>Allow group <code>DevTeam</code> to manage volume-attachments in compartment <code>OCI_Labs:DevTeam</code></li> <li>Allow group <code>DevTeam</code> to use virtual-network-family in compartment <code>OCI_Labs:Networks</code></li> </ol> <p>The first statement lets the dev team manage instance-family in the DevTeam compartment. Instance-family refers to a family of compute resources. The verb <i>manage</i> lets the group do everything with those resources.</p> <p>The second and third statements let the dev team attach block volumes to compute instances, however they cannot create, delete, or backup those volumes.</p> <p>The fourth statement lets the dev team use networking resources in the Networks compartment. This policy is required to provision compute instances in a subnet. Similar to the second policy statement, the dev team only has permission to</p> |

use resources, not manage them.

## 7. Verify the Policies Work

7.1. Log in to the OCI Console as Han Lee, who is a member of the DevTeam.

7.2. Create an Always Free Eligible compute instance in the DevTeam compartment with the following parameters:

Create in compartment: DevTeam

Shape: *Any Always Free Eligible Shape*

### Under Networking...

Select the test-vcn from the Networks compartment.

Select the Private Subnet-test-vcn from the Networks compartment.

Accept all other default values and click Create. A compute instance should be provisioned in the DevTeam compartment as shown below:

### Instances in DevTeam Compartment

The [Compute service](#) helps you provision VMs and bare metal instances to meet your compute and application requirements. An [instance](#) is a compute host. Choose between virtual machines (VMs) and bare metal instances. The image that you use to launch an instance determines its operating system and other software.

| Create Instance                        |         |           |                     |            |             |                     |              |                                |
|----------------------------------------|---------|-----------|---------------------|------------|-------------|---------------------|--------------|--------------------------------|
| Name                                   | State   | Public IP | Shape               | OCPU Count | Memory (GB) | Availability domain | Fault domain | Created                        |
| <a href="#">instance-20210221-0800</a> | Running | -         | VM.Standard.E3.Flex | 1          | 16          | AD-2                | FD-1         | Sun, Feb 21, 2021, 15:06:37 UT |
| Showing 1 item < 1 of 1 >              |         |           |                     |            |             |                     |              |                                |

7.3. Try to attach the app\_datavol2 block volume created earlier to the compute instance.

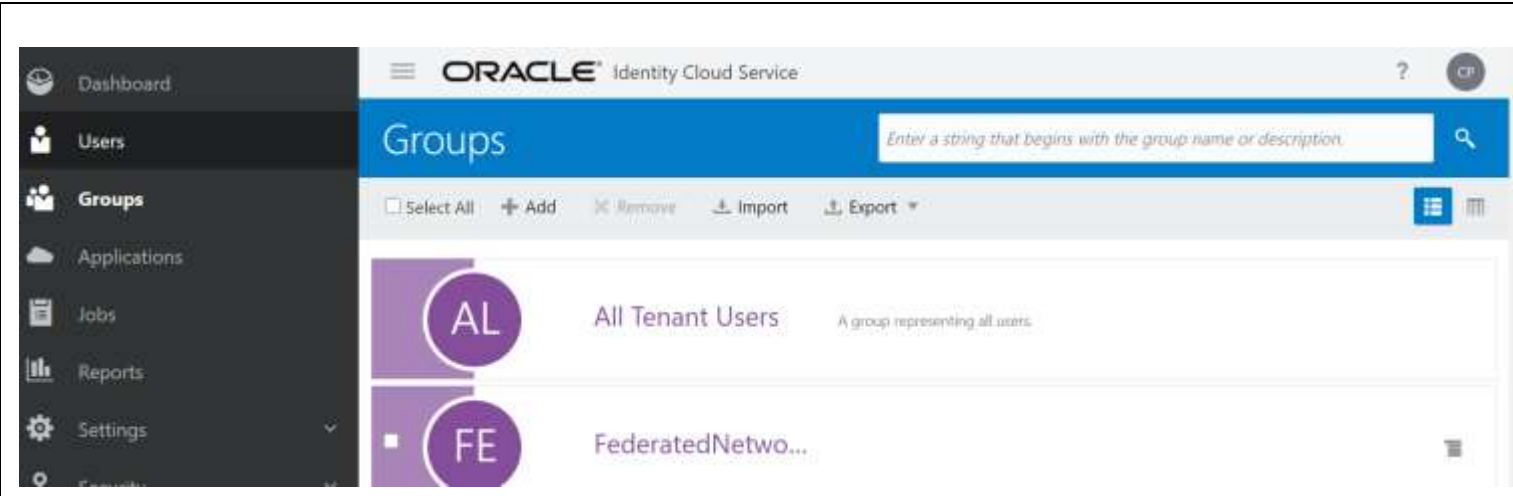
Click on the compute instance you just created, then select Attached Block Volumes under Resources.

Disregard the authorization error you may see in the OCI Console, as the Console is attempting to list block storage volumes in the DevTeam compartment, to which you do not have access.

7.4. Click Attach Block Volume

- a. Select Paravirtualized
- b. Select the app\_datavol2 from the DevTeam compartment
- c. Click Attach

|           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>8.</b> | <b>Creating Federated Users and Groups</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 8.1.      | <p>Up to this point we have created and worked with local users and groups only. OCI allows you to use federated users and groups with an external Identity Provider. Federation between an IdP and OCI allows your users to login to OCI using Single-Sign-On (SSO) with the IdP being responsible for authentication of those users.</p> <p>Users and groups are created and managed in the Identity Provider and are federated with your OCI tenancy. The federated groups are mapped to local OCI groups so that those federated users can be granted access to OCI resources through IAM policies.</p> <p>When you sign up for an Oracle cloud tenancy, you get a free Oracle Identity Cloud Service instance. This IDCS instance is automatically federated with OCI.</p> <p>In this lab you will learn how create and manage a federated user and group.</p> |
| 8.2.      | Log into the OCI Console as yourself or someone with tenancy administration privileges.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| 8.3.      | <b>Under Identity select Federation.</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| 8.4.      | <p><b>Select OracleIdentityCloudService.</b></p> <p>An identity federation with IDCS is already setup for you to use.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| 8.5.      | <p>On the OracleIdentityCloudService details page, <b>click the link for the Oracle Identity Cloud Service Console.</b></p> <p>This link will launch the login page for the IDCS console, which is a separate console from the OCI console.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| 8.6.      | <p><b>Log in using your OCI credentials.</b> You will be presented with the IDCS console.</p> <p>IDCS is a full-featured Identity Management Service from Oracle that supports federation with on-prem IdP as well as acting as an IdP itself. In this lab, IDCS is our IdP and we will create a user and group in the IdP.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| 8.7.      | In the upper left, <b>click on the stacked bars and select groups.</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |



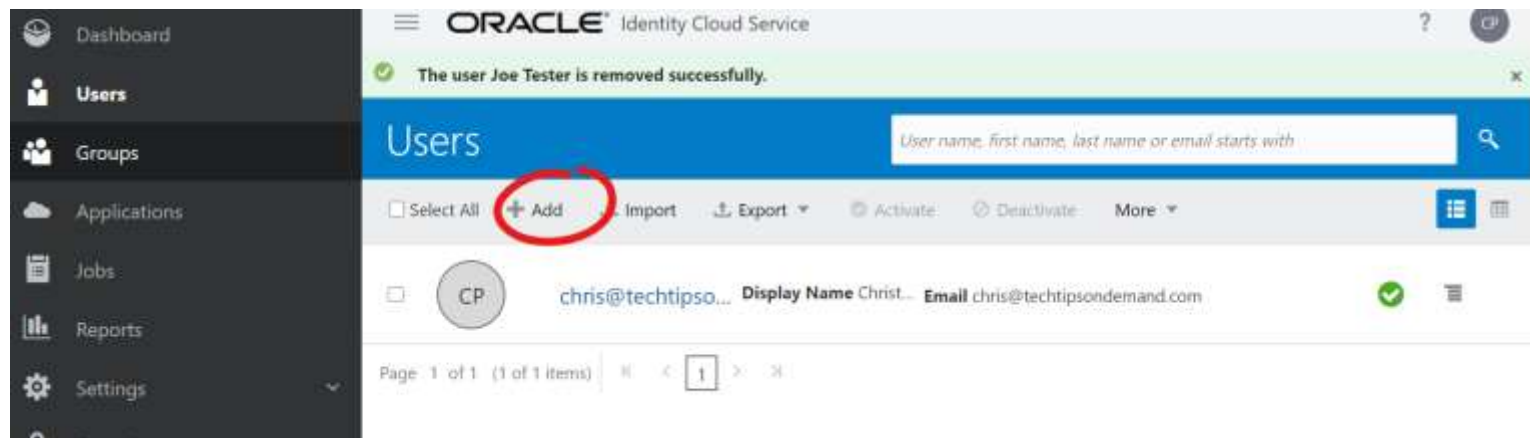
8.8. **Click the Add button to add a group, specifying the following parameters:**

Name: NetworkAdminsFederated

**Click Finish.**

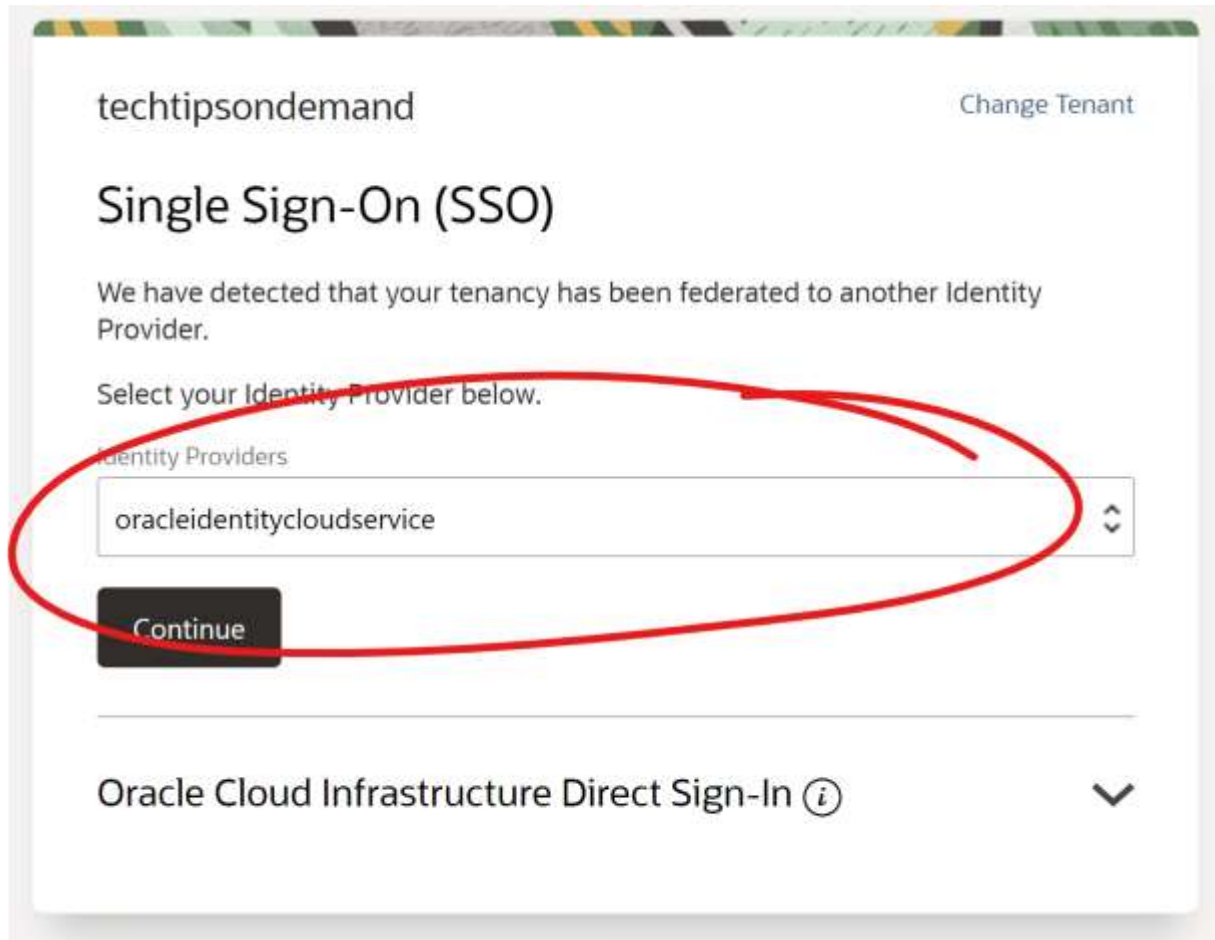


8.9. Click on Users in the left hand side then click the Add button to add a new user.



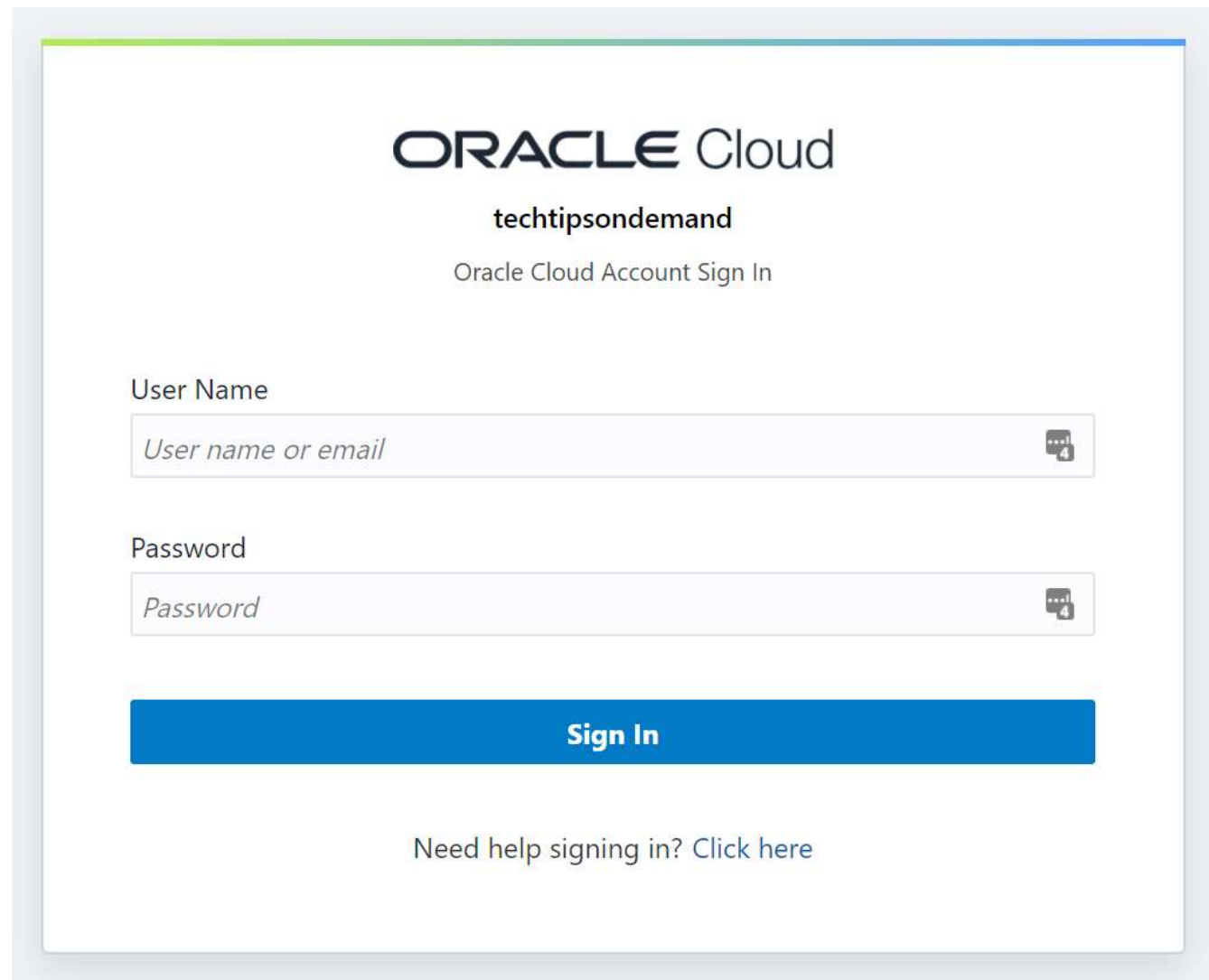
8.10. In the New User dialog, first uncheck the 'Use the email address as the user name' box enter the following information:

|       |                                                                                                                                                                                                                                                     |
|-------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       | <p>First Name: Joe<br/>Last Name: Smith<br/>Username: joe_smith<br/>Email: <i>Use your email address here. Unlike Local users, Federated users require an email address.</i></p>                                                                    |
| 8.11. | <p><b>Click Next and then select the NetworkAdminsFederated group then click Finish.</b></p> <p>IDCS will create the user and map it to the group. IDCS will also send an email with a link to activate the account and for setting a password.</p> |
| 8.12. | <p>Before activating the account, log out of both IDCS and the OCI Console.</p> <p><b>Activate the account and set a password using the link provided in the email from Oracle.</b></p>                                                             |
| 8.13. | <p><b>Now navigate back to the OCI console login page.</b></p> <p>Select the oracleidentitycloudservice Identity Provider under Single Sign-On and click Continue.</p>                                                                              |



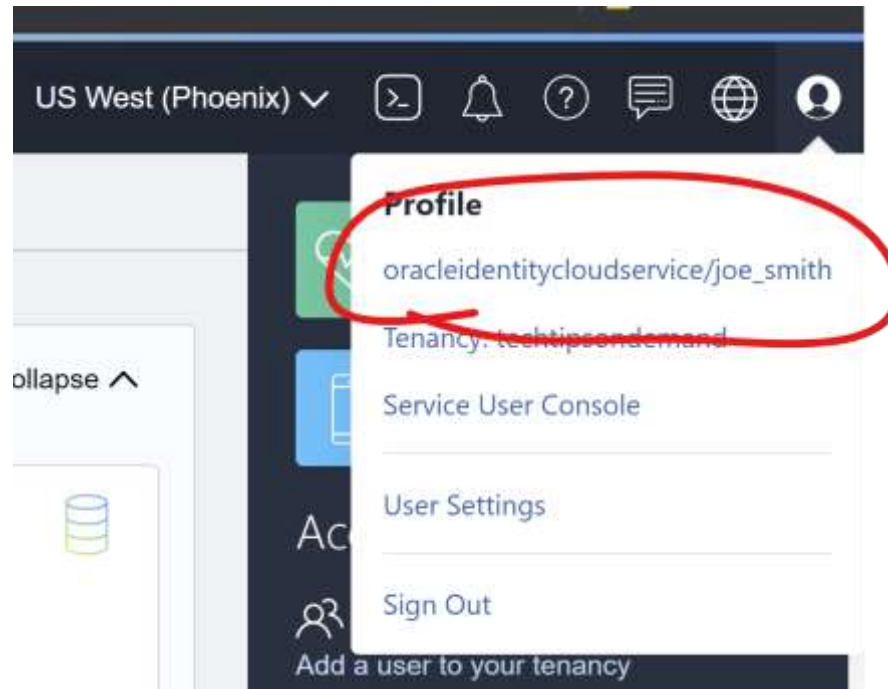
8.14. **Log in using joe\_smith as the username and the password you specified.**

You have now logged in using the joe\_smith federated account.



The screenshot shows the Oracle Cloud Account Sign In page for the 'techtipsondemand' account. The page has a clean, modern design with a light blue header and a white main content area. The Oracle Cloud logo is prominently displayed at the top, followed by the account name 'techtipsondemand' and the text 'Oracle Cloud Account Sign In'. Below this, there are two input fields: 'User Name' and 'Password'. The 'User Name' field contains the placeholder text 'User name or email' and has a small icon of a person with a plus sign. The 'Password' field contains the placeholder text 'Password' and has a small icon of a key with a plus sign. A large blue 'Sign In' button is positioned below the input fields. At the bottom of the form, there is a link that says 'Need help signing in? Click here'.

- 8.15. Once you are logged in, you can tell that you are logged in through SSO using IDCS by clicking on the profile icon in the upper right hand corner of the console. Your username will be prefixed with the name of the identity provider.



8.16. Under Profile, click on oracleidentitycloudservice/joe\_smith.

You will be taken to the user's profile page. Under Groups you will see a message stating that group membership for federated users is done by the identity provider, not by OCI.

When we created joe\_smith in IDCS, we placed him in a group called NetworkAdminsFederated. This IDCS group is also federated with OCI, so it is available for us to use in OCI.

8.17. Log out of the OCI Console and log back in as yourself or someone with tenancy admin privileges.

8.18. Navigate to Identity > Federation in the OCI Console and click on OracleIdentityCloudService.

8.19. You should see a list of federated users from IDCS.

## Users

| <a href="#">Create User</a> | <a href="#">Delete</a>                     |        |             |           |                                                                       |                                 |
|-----------------------------|--------------------------------------------|--------|-------------|-----------|-----------------------------------------------------------------------|---------------------------------|
| <input type="checkbox"/>    | Username                                   | Status | First Name  | Last Name | OCI Synched User                                                      | Created                         |
| <input type="checkbox"/>    | <a href="#">joe_smith</a>                  | Active | Joe         | Smith     | <a href="#">oracleidentitycloudservice/joe_smith</a>                  | Wed, Aug 12, 2020, 20:25:08 UTC |
| <input type="checkbox"/>    | <a href="#">chris@techtipsondemand.com</a> | Active | Christopher | Parent    | <a href="#">oracleidentitycloudservice/chris@techtipsondemand.com</a> | Fri, Aug 7, 2020, 15:25:03 UTC  |
| 0 Selected                  |                                            |        |             |           |                                                                       | Displaying 2 Users < Page 1 >   |

8.20. Click on Groups to see a list of federated groups, including NetworkAdminsFederated.

8.21. OCI allows you to use federated groups and users in IAM policies. To do this, you must map the federated group to a local OCI group.

Let's map the NetworkAdminsFederated group to the NetworkAdmins local OCI group.

- Click on Group Mappings under Resources for the OracleIdentityCloudService federation.
- Click Add Mappings and select NetworkAdminsFederated and NetworkAdmins
- Click Add Mappings again to create the mapping.

## Add Mappings

[Help](#)

Here you'll map groups defined in your Identity Provider to groups defined in Oracle Cloud Infrastructure (OCI). Each group can be mapped to one or more groups of the other kind.

Identity Provider Group

NetworkAdminsFederated



OCI Group

NetworkAdmins

[+ Another Mapping](#)[Add Mappings](#)[Cancel](#)

|       |                                                                                                                                                                                                                                                                                                                                                                         |
|-------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 8.22. | <p>The federated group is now mapped to the NetworkAdmins group and is subject to all existing IAM policies. So Joe Smith, our network admin, can log into OCI using SSO/IDCS and create and manage network resources just like a local user.</p> <p>Feel free to verify group mapping and policies work by logging in to OCI using SSO rather than Direct Sign-in.</p> |
|-------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## References

Create an Oracle Account

<https://login.oracle.com/mysso/signon.jsp>

SSH Agent Forwarding

<https://www.cloudsavvyit.com/25/what-is-ssh-agent-forwarding-and-how-do-you-use-it/>

## Appendix A : How to Access Private OCI Compute Instances using a Jump Server

To connect to a private compute instance that does not have a public IP address, you use another server to jump through that has a public IP address. This jump server, sometimes called a bastion has both a public IP address and a private IP address that is part of the VCN where the private compute instance lives. To connect to a private instance, you first ssh to the bastion using its public IP address, then jump to the private instance using the private instance's private IP.

SSH agent forwarding handles passing your private SSH key to the private instance that you are trying to connect to without having to store the private key on the bastion host.

This guide will show you how to set up SSH agent forwarding for both Windows and Linux

### SSH Agent Forwarding on Windows using PuTTY

You will need the following things before proceeding:

1. PuTTY installed
2. Pageant installed (usually comes bundled with PuTTY)
3. Private SSH keys for the bastion and private compute instance you want to connect to. This is covered in the lab on Core Compute.

#### Step 1: Load your SSH keys into Pageant

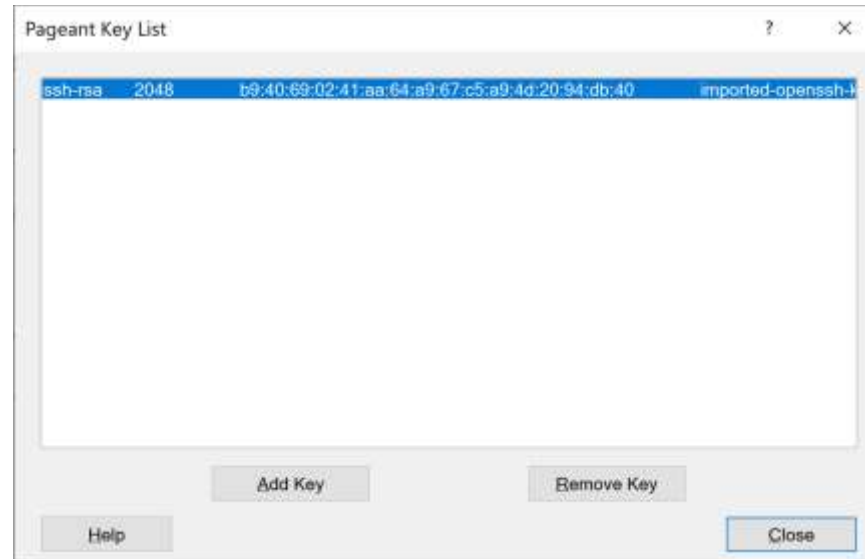
Pageant is a Putty utility that allows you to load SSH keys into memory.



- 1) Launch Paegant from the Start Menu. Paegant will appear in the system tray.



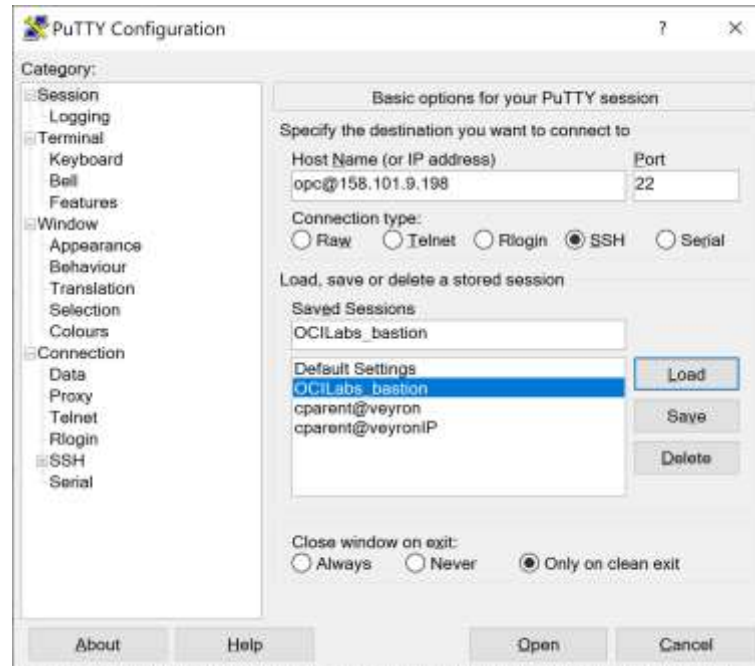
- 2) Right click on the Paegant icon and select View Keys.
- 3) Click Add Key and add any private SSH keys you need to access the bastion and the private compute instance.



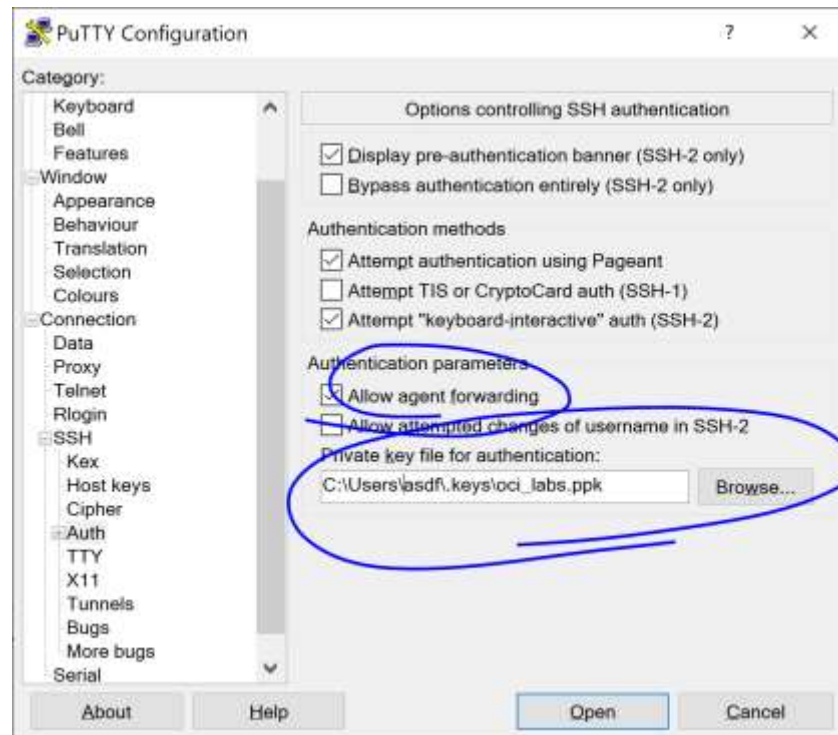
## Step 2: Configure a PuTTY Session

Next we need to configure PuTTY to forward our SSH keys to the target private compute instance by configuring SSH agent forwarding.

- 1) Launch PuTTY
- 2) Create a new session for connecting to the bastion server by specifying the username and public IP address in the Hostname field. The default username for Oracle Linux images is opc or oci. The default username for Ubuntu images is ubuntu.



- 3) Under Connections > SSH > Auth, check the box to allow agent forwarding.
- 4) On the same screen, under Private key file for authentication, specify the private key for the bastion server.



- 4) Go back to the Session category and save the session.

### Step 3: Connect to the private instance through the jump server

- 1) In PuTTY connect to the bastion server by opening the session.
- 2) Once connected to the bastion, verify that you see the message: "imported-openssh-key" from agent." This message indicates that SSH agent forwarding is working. If you do not see this message, ensure that you have configured SSH agent forwarding and loaded your SSH key into Pageant.
- 3) Once connected to the bastion, you should be able to ssh into the private compute instance using its private IP address. The username will be the default username for the type of VM image used on the compute instance (oci/opc for Oracle Linux, ubuntu for Ubuntu).

