ORACLE
University

Oracle Cloud Infrastructure Security Professional: Hands-on Workshop

Activity Guide

D1103613GC20

Learn more from Oracle University at ***education.oracle.com***

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Copyright © 2023, Oracle and/or its affiliates.

Disclaimer

This document contains proprietary information and is protected by copyright and other intellectual property laws. The document may not be modified or altered in any way. Except where your use constitutes "fair use" under copyright law, you may not use, share, download, upload, copy, print, display, perform, reproduce, publish, license, post, transmit, or distribute this document in whole or in part without the express authorization of Oracle.

The information contained in this document is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

Restricted Rights Notice

If this documentation is delivered to the United States Government or anyone using the documentation on behalf of the United States Government, the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software" or "commercial computer software documentation" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

Trademark Notice

Oracle®, Java, MySQL, and NetSuite are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

Third-Party Content, Products, and Services Disclaimer

This documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

2009262023

Ramanivas Sangwal (ramaniwas@gmail.com) has a non-transferable license to use this Student Guide

Table of Contents

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Nivas Sangwan (ram.nivas@tseprou.com) has a non-transferable license to use this Guide

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Ilwas Gangwan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Copyright © 2023, Oracle and/or its affiliates.

Ram Niwas Sangwan (ram.niwas@tseeod.com) has a non-transferable license to use this Guide.

Ram Nivas Sarovar (ram.nivas@tseeout.com) has a non-transferable license to use this Guide

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Identity and Access Management: Enable Multi-Factor Authentication

Lab 1 Practices

Ram Niwas Sangwan (ram.niwas@oracle.com) has a non-transferable license to use this Guide.

Get Started

Overview

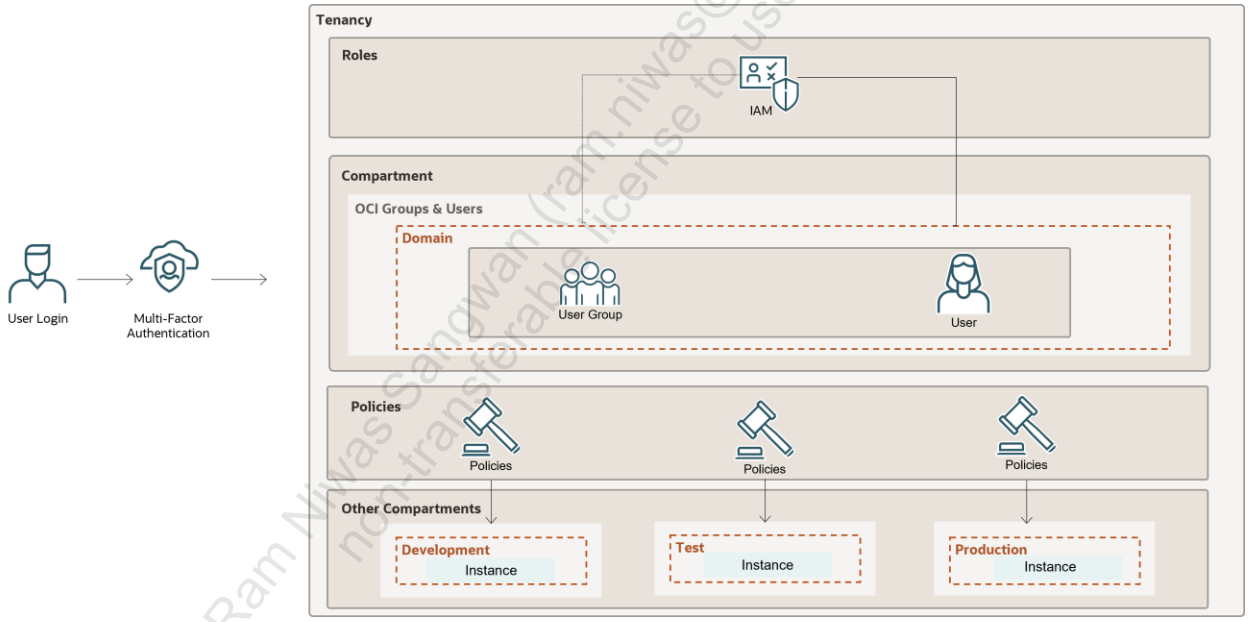
Multi-Factor Authentication (MFA) is a method of authentication that requires the use of more than one factor to verify a user's identity.

With MFA enabled in the IAM service, a user signing in to the Oracle Cloud Infrastructure (OCI) console is prompted to enter two factors:

- Their username and password, which are things that they *know*
- A verification code from a registered MFA device, which is something that they have

The two factors work together, requiring an extra layer of security to verify the user's identity and complete the sign-in process.

In this lab, you'll enable Multi-Factor Authentication in OCI.



Prerequisites

- The required IAM policies have been implemented.
- You must install a supported authenticator app (Oracle Mobile Authenticator or Google Authenticator) on the mobile device you intend to register for MFA.

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Niwas Sangwan (ram.niwas@ceedu.com) has a non-transferable license to use this Guide.

Enable Multi-Factor Authentication

You will learn how to enable Multi-Factor Authentication (MFA) for your Oracle Cloud Infrastructure (OCI) account.

You will also learn the sign-in process after enabling MFA.

Tasks

1. Sign-in to the Oracle Cloud Infrastructure (OCI) Console by using the Direct Sign-In method.

   Note: If the Customize Your Console pop-up window appears, select the profiles that best describe your Oracle Cloud Infrastructure work or interests.

2. In the console ribbon at the top of the screen, click the **Profile** icon and click the *<username>* with which you logged in to the OCI Console.

3. On the user details page, click **Enable Multi-Factor Authentication** to open a dialog box.

4. Follow the instructions listed in the dialog box:

   a. Install Oracle Mobile Authenticator or a similar authenticator app on your mobile device**.**

   a. Open the app and add a new account. Scan the QR code from the dialog box when prompted.

   b. Enter the code displayed by the app.

5. Once you've entered the code into the Verification Code box, click **Verify.** Multi-Factor Authentication is now enabled.

6. Click the **Profile** icon at the top of the screen and click **Sign out.**

Ram Nivas Sangwan (ram.nivas@tsedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

7. Sign-in to your Oracle Cloud Infrastructure (OCI) Console by using the Direct Sign-In method:

    a. Enter *<your username>* in the **User Name** field.

    b. Enter *<your password>* in the **Password** field.

    c. Click **Sign In**.

    Note: After your username and password are authenticated, you have successfully supplied the first factor for authentication. The second factor appears on an authentication page and prompts you to enter a one-time passcode.

8. Open the Oracle Mobile Authenticator app on your registered mobile device and then open the account for your Oracle Cloud Infrastructure (OCI) tenancy.

9. Enter the passcode displayed by your authenticator app and then click **Sign In**. You are now successfully signed in to the OCI Console.

    Important: The authenticator app generates a new time-based, one-time passcode every 30 seconds. You must enter a code while the code is still valid. If you miss the time window for one passcode, you can enter the next one that is generated.

Ram Niwas Sangwan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Infrastructure Security - Network: Create and Configure a VCN and Web Server Instance in Public Subnet

Lab 3 Practices

Ram Niwas Sangwan (ramniwas@ts.edu.com) has a non-transferable license to use this Guide.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Get Started

Overview

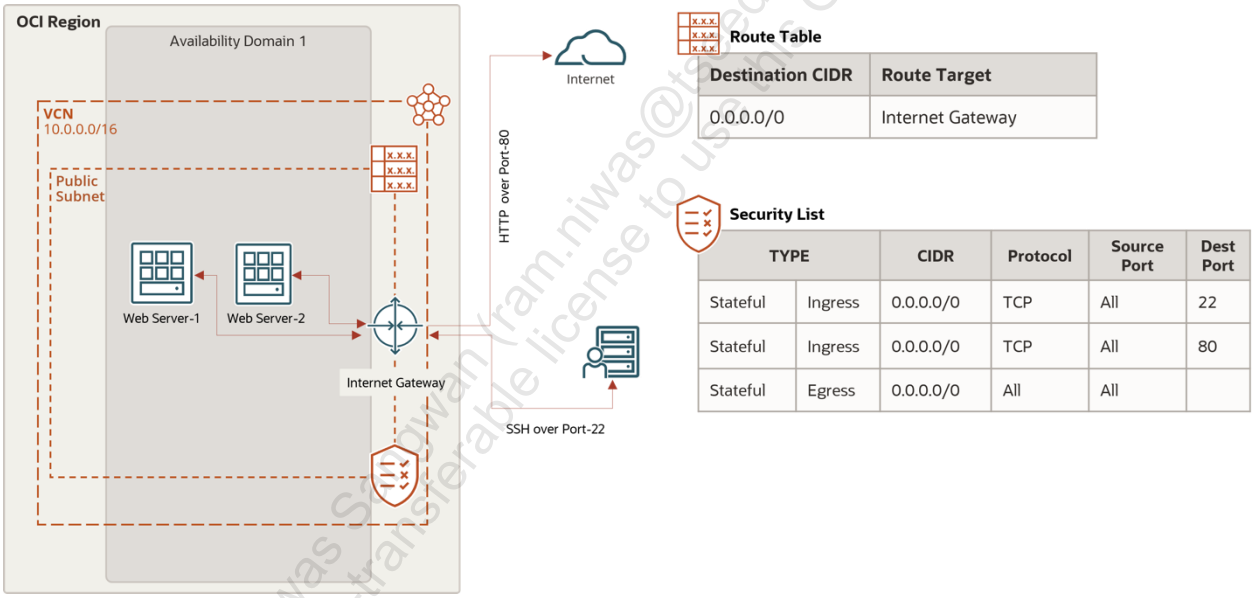
Oracle Cloud Infrastructure Compute lets you provision and manage compute hosts, known as instances. You can launch instances as needed to meet your compute and application requirements.

In this lab, you will:

a. Create and configure a Virtual Cloud Network

b. Create SSH keys using Oracle Cloud Shell

c. Create two compute instances and install the web server



Route Table

Destination CIDR	Route Target
0.0.0.0/0	Internet Gateway

Security List

TYPE		CIDR	Protocol	Source Port	Dest Port
Stateful	Ingress	0.0.0.0/0	TCP	All	22
Stateful	Ingress	0.0.0.0/0	TCP	All	80
Stateful	Egress	0.0.0.0/0	All	All	

Ram Niwas Sagwan (ram.niwas@tcs.edu.com) has a non-transferable license to use this Guide.

Prerequisites

- The required IAM policies have been implemented.
- You must have access to the OCI Console.

Assumptions

- Select the region that's available in the tenancy allotted to you. In this lab, we are considering US East (Ashburn) (IAD) as your region.
- You must be familiar with navigating the OCI Console.

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Create and Configure a Virtual Cloud Network

You will learn how to create a Virtual Cloud Network in OCI with a public and a private subnet using the VCN Wizard. The compute instance that you will create later will be hosted in this VCN's public subnet.

Tasks

1. Sign in to your Oracle Cloud Infrastructure (OCI) account.
2. From the navigation menu, select **Networking**, then click **Virtual Cloud Network**.
3. In the left navigation pane, under List Scope, select *<your assigned compartment>* from drop-down menu.
4. Click **Start VCN Wizard.**
5. Select **Create VCN with Internet Connectivity** and click **Start VCN Wizard.**
6. On the Configuration page, enter the following details:
   - **Name**: `IAD-SP-LAB03-1-VCN-01`
   - **Compartment:** Select *<your assigned compartment>*

   Note: Leave all the other options in their default setting.
7. Click **Next.**
8. Verify the details on the **Review and Create** page.
9. Click **Create** to start creating the VCN and its resources and wait for the VCN Wizard to successfully complete the VCN creation.
10. Click **View Virtual Cloud Network** to verify the creation of the VCN and its resources.

Ram Nivas Sungwan (ram.niwas@tceedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

You can now see that the VCN was successfully created and is in the Available state, with the following components:

- VCN
- Public subnet
- Private subnet
- Internet gateway
- NAT gateway
- Service gateway

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Niwas Sangwan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

Create SSH Keys Using Oracle Cloud Shell

You will learn how to create Secure Shell (SSH) keys using Cloud Shell. The SSH protocol is a method for secure remote login from one computer to another.

Tasks

1. In the console ribbon at the top of the screen, click the **Cloud Shell** icon next to the Region selection menu.

2. After the Cloud Shell is ready, enter the following commands. Choose the key name you can remember. This will be the key name you will use to connect to any compute instances you create. Press Enter twice for no passphrase.

   ```
   $ mkdir .ssh
   $ cd .ssh
   $ ssh-keygen -b 2048 -t rsa -f <<sshkeyname>>
   ```

   Note: Replace `<<sshkeyname>>` with `ociseclabkey`.

   Reminder: The angle brackets `<< >>` should not appear in your code.

3. Examine the two files that you just created using the following command:

   ```
   $ ls
   ```

   Note: In the output, there are two files, **a private key:** `<<sshkeyname>>`**and a public key:** `<<sshkeyname>>`**.pub**, keep the private key safe and don't share its content with anyone. The public key will be needed for various activities and can be uploaded to certain systems as well as copied and pasted to facilitate secure communications in the cloud.

4. To list the contents of the public key, use the following command:

   ```
   $ cat <<sshkeyname>>.pub
   ```

   Note: Replace `<<sshkeyname>>` with `ociseclabkey`.

   Note: Make a note of the public key as you will need this in a subsequent step. When pasting the key into the compute instance, make sure that you remove any hard returns that may have been added when copying. The `.pub` key should be one line.

Ram Nivas Sangwan (ram.niwas@seedu.com) has a non-transferable license to use this Guide.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Create Two Compute Instances and Install the Web Server

You will provision two compute instances, install an Apache Web server, and connect to it over the public Internet.

Task-1

1. From the navigation menu, select **Compute**, and then click **Instances**.
2. In the left navigation pane, under List Scope, select *<your assigned compartment>* from the drop-down menu.
3. Click **Create Instance**. In the Create Instance dialog box, provide the following details:
   - **Name:** IAD-SP-LAB03-1-VM-01
   - **Create in compartment**: Select your *<assigned compartment>*.
   - **Placement:** Select Availability Domain AD1.

     Note: If Service limit error is displayed, choose a different Availability Domain.
   - **Image**: Ensure that the Oracle Linux 8 image is selected.
   - **Shape:** Click **Change shape**, then in the **Shape** field, click **Change Shape**. Then, select **Ampere shape series** field and select the **VM.Standard.A1.Flex** shape with **1** OCPU and **6 GB** memory**.**
   - **Networking:** Pick your VCN **IAD-SP-LAB03-1-VCN-01** and Public Subnet.
   - **Public IP address**: Select a public IPv4 address.
   - **Add SSH Keys**: Choose **Paste public Keys** and paste the public key from the `ociseclabkey.pub` file you created in Cloud Shell. Ensure that the public key is pasted in one line.
4. **Click Create.**

   Note: After a couple of minutes, you can see that the Instance is successfully created, and the state is Running.
5. Under Instance access, copy the Public IP address value to notepad. We refer to this IP address as VM-01-Public IP address later in this practice.
6. Repeat steps 1 - 5 to launch a second compute instance with the name `IAD-SP-LAB03-1-VM-02`.

Ram Nivas Sharma (ram.nivas@tseedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

7. After the second instance `IAD-SP-LAB03-1-VM-02` is in Running state, under Instance access, copy the Public IP address value to Notepad. We refer to this as VM-02-Public IP address later in this practice.

8. Click the **Cloud Shell** icon to open Cloud Shell, and use SSH to log in to your instance, `IAD-SP-LAB03-1-VM-01` by using the following command:

   ```
   $ ssh -i <private_key_file> <username>@<public-ip-address of VM-01>
   ```

   Reminders:

   - `<private_key_file>` is the full path and name of the file that contains the private key associated with the instance you want to access.
   - `<username>` is the default user `opc`.
   - `<public-ip-address>` is the Public IP address of the instance. In our case, we refer to it as VM-01-Public IP or VM-02-Public IP.

     Note: Enter **yes** in response to "Are you sure you want to continue connecting (yes/no)?"

     You are now connected to the instance `IAD-SP-LAB03-1-VM-01`.

9. While connected to your compute instance via SSH, run the following commands to install and configure Apache Web server:

   - Install Apache Server:

     ```
     $ sudo yum -y install httpd
     ```

   - Enable Apache and start Apache server:

     ```
     $ sudo systemctl enable httpd
     $ sudo systemctl restart httpd
     ```

   - Create a firewall rule to enable HTTP connection through port 80 and reload the firewall:

     ```
     $ sudo firewall-cmd --permanent --add-port=80/tcp
     $ sudo firewall-cmd --reload
     ```

   - Create an index file for your web server:

     ```
     $ sudo bash -c 'echo You are visiting Web Server 1 >> /var/www/html/index.html'
     ```

   - Exit the SSH connection:

     ```
     $ exit
     ```

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Nivas Sangwan (ram.niwas@tsedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

10. Again, use Cloud Shell to SSH in to second instance, `IAD-SP-LAB03-1-VM-02` by using the following command:

```
$ ssh -i <private_key_file> <username>@<public-ip-address of VM-02>
```

Note: Enter **yes** in response to "Are you sure you want to continue connecting (yes/no)?"

11. Repeat step 9 to install Apache Web server on second compute instance.

Note: Make sure that the index file command for the second web server looks like this:

```
$ sudo bash -c 'echo You are visiting Web Server 2 >> /var/www/html/index.html'
```

12. After executing all the commands successfully, open a browser in your local system and enter the URL `http://<Public IP of IAD-SP-LAB03-VM-01 >`

Note: Because port 80 traffic is not yet open in the Security Lists, your browser will return nothing.

Task-2

Configure the security list to allow http protocol and port 80 traffic to the web server's VNIC.

1. From the navigation menu, select **Networking**, and then click **Virtual Cloud Network**.
2. Click the **VCN** you created - **`IAD-SP-LAB03-1-VCN-01`** in your assigned compartment.
3. In the left navigation pane, under Resources, click **Security Lists**.
4. Click **Default Security List** for IAD-SP-LAB03-1-VCN-01 from the list of security lists.
5. Click **Add Ingress Rules** and enter the following:
   - **Do not select the Stateless check box.**
   - **Source Type:** `CIDR`
   - **Source CIDR:** `0.0.0.0/0`
   - **IP Protocol: Select** `TCP`
   - **Source Port Range:** `All`
   - **Destination Port Range: Enter** `80`**.**
6. **Click Add Ingress Rules.**

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Nivas Sengwar (ram.nivas@tseedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

Task-3

Verify that you can access the web server from the public Internet.

1. Enter the URL into the browser on your local system.

   URL: `http://<Public IP of IAD-SP-LAB03-1-VM-01 >`

   The browser will display the index page of the first webserver.

   ```
   You are visiting Web Server 1
   ```

2. Verify that you can also access second web server by entering the URL:

   `http://<Public IP of IAD-SP-LAB03-1-VM-01 >`

   The browser will display the index page of the second web server.

   ```
   You are visiting Web Server 2
   ```

Congratulations! You have created a VCN, two compute instances, and installed Apache Web servers.

Ram Niwas Sangwan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Copyright © 2023, Oracle and/or its affiliates.

Purge Instructions

Perform the purge operations, as instructed below, before proceeding to the next practice.

Delete Compute Instance

1. From the navigation menu, select **Instances** under Compute.
2. Ensure that you are in the same Compartment as the **Instance** you created.
3. Locate the first Compute Instance and click its name.
4. Click **Terminate**. Ensure you select **Permanently delete the attached Boot Volume**, and then click **Terminate Instance**.
5. Repeat steps 1 through 4 to terminate all the Compute Instances. Once the instances are terminated, the color changes from yellow to grey. Wait for both instances termination to be completed.

Delete VCN

1. Open the navigation menu, click **Virtual Cloud Networks** under Networking.
2. Ensure that you are in the same Compartment as the VCN you created.
3. Click the name of your VCN.
4. Click **Delete.**

   Note: You must delete all resources associated with a VCN, before deleting it.
   - When you click **Delete**, a message box appears. Select the **Specific compartment** check box to search the compartments for resources associated with this VCN, and click **Scan**.
   - Wait for the Scan operation to complete.
5. Click Delete All.
6. Click **Close** after **VCN** is deleted.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Nivas Sangwan (ram.nivas@tcs.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Infrastructure Security - Network: Create and Configure Security List and Network Security Group

Lab 4 Practices

Ram Niwas Sangwan (ram.niwas@ts.edu.com) has a non-transferable license to use this Guide.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Get Started

Overview

You will create and configure a security list and network security group (NSG).
The Networking service offers two virtual firewall features to control traffic at the packet level:

- **Security lists:** Original type of virtual firewall offered by the Networking service
- **Network security groups:** Another type of virtual firewall that Oracle recommends over security lists

A security list acts as a virtual firewall for an instance, with ingress and egress rules that specify the types of traffic allowed in and out. Each security list is enforced at the VNIC level. However, you configure your security lists at the subnet level, which means that all VNICs in a given subnet are subject to the same set of security lists. The security lists apply to a given VNIC whether it's communicating with another instance in the Virtual Cloud Network (VCN) or a host outside the VCN.

Network security groups act as a virtual firewall for your compute instances and other kinds of resources. An NSG consists of a set of ingress and egress security rules that apply only to a set of VNICs of your choice in a single VCN (for example, all the compute instances that act as web servers in the web tier of a multi-tier application in your VCN).

In this lab, you will:

a. Create a Virtual Cloud Network (VCN) and its components

b. Create two VM instances

c. Create a security list to enable SSH

d. Establish an SSH connection to the compute instance

e. Create a network security group to allow ICMP

f. Test the network security group configuration

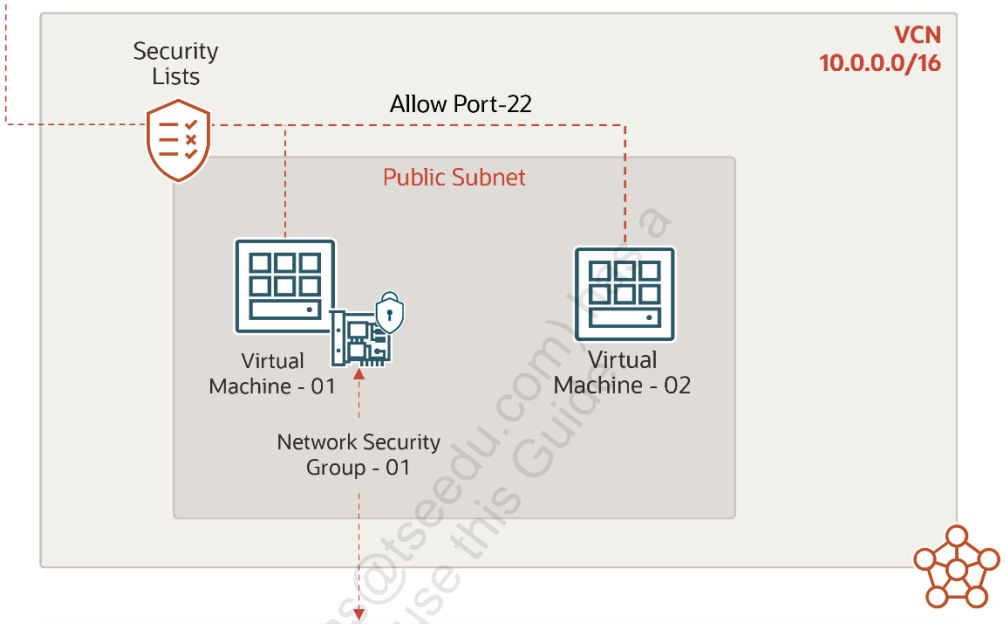
Ram Nivas Sangwan (ram.nivas@tseelu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Allow SSH to all VMs in subnet

TYPE	Direction	CIDR	Protocol	Source Port	Dest Port
Stateful	Ingress	0.0.0.0/0	TCP	All	22
Stateful	Egress	0.0.0.0/0	All	All	All



Allow ICMP on VM - 01

	TYPE	Direction	CIDR	Protocol	Source Port	Dest Port
NSG01	Stateful	Ingress	0.0.0.0/0	ICMP	All	All

Prerequisites

- You must have access to the OCI Console.
- The Oracle University lab team has set up all the IAM policies required for you to complete this lab.

Assumptions

- Select the region that's available in the tenancy allotted to you. In this lab, we are considering US East (Ashburn) (IAD) as your region.
- You must be familiar with navigating the OCI Console.

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Create a Virtual Cloud Network and Its Components

You will learn how to create a Virtual Cloud Network, Subnet, and Internet Gateway, and add route rules in the Route Table.

Tasks

1. Sign in to your Oracle Cloud Infrastructure (OCI) account.
2. From the navigation menu, select **Networking**, and then click **Virtual Cloud Network**.
3. In the left navigation pane, under **List Scope**, select the assigned **compartment** from drop-down menu.
4. Click **Create VCN.**

   Enter the following:
   - **Name:** `IAD-SP-LAB04-1-VCN-01`
   - **Create in Compartment:** Select the <*compartment name*> assigned to you
   - **IPv4 CIDR Blocks:** `10.0.0.0/16`
   - Press **Enter** to add.

   Note: Leave all the other options in their default setting.
5. Click **Create VCN**.

   You now see that the VCN is created successfully and in the Available state.
6. Click **Create Subnet**.
7. In the Create Subnet dialog box, enter the following:
   - **Name:** IAD-SP-LAB04-1-SNET-01
   - **Create in Compartment:** Select the <*compartment name*> assigned to you.
   - **Subnet Type:** Regional (Recommended)
   - **IPv4 CIDR Block:** 10.0.1.0/24
   - **Subnet Access:** Public Subnet

   Note: Leave all the other options in their default setting.
8. Click **Create Subnet.**

   You now see that the public subnet is created successfully and in the Available state.

Copyright © 2023, Oracle and/or its affiliates.

9. In the left navigation pane, under **Resources**, click **Internet Gateways.**

10. Click **Create Internet Gateway**.

11. Enter the following:

    - **Name:** IAD-SP-LAB04-1-IGW-01
    - **Create in Compartment:** Select <your *compartment name*>.

12. Click **Create Internet Gateway.**

    You now see that the Internet Gateway is created successfully and in the Available state.

13. In the left navigation pane, under Resources, click **Route Tables.**

14. Click to open **Default Route Table for IAD-SP-LAB04-1-VCN-01**.

15. Click **Add Route Rules** and enter the following:
    - **Target Type:** Internet Gateway
    - **Destination CIDR Block:** 0.0.0.0/0
    - **Target Internet Gateway:** IAD-SP-LAB04-1-IGW-01

16. Click **Add Route Rules**.

    You now see that the route rule is successfully added in the default Route Table.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Niwas Sangwan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

Create SSH Keys by Using Oracle Cloud Shell

In this practice, you will learn how to create SSH (Secure Shell) keys using Cloud Shell. The SSH protocol is a method for secure remote login from one computer to another. SSH keys are an important part of securely accessing Oracle Cloud Infrastructure compute instances in the cloud.

Note: Note that you can skip this step if you have already created SSH keys in earlier practice and they are available.

Tasks

1. In the console ribbon at the top of the screen, click the **Cloud Shell** icon next to the Region selection menu.

2. After the cloud shell is ready, enter the following commands. Choose the key name you can remember. This will be the key name you will use to connect to any compute instances you create. Press Enter twice for no passphrase.

   ```
   $ mkdir .ssh
   $ cd .ssh
   $ ssh-keygen -b 2048 -t rsa -f <<sshkeyname>>
   ```

   Note: Replace `<<sshkeyname>>` with `ociseclabkey`.

   Reminder: The angle brackets `<< >>` should not appear in your code.

   Reminder: Do not include the `$` symbol when pasting code into Cloud Shell.

3. Examine the two files that you just created by using the following command:

   ```
   $ ls
   ```

   Note: In the output, there are two files, **a private key:** `<<sshkeyname>>`**and a public key:** `<<sshkeyname>>`**.pub**. Keep the private key safe and don't share its content with anyone. The public key will be needed for various activities and can be uploaded to certain systems as well as copied and pasted to facilitate secure communications in the cloud.

4. To list the contents of the public key, use the following command:

   ```
   $ cat <<sshkeyname>>.pub
   ```

   Note: Replace `<<sshkeyname>>` with `ociseclabkey`.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Copyright © 2023, Oracle and/or its affiliates.

Copy the contents of the public key to a Notepad as you will need this in a subsequent step. When pasting the key into the compute instance, make sure that you remove any hard returns that may have been added when copying. The `.pub` key should be one line.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Niwas Sangwan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

Create Two Compute Instances

You will provision two compute instances.

Note: Note that you can skip this step if you already have two compute instances in a public subnet created in earlier practice and they are available.

Tasks

1. From the navigation menu, select **Compute**, and then click **Instances**.
2. In the left navigation pane, under **List Scope**, select the assigned **compartment** from the drop-down menu.
3. Click **Create Instance**. In the Create Instance dialog box, provide the following details:
   - **Name**: `IAD-SP-LAB04-1-VM-01`
   - **Create in compartment**: Select the <*compartment name*> assigned to you.
   - **Placement:** Availability Domain AD1

   Note: If Service limit error is displayed, choose a different Availability Domain.
   - **Image**: Select the image Oracle Linux 8.
   - **Shape:** Click **Change shape**, then in the **Shape** field, click **Change Shape**. Then, select **Ampere shape series** field and select the **VM.Standard.A1.Flex** shape with **1** OCPU and **6 GB** memory**.**
   - **Networking**: Pick your VCN **IAD-SP-LAB04-1-VCN-01** and public subnet.
   - **Public IP address**: Assign a public IPv4 address.
   - **Add SSH Keys**: Choose **Paste public Keys** and paste the public key you created in Cloud Shell.

   Note: Ensure you are pasting the key in one line.
4. Click **Create.**

   Note: After a couple of minutes, you can see that the Instance is successfully created, and the state is Running.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Niwas Sangwan (ramniwas@ieee.org) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

5. Under **Instance access**, copy the **Public IP address** value to notepad. We refer to it as **VM-01-Public IP** address.

6. Repeat steps 1 - 5 to launch a **second** compute instance with name `IAD-SP-LAB04-1-VM-02`.

Note: Keep a note of the Public IP addresses of both the compute instances.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Niwas Sangwan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Create a Security List to Enable SSH on Port 22

You will create a security list that enables SSH on port 22, and then attach it to the public subnet. This rule allows SSH access to all compute instances in a subnet.

Tasks

1. From the navigation menu, select **Networking**, and then click **Virtual Cloud Network**.
2. In the left navigation pane, under **List Scope**, select the assigned **compartment** from the drop-down menu.
3. Select **IAD-SP-LAB04-1-VCN-01** from the list of VCNs .
4. In the left navigation pane, under Resources, click **Security Lists.**
5. Click **Create Security List**.
6. In the Create Security List dialog box, enter the following:
   - **Name**: `IAD-SP-LAB04-1-SL-01`
   - **Create In Compartment**: Select <*your compartment name*>.
   - Do not add any Ingress or Egress rules.
7. Click **Create Security List**.

   You now see that the security list is created and displayed on the **Security Lists** page.
8. Select **IAD-SP-LAB04-1-SL-01** from the list of security lists.
9. In the left navigation pane, under **Resources**, click **Ingress Rules**.
10. Click **Add Ingress Rules** and enter the following:
    - Do not select the **Stateless** check box.
    - **Source Type**: `CIDR`
    - **Source CIDR**: `0.0.0.0/0`
    - **IP Protocol**: `TCP`
    - **Source Port Range**: `All`
    - **Destination Port Range**: `22 (the listener port for SSH)`
11. Click **Add Ingress Rules.**

    You now see that the ingress rule is successfully added in the security list.

Ram Nivas Sangwan (ramnivas@seedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

12. In the left navigation pane, under Resources, click **Egress Rules**.

13. Click **Add Egress Rules** and enter the following:
    - Do not select the **Stateless** check box.
    - **Destination Type**: `CIDR`
    - **Destination CIDR**: `0.0.0.0/0`
    - **IP Protocol**: `TCP`
    - **Source Port Range**: `All`
    - **Destination Port Range**: `All`

14. Click **Add Egress Rules.**

    You now see that the egress rule is successfully added to the security list.

    Note: As of now, Public Subnet IAD-SP-LAB04-1-SNET-01 is using the default security list. Change the security list for Public Subnet IAD-SP-LAB04-1-SNET-01.

15. From the navigation menu, select **Networking**, and then click **Virtual Cloud Networks**. Click **IAD-SP-LAB04-1-VCN-01** to display its details.

16. In the left navigation pane, under **Resources**, click **Subnets**.

17. Locate and click **IAD-SP-LAB04-1-SNET-01**.

18. In the left navigation pane, under **Resources**, click **Security Lists**.

19. To add a security list, click **Add Security List**.

20. In the **Add Security List** dialog box, provide the following details:
    - **Security List Compartment**: Select the <*compartment name*> assigned to you.
    - **Security List**: `IAD-SP-LAB04-1-SL-01`

21. Click **Add Security List**.

22. To remove the default security list, **Default Security List for IAD-SP-LAB04-1-VCN-01**, click the **three dots** on the right to open the Actions menu, and then click **Remove**.

23. Click **Remove** when prompted to confirm removal.

    Note: The changes take effect within a few seconds.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Nivas Sadagopan (ramnivas@tsedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Establish an SSH Connection to the Compute Instance

You will verify the security list configuration that is attached to the public subnet. You'll see that all compute instances belonging to the public subnet allow SSH connections.

Tasks

1. From the navigation menu, select **Compute**, and then click **Instances**.
2. Select the assigned compartment from drop-down menu on the left part of the screen under **List Scope**.
3. Ensure instances are in **Running** state and note down its public IP address:

   Public addresses of IAD-SP-LAB04-1-VM-01 and IAD-SP-LAB04-1-VM-02
4. Click the **Cloud Shell** icon to open Cloud Shell, and use SSH to log in to your instance, `IAD-SP-LAB04-1-VM-01` by using the following command:

   ```
   $ ssh -i <private_key_file> <username>@<public-ip-address of VM-01>
   ```

   Reminders:

   - `<private_key_file>` is the full path and name of the file that contains the private key associated with the instance you want to access.
   - `<username>` is the default user `opc`.
   - `<public-ip-address>` is the Public IP address of the instance. In our case, we refer to it as VM-01-Public IP and VM-02-Public IP.

     Note: Enter **yes** in response to "Are you sure you want to continue connecting (yes/no)?"

   Verify that the opc@<COMPUTE_INSTANCE_NAME> appears on the prompt. You are now connected to the instance `IAD-SP-LAB04-1-VM-01`.
5. Once connected and verified, enter the following command to close the SSH connection:

   ```
   $ exit
   ```
6. Repeat steps 1 through 5 for second compute instance IAD–SP–LAB04-1–VM–02. Verify that the SSH connection is successful for each instance created. This ensures that the security list associated with the public subnet has permitted SSH connection over TCP port 22.

Ram Jiwas Sangwan (ram.niwas@outlook.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

Create a Network Security Group (NSG) to Allow ICMP

You will create a network security group that will enable ICMP ping packets and then attach it to a specific compute instance in a public subnet.

Task-1

1. From the navigation menu, select **Networking**, and then click **Virtual Cloud Networks**.
2. In the left navigation pane, under **List Scope**, select the assigned **compartment** from drop-down menu.
3. Click **IAD-SP-LAB04-1-VCN-01** from the list of VCNs.
4. In the left navigation pane, under **Resources**, click **Network Security Group.**
5. Click **Create Network Security Group**.
6. In the **Create Network Security Group** dialog box, enter the following:
   - **Name**: `IAD-SP-LAB04-1-NSG-01`
   - **Create In Compartment**: Select the <*compartment name*> assigned to you.
   - Click **Next**.
7. In the **Add Security Rules** dialog box, provide the following details:
   - **Direction**: `Ingress`
   - **Source Type**: `CIDR`
   - **Source CIDR**: Enter `0.0.0.0/0`.
   - **IP Protocol**: Select `ICMP`
   - **Type**: `All`
   - **Code**: `All`
8. Click **Create**.

   You now see that the NSG rule is successfully created.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Niwas Gangwan (ram.niwas@seedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Task-2

Add the VNIC of a compute instance to network security group.

1. From the navigation menu, select **Compute**, and then click **Instances**.
2. In the left navigation pane, under **List Scope**, select the assigned **compartment** from the drop-down menu.
3. Click **IAD-SP-LAB04-1-VM-01** from list of instances.
4. Navigate to **Primary VNIC** on the Instance information tab.
5. Next to **Network Security Groups**, click **Edit**.
6. In the **Edit Network Security Group** dialog box:
   - Select IAD-SP-LAB04-NSG-01.

   Note: This is the network security group you created earlier from the drop-down menu.
   - Click **Save Changes**.
7. Verify that the network security group is updated under Primary VNIC.

Ram Niwas Sangwan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

Test the Network Security Group Configuration

You will verify the network security group configuration that is attached to a VM-01 compute instance. Ping both the compute instances and evaluate the results.

Tasks

1. From the navigation menu, select **Compute**, and then click **Instances**.
2. Select the assigned compartment from the drop-down menu on the left of the screen under **List Scope**.
3. Ensure that instances are in **Running** state and note down the public IP address of IAD-SP-LAB04-1-VM-01 and IAD-SP-LAB04-1-VM-02.
4. Open the terminal (Linux/Mac) or command prompt (Windows) on your host computer.
5. Enter the following commands:

   ```
   $ ping <PUBLIC_IP_OF_COMPUTE_VM-01>
   ```

   Example:

   ```
   $ ping 8.8.8.8
   ```

   You'll observe that only VM-01 receive a successful ICMP ping reply. Since NSG is attached to the VNIC of the VM-01 compute instance, ICMP packets are permitted.

6. Try pinging the VM-02 compute instance:

   ```
   $ ping <PUBLIC_IP_OF_COMPUTE_VM-02>
   ```

   You'll see that only VM-02 failed to receive a response to an ICMP ping.

   At the level of VNICs, NSG has provided more granular security.

   Note: Security Lists act as virtual firewalls for compute instances and other resources. A security is a set of ingress and egress security rules that apply to all VNICs in any subnet with which the security list is associated. That is, all VNICs in each subnet are subject to the same set of security lists.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Nivas Sangwan (ram.niwas@tseetu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

Note: Network security groups (NSGs) allow you to specify a set of security rules that apply to a group of VNICs (or the parent resources of the VNICs, such as compute instance, load balancers or DB systems), for example, VNICs belonging to a group of compute instances with the same security posture. To use a particular NSG, add the VNICs of interest to the group. Any VNICs added to that group are subject to the security rules of that NSG. A VNIC can be added to a maximum of five NSGs.

Congratulations! In this lab, you created and configured a security list and a network security group. Also, you observed a difference between the two virtual network firewalls. The security list that serves as a virtual firewall at the networking service, and the NSG is designed for application components with different security postures.

Ram Niwas Sangwan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Purge Instructions

Perform the purge operations, as instructed below, before proceeding to the next practice:

Delete Compute Instance

1. From the navigation menu, select **Compute,** and then click **Instances**.
2. Ensure you are in the same **Compartment** as the **Instance** you created.
3. Locate the first **Compute Instance** and click its name.
4. Click **Terminate**. Ensure you check the **Permanently delete the attached Boot Volume**, and then click **Terminate Instance**.
5. Repeat steps 1 through 4 to terminate all the Compute Instances. Once the instances are terminated, the color changes to grey from yellow. Wait for both instances termination to be completed.

Delete Subnet

1. From the navigation menu, select **Networking**, and then click **Virtual Cloud Networks**.
2. Click the VCN you're interested in.
3. Click **Subnets**.
4. Click the subnet you're interested in.
5. Click **Terminate**.
6. Confirm when prompted.

Delete Security List

1. Open the navigation menu, click **Networking**, and then click **Virtual Cloud Networks**.
2. Ensure you are in the same **Compartment** as the **VCN** you created.
3. Click the name of your **VCN**.
4. Under **Resources,** click **Security Lists**.

Rama Nivas Sangwan (ram.nivas@tcs.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

5. For the **Security List** you want to delete, click the **Actions** menu, and then click **Terminate**.

6. Confirmed when prompted.

Delete Network Security Group

1. Open the navigation menu, click **Networking**, and then click **Virtual Cloud Networks**.

2. Ensure you are in the same **Compartment** as the **VCN** you created.

3. Click the name of your **VCN**.

4. Under **Resources**, click **Network Security Group**.

5. For the **Network Security Group,** you want to delete, click the **Actions** menu, and then click **Delete**.

6. Confirmed when prompted.

Delete Route Rules

1. Open the navigation menu, click **Networking**, and then click **Virtual Cloud Networks**.

2. Ensure you are in the same **Compartment** as the **VCN** you created.

3. Click on the name of your **VCN**.

4. In the left navigation pane, under **Resources**, click **Route Tables**.

5. Click on the name of your Route Table.

6. Select your **Route Rules** by checking their checkboxes.

7. Click **Remove**.

8. Confirm **Remove**.

Ram Niwas Sangwan (ramniwas@tseedu.com) has a non-transferable license to use this Guide.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Copyright © 2023, Oracle and/or its affiliates.

Delete Internet Gateway

1. From the navigation menu, select **Networking**, and then click **Virtual Cloud Networks**.
2. Click the VCN you're interested in.
3. Under Resources, click Internet Gateways.
4. Click the Actions menu for the Internet gateway, and then click **Terminate**.
5. Confirm when prompted.

Delete VCN

1. From the navigation menu, select **Networking**, and then click **Virtual Cloud Networks**.
2. Ensure you are in the same **Compartment** as the **VCN** you created.
3. Click the name of your **VCN**.
4. Click **Delete**.
5. In the Delete Virtual Cloud Network dialog box, ensure that the **Search compartments for resources associated with this VCN** checkbox is selected. Then select the **Specific compartments** option.
6. Click **Scan**.
7. Click **Delete All**.
8. Click **Close** once **VCN** is deleted.

Ram Niwas Sangwan (ramniwas@tseedu.com) has a non-transferable license to use this Guide.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Niwas Sangwan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Infrastructure Security - Network: Create a Network Source to Restrict Access to Object Storage Service

Lab 5 Practices

Ram Niwas Sangwan (ram.niwas@tcs.edu.com) has a non-transferable license to use this Guide.

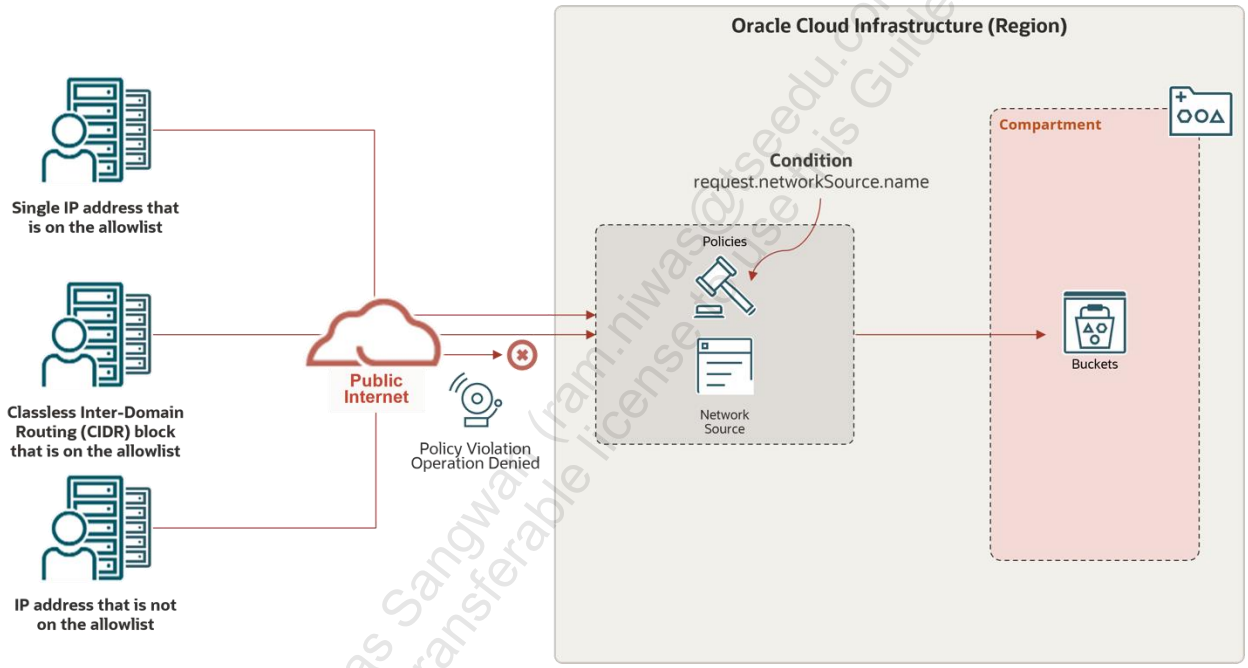
Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Get Started

Overview

A network source allows you to specify the IP addresses that are allowed. Then, in your policy, include a condition that only allows access from IP addresses specified in your network source. When a policy specifies it, IAM verifies that a request to access a resource comes from an allowed IP address.

For example, you can restrict access to Object Storage buckets in your compartment to only users who are signed in to Oracle Cloud Infrastructure through your corporate network. Similarly, you can restrict access requests from specific VCN subnets.



Prerequisites

- You must have access to the OCI Console.
- The Oracle University lab team has set up all the IAM policies required for you to complete this lab.
- You have the precreated Network source in your tenancy.

Assumptions

- Select the region that's available in the tenancy allotted to you. In this lab, we are considering US East (Ashburn) (IAD) as your region.
- You must be familiar with navigating the OCI Console.

Copyright © 2023, Oracle and/or its affiliates.

Create a Network Source

You will learn how to create a network source that can restrict access to requests made from a specific VCN's IP address, public IP addresses, or both.

Note: The following steps are only for reference; the required network source `IAD-SP-LAB05-1-NS-01` has already been created and added to your practice environment.

Tasks

1. From the navigation menu, select **Identity & Security**, and then click **Network Sources.**
2. In the **Create Network Source** dialog box, enter the following details:
   - **Name**: IAD-SP-LAB05-1-NS-01
   - **Description**: Add a meaningful description.
   - In the **Networks** section:
     - **Network type**: Select Public Network.
     - **IP Address/CIDR Block:** Enter `1.1.1.1`.

       Note: Use any Random IP Address for now; later we will add the IP address that needs to have the permission to create resources.
3. Click **Create**.

   The network source is successfully created.

Ram Niwas Sangwan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Copyright © 2023, Oracle and/or its affiliates.

Specify the Network Source in an IAM Policy

You will learn how to create a policy that makes use of the network source variable `request.networkSource.name` in a condition to restrict resource access.

Note: The following steps are for reference only; the required policy for Object Storage have already been created and added to your practice environment.

For Example: You create a network source named "OfficeNet." You can restrict users of the group "OfficeUsers" to access your Object Storage resources only when their requests originate from the IP addresses you specified in OfficeNet.

Tasks

1. From the navigation menu, select **Identity & Security**, and then click **Policies**.
2. Click **Create Policy**.
3. In the **Create Policy** dialog box, enter the following:
   - **Name:** `<Enter the Policy Name>`
   - **Description**: Add meaningful description
   - **Compartment:** `<Select compartment where policies to be applied>`
   - Under Policy Builder, enable **Show manual editor**.
   - Add the following policy:

     ```
     ALLOW GROUP <Group_Name> TO MANAGE object-family IN COMPARTMENT
     <compartment_name> where request.networkSource.name='IAD-SP-
     LAB05-1-NS-01'
     ```

     Note: The IAM service includes a variable `request.networkSource.name` to use in policy that allows you to scope your policy using a condition.
4. Click **Create**.

This policy allows users in a group to manage Object Storage resources only when their requests originate from an allowed IP address specified in the network source "`IAD-SP-LAB05-1-NS-01`". Requests from IP addresses outside the specified ranges are denied.

Ram Srinivas Srinivasan (ram.srinivas@tseedu.com) has a non-transferable license to use this Guide.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Copyright © 2023, Oracle and/or its affiliates.

Add Network to Access Object Storage Service

You will learn how to add the allowed IP addresses to the network source. This restricts access to Object Storage buckets in your compartment to users who are signed in to Oracle Cloud Infrastructure through the IP addresses listed in network sources.

Note: When you try to create an object storage in the assigned compartment, you will now encounter the Authorization failed error because in the previous steps, a random IP address, 1.1.1.1, was added to the network source.

Task-1

1. From the navigation menu, select **Storage**. Under Object Storage, click **Buckets**.
2. In the left navigation pane, under **List Scope**, select the assigned **compartment** from the drop-down menu.
3. Click **Create Bucket**.
4. In the **Create Bucket** dialog box, specify the attributes of the bucket:
   - **Bucket Name:** IAD-SP-LAB05-1-BKT-01-<user-id>
     Specify your user ID in place of <user-id> to make it unique.
   - **Default Storage Tier:** Select Standard.

   Note: Leave all the other options in their default setting.
5. Click **Create**.

   On the bucket creation page, you get the authorization or bucket already exists error.

Task-2

You will now update your public IP address in Network Source and attempt to create a bucket again.

1. To obtain your public IP address, open a web browser and perform a Google search for "what is my public ip?"

   Note down the Public IP address.
2. From the navigation menu, select **Identity & Security**, and then click **Network Sources.**

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Niwas Sangwan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide.

3. Locate and click `IAD-SP-LAB05-1-NS-01` network source in the list to view its details.

   In your environment, an `IAD-SP-LAB05-1-NS-01` network source was precreated.

4. Click **Add Networks.**

5. In the **Add Networks** dialog box, enter the following:
   - **Network type**: Select Public Network.
   - **IP Address/CIDR Block**: `<YOUR_PUBLIC_IP_ADDRESS>`

6. Click **Update.**

   Your public IP address or CIDR block has successfully been added as a network to the IAD-SP-LAB05-1-NS-01 network source.

Ram Niwas Sangwan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Copyright © 2023, Oracle and/or its affiliates.

Verify Your Access to Create a Bucket

After adding your public IP address to the Network Source, verify the access to create a bucket.

Tasks

1. From the navigation menu, select **Storage**, and then click **Buckets**.
2. In the left navigation pane, under **List Scope**, Select the assigned **compartment** from the drop-down menu.
3. Click **Create Bucket**.
4. In the **Create Bucket** dialog box, specify the attributes of the bucket:
   - **Bucket Name:** IAD-SP-LAB-05-1-BKT-01-<user-id>
     Specify your user ID in place of <user-id> to make it unique.
   - **Default Storage Tier:** Select Standard.

   Note: Leave all the other options in their default setting.
5. Click **Create**.

   You can see the bucket created and listed in your compartment.

Congratulations! You've created a Network Source in this lab to restrict resource access from either a specific VCN's IP address, a list of public IP addresses, or both.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Niwas Sangwan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide

Copyright © 2023, Oracle and/or its affiliates.

Purge Instructions

Perform the purge operation, as instructed below, before proceeding to the next practice.

Delete Bucket

1. From the navigation menu, select **Storage**, and then click **Buckets**.
2. Select the **Compartment** assigned to you from the drop-down menu on the left of the screen under List Scope.
3. Click the Bucket: `IAD-SP-LAB05-1-BKT-01-<user-id>`
4. Click **Delete** and then click **Delete** in the Confirmation window. Click **Close** after Bucket is deleted.

Ram Niwas Sangwan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Infrastructure Security - Network: Create a Self-Signed Certificate and Perform SSL Termination on OCI Load Balancer

Lab 6 Practices

Ram Niwas Sangwan (ramniwas@ts.edu.com) has a non-transferable license to use this Guide.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Get Started

Overview

In this practice, you will deploy web servers on two compute instances in Oracle Cloud Infrastructure (OCI), configured in High Availability mode by using a load balancer; create a Self-Signed Certificate; create an OCI Load Balancer with SSL Termination configuration; and test the SSL Termination at OCI Load Balancer.

Most web servers provide a secure socket layer (SSL) connection so that all communication is encrypted. An SSL connection uses a certificate to encrypt data sent between a web browser and a web server. However, the decryption process requires more computation power on the web server. SSL termination, also known as SSL offloading, helps in the SSL decryption process at the OCI Load Balancer and reduces the load on the web server. After SSL termination at the OCI Load Balancer, unencrypted traffic is routed to web server over the OCI network.

In this lab, you will:

a. Create a Virtual Cloud Network

b. Create a compute instance and install a web server

c. Create a security list and an additional Load Balancer Subnet

d. Create a self-signed certificate

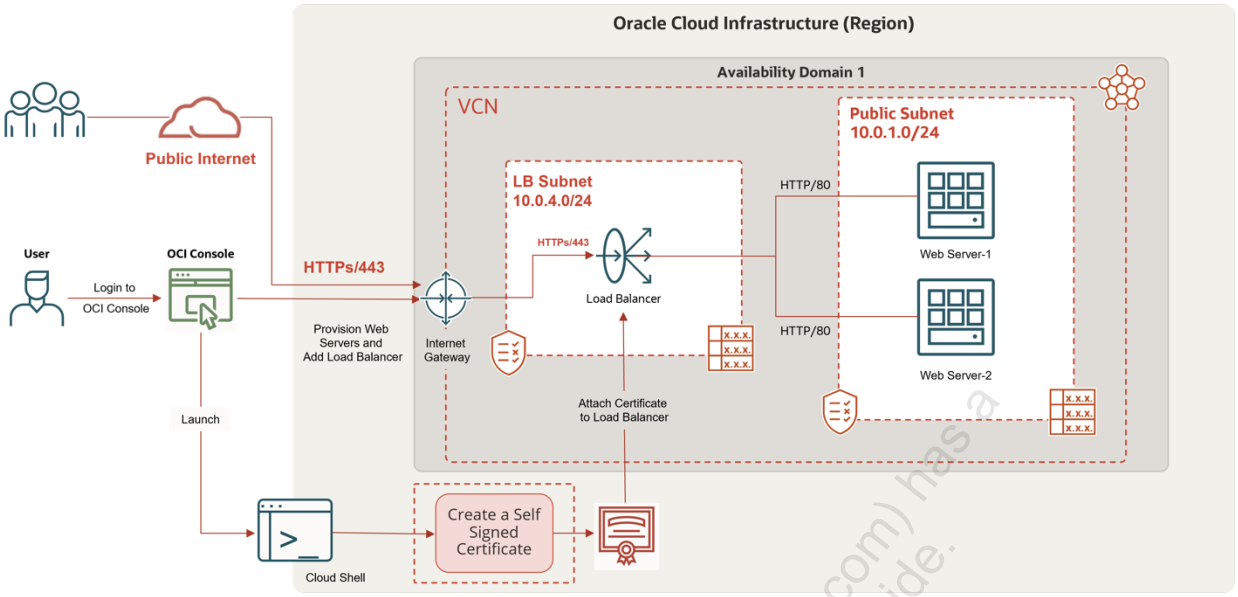
e. Create a load balancer with SSL Termination configuration

f. Update the security list for the Load Balancer Subnet

g. Test SSL Termination (SSL Offloading) at OCI Load Balancer

Ram Jiwas Sangwan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.



Prerequisites

- You must have access to the OCI Console.
- The Oracle University lab team has set up all the IAM policies required for you to complete this lab.

Assumptions

- Select the region that's available in the tenancy allotted to you. In this lab, we are considering US East (Ashburn) (IAD) as your region.
- You must be familiar with navigating the OCI Console.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Niwas Sangwan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Create a Virtual Cloud Network

In this practice, you will learn how to create a Virtual Cloud Network in OCI with a public and a private subnet by using the VCN Wizard. The compute instance that we will create later will be hosted in this VCN's public subnet.

Note: If you have already created a VCN in the previous practice and have it in your compartment, you can skip this practice.

Tasks

1. From the navigation menu, select **Networking**, and then click **Virtual Cloud Network**.
2. In the left navigation pane, under **List Scope**, select the assigned **compartment** from the drop-down menu.
3. Click **Start VCN Wizard.**
4. Select **Create VCN with Internet Connectivity** and click **Start VCN Wizard.**
5. On the Configuration page, enter the following:
   - **Name**: IAD-SP-LAB06-1-VCN-01
   - **Compartment:** Select <*your compartment name*>.

     Note: Leave all the other options in their default setting.
   - Click **Next**.
   - Verify the details on the **Review and Create** page.
6. Click **Create** to start creating the VCN and its resources.
7. Click **View Virtual Cloud Network** to verify the creation of the VCN and its resources.

   You can now see that the VCN was successfully created and is in the Available state, with the following components:

   VCN, Public subnet, Private subnet, Internet gateway, NAT gateway, Service gateway

Ram Nivas Sangwan (ram.nivas@tseedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Create a Compute Instance and Install a Web Server

In this practice, you will provision two compute instances, install an Apache web server, and connect to it over the public Internet.

Tasks

1. From the navigation menu, select **Compute**, and then click **Instances**.
2. In the left navigation pane, under **List Scope**, select the assigned **compartment** from the drop-down menu.
3. Click **Create Instance**. In the Create Instance dialog box, provide the following details:
   - **Name:** IAD-SP-LAB06-1-VM-01
   - **Create in compartment**: Select <*your compartment name*>.
   - **Placement:** Select Availability Domain AD1.

     Note: If the Service limit error is displayed, choose a different Availability Domain.
   - **Image**: Select the image Oracle Linux 8.
   - **Shape:** Click **Change shape**, then in the **Shape** field, click **Change Shape**. Then, select **Ampere shape series** field and select the **VM.Standard.A1.Flex** shape with **1** OCPU and **6 GB** memory**.**
   - **Networking**: Pick your VCN **IAD-SP-LAB06-1-VCN-01** and Public Subnet.
   - **Public IP address** – Assign a public IPv4 address.
   - **Generate (or upload) SSH Keys**:

     a. Click Generate a key pair for me.

     b. Click **Save private key**. This will save the private key to your local workstation.

     c. Click **Save public key**. This will save the public key to your local workstation.
4. Click **Create.**

   Note: After a couple of minutes, you can see that the Instance is successfully created, and the state is Running.
5. Under **Instance access**, copy the **Public IP address** value to Notepad. We refer to it as **VM-01-Public IP** address.

Ram Nivas Sanjeevan (ram.nivas@tseed.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

6. Repeat steps 1 through 5 to launch a **second** compute instance with the name `IAD-SP-LAB06-1-VM-02`.

7. When the second instance, `IAD-SP-LAB06-1-VM-02`, is in **Running** state, under **Instance access**, copy the **Public IP address** value to Notepad. We refer to it as the **VM-02-Public IP** address.

8. Click the **Developer Tools** icon at the right of the OCI console header and click **Cloud Shell** to launch your Cloud Shell. Use SSH to log in to your instance, `IAD-SP-LAB06-1-VM-01`, by using the following command:

   ```
   $ ssh -i <private_key_file> <username>@<public-ip-address of VM-01>
   ```

   Reminders:

   - **Note:** Upload the private key to the Cloud Shell that you downloaded earlier to your workstation. Change the permission of the private key file by executing `chmod 400 <private_key_file>`. Refer to upload file to cloud shell:

     https://docs.oracle.com/en-us/iaas/Content/API/Concepts/devcloudshellgettingstarted.htm#Cloud_Shell_Transferring_Files
   - `<private_key_file>` is the full path and name of the file that contains the private key associated with the instance you want to access.
   - `<username>` is the default user `opc`.
   - `<public-ip-address>` is the Public IP address of the instance. In our case, we refer to it as VM-01-Public IP and VM-02-Public IP.
   - **Note:** Enter **yes** in response to "Are you sure you want to continue connecting (yes/no)?"

   You are now connected to the instance `IAD-SP-LAB06-1-VM-01`.

9. While connected to your compute instance via SSH, run the following commands to install and configure Apache web server:
   - Install the Apache server:
     ```
     $ sudo yum -y install httpd
     ```
   - Enable Apache and start the Apache server:
     ```
     $ sudo systemctl enable httpd
     $ sudo systemctl restart httpd
     ```
   - Create a firewall rule to enable HTTP connection through port 80 and reload the firewall:
     ```
     $ sudo firewall-cmd --permanent --add-port=80/tcp
     $ sudo firewall-cmd --reload
     ```

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Jiwas Sahrawat (ram.jiwas@tseaf.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

- Create an index file for your web server:

```
$ sudo bash -c 'echo You are visiting Web Server 1 >>
/var/www/html/index.html'
```

- Exit the SSH connection:

```
$ exit
```

10. Again, use Cloud Shell to SSH to the second instance, `IAD-SP-LAB06-1-VM-02` by using the following command:

```
$ ssh -i <private_key_file> <username>@<public-ip-address of VM-
02>
```

Note: Enter **yes** in response to "Are you sure you want to continue connecting (yes/no)?"

11. Repeat step 9 to install Apache web server on the second compute instance.

Note: Make sure that the index file command for the second web server looks like this:

```
$ sudo bash -c 'echo You are visiting Web Server 2 >>
/var/www/html/index.html'
```

12. After executing all the commands successfully, open a browser in your local system and enter the URL http://<Public IP of IAD-SP-LAB06-VM-01 >.

Note: Your browser will not return anything because port 80 is not opened yet for instance subnet.

Ram Niwas Sangwan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Create a Security List and an Additional Load Balancer Subnet

Before you create the load balancer, you will create a new security list. This security list will be used by the load balancer (which will be created later). This will ensure all traffic to the web server is allowed. Load balancers should always reside in different subnets than your web server/application instances. This allows you to keep your web server/application instances secured in different subnets while allowing public Internet traffic to the load balancers in another subnets.

Tasks

1. From the navigation menu, select **Networking**, and then click **Virtual Cloud Network**.
2. In the left navigation pane, under **List Scope**, select the assigned **compartment** from the drop-down menu.
3. Click **IAD-SP-LAB06-1-VCN-01** from the list of VCNs.
4. In the left navigation pane, under **Resources**, click **Security Lists.**
5. Click **Create Security List**.
6. In the Create Security List dialog box, enter the following:
   - **Name**: IAD-SP-LAB06-1-LB-SL-01
   - **Create In Compartment**: Select <*your compartment name*>.
   - Do not add any Ingress or Egress rules.
7. Click **Create Security List**.

   You now see that the security list is created and displayed on the **Security Lists** page.

   Assuming you are still on your VCN details page, create a subnet for a Load Balancer.
8. In the left navigation pane, under **Resources**, click **Subnets.**
9. Click **Create Subnet**.

Ram Niwas Sangwan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

10. In the Create Subnet dialog box, enter the following:
    - **Name:** `LB-Subnet-IAD-SP-LAB06-1-SNET-02`
    - **Create In Compartment:** Select the <*compartment name*> assigned to you.
    - **Subnet Type:** Select **`Regional`.**
    - **IPv4 CIDR Block:** Enter `10.0.4.0/24`.
    - **Security List:** From the drop-down, select the Security List you created earlier `IAD-SP-LAB06-1-LB-SL-01`.

    Note: Leave all the other options in their default setting.

11. Click **Create Subnet.**

    You now see that the subnet is created successfully.

Ram Niwas Sangwan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Copyright © 2023, Oracle and/or its affiliates.

Create a Self-Signed Certificate

Tasks

1. Click the **Developer Tools** icon at the right of the OCI console header and click **Cloud Shell** to launch your Cloud Shell.

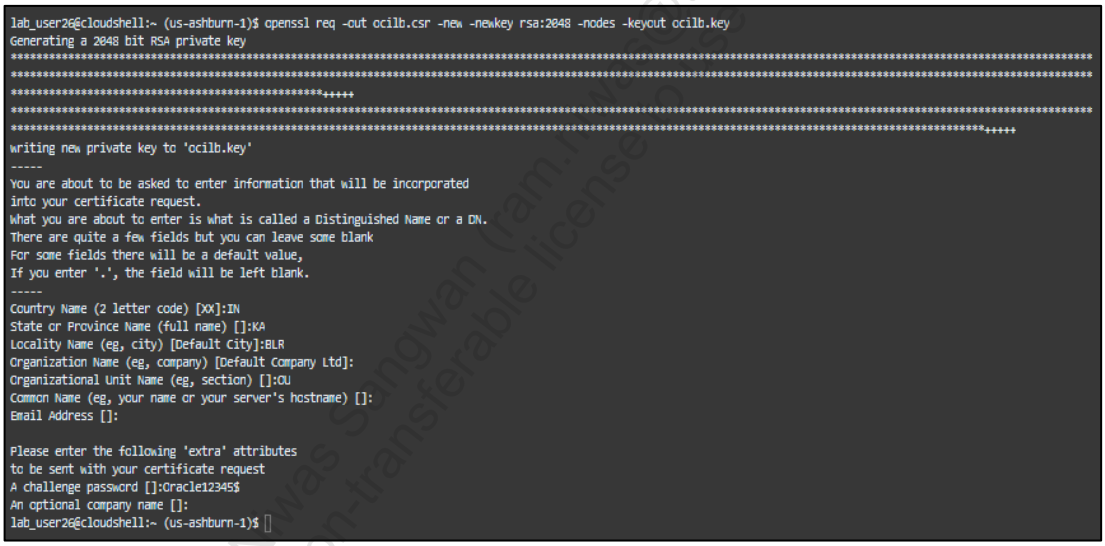
2. Verify that you are in the home directory:

```
$ cd ~
```

3. Enter the following command to generate a Certificate Signing Request (CSR) as the **opc** user:

```
$ openssl req -out ocilb.csr -new -newkey rsa:2048 -nodes -
keyout ocilb.key
```

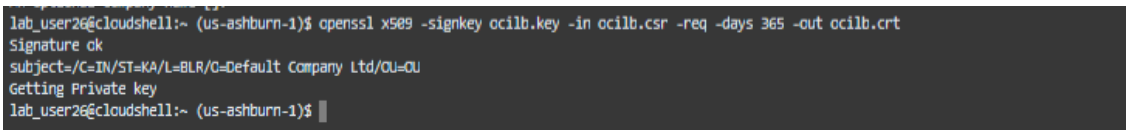
4. Enter the details prompted as shown in the following screenshot. Note down the password entered.



5. Enter the following command to generate a Self-Signed Certificate:

```
$ openssl x509 -signkey ocilb.key -in ocilb.csr -req -days 365 -
out ocilb.crt
```

Verify that the Self-Signed Certificate gets created as shown in the following:



This completes the task of creating a Self-Signed Certificate.

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Create a Load Balancer with SSL Termination Configuration

In this practice, you will create a load balancer with SSL Termination configuration.

Tasks

1. From the navigation menu, select **Networkin**g, and then click **Load Balancers**.
2. In the left navigation pane, under **List Scope**, select the assigned **compartment** from the drop-down menu.
3. Click **Create Load Balancer.**
4. Select **Load Balancer** and click **Create Load Balancer**.
5. In the Create Load Balancer dialog box, enter the following:

   a. In the **Add Details** section:

   - **Load Balancer Name**: `IAD-SP-LAB06-1-LB-01`
   - **Choose visibility type**: `Public`
   - **Assign a public IP address**: Select `Ephemeral IP Address`.
   - **Shapes**: Select `Flexible Shapes`.
   - **Choose the minimum bandwidth**: `10 Mbps`
   - **Virtual Cloud Network**: Select `IAD-SP-LAB06-1-VCN-01`
   - **Subnet**: Select the Regional Subnet we created (10.0.4.0 in this lab) - `LB-Subnet-IAD-SP-LAB06-1-SNET-02`.
   - Click **Next** or **Choose Backends**.

   b. In the **Choose Backends** section:

   - Specify a Load Balancing Policy: Select Weighted Round Robin
   - Click Add Backend. Select the compute instances created earlier and click Add Selected Backends - `IAD-SP-LAB06-1-VM-01` and `IAD-SP-LAB06-1-VM-02`

Copyright © 2023, Oracle and/or its affiliates.

c. **Specify Health Check Policy:**

- Protocol: `HTTP`
- Port: Enter `80`
- URL PATH (URI): /

Note: Leave all the other options in their default setting.

d. Click **Next** or **Configure Listener**.

e. In the **Configure Listener** section:

- **Listener Name**: `IAD-SP-LAB06-1-LB-LISN-01`
- **Specify the type of traffic your listener handles**: Select HTTPS.
- **Specify the port your listener monitors for ingress traffic**: 443

f. Go to Cloud Shell and run the following command to display the certificate details:

```
$ cat ocilb.crt
```

g. Copy the text from -----BEGIN CERTIFICATE----- to -----END CERTIFICATE-----.

h. In the SSL Certificate section:

- Select **Load Balancer Managed Certificate** from Certificate Resource
- Select the Paste SSL Certificate option

Paste the certificate contents copied from Cloud Shell.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Copyright © 2023, Oracle and/or its affiliates.

i. Go to Cloud Shell and run the following command to display the private key details:

```
$ cat ocilb.key
```

j. Copy the text from -----BEGIN PRIVATE KEY----- to -----END PRIVATE KEY-----.

k. In the **SSL Certificate** section:

- Select the **Specify Private Key** check box.
- Select the **Paste Private Key** option.

  Paste the private key contents copied from Cloud Shell.

l. Enter the **password** used while creating the Self-Signed Certificate in the field. Enter Private Key Passphrase.

m. Click **Next** to display the Manage Logging page.

  Note: Leave all options in their default setting.

n. Click **Submit**.

Wait for the load balancer to be provisioned and the status to become Active.

Note down the Public IP address of Load Balancer to be used in the subsequent step.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Update the Security List for Load Balancer Subnet

In this practice, configure the subnet to allow traffic to load balancer.

Tasks

1. From the navigation menu, select **Networking**, and then click **Virtual Cloud Network**.
2. In the left navigation pane, under **List Scope**, select the assigned **compartment** from the drop-down menu.
3. Click **IAD-SP-LAB06-1-VCN-01** from the list of VCNs.
4. In the left navigation pane, under **Resources**, click **Security Lists.**
5. Click **IAD-SP-LAB06-1-LB-SL-01** from the list of Security Lists.
6. In the left navigation pane, under **Resources**, click **Ingress Rules**.
7. Click **Add Ingress Rules** and enter the following:
   - Do NOT select the **Stateless** check box.
   - **Source Type:** `CIDR`
   - **Source CIDR:** Enter `0.0.0.0/0`
   - **IP Protocol:** Select `TCP`
   - **Source Port Range:** `All`
   - **Destination Port Range:** Enter `443 (the listener port for HTTPs).`
   - Click **Add Ingress Rules**.

   You now see that the ingress rule is successfully added in the security list.
8. In the left navigation pane, under **Resources**, click **Egress Rules**.

Ram Viwas Sahawan (ram.niwas@tcseol.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

9. Click **Add Egress Rules** and enter the following:
    - Do NOT select the **Stateless** check box.
    - **Destination Type:** `CIDR`
    - **Destination CIDR:** Enter `0.0.0.0/0`
    - **IP Protocol:** Select `TCP`.
    - **Destination Port Range:** All
10. Click **Add Egress Rules**.

    You now see that the egress rule is successfully added in the security list.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Niwas Sangwan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

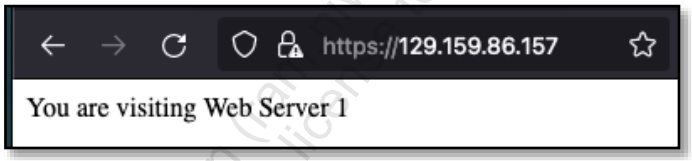
Test the SSL Termination at OCI Load Balancer

Tasks

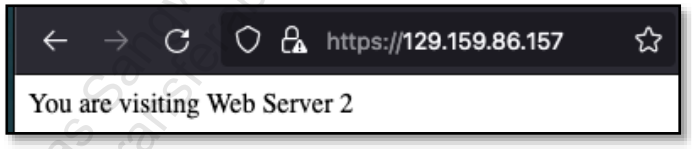
1. From the navigation menu, select **Networking**, and then click **Load Balancer.**
2. In the left navigation pane, under **List Scope**, select the assigned **compartment** from the drop-down menu.
3. Click **IAD-SP-LAB06-1-LB-01** from list of load balancers

   Note down the Public IP address.
4. Open a web browser and enter the URL.

   ```
   https://<Public IP of IAD-SP-LAB06-1-LB-01>
   ```
5. If it prompts with a certificate error, accept the risk, and go ahead.
6. Verify that Web Server 1 or 2 is accessible, and the browser will display any one of the following messages:




```
You are visiting Web Server 1
```




```
You are visiting Web Server 2
```

   This demonstrates SSL gets terminated at OCI Load Balancer and back-end communication between load balancer and web servers is port 80 (http protocol) with encryption.
7. Refresh the browser and observe that the response changes between Web Server 1 and Web Server 2.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Copyright © 2023, Oracle and/or its affiliates.

8. Click the **Developer Tools** icon at the right of the OCI console header and click **Cloud Shell** to launch your Cloud Shell.

9. Enter the following `curl command` to verify the `https` connection to load balancer using CLI:

   ```
   $ curl -k https:// <Public IP of IAD-SP-LAB06-1-LB-01>
   ```

   Use the same `curl` command more than once to see the back-end servers switching.

   This indicates that the load balancer is distributing the requests based on Weighted Round Robin algorithm.

Congratulations! In this lab, you've created a Self-Signed Certificate, a Load Balancer with SSL Termination configuration, and tested SSL Termination (SSL Offloading) at OCI Load Balancer.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Niwas Sangwan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

Purge Instructions

Perform the purge operation, as instructed below, before proceeding to the next practice:

Delete Load Balancer

1. From the navigation menu, select **Networking**, and then click **Load Balancers**.
2. Make sure you are in the same compartment as the VCN you created. Click your **Load Balancer Name:** `IAD-SP-LAB-06-LB-01`
3. Click **Terminate** and click **Terminate** in the Confirm Window. Wait for the termination to be completed.

Delete Compute Instances

1. From the navigation menu, select **Compute**, and then click **Instances**.
2. Make sure that you are in the same compartment as the VCN you created, locate the first compute instance, and click the **compute instance name:** IAD-SP-LAB-06-VM-01.
3. Click the **More Actions** and then select **Terminate**. Ensure that you select **Permanently delete the attached Boot Volume**, and then click **Terminate** instance.
4. Repeat steps **2** and **3** to terminate the **second compute instance** IAD-SP-LAB-06-VM-02. After the instances are terminated, the color changes to gray from yellow. Wait for both instances termination to be completed.

Delete Virtual Cloud Networks

1. From the navigation menu, select **Networking**, and then click **Virtual Cloud Networks.**
2. Make sure you are in the correct compartment. From the list of all VCNs, locate your VCN and click the **VCN name**: `IAD-SP-LAB-06-VCN-01`.

Ram Nivas Garhwal (ram.niwas@tsedu.com) has a non-transferable license to use this Guide.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Copyright © 2023, Oracle and/or its affiliates.

3. Click **Delete**.

   Note: You must delete all resources associated with a VCN, before deleting it.

   - When you click **Delete**, a message box appears. Select the **Specific compartment** check box to search the compartments for resources associated with this VCN, and click **Scan**.
   - Wait for the Scan operation to complete.

4. Click **Delete All**.

5. Click **Close** once the **VCN** is deleted.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Niwas Sangwan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Niwas Sangwan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Infrastructure Security - Compute: Configure OS Management

Lab 7 Practices

Ram Niwas Sangwan (ram.niwas@tcs.edu.com) has a non-transferable license to use this Guide.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

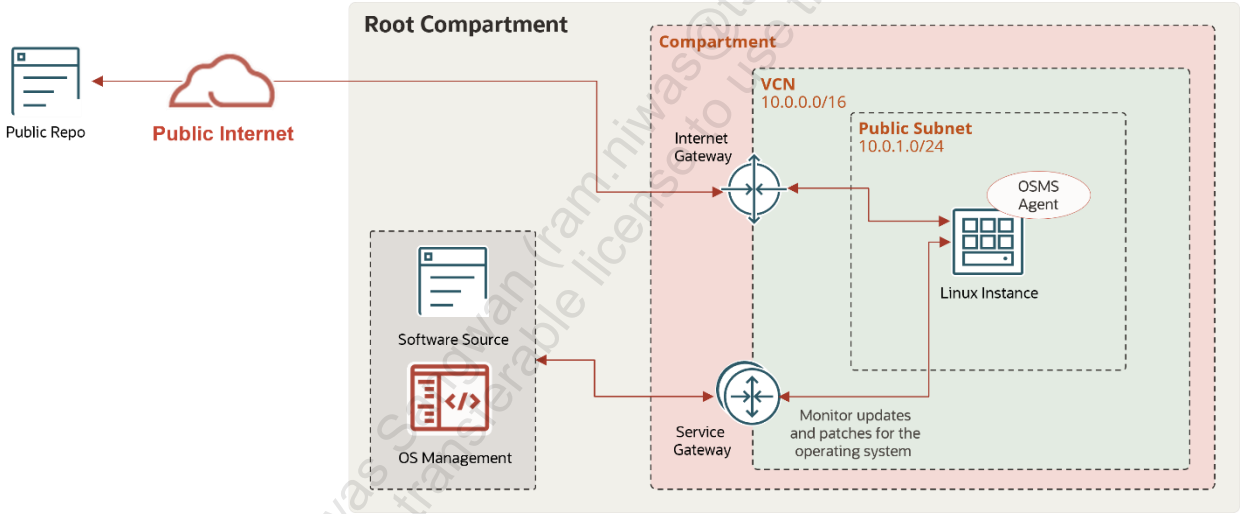
Get Started

Overview

The Oracle Cloud Infrastructure OS Management service allows you to manage and monitor operating system updates and patches on your Oracle Cloud instances, including those managed by the OS Management Oracle Autonomous Linux service. OS Management additionally includes resources for discovering and monitoring your instances.

In this lab, you'll:

- Set up IAM polices for OS management
- Create and configure a Virtual Cloud Network
- Enable OS management agent on compute instance
- Install and verify OS Management service agent and plug-in using CLI
- Install packages on a Managed Instance



Ram Niwas Sharan (ram.niwas@tseec.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

Prerequisites

- You must have access to the OCI Console.
- The required IAM policies have been implemented.

Assumptions

- Select the region that's available in the tenancy allotted to you. In this lab, we are considering US East (Ashburn) (IAD) as your region.
- You must be familiar with navigating the OCI Console.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Niwas Sangwan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

Set Up IAM Polices for OS Management

You will learn about the policies and networking requirement that must be observed when using the OS management service. To begin, we will create a dynamic group that includes all instances in your compartment. Then we will set up IAM policies to allow instances to make API calls to the OS management service.

Note: The following steps are for reference only; the required dynamic group and IAM policy for the principal instance have already been created and added to your environment.

Tasks

Create a Dynamic Group

1. From the navigation menu, select **Identity & Security**, and then click **Dynamic Groups.**
2. Click **Create Dynamic Group.**
3. Enter the following details:
   - **Name:** *<Enter Unique Group Name>*
   - **Description:** <Describe the Dynamic group>
4. Under the Matching Rules section, click **Rule Builder**. To include all instances that are in a specific compartment.
5. From the Include instances that match menu:
   - **Select All of the following.**
   - **For Match instances with: Select Compartment OCID.**
   - **For Value: Enter your assigned compartment OCID.**

     Example: `ocid1:compartment:oc1:phx:sample-compartment-ocid-ythkslsoel`

Policies to Permit Instances to Use OS Management Features

1. IAM policy for a compartment:

```
Allow dynamic-group <dynamic_group_name> to read instance-family
in compartment <compartment_name>
Allow dynamic-group <dynamic_group_name> to use osms-managed-
instances in compartment <compartment_name>
```

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Niwas Sangwan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

2. IAM policy for Metrics:

```
Allow service osms to read instances in tenancy
```

Create a Service Gateway and Add a Route Rule

Note: Required only if instance is in private subnet

3. From the navigation menu, select **Networking**, and then click **Virtual Cloud Networks**.
4. Click the VCN you're interested in.
5. Under Resources, click **Service Gateways**.
6. Click **Create Service Gateway**, and enter the following:
   - **Name:** `IAD-SP-LAB07-1-SG-01`
   - **Create in compartment:** Select your *<compartment name>.*
   - **Service:** All <region> Services in Oracle Services Network

   For example: Region= IAD for Ashburn or PHX for Phoenix.
7. Under Resources, click **Route Tables**.
8. Click the route table you're interested in.
9. Click **Edit Route Rules**.
10. Click **Add Route Rule** and enter the following values:
    - **Target Type**: Service Gateway.
    - **Destination Service**: 0.0.0.0/0 or Service CIDR Labels
    - **Compartment**: The compartment where the service gateway is located
    - **Target**: The service gateway
    - **Description**: An optional description of the rule
11. Click **Save**.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Rahi Niwas Sangvan (rahi.niwas@tsocial.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Create and Configure a Virtual Cloud Network

You will learn how to create a Virtual Cloud Network in OCI with a public and a private subnet by using the VCN Wizard. The compute instance that we will create later will be hosted in this VCN's public subnet.

Note: If you have already created VCN in the previous lab and have it in your compartment, you can skip this practice.

Tasks

1. From the navigation menu, select **Networking**, and then click **Virtual Cloud Network**.
2. In the left navigation pane, under List Scope, select your assigned compartment from the drop-down menu.
3. Click **Start VCN Wizard.**
4. Select **Create VCN with Internet Connectivity** and click **Start VCN Wizard**.
5. On the Configuration page, enter the following:
   - **Name**: IAD-SP-LAB07-1-VCN-01
   - **Compartment:** Select the <*compartment name*> assigned to you.
   - **Note:** Leave all the other options in their default setting.
   - Click **Next.**
   - Verify the details on the **Review and Create** page.
6. Click **Create** to start creating the VCN and its resources.
7. Click **View Virtual Cloud Network** to verify the creation of the VCN and its resources.

   You can now see that the VCN was successfully created and is in the Available state, with the following components:

   VCN, Public subnet, Private subnet, Internet gateway, NAT gateway, Service gateway

Ram Nivas Sanwal (ram.nivas@tseedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Enable OS Management Agent on the Compute Instance

You will learn how to enable OS Management service on the compute instance.

Tasks

1. From the navigation menu, select **Compute**, and then click **Instances**.
2. In the left navigation pane, under List Scope, select *<your assigned compartment>* from the drop-down menu.
3. Click **Create Instance**. In the Create Instance dialog box, provide the following details:
   - **Name**: IAD-SP-LAB07-1-VM-01
   - **Create in compartment**: Select the *<compartment name>* assigned to you.
   - **Placement:** Select Availability Domain AD1.
   - **Note:** If Service limit error is displayed, choose a different Availability Domain.
   - **Image**: Select the image Oracle Linux 8.
   - **Shape:** Click **Change shape**, then in the **Shape** field, click **Change Shape**. Then, select **Ampere shape series** field and select the **VM.Standard.A1.Flex** shape with **1** OCPU and **6 GB** memory**.**
   - **Networking:** Select VCN IAD-SP-LAB07-1-VCN-01 and Public Subnet.
   - Public IP address – Assign a public IPv4 address.
   - Generate (or upload) SSH Keys:
     - Click **Generate a key pair for me**.
     - Click **Save private key**. This will save the private key to your local workstation.
     - Click **Save public key**. This will save the public key to your local workstation.

     Note: Leave all the other options in their default setting.
4. Click **Show Advanced Options**.
5. On the **Oracle Cloud Agent** tab, select the **OS Management Service Agent** and **Management Agent** check box.
6. Click **Create.**

   After a couple of minutes, you can see that the Instance is successfully created, and the state is Running.
7. On the Instance details page, click the **Oracle Cloud Agent** tab.

Copyright © 2023, Oracle and/or its affiliates.

8. Toggle the **Enable Plugin** switch to **Enabled** for **OS Management Service agent** plug-in Name, if the switch is disabled.

   It takes up to 5-10 minutes for the change to take effect. After OS Management service agent plug-in is running, you can check the identified updates and patches required.

9. In the left navigation pane, under Resources, click **OS Management**.

10. You can view the required updates and patches on the compute instance. They are categorized as follows:
    - Security
    - Bug fixes
    - Enhancement
    - Others

    Note: The process to install updates and patches will be covered in subsequent steps.

Ram Niwas Sangwan (ram.niwas@tse.edu.com) has a non-transferable license to use this Guide.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Copyright © 2023, Oracle and/or its affiliates.

Install and Verify the OS Management Service Agent and Plug-in Using CLI

You will learn the steps to install and verify OS management service agent and plug-in using CLI.

> **Note:** This is an optional step; you can skip this if OS Management service agent is already configured in the previous step.

Tasks

1. Click the **Developer Tools** icon at the right of the OCI console header and click **Cloud Shell** to launch your Cloud Shell.

2. SSH to log in to your instance, `IAD-SP-LAB07-1-VM-01` by using the following command:

   ```
   $ ssh -i <private_key_file> <username>@<public-ip-address of VM-01>
   ```

Reminders:

- **Note:** Upload the private key to the cloud shell that you downloaded earlier to your workstation. Change the permission of the private key by executing `chmod 400 <private_key_file>`. Reference to upload file to cloud shell.
- `<private_key_file>` is the full path and name of the file that contains the private key associated with the instance you want to access.
- `<username>` is the default user `opc`.
- `<public-ip-address>` is the Public IP address of the instance.
- **Note:** Enter **yes** in response to "Are you sure you want to continue connecting (yes/no)?"

You are now connected to the instance `IAD-SP-LAB08-1-VM-01`.

3. Check if the Oracle Cloud agent is installed.

   ```
   $ sudo yum info oracle-cloud-agent
   ```

   The output will show the version installed on the instance and the latest version if available.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Niwas Sangwan (ramniwas@tcs.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

4. To install the latest available version of Oracle cloud agent, run the command:

```
$ sudo yum install -y oracle-cloud-agent
```

The command will install the latest available version.

5. Restart the Oracle Cloud Agent service.

```
$ sudo systemctl restart oracle-cloud-agent.service
```

The command will restart the Oracle Cloud Agent service. It will not show any output if Oracle Cloud Agent is configured successfully.

6. Run the following command to verify if it is enabled and active:

```
$ sudo systemctl is-enabled oracle-cloud-agent
$ sudo systemctl is-active oracle-cloud-agent
```

Output: “enabled” and “active”

7. Verify that the OS Management Service Agent plug-in is running on the instance:

```
$ ps -elf | grep osms | grep -v grep
```

For example:

```
$ ps -elf | grep osms | grep -v grep
4 S root     24269 24245  0  80   0 - 62257 -      Jun30 ?
00:00:00 /usr/bin/sudo -n /usr/libexec/oracle-cloud-
agent/plugins/osms/osms-agent
4 S root     24273 24269  0  80   0 -  2165 -      Jun30 ?
00:00:00 /usr/libexec/oracle-cloud-agent/plugins/osms/osms-agent
4 S root     24274 24273  0  80   0 - 406892 -     Jun30 ?
00:50:28 /usr/libexec/oracle-cloud-agent/plugins/osms/osms-agent
```

Ram Niwas Sadawat (ram.niwas@tsu.edu.com) has a non-transferable license to use this Guide.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Install Packages on a Managed Instance

You will learn how to install packages on managed instances.

Tasks

To install a particular update on managed instance:

1. From the navigation menu, select **Compute**, and then click **Instances**.
2. In the left navigation pane, under List Scope, select the assigned **compartment** from the drop-down menu.
3. Select `IAD-SP-LAB07-1-VM-01` from list of instances.
4. On the Instance Details page, under Resources, click **OS Management**.
5. Click the three dots on the right to open the Actions menu and click **View OS Management Details.**
6. Under Resources, click **Available Package Updates/Available Packages**.
7. In the Available Packages Updates/Available Packages section, find and select the packages you want to install. You can also select all and schedule the updates.
8. Click **Install/Install Updates**.
9. Select the **Install Now** option in the window and click **Install Package/Install Package Update**.

   After a couple of minutes, you can see that the package is successfully installed under work requests.

   You can also repeat the procedure to install security updates.

Ram Niwas Sanjwan (ramniwas@tsedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

Purge Instructions

Perform the purge operation, as instructed below, before proceeding to the next practice:

Delete Compute Instance

1. From the navigation menu, select **Compute**, and then click **Instances**.
2. Make sure you are in the same compartment as the VCN you created, locate your compute instance, and click **IAD-SP-LAB07-1-VM-01.**
3. Click **Terminate**. Make sure to select the **Permanently delete the attached Boot Volume** check box and then click **Terminate instance**.

   Wait for the instance termination to be completed.

Delete Internet Gateway, Route Rule, and VCN

1. From the navigation menu, select **Networking**, and then click **Virtual Cloud Networks**.
2. Make sure you are in your assigned compartment.
3. Click **IAD-SP-LAB07-1-VCN-01.**
4. Click **Delete.**

   Note: You must delete all resources associated with a VCN, before deleting it.
   - When you click **Delete**, a message box appears. Select the **Specific compartment** check box to search the compartments for resources associated with this VCN, and click on **Scan**.
   - Wait for the Scan operation to complete.
5. Click **Delete All**.
6. Click **Close** after **VCN** is deleted.

Ram Sliwal Sangwan (ram.sliwal@tseedu.com) has a non-transferable license to use this Guide.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Infrastructure Security - Compute: Configure Vulnerability Scanning with Cloud Guard

Lab 8 Practices

Ram Niwas Sangwan (ram.niwas@tcs.com) has a non-transferable license to use this Guide.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Get Started

Overview

Oracle Cloud Infrastructure Vulnerability Scanning Service improves your security posture by checking hosts for potential vulnerabilities on a regular schedule. The service provides comprehensive visibility into misconfigured or vulnerable resources and creates reports with metrics and information about these vulnerabilities, including remediation information, for developers, operations, and security administrators.

In this lab, you will:

a. Create a Virtual Cloud Network

b. Create a compute instance

c. Create Scan Recipe

d. Create Vulnerability Scanning Target

e. View scan results

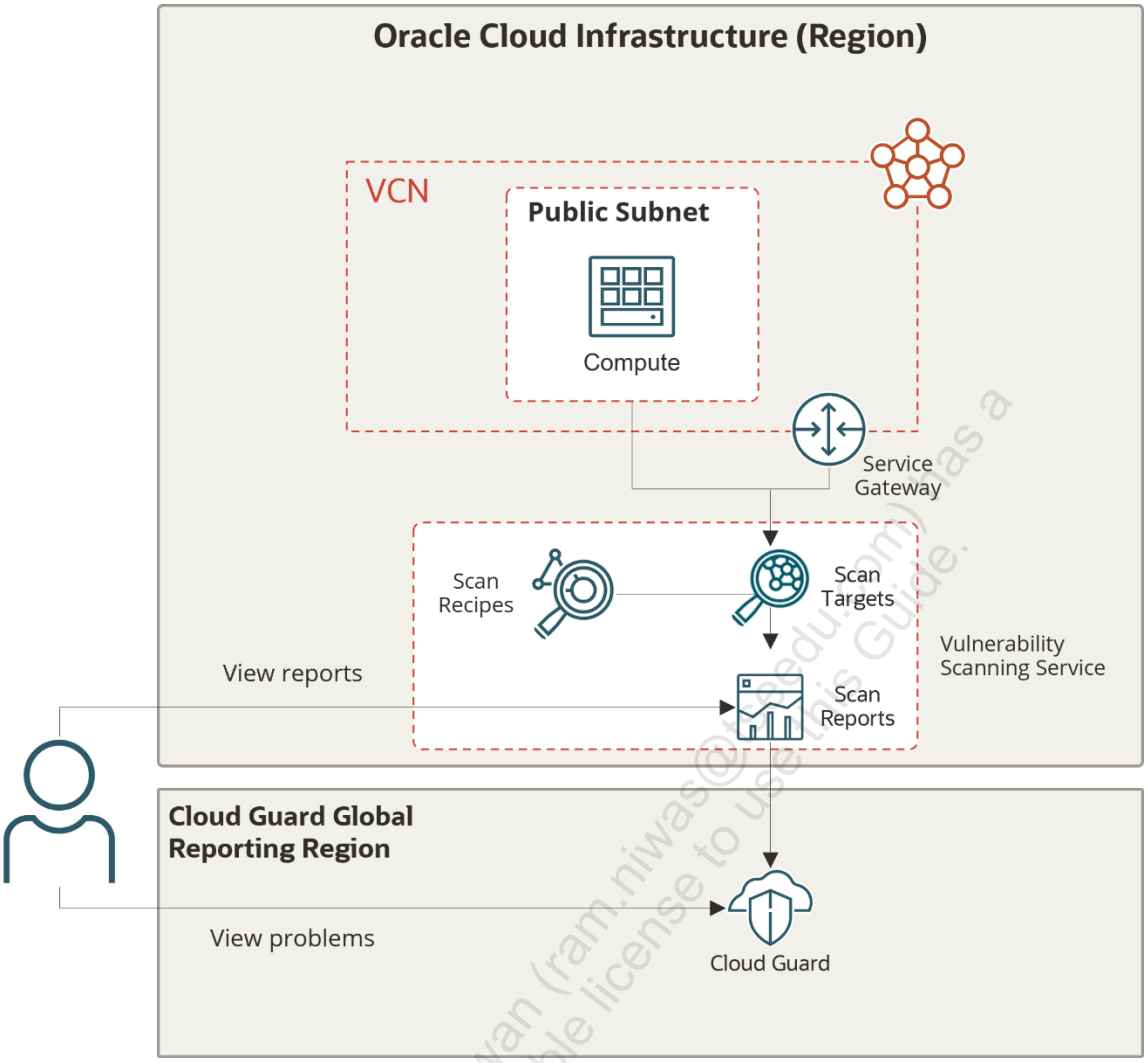
f. View Vulnerability Reports

g. Configure Cloud Guard

h. View Vulnerability Scanning problem in Cloud Guard

Ram Niwas Sangwan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.



Prerequisites

- You must have access to the OCI Console.
- The Oracle University lab team has set up all the IAM policies required for you to complete this lab.

Assumptions

- Select the region that's available in the tenancy allotted to you. In this lab, we are considering US East (Ashburn) (IAD) as your region.
- You must be familiar with navigating the OCI Console.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Niwas Sangwan (ram.niwas@tcs.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Create a Virtual Cloud Network

You will learn how to create a Virtual Cloud Network in OCI with a public and a private subnet using the VCN Wizard. The compute instance that we will create later will be hosted in this VCN's public subnet.

Note: If you have already created VCN in the previous lab and have it in your compartment, you can skip this practice.

Tasks

1. From the navigation menu, select **Networking**, and then click **Virtual Cloud Network**.
2. In the left navigation pane, under List Scope, select your assigned **compartment** from drop-down menu.
3. Click **Start VCN Wizard**
4. Select **Create VCN with Internet Connectivity** and click **Start VCN Wizard.**
5. On the Configuration page, enter the following:
   - **Name**: IAD-SP-LAB08-1-VCN-01
   - **Compartment:** Select the <*compartment name*> assigned to you.

     Note: Leave all the other options in their default setting.
   - Click **Next.**
   - Verify the details on the Review and Create page.
6. Click **Create** to start creating the VCN and its resources.
7. Click **View Virtual Cloud Network** to verify the creation of the VCN and its resources.

   You can now see that the VCN was successfully created and is in the Available state, with the following components:

   VCN, Public subnet, Private subnet, Internet gateway, NAT gateway, Service gateway

Ram Nivas Sanwal (ram.nivas@tseedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Create a Compute Instance

You will provision compute instances with the Vulnerability Scanning plug-in enabled.

Note: If you already created/provisioned a compute instance in the previous lab and have it in your compartment, you can skip this practice. Refer step-7 in this task and enable the vulnerability scanning plug-in.

Tasks

1. From the navigation menu, select **Compute**, and then click **Instances**.
2. In the left navigation pane, under List Scope, select your assigned **compartment** from the drop-down menu.
3. Click **Create Instance**. In the Create Instance dialog box, provide the following details:
   - **Name**: IAD-SP-LAB08-1-VM-01
   - **Create in compartment**: Select the <*compartment name*> assigned to you.
   - **Placement:** Select Availability Domain AD1.

   Note: If the Service limit error is displayed, choose a different Availability Domain.
   - **Image**: Select the image Oracle Linux 8.
   - **Shape:** Click **Change shape**, then in the **Shape** field, click **Change Shape**. Then, select **Ampere shape series** field and select the **VM.Standard.A1.Flex** shape with **1** OCPU and **6 GB** memory**.**
   - **Networking**: Pick your VCN **IAD-SP-LAB08-1-VCN-01** and Public Subnet.
   - **Public IP address** – Assign a public IPv4 address.
   - **Generate (or upload) SSH Keys**:
     a. Click Generate a key pair for me.
     b. Click **Save private key**. This will save the private key to your local workstation.
     c. Click **Save public key**. This will save the public key to your local workstation.

   Note: Leave all the other options in their default setting.
4. Click **Show Advanced Options**.
5. On the **Oracle Cloud Agent** tab, select the **Vulnerability Scanning** check box.

Ram Tiwari Sanjwal (ram.nivas@seedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

6. Click **Create.**

   Note: After a couple of minutes, you can see that the Instance is successfully created, and the state is Running.

7. On the Instance details page, click **Oracle Cloud Agent** tab.

8. Toggle the **Enable Plugin** switch to **Enabled** for **Vulnerability Scanning** plug-in name, if the switch is disabled.

   It can take up to 5-10 minutes for the change to take effect. After a few moments, the status **Running** for Vulnerability Scanning enabled service will be displayed.

Ram Niwas Sangwan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Create Scan Recipes

You will use Oracle Cloud Infrastructure Vulnerability Scanning Service to create and manage recipes that scan target compute instances (hosts) for potential security vulnerabilities.

Tasks

1. From the navigation menu, select **Identity & Security**, and click **Scan Recipes**.

   Skip the Vulnerability Scanning home page that may appear, providing an overview of the service and the policies required.

2. In the left navigation pane, under List Scope, select your assigned **compartment** from the drop-down menu.

3. Click the **Hosts** tab, and then click **Create**.

4. In the **Create scan recipe** dialog box, enter the following:
   - **Type**: Compute
   - **Name:** `IAD-SP-LAB08-1-CSC-01`
   - **Create in compartment**: *<your compartment name>*
   - **Public IP port scanning:** Select **Standard (Top 1000 ports)**.
   - Select the **Agent based scanning** check box.
   - Under **Agent based scanning**, configure CIS benchmark scanning:
     - **Agent to use**: OCI free agent
     - **CIS benchmark profile**: Select **Strict (More than 20% of the benchmarks failing is a critical risk.)**
     - Deselect the **Enable file scans** check box.
   - Schedule: Select **Daily**.

5. Click **Create scan recipe**.

   You will see that the scan recipe is successfully created, and the status is Active.

Ram Nivas Sonwani (ramnivas@ieeedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Create Vulnerability Scanning Target

You will use Oracle Cloud Infrastructure Vulnerability Scanning Service to create compute (host) targets and to assign them to compute scan recipes. A target is a collection of instances that you want routinely scanned for security vulnerabilities.

Tasks

1. From the navigation menu, select **Identity & Security**, and then click **Targets.**
2. In the left navigation pane, under List Scope, select your assigned **compartment** from the drop-down menu.
3. Click the **Hosts** tab, and then click **Create.**
4. In the **Create target** dialog box, enter the following:
   - **Type**: Compute
   - **Name:** `IAD-SP-LAB08-1-CTRG-01`
   - **Create in compartment**: Select the <*compartment name*> assigned to you.
   - **Description**: Add a meaningful description.
   - **Scan recipe in**: Select **IAD-SP-LAB08-1-CSC-01.**

     Note: Click **Change compartment** and select assigned compartment to locate scan recipe, if not available by default.
   - **Target compartment**: <*your compartment name*>
   - Under **Targets**:
     - Select **Selected compute instance**s in the selected target compartment option.
     - **Targets:** Select IAD-SP-LAB08-1-VM-01 instance as target.
5. Click **Create target**.

   You will see that the target is successfully created, and the status is Active.

   Scanning service may take up to 30-35 minutes to check your compute instance for security vulnerabilities and open ports, based on the parameters and schedule configured in the scan recipe.

   Note: Perform the next task of configuring cloud guard to view identified vulnerability scanning problems until the scanning report is populated.

Ram Niwas Sangwan (ramniwas@tseedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Configure Cloud Guard

You will configure and use Cloud Guard to monitor security problems detected in Vulnerability Scanning.

Note: Before using Cloud Guard, at least one Scanning target must exist before the Scanning service creates any reports. These reports are used by the Cloud Guard detector.

Tasks

1. From the navigation menu, select **Identity & Security**, and then click **Cloud Guard**.
2. In the left navigation pane, under **Cloud Guard**, click **Detector Recipes.**
3. In the left navigation pane, under Scope, select **root compartment** from the drop-down menu.
4. Click **OCI Configuration Detector Recipe (Oracle managed)**.

   View the detector rules that are included in this recipe.
5. Under **Detector Rules**, in the **Filter by detector rule** field on the right, enter `scan`.
   a. Verify that the following Vulnerability Scanning rules are enabled:
      - Scanned container image has vulnerabilities
      - Scanned host has vulnerabilities
      - Scanned host has open ports
6. In the left navigation pane, under Cloud Guard, click **Targets**.
7. In the left navigation pane, under List Scope, select your assigned **compartment** from the drop-down menu.

   Note: If you already have a specific target set for your compartment, delete it.

Ram Nivas Sahoo (ramnivas@tseelu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

8. Click Create New Target.

9. Enter the following:

   - **Target Name:** IAD-SP-LAB08-1-CG-01
   - **Description:** Enter a meaningful description (optional).
   - **Compartment:** Select the <*compartment name*> assigned to you.
   - **Configuration detector recipe:** OCI Configuration Detector Recipe (Oracle managed)
   - **Threat detector recipe:** OCI Threat Detector Recipe (Oracle managed)
   - **Activity Detector Recipe:** Oracle Activity Detector Recipe (Oracle managed)
   - **Responder recipe:** OCI Responder Recipe (Oracle managed)

10. Click **Create** to create the target.

    The details page for the new target will be displayed.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Niwas Sangwan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

View Scan Result

You will view and explore security vulnerabilities discovered in your compute instance, such as open ports, critical OS patches, and failed benchmark tests.

Note: Scanning service may take up to 30-35 minutes to check your compute instance for security vulnerabilities and open ports, based on the parameters and schedule configured in the scan recipe.

Tasks

1. From the navigation menu, select **Identity & Security**, and then click **Scanning Reports**.
2. In the left navigation pane, under List Scope, select your assigned **compartment** from the drop-down menu.
3. Click the **Hosts** tab.
4. Locate the **Risk level** filter drop-down menu. Select **All**.
5. Locate the **Scan start date** and **Scan end date** filter drop-down menus.

   By default, only the most recent scan reports are displayed. To view older reports, choose specific start and end dates.
6. Locate the **Reset** button. Click **Reset** at any time to set the risk level and date ranges back to the default values.
7. (Optional) Click the table columns to sort the container image scans by:
   - Risk level
   - Issues found
   - Scan completed
8. To view a compute scan report, click the name of the compute instance.

   Example: IAD-SP-LAB08-1-VM-01

   A host scan includes metrics, open ports, vulnerabilities, and benchmarks for a selected compute instance.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Niwas Sengwan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

9. In the left navigation pane, under **Resources**, click **Metrics** if not already selected.
    - On the Host scan information tab, locate the number of **CIS benchmarks passed**.
    - The Vulnerabilities panel shows the number of security vulnerabilities of each risk level that were detected during the most recent scan of the selected compute instance.

10. In the left navigation pane, under Resources, click **Open ports**.
    - The first panel shows the number of open ports that are detected on each Virtual Network Interface Card (VNIC) in the selected compute instance.
    - The second panel shows the specific port numbers that were detected in this compute instance.

11. In the left navigation pane, under Resources, click **Vulnerabilities**.

12. The following details are shown for each issue that were detected in the selected compute instance:
    - Issue ID
    - Risk level
    - Issue description
    - Last detected
    - First detected
    - Cause and remediation

13. Click any of the **View detail** buttons, in the **Cause and remediation** column, to get more information about how to address the corresponding vulnerability.

14. In the left navigation pane, under Resources, click **CIS benchmarks**.

15. The following details are shown for each CIS benchmark the Scanning service tested on the selected compute instance:
    - Benchmark ID
    - Result - Pass or Fail
    - Summary

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Niwas Sarmavan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

View Vulnerability Reports

You will view and explore Vulnerability Reports, accessing information about specific vulnerabilities that were detected in compute instance targets.

Tasks

1. From the navigation menu, select **Identity & Security**. Under Scanning, click **Vulnerability Reports**.
2. In the left navigation pane, under List Scope, select your assigned **compartment** from the drop-down menu.
3. In the left navigation pane, under Filters, select the Risk level, **All.**
4. Click the **Risk level** column header to sort by risk level.
5. To view a description of a specific vulnerability, click **Show** in the CVE description column.
6. To view details about a specific vulnerability, click a reported **CVE ID**.

   Example: CVE-2022-40674 under CVE ID column

   This will show a vulnerability report for the selected CVE, which includes details about the affected resources and CVE information.
7. On the Vulnerabilities report page, click the **CVE ID** link.

   It will redirect to the source of the CVEs database and provide more information about it.
8. In the left navigation pane, under Resources, select **Hosts** to view a list of compute instance that are affected by the selected vulnerability.

Ram Narayan Sengupta (ram.niwas@tceedu.com) has a non-transferable license to use this Guide.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

View Vulnerability Scanning Problem in Cloud Guard

You will view and explore Cloud Guard reported security problems identified through vulnerability scanning.

Note: Before using Cloud Guard, at least one Scanning target must exist before the Scanning service creates any reports. These reports are used by the Cloud Guard detector.

Tasks

1. From the navigation menu, select **Identity & Security**, and then click **Cloud Guard**.
2. In the left navigation pane, under Cloud Guard, click **Problems.**
3. In the left navigation pane, under List Scope, select your assigned **compartment** from the drop-down menu.
4. View the list of problems Cloud Guard has identified with the resources in your assigned compartment based on your previous practices. The Problems page displays information about each problem, including:
    - Problem Name
    - Risk Level
    - Detector Type
    - Resource affected
    - Target
    - Region
    - Labels
    - First Detected
    - Last Detected
5. To show only Vulnerability Scanning problems, set Filters to:

    Example: `Labels = VSS` (case-sensitive).

Ram Nivas Sangwan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

6. Click the name of a Vulnerability Scanning problem to view its details.

   Example:

   - Scanned host has vulnerabilities
   - Scanned host has open ports

Note: If no Vulnerability Scanning problems are displayed in Cloud Guard, then consider the following scenarios:

- The Vulnerability Scanning service did not create any reports yet. The schedule (daily/weekly) is configured in the Scanning target.
- You recently enabled Cloud Guard or the Vulnerability Scanning detector rules, and Cloud Guard has not run them yet.

7. You can take the necessary steps to eliminate the detected vulnerability and mark the problem as resolved.

Ram Niwas Sangwan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Purge Instructions

Perform the purge operation, as instructed below, before proceeding to the next practice:

Delete cloud guard target

1. From the navigation menu, click **Identity & Security**, and then click **Cloud Guard**.
2. In the left navigation pane, under **Cloud Guard**, click **Targets.**
3. In the left navigation pane, under Scope, ensure that your assigned **compartment** is selected.
4. Click **IAD-SP-LAB08-1-CG-01.**
5. Click **Delete.**
6. In the Delete target window, select the **I understand checkbox.** Then click **Delete Target(s).**

Delete vulnerability scanning target

1. From the navigation menu, click **Identity & Security**. Under **Scanning**, click **Targets.**
2. In the left navigation pane, under List Scope, ensure that your assigned **compartment** is selected.
3. Click the **Hosts** tab, and then click **IAD-SP-LAB08-1-CTRG-01**.
4. Click **Delete**. Click **Delete** again in the confirmation window.

Delete the scan recipe

1. From the navigation menu, click **Identity & Security**. Under **Scanning**, click **Scan Recipes.**
2. In the left navigation pane, under List Scope, ensure your assigned **compartment** is selected.
3. Click the **Hosts** tab, and then click **IAD-SP-LAB08-1-CSC-01**.
4. Click **Delete**. Click **Delete** again in the confirmation window.

Ram Niwas Sangwan (ram.niwas@stseedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

Delete the compute instance

1. From the navigation menu, click **Compute**. Under Compute, click **Instances**.
2. In the left navigation pane, under List Scope, ensure that your assigned **compartment** is selected.
3. Click **IAD-SP-LAB08-1-VM-01.**
4. Click **Terminate**. Make sure to select the **Permanently delete the attached boot volume** check box and then click **Terminate instance**.

Delete the VCN components and then VCN

1. From the navigation menu, click **Networking**. Under Networking, click **Virtual Cloud Network**.
2. In the left navigation pane, under List Scope, ensure that your assigned **compartment** is selected.
3. Click **IAD-SP-LAB08-1-VCN-01.**
4. Click **Delete** at the top to delete the VCN.
5. Select the **Specific Compartments** option and click **Scan**.
6. Click **Delete All** in the window. Click Close once VCN is deleted.

Ram Niwas Sangwan (ram.niwas@tsfedu.com) has a non-transferable license to use this Guide.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Niwas Sangwan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Infrastructure Security - Compute: Set Up a Bastion Host

Lab 9 Practices

Ram Niwas Sangwan (ram.niwas@tcs.edu.com) has a non-transferable license to use this Guide.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

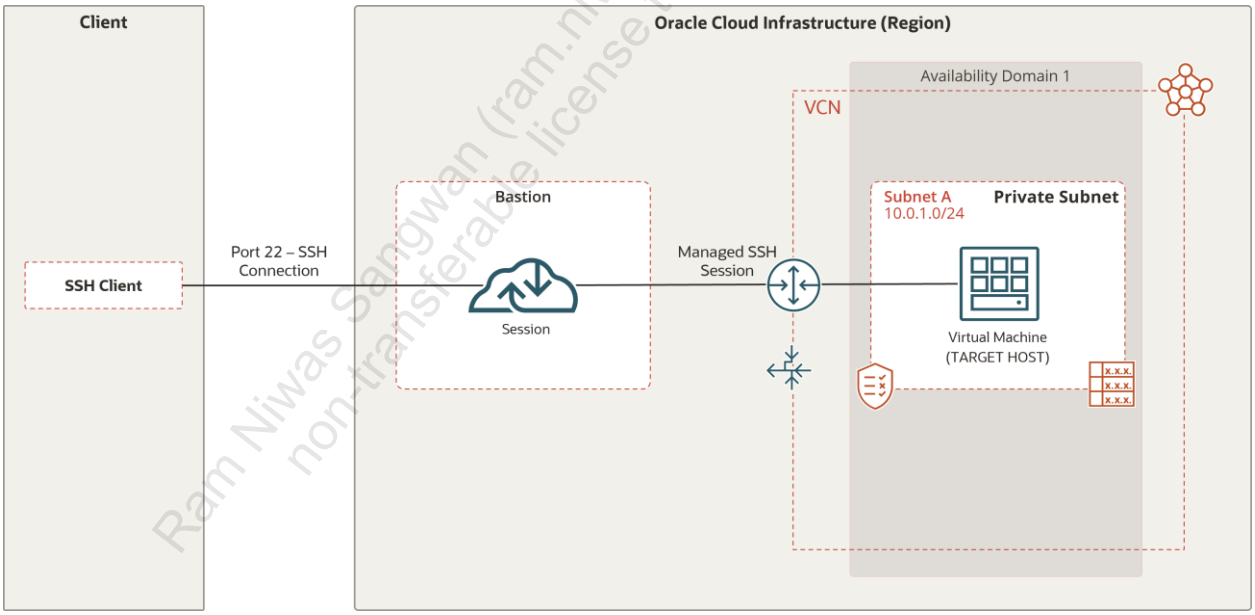
Get Started

Overview

Oracle Cloud Infrastructure (OCI) Bastion restricts and limits access to target resources that do not have public endpoints. Bastions enable authorized users to connect to target resources via Secure Shell (SSH) sessions from certain IP addresses. Targets can include resources such as compute instances, DB systems, and Autonomous Database for Transaction Processing and Mixed Workloads databases. Bastions provide an extra layer of security through the configuration of CIDR block allowlists. Client CIDR block allowlists specify what IP addresses or IP address ranges can connect to a session hosted by the bastion.

In this lab, you'll:

- Create and configure a Virtual Cloud Network
- Enable Bastion plug-in on a compute instance
- Create a Bastion
- Create a Bastion session
- Connect to a compute instance using a managed SSH session



Ram Niwas Sangwan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide.

Prerequisites

- You must have access to the OCI Console.
- The Oracle University lab team has set up all the IAM policies required for you to complete this lab.

Copyright © 2023, Oracle and/or its affiliates.

Assumptions

- Select the region that's available in the tenancy allotted to you. In this lab, we are considering US East (Ashburn) (IAD) as your region.
- You must be familiar with navigating the OCI Console.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Niwas Sangwan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

Create and Configure a Virtual Cloud Network

In this practice, you will learn how to create a Virtual Cloud Network in OCI with a public and a private subnet. The compute instance that you will create later will be hosted in this VCN's private subnet and OCI Bastion in a public subnet.

Tasks

1. Sign in to your Oracle Cloud Infrastructure (OCI) account.
2. From the navigation menu, select **Networking**, and then click **Virtual Cloud Networks (VCN)**.
3. In the left navigation pane, under **List Scope**, select your assigned **compartment** from the drop-down menu.
4. Click **Create VCN**.
5. In the **Create a Virtual Cloud Network** dialog box, enter the following details:
   - **Name:** IAD-SP-LAB09-1-VCN-01
   - **Create in Compartment:** Select the <compartment name> assigned to you.
   - **IPv4 CIDR Blocks:** 10.0.0.0/16

   Note: Leave all the other options in their default setting.
6. Click **Create VCN**.
   You can now see that the VCN is created successfully.
7. Click **Create Subnet**.
8. In the **Create Subnet** dialog box, enter the following details:
   - **Name:** IAD-SP-LAB09-1-SNET-01
   - **Create in Compartment:** Select the <*compartment name*> assigned to you.
   - **Subnet Type**: Regional
   - **IPv4 CIDR Blocks**: 10.0.1.0/24
   - **Subnet Access**: Private Subnet

   Note: Leave all the other options in their default setting.
9. Click **Create Subnet**.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Niwas Sangwan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

You can see that the subnet is created successfully.

10. In the left navigation pane, under **Resources**, click **Service Gateways**.
11. Click **Create Service Gateway**, and enter the following details:
    - **Name:** IAD-SP-LAB09-1-SG-01
    - **Create in compartment:** Select the <*compartment name*> assigned to you.
    - **Services:** All <region> Services in Oracle Services Network

      Note: Region= IAD for Ashburn or PHX for Phoenix.
12. Click **Create Service Gateway.**

    You can see that the service gateway is created successfully.
13. Click **Close**.
14. In the left navigation pane, under **Resources**, click **NAT Gateways**.
15. Click **Create NAT Gateway**, and enter the following details:
    - **Name**: IAD-SP-LAB09-1-NATG-01
    - **Create in compartment:** Select the <*compartment name*> assigned to you.
    - Select Ephemeral Public IP Address.
16. Click **Create NAT Gateway.**

    You can see that the NAT gateway is created successfully.
17. In the left navigation pane, under **Resources**, click **Route Tables**.
18. Click **Default Route Table** from the list.
19. Click **Add Route Rules** and enter the following values:
    - **Target Type**: Service Gateway
    - **Destination Service**: All <region> Services in Oracle Services Network.
    - **Target Service Gateway:** `IAD-SP-LAB09-1-SG-01`

      Click **Change compartment** and select assigned compartment to locate service gateway.
    - **Description**: Description for service gateway route rule

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Nivas Sarawan (ramniwas@tseedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

20. Click **+ Another Route Rule**, and enter the following details:
    - **Target Type**: NAT Gateway.
    - **Destination CIDR Block:** `0.0.0.0/0`
    - **Target NAT Gateway**: `IAD-SP-LAB09-1-NATG-01`

      Click **Change compartment** and select the assigned compartment to locate NAT gateway.
    - **Description**: Description for NAT gateway route rule
21. Click **Add Route Rules.**

    You can see that the new rules are added to route table.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Niwas Sangwan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

Enable Bastion Plug-in on a Compute Instance

In this practice, you will learn how to create a compute instance in a private subnet and enable the Bastion plug-in on that compute instance.

Tasks

1. From the navigation menu, select **Compute**, and then click **Instances**.
2. In the left navigation pane, under **List Scope**, select your assigned **compartment** from the drop-down menu.
3. Click **Create Instance**. In the **Create Instance** dialog box, provide the following details:
   - **Name**: IAD-SP-LAB09-1-VM-01
   - **Create in compartment**: Select the <*compartment name*> assigned to you.
   - **Placement:** Select Availability Domain AD1.

     Note: If the Service limit error is displayed, choose a different Availability Domain.
   - **Image**: Select the image **Oracle Linux 8**.
   - **Shape:** Click **Change shape**, then in the **Shape** field, click **Change Shape**. Then, select **Ampere shape series** field and select the **VM.Standard.A1.Flex** shape with **1** OCPU and **6 GB** memory**.**
   - Click **Select Shape** to return to the Create compute instance window**.**
   - **Networking**: Pick your VCN **`IAD-SP-LAB09-1-VCN-01`** and Private Subnet.
   - Public IP address – Do not assign a public IPv4 address.
   - Add SSH keys: Don't add any SSH key.

   Note: Leave all the other options in their default setting.
4. Click **Show Advanced Options**.
5. On the **Oracle Cloud Agent** tab, select the **Bastion.**
6. Click **Create.**

   Click **Yes, create instance anyway** on No SSH access prompt.

   After a couple of minutes, you can see that the Instance is successfully created, and the state is Running.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Nivas Sanghal (ram.nivas@tseed.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

7. On the Instance details page, click the **Oracle Cloud Agent** tab.
8. Toggle the **Enable Plugin** switch to **Enabled** for **Bastion** Plugin Name, if the switch is disabled.

   It can take up to 5-10 minutes for the change to take effect. After a few moments, the status **Running** for Bastion enabled service will be displayed.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Niwas Sangwan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Create a Bastion

In this practice, you will learn how to create an OCI Bastion to enable restricted and time-limited access to target resources that do not have public endpoints.

Tasks

1. From the navigation menu, select **Identity & Security**, and then click **Bastion**.
2. In the left navigation pane, under **List Scope**, select your assigned **compartment** from the drop-down menu.
3. Click **Create bastion**, and enter the following details:
   - **Bastion name**: SPLAB09BASTION01
   - Configure Networking:
     - Target virtual cloud network: Select **IAD-SP-LAB09-1-VCN-01**
     - Target Subnet: Select **IAD-SP-LAB09-1-SNET-01** (Private Subnet)

       Note: Click **Change compartment** and select assigned compartment to locate VCN and Private subnet gateway.
   - **CIDR block allowlist:** `0.0.0.0/0` (from anywhere)

     You can add one or more address ranges in CIDR notation that you want to allow to connect to sessions hosted by this bastion.
4. Click **Create bastion.**

   After a couple of minutes, you can see that the Bastion is successfully created, and the state is Active.

Ram Niwas Sangwan (ramniwas@oci-edu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

Create a Bastion Session

In this practice, you will learn how to create a Managed SSH Bastion session to access target resources that do not have public endpoints.

Tasks

1. From the navigation menu, select **Identity & Security**, and then click **Bastion**.
2. In the left navigation pane, under **List Scope**, select your assigned **compartment** from the drop-down menu.
3. Click the `SPLAB09BASTION01` Bastion.
4. Click **Create session**, and enter the following details:
   - **Bastion name**: `SPLAB09BASTION01` (Default)
   - **Session type:** Select **Managed SSH session**.
   - **Session name:** `LAB09-1-Session-01`
   - **Username:** Enter `opc`.
   - **Compute instance in:** Select `IAD-SP-LAB09-1-VM-01`.

     Note: Click **Change compartment** and select assigned compartment to locate VCN for compute instance.
   - Add SSH key:

     a. Click **Generate SSH key pair**.

     b. Click **Save private key**. This will save the private key to your local workstation.

     c. Click **Save public key**. This will save the public key to your local workstation.
5. Click **Create session.**

   After a couple of minutes, you can see that the Bastion session is successfully created, and the state is Active.

Ram Nivas Sangwan (ram.nivas@tseedu.com) has a non-transferable license to use this Guide.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Copyright © 2023, Oracle and/or its affiliates.

Connect to a Compute Instance Using a Managed SSH Bastion Session

In this practice, you will learn how to create a Managed SSH Bastion session to access target resources that do not have public endpoints.

Tasks

1. From the navigation menu, select **Identity & Security**, and then click **Bastion**.
2. In the left navigation pane, under **List Scope**, select your assigned **compartment** from the drop-down menu.
3. Click the **SPLAB09BASTION01** Bastion.
4. Click the **three dots** next to the **LAB09-1-Session-01** managed SSH session to open the actions menu and click **View SSH command.**
5. Click **Copy,** next to SSH command, and then click **Close**.

   Copy the SSH command to Notepad.
6. Use a Notepad text editor to replace *<privateKey>* with the private key of the SSH key pair that you provided when you created the session.

   For example:

   ```
   ssh -i ssh-key-2022-10-17.key -o ProxyCommand="ssh -i ssh-key-2022-10-17.key -W %h:%p -p 22 ocid1.bastionsession.oc1.iad.axxxxxxxxxxxxxxxxxxxxxxxxx@host.bastion.us-ashburn-1.oci.oraclecloud.com" -p 22 opc@10.0.1.162
   ```
7. Click the Cloud Shell icon at the right of the OCI console header.
8. Verify that you are in the home directory.

   ```
   $ cd ~
   ```
9. Upload the private key to the cloud shell that you downloaded earlier to your workstation. Reference to upload file to cloud shell.

   The file will be named similarly to *ssh-key-<date>.key*.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Niwas Sangwan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

10. Locate and change the permission of the private key by executing the following commands:

```
$ ls
$ chmod 400 <private_key_file>
```

11. Run the SSH command to connect the compute instance in private subnet.

    Copy and run the command edited in step 7, replacing *<privateKey>* with actual private key name.

    For example:

```
$ ssh -i ssh-key-2022-10-17.key -o ProxyCommand="ssh -i ssh-key-
2022-10-17.key -W %h:%p -p 22
ocid1.bastionsession.oc1.iad.axxxxxxxxxxxxxxxxxxxxxxxx@host.bastion
.us-ashburn-1.oci.oraclecloud.com" -p 22 opc@10.0.1.1
```

    Note: Enter **yes** in response to - Are you sure you want to continue connecting (yes/no)?

12. Verify the connected instance private IP address.

```
$ ifconfig
```

    Take note of the inet/IP address for the ens3 interface in the output and compare it to the instance private IP address created in this lab. i.e. `IAD-SP-LAB09-1-VM-01`

Congratulations! You have successfully created an instance, enabled Bastion, and created a Bastion and session to connect the resources to a private endpoint.

Ram Niwas Sangwan (ram.niwas@tsedu.com) has a non-transferable license to use this Guide.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Copyright © 2023, Oracle and/or its affiliates.

Purge Instructions

Perform the purge operation, as instructed below, before proceeding to the next practice:

Delete Bastion

Note: When you delete a bastion that has active sessions, the sessions are terminated.

1. From the navigation menu, select **Identity & Security**, and then **Bastion**.
2. Under **List Scope**, in the **Compartment** list, click the name of the compartment where the bastion was created.
3. In the **Actions** menu for the listed bastion, click **Delete bastion**.
4. Enter the name of this Bastion.
5. Click **Delete**.

Delete Compute Instance

1. From the navigation menu, select **Compute**, and then click **Instances**.
2. Ensure you are in the same **Compartment** as the **VCN** you created.
3. Locate the first **Compute Instance** and click its name.
4. Click **Terminate**. Ensure that you select **Permanently delete the attached Boot Volume** and then click **Terminate Instance**.

Delete Subnet

1. From the navigation menu, select **Networking**, and then click **Virtual Cloud Networks**.
2. Click the VCN you're interested in.
3. Click **Subnets**.
4. Click the subnet you're interested in.
5. Click **Terminate**.

   Confirm when prompted.

Ram Niwas Sanwan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Copyright © 2023, Oracle and/or its affiliates.

Delete Route Rules

1. From the navigation menu, select **Networking**, and then click **Virtual Cloud Networks**.
2. Ensure that you are in the same **Compartment** as the **VCN** you created.
3. Click the name of your **VCN**.
4. In the left navigation pane, under **Resources**, click **Route Tables**.
5. Click the name of your Route Table.
6. Select your **Route Rules** by checking their check boxes.
7. Click **Remove**.
8. Confirm **Remove**.

Delete VCN

1. From the navigation menu, select **Networking**, and then click **Virtual Cloud Networks**.
2. Ensure you are in the same **Compartment** as the **VCN** you created.
3. Click the name of your **VCN**.
4. Click **Delete**.
5. In the Delete Virtual Cloud Network dialog box, ensure that the **Search compartments for resources associated with this VCN** check box is selected, and then select the **Specific compartments** option.
6. Click **Scan**.
7. Click **Delete All**.
8. Click **Close** once **VCN** is deleted.

Ram Niwas Sangwan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Data and Database Security: Manage Vault Master Encryption Keys and Perform Encryption and Decryption

Lab 10 Practices

Ram Niwas Sangwan (ram.niwas@tcs.com) has a non-transferable license to use this Guide.

Get Started

Overview

OCI Vault is a cloud native service that allows customers to securely store and manage their master encryption keys and configuration information. The OCI Vault service supports several key encryption algorithms, such as the Advanced Encryption Standard (AES), Rivest-Shamir-Adleman (RSA), and the Elliptic Curve Digital Signature Algorithm (ECDSA).

This lab enables you to encrypt or decrypt sensitive information (such as credit card details, salary information, and so on) using master encryption key stored in OCI Vault.

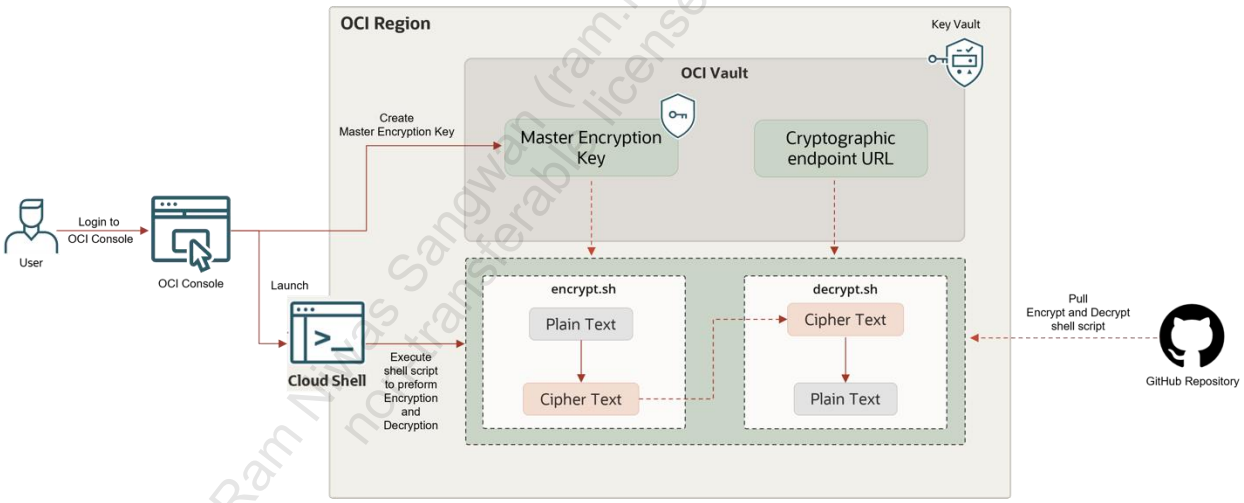
In this lab, you'll:

a. Create a Master Encryption Key

b. Perform basic encryption and decryption using the Master Encryption Key

c. Rotate the Master Encryption Key

d. Repeat the decryption operation and note the key version OCID



Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Prerequisites

- You must have access to the OCI Console.
- The Oracle University lab team has set up all the IAM policies required for you to complete this lab.
- A precreated Vault console setting configured to leverage a Hardware Security Module (HSM)
- URL of a precreated encryption script located at a predetermined location git
- URL of a precreated decryption script located at a predetermined location git

Assumptions

- Select the region that's available in the tenancy allotted to you. In this lab, we are considering US East (Ashburn) (IAD) as your region.
- You must be familiar with navigating the OCI Console.

Ram Niwas Sangwan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Copyright © 2023, Oracle and/or its affiliates.

Create a Master Encryption Key

You'll use an existing OCI Vault that is at the root level compartment, and you will create a master encryption key required to perform cryptographic operations.

Tasks

1. From the navigation menu, select **Identity & Security,** and then click **Vault**.
2. In the left navigation pane, under List Scope, select the **root compartment** from the drop-down menu.
3. From the list of vaults in the root compartment, select **OCI-SECPRO-VAULT**.

   This resource has been precreated for you and is configured to leverage a Hardware Security Module (HSM).
4. On the Vault details page, under the Vault Information tab, copy Cryptographic Endpoint URL.

   This will be required during the encryption process.

   Sample: `https://xxxxxx-crypto.kms.us-ashburn-1.oraclecloud.com`

   Copy the details in a Notepad.
5. In the left navigation pane, under **Resources**, click **Master Encryption Keys.**
6. Click **Create Key**.
7. In the Create Key dialog box, provide the following details:

   a. **Create in Compartment**: *<your assigned compartment>*

   b. **Protection Mode**: HSM

   c. **Name**: `IAD-SP-LAB10-1-VK-01`

   Note: Leave all the other options in their default setting.
8. Click **Create Key**.

   It will take about a minute to create the Master Encryption Key. The keys will go through the **Creating** state to the **Active** state.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Nivas Sangwan (ram.nivas@ieee.org) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

9. Under **List Scope**, select *<your assigned compartment>.* You will see the Master Encryption Key that you have created.

10. Click your Master Encryption Key - **IAD-SP-LAB10-1-VK-01.**

11. On the Key Details page, locate the OCID value on the Key Information tab. Click the **Copy** link located to the right of the OCID value. Save the OCID value somewhere to use later during the encryption process.

    Sample:

    ocid1.key.oc1.iad.xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Ram Niwas Sangwan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Copyright © 2023, Oracle and/or its affiliates.

Perform Encryption

You will now run the provided shell script, which will take as input the OCI Vault cryptographic endpoint, the OCID of the Master Encryption Key you created, and plain text to encrypt. The provided shell script invokes `oci kms crypto encrypt` to perform data encryption.

Tasks

1. Click the **Developer Tools** icon at the right of the OCI console header and click Cloud Shell to launch your Cloud Shell.

   a. Go to your home directory:

   ```
   $ cd ~
   ```

   b. Get the shell script to encrypt the plain text:

   ```
   $ wget https://raw.githubusercontent.com/ou-developers/oci-vaultoperations/main/ocivault-encrypt.sh
   ```

   c. Make the downloaded shell script executable:

   ```
   $ chmod +x ocivault-encrypt.sh
   ```

   d. Run the shell script:

   ```
   $ ./ocivault-encrypt.sh
   ```

   Note: This command will execute the downloaded interactive script, which will prompt you for the following values. When prompted, locate and enter the values that you saved in the previous section.

2. Provide the required parameters as input:

   a. `Please enter the OCI Vault Cryptographic Endpoint URL`

   < OCI Vault Cryptographic Endpoint URL>

   Example: https://xxxxxx-crypto.kms.us-ashburn-1.oraclecloud.com

   b. `Please enter your Master Encryption Key OCID`

   < Master Encryption Key OCID>

   Example: ocid1.key.oc1.iad.xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Niwas Sangwan (ram.niwas@tcs.edu.com) has a non-transferable license to use this Guide.

c. `Please enter the text you wish to encrypt`

<Plain text to be encrypted>

Example: HelloWorld

3. The Shell script will invoke `oci kms crypto encrypt` and perform a cryptographic operation. The following is a sample output of the script:

```
Please enter the OCI Vault Cryptographic Endpoint URL

https://xxxx-crypto.kms.us-ashburn-1.oraclecloud.com

Please enter your Master Encryption Key OCID

ocid1.key.oc1.iad.xxxxxxxxxxxxxxxxxxxxxxxxx

Please enter the text you wish to encrypt

HelloWorld
{
"data": {
    "ciphertext":
"QRu3Y6UBExxxxxaSCNyAKuhqRsxxxxxuk/shqzs4iimhWgyyAA==",
    "encryption-algorithm": "AES_256_GCM",
    "key-id": "ocid1.key.oc1.iad.xxxxxxxxxxbbbbbbbbbxxxx",
    "key-version-id": "ocid1.keyversion.oc1.iad.aaaabbbbb"
  }
}

---------- Encrypted Text ----------

QYcEncB2aSYnAC7QkpXd589LxN8XdddFWJzHyFg2gTKCaCcht97rAAAA==
```

4. Copy and save the **Encrypted Text** somewhere to use later during the decryption process.

Ram Nivas Songwan (ramniwas@tseedu.com) has a non-transferable license to use this Guide.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Perform Decryption

You will now run the provided shell script, which will take as input the OCI Vault cryptographic endpoint, the OCID of the Master Encryption Key you created, and the encrypted text to decrypt. The provided shell script invokes `oci kms crypto decrypt` to perform data decryption.

1. Click the **Developer Tools** icon at the right of the OCI console header and click Cloud Shell to launch your Cloud Shell.

   a. Go to your home directory:

   ```
   $ cd ~
   ```

   b. Get the shell script to decrypt the encrypted text:

   ```
   $ wget https://raw.githubusercontent.com/ou-developers/oci-vaultoperations/main/ocivault-decrypt.sh
   ```

   c. Make the downloaded shell script executable:

   ```
   $ chmod +x ocivault-decrypt.sh
   ```

   d. Run the shell script:

   ```
   $ ./ocivault-decrypt.sh
   ```

   Note: This command will execute the downloaded interactive script, which will prompt you for the following values. When prompted, locate and enter the values that you saved in the previous section.

2. Provide the required parameters as input.

   a. `Please enter the OCI Vault Cryptographic Endpoint URL`

   < OCI Vault Cryptographic Endpoint URL>

   Example: https://xxxxxx-crypto.kms.us-ashburn-1.oraclecloud.com

   b. `Please enter your Master Encryption Key OCID`

   < Master Encryption Key OCID>

   Example: ocid1.key.oc1.iad.xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Ram Niwas Sangwan (ram.niwas@tseelab.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

c. `Please enter the Encrypted Text (Generated Above)`

<Encrypted_Text_from_above_step>

Example: QYcEncB2aSYnAC7QkpXd589LxN8XdddFWJzHyFg2gTKCaCcht97rAAAA==

3. The Shell script will invoke `oci kms crypto decrypt` and perform the decryption operation. The following is a sample output of the script:

```
Please enter the OCI Vault Cryptographic Endpoint URL

https://xxxx-crypto.kms.us-ashburn-1.oraclecloud.com

Please enter your Master Encryption Key OCID

ocid1.key.oc1.iad.xxxxxxxxxxxxxxxxxxxxxxxxx

Please enter the Encrypted Text (Generated Above)

QYcEncB2aSYnAC7QkpXd589LxN8XdddFWJzHyFg2gTKCaCcht97rAAAA==

{
"data": {
     ....
    "key-id": "ocid1.key.oc1.iad.xxxxxxxxxxbbbbbbbbbbxxxx",
    "key-version-id": "ocid1.keyversion.oc1.iad.aaaabbbbb"
     "plaintext": "ampqanNzc3NzCg==",
     "plaintext-checksum": "2060560141"
  }
}

---------- Plain Text ----------

HelloWorld

------------------------------
```

Ram Niwas Sangwan (ram.niwas@tcsedu.com) has a non-transferable license to use this Guide.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Repeat the Decryption Operation and Note the Key Version OCID

You will rotate the Master Encryption Key to limit the data/sensitive information encrypted with a single Master Encryption Key version. Rotating the Master Encryption Key is good practice that reduces the risk if a Master Encryption Key is ever compromised.

Tasks

1. From the navigation menu, select **Identity & Security,** and then click **Vault**.
2. In the left navigation pane, under List Scope, select the **root compartment** from the drop-down menu.
3. From the list of vaults in the root compartment, select **OCI-SECPRO-VAULT**.
4. Under List Scope, select *<your assigned compartment>.* You will see the key that you have created.
5. Click your Master Encrypted Key: **IAD-SP-LAB-10-1-VK-01.**
6. Under Resources, click **Versions.**
7. On the Key Details page, take note of the OCID value on the Key Information tab. When you rotate a key, the Vault service generates a new key version. But Master Encryption Key's unique, Oracle Cloud ID (OCID), remains the same across rotations.
8. On the Key details page, click **Rotate Key.**

   Confirm that you want to rotate the key by clicking the **Rotate Key**. Close the pop-up after success. You will notice that the Vault service generated a new key version.
9. Perform the process of decryption again as earlier on the same encrypted text.

   Observation on Output: The key version ID in the output is no longer the same as the one displayed on the key information page. As a result, cryptographic operations involving data/objects encrypted with a previous version of this key will continue to use the previous key version.

Congratulations! In this lab, you learned how to generate a Master Encryption Key and use it to conduct cryptographic operations. You also learned to rotate the key to reduce the risk if the key is ever compromised.

Copyright © 2023, Oracle and/or its affiliates.

Purge Instructions

Delete Master Encryption Key

1. From the navigation menu, select **Identity & Security**, and then click **Vault**.
2. Under List Scope, in the **Compartment** list, select the root compartment.
3. From the list of vaults in the compartment, click the **OCI-SECPRO-VAULT.**
4. Click **Master Encryption Keys** and locate the key with the name **IAD-SP-LAB-10-1-VK-01**. (If needed, first change the list scope to the assigned compartment.)
5. Click the three dots on the right to open the Actions menu. Select **Delete Key**.
   - Confirm that you want to delete the key by clicking the box and then typing the key name.
   - Schedule when you want the Vault service to delete the key. You can set a date after 8 days.
6. Click **Delete Key**.

Ram Niwas Sangwan (ram.niwas@tssedu.com) has a non-transferable license to use this Guide

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Niwas Sangwan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Data and Database Security: Using the OCI Instance Principals and Vault to Retrieve Secret

Lab 11 Practices

Ram Niwas Sangwan (ram.niwas@tcs.com) has a non-transferable license to use this Guide.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Get Started

Overview

Secrets are credentials such as passwords, certificates, SSH keys, or authentication tokens for third-party cloud services that you use with Oracle Cloud Infrastructure services. Storing secrets in a vault offers more security than storing them elsewhere, such as in code or configuration files. When you need to access resources or other services, you can extract secrets from the vault. To retrieve secrets, you leverage an OCI feature called Instance Principals.

Instance Principals is a feature specific to OCI in which the compute instance itself can be allowed to make API requests to other services. There is no need for a password to get the secret! It's the Instance Principals at work.

In this lab, you will:

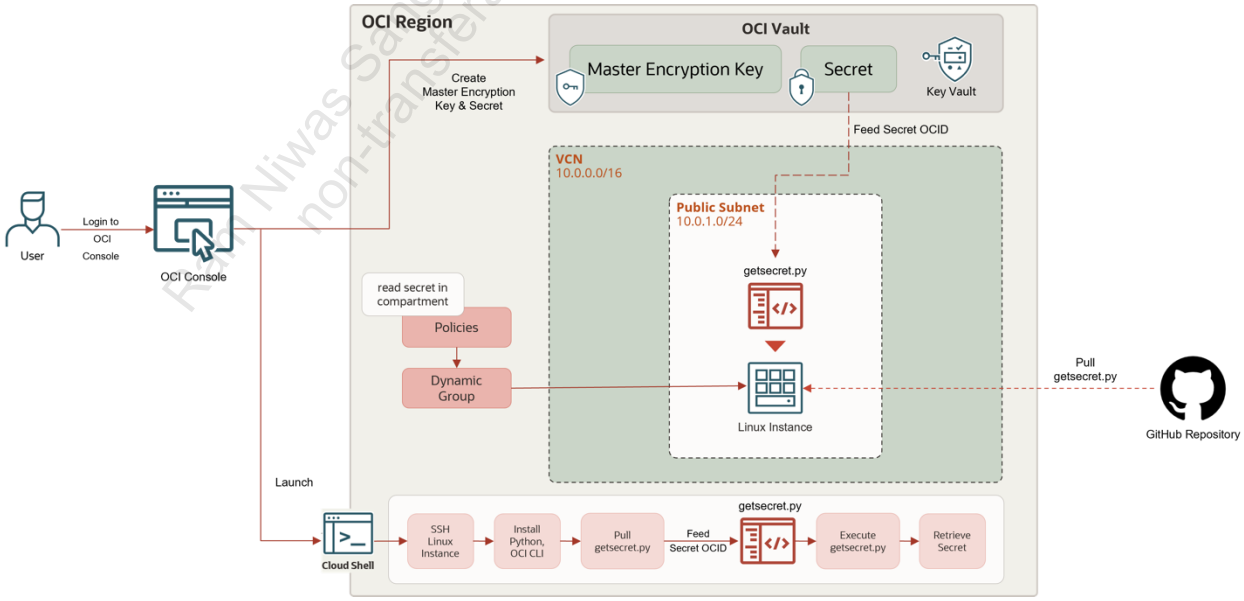
a. Create a Master Encryption Key and a secret

b. Create a Virtual Cloud Network

c. Create a compute instance

d. Authorize an instance to make API calls to OCI Vault service

e. Retrieve the secret



Copyright © 2023, Oracle and/or its affiliates.

Prerequisites

- You must have access to the OCI Console.
- The Oracle University lab team has set up all the IAM policies required for you to complete this lab.

Assumptions

- Select the region that's available in the tenancy allotted to you. In this lab, we are considering US East (Ashburn) (IAD) as your region.
- You must be familiar with navigating the OCI Console.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Niwas Sangwan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

Create Master Encryption Key and a Secret

Tasks

1. From the navigation menu, select **Identity & Security**, and then click **Vault**.
2. In the left navigation pane, under List Scope, select the **root compartment** from the Compartment drop-down menu.
3. Select **OCI-SECPRO-VAULT** from the list of vaults in the root compartment.
4. On the OCI-SECPRO-VAULT Details page, select *<your assigned compartment>* from the **Compartment** drop-down menu in the left column under List Scope.
5. From the left navigation pane under Resources, click **Master Encryption Keys**, and then click **Create Key**.
6. On the **Create Key** page, enter the following details:
   a. **Create in compartment**: <your assigned compartment>
   b. **Protection Mode** – HSM
   c. **Name** – `IAD-SP-LAB11-1-VK-01`
   d. **Key Shape**: Algorithm – Accept the default values.
   e. **Key Shape**: Length – 256 bits
7. Click **Create Key** to save.

   It will take about a minute to create the master encryption key. The keys will go through the **Creating** state to the **Active** state.
8. From the left navigation pane under Resources, select **Secrets** and click **Create Secret**.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Nivas Sarnawat (ram.niwas@tseedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

9. On the **Create Secret** page, enter the following details:
    - **Create in compartment**: <your assigned compartment>
    - **Name**: `IAD-SP-LAB11-1-SK-01`
    - **Description**: "My application secret key"
    - **Encryption Key**: Select the **IAD-SP-LAB11-VK-01** key created earlier.
    - **Secret Contents**: <Your secret here>

10. Click **Create Secret**.

11. After the secret is created, click **IAD-SP-LAB11-1-SK-01**.

12. Click the **Copy** link located to the right of the Secret Key's OCID value. Later, it will be included in a Python script.

    Sample: ocid1.vaultsecret.oc1.iad.xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Ram Niwas Sangwan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Create a Virtual Cloud Network

You will learn how to create a Virtual Cloud Network in OCI with a public and a private subnet using the VCN Wizard. The compute instance that you will create later will be hosted in this VCN's public subnet.

Note: If you have already created the VCN in the previous practice and have it in your compartment, you can skip this practice.

Tasks

1. From the navigation menu, select **Networking**, and then click **Virtual Cloud Network**.
2. In the left navigation pane, under List Scope, select *<your assigned compartment>* from the drop-down menu.
3. Click **Start VCN Wizard**.
4. Select **Create VCN with Internet Connectivity** and click **Start VCN Wizard**.
5. On the Configuration page, enter the following:
   - **Name:** IAD-SP-LAB11-1-VCN-01
   - **Compartment:** *< your compartment name>*

   Note: Leave all the other options in their default setting.
6. Click **Next.**
7. Verify the details on the **Review and Create** page.
8. Click **Create** to start creating the VCN and its resources.
9. Click **View Virtual Cloud Network** to verify the creation of the VCN and its resources.

   You can now see that the VCN was successfully created and is in the Available state, with the following components:

   VCN, Public subnet, Private subnet, Internet gateway, NAT gateway, Service gateway

Ram Nivas Sangwan (ram.nivas@tseedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

Create a Compute Instance

You will provision a compute instance to authorize API calls and retrieve the secret as a principal instance.

Tasks

1. From the navigation menu, select **Compute**, and then click **Instances**.
2. In the left navigation pane, under List Scope, select *<your assigned compartment>* from the drop-down menu.
3. Click **Create Instance**. In the Create Instance dialog box, provide the following details:
   - **Name**: IAD-SP-LAB11-1-VM-01
   - **Create in compartment**: Select the <*compartment name*> assigned to you.
   - **Placement:** Select Availability Domain AD1.

     Note: If the Service limit error is displayed, choose a different Availability Domain.
   - **Image:** Oracle Linux 8
   - **Shape:** Click **Change shape**, then in the **Shape** field, click **Change Shape**. Then, select **Ampere shape series** field and select the **VM.Standard.A1.Flex** shape with **1** OCPU and **6 GB** memory**.**
   - **Networking**: Pick your VCN **IAD-SP-LAB11-1-VCN-01** and Public Subnet.
   - **Public IP address** – Assign a public IPv4 address
   - **Generate (or upload) SSH Keys**
   - Click **Generate a key pair** for me.
   - Click **Save private key**. This will save the private key to your local workstation.
4. Click **Create.**

   Note: After a couple of minutes, you can see that the Instance is successfully created, and the state is Running.

After the instance is provisioned, details about it appear in the instance list. Copy and save the public IP addresses, which will be required to connect to the instance using SSH.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Niwas Singh (ram.niwas@seeqt.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Authorize an Instance to Make API Calls to OCI Vault Service

You will learn how to authorize an instance to make API calls to the OCI Vault service. By adding an instance to a dynamic group and providing the required policies, an application running on an instance can call the OCI Vault service without requiring user credentials or a configuration file.

Note: The following steps are for reference only; the required dynamic group and IAM policy for the principal instance have already been created and added to your environment.

Create a Dynamic group and Add Matching Rules

1. From the navigation menu, select **Identity & Security**, and then click **Dynamic Groups**.
2. Click **Create Dynamic Group**.
3. Enter the following:
   - **Name:** <Enter Unique Group Name>
   - **Description:** <Describe the Dynamic group>
4. Under the Matching Rules section, click **Rule Builder**. To include all instances that are in a specific compartment.
5. From the Include Instances That Match menu:
   a. Select **All of the following**
   b. For **Match Instances** With: Select **Compartment OCID.**
   c. For Value: Enter the **compartment OCID**, for example
   `ocid1:compartment:oc1:phx:samplecompartmentocidythkslsoelu2`

Create Policies to Permit the Dynamic Groups to Access OCI Vault Secret Service

The policy to permit a dynamic group access to secret in a compartment is:

```
ALLOW DYNAMIC-GROUP <dynamic_group_name> TO READ secret-family
IN COMPARTMENT <compartment_name>
```

Ram Nivas Sangwan (ram.nivas@tseedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

Retrieve the Secret for Encryption and Decryption

When used for encryption, a key or key pair encrypts and decrypts data, protecting the data where the data is stored or while the data is in transit.

Tasks

1. Select the **Developer Tools** icon at the right of the OCI console header and click **Cloud Shell** to launch your Cloud Shell.

   While the Cloud Shell is launching, take a moment to locate the public and private keys that you downloaded to your workstation in the previous section.

   Example Public Key name: ssh-key-*<date>*.key.pub

   Example Private Key name: ssh-key-*<date>*.key

2. Once the Cloud Shell window is open, upload the private key to the Cloud Shell:

   a. Click the **Settings icon** in the top-right corner of the Cloud Shell window and click **Upload**.

   b. Navigate to and select the private key. Either drag the private key to the **Drop a file** window, or click **Select from your computer**, select the private key, and click **Upload**.

3. Change the private key permissions by issuing the following command.

   ```
   $ chmod 400 <private_key_name>
   ```

   Where *private_key_name* is the name of the private key that you uploaded in the previous section. Example:

   ```
   $ chmod 400 ssh-key-<date>.key
   ```

4. Retrieve the Public IP address of the instance that you created in the previous section and paste it to connect to the instance using the `opc` user in the Cloud Shell.

   ```
   $ ssh -i <private key name> opc@<public IP address of instance>
   ```

5. After connecting to the compute instance, run the following commands to install/verify python and OCI CLI packages on Linux Instance.

   ```
   $ sudo dnf -y install oraclelinux-developer-release-el8
   $ sudo dnf install python36-oci-cli
   ```

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Nivas Gautam (ram.nivas@tceedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

6. After installing Python and required dependencies, download the Python script to retrieve secret.

```
$ wget https://raw.githubusercontent.com/ou-developers/oci-vaultoperations/main/getsecret.py
```

7. Open a Python file with nano editor.

```
$ nano getsecret.py
```

In the Python script, replace the secret ID ocid with your secret ID.

```
# Replace secret_id value below with the ocid of your secret
secret_id = <secret_id>
```

For example:

```
secret_id = "ocid1.vaultsecret.oc1.iad.xxxxxxxxxxxxxxxxxxxxxxxxxxxx"
```

Note: If you haven't already copied the secret ID, go to Vault, and select the **Secret** link from the resources. Then, in List Scope, choose *<your assigned compartment>,* click on your secret key, and copy the OCID.

8. To save the script, hit:

`ctrl+o > Enter` [To write/save]

`ctrl+x > Yes > Enter` [To exit]

9. Make the `getsecret.py` script executable.

```
$ chmod +x getsecret.py
```

10. Run the following command to retrieve the secret:

```
$ python getsecret.py
```

The secret content created in vault has been retrieved by the application running on the instance. Instance Principal and Vault enable you to abstract the difficulty of developing your own security strategy for storing and encrypting passwords and other sensitive information.

Ram Niwas Sangwan (ramniwas@tseco.com) has a non-transferable license to use this Guide

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Copyright © 2023, Oracle and/or its affiliates.

Purge Instructions

Delete Encryption Key and the Secret

1. From the navigation menu, select **Identity & Security**, and then click **Vault**. Ensure that the **root** compartment is selected.
2. Click **OCI-SECPRO-VAULT.**
3. Click the **Secrets** link under Resources.
4. Now, change the list scope to your assigned compartment.
5. Click the Secret you created: **IAD-SP-LAB11-1-SK-01.**
6. Click **Delete Secret**. Confirm that you want to delete this secret by clicking the box and typing " `IAD-SP-LAB11-1-SK-01`". You can select a delete date. Click **Delete Secret**. Wait for the deletion schedule to be confirmed.
7. On the OCI-SECPRO-VAULT page, click on the **Master Encryption Keys** link under Resources. Ensure your assigned compartment is selected in the scope.
8. Click the key you created: **IAD-SP-LAB11-1-VK-01**
9. Click **Delete Key**. Confirm that you want to delete this key by clicking the box and typing " `IAD-SP-LAB11-1-VK-01`". You can select a delete date. Click **Delete Key**. Wait for the deletion schedule to be confirmed.

Delete Compute Instances

1. Open the navigation menu, click **Instances** under Compute.
2. Make sure you are in the same compartment as the VCN you created, locate your compute instance, and click its name: **IAD-SP-LAB11-1-VM-01.**
3. Click **Terminate**. Make sure check the **Permanently delete the attached boot volume** and then click **Terminate instance**.
4. Wait for the instance termination to be completed.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Niwas Sangwan (ram.niwas@tseelin.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

Delete the VCN

1. Open the navigation menu, and click **Virtual Cloud Networks** under **Networking**.
2. Make sure you are in your given compartment. From the list of all VCNs, locate your VCN and click on its name: **IAD-SP-LAB11-1-VCN-01.**
3. Click **Delete** and then click **Delete VCN** in the Confirmation window. Click **Close** once VCN is deleted.

Ram Niwas Sangwan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Application Security: Create and Configure Web Access Firewall

Lab 13 Practices

Ram Niwas Sangwan (ram.niwas@tcs.com) has a non-transferable license to use this Guide.

Get Started

OCI WAF is a cloud-based security service that aids in the protection of your web applications against malicious and unwanted Internet traffic. It employs a multilayered approach to help safeguard web applications against a variety of cyber threats such as malicious bots, application layer (L7) DDOS attacks, cross-site scripting, SQL injection, and other vulnerabilities defined by the Open Web Application Security Project (OWASP). It can protect any Internet-facing endpoint by enforcing consistent rules across applications and filtering out malicious requests to your web application.

This lab will enable you to create a web application policy for rate limiter, protection rules, and access control. Then, enforce WAF on load balancer to strengthen the security posture.

Overview

In this lab, you will:

a. Create a Virtual Cloud Network

b. Create a compute instance and install the web server

c. Create a security list and an additional Load Balancer Subnet

d. Create a Load Balancer and update the security list

e. Create a Web Application Firewall policy

f. Configure Rate Limiter and verify

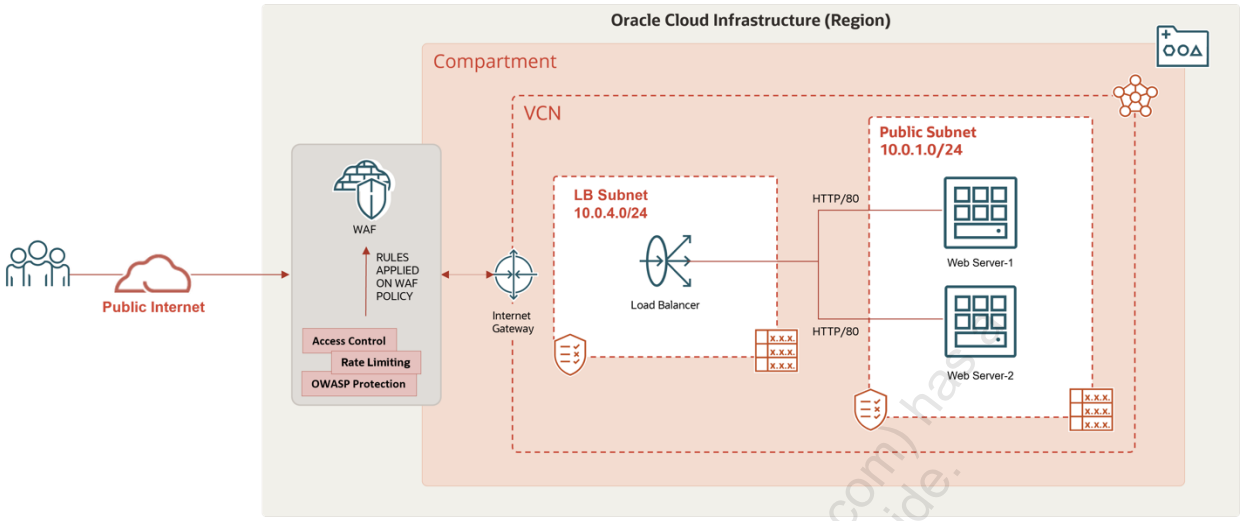
g. Configure Protections and verify XSS attack

Ram Niwas Sangwan (ramniwas@tseedu.com) has a non-transferable license to use this Guide.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Copyright © 2023, Oracle and/or its affiliates.

h. Configure access control and verify conditions



Prerequisites

- You must have access to the OCI Console.
- The Oracle University lab team set up all the IAM policies required for you to complete this lab.

Assumptions

- Select the region that's available in the tenancy allotted to you. In this lab, we are considering US East (Ashburn) (IAD) as your region.
- You must be familiar with navigating the OCI Console.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Niwas Sangwan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Create a Virtual Cloud Network

You will create a Virtual Cloud Network in OCI with a public and a private subnet by using the VCN Wizard. The compute instance that you create later will be hosted in this VCN's public subnet.

Note: If you have already created a VCN in the previous practice and have it in your compartment, you can skip this practice.

Tasks

1. From the navigation menu, select Networking, then click **Virtual Cloud Network**.
2. In the left navigation pane, under List Scope, select *<your assigned compartment>* from the drop-down menu.
3. Click **Start VCN Wizard.**
4. Select **Create VCN with Internet Connectivity** and click **Start VCN Wizard.**
5. On the Configuration page, enter the following:
   - **Name**: IAD-SP-LAB13-1-VCN-01
   - **Compartment:** *<your assigned compartment>*

   Note: Leave all the other options in their default setting.

   a. Click **Next.**

   b. Verify the details on the Review and Create page.
6. Click **Create** to start creating the VCN and its resources.
7. Click **View Virtual Cloud Network** to verify the creation of the VCN and its resources.

   You can now see that the VCN was successfully created and is in the Available state, with the following components:

   VCN, Public subnet, Private subnet, Internet gateway, NAT gateway, Service gateway

Ram Nivas Sangwan (ram.nivas@tseedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Create a Compute Instance and Install Web Server

You will provision compute instance, install an Apache web server, and connect to it over the public Internet.

Tasks

1. From the navigation menu, select Compute, and then click **Instances**.
2. In the left navigation pane, under List Scope, select *<your assigned compartment>* from the drop-down menu.
3. Click **Create Instance**. In the Create Instance dialog box, provide the following details:
    a. **Name**: `IAD-SP-LAB13-1-VM-01`
    b. **Create in compartment**: *<your assigned compartment>*
    c. **Placement:** AD1

    Note: If the Service limit error is displayed, choose a different Availability Domain.

    d. **Image**: Oracle Linux 8
    e. **Shape:** Click **Change shape**, then in the **Shape** field, click **Change Shape**. Then, select **Ampere shape series** field and select the **VM.Standard.A1.Flex** shape with **1** OCPU and **6 GB** memory**.**
    f. **Networking**: **IAD-SP-LAB13-1-VCN-01** and Public Subnet
    g. **Public IP address** – Assign a public IPv4 address
    h. **Generate (or upload) SSH Keys**:
        1) Select **Generate a key pair for me**.
        2) Click **Save private key**. This will save the private key to your local workstation.
        3) Click **Save public key**. This will save the public key to your local workstation.
4. Click **Create.**

Copyright © 2023, Oracle and/or its affiliates.

Note: After a couple of minutes, you can see that the Instance is successfully created, and the state is Running.

5. Under Instance access, copy the Public IP address value to Notepad. We refer to it as the VM-01-Public IP address.

6. Click the **Developer Tools** icon at the right of the OCI console header and click **Cloud Shell** to launch your Cloud Shell, and use SSH to log in to your instance, `IAD-SP-LAB13-1-VM-01` by using the following command:

```
$ ssh -i <private_key_file> <username>@<public-ip-address of VM-01>
```

Reminders:

- Upload the private key to the Cloud Shell that you downloaded earlier to your workstation. Change the permission of the private key file by executing `chmod 400 <private_key_file>`. Reference to upload file to cloud shell.
- `<private_key_file>` is the full path and name of the file that contains the private key associated with the instance you want to access.
- `<username>` is the default user `opc`.
- `<public-ip-address>` is the Public IP address of the instance. In our case, we refer to it as VM-01-Public IP.

  Note: Enter **yes** in response to "Are you sure you want to continue connecting (yes/no)?"

You are now connected to the instance `IAD-SP-LAB13-1-VM-01`.

7. While connected to your compute instance via SSH, run the following commands to install and configure Apache web server:

   - Install Apache Server

     ```
     $ sudo yum -y install httpd
     ```

   - Enable Apache and start Apache server:

     ```
     $ sudo systemctl enable httpd

     $ sudo systemctl restart httpd
     ```

   - Create a firewall rule to enable HTTP connection through port 80 and reload the firewall:

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Nivas Sangwan (ram.nivas@tcs.com) has a non-transferable license to use this Student Guide.

Copyright © 2023, Oracle and/or its affiliates.

```
$ sudo firewall-cmd --permanent --add-port=80/tcp

$ sudo firewall-cmd --reload
```

- Create an index file for your web server:

```
$ sudo bash -c 'echo You are visiting Web Server 1 >>
/var/www/html/index.html'
```

- Exit the SSH connection:

```
$ exit
```

8. After executing all the commands successfully, open a browser in your local system and enter the URL `http://<Public IP of IAD-SP-LAB13-VM-01 >`.

   Note: Your browser will not return anything because port 80 is not opened yet for the instance subnet.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Niwas Sangwan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Create a Security List and an Additional Load Balancer Subnet

Before you create the load balancer, you will create a new security list. This security list will be used by the load balancer (which will be created later). This will ensure all traffic to the web server is allowed. Load balancers should always reside in different subnets than your web server/application instances. This allows you to keep your web server/application instances secured in different subnets while allowing public Internet traffic to the load balancers in another subnets.

Tasks

1. From the navigation menu, select Networking, then click **Virtual Cloud Network**.
2. In the left navigation pane, under List Scope, select *<your assigned compartment>* from the drop-down menu.
3. Click **IAD-SP-LAB13-1-VCN-01** from the list of VCNs.
4. In the left navigation pane, under Resources, click **Security Lists.**
5. Click **Create Security List**.
6. In Create Security List dialog box, enter the following:
    a. **Name**: `IAD-SP-LAB13-1-LB-SL-01`
    b. **Create In Compartment**: *<your assigned compartment>*
    c. Do not add any Ingress or Egress rules.
7. Click **Create Security List**.

    You now see that the security list is created and displayed on the **Security Lists** page.

    Assuming you are still on your VCN details page, create a Load Balancer subnet.
8. In the left navigation pane, under Resources, click **Subnets.**
9. Click **Create Subnet**.

Ram Nivas Sangwan (ram.nivas@tseed.com) has a non-transferable license to use this Guide

Copyright © 2023, Oracle and/or its affiliates.

10. In the Create Subnet dialog box, enter the following:
    - **Name:** `LB-Subnet-IAD-SP-LAB13-1-SNET-02`
    - **Create In Compartment:** *<your assigned compartment name>*
    - **Subnet Type:** Regional
    - **IPv4 CIDR Block:** `10.0.4.0/24`
    - **Security List:** From the drop-down, select the Security List you created earlier, IAD-SP-LAB13-1-LB-SL-01.

    Note: Leave all the other options in their default setting.

11. Click **Create Subnet.**

    You now see that the subnet is created successfully.

Ram Niwas Sangwan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Copyright © 2023, Oracle and/or its affiliates.

Create a Load Balancer and Update the Security List

You will create a load balancer with SSL Termination configuration.

Task-1

1. From the navigation menu, select Networking, and then click **Load Balancers.**
2. In the left navigation pane, under List Scope, select the assigned **compartment** from the drop-down menu.
3. Click **Create Load Balancer.**
4. Select **Load Balancer** and click **Create Load Balancer**.
5. In the Create Load Balancer dialog box, enter the following:
    a. **Under Add Details** section:
        1) **Load Balancer Name**: `IAD-SP-LAB13-1-LB-01`
        2) **Choose visibility type**: Public
        3) **Assign a public IP address**: Ephemeral IP Address
        4) **Shapes**: Flexible Shapes
        5) **Choose the minimum bandwidth**: 10 Mbps
        6) **Virtual Cloud Network**: IAD-SP-LAB13-1-VCN-01
        7) **Subnet**: Select the Regional Subnet you created (10.0.4.0 in this lab) - LB-Subnet-IAD-SP-LAB13-1-SNET-02
        8) Click **Next** or **Choose Backends.**
    b. **Under Choose Backends section:**
        1) **Specify a Load Balancing Policy**: Select **Weighted Round Robin**
        2) Click **Add Backend**, select the compute instance created earlier and click **Add Selected Backends -** IAD-SP-LAB13-1-VM-01
    c. **Specify Health Check Policy:**
        1) **Protocol**: HTTP

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Nwas Sanwan (ramniwas@tseedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

2) **Port**: 80

3) **URL PATH (URI):** /

Note: Leave all the other options in their default setting.

d. Click **Next** or **Configure Listener**.

e. **Under Configure Listener section:**

1) **Listener Name**: `IAD-SP-LAB13-1-LB-LISN-01`

2) **Specify the type of traffic your listener handles**: HTTP

3) **Specify the port your listener monitors for ingress traffic**: 80

Note: Leave other options with the default values.

f. Click **Next** or **Manage Logging**.

Under Manage Logging section, ensure that **Error Logs** is disabled. Leave all other options in their default setting.

6. Click **Submit**. Wait for the load balancer to become active and then note down its **Public IP address**.

Task-2

You will update Security List for Load Balancer Subnet to allow port 80.

1. From the navigation menu, select Networking, and then click **Virtual Cloud Network**.
2. In the left navigation pane, under List Scope, select the assigned **compartment** from the drop-down menu.
3. Select IAD-SP-LAB13-1-VCN-01 from the list of VCNs.
4. In the left navigation pane, under Resources, click Security Lists.
5. Click **IAD-SP-LAB13-1-LB-SL-01** from the list of Security Lists.
6. In the left navigation pane, under Resources, click **Ingress Rules**.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Nivas Sangwan (ram.nivas@seedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

7. Click **Add Ingress Rules** and enter the following:

    a. Do not select the **Stateless** check box**.**

    b. **Source Type:** CIDR

    c. **Source CIDR:** `0.0.0.0/0`

    d. **IP Protocol: Select** TCP

    e. **Source Port Range:** All

    f. **Destination Port Range:** 80 (the listener port for HTTP)

8. Click **Add Ingress Rule.**

    You now see that the ingress rule is successfully added in the security list.

9. In the left navigation pane, under Resources, click **Egress Rules**.

10. Click **Add Egress Rules** and enter the following:

    a. Do not select the **Stateless** check box**.**

    b. **Destination Type:** `CIDR`

    c. **Destination CIDR:** `0.0.0.0/0`

    d. **IP Protocol: TCP**

    e. **Destination Port Range: All**

11. Click **Add Egress Rules.**

You have the setup configured with a compute instance running HTTP server with an `index.html` file, Load Balancer with all relevant policies and components.

Next, you will attach Web Application Firewall (WAF) to an enforcement point, a load balancer.

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Nivas Sangwan (ram.niwas@ltseed.com) has a non-transferable license to use this Guide.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Create a Web Application Firewall (WAF) Policy

You will create a Web Application Firewall Policy.

Tasks

1. From the navigation menu, select **Identity & Security**. Navigate to **Web Application Firewall** and click **Policies** under it.
2. In the left navigation pane, under List Scope, select *<your assigned compartment>* from the drop-down menu.
3. Click **Create WAF Policy.**
4. The Create WAF Policy dialog box appears. Creating a WAF policy consists of the following sections accessible from the left-side navigation:
   - Basic information
   - Access control
   - Rate limiting
   - Protections
   - Select enforcement point
   - Review and create
5. In the Basic Information section:
   a. **Name:** `IAD-SP-LAB13-1-WAF-01`
   b. **WAF Policy Compartment:** Select the assigned compartment
   c. **Action:** Keep the default preconfigured actions; do not edit.
   d. Click **Select enforcement point** section accessible from the left-side navigation.

   Note: You will configure the other section later in this practice. You will directly configure Enforcement point.

Ram Niwas Sangwan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

6. In the Select enforcement point section:

    a. Add Firewalls: Select a load balancer **IAD-SP-LAB13-1-LB-01** contained in your current compartment from the list.

    b. Click **Next** for Review and Create**.**

7. Under Review and Create Section:

    a. Verify the enforcement point added in previous step.

8. Click **Create WAF Policy.**

    The Create WAF Policy dialog box closes, and you are returned to the WAF Policy page. The WAF policy you created is listed.

Ram Niwas Sangwan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Copyright © 2023, Oracle and/or its affiliates.

Adding a Rate Limiting Rule to a WAF Policy

In this practice, you will configure the Rate Limiting option to set a threshold for the number of requests from a unique IP address over a specified time period.

Tasks

1. From the navigation menu, select **Identity & Security**. Navigate to **Web Application Firewall** and click **Policies** under it.
2. In the left navigation pane, under List Scope, select *<your assigned compartment>* from the drop-down menu.
3. Click the **IAD-SP-LAB13-1-WAF-01** WAF policy to add a rate limiting rule.
4. On policy details page, click **Rate Limiting** under Policy.
5. Click **Manage rate limiting**.
6. On the Manage rate limiting page, click **Add rate limiting rule.**
7. In the Add rate limiting rule dialog box, enter the following:
    a. **Name:** `IAD-SP-LAB13-1-RLP-01`
    b. **Conditions**: Don't add any condition

In the Rate limiting configuration section, enter following conditions:

a. **Request limit**: 3
b. **Period in seconds**: 5
c. **Action duration in seconds**: Keep it blank

Under Rule action:

a. **Action name:** Select **Create New Action** from the drop-down menu.

Ram Nivas Sanjwan (ram.nivas@tseedu.com) has a non-transferable license to use this Guide.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Copyright © 2023, Oracle and/or its affiliates.

In the Add Action dialog box, enter the following details:

a. **Name**: `WAF-LAB13-1-Rate-Limit-Action`

b. **Type**: Return HTTP Response

c. **Response code:** Select "**503 Service unavailable**" from drop-down menu

d. **Response page body**: Type "Too many requests are being sent to Web Server-1."

e. Click **Add action.**

8. Click **Add rate limiting rule**.

9. Click **Save Changes** in the Manage Actions dialog box.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Niwas Sangwan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide.

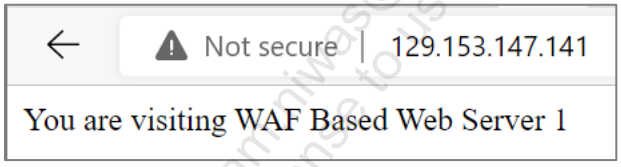
Copyright © 2023, Oracle and/or its affiliates.

Verify the Rate Limiting Rule Configuration

You will connect to the web server and send multiple requests in a short period of time. The rate-limiting rule will evaluate the number of requests and send out responses accordingly.

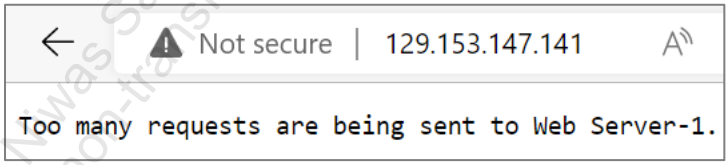
Tasks

1. From the navigation menu, select **Networking**, then click **Load Balancer**.
2. In the left navigation pane, under List Scope, select *<your assigned compartment>* from the drop-down menu.
3. Select Load Balancer **IAD-SP-LAB13-1-LB-01.** Note down the Public IP address.
4. Open a web browser and enter URL `http://<Public IP of IAD-SP-LAB13-1-LB-01>`.
5. Verify the text in `index.html` is displayed.



`You are visiting WAF Based Web Server 1`

6. Refresh the web browser page more than three times in five seconds to view the HTTP Response specified in the action rule.



`Too many requests are being sent to Web Server-1`

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Nwas Sanjwan (ramniwas@tseedu.com) has a non-transferable license to use this Guide.

Add a Protection Rule to Prevent XSS Attack

You will configure the Protections rule to use Oracle-managed request protection capabilities to detect malicious traffic.

Tasks

1. From the navigation menu, select **Identity & Security**. Navigate to **Web Application Firewall** and click **Policies** under it.
2. In the left navigation pane, under **List Scope**, select the assigned **compartment** from the drop-down menu.
3. Click the `IAD-SP-LAB13-1-WAF-01` WAF policy to add a protection rule.
4. On the policy details page, click **Protections** under Policy.
5. In the Protection section on the console, click **Manage request protection rules**.
6. Click **Add Request Protection Rule**.
7. In **Add protection rule** dialog box, enter the following details:
   a. **Name**: `WAF-LAB13-1-XSS-Protection`
   b. **Conditions**: Don't add any condition.
   c. Under **Rule action -** Action name: Select **Create New Action** from the drop-down menu.
8. In the Add Action dialog box, enter the following details:
   a. **Name**: `WAF-LAB13-1-XSS-Action`
   b. **Type**: Return HTTP Response
   c. **Response code**: Select "503 Service unavailable" from the drop-down menu.
   d. **Response page body:** Type "`Service Unavailable: Web Server is secured against XSS attacks.`"
   e. Click **Add action**.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Niwas Sahrawat (ram.niwas@ceedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

9. Under Protection capabilities, click **Choose protection capabilities**.

10. In the **Choose protection capabilities** dialog box, complete the following:

    a. **Filter by tags**: Type "`XSS`" and press Enter.

    b. **Filter by version**: Latest

    c. **Protection list**: Check all protections. Select the check box in the header to add all.

    d. Click **Choose protection capabilities**.

    e. Review and click **Add request protection rule**.

    f. Click **Save Changes** in the Manage Request Protection Rules dialog box.

The rule you created appears in the list. WAF policy will update and get back to active state.

Ram Niwas Sangwan (ram.niwas@tseed.com) has a non-transferable license to use this Guide.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

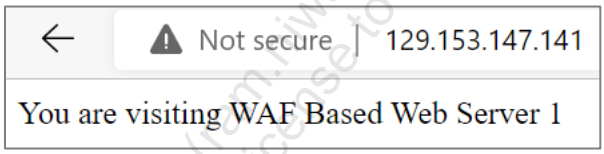
Copyright © 2023, Oracle and/or its affiliates.

Verify the Protection Rule Configuration Against XSS Attack

You will connect to the web server and append an XSS script. The protection rule will evaluate the requests and respond accordingly.

Tasks

1. From the navigation menu, select **Networking**, then click **Load Balancer**.
2. In the left navigation pane, under List Scope, select *<your assigned compartment>* from the drop-down menu.
3. Select Load Balancer **IAD-SP-LAB13-1-LB-01.** Note down the Public IP address.
4. Open a web browser and enter URL `http://<Public IP of IAD-SP-LAB13-1-LB-01>`.
5. Verify the text in `index.html` is displayed.




```
You are visiting WAF Based Web Server 1
```

6. Now enter the following URL:

```
http://Public IP of LB-01/index.html?<p
style="background:url(javascript:alert(1))">
```


```
Service Unavailable: Web Server is secured against XSS attacks.
```

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Niwas Sangwan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

Add Access Control Rule

You'll set up Access Control to define explicit actions for both requests and responses that meet various criteria.

Tasks

1. From the navigation menu, select **Identity & Security**. Navigate to **Web Application Firewall** and click **Policies** under it.
2. In the left navigation pane, under **List Scope**, select the assigned **compartment** from the drop-down menu.
3. Click the **IAD-SP-LAB13-1-WAF-01** WAF policy to add an access control rule.
4. On the policy details page, click **Access control** under Policy.
5. In the Access control section on the console, click **Manage request control**.
6. Click **Add access rule**.
7. In the Add access rule dialog box, enter the following details:

   a. **Name:** `WAF-LAB13-1-Access-Control`

   Under **Conditions**: When the following conditions are met …

   b. **Condition type**: Select Country/Region from the drop-down list.

   c. **Operator**: In list

   d. **Countries**: Add your IP address origin country for testing and press Enter. (Check the IP location on Google.)

   Note: You can add a list of countries that should be restricted from visiting the web server if the company is from a specified region.

   Under **Rule action - Action name**: Select **Create New Action** from the drop-down menu.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Srivas Sarangan (ram.srivas@teeku.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

8. In the Add Action dialog box, enter the following details:

   a. **Name:** `WAF-LAB13-1-Access-Action`

   b. **Type:** Return HTTP Response

   c. **Response code:** Select "**503 Service unavailable**" from drop-down menu.

   d. **Response page body:** Type "Service Unavailable: The web server cannot be accessed by the requested source region."

   e. Click **Add action**.

   f. Click **Add access rule**.

   g. Click **Save Changes** in the Manage request control dialog box.

The rule you created appears in the list. WAF policy will update and get back to active state.

Ram Niwas Sangwan (ram.niwas@tseadu.com) has a non-transferable license to use this Guide.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

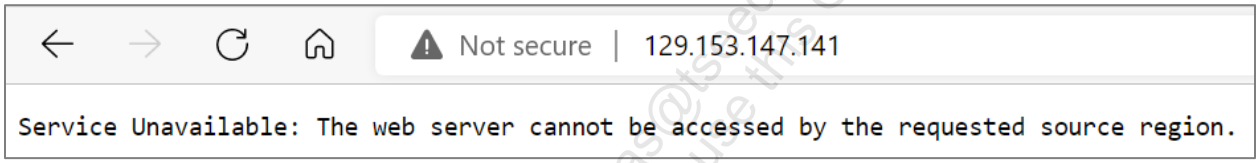
Copyright © 2023, Oracle and/or its affiliates.

Verify the Access Control Rule Configuration

You will connect to the web server from a location that the web server is not permitted to access. The access control rule will assess the requests and respond appropriately.

Tasks

1. From the navigation menu, select **Networking**, then click **Load Balancer**.
2. In the left navigation pane, under List Scope, select *<your assigned compartment>* from the drop-down menu.
3. Select Load Balancer **IAD-SP-LAB13-1-LB-01.** Note down the Public IP address.
4. Open a web browser and enter URL http://<Public IP of IAD-SP-LAB13-1-LB-01>.




```
Service Unavailable: The web server cannot be accessed by the
requested source region.
```

The web server will be inaccessible due to the access rule configured for your IP address' origin country.

You can modify the access control rule, change the Country/Region, and retest the scenario.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Niwas Sangwan (ram.niwas@ts.edu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

Purge Instructions

Perform the purge operation, as instructed below, before proceeding to the next practice:

Delete a Web Application Firewall (WAF) policy

1. From the navigation menu, select **Identity & Security**. Navigate to **Web Application Firewall** and click **Policies** under it.
2. Select *<your assigned compartment>* from the drop-down menu on the left of the screen under List Scope.
3. Click the **IAD-SP-LAB13-1-WAF-01** WAF policy.
4. Select **Firewalls** under Policy, listed on the left.
5. Select the Firewall listed and click **Delete.** Then click **Delete** in the Confirmation window.
6. Once the firewall status is updated to deleted, click **Delete** for **`IAD-SP-LAB13-1-WAF-01`** WAF policy. Then click **Delete** in the Confirmation window.

Delete Load Balancer

1. From the navigation menu, select **Networking**, and then click **Load Balancer**.
2. Select *<your assigned compartment>* from the drop-down menu on the left of the screen under List Scope.
3. Click **IAD-SP-LAB13-1-LB-01.**
4. Click **Terminate.** Then click **Terminate** in the Confirmation window. Click **Close**.

Ram Nivas Sangwan (ram.niwas@seedu.com) has a non-transferable license to use this Guide.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Copyright © 2023, Oracle and/or its affiliates.

Delete Compute Instance

1. From the navigation menu, select **Compute**, then click **Instances**.
2. Make sure you are in the same compartment as the VCN you created, locate the first compute instance, and click the compute instance name: **IAD-SP-LAB-13-1-VM-01**
3. Click **More Actions** and then select **Terminate**. Make sure to select **Permanently delete the attached Boot Volume** and then click the **Terminate** instance.

Delete Virtual Cloud Networks

1. From the navigation menu, select **Networking**, then click **Virtual Cloud Networks**.
2. Make sure you are in the correct compartment. From the list of all VCNs, locate your VCN and click VCN name: **IAD-SP-LAB-13-1-VCN-01**
3. Click **Delete**.

   Note: You must delete all resources associated with a VCN, before deleting it.
   - When you click **Delete**, a message box appears. Select the **Specific compartment check box** to search the compartments for resources associated with this VCN, and click **Scan**.
   - Wait for the Scan operation to complete.
4. Click **Delete All**.
5. Click **Close** once **VCN** is deleted.

Ram Niwas Sangwan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Niwas Sangwan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Create and Manage Certificates: Manage CAs and Certificates, and Attach a Certificate to a Load Balancer

Lab 14 Practices

Ram Niwas Sangwan (ram.niwas@tcs.com) has a non-transferable license to use this Guide.

Get Started

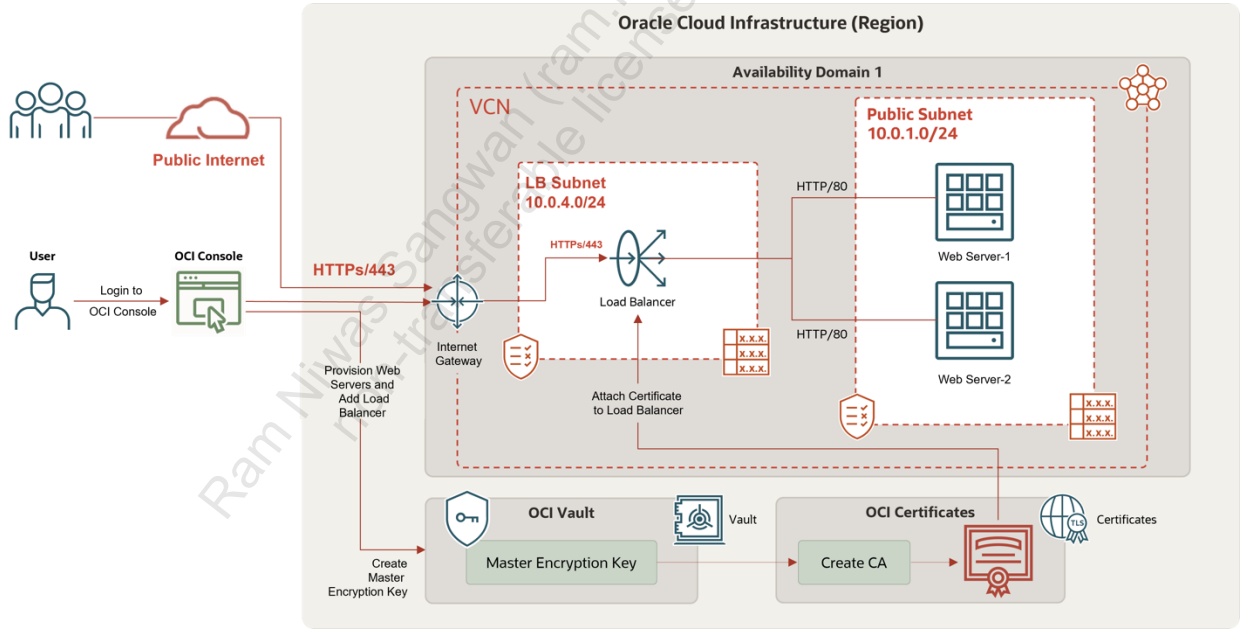
Overview

Oracle Cloud Infrastructure Certificate provides organizations with certificate issuance, storage, and management capabilities, including revocation and automatic renewal. The Certificate service lets you create Certificate authorities (CAs), Certificates, and CA bundles

This lab will enable you to create a certificate authority (CA) and a TLS/SSL server and client certificate. Then, attach created certificate to load balancer to ensure secure communication between clients and back-end servers.

In this lab, you'll:

- Create a Master Encryption Key in OCI Vault
- Create a Certificate Authority
- Create a certificate
- Attach the certificate to Load Balancer



Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Nivas Sangwan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide.

Prerequisites

- You must have access to the OCI Console.
- The Oracle University lab team has set up all the IAM policies required for you to complete this lab.

Assumptions

- Select the region that's available in the tenancy allotted to you. In this lab, we are considering US East (Ashburn) (IAD) as your region.
- You must be familiar with navigating the OCI Console.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Niwas Sangwan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Create a Master Encryption Key (MEK) in an OCI Vault

You will use an existing vault that is at the root-level compartment, and you will create a Master Encryption Key required to create a certification authority.

Tasks

1. From the navigation menu, select **Identity & Security**, and then click **Vault**.
2. In the left navigation pane, under List Scope, select *<your root compartment>* from the drop-down menu.
3. Click **OCI-SECPRO-VAULT** from the list of Vaults.
4. In the left navigation pane, under **Resources**, click **Master Encryption Keys**
5. Click **Create Key**.
6. In the **Create Key** dialog box, enter the following:
   a. **Create in Compartment:** *<your assigned compartment>*
   b. **Protection Mode**: HSM
   c. **Name**: `IAD-SP-LAB14-1-MEK-01`
   d. **Key Shape Algorithm**: RSA (Asymmetric Key used for Encrypt, Decrypt, Sign and Verify)
   e. **Key Shape**: 4096 bits
7. Click **Create Key**.
8. In the left navigation pane, under List Scope, select *<your assigned compartment>* from the drop-down menu.

   It will take about a minute to create the Master Encryption Key. The key will go through the Creating state to the Active state.

   You can view the Master Encryption Key created in your assigned compartment.

Ram Niwas Sangwan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

Create a Certificate Authority (CA)

You will create and manage the certificate authorities that issue digital certificates.

Tasks

1. From the Navigation menu, select **Identity & Security**. Navigate to **Certificates** and click **Certificate Authorities** under it.
2. In the left navigation pane, under List Scope, select *<your assigned compartment>* from the drop-down menu.
3. Click **Create Certificate Authority.**
4. In the Create Certificate Authority dialog box, enter the following:
    a. In the Basic Information section:
        1) **Compartment**: *<your assigned compartment>*
        2) **Certificate Authority Type**: Root Certificate Authority
        3) **Name**: `IAD-SP-LAB14-1-CA-01`
        4) **Description**: Certificate authority for Security Practice
        5) Click **Next.**
    b. Under Subject Information section:
        1) **Common Name**: `IAD-SP-LAB14-1-OCICA-01`
        2) **Click Show Additional Fields**: Fill relevant information (Optional)
        3) Click **Next.**

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Nirwan Sangwan (ramniwas@tseedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

c. In the Authority Configuration section:

1) **Not Valid Before**: Keep it blank.

2) **Not Valid After**: Keep the default value.

3) **Vault in**: (Click Change Compartment and select the root compartment.)

Select **OCI-SECPRO-VAULT** from the drop-down list.

4) **Key in**: Select **IAD-SP-LAB14-1-MEK-01** (Click Change Compartment and select the assigned compartment.)

5) **Signing Algorithm**: **SHA512_WITH_RSA**

6) Click **Next.**

d. In the Rules section:

1) **Maximum Validity Duration for Certificates (Days):** `90`

2) **Maximum Validity Duration for Subordinate CA (Days):** `3600`

3) Click **Next**.

e. In the Revocation Configuration section:

1) Select the **Skip Revocation** check box.

2) Click **Next**.

f. In the Summary section:

1) Review and confirm that the information is correct.

2) Click **Create Certificate Authority.**

3) Click **View Certificate Authority Details**

The Certificate Authority Details page will provide detailed information.

Ram Nivas Sangwan (ram.nivas@tseedu.com) has a non-transferable license to use this Guide.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Copyright © 2023, Oracle and/or its affiliates.

Create a Certificate

You will create a certificate that will be attached to a load balancer to have secure communication.

Tasks

1. From the Navigation menu, select **Identity & Security**. Navigate to **Certificates** and click **Certificates** under it.
2. In the left navigation pane, under List Scope, select *<your assigned compartment>* from the drop-down menu.
3. Click **Create Certificate.**
4. In the Create Certificate dialog box, enter the following:
   a. In the Basic Information section:
      1) **Compartment**: *<your assigned compartment>*
      2) **Certificate Type**: Issued by internal CA
      3) **Name**: `IAD-SP-LAB14-1-CERT-01`
      4) **Description**: `Certificate for Security Practice`
      5) Click **Next.**
   b. In the Subject Information section:
      1) **Common Name**: `IAD-SP-LAB14-1-OCICERT-01`
      2) **Subject Alternative Names**: (Optional) keep as it is.
      3) Click **Show Additional Fields**: Fill relevant information (Optional).
      4) Click **Next.**
   c. In the Certificate Configuration section:
      1) **Certificate Profile Type**: TLS Server Or Client
      2) **Issuer Certificate Authority in <assigned compartment>**:

         `IAD-SP-LAB14-1-CA-01`

         (If needed, click Change Compartment, and then choose a assigned compartment where CA was created)

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Rajan Tiwari Sangwan (rajan.tiwari@tseedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

3) **Not Valid Before**: Keep it blank

4) **Not Valid After**: Enter a date after 45 days from current date.

5) **Key Algorithm**: `RSA4096`

6) Click **Next.**

d. In the Rules section:

1) **Renewal Interval (Days):** default

2) **Advance Renewal Period (Days)**: 30

3) Click **Next**.

e. In the Summary section:

1) Review and confirm that the information is correct

2) Click **Create Certificate**.

5. Click **View Certificate Details**.

The Certificate Details page will provide detail information.

Ram Niwas Sangwan (ram.niwas@tseed.com) has a non-transferable license to use this Guide.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Create a Virtual Cloud Network

In this practice, you will learn how to create a Virtual Cloud Network in OCI with a public and a private subnet by using the VCN Wizard. The compute instance that you will create later will be hosted in this VCN's public subnet.

Note: If you have already created VCN in the previous practice and have it in your compartment, you can skip this practice.

Tasks

1. From the navigation menu, select **Networking**, then click **Virtual Cloud Network**.
2. In the left navigation pane, under List Scope, select the assigned **compartment** from the drop-down menu.
3. Click **Start VCN Wizard**
4. Select **Create VCN with Internet Connectivity** and click **Start VCN Wizard.**
5. On the Configuration page, enter the following:
   a. **Name**: `IAD-SP-LAB14-1-VCN-01`
   b. **Compartment:** Select the <*compartment name*> assigned to you.

      Note: Leave all the other options in their default setting.
   c. Click **Next.**
   d. Verify the details on the Review and Create page.
6. Click **Create** to start creating the VCN and its resources.
7. Click **View Virtual Cloud Network** to verify the creation of the VCN and its resources.

   You can now see that the VCN was successfully created and is in the Available state, with the following components:

   VCN, Public subnet, Private subnet, Internet gateway, NAT gateway, Service gateway

Ram Nivas Sangwan (ram.nivas@tseedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Create a Compute Instance and Install Web Server

You will provision two compute instances, install an Apache web server, and connect to it over the public Internet.

Note: If you already created/provisioned a web server in the previous practice and have it in your compartment, you can skip this practice.

Tasks

1. From the navigation menu, select **Compute**, then click **Instances**.
2. In the left navigation pane, under List Scope, select *<your assigned compartment>* from the drop-down menu.
3. Click **Create Instance**. On the Create Instance dialog box, provide the following details:
    a. **Name**: `IAD-SP-LAB14-1-VM-01`
    b. **Create in compartment**: *<your assigned compartment>*
    c. **Placement:** AD1

    Note: If Service limit error is displayed, choose a different Availability Domain.

    d. **Image**: Oracle Linux 8
    e. **Shape:** Click **Change shape**, then in the **Shape** field, click **Change Shape**. Then, select **Ampere shape series** field and select the **VM.Standard.A1.Flex** shape with **1** OCPU and **6 GB** memory**.**
    f. **Networking**: Pick your VCN **IAD-SP-LAB14-1-VCN-01** and Public Subnet
    g. **Public IP address** – Assign a public IPv4 address
    h. **Generate (or upload) SSH Keys**:
        1) Click **Generate a key pair for me**.
        2) Click **Save private key**. This will save the private key to your local workstation.
        3) Click **Save public key**. This will save the public key to your local workstation.

Ram Nivas Gaiwan (ram.niwas@tseelu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

4. Click **Create.**

   Note: After a couple of minutes, you can see that the Instance is successfully created, and the state is Running.

5. Under Instance access, copy the **Public IP address** value to Notepad. We refer to it as VM-01-Public IP address.

6. Repeat steps 1 - 5 to launch a second compute instance with name IAD-SP-LAB14-1-VM-02.

7. When the second instance, IAD-SP-LAB14-1-VM-02, is in Running state, under Instance access, copy the **Public IP address** value to Notepad. We refer to it as VM-02-Public IP address.

8. Click the **Developer Tools** icon at the right of the OCI console header and click **Cloud Shell** to launch your Cloud Shell, and use SSH to log in to your instance, `IAD-SP-LAB14-1-VM-01` by using the following command:

   ```
   $ ssh -i <private_key_file> <username>@<public-ip-address of VM-01>
   ```

   Reminders

   - Upload the private key to the Cloud Shell that you downloaded earlier to your workstation. Change the permission of the private key file by executing `chmod 400 <private_key_file>`. Reference to upload file to cloud shell.
   - `<private_key_file>` is the full path and name of the file that contains the private key associated with the instance you want to access.
   - `<username>` is the default user `opc`.
   - `<public-ip-address>` is the Public IP address of the instance. In our case, we refer to it as VM-01-Public IP and VM-02-Public IP.
   - **Note:** Enter **yes** in response to "Are you sure you want to continue connecting (yes/no)?"

   You are now connected to the instance IAD-SP-LAB14-1-VM-01.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Niwas Sangwan (ram.niwas@tsecool.com) has a non-transferable license to use this Guide.

9. While connected to your compute instance via SSH, run the following commands to install and configure Apache Web server:

    - Install Apache server:

      ```
      $ sudo yum -y install httpd
      ```

    - Enable Apache and start Apache server:

      ```
      $ sudo systemctl enable httpd

      $ sudo systemctl restart httpd
      ```

    - Create the firewall rule to enable HTTP connection through port 80 and reload firewall:

      ```
      $ sudo firewall-cmd --permanent --add-port=80/tcp

      $ sudo firewall-cmd --reload
      ```

    - Create an index file for your web server:

      ```
      $ sudo bash -c 'echo You are visiting Web Server 1 >>
      /var/www/html/index.html'
      ```

    - Exit the SSH connection:

      ```
      $ exit
      ```

10. Again, use the Cloud shell to SSH to the second instance, `IAD-SP-LAB14-1-VM-02`, by using the following command:

    ```
    $ ssh -i <private_key_file> <username>@<public-ip-address of VM-02>
    ```

    Note: Enter yes in response to "Are you sure you want to continue connecting (yes/no)?"

11. Repeat step 9 to install Apache Web server on the second compute instance.

    Note: Make sure that the index file command for the second web server looks like this:

    ```
    $ sudo bash -c 'echo You are visiting Web Server 2 >>
    /var/www/html/index.html'
    ```

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Iliwas Saraswan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

12. After executing all the commands successfully, open a browser in your local system and enter the URL http://<Public IP of IAD-SP-LAB14-VM-01 >.

Note: Your browser will not return anything because port 80 is not opened yet for instance subnet.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Niwas Sangwan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Create a Security List and an Additional Load Balancer Subnet

Before you create the load balancer, you will create a new security list. This security list will be used by the load balancer (which will be created later). This will ensure all traffic to the web server is allowed. Load balancers should always reside in different subnets than your web server/application instances. This allows you to keep your web server/application instances secured in different subnets while allowing public Internet traffic to the load balancers in other subnets.

Tasks

1. From the navigation menu, select **Networking**, and then click **Virtual Cloud Network**.
2. In the left navigation pane, under List Scope, select *<your assigned compartment>* from the drop-down menu.
3. Select **IAD-SP-LAB14-1-VCN-01** from the list of VCNs.
4. In the left navigation pane, under Resources, click **Security Lists.**
5. Click **Create Security List**.
6. In the Create Security List dialog box, enter the following:
   - **Name**: IAD-SP-LAB14-1-LB-SL-01
   - **Create In Compartment**: *<your assigned compartment>*
   - Do not add any Ingress or Egress rules.
7. Click **Create Security List**.

   You now see that the security list is created and displayed on the **Security Lists** page.

   Assuming you are still on your VCN details page, you will next create a Load Balancer subnet.
8. In the left navigation pane, under Resources, click **Subnets.**

Ram Nivas Sangwan (ram.niwas@iseed.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

9. Click **Create Subnet**.

10. In the Create Subnet dialog box, enter the following:

    a. **Name:** `LB-Subnet-IAD-SP-LAB14-1-SNET-02`

    b. **Create In Compartment:** *<your assigned compartment>*

    c. **Subnet Type: Regional**

    d. **IPv4 CIDR Block:** `10.0.3.0/24`

    e. **Security Lists: From the drop-down, select the Security List you created earlier - IAD-SP-LAB14-1-LB-SL-01**

    Note: Leave all the other options in their default setting.

11. **Click Create Subnet.**

    You now see that the subnet is created successfully and in the Available state.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Niwas Sangwan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

Create a Load Balancer and Update Security List

Task-1

1. From the navigation menu, select **Networking**, and then click **Load Balancers.**
2. In the left navigation pane, under List Scope, select <*your assigned compartment*> from the drop-down menu.
3. Click **Create Load Balancer.**
4. Select **Load Balancer** and click **Create Load Balancer**.
5. In the Create Load Balancer dialog box, enter the following:
   a. **Under Add Details** section:
      1) **Load Balancer Name**: `IAD-SP-LAB14-1-LB-01`
      2) **Choose visibility type**: Public
      3) **Assign a public IP address**: Ephemeral IP Address
      4) **Shapes**: Flexible Shapes
      5) **Choose the minimum bandwidth**: 10 Mbps
      6) **Virtual Cloud Network**: IAD-SP-LAB14-1-VCN-01
      7) **Subnet**: Select the Regional Subnet that you created (10.0.4.0 in this lab) - LB-Subnet-IAD-SP-LAB14-1-SNET-02
      8) Click **Next** or **Choose Backends.**
   b. In the **Choose Backends** section:
      1) **Specify a Load Balancing Policy**: Weighted Round Robin
      2) Click **Add Backend**, select the compute instance created earlier, and click **Add Selected Backends -** IAD-SP-LAB14-1-VM-01 and - IAD-SP-LAB14-1-VM-02

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Nivas Sangwan (ram.nivas@tsedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

c. **Specify Health Check Policy:**

1) **Protocol**: HTTP

2) **Port**: 80

3) URL PATH (URI): /

Note: Leave all the other options in their default setting.

4) Click **Next** or **Configure Listener**.

d. In the **Configure Listener** section:

1) **Listener Name**: `IAD-SP-LAB14-1-LB-LISN-01`

2) **Specify the type of traffic your listener handles**: HTTPS

3) **Specify the port your listener monitors for ingress traffic**: 443

e. **Under SSL Certificate:**

1) **Certificate Resource**: Select Certificate Service Managed Certificate.

2) **Certificate in <assigned compartment>**: `IAD-SP-LAB-14-1-CERT-01`

3) If needed, click **Change Compartment**, and then choose the assigned compartment where CA was created.

4) Click **Next** or **Manage Logging**.

f. In the **Manage Logging** section**:**

In the Manage Logging section, ensure that **Error Logs** is disabled. Leave all other options in their default setting.

6. Click **Submit**.

Wait for the load balancer to become active and then note down its **Public IP address**.

Ram Nivas Sangwan (ram.nivas@tseedot.com) has a non-transferable license to use this Guide.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Task-2

You will update Security List for Load Balancer Subnet to allow port 443.

1. From the navigation menu, select **Networking**, and then click **Virtual Cloud Network**.
2. In the left navigation pane, under List Scope, select *<your assigned compartment>* from the drop-down menu.
3. Click **IAD-SP-LAB14-1-VCN-01** from the list of VCNs.
4. In the left navigation pane, under Resources, click **Security Lists.**
5. Click **IAD-SP-LAB14-1-LB-SL-01** from the list of Security Lists.
6. In the left navigation pane, under Resources, click **Ingress Rules**.
7. Click **Add Ingress Rules** and enter the following:
   a. **Do not select the Stateless check box.**
   b. **Source Type:** `CIDR`
   c. **Source CIDR:** `0.0.0.0/0`
   d. **IP Protocol:** `TCP`
   e. **Source Port Range:** `All`
   f. **Destination Port Range:** `443 (the listener port for HTTPs)`
8. Click **Add Ingress Rules.**

   You now see that the ingress rule is successfully added in the security list.
9. In the left navigation pane, under Resources, click **Egress Rules**.

Ram Niwas Sengwan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

10. Click **Add Egress Rules** and enter the following:

    a. **Do not select the Stateless check box.**

    b. **Destination Type:** `CIDR`

    c. **Destination CIDR:** `0.0.0.0/0`

    d. **IP Protocol: TCP**

    e. **Destination Port Range: All**

11. Click **Add Egress Rules.**

    You now see that the egress rule is successfully added in the security list.

You now have the setup configured with a Compute instance running HTTP server with an `index.html` file, and a Load Balancer with all relevant policies and components.

Ram Niwas Sangwan (ram.niwas@tseccu.com) has a non-transferable license to use this Guide.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Copyright © 2023, Oracle and/or its affiliates.

Verify the OCI Certificate with Load Balancer

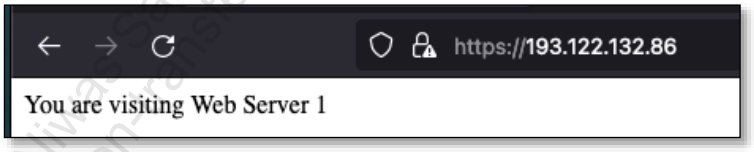
Tasks

1. From the navigation menu, select **Networking**, and then click **Load Balancers.**
2. In the left navigation pane, under List Scope, select *<your assigned compartment>* from the drop-down menu.
3. Select **IAD-SP-LAB14-1-LB-01** from list of load balancers

   Note down the Public IP address.
4. Click the **Developer Tools** icon at the right of the OCI console header and click **Cloud Shell** to launch your Cloud Shell.
5. Enter the following `curl` command to verify the `https` connection to load balancer using CLI:

   ```
   $ curl -k https://<Public IP of IAD-SP-LAB06-1-LB-01>
   ```
6. Open a web browser and enter the URL.

   ```
   https://<Public IP of IAD-SP-LAB14-1-LB-01>.
   ```
7. If it prompts with certificate error, accept the risk and go ahead.
8. Verify that the text in `index.html` is displayed.




```
You are visiting Web Server 1
```

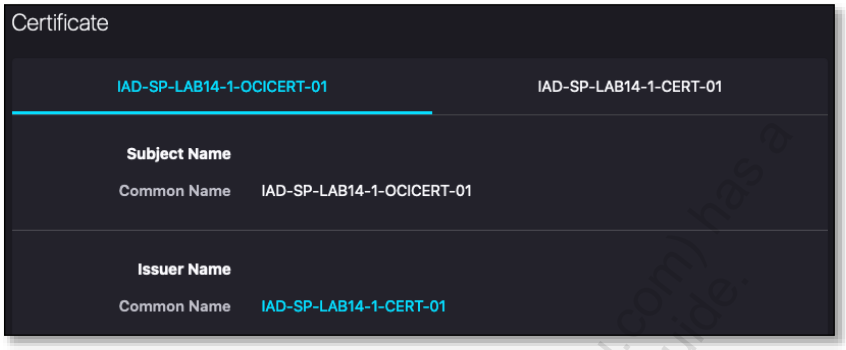
Ram Niwas Sangwan (ram.niwas@tseadu.com) has a non-transferable license to use this Guide

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Copyright © 2023, Oracle and/or its affiliates.

9. You can validate the Web Server's certificate. On a web browser, the created certificate name can be confirmed with the connected Web Server. Click the padlock icon in the address bar for the website or check the site settings to view the certificate.

   The following is a sample screenshot using Mozilla web browser:



Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Niwas Sangwan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

Purge Instructions

Perform the purge operation, as instructed below, before proceeding to the next practice:

Delete Load Balancer

1. From the navigation menu, select **Networking**, then click **Load Balancers.**
2. Select <*your assigned compartment*> from the drop-down menu on the left part of the screen under List Scope.
3. Click **IAD-SP-LAB14-1-LB-01.**
4. Click **Terminate.** Then click **Terminate** in the Confirmation window. Click **Close**.

Delete Certificate

1. From the navigation menu, select **Identity & Security**. Navigate to Certificates and click **Certificates** under it.
2. Select <*your assigned compartment*> from the drop-down menu on the left part of the screen under List Scope.
3. Click **IAD-SP-LAB14-1-CERT-01.**
4. Click **Delete**.
5. Confirm the deletion by entering the certificate name.
6. Click **Select deletion date**, and then choose the date when you want to delete the certificate permanently.
7. Click **Delete Certificate**.

Ram Nivas Sangwan (ram.nivas@ieedu.com) has a non-transferable license to use this Guide

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Delete Compute Instance

1. From the navigation menu, select Compute, and then click **Instances**.
2. Make sure you are in the same compartment as the VCN you created, locate the first compute instance, and click the compute instance name: **IAD-SP-LAB-14-VM-01**
3. Click **More Actions** and then select **Terminate**. Make sure to select **Permanently delete the attached Boot Volume**, and then click the **Terminate** instance.
4. Repeat steps **2** and **3** to terminate the **second compute instance** IAD-SP-LAB-14-VM-02. After the instances are terminated, the color changes to gray from yellow. Wait for both instances termination to be completed.

Delete Virtual Cloud Networks

1. From the navigation menu, select **Networking**, then click **Virtual Cloud.**
2. Make sure you are in the correct compartment. From the list of all VCNs, locate your VCN and click the VCN name: **IAD-SP-LAB-14-1-VCN-01**
3. Click **Delete**.

   Note: You must delete all resources associated with a VCN, before deleting it.
   - When you click **Delete**, a message box appears. Select the **Specific compartment** check box to search the compartments for resources associated with this VCN, and click **Scan**.
   - Wait for the Scan operation to complete.
4. Click **Delete All**.
5. Click **Close** after the **VCN** is deleted.

Ram Niwas Sengwal (ram.niwas@tseodu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Niwas Sangwan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Cloud Security Posture Management: Remediate Problems Identified by Cloud Guard

Lab 15 Practices

Ram Niwas Sangwan (ram.niwas@seelu.com) has a non-transferable license to use this Guide.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Get Started

Overview

Cloud Guard examines your Oracle Cloud Infrastructure resources for security weakness related to configuration, and your operators and users for risky activities. Upon detection, Cloud Guard can suggest, assist, or take corrective actions, based on your configuration.

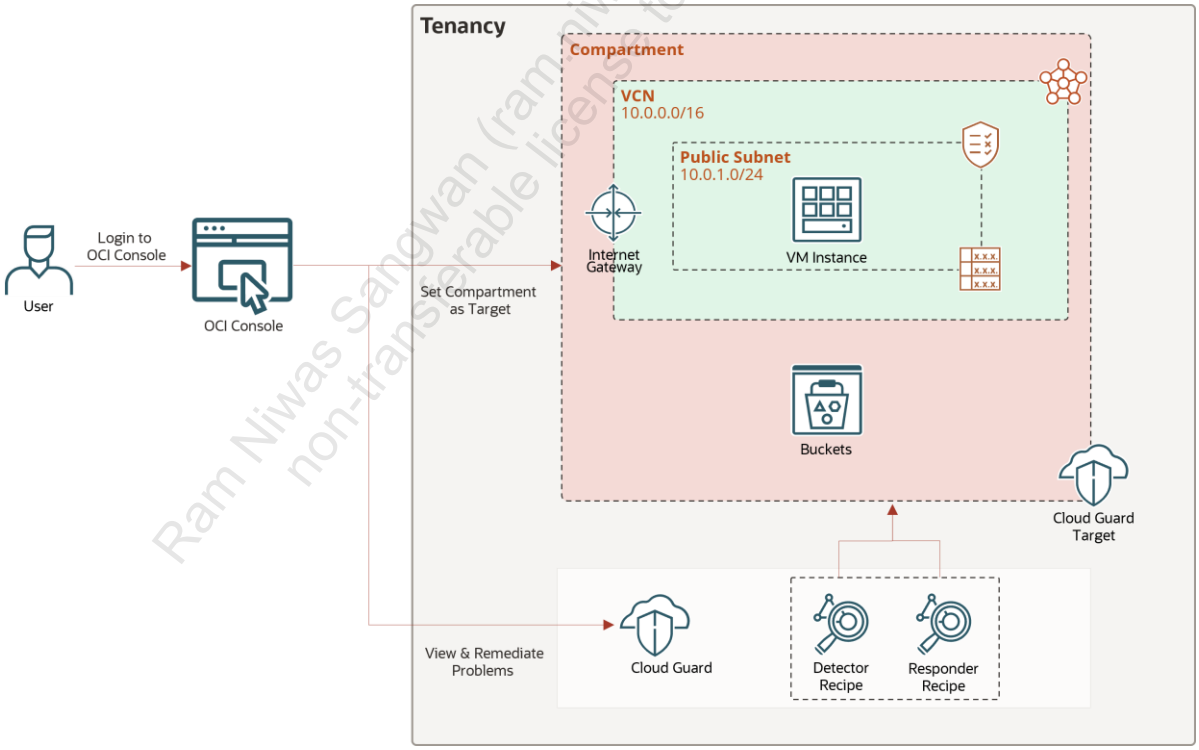
In this lab, you will:

a. Explore Cloud Guard

b. Create a Cloud Guard Target

c. Create a scenario to verify Cloud Guard monitoring

d. Remediate problems identified by Cloud Guard



Ram Niwas Sangwan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

Prerequisites

- You must have access to the OCI Console.
- The Oracle University lab team has set up all the IAM policies required for you to complete this lab.

Assumptions

- Select the region that's available in the tenancy allotted to you. In this lab, we are considering US East (Ashburn) (IAD) as your region.
- You must be familiar with navigating the OCI Console.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Niwas Sangwan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

Explore Cloud Guard

You will explore Cloud Guard to obtain a unified view of your tenancy's cloud security posture. You will also explore Detector recipes for monitoring targets and responder recipes for responding with any problems that occur.

Tasks

1. From the navigation menu, select **Identity & Security**, and then click **Cloud Guard**.

   Note: A dashboard with the current Cloud Guard observations is displayed. If the Guided Tour is displayed, go through the same to explore the various features. You can also click **Stop tour** if you are not interested in the tour. After you are done with the tour, the dashboard, with various options under Cloud Guard on the left side in the browser window, is displayed.

2. In the left navigation pane, under **Cloud Guard**, click **Detector Recipes.**

3. In the left navigation pane, under **Scope**, select the *<Tenancy root compartment>* from the drop-down menu.

   Oracle-managed recipes are listed within the root compartment.

4. Click **OCI Configuration Detector Recipe (Oracle managed)**.

   View the detector rules that are included in this recipe.

5. To view the details of a particular rule, click the **disclosure triangle,** a downward arrow located next to the three dots to the right of the rule.

6. Click **Risk level** to organize rules by their risk level.

7. Click **Detector Recipes** from the breadcrumb list at the top left.

8. Click **OCI Activity Detector Recipe (Oracle Managed)**.

   Explore the rules that are within activity detector recipe. You also see that for the built-in Oracle-managed detector recipes, you can clone the recipe. You may clone an existing recipe and customize it to your needs.

9. Click **Detector recipes** from the breadcrumb list at the top left.

10. In the left navigation pane, under **Cloud Guard**, click **Responder Recipes.**

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Nivas Gangwar (ramniwas@tssedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

11. Click the **OCI Responder Recipe (Oracle Managed)**.

    View the responder rules that are included in this recipe.

12. To view the details of a particular rule, click the **disclosure triangle,** a downward arrow located next to the three dots to the right of the rule.

13. Click **Risk level** to organize rules by their risk level.

14. Click **Responder recipes** from the breadcrumb at the top left.

15. In the left navigation pane, under **Cloud Guard**, click **Managed Lists**.

16. Click the **Oracle Cloud Guard CIDR Managed List**.

    Note: A managed list is a reusable list of parameters that makes it easier to set the scope for detector and responder rules. A managed list is a tool that can be used to apply certain configurations to detectors.

    Under **Entries,** observe the predefined list of trusted IP Address ranges used by Oracle Cloud Infrastructure (OCI). Cloud Guard also lets you define your own managed lists as needed.

    For example, you can define lists of states or provinces, ZIP codes, OCIDs, or whatever else you may define. Click the **Managed Lists** breadcrumbs and you will see an option to create your own managed list.

17. In the left navigation pane, under **Cloud Guard**, click **Settings**.

    Note: Observe the reporting region listed. If you are in the home region of your tenancy, you will also see the option to **Disable Cloud Guard** (if it is already enabled). If you are in any other region, this button will be disabled.

Ram Narasimhan (ram.niwas@tseet.com) has a non-transferable license to use this Guide.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Creating a Cloud Guard Target

You will learn to add a target to set the scope of resources that Cloud Guard monitors.

Note: Cloud Guard is enabled in your practice tenancy.

Tasks

1. From the navigation menu, select **Identity & Security**, and then click **Cloud Guard**.
2. In the left navigation pane, under **Cloud Guard**, click **Targets.**
3. In the left navigation pane, under **Scope**, select *<your assigned compartment>* from the drop-down menu.

Note: If you already have a specific target set for your compartment, delete it.

4. Click **Create new target**.
5. Enter the following:
   a. **Target Name:** `IAD-SP-LAB15-1-CG-01`
   b. **Description:** Enter a meaningful description.
   c. **Compartment:** *<your assigned compartment>*
   d. **Configuration detector recipe:** OCI Configuration Detector Recipe (Oracle managed)
   e. **Threat detector recipe:** OCI Threat Detector Recipe (Oracle managed)
   f. **Activity Detector Recipe:** Oracle Activity Detector Recipe (Oracle managed)
   g. **Responder recipe:** OCI Responder Recipe (Oracle managed)
6. Click **Create** to create the target.

   The detail page for the new target will be displayed.
7. In the left navigation pane, under **Resources**, click **Detector recipes**

   View the detector recipes associated with the created target.

Ram Nivas Sanwal (ram.nivas@tseed.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

Creating a Scenario to Verify Cloud Guard Monitoring

To identify a problem in the set target, you will create a Virtual Cloud Network in OCI with a public and a private subnet, create a bucket and make its visibility public, as well as create an instance with a public IP address.

Task-1

To create a Virtual Cloud Network in OCI with a public and a private subnet using the VCN Wizard.

1. Open the navigation menu and click **Networking**. Under Networking, click **Virtual Cloud Network**.
2. In the left navigation pane, under **List Scope**, select the assigned **compartment** from the drop-down menu.
3. Click **Start VCN Wizard**
4. Select **Create VCN with Internet Connectivity** and click **Start VCN Wizard.**
5. On the Configuration page, enter the following:
   a. **Name**: `IAD-SP-LAB15-1-VCN-01`
   b. **Compartment:** *<your assigned compartment>*

      Note: Leave all the other options in their default setting.

   c. Click **Next**.
   d. Verify the details on the **Review and Create** page.
6. Click **Create** to start creating the VCN and its resources.
7. Click **View Virtual Cloud Network** to verify the creation of the VCN and its resources.
8. You can now see that the VCN is successfully created and is in the Available state, with the following components:

   VCN, Public subnet, Private subnet, Internet gateway, NAT gateway, Service gateway

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Nivas Sarawan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Task-2

To create a compute instance hosted in this VCN's public subnet.

1. From the navigation menu, click **Compute**, and then click **Instances**.
2. In the left navigation pane, under List Scope, select *<your assigned compartment>* from the drop-down menu.
3. Click **Create Instance**. In the Create Instance dialog box, provide the following details:
    a. **Name**: `IAD-SP-LAB15-1-VM-01`
    b. **Create in compartment**: < *your assigned compartment* >
    c. **Placement:** `AD1`

    Note: If Service limit error is displayed, choose a different Availability Domain.

    d. **Image**: Oracle Linux 8
    e. **Shape:** Click **Change shape**, then in the **Shape** field, click **Change Shape**. Then, select **Ampere shape series** field and select the **VM.Standard.A1.Flex** shape with **1** OCPU and **6 GB** memory**.**
    f. **Networking**: Pick available VCN and Public Subnet

    Note: If no VCN and Public Subnet are available, select Create new virtual cloud network.

    g. **Public IP address** – Assign a public IPv4 address
    h. **SSH Key:** This entry is not required.

    Note: Leave all the other options in their default setting.
4. Click **Create.**

    Note: After a couple of minutes, you can see that the Instance is successfully created, and the state is Running.

Ram Nivas Sangwan (ramnivas@tsedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Task-3

You need to update your public IP address in Network Source before creating a bucket.

Note: If your public IP address is already listed as a network source, you can skip task 3 and proceed to task 4.

1. To obtain your public IP address, open a web browser and perform a Google search for "what is my public ip?"

   Note down the Public IP address.

2. From the navigation menu, click **Identity & Security**, and then click **Network Sources**

3. Locate and click the `IAD-SP-LAB05-1-NS-01` network source in the list to view its details.

   In your environment, an `IAD-SP-LAB05-1-NS-01` network source is precreated.

4. Click **Add Networks**.

5. In the **Add Networks** dialog box, enter the following:

   - **Network type**: Public Network
   - **IP Address/CIDR Block**: `<YOUR_PUBLIC_IP_ADDRESS>`

6. Click **Update**.

   Your public IP address or CIDR block has successfully been added as a network to the IAD-SP-LAB05-1-NS-01 network source.

Task-4

To create a bucket with public visibility.

1. From the navigation menu, click **Storage**. Navigate to Object Storage, and then click **Buckets**.

2. In the left navigation pane, under List Scope, select *<your assigned compartment>* from the drop-down menu.

3. Click **Create Bucket**.

Copyright © 2023, Oracle and/or its affiliates.

4. In the **Create Bucket** dialog box, specify the attributes of the bucket:

   a. **Bucket Name:** `IAD-SP-LAB15-1-BKT-01-<user-id>`
   Please specify your user id in place of `<user-id>` to make it unique.

   b. **Default Storage Tier:** Select `Standard`.

   Note: Leave all the other options in their default setting.

5. Click **Create**.

   You can see the bucket listed for your compartment.

6. Click the three dots on the right to open the Actions menu and select **Edit Visibility**. Select **Public** and click **Save Changes**.

   Note: You have now created an instance with a public IP address and a bucket with public visibility in the assigned compartment. To assure cloud security posture, the detector recipe includes a configuration rule for instance with a public IP address and Bucket with a public visibility.

   As a result, you must wait for Cloud Guard to evaluate your allocated detector configuration and list its observations on the set target. Wait 25-30 minutes before checking the Cloud Guard Dashboard to see if the problem has been identified and resolving it.

Ram Niwas Sangwan (ramniwas@tseclu.com) has a non-transferable license to use this Guide

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Copyright © 2023, Oracle and/or its affiliates.

Remediate the Problem Identified by Cloud Guard

To view details of Cloud Guard-identified problems and take action on them using the responder recipe:

1. From the navigation menu, select **Identity & Security**, and then click **Cloud Guard**.
2. In the left navigation pane, under **Cloud Guard**, click **Problems.**
3. In the left navigation pane, under List Scope, select *<your assigned compartment>* from the drop-down menu.
4. View the list of problems that Cloud Guard has identified with the resources in your assigned compartment based on your previous practices. The Problems page displays information about each problem, including:
   - Problem Name
   - Risk Level
   - Detector Type
   - Resource affected
   - Target
   - Region
   - Labels
   - First Detected
   - Last Detected

Task-1

Follow this process to remediate the problem - Instance has a public address:

1. In the left navigation pane, under Resource type**,** select **Instance**
2. Click **Instance has a public address**.
3. Review the problem details and problem history before taking action.

   Note: As per the problem details, you have the option to remediate (if there are any responder suggestions) or mark it as resolved or dismiss the problem.

   The problem specifies that Instance has a public IP address, it is recommended to carefully assess whether Instance requires internet connection via a public IP address and to act if it does not.

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Niwas Sangwan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide

4. Click **Remediate** to deallocate instance public IP address.

5. On **Remediate** dialog box, enter the following:

    a. Remediation responder rule: Select **Delete Public IP(s)** from the drop-down list.

    b. Confirm the necessary permissions. Policy statements are already present in your environment; there is no need to add them.

    Note: To remediate, Cloud Guard will need permissions to take actions on your behalf for that resource.

6. Click **Remediate** and confirm that you want to execute the responder to remediate the problem.

    Note: After a couple of minutes, you can see that the problem is successfully resolved, and the problem icon turns green.

7. In the left navigation pane, under Resources, select **Responder activity** to view the responder's actions related to this problem.

8. To verify that the problem has been resolved, click the navigation menu and click **Instances** under **Compute**. Click the instance **IAD-SP-LAB15-1-VM-01**. You will now see that the instance does not have a Public IP address.

Task-2

Follow this process to remediate problem - Bucket is Public.

1. In the breadcrumb on the top left, click **Problems**.

2. In the left navigation pane, under Resource type**,** select **Bucket** from the drop-down menu.

3. Click "**Bucket is Public**" from the problem list.

4. Check problem details and problem history, before actions are taken.

    Note: As per the problem details, you have the option to remediate (if there are any responder suggestions) or mark it as resolved or dismiss the problem.

    The problem specifies that the bucket has a public visibility; it is recommended to carefully assess whether public visibility is required for the mentioned resource and to act if it does not.

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram N was Sangwan (ram.nwas@seedtl.com) has a non-transferable license to use this Guide.

5. Click **Remediate** and confirm that you want to execute the responder to remediate the problem.

   Confirm the necessary permissions. Policy statements are already present in your environment; there is no need to add them.

6. In the left navigation pane, under Resource type**,** select **Responder activity** to view responder actions related to this problem.

   Note: After a couple of minutes, you can see that the problem is successfully resolved, and problem icon turns green.

7. To verify the problem has been resolved, click **Buckets** under **Object storage**. Click the bucket **IAD-SP-LAB15-1-BKT-01-<usert-id>.** You will now see that the visibility is now Private.

Similarly, look at other problems reported, related to VCN and other resources.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Niwas Sangwan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Purge Instructions

Perform the purge operation, as instructed below, before proceeding to the next practice:

Delete Instance

1. From the navigation menu, select Compute, and then click **Instances**.
2. In the left navigation pane, under List Scope, select the assigned **compartment** from the drop-down menu.
3. Locate and click the **IAD-SP-LAB15-1-VM-01** compute instance**.**
4. Click **Terminate**. Make sure to check the **Permanently delete the attached Boot Volume** and then click **Terminate** instance.
5. Wait for the instance termination to be completed.

Delete Bucket

1. From the navigation menu, select **Storage**. Navigate to Object Storage, then click **Buckets**.
2. In the left navigation pane, under List Scope, select *<your assigned compartment>* from the drop-down menu.
3. Click the Bucket: **IAD-SP-LAB15-1-BKT-01-<user-id>**
4. Click **Delete** and then enter the Bucket name and click **Delete** in the Confirmation window.

Delete Cloud guard Target

1. From the navigation menu, select Identity & Security, and then click **Cloud Guard**.
2. In the left navigation pane, under List Scope, select *<your assigned compartment>* from the drop-down menu.
3. Select **Targets** from the options listed on the left.
4. Click **IAD-SP-LAB15-1-CG-01**.
5. Click **Delete.**

Copyright © 2023, Oracle and/or its affiliates.

6. Then select the check box and click **Delete target(s)** in the Confirmation window.

Delete VCN

1. From the navigation menu, select Networking, and then click **Virtual Cloud Networks**.
2. In the left navigation pane, under **List Scope**, select *<your assigned compartment>* from the drop-down menu.
3. In the list of VCNs, click the three dots on the right of IAD-SP-LAB15-1-VCN-01 to open the Actions menu. Select **Delete**.
4. Make sure that the **Search compartments for resources associated with this VCN** check box is selected.
5. In the white box that starts with **Select which compartments to search for associated resources**, click the **Specific compartments** option and select *<your assigned compartment>* from the drop-down menu.
6. Click **Scan.**
7. After the scan has completed, click **Delete All**.

   Note: This process can take up to two minutes.

Ram Niwas Sangwan (ram.niwas@tcs.com) has a non-transferable license to use this Guide.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Niwas Sangwan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Cloud Security Posture Management: Configure Security Zones Using Maximum Security Zones

Lab 16 Practices

Ram Niwas Sangwan (ram.niwas@oracle.com) has a non-transferable license to use this Guide.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Get Started

Overview

Security Zones enforce security posture on OCI cloud compartments and prevent actions that can compromise a customer's security posture. Security Zone policies can be applied to various cloud infrastructure types (network, compute, storage, database, and so on) to guarantee cloud resources ensure security and to prevent potential misconfigurations.

In this lab, you'll:

a. Set up a security zone with Maximum Security Recipe

b. View the security zone policies attached to a created security zone

c. Test creating a bucket in an assigned compartment using an Oracle-managed key

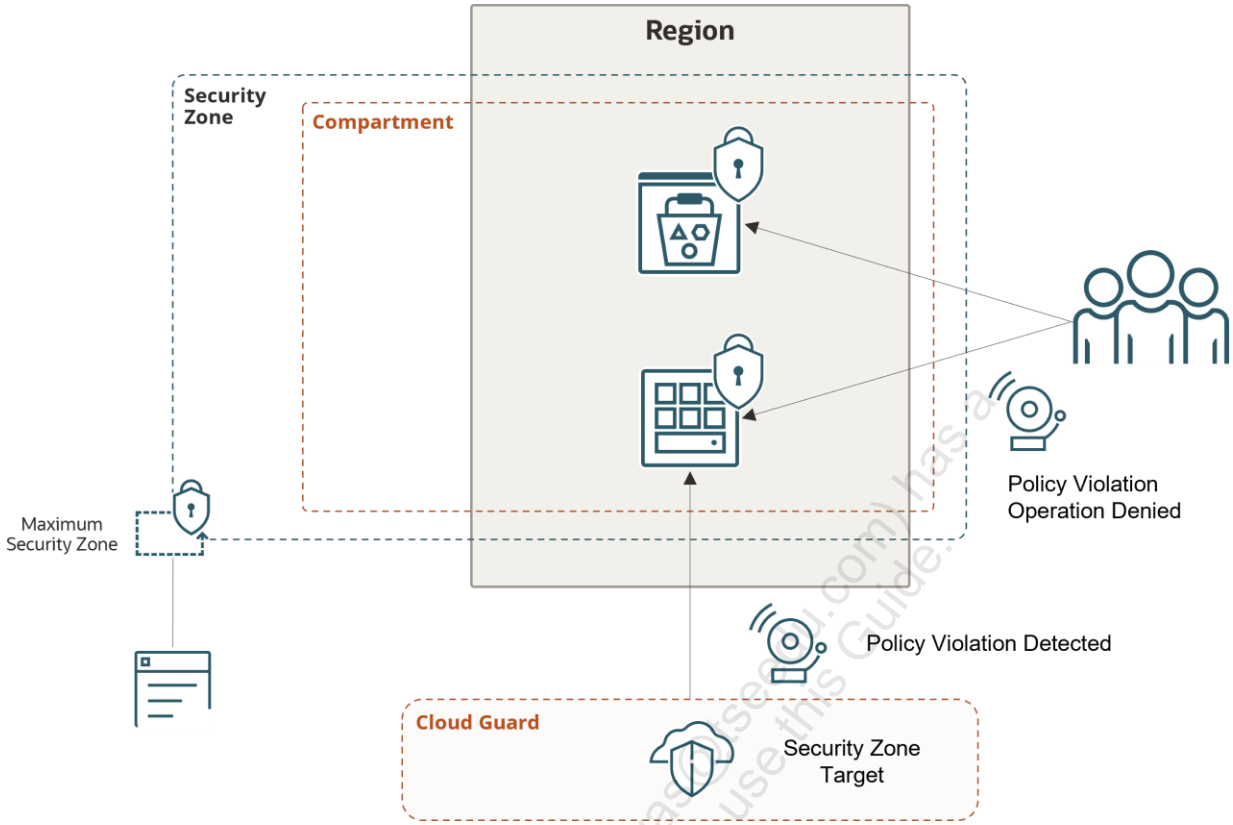
d. Create Master Encryption Key (MEK) in an OCI Vault

e. Test creating a bucket in an assigned compartment by using a customer-managed key

f. Test the security zone policy that restricts public access

Ram Niwas Sangwan (ram.niwas@ceeiu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.



Prerequisites

- You must have access to the OCI Console.
- Your tenancy should have Cloud Guard enabled.
- Precreated Vault in root compartment
- The Oracle University lab has all the necessary configuration, such as security service level permission and required IAM policies.

Assumptions

- Select the region that's available in the tenancy allotted to you. In this lab, we are considering US East (Ashburn) (IAD) as your region.
- You must be familiar with navigating the OCI Console.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Set Up Security Zone with Maximum Security Recipe

You'll create a security zone for an allocated compartment and check for any security zone policy violations.

Tasks

1. From the navigation menu, select **Identity & Security**. Navigate to Security Zones, and then click **Overview**.
2. In the left navigation pane, under **Scope**, select *<your assigned compartment>* from the drop-down menu.

   Notes

   - The compartment should not be associated with a security zone.
   - By default, all subcompartments are also in the same security zone.
3. Click **Create Security Zone.**
4. On the Create Security Zone page, enter the following values:
   a. **Security Zone Recipe:** Select **Oracle-managed** to use Maximum Security Recipe.
   b. **Name**: `IAD-SP-LAB16-1-SZ-01`
   c. **Description**: My Security Zone
   d. **Create for compartment**: *<your assigned compartment>*
5. Click **Create Security Zone**.

   Note: When you create a security zone for a compartment, Cloud Guard does the following:
   - Deletes any existing Cloud Guard target for the compartment and for any child compartments
   - Creates a security zone target for the compartment
   - Adds the default Oracle-managed detector recipes to the security zone target

Ram Nivas Sarawan (ram.nivas@ucedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

View the Security Zone Policies Attached with a Created Security Zone

You'll identify the recipe associated with the newly formed security zone, and then review its policies.

1. From the navigation menu, select **Identity & Security**. Navigate to Security Zones, and then click **Overview**.
2. In the left navigation pane, under Scope, select *<your assigned compartment>* from the drop-down menu.
3. Click the **IAD-SP-LAB16-1-SZ-01** security zone and view the Security Zone details page.
4. On the Security Zone information tab, locate the attached Recipe and click the **Recipe** for this security zone - Maximum Security Recipe – 20200914.
5. View the Oracle-managed recipe attached to the Security Zone created on the **Recipe details** page.
6. View few policy statements with associated Resource types:

```
deny public_subnets in VIRTUALNETWORK
deny public_buckets in OBJECTSTORAGE
deny buckets_without_vault_key in in OBJECTSTORAGE
```

Next, you'll put a security zone to test by attempting to violate a few of its policies.

Ram Niwas Sangwan (ram.niwas@seedu.com) has a non-transferable license to use this Guide.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Verify Creating a Bucket in an Assigned Compartment Using Oracle Managed Key

You will test the security zone. Create a bucket to check if it is restricted in the security zone. As a reference, the security zone recipe has a policy that prohibits bucket creation without a customer-managed vault key.

Task-1

You need to update your public IP address in Network Source before creating a bucket.

Note: If your public IP address is already listed as a network source, you can skip task 1 and proceed to task 2.

1. To obtain your public IP address, open a web browser and perform a Google search for "what is my public ip?"

   Note down the Public IP address.

2. From the navigation menu, select **Identity & Security**, and then click **Network Sources**.

3. Locate and click the **IAD-SP-LAB05-1-NS-01** network source in the list to view its details.

   In your environment, an IAD-SP-LAB05-1-NS-01 network source is precreated.

4. Click **Add Networks.**

5. In the **Add Networks** dialog box, enter the following:
   - **Network type**: Public Network
   - **IP Address/CIDR Block**: `<YOUR_PUBLIC_IP_ADDRESS>`

6. Click **Update**.

   Your public IP address or CIDR block has successfully been added as a network to the IAD-SP-LAB05-1-NS-01 network source.

Ram Niwas Sangwan (ramniwas@tseedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Task-2

To create a bucket to observe the security zone violations:

1. Open the navigation menu and click **Storage**. Navigate Object Storage, click **Buckets**.
2. In the left navigation pane, under **List Scope**, select the assigned compartment from the drop-down menu.
3. Click Create Bucket.
4. In the **Create Bucket** dialog box, specify the attributes of the bucket:
   a. **Bucket Name:** `IAD-SP-LAB16-1-BKT-01-<user-id>`
      Please specify your user ID in place of `<user-id>` to make it unique.
   b. **Default Storage Tier:** `Standard`
   c. **Encryption**: Encrypt using Oracle-managed keys.
      Note: Leave all the other options in their default setting.
5. Click **Create**.
   You will receive an error indicating Security zone violation: Encrypt the bucket with a customer-managed encryption key.
   Note: If you receive an authorization error, go back to task 1 and add your public IP address to the network source.
6. Click **Cancel**.

Now, you'll generate a master encryption key in your assigned compartment and then try again to create a bucket in line with the security zone policy.

Ram Nivas Sangwan (ram.nivas@tseedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Create a Master Encryption Key (MEK) in an OCI Vault

You'll use an existing Vault that is at the root level compartment, and create a master encryption key, which is required to create a bucket with a customer-managed key.

Tasks

1. From the navigation menu, select **Identity & Security**, and then click **Vault**.
2. In the left navigation pane, under List Scope, select the root compartment from the drop-down menu.
3. Click **OCI-SECPRO-VAULT** from the list of Vaults.
4. In the left navigation pane, under Resources, click **Master Encryption Keys**.
5. Click **Create Key**.
6. In the **Create Key** dialog box, enter the following:
   a. **Create in Compartment:** *<your assigned compartment name>*
   b. **Protection Mode**: `HSM`
   c. **Name**: `IAD-SP-LAB16-1-MEK-01`
   d. **Key Shape Algorithm**: `AES (Symmetric Key used for Encrypt and Decrypt)`
   e. **Key Shape**: `256 bits`
7. Click **Create Key**.
8. In the left navigation pane, under List Scope, select *<your assigned compartment>* from the drop-down menu.

   It will take about a minute to create the master encryption key. The key will go through the Creating state to the Active state.

   You can view the master encryption key created in your assigned compartment.

Ram Niwas Sangwan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Verify Creating a Bucket in an Assigned Compartment Using Customer Managed Key

You will test the security zone. Create a bucket and see if it is restricted. As a reference, the security zone recipe has a policy that prohibits bucket creation without a customer-managed vault key.

1. Open the navigation menu, select **Storage**. Navigate to Object Storage, and then click **Buckets**.
2. In the left navigation pane, under List Scope, select *<your assigned compartment>* from the drop-down menu.
3. Click **Create Bucket**.
4. In the **Create Bucket** dialog box, specify the attributes of the bucket:
   a. **Bucket Name:** `IAD-SP-LAB16-1-BKT-01-<user-id>`
      Please specify your user ID in place of `<user-id>` to make it unique.
   b. **Default Storage Tier:** `Standard`
   c. **Encryption:** Select **Encrypt using customer-managed keys**.
   d. Change Compartment and select **root compartment** from the drop-down list.
   e. **Vault:** Select **OCI-SECPRO-VAULT**
   f. **Master Encryption Key:** Select key created earlier - `IAD-SP-LAB16-1-MEK-01`.
      Note: If the key is not visible, change the compartment to the assigned compartment.
   g. Keep all other parameters to its default value.
5. Click **Create**.

According to the security zone policy, the bucket is created immediately. It enforces security posture on OCI cloud compartments and prevents actions, which could compromise the security posture of a customer.

Ram Nivas Sanjiwan (ram.niwas@seedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

Verify the Security Zone Policy That Restricts Public Access

You will test the security zone. Create a VCN and create a public subnet or Internet gateway to verify whether it is restricted. As a reference, the security zone recipe has a policy that restricts public access.

1. From the navigation menu, select **Networking**, and then click **Virtual Cloud Network**.
2. In the left navigation pane, under List Scope, select *<your assigned compartment>* from the drop-down menu.
3. Click **Create VCN.**

   Enter the following:

   - **Name**: `IAD-SP-LAB16-1-VCN-01`
   - **Create in Compartment:** *<your assigned compartment>*
   - **IPv4 CIDR Blocks:** `10.0.0.0/16`
   - Press **Enter** to add.

   Note: Leave all the other options in their default setting.
4. Click **Create VCN**.

   You now see that the VCN is created successfully and in the Available state.
5. Click **Create Subnet**.
6. In the Create Subnet dialog box, enter the following:
   - **Name**: `IAD-SP-LAB16-1-SNET-01`
   - **Create in Compartment:** *<your assigned compartment>*
   - **Subnet Type:** Regional (Recommended)
   - **IPv4 CIDR Block:** `10.0.1.0/24`
   - **Subnet Access:** Public Subnet

   Note: Leave all the other options in their default setting.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Nivas Sangwan (ram.niwas@seedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

7. Click Create Subnet.

   You will receive an error indicating Security zone violation: Subnets in a security zone can't be public. All subnets must be private.

Congratulations! Using the maximum security zone recipes, you were able to successfully imply the security zone on the compartment. In addition, the security zone environment was evaluated against the aforementioned policies.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Niwas Sangwan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

Purge Instructions

Perform the purge operation, as instructed below, before proceeding to the next practice:

Delete Virtual Cloud Networks

1. From the navigation menu, select **Networking**, then click **Virtual Cloud Networks**.
2. Make sure you are in the correct compartment. From the list of all VCNs, locate your VCN and click its name - **IAD-SP-LAB16-VCN-01.**
3. Click **Terminate**, and then click **Terminate All** in the Confirmation window.
   Click **Close** once VCN is deleted.

Delete Bucket

1. From the navigation menu, select **Storage**. Navigate to **Object Storage**, click **Buckets**.
2. Select the assigned **compartment** from the drop-down menu on the left part of the screen under List Scope.
3. From the list of buckets, click **IAD-SP-LAB16-1-BKT-01-<user-id>**.
4. Click **Delete.** Then click **Delete** in the Confirmation window.

Delete Key

1. From the navigation menu, select **Identity & Security**, and then click **Vault**.
2. Select the **root compartment** from drop-down menu on the left part of the screen under List Scope.
3. From the list of vaults in the root compartment, click **OCI-SECPRO-VAULT**.
4. Select your given compartment. From the list of keys given, locate your master key and click its name - **IAD-SP-LAB16-1-MEK-01**.
5. Click **Delete Key**. Confirm that you want to delete this key by clicking the box and entering `IAD-SP-LAB16-1-MEK-01`. You can select a delete date. Click **Delete Key**. Wait for the deletion schedule to be confirmed.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Niwas Sangwan (ram.niwas@tsedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

Delete Security Zone

1. From the navigation menu, select **Identity & Security**. Navigate to **Security Zones**, and click **Overview**.

2. Make sure you are in your given compartment.

3. From the list of Security Zones, locate your Security Zone and click its name - **IAD-SP-LAB16-1-SZ-01**.

4. Click **Delete.** Then click **Delete** in the Confirmation window.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Niwas Sangwan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Niwas Sangwan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Cloud Security Posture Management: Enforcing Least-Privileged Model Using Custom Security Zones

Lab 17 Practices

Ram Niwas Sangwan (ram.niwas@tcs.com) has a non-transferable license to use this Guide.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Get Started

Overview

Custom Security Zones (CSZ) enable users to quickly and easily deploy security policies to enforce desired security postures and prevent changes that could compromise a customer's security configuration. Security Zone policies can be applied to various types of cloud infrastructure (network, compute, storage, database, and so on) to assure the security of cloud resources and prevent security misconfigurations. Users define Custom Security Zone policy sets to determine which policies are appropriate for their application/resources need.

The advantage of the custom security zone option is that you can not only create a recipe that helps meet your security requirements, but you can also create multiple policy sets representing various security needs for each compartment or resource type. Policies that support various application areas or resource types can be readily applied to specific resources in your tenancy. As an example, you could have a database security zone policy that applies to all your database resources and only allows rules related to database security to be activated.

In this lab, you'll:

- Set up a security zone with Maximum Security Recipe
- Create a custom security zone recipe
- Set up a custom security zone and attach to a compartment
- Test the environment by creating a bucket in an assigned compartment

Prerequisites

- Your tenancy should have Cloud Guard enabled.
- The Oracle University lab has all the necessary configuration, such as security service level permission and required IAM policies.

Ram Nawas Sangwan (ram.nawas@teqcloud.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

Set Up a Security Zone with Maximum Security Recipe

You will use the Oracle-managed Maximum Security Recipe and apply all restrictions, and then create a security zone in the assigned compartment.

Note: Ignore the following steps if you have already used Oracle-managed Maximum Security Recipe on the assigned compartment.

Tasks

1. From the navigation menu, select **Identity & Security**. Navigate to Security Zones and click **Overview**.

2. In the left navigation pane, under Scope, select *<your assigned compartment>* from the drop-down menu.

   Notes

   - Select a compartment that is not already associated with a security zone.
   - By default, all subcompartments are also in the same security zone.

3. Click **Create Security Zone.**

4. On the Create Security Zone page, enter the following values:

   a. **Security Zone Recipe:** Select **Oracle-managed** to use Maximum Security Recipe.

   b. **Name**: `IAD-SP-LAB17-1-SZ-01`

   c. **Description**: My Security Zone

   d. **Create for compartment**: Select the assigned compartment from the drop-down list.

5. Click **Create Security Zone**.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Niwas Sanwal (ram.niwas@seedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Create a Bucket in Compartment to Test the Environment

You will test the maximum security zone associated with the assigned compartment.

As a reference, Maximum Security Recipe has a policy that prohibits bucket creation without a customer-managed vault key.

Task-1

You need to update your public IP address in Network Source before creating a bucket.

Note: If your public IP address is already listed as a network source, you can skip task 1 and proceed to task 2.

1. To obtain your public IP address, open a web browser and perform a Google search for "what is my public ip?"

   Note down the Public IP address.

2. Open the navigation menu and select **Identity & Security**. Under Identity & Security, click **Network Sources**.

3. Locate and select the `IAD-SP-LAB05-1-NS-01` network source in the list to view its details.

   In your environment, an `IAD-SP-LAB05-1-NS-01` network source is precreated.

4. Click **Add Networks.**

5. In the **Add Networks** dialog box, enter the following:
   - **Network type**: Select Public Network.
   - **IP Address/CIDR Block**: `<YOUR_PUBLIC_IP_ADDRESS>`

6. Click **Update**.

   Your public IP address or CIDR block has successfully been added as a network to the IAD-SP-LAB05-1-NS-01 network source.

Ram Nivas Sanjwan (ram.nivas@tseedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Task-2

Create a bucket in the assigned compartment.

1. From the navigation menu, click **Storage**. Navigate to Object Storage and click **Buckets**.
2. In the left navigation pane, under Scope, select *<your assigned compartment>* from drop-down menu.
3. Click **Create Bucket**.
4. On the **Create Bucket** page, enter the following values:
   a. **Bucket Name**: `IAD-SP-LAB17-1-BKT-01-<user-id>`
      Please specify your user ID in place of `<user-id>` to make it unique.
   b. **Default Storage Tier**: Select **Standard.**
   c. **Encryption**: Select Encrypt using Oracle-managed keys.

      Note: Leave all the other options in their default setting.
5. Click **Create**.

   You will receive an error indicating **Security zone violation: Encrypt the bucket with a customer-managed encryption key.**

   As expected, this will not be allowed due to the maximum-security zone policy enforcement that is in place - requiring the use of Vault encryption keys.
6. Click **Cancel.**

Ram Niwas Sharma (ram.niwas@tseedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

Task-3

Delete the Security Zone with Maximum Security Recipe.

1. From the navigation menu, click **Identity & Security**. Under Security Zones, click **Overview**.
2. Select *<your assigned compartment>* from the drop-down menu on the left of the screen under List Scope.
3. Click **IAD-SP-LAB17-1-SZ-01.**
4. Click **Delete** on the Security Zone Details page.
5. When prompted for confirmation, click **Delete**.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Niwas Sangwan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

Create a Custom Security Zone Recipe

You'll create a custom recipe based on Oracle-managed Maximum Security Recipe allowing the creation of Buckets with Oracle Managed Keys and can have public visibility.

Tasks

1. From the navigation menu, select **Identity & Security**. Navigate to Security Zones and click **Recipes**.
2. In the left navigation pane, under Scope, select *<your assigned compartment>* from the drop-down menu.
3. Click **Create Recipe.**
4. On the Create Recipe page, enter the following values:
    a. Recipe name: `IAD-SP-LAB17-1-CSP-01`
    b. Description: My custom security zone recipe for object storage.
    c. Create for compartment: Select assigned compartment from the drop-down list.
    d. Click **Next.**
    e. Policy type: All
    f. Resource type: **OBJECTSTORAGE**
    g. Deselect **deny public_bucket** and **deny buckets_without_vault_key.**
    h. Click **Next.**
    i. On the Review page, review the number of policies that are enabled and disabled in this recipe.
5. Click **Create.**

    Custom security zone recipe is created and you are redirected to the Recipe details page.

Next, after creating a recipe, you can create a custom security zone for an assigned compartment that gets associated with the created recipe.

Ram Niwas Sahnwan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Copyright © 2023, Oracle and/or its affiliates.

Set Up a Custom Security Zone

You will create a security zone for the assigned compartment and attach a custom security zone recipe.

Tasks

1. From the navigation menu, select **Identity & Security**. Navigate to Security Zones and click **Overview**.
2. In the left navigation pane, under Scope, select *<your assigned compartment>* from the drop-down menu.
3. Click **Create Security Zone**.
4. On the Create Security Zone page, enter the following values:
   a. **Security Zone Recipe**: Select **Customer-managed** to use Custom Security Zone Recipe.
   b. Select Security Zone Recipe **IAD-SP-LAB17-1-CSP-01** in the assigned compartment.

      If the assigned compartment is not selected by default, click **Change Compartment,** and select the assigned compartment.
   c. **Name:** `IAD-SP-LAB17-1-CSZ-01`
   d. **Description**: My Custom Security Zone.
   e. **Create for compartment**: Select the assigned compartment from the drop-down list.
   f. Click **Create Security Zone**.

   The new security zone is in the **Creating** state. It can take several minutes to associate assigned compartment with the security zone. When finished, the security zone is in the **Active** state.
5. On the Security Zone information tab, you can view attached **IAD-SP-LAB17-1-CSP-01** recipe.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Nivas Sangwan (ramnivas@seedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

Create a Bucket in an Assigned Compartment to Test the Environment

You will test the custom security zone attached to an assigned compartment.

As a reference, the Maximum Security Recipe has a policy that prohibits bucket creation without a customer-managed vault key. But the custom security zone recipe allows bucket with Oracle-managed key and public visibility.

Task-1

You need to update your public IP address in network source before creating a bucket.

Note: If your public IP address is already listed as a network source, you can skip task 1 and proceed to task 2.

1. To obtain your public IP address, open a web browser and perform a Google search for "what is my public ip?"

   Note down the Public IP address.

2. From the navigation menu, select Identity & Security. Under Identity & Security, click **Network Sources**.

3. Locate and click the `IAD-SP-LAB05-1-NS-01` network source in the list to view its details.

   In your environment, an `IAD-SP-LAB05-1-NS-01` network source is precreated.

4. Click **Add Networks.**

5. In the **Add Networks** dialog box, enter the following:

   - **Network type**: Select Public Network.
   - **IP Address/CIDR Block**: `<YOUR_PUBLIC_IP_ADDRESS>`

6. Click **Update**.

   Your public IP address or CIDR block has successfully been added as a network to the IAD-SP-LAB05-1-NS-01 network source.

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Niwas Samwan (ramniwas@tssedu.com) has a non-transferable license to use this Guide.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Task-2

1. From the navigation menu, select **Storage**. Navigate to Object Storage and click **Buckets**.
2. In the left navigation pane, under Scope, select *<your assigned compartment>* from the drop-down menu.
3. Click **Create Bucket**.
4. On the **Create Bucket** page, enter the following values:
   a. **Bucket Name**: `IAD-SP-LAB17-1-BKT-01-<user-id>`

      Please specify your user ID in place of `<user-id>` to make it unique.

   b. **Default Storage Tier**: Select Standard.

   c. **Encryption**: Select Encrypt using Oracle-managed keys.

      Note: Leave all the other options in their default setting.
5. Click **Create**.

   It will succeed since the custom IAD-SP-LAB17-1-CSP-01 recipe and Security Zone have specifically permitted this bucket creation in assigned compartment.

Ram Niwas Sangwan (ram.niwas@ts.edu.com) has a non-transferable license to use this Guide

Copyright © 2023, Oracle and/or its affiliates.

Purge Instructions

Delete Bucket

1. From the navigation menu, click **Storage**. Navigate to Object Storage and click **Buckets**.
2. Select *<your assigned compartment>* from the drop-down menu on the left of the screen under List Scope.
3. From the list of buckets, select `IAD-SP-LAB17-1-BKT-01-<user-id>`.
4. Click the **Actions menu**, and then click **Delete**.
5. Alternatively, you can choose a bucket and click **Delete** on the bucket details page.
6. Review the summary of resources that will be deleted.
7. Enter the name of the bucket to confirm resource and bucket deletion and click **Delete**.

Delete Security Zone

1. From the navigation menu, select **Identity & Security**. Navigate to Security Zones and click **Overview**.
2. Select *<your assigned compartment>* from the drop-down menu on the left part of the screen under List Scope.
3. Select **IAD-SP-LAB17-1-CSZ-01** that you want to delete.
4. Click **Delete**.
5. When prompted for confirmation, click **Delete**.

Ram Nivas Sangwan (ram.nivas@tseedu.com) has a non-transferable license to use this Guide
Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Copyright © 2023, Oracle and/or its affiliates.

Delete Security Zone Recipe

1. From the navigation menu, select **Identity & Security**. Navigate to Security Zones and click **Recipes**.
2. Select the compartment that contains the recipe you want to delete.
3. Click the recipe **IAD-SP-LAB17-1-CSP-01**, to view its details.
4. Click **Delete** on the Recipe details page.
5. When prompted for confirmation, click **Delete**.

Ram Niwas Sangwan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Security Operations: Configure Alarms with Notifications and Create Monitoring Queries

Lab 18 Practices

Ram Niwas Sangwan (ram_niwas@seed.com) has a non-transferable license to use this Guide.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Get Started

Overview

Oracle Cloud Infrastructure (OCI) Observability and Management provides visibility and actionable insights derived using Machine Learning Algorithms. This platform is open and extensible, and provides cloud-based monitoring and analytics.

Some of the Observability and Management services include Monitoring, Logging, Event Services, Logging Analytics, and Application Performance Monitoring. In this lab, you will create alarms and queries and trigger alarms.

In this lab, you will:

- Create a Virtual Cloud Network (VCN)
- Launch three Compute Virtual Machine instances
- Create alarms and view service metrics
- Create CPU stress and fire alarms
- Create queries

Prerequisites

- The Oracle University lab team has set up all the IAM policies required for you to complete this lab.

Assumptions

- You must be familiar with navigating the OCI Console.
- Select the region available in the tenancy allotted to you. In this lab, **US East (Ashburn)** is considered as your region.

Ram Niwas Singwan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Set Up the Environment

You will configure the cloud environment, and create a virtual network and compute instances. The resources created in this practice will help you complete the rest of the lab.

Task 1: Create a VCN

A **Virtual Cloud Network** (**VCN**) defines a private network in the cloud environment where you can specify networking parameters, such as CIDR block and route tables, along with security controls, such as access control lists and virtual firewalls. You can also allow connectivity to the public Internet. In this task, you will create a VCN.

Note: For a production **VCN** environment, it is recommended to further restrict network access controls to meet your security requirements.

1. In the console ribbon at the top of the screen, click the Region icon to expand the menu and select **US East (Ashburn)**.
2. From the navigation menu, select **Networking**, and then click **Virtual Cloud Networks**.
3. In the left navigation pane, under **Scope**, select *<your assigned compartment>* from the drop-down menu.
4. Click **Create VCN**.
5. In the **Create a Virtual Cloud Network** dialog box, populate the following information:
   - **Name**: IAD-SP-LAB18-1-VCN-01
   - **Create In Compartment**: <*your assigned compartment*>.
   - **IPv4 CIDR Block**: 10.0.0.0/16 (Press **Enter** to add the IP block.)

   Leave other fields as default.
6. Click **Create VCN**.
7. Once the VCN is created, click **IAD-SP-LAB18-1-VCN-01** VCN to view the details page.
8. Under **Resources** in the left navigation panel, click **Internet Gateways**.
9. Click **Create Internet Gateway**.

Ram Nivas Sangwan (ram.nivas@tseedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

10. In the **Create Internet Gateway** dialog box, populate the following information:

    - **Name**: IAD-SP-LAB18-1-IG-01
    - **Create In Compartment**: <*your assigned compartment*>.

11. Click **Create Internet Gateway**.

    Next, make a quick update to the VCN route table to make use of the Internet gateway created in the previous step.

12. Under **Resources** in the left navigation panel, click **Route Tables**.
13. Click **Default Route Table for IAD-SP-LAB18-1-VCN-01**, and then click **Add Route Rules**.
14. In the **Add Route Rules** dialog box, populate the following information:

    - **Target Type:** Internet Gateway
    - **Destination CIDR Block**: `0.0.0.0/0`
    - **Target Internet Gateway**: `IAD-SP-LAB18-1-IG-01`

15. Click **Add Route Rules** to complete the process.

    Finally, create a Subnet within the VCN to identify IP space and deploy a VM.

16. Return to the VCN details page by clicking **IAD-SP-LAB18-1-VCN-01** in the breadcrumb list at the top of the page.
17. Under Resources in the left navigation panel, click **Subnets**. Then click **Create Subnet**.
18. In the Create Subnet dialog box, populate the following information:

    - **Name**: `IAD-SP-LAB18-1-SNET-01`
    - **Create In Compartment**: <*your assigned compartment*>.
    - **Subnet Type**: Regional (Recommended)
    - **IPv4 CIDR Block**: `10.0.0.0/24`
    - **Route Table Compartment in <*your compartment*>**: Default Route Table
    - **Subnet Access**: Public Subnet

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Nivas Sangwan (ram.nivas@tseedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

19. Leave other fields as default.

20. Click **Create Subnet**.

Task 2: Set Up SSH Keys for the Virtual Machine Instance

Before launching a virtual machine instance, you will create SSH keys to authenticate the Instance using the Oracle Cloud Shell.

1. In the OCI Console ribbon at the top of the screen, ensure the correct Region is selected. In this case, the region is **US East (Ashburn)**.

2. Select the Developer Tools icon at the right of the OCI console header and click **Cloud Shell** to launch your Cloud Shell.

3. In the Cloud Shell, ensure you are on the home directory of your account. To check, run the following command:

   ```
   $ pwd
   ```

   Reminder: Do not include the `$` symbol when pasting code into Cloud Shell.

   If you are on your home directory, the value will be `/home/<user_name>`.

4. To change the directory to `.ssh`, run the following command:

   ```
   $ cd .ssh/
   ```

5. If the directory does not exist, create a hidden directory. To do so, run the following command:

   ```
   $ mkdir .ssh/
   ```

6. Now, change directory to `.ssh/` by running the following command:

   ```
   $ cd .ssh/
   ```

7. To create ssh keys, run the following command:

   ```
   $ ssh-keygen -b 2048 -t rsa -f sshkeys
   ```

8. Do not enter a password when prompted. Press **Enter**.

   Note: There are two files saved into the `.ssh` directory: `sshkeys.pub` (public key) and `sshkeys` (private key). The `sshkeys.pub` will be used while creating compute instances, and `sshkeys` will be used to authenticate.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Niwas Sangwan (ram.niwas@tseedr.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

9. Run the following command to view the contents of the `sshkeys.pub` public key.

```
$ cat sshkeys.pub
```

10. Copy and paste the content of `sshkeys.pub` public key into a Notepad file. You will use this content while creating compute instance.

11. Close the Cloud Shell by clicking X at the top-right corner. Then click Exit.

Task 3: Launch Compute Virtual Machine Instance

Now, you will launch a virtual machine in your newly created VCN. For this lab, you will create three instances.

1. In the OCI Console ribbon at the top of the screen, ensure you have selected the same region where you created the VCN.

2. From the navigation menu, select **Compute**, and then click **Instances**.

3. From the left-navigation panel, ensure you are in the compartment allotted to you.

4. Click **Create instance** to create the first instance.

5. In the Create Instance dialog box, provide the following details:

   - **Name**: `IAD-SP-LAB18-1-VM-01`
   - **Create in compartment**: < *your assigned compartment* >
   - **Placement:** Availability Domain will be prepopulated to match the subnet you created earlier.

     Note: If a Service limit error is displayed, choose a different Availability Domain.

   - **Image**: Oracle Linux 8
   - **Shape:** Click **Change shape**, then in the **Shape** field, click **Change Shape**. Then, select **Ampere shape series** field and select the **VM.Standard.A1.Flex** shape with **1** OCPU and **6 GB** memory**.**

   Note: Your options and naming conventions may not match exactly as given here, so select an appropriate shape if it is shown different for your region.

6. In the Primary network field, select Existing Virtual Cloud Network and ensure IAD-SP-LAB18-1-VCN-01 is specified in the Virtual cloud network field.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Nivas Sengvan (ramnivas@tse.edu.com) has a non-transferable license to use this Guide

Copyright © 2023, Oracle and/or its affiliates.

7. In the Subnet field, select **Select Existing Subnet**. Ensure that the subnet is specified as **IAD-SP-LAB18-1-SNET-01**.

   If not, double-check if the compartment is set to <*your assigned compartment*>. You may have to switch to a different Availability Domain (see above – the Availability Domain of your subnet and compute instance must match) to allow the selection of your existing subnet, if not already selected.

8. In the Public IP address field, select **Assign a public IPv4 address**.

9. In the Add SSH keys field, select Paste public keys. Then, copy the `sshkeys.pub` public key from the Notepad (copied earlier in previous task) and paste it in the SSH keys field.

10. Keep the other options default and click **Create**. The first compute instance is successfully created.

11. Navigate back to the Instances page from the navigation menu. Ensure that the state of the instance you just created is Running.

12. Copy the Public IP corresponding to the IAD-SP-LAB18-1-VM-01 instance and paste it in Notepad.

13. Click the **Developer Tools** icon at the right of the OCI console header and click Cloud Shell to launch your Cloud Shell.

14. Run the following command using the sshkeys - private key and Public IP:

    ```
    $ ssh -i /home/<user_name>/.ssh/sshkeys opc@X.X.X.X
    ```

    - Replace `<user_name>` with your username.
    - Replace `X.X.X.X` with the public IP address copied in step 15.

    Note: The SSH Key is the private key created in the previous task. It is used to authenticate.

15. Enter **Yes** when prompted to connect and ensure you are connected to the instance.

16. Enter **exit** to close the connection.

    You will now deploy a second virtual machine instance that uses the shape – **Ampere VM.Standard.A1.Flex** shape with **1** OCPU and **6 GB** memory.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Niwas Sanwan (ram_niwas@tsedu.com) has a non-transferable license to use this Guide

Copyright © 2023, Oracle and/or its affiliates.

17. To create a second instance, repeat steps 1 through 10. Keep all settings the same except the Name of the instance. Enter the Name of the second instance as **IAD-SP-LAB18-1-VM-02**.

    Note: In the **Public IP address** field, select **Do not assign a public IPv4 address**. In the **Add SSH keys** field, select **No SSH keys**.

    Note: The instance is not required to be accessed; therefore, assigning a Public IP address and SSH keys for this instance can be skipped.

18. Keep the other options default and click **Create**. The second compute instance is successfully created.

19. Navigate back to the Instances page from the **Main** menu. Ensure that the State of the second instance created is **Running**.

    You will now deploy a third virtual machine instance that uses the shape - **Ampere VM.Standard.A1.Flex** shape with **1** OCPU and **6 GB** memory.

    To create a third instance, repeat steps 1 through 10. Keep all settings the same except the Name of the instance. Enter the Name of the third instance as **IAD-SP-LAB18-1-VM-03**.

    Note: In the **Public IP address** field, select **Do not assign a public IPv4 address**. In the **Add SSH keys** field, select **No SSH keys**.

    Note: The instance is not required to be accessed; therefore, assigning a Public IP address and SSH keys for this instance can be skipped.

20. Click **Create**. The third compute instance is successfully created.

21. Navigate back to the **Instances** page from the **Main Menu**. Ensure that the State of the third instance created is **Running**.

Ram Nivas Sengwan (ram.nivas@tcs.edu.com) has a non-transferable license to use this Guide.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Copyright © 2023, Oracle and/or its affiliates.

Create Alarms and View Service Metrics

You will view the service metrics for your instances, confirm that the required monitoring plug-in is enabled, and set up alarm notifications.

Task 1: Confirm that the Compute Instance Monitoring Plug-In Is Enabled

To view the service metrics available in the OCI Console, the compute instance monitoring plug-in must be enabled. This plug-in emits metrics about the instance's health, capacity, and performance—such as CPU and memory utilization.

Note: The plug-in will be enabled by default, but it should be confirmed.

1. From the navigation menu, select **Compute**, and then click **Instances**.
2. Click the instance **IAD-SP-LAB18-1-VM-01**.
3. Click **Oracle Cloud Agent** tab.
4. Scroll down to find the **Compute Instance Monitoring** plug-in and ensure that it is running and enabled.

Task 2: Create a Topic and a Subscription Inside a Topic

Now that you have confirmed that Monitoring is enabled, you will create an alarm that is triggered when the service metrics reach a designated threshold. You will see that this alarm gets triggered later in the practice when you perform a CPU stress test.

To create an alarm, you must first create a notification so that the alarm has a way to notify the relevant parties. For example, an alarm can email an administrator when a CPU usage threshold has been breached.

1. From the navigation menu, select **Developer Services**. Navigate to **Application Integration** and select **Notifications**.
2. From the left-navigation panel, ensure that you are in *<your assigned compartment>*.
3. Click **Create Topic**.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Copyright © 2023, Oracle and/or its affiliates.

4. In the Create Topic dialog box, provide the following details:
    - **Name**: `IAD-SP-LAB18-1-TOP-01`
    - **Description**: Optional
5. Click **Create**.
6. After the topic state changes to **Active**, click the topic to view the details.
7. Under Resources, click **Create Subscription**.
8. Select **Email** in the Protocol field.
9. In the Email field, enter your email address.
10. Click **Create**.
11. Click the subscription that you just created.

    The Subscription Information will be displayed with the status as Pending Confirmation.
12. Check the email account you specified and click the "Confirm subscription" verification link in it. A pop-up browser window will tell you that the subscription has been confirmed.
13. Navigate back to the **Subscriptions** page and verify that the subscription status has changed to **Active**.

    Note: You may need to refresh your browser if the status is not updated.

A topic and a subscription inside a topic are successfully created.

Task 3: Create an Alarm for CPU Utilization

Now that you've created the topic and subscription for a notification, you will create an alarm. This alarm will be activated when the CPU utilization reaches a threshold that you designate.

1. From the OCI Console **Main Menu**, select **Observability & Management**. Under **Monitoring**, click **Alarm Definitions**.
2. From the left-navigation panel, ensure you are in the compartment assigned to you.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Nivas Sangwan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

3. Click **Create Alarm**.

4. In the Create Alarm dialog box, populate the following information in the **Delete alarm** section:

   - **Alarm name**: `IAD-SP-LAB18-1-ALA-01`
   - **Alarm severity**: Critical
   - **Alarm body**: High Usage of CPU

5. The **Tags** section is optional. Therefore, keep the default selections.

6. Populate the following information in the **Metric description** section:

   - **Compartment**: <*your assigned compartment*>
   - **Metric namespace**: oci_computeagent
   - **Metric name**: CpuUtilization
   - **Interval**: 1m
   - **Statistic**: Max

   Note: The Resource Group field is optional. Therefore, you can skip it for now.

7. Populate the following information in the **Metric dimensions** section:

   - **Dimension name**: resourceDisplayName
   - **Dimension value**: IAD-SP-LAB18-1-VM-01

8. Populate the following information in the **Trigger rule** section:

   - **operator**: greater than
   - **Value**: 70
   - **Trigger delay minutes**: 1

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Niwas Sungwan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

9. Populate the following information in the **Define alarm notifications** section:

    - **Destination service**: Notifications
    - **Compartment**: <*your compartment*>
    - **Topic**: IAD-SP-LAB18-1-TOP-01

    You have created the topic earlier and recall that the topic is the communication channel, such as email. When the alarm is triggered, a notification is sent to the subscribed email addresses.

10. Select the **Split notifications per metric stream** option in the **Message grouping** section.

    With this setting, you are configuring the Alarm to send a message for the specific instance when it reaches the CPU threshold. The UI shows a message which is just a reference- **Consider limits when the alarm contains a high number of metric streams**.

11. You can select the message format, which is generally the first option **Send formatted messages**.

12. You can also choose to have a notification repeated at certain frequencies if an alarm continues. Keep the **Repeat notification** option deselected.

13. You have the option to suppress the notification. Keep the **Suppress notifications** option deselected.

14. Select **Enable this alarm** and click **Save alarm**.

    You should now be able to see the alarm's details.

Ram Niwas Sangwan (ram.niwas@tcs.com) has a non-transferable license to use this Guide.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Copyright © 2023, Oracle and/or its affiliates.

Create CPU Stress and Fire Alarm

You will create a CPU stress on the first instance (IAD-SP-LAB18-1-VM-01), monitor the effect of the CPU stress on the instance, and see an event triggered when the CPU Utilization is greater than the threshold, which causes the alarm to fire.

Task 1: Create CPU Stress for an Instance

Now that you have created an alarm, Observability and Management monitors the working of instances and sends a notification when the alarm is triggered. For this purpose, the CPU is subjected to stress and forced to run to its maximum capacity. When the CPU Utilization metric is greater than the threshold value, the alarm gets triggered.

This is simulated by means of a CPUStress generator. The following steps are with respect to Linux OS.

1. From the navigation menu, select **Compute**, then click **Instances.**
2. Click the instance **IAD-SP-LAB18-1-VM-01.** Copy the Public IP address.
3. Select the Developer Tools icon at the right of the OCI console header and click **Cloud Shell** to launch your Cloud Shell.
4. Connect to the instance by running the following command:

   ```
   $ ssh -i /home/<user_name>/.ssh/sshkeys opc@<X.X.X.X>
   ```

   - Replace `<user_name>` with your username.
   - Replace *X.X.X.X* with the public IP address.
5. If prompted to continue connecting, enter **yes**.
6. You might get a message that the FIPS mode is initialized. Enter **Yes** to confirm.
7. Run the following command to install the Extra Packages for Enterprise Linux (EPEL) repository on Linux distributions to install additional standard open-source software packages by using YUM and DNF package manager. If you are asked if it is OK, enter **Y**.

   ```
   $ sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
   ```
8. Enter **Y**. You will see **Complete!** when it is complete.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Nivas Sangwan (ram.nivas@tcs.edu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

9. Install the stress package. Stress is a generator tool, devised to subject your system to configurable measure of CPU, memory, I/O, disk stress. To install, run the following command:

```
$ sudo yum install stress-ng
```

Note: If you are asked if it is OK, enter **Y** again.

You will get a message when the installation is successful.

Task 2: Induce Stress to the Compute Instance

Now, you need to induce stress to the instance. The stress on the compute instances increases on repeated use of the stress command. Run the following command:

```
$ uptime
$ stress-ng --cpu 8 --timeout 300
```

Task 3: Trigger the Alarm

1. From the navigation menu, select **Observability & Management**. Navigate to **Monitoring**, then click **Alarm Definitions**.
2. Click **IAD-SP-LAB18-1-ALA-01**, the alarm that you created earlier.
3. The icon in IAD-SP-LAB18-1-ALA-01 would have changed to Firing mode due to the stress induced. This happens when the load on the CPU Utilization crosses the threshold limits. Please wait for a minute if the status is not changed to Firing, and then refresh the page.
4. Scroll down to the **Alarm history** graph, which signifies that the CPU stress has surpassed the set threshold.
5. An email notification is sent to the configured subscription email of the Notifications Topic as Alarm status changes from OK to Firing.
6. The email provides details about Alarm OCID, Number of Metrics breaching threshold, and Dimensions.
7. Navigate back to the **Alarm Definitions** page and select the check box against the IAD-SP-LAB18-1-ALA-01 alarm.
8. Click **Actions** and select **Add suppressions** from the drop-down menu.
9. In the Suppress Alarms Wizard, select the default **Start time** and **End time** and click **Apply suppressions** to confirm.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Niwas Sangwan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

10. Click **Close** and verify that the column Suppressed shows the alarm is suppressed for the period.

11. Click the Developer Tools icon at the right of the OCI console header and click **Cloud Shell** to open Cloud Shell where the stress was initiated on the Instance. Press Ctrl + C to stop the stress.

12. Navigate back to the **Alarm Definitions** page and click IAD-SP-LAB18-1-ALA-01 alarm.

13. The CPU-usage-alarm icon would have changed to OK mode as the stress is now stopped.

14. Verify an email notification is not received by the configured subscription email for the status being changed from Firing to OK. This notification is not sent due to Alarm being suppressed for the period.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Niwas Sangwan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Create Queries

You will create different types of queries and see how they are all represented graphically.

Task 1: Create Standard Queries

In this task, you will learn about query expressions and components, and you will execute sample queries that can be used with the Monitoring service. The Metrics Explorer creates queries that are used to search and aggregate metric data points collected from resources.

A standard query includes a metric namespace (the source or application being measured), metric (what is being measured), interval (over what period), and statistic (how it's being measured, for example, a sum, rate, or max value).

1. From the navigation menu, select **Observability & Management**. Navigate to **Monitoring** and click **Metrics Explorer**.

2. To create a standard query, populate the following information in the **Query** section:

   - **Compartment**: *<your assigned compartment>*
   - **Metric namespace**: oci_computeagent
   - **Metric name**: CpuUtilization
   - **Interval**: 5m
   - **Statistic**: Max

3. Click Update Chart.

   The chart generated is the output of the query. It represents the CPU utilization (CpuUtilization) of all instances (oci_computeagent) in the past five minutes. The corresponding Monitoring Query Language (MQL) is displayed under Query 1.

Ram Nivas Sangwan (ram.niwas@seedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Task 2: Create Standard Queries with a Filter

A filter condition is used along with a standard query to display graphs that satisfy specific conditions. The filter condition is entered in the Metric Dimensions area and includes a name and (optional) a value.

1. From the navigation menu, select **Observability & Management**. Navigate to **Monitoring** and click **Metrics Explorer**.
2. Populate the following information to create a grouping function using Basic mode in the **Query** section:
   - **Compartment**: <*your assigned compartment*>
   - **Metric namespace**: oci_computeagent
   - **Metric name**: CpuUtilization
   - **Interval**: 5m
   - **Statistic**: Max
3. In the **Metric dimensions** section, populate the following information:
   - **Dimension name**: availabilityDomain
   - **Dimension value**: *Select an availability domain.*
4. Click **Update Chart**.

   The chart displays the CPU utilization of the compute instances in an interval of one minute for the inputted availability domain.

Ram Niwas Sangwan (ramniwas@tseedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Task 3: Create Aggregation Using Basic Queries

Simple aggregation (grouping) function queries return the combined value of all metric streams for the selected statistic. They can be written manually in the Query Code Editor pane by checking the Advanced mode option, or you can use the Standard Query mode used above.

1. From the navigation menu, select **Observability & Management**. Navigate to **Monitoring** and click **Metrics Explorer**.

2. Populate the following information to create a grouping function using Basic mode in the **Query** section:

   - **Compartment**: <*your assigned compartment*>
   - **Metric namespace**: oci_computeagent
   - **Metric name**: CpuUtilization
   - **Interval**: 5m
   - **Statistic**: Max

3. In the **Metric dimensions** section, populate the following information:

   - **Dimension name**: availabilityDomain
   - Select the **Aggregate metric streams** check box.

   Note: You can leave the **Dimension value** field blank for now.

4. Click **Update Chart**.

   The graph displays the aggregation of CPU utilization of all availability domains, with an interval of five minutes, and a statistic option of the Max function.

   The selection of **Aggregate metric streams** check box is referred to as the **grouping** function while using Advanced mode. This query can be viewed by selecting the **Advanced mode** check box.

Ramniwas Sangwan (ramniwas@tseedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

Task 4: Create Advanced Queries

The nested queries are written as part of the Advanced mode in the **Query code editor**.

1. From the navigation menu, select **Observability & Management**. Navigate to **Monitoring** and click **Metrics Explorer**.

2. Select the **Advanced mode** check box at the top right of the **Query 1** section.

3. Populate the following information to create a grouping function using Basic mode in the **Query** section:

   - **Compartment**: <*your assigned compartment*>

   - **Metric namespace**: oci_computeagent

4. Enter the following code in the **Query code editor** field.

   ```
   (CpuUtilization[1m].max() > 5).grouping().max()
   ```

5. Click **Update Chart**.

   The displayed output groups the compute instances and displays the ones whose CpuUtilization is more than 5 percent in the past minute.

   GroupBy is a grouping function which can be written using the Advanced mode. It is another way to aggregate metric streams. For example, you can group by **shape** used by the Instance.

6. To group by shape, enter the following code into the **Query code editor**.

   ```
   CpuUtilization[5m].groupBy(shape).max()
   ```

7. Click **Update Chart**.

   The displayed output groups compute instances by shape and displays CpuUtilization with an interval of 5 mins and showing the maximum reported value in the graph.

Ram Niwas Cangwal (ram.niwas@seedu.com) has a non-transferable license to use this Guide.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Copyright © 2023, Oracle and/or its affiliates.

Purge Instructions

Perform the purge operation, as instructed below:

Delete Resources

1. In the console ribbon at the top of the screen, click the Region icon to expand the menu and select **US East (Ashburn)**.
2. From the navigation menu, select **Observability & Management**. Navigate to **Monitoring** and click **Alarm Definitions.**
3. From the left navigation panel, ensure you are in the compartment assigned to you.
4. Select the check box that corresponds to the alarm **IAD-SP-LAB18-1-ALA-01**.
5. From the **Actions** drop-down menu, select **Delete alarms**.
6. Confirm to Delete, and click **Close.**

Delete Topics and Subscriptions

1. From the navigation menu, select **Developer Services**. Navigate to **Application Integration** and click **Notifications**.
2. Click the topic **IAD-SP-LAB18-1-TOP-01**.
3. Click the three dots on the right corresponding to the subscription to open the Actions menu and select **Delete**.
4. Click **Delete Subscription** to confirm.
5. Navigate back to the **Notifications** page.
6. Click the three dots on the right corresponding to the topic to open the Actions menu and select **Delete**.
7. Click **Delete Topic** to confirm.

Ram Niwas Sangwan (ram.niwas@tsedu.com) has non-transferable license to use this Guide.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Delete Compute Instances

1. From the navigation menu, select **Compute**, and then click **Instances**.
2. From the left navigation panel, ensure you are in *<your assigned compartment>.*
3. Click the three dots on the right corresponding to the instance **IAD-SP-LAB18-1-VM-01** to open the Actions menu and click **Terminate**.
4. Select the **Permanently delete the attached boot volume** check box.
5. Click **Terminate Instance**.
6. Wait until the **State** shows **Terminated** for the instance.

Delete VCN and Resources

1. From the navigation menu, select **Networking**, and then click **Virtual Cloud Networks**.
2. From the left navigation panel, ensure you are in *<your assigned compartment>.*
3. Click **IAD-SP-LAB18-1-VCN-01**.
4. From the left navigation panel, under Resources, click Route Tables.
5. Click **Default Route Table for IAD-SP-LAB18-1-VCN-01.**
6. Select Internet Gateway route rule and click **Remove.**
7. Return to the VCN details page by clicking **IAD-SP-LAB18-1-VCN-01** in the breadcrumb list at the top of the page.
8. Click **Delete.**
9. Ensure that the **Search compartments for resources associated with this VCN** check box is selected.
10. Select **Specific Compartment** and ensure that <*your compartment*> is selected.

Ram Niwas Sangwan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

11. Click **Scan** and wait until scan is completed.

    The following message will be shown, which is a warning to delete the VCN.

    The resources and VCN will be deleted in sequence. The process will stop if an error occurs, or you don't have permission to delete a resource.

    Resources deleted up to that point cannot be restored.

12. Verify that there are no errors reported and click **Delete All**.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Niwas Sangwan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Cloud Security Posture Management: Cloud Guard Notification

Lab 20 Practices

Estimated time: 30 mins

Ram Niwas Sangwan (ram.niwas@oracle.com) has a non-transferable license to use this Guide.

Get Started

Overview

Cloud Guard Notification is a feature in Oracle Cloud Infrastructure (OCI) that sends real-time alerts for security problems detected by Cloud Guard. These alerts can be customized and delivered to various notification channels such as email, SMS, or PagerDuty. Cloud Guard Notification helps organizations to proactively detect and respond to security threats in their OCI environments.

In this lab, you will:

- Create and configure a Cloud Guard target
- Ensure Cloud Event rule is enabled
- Configure Notification service
- Configure Events service
- Create a scenario for Cloud Guard Notification
- Verify Cloud Guard Notification

Prerequisites

- You must have access to the OCI Console.
- The Oracle University lab team has set up all the IAM policies required for you to complete this lab.

Assumptions

- Select the region that is available in the tenancy allotted to you. In this lab, we are considering US East (Ashburn) (IAD) as your region.
- You must be familiar with navigating the OCI Console.

Ram Nivas Gangwan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Copyright © 2023, Oracle and/or its affiliates.

Create and Configure a Cloud Guard Target

You will learn how to add a target to set the scope of resources that Cloud Guard monitors. You will also learn how to check if the Cloud Event rule in the responder recipe is enabled for your specified target.

Note: It is important to note that Cloud Guard is already enabled in your practice tenancy.

Task 1: Create a Cloud Guard for your assigned compartment

1. From the navigation menu, select **Identity & Security** and then click **Cloud Guard**.
2. In the left navigation pane, under **Cloud Guard**, click **Targets.**
3. In the left navigation pane, under **Scope**, select *<your assigned compartment>* from the drop-down menu.

Note: If you already have a specific target set for your compartment, delete it.

1. Click **Create new target**.
2. Enter the following:
    a. **Target Name:** `IAD-SP-LAB20-1-CG-01`
    b. **Description:** Enter a meaningful description.
    c. **Compartment:** *<your assigned compartment>*
    d. **Configuration detector recipe:** OCI Configuration Detector Recipe (Oracle managed)
    e. **Threat detector recipe:** OCI Threat Detector Recipe (Oracle managed)
    f. **Activity Detector Recipe:** Oracle Activity Detector Recipe (Oracle managed)
    g. **Responder recipe:** OCI Responder Recipe (Oracle managed)
3. Click **Create** to create the target.

    The details page for the new target will be displayed.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Niwas Saharwan (ram.niwas@ltceedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Task 2: Ensure Cloud Event rule is enabled

You can utilize Cloud Guard's notification responder called Cloud Event, which emits problem details to the Events service. To make use of the Cloud Event responder rule, you must attach the OCI Responder Recipe (Oracle managed) to your target. It is important to note that the Cloud Event rule is already enabled by default. However, if you clone the recipe to customize it, you must ensure that you enable the Cloud Event rule.

1. From the navigation menu, select **Identity & Security** and then click **Cloud Guard**.
4. In the left navigation pane, under **Cloud Guard**, click **Targets.**
5. In the left navigation pane, under **Scope**, select *<your assigned compartment>* from the drop-down menu.
6. Click the **IAD-SP-LAB20-1-CG-01** target.
7. Under **Resources** in the left navigation panel, click **Responder recipe**.
8. Click **OCI Responder Recipe (Oracle managed).**
9. Locate the **Cloud Event** rule, under Responder rules.
10. Confirm that the status column for the Cloud Event rule is **Enabled**.
11. Next, ensure that the Cloud Event responder rule is set to execute automatically.
12. In the Cloud Event responder rule row, open the Actions menu and select **Edit**.
13. In the **Configure Responder Rule** dialog box, **Setting** section, check the **Rule Trigger** setting.
    - Ensure the **Execute Automatically** check box is selected.
    - Select the CONFIRM EXECUTE AUTOMATICALLY check box.
14. Click **Save**.

You have created a Cloud Guard target and confirmed that the Cloud Event responder rule is enabled.

Ram Nivas Gangwar (ram.niwas@tceedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

Configure Notification Service

Once you have confirmed that the Cloud Event responder rule is enabled, you will learn how to create a notification so that the relevant parties can be informed when Cloud Guard detects a problem in the monitoring target. For instance, you may want to set up an email to be sent to an administrator in response to an event.

Task: Create a topic and a subscription inside a topic

1. From the navigation menu, select **Developer Services**. Navigate to **Application Integration** and select **Notifications**.
2. From the left navigation panel, ensure that you are in *<your assigned compartment>.*
3. Click **Create Topic**.
4. In the Create Topic dialog box, provide the following details:
   - **Name:** IAD-SP-LAB20-1-TOP-01
   - **Description:** Optional
5. Click **Create**.
6. After the topic state changes to **Active**, click the topic to view the details.
7. Under Resources, click **Create Subscription**.
8. Select **Email** in the Protocol field.
9. In the Email field, enter your email address.
10. Click **Create**.
11. Click the subscription that you just created.

    The subscription information will be displayed with the status as Pending Confirmation.
12. Check the email account you specified and click the “Confirm subscription” verification link in it. A pop-up browser window will tell you that the subscription has been confirmed.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Copyright © 2023, Oracle and/or its affiliates.

13. Navigate back to the **Subscriptions** page and verify that the subscription status has changed to **Active**.

    Note: You may need to refresh your browser if the status is not updated.

A topic and a subscription inside a topic have been successfully created.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Niwas Sangwan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

Configure Events Service

You will learn how to configure a rule in the Event service that specifies the conditions under which a Cloud Guard event notification should be sent.

Task: Configure a rule for Cloud Guard event type

1. From the navigation menu, select **Observability & Management** and then click **Events Service**.
2. From the left navigation panel, ensure that you are in *<your assigned compartment>.*
3. Under Resources, select **Rules** and then click **Create Rule.**
4. In the **Create Rule** dialog box, enter the following:
   - **Name**: IAD-SP-LAB20-1-RULE-01
   - **Description:** Enter a meaningful description.
   - Under the **Rule Condition** section:
     - **Condition**: Select **Event Type**
     - **Service Name:** Select **Cloud Guard**
     - **Event Type**: Set **Detected—Problem, Remediated—Problem,** and **Cloud Guard—Announcements**
   - Under the **Action** section:
     - **Action Type**: Select **Notification**
     - **Notification Compartment**: Select *<your assigned compartment>*
     - **Topic**: Select **`IAD-SP-LAB20-1-TOP-01`**
5. Click **Create Rule.**

   Your Cloud Guard event rule has been successfully created.
6. Under **Resources** in the left navigation panel, click **Event Matching**.

   Verify that the appropriate event types are set for this rule.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Niwas Sangwan (ramniwas@tseedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

7. Under **Resources** in the left navigation panel, click **Action**.

   Check that the action type is set to notification, the state is Enabled, and the topic is configured to IAD-SP-LAB20-1-TOP-01.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Niwas Sangwan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

Create a Scenario for Cloud Guard Notification

To receive notifications for any problems detected in your set target, you need to create a bucket and make it publicly visible. Additionally, you can also verify the activity of the Cloud Event responder rule.

Task 1: Configure Network Source to allow bucket creation

You need to update your Public IP address in Network Source before creating a bucket.

Note: if your Public IP address is already listed as a network source, you can skip Task 1 and move directly to Task 2.

1. To obtain your Public IP address, open a web browser and perform a Google search for "what is my public IP?"

   Note down the Public IP address.

2. From the navigation menu, click **Identity & Security** and then click **Network Sources.**

3. Locate and click the `IAD-SP-LAB05-1-NS-01` network source in the list to view its details.

   In your environment, an `IAD-SP-LAB05-1-NS-01` network source has been pre-created.

4. Click **Add Networks**.

5. In the **Add Networks** dialog box, enter the following:
   - **Network type**: Public Network
   - **IP Address/CIDR Block**: `<YOUR_PUBLIC_IP_ADDRESS>`

6. Click **Update**.

   Your Public IP address or CIDR block has successfully been added as a network to the IAD-SP-LAB05-1-NS-01 network source.

Task 2: Create a bucket with public visibility

1. From the navigation menu, click **Storage**. Navigate to Object Storage and then click **Buckets**.

2. In the left navigation pane, under List Scope, select *<your assigned compartment>* from the drop-down menu.

Copyright © 2023, Oracle and/or its affiliates.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Niwas Sangwan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide.

3. Click **Create Bucket**.

4. In the **Create Bucket** dialog box, specify the attributes of the bucket:
   - **Bucket Name:** IAD-SP-LAB20-1-BKT-01-<user-id>
     Please specify your user id in place of `<user-id>` to make it unique.
   - **Default Storage Tier:** Select `Standard`.
     Note: Leave all the other options in their default setting.

5. Click **Create**.

   You can see the bucket listed for your compartment.

6. Click the three dots on the right to open the Actions menu and select **Edit Visibility**. Select **Public** and click **Save Changes**.

   Note: You have successfully created a bucket with public visibility in the assigned compartment. However, to ensure proper cloud security posture, the detector recipe has a configuration rule that requires buckets to be private.

   So, you need to wait for Cloud Guard to evaluate your allocated detector configuration and check for any problems in the set target.

   It is suggested that you wait for 25–30 minutes before reviewing the Cloud Guard Dashboard to check if any problems have been identified and to receive notifications triggered by the Event service.

Ram Niwas Sangwan (ram.niwas@tsiedu.com) has a non-transferable license to use this Guide.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Copyright © 2023, Oracle and/or its affiliates.

Verify Cloud Guard Notification

After a problem is detected in your set target, you will receive an email notification that contains detailed information about the detected problem. You can also verify the activity of the Cloud Event responder rule.

Task 1: Reading the email notification

1. You will receive an email notification to the configured subscription email of the Notifications Topic with the subject:

   "OCI Event Notification :com.oraclecloud.cloudguard.problemdetected".

2. The email contains important information such as the resource OCID, problem name, risk level, target ID, and more.

   Here is a sample of what the email might look like:


```
{
  "eventType" : "com.oraclecloud.cloudguard.problemdetected",
  "cloudEventsVersion" : "0.1",
  "eventTypeVersion" : "2.0",
  "source" : "CloudGuardResponderEngine",
  "eventTime" : "2022-12-24T02:38:00Z",
  "contentType" : "application/json",
  "data" : {
    "compartmentId" : "ocid1.compartment.oc1..aaaaaxxxxxxxxxx",
    "compartmentName" : "demo",
    "resourceName" : "Bucket is public",
    "resourceId" : "ocid1.cloudguardproblem.oc1.iad.amaaaaaajcisnjkxxxxxxxxx",
    "additionalDetails" : {
      "tenantId" : "ocid1.tenancy.oc1..aaaaaaaxxxxxxxxx",
      "status" : "OPEN",
      "reason" : "New Problem detected by CloudGuard",
      "problemName" : "BUCKET_IS_PUBLIC",
      "riskLevel" : "CRITICAL",
      "problemType" : "CONFIG_CHANGE",
      "resourceName" : "bucket-20xxx5-1410",
      "resourceId" : "ocuocxxxxx/bucket-20xxxx5-1410",
      "resourceType" : "Bucket",
      "targetId" : "ocid1.cloudguardtarget.oc1.iad.amaaaaallkxxxxxxxxxx",
      "labels" : "CIS_OCI_V1.1_OBJECTSTORAGE, ObjectStorage",
      "firstDetected" : "2022-12-24T02:37:41.435Z",
      "lastDetected" : "2021-12-24T08:37:41.435Z",
      "region" : "us-ashburn-1",
```


Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Copyright © 2023, Oracle and/or its affiliates.

Task 2: Check activities for the Cloud Event responder rule

1. From the navigation menu, select **Identity & Security** and then click **Cloud Guard**.

14. In the left navigation pane, under **Cloud Guard**, click **Problems.**

15. In the left navigation pane, under **Scope**, select *<your assigned compartment>* from the drop-down menu.

16. In the left navigation pane, under Resource type**,** select **Bucket** from the drop-down menu.

17. Click "**Bucket is Public**" from the problem list.

18. Under **Resources** in the left navigation panel, click **Responder activity**.

19. Check the **Cloud Event** activity row:
    - **Activity**: Completed
    - **Responder execution status**: Succeeded

    This activity confirms that the Cloud Event responder rule is being triggered and events are being created for the problem in the Events service.

Similarly, you will receive a notification whenever a problem is detected or remediated for a set target.

Congratulations! You have successfully completed the task of configuring Cloud Guard notifications. You will now receive email notifications whenever Cloud Guard detects a problem in your set target. You have also verified the activity of the Cloud Event responder rule in the Cloud Guard problem console, ensuring that event service is being triggered for detected problems. These timely notifications will help you maintain the security and integrity of your OCI resources.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Parthiv Jivan Sangwan (ram.nivas@tseedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

Purge Instructions

Perform the purge operation, as instructed below:

Delete Bucket

1. From the navigation menu, select **Storage**. Navigate to Object Storage and then click **Buckets**.
2. In the left navigation pane, under List Scope, select *<your assigned compartment>* from the drop-down menu.
3. Click the bucket: **IAD-SP-LAB20-1-BKT-01-<user-id>**
4. Click **Delete** and then enter the bucket name and click **Delete** in the Confirmation window.

Delete Cloud Guard Target

1. From the navigation menu, select Identity & Security and then click **Cloud Guard**.
2. In the left navigation pane, under List Scope, select *<your assigned compartment>* from the drop-down menu.
3. Select **Targets** from the options listed on the left.
4. Click **IAD-SP-LAB20-1-CG-01**.
5. Click **Delete.**
6. Then select the check box and click **Delete target(s)** in the Confirmation window.

Delete Topics and Subscriptions

1. From the navigation menu, select **Developer Services**. Navigate to **Application Integration** and click **Notifications**.
2. Click the topic **IAD-SP-LAB20-1-TOP-01**.
3. Click the three dots on the right corresponding to the subscription to open the Actions menu and select **Delete**.
4. Click **Delete Subscription** to confirm.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Ram Nivas Sangwan (ram.niwas@tseedu.com) has a non-transferable license to use this Guide.

Copyright © 2023, Oracle and/or its affiliates.

5. Navigate back to the **Notifications** page.

6. Click the three dots on the right corresponding to the topic to open the Actions menu and select **Delete**.

7. Click **Delete Topic** to confirm.

Delete Event Service Rule

1. From the navigation menu, select **Observability & Management** and then click **Events Service**.

2. In the left navigation panel, ensure that you are in *<your assigned compartment>.*

3. Under Resources, select **Rules.**

4. Click the **IAD-SP-LAB20-1-RULE-01** rule.

5. On the rule details page, click **More actions** and click **Delete.**

6. Type **"DELETE"** and click **Delete** to confirm.

Ram Niwas Sangwan (ram.niwas@seedu.com) has a non-transferable license to use this Guide.

Unauthorized reproduction or distribution prohibited. Copyright© 2024, Oracle University and/or its affiliates.

Copyright © 2023, Oracle and/or its affiliates.