Oracle Cloud Infrastructure (OCI) Security Workshop

Laboratory and Exercise Guide

November 22, 2024, Version 0.14.1

Stefan Oehrli, Martin Berger

accenture

Table of Contents

Copyright © 2024 Accenture. All rights reserved.

List of Tables

Copyright © 2024 Accenture. All rights reserved.

1 Workshop Introduction

The *Oracle Cloud Infrastructure Security Workshop* (OCI-SEC-WS) provides an in-depth look at the security features of Oracle Cloud Infrastructure (OCI). This hands-on workshop is tailored for IT professionals who want to improve their understanding of cloud security. After a brief theoretical introduction, participants will dive into hands-on exercises and configure key OCI security services.

You will learn about services such as Cloud Guard, Security Zones and Data Safe to protect your environment. In addition, we will cover important topics such as in-transit encryption, shielded instances and key management.

1.1 Workshop Overview

This workshop offers a comprehensive insight into OCI security. Starting with the setup of your cloud environment, you will gain practical experience in using important security tools. The workshop covers the following areas:

- Using **Cloud Guard** to manage security recipes, performing CIS scans and handling alerts and events.
- Setting up **Data Safe** for auditing, data masking, assessments and alert management.
- Managing **Security Zones**, applying rule sets and ensuring CIS compliance.
- Addressing **Other security topics**, including in-transit encryption, shielded instances and key management.
- Hands-on experience with a **lab environment** for secure access to Oracle Cloud.
- Concludes with additional resources, next steps and a Q&A session.

1.2 Learning Outcomes

At the end of this workshop, participants will:

- Be proficient in using **Cloud Guard** to manage security recipes, CIS scans and alerts.
- Know how to configure **Data Safe** for audits, data masking and security assessments.
- Understand how to manage **Security Zones**, apply rule sets and ensure compliance with security standards.
- You are familiar with **Other security topics**, such as in-transit encryption, shielded instances and key management.
- You have hands-on experience with setting up and working in a secure **lab environment** in Oracle Cloud.
- You have the knowledge and tools to further implement Oracle Cloud security solutions.

Copyright © 2024 Accenture. All rights reserved.

2 Lab Overview

2.1 Oracle Cloud Infrastructure (OCI) Security Workshop Architecture

The following diagram illustrates the architecture set up for the Oracle Cloud Infrastructure (OCI) Security Workshop environment. Each participant will have access to a similar setup to perform a series of hands-on security exercises.

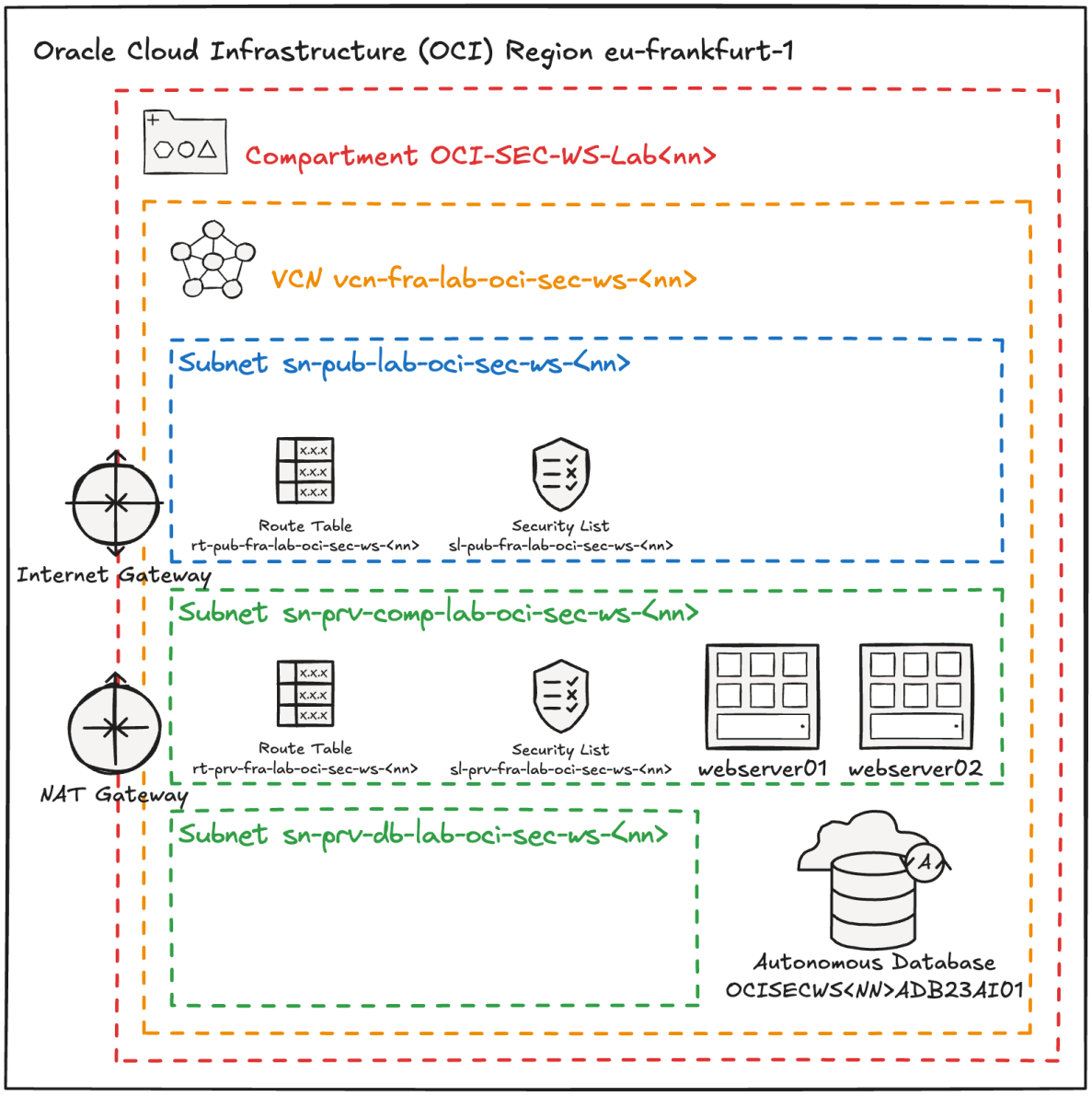


Figure 1: OCI Security Workshop Architecture

2.2 Key Components of the Architecture

- **Region: eu-frankfurt-1** - The environment is hosted in the Frankfurt region.

Copyright © 2024 Accenture. All rights reserved.

- **Compartment (OCI-SEC-WS-Lab):** A dedicated compartment is created for each workshop environment, isolating resources and managing security controls.
- **Virtual Cloud Network (VCN):** The VCN (`vcn-fra-lab-oci-sec-ws-<nn>`) forms the network boundary for the resources within the lab.
  - **Public Subnet:** Contains resources accessible from the internet, secured by a route table and security lists.
  - **Private Subnet for Compute:** A private subnet hosting compute instances (e.g., web servers `webserver01` and `webserver02`), isolated from public access.
  - **Private Subnet for Database:** A subnet dedicated to hosting the Autonomous Database (`OCISECWS<nn>ADB23AI01`).
- **Gateways:**
  - **Internet Gateway:** Allows public internet access for the resources in the public subnet.
  - **NAT Gateway:** Facilitates secure outbound internet traffic for the private resources.

2.3 Lab Exercise Focus Areas:

1. **Key Management:** Create a vault to manage encryption keys and apply them to resources.
2. **Cloud Guard:**
   - **Manual Remediation:** Detect and manually resolve public object storage buckets.
   - **Auto Remediation:** Automatically respond to potential security risks, like public bucket visibility.
   - **Notification Setup:** Configure alerts to be informed of any detected issues.
3. **Data Safe:** Setting up and configuring Oracle Data Safe for enhanced data security.
4. **Security Zones / Web Application Firewall:** Ensuring compliance with Security Zones and protecting web applications.

Copyright © 2024 Accenture. All rights reserved.

3 OCI Setup

3.1 Exercise 00: Getting Started with OCI

In this exercise, you will explore the Oracle Cloud Infrastructure (OCI) environment. This includes logging in, navigating the OCI Console, using the Cloud Shell, and configuring network and database access to the Autonomous Database (ADB).

3.1.1 Objectives

- Log in to the OCI Console and explore its interface.
- Access and use the OCI Cloud Shell for basic tasks.
- Verify connectivity to the Autonomous Database (ADB).
- Configure network and database access for ADB.

Environment

Perform this exercise within the following environment:

- **Compartment:** `OCI-SEC-WS-LAB-nn`
- **Region:** Germany Central (Frankfurt)
- **OCI Console URL:** OCI Console Frankfurt - Login
- **OCI User:** *lab-oci-sec-ws**NN***
- **OCI Password:** *provided by trainer*

Verify that you are in the correct compartment and region. Any new resources, including Cloud Shell configurations and ADB access settings, should be created within the specified compartment.

Solution

3.1.2 Step 1: First Login to OCI Console

1. Log in to the **Oracle Cloud Console** with your assigned credentials.
2. Familiarize yourself with the main console features:
    - **Navigation Menu**: Provides access to services such as Compute, Networking, Storage, and Databases.
    - **Resource Summary**: Displays an overview of resources in your compartment.
    - **Quick Actions**: Offers shortcuts for frequently used tasks like creating instances.
3. Navigate to the **Oracle Database** - **Autonomous Transaction Processing**

Copyright © 2024 Accenture. All rights reserved.

- set the compartment to your compartment **OCI-SEC-WS-LAB-nn**

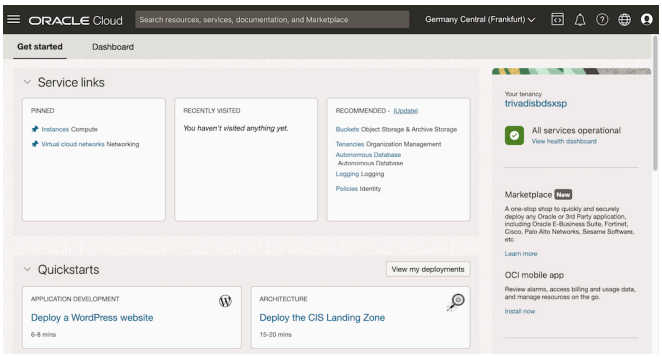


Figure 2: Cloud Console

3.1.3 Step 2: Using the Cloud Shell

1. Open the **Cloud Shell** from the top-right corner of the OCI Console.
2. Explore basic Cloud Shell commands:

```
# Verify the active user
whoami

# List the current files and directories
ls -la
```

```
# Check current Object Storage Namespace
oci os ns get
```

```
# Check environment variables for OCI_CS e.g. User ID, Hosts etc.
env |grep -i oci_cs
```

3. **Create Private Network for Cloud Shell** To be able to connect from OCI Clud Shell to the Autonomous Database, private network connection is required.

   Select *Private network definition list*.

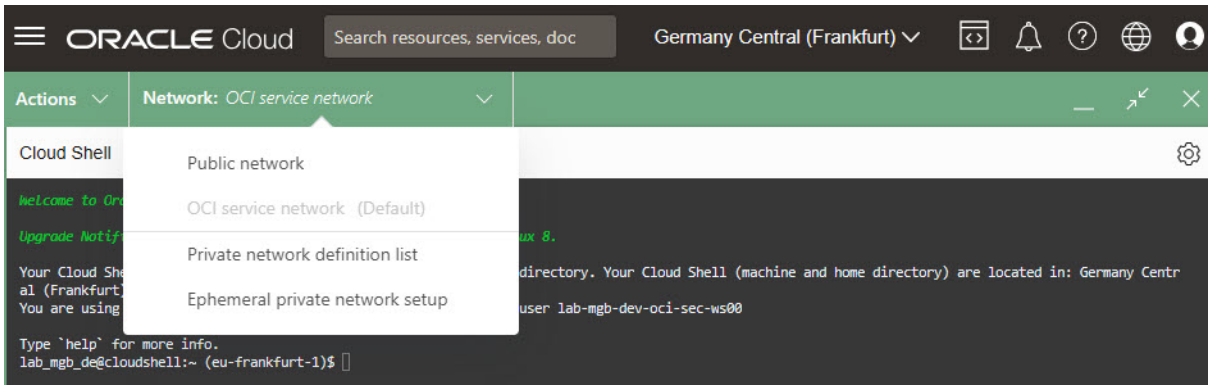


Figure 3: Cloud Shell 01

Copyright © 2024 Accenture. All rights reserved.

Click on *Create private network definition*.

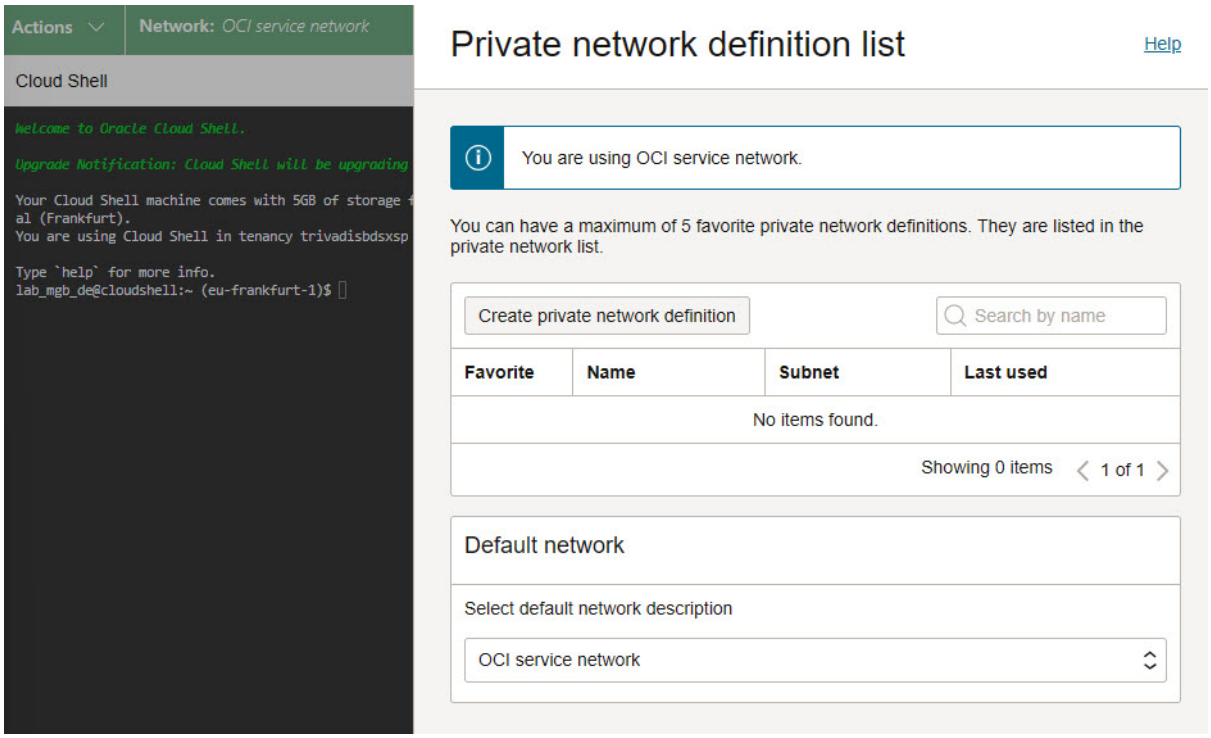


Figure 4: Cloud Shell 02

It is important to create the cloud shell network for the private subnet. Set:

- Name: A simple name to identify the cloud shell network
- VCN in Compartment: Select your lab VCN, if the list is empty, verfy the proper compartment is selected.
- Subnet in Compartment: Select your lab subnet starting with sn-prv-comp-fra, if the list is empty, verfy the proper compartment is selected.
- Use as actve network: Enable checkbox

Copyright © 2024 Accenture. All rights reserved.

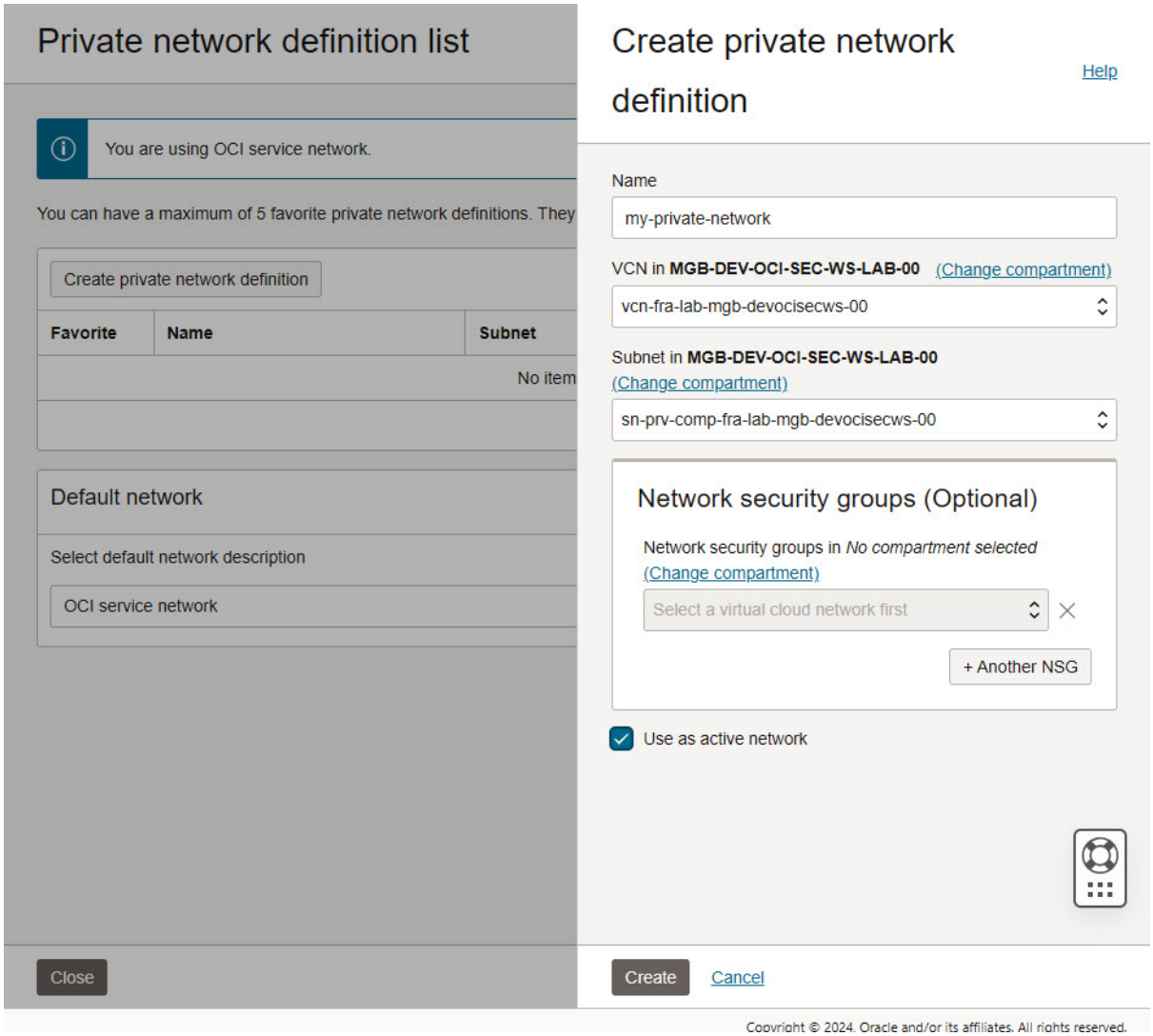


Figure 5: Cloud Shell 03

Create the private network definition. When the network is created, you can close the window.

Copyright © 2024 Accenture. All rights reserved.

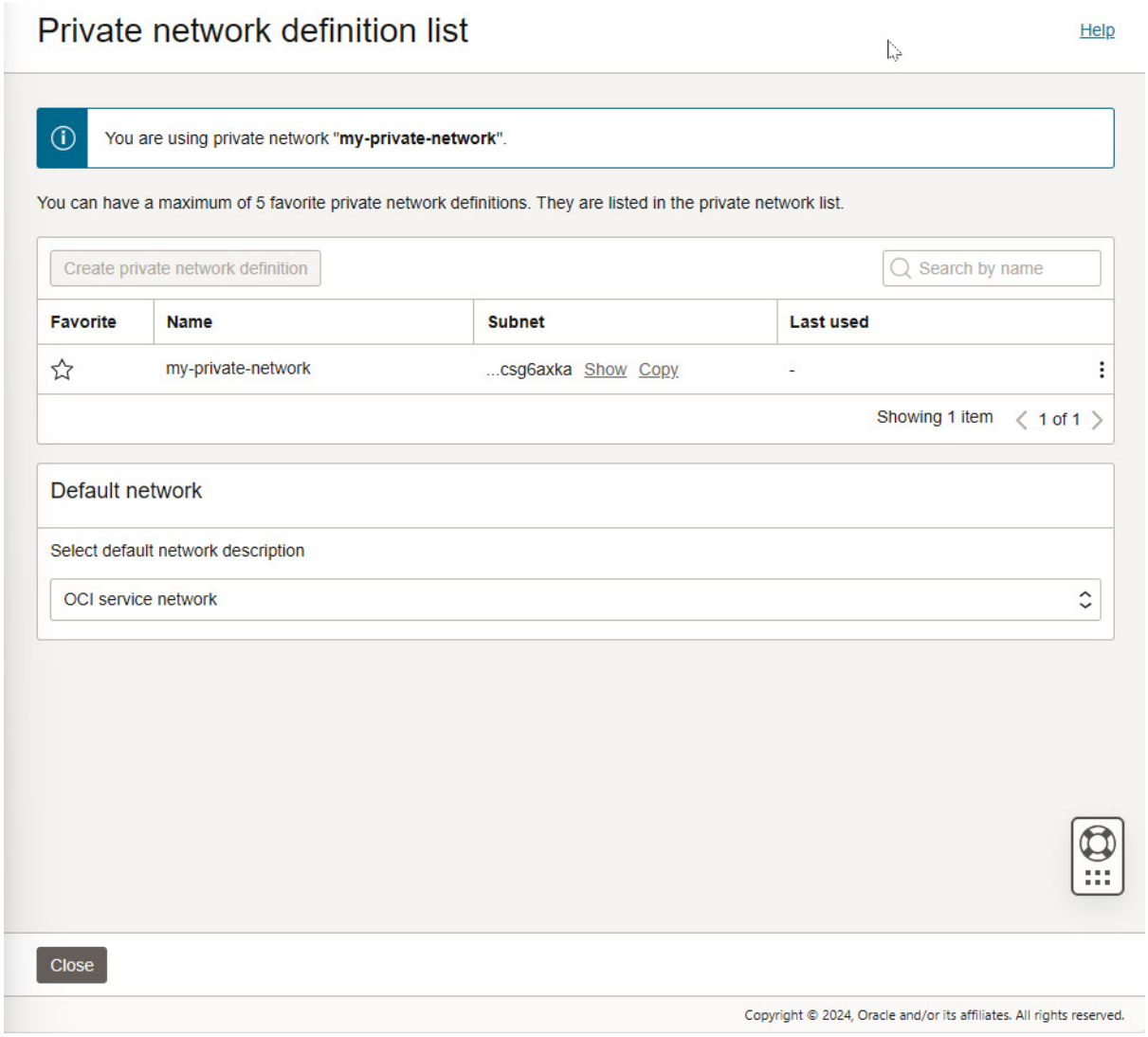


Figure 6: Cloud Shell 04

On top bar of the cloud shell, the new network is active. This requires a couple of seconds, please be patient.

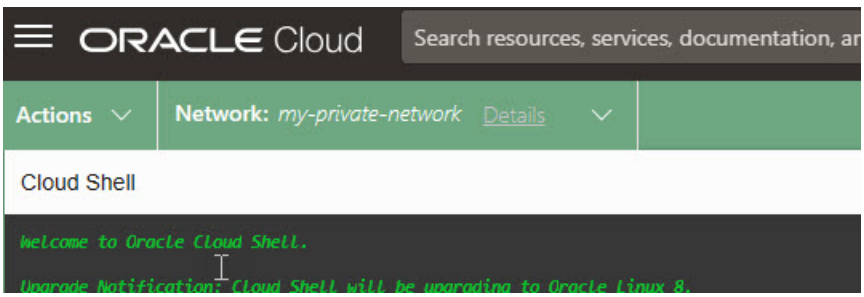


Figure 7: Cloud Shell 05

Copyright © 2024 Accenture. All rights reserved.

3.1.4 Step 3: Configure Autonomous Database ACL

1. Retrieve your **Cloud Shell IP address**:

   ```
   curl ifconfig.me
   ```

   - Example output: `138.2.168.154`.
   - If no value is returned, it indicates that the wrong network is active.

2. Add your Cloud Shell IP address to the **Access Control List (ACL)** of the ADB instance.

Go to Oracle Database -> Autonomous Database.

Select your Autonomous Database by a click on the display name. Verify, correct compartment is selected.

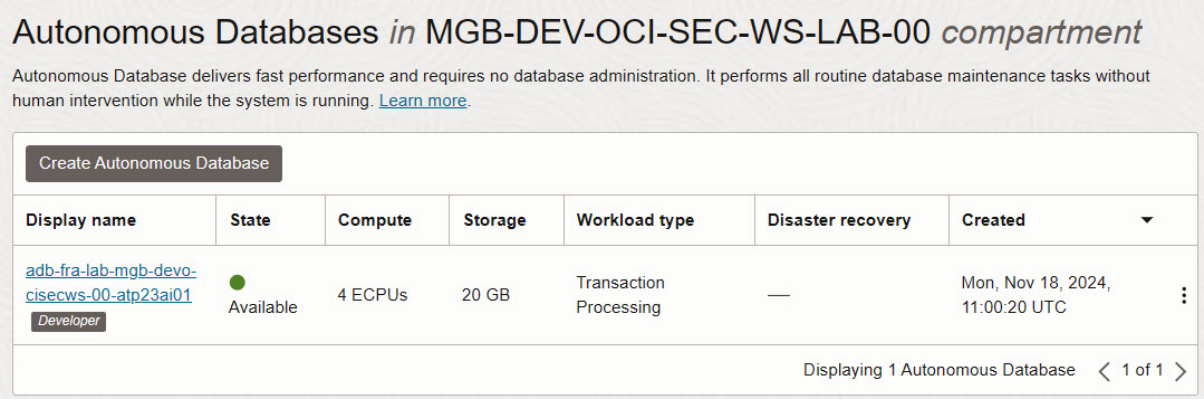


Figure 8: ADB Connect 01

In dashboard, click on the link to edit the Access control list.

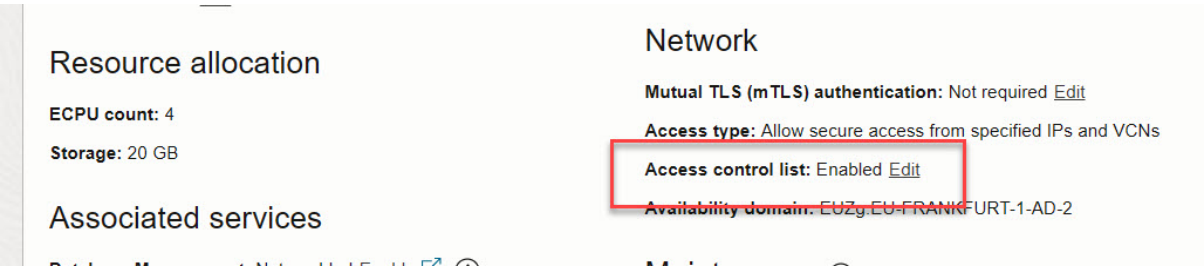


Figure 9: ADB Connect 02

There is always an entry for a VCN, we add another entry by click on *Add access control rule*.

Copyright © 2024 Accenture. All rights reserved.

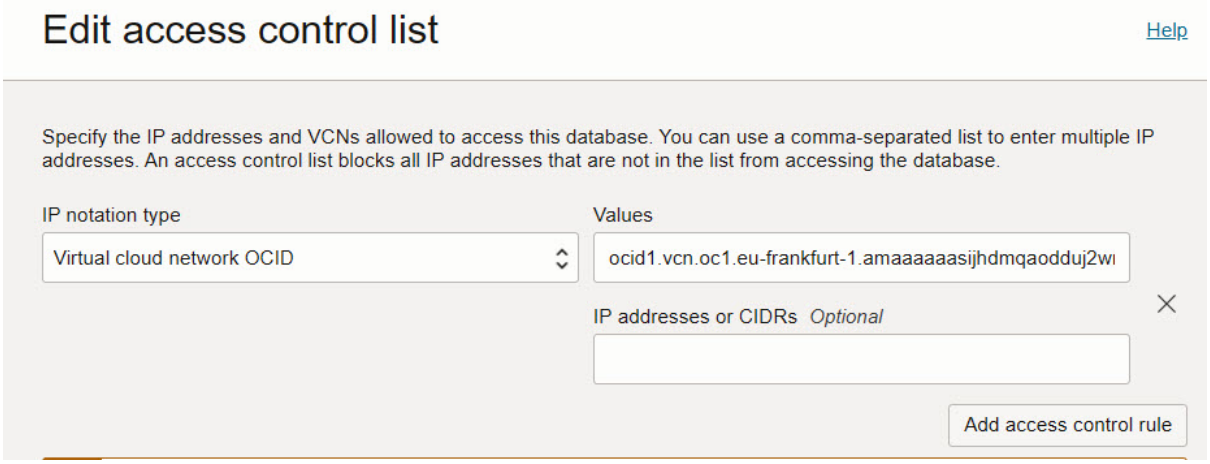


Figure 10: ADB Connect 03

- IP notation type: IP address
- Values: your Cloud Shell IP address from above output, as example 138.2.168.154
- In addition to the IP address of the cloud shell, also add your client IP address. To do this, click the *Add my IP address* button.

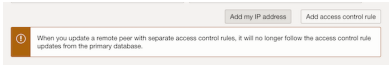


Figure 11: ADB Connect 04

Click on *Save* to store the settings.

Copyright © 2024 Accenture. All rights reserved.

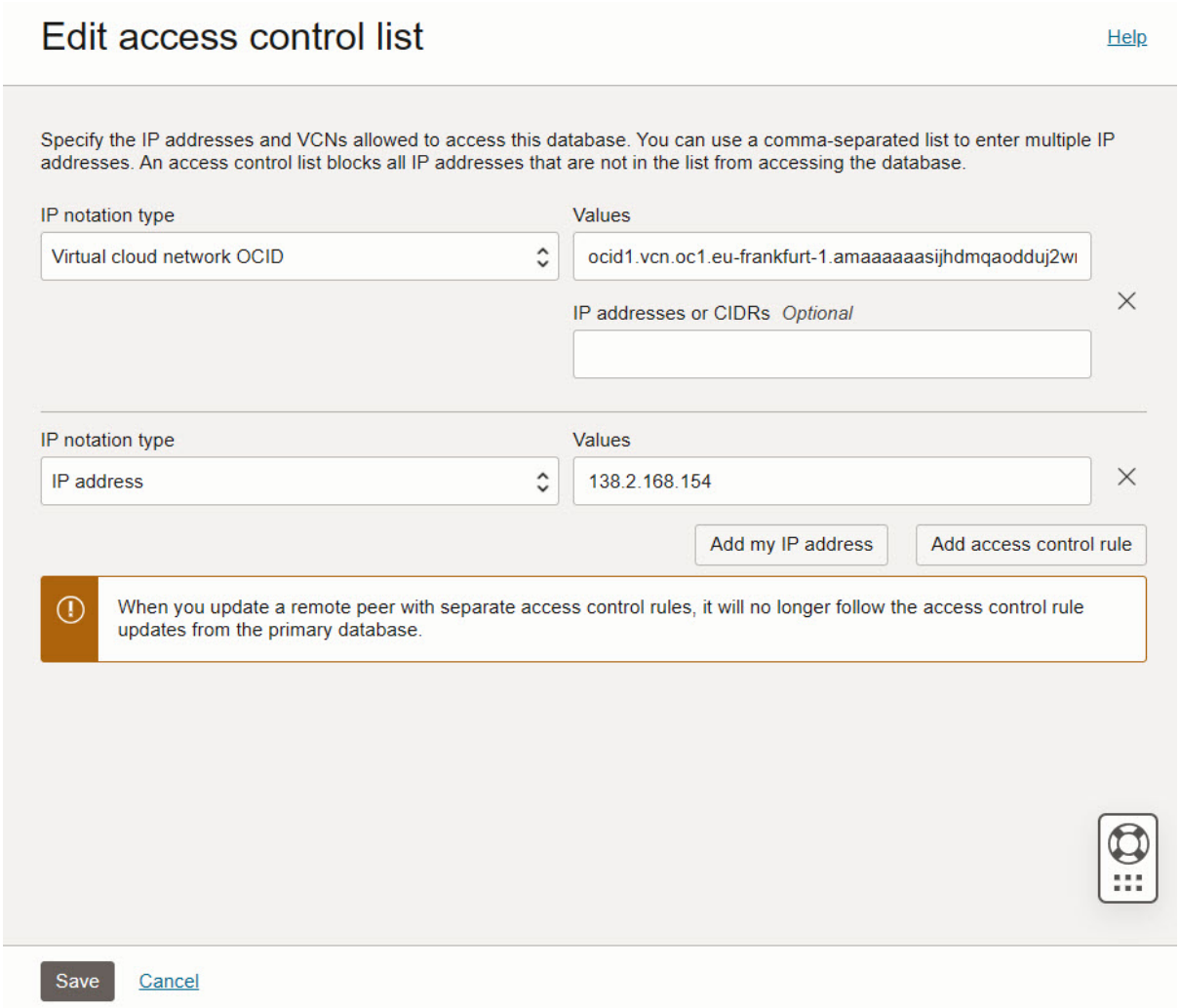


Figure 12: ADB Connect 05

3.1.5 Step 4: Download ADB Wallet and Connect

Go back to your Cloud Shell, ensure the private network is active.

List your Autonomous Database in your compartment. Replace the filter for compartment by your compartment name. Example for compartment

Example for compartment OCI-SEC-WS-LAB-00, an OCID is returned, this OCID is used to get the ADB connection wallet.

```
export MY_COMPARTMENT="OCI-SEC-WS-LAB-00"
export MY_ADBOCID=$(
    oci db autonomous-database list --compartment-id $(
        oci iam compartment list --all --compartment-id-in-subtree true | \
        jq -r --arg COMPARTMENT "$MY_COMPARTMENT" '.data[] | select(.name
            == $COMPARTMENT) | .id'
    ) | jq -r '.data[].id'
)
```

Create a new directory, change into this directory.

Copyright © 2024 Accenture. All rights reserved.

```
mkdir -p $HOME/my_wallet && cd $HOME/my_wallet
```

Download the Autonomous Database wallet, use the ADB OCID from query above. Define the output filename and the wallet password. Example:

```
echo $MY_ADBOCID
oci db autonomous-database generate-wallet --autonomous-database-id
    $MY_ADBOCID \
--file $HOME/my_wallet/my-wallet.zip --password Oracle123
```

A file is created locally in Cloud Shell. Extract the file.

```
unzip $HOME/my_wallet/my-wallet.zip -d $HOME/my_wallet
```

Change parameter in *sqlnet.ora* file with your path:

```
sed -i "s|?\(/network/admin\)|$(pwd)|" $HOME/my_wallet/sqlnet.ora
```

Verify the file using `cat sqlnet.ora`, your path should be inserted, as example:

```
cat $HOME/my_wallet/sqlnet.ora
```

Get the connect alias for TPURGENT connect, example:

```
grep -o '^[^ ]*tpurgent' $HOME/my_wallet/tnsnames.ora
```

Set TNS_ADMIN and ADB_SERVICE variable.

```
export TNS_ADMIN=$HOME/my_wallet
export ADB_SERVICE=$(grep -o '^[^ ]*tpurgent' $HOME/my_wallet/tnsnames.ora)
```

Add the variable to the profile

```
echo "export TNS_ADMIN=$TNS_ADMIN" >> $HOME/.bash_profile
echo "export ADB_SERVICE=$ADB_SERVICE" >> $HOME/.bash_profile
```

Navigate to the **Autonomous Database information** page and select **More actions** - **Administrator password** to set respectively reset your ADB password.

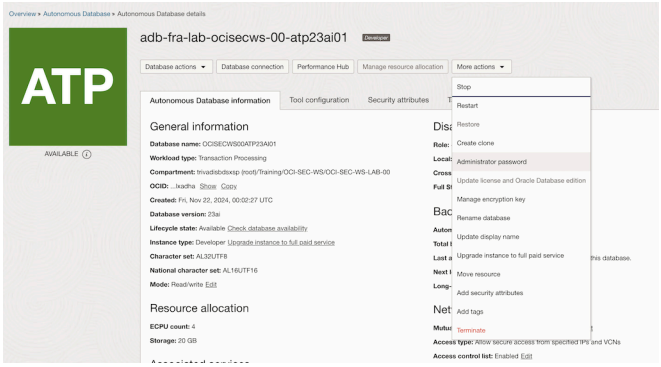


Figure 13: ADB More Actions

Copyright © 2024 Accenture. All rights reserved.

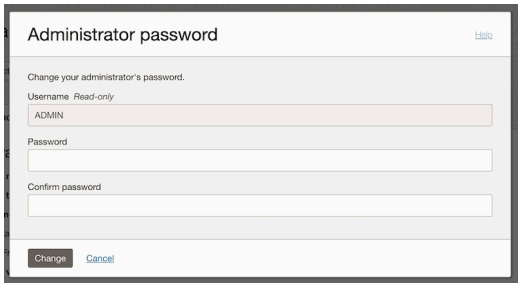


Figure 14: ADB Password Reset

Connect by sqlplus, use the alias or ADB_SERVICE variable from above. Example:

```
sqlplus admin@$ADB_SERVICE
```

Example Output:

```
sqlplus admin@$ADB_SERVICE

SQL*Plus: Release 19.0.0.0.0 - Production on Wed Nov 20 15:31:48 2024
Version 19.10.0.0.0

Copyright (c) 1982, 2021, Oracle.  All rights reserved.

Enter password:
Last Successful login time: Mon Nov 18 2024 22:14:53 +00:00

Connected to:
Oracle Database 23ai Enterprise Edition Release 23.0.0.0.0 - Production
Version 23.6.0.24.10

SQL>
```

3.1.6 Step 5: Test ADB Actions

Go to Oracle Database -> Autonomous Database.

Select your Autonomous Database by a click on the display name. Verify, correct compartment is selected.

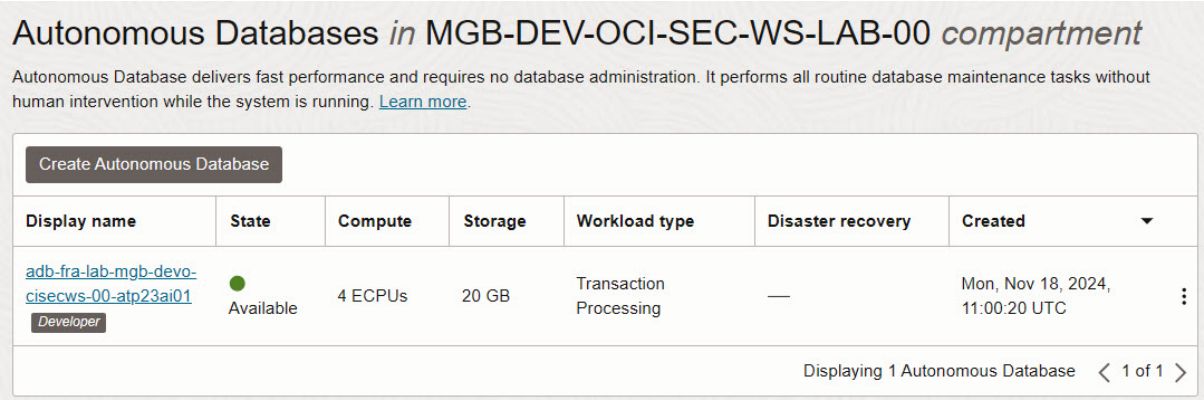


Figure 15: ADB Connect 01

Copyright © 2024 Accenture. All rights reserved.

On the top click on the left button **Database Actions** and select **SQL**.

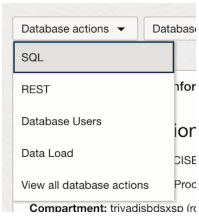


Figure 16: ADB SQL Action

Start the SQL Worksheet and run a test query.

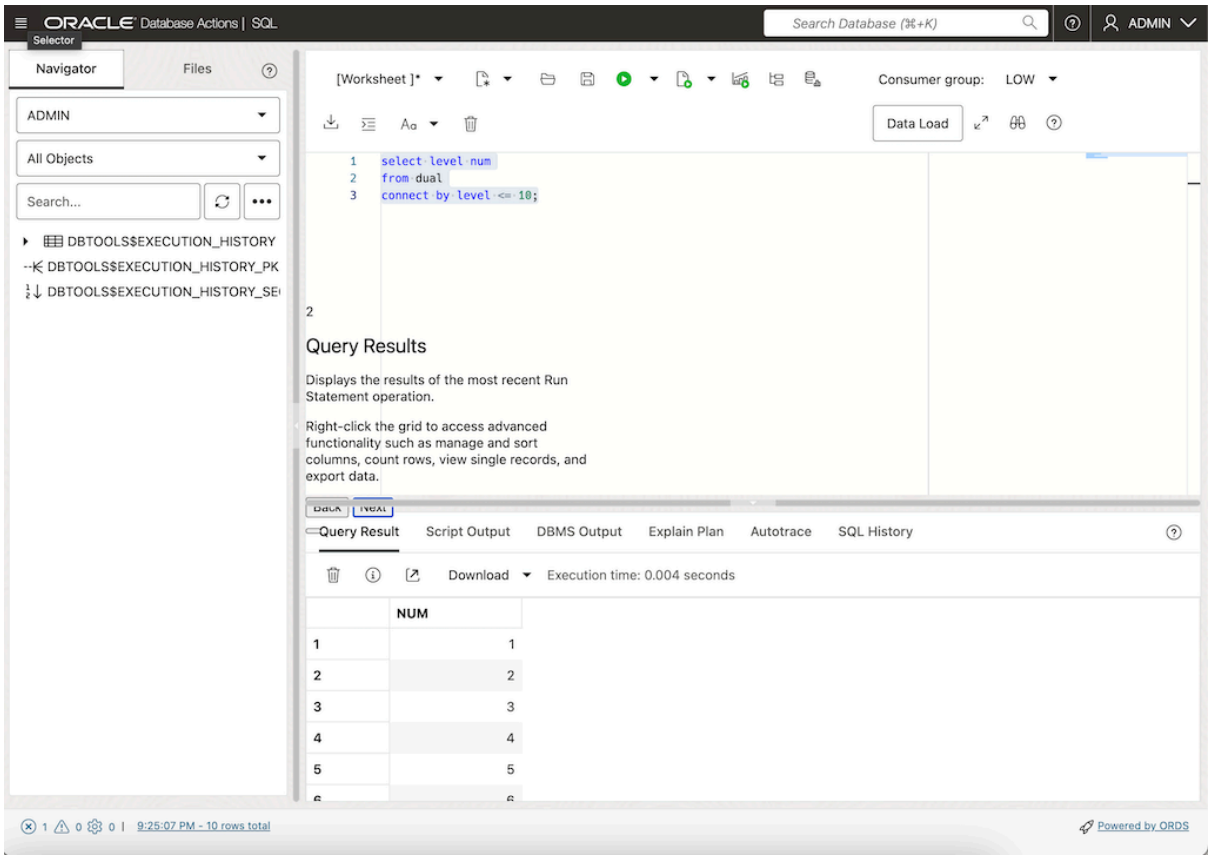


Figure 17: ADB SQL Worksheet

Summary

In this exercise, you:

- Logged in to the OCI Console and explored its features.
- Used the Cloud Shell for basic commands and configurations.
- Configured network access to connect to the Autonomous Database (ADB).
- Downloaded the ADB Wallet and successfully connected to the database using `sqlplus`.

Copyright © 2024 Accenture. All rights reserved.

You are now ready to proceed to the next exercise, where you will explore key management and advanced OCI security features.

- **Previous Exercise:** Workshop Overview
- **Next Exercise:** Exercise 01: Key Management

Copyright © 2024 Accenture. All rights reserved.

4 Basic OCI Security

4.1 Exercise 01: Key Management

In this exercise, we will set up a Vault to store a master encryption key, allowing us to replace the Oracle-provided key for an Object Storage bucket with a customer-managed key.

4.1.1 Objectives

- Create a Vault and generate a master encryption key.
- Apply the master encryption key to a new Object Storage bucket.

Environment

Perform this exercise within the following environment:

- **Compartment:** `OCI-SEC-WS-LAB-nn`
- **Region:** Germany Central (Frankfurt)
- **OCI Console URL:** OCI Console Frankfurt - Login
- **OCI User:** *lab-oci-sec-ws**NN***
- **OCI Password:** *provided by trainer*

Ensure you are in the correct compartment and region. New resources, such as Cloud Shell configurations and ADB access settings, should be created within your designated compartment.

Solution

Login as User XYZ in OCI console. Ensure you have select the proper compartment in from the dropdown list on left side.

Go to Identity -> Security -> Key Management & Secret Management -> Vault

4.1.2 Create Vault and Keys

4.1.2.1 Vault and Master Encryption Key

1. Create a Vault Do NOT create a PRIVATE VAULT. Set name according compartment name, as example *vault-oci-sec-ws-lab-00* for compartment *OCI-SEC-WS-LAB-00*.

Copyright © 2024 Accenture. All rights reserved.

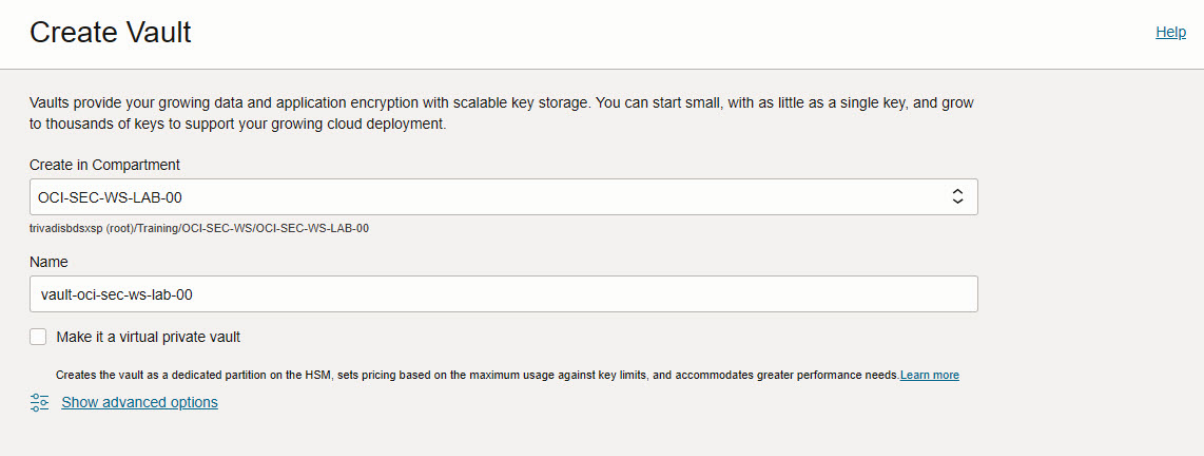


Figure 18: » step_1

2. Verify create Vault is in state Active. Be patient.

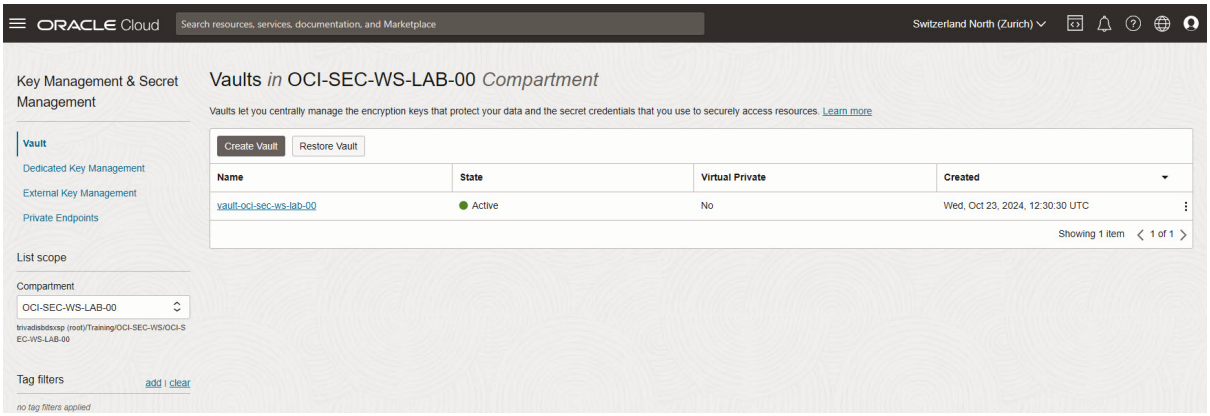


Figure 19: » step_2

3. Select the created Vault to add a Master Encryption Key. *Create Key*.

Copyright © 2024 Accenture. All rights reserved.

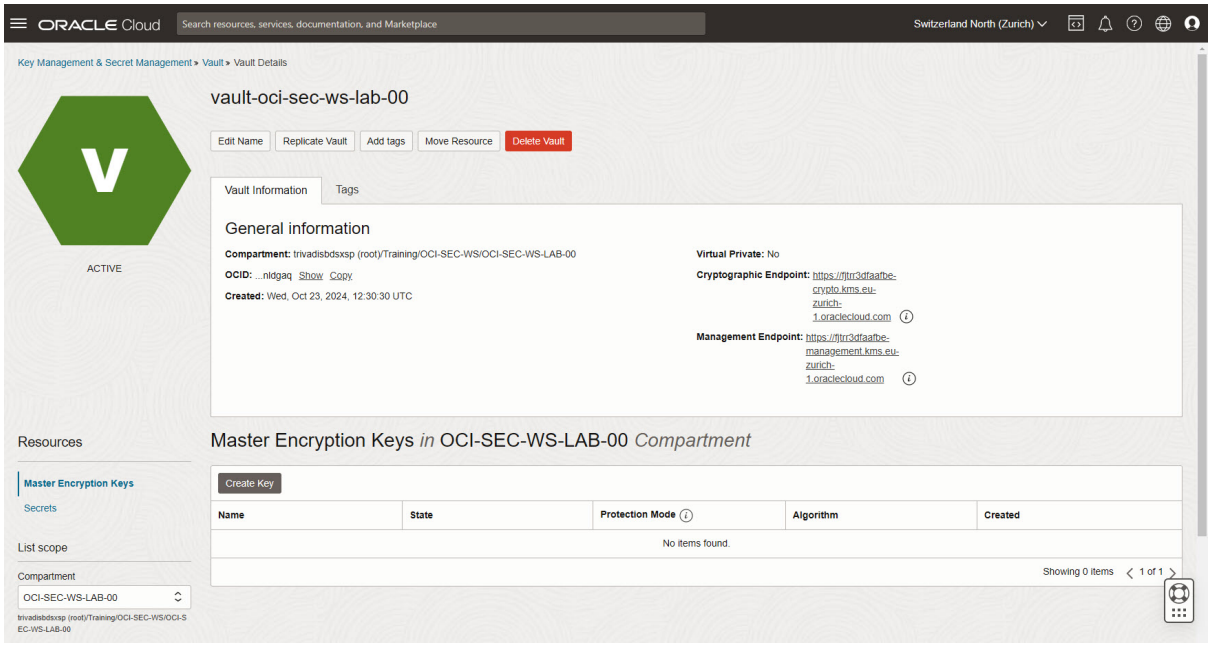


Figure 20: » step_3

4. Select Protection Mode *Software*, use Key Shape: Algorithm and Key Shape: Length as per default. *Create Key*. Do not import any external key.

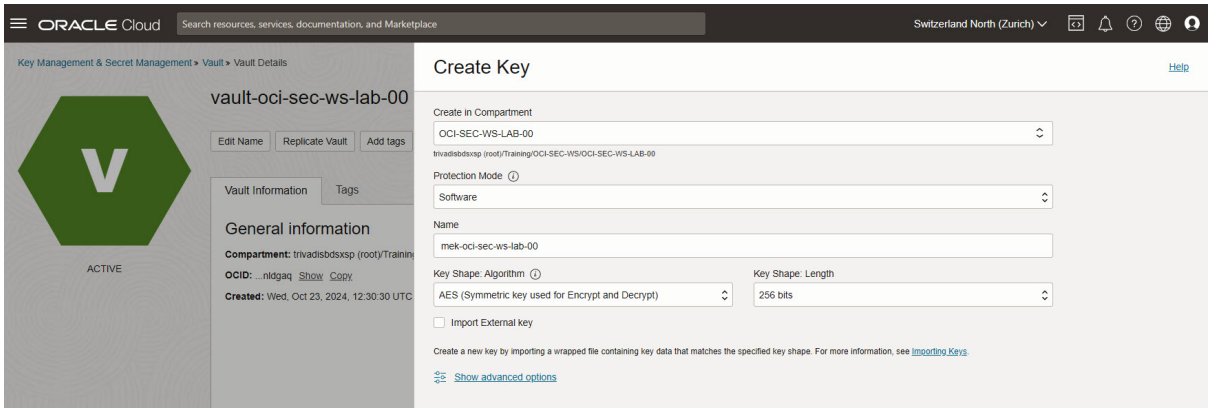


Figure 21: » step_4

5. Verify Master Encryption Key is in State *Enabled*.

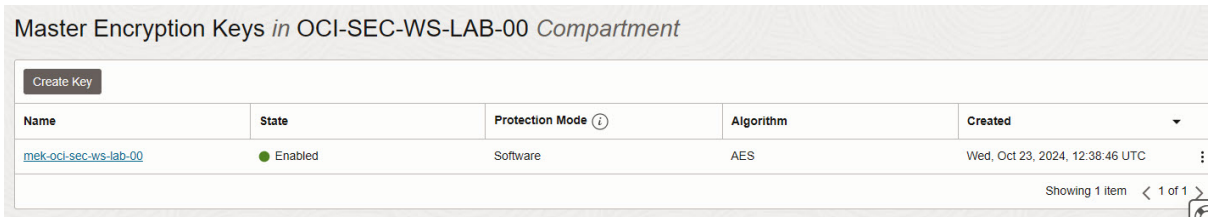


Figure 22: » step_5

Copyright © 2024 Accenture. All rights reserved.

4.1.2.2 Create new Object Storage with a customer managed Master Encrytion Key

Go to Storage -> Object Storage & Archive Storage -> *Create Bucket*.

Set bucket name, in section *Encryption* now you can select your Master Encryption Key. Key not visible? Verify compartment and region (Frankfurt).

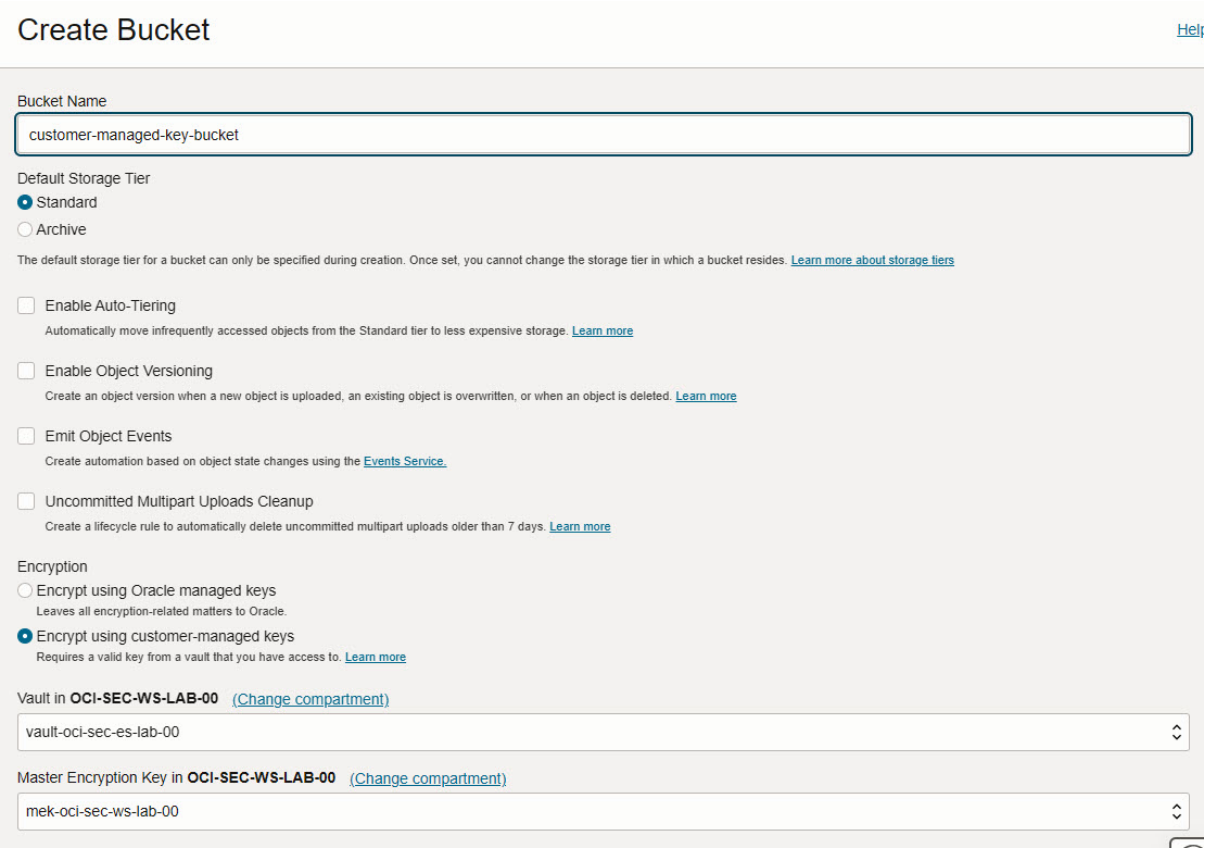


Figure 23: » step_6

Verify the key is set, you can edit or unassign it.

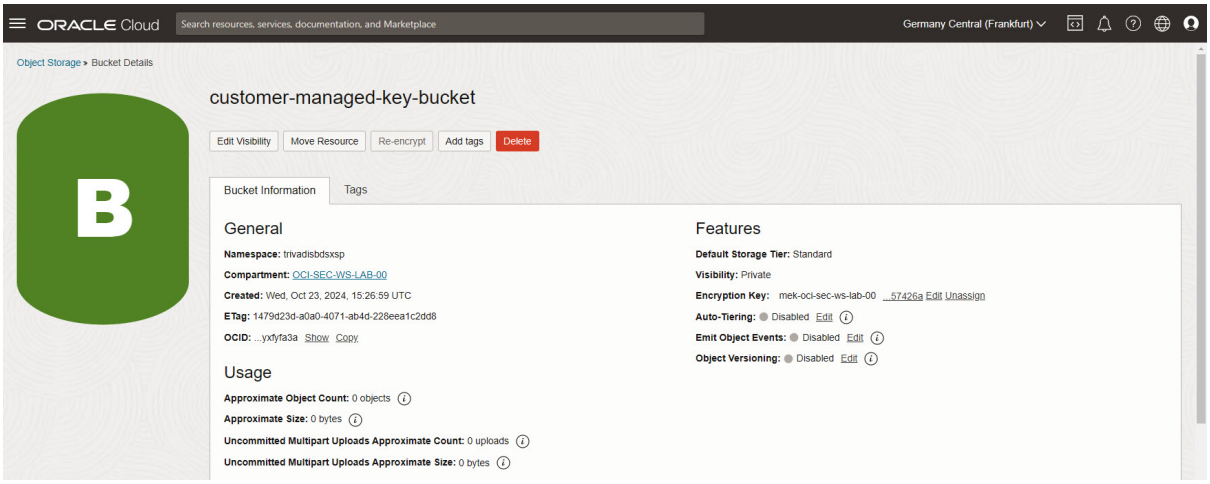


Figure 24: » step_7

Copyright © 2024 Accenture. All rights reserved.

4.1.2.3 Change Compute Instance Boot Volume with a Master Encrytion Key Go to Compute -> Instances -> Webserver 01 (as example: ci-fra-lab-ocisecws-00-webserver01).

Under resources, select the Boot volume name attached to the compute instance.

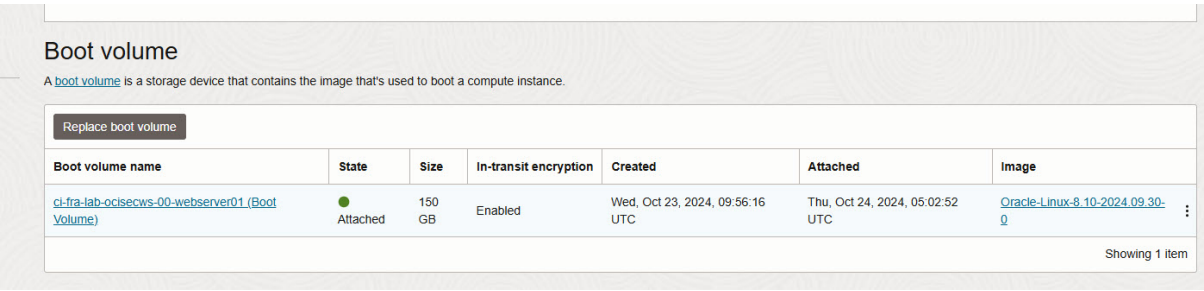


Figure 25: » step_8

Assign a new MEK.

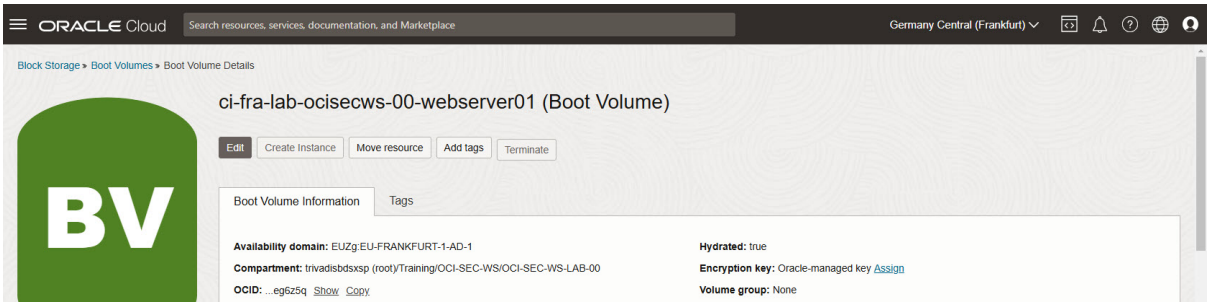


Figure 26: » step_9

Select your created Vault and Master Encrption Key. *Assign*. The Boot Volume will be updated and the key set.

Copyright © 2024 Accenture. All rights reserved.

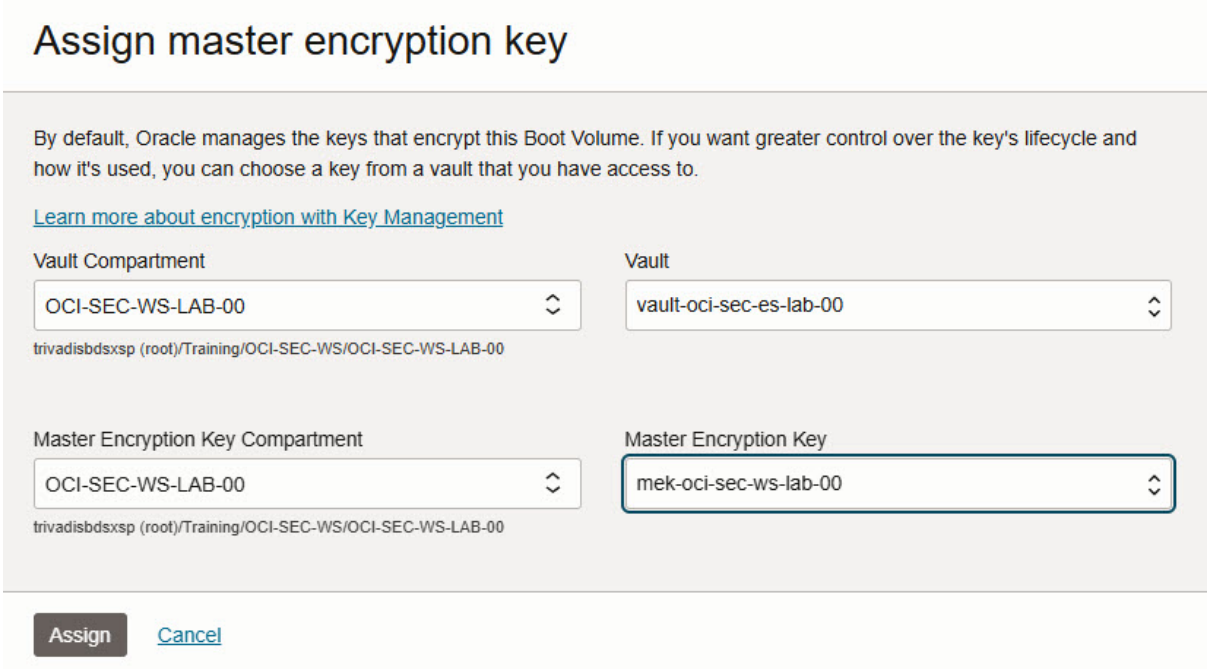


Figure 27: » step_10

Summary

In this exercise, you:

- Created a Vault to securely store encryption keys.
- Generated a master encryption key within the Vault.
- Applied the master encryption key to a new Object Storage bucket, enabling customer-managed encryption.

You are now ready to continue with the next exercise, where you will configure Cloud Guard for manual remediation of security alerts.

- **Previous Exercise:** Exercise 00: Getting Started with OCI
- **Next Exercise:** Exercise 02: Manual Remediation

Copyright © 2024 Accenture. All rights reserved.

5 Cloud Guard

5.1 Exercise 02: Manual Remediation

In this exercise, we will configure Cloud Guard to detect public Object Storage buckets by creating a custom detector recipe. You will also set up a target to monitor your compartment and test the configuration by creating a public bucket.

5.1.1 Objectives

- Clone an existing Oracle-managed detector recipe.
- Create a new target to monitor objects in your compartment.
- Create an Object Storage bucket and set its visibility to public.
- Verify that Cloud Guard generates an alert for the public bucket.

Environment

Perform this exercise within the following environment:

- **Compartment:** `OCI-SEC-WS-LAB-nn`
- **Region:** Germany Central (Frankfurt)
- **OCI Console URL:** OCI Console Frankfurt - Login
- **OCI User:** *lab-oci-sec-ws**NN***
- **OCI Password:** *provided by trainer*

Ensure you are in the correct compartment and region. New resources, such as Cloud Shell configurations and ADB access settings, should be created within your designated compartment.

Solution

Login as User XYZ in OCI console and go to *Security -Cloud Guard Overview*. Ensure you have select the proper compartment in from the dropdown list on left side.

Copyright © 2024 Accenture. All rights reserved.

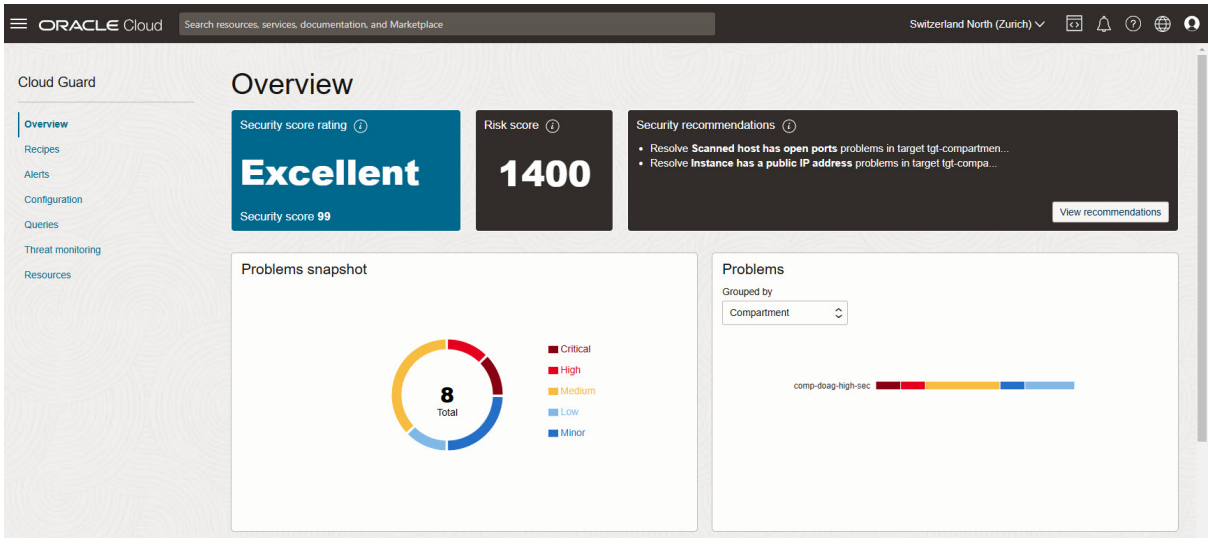


Figure 28: » overview

5.1.2 Clone existing Oracle managed recipes

From left menu, select *Recipes* and *Clone*.

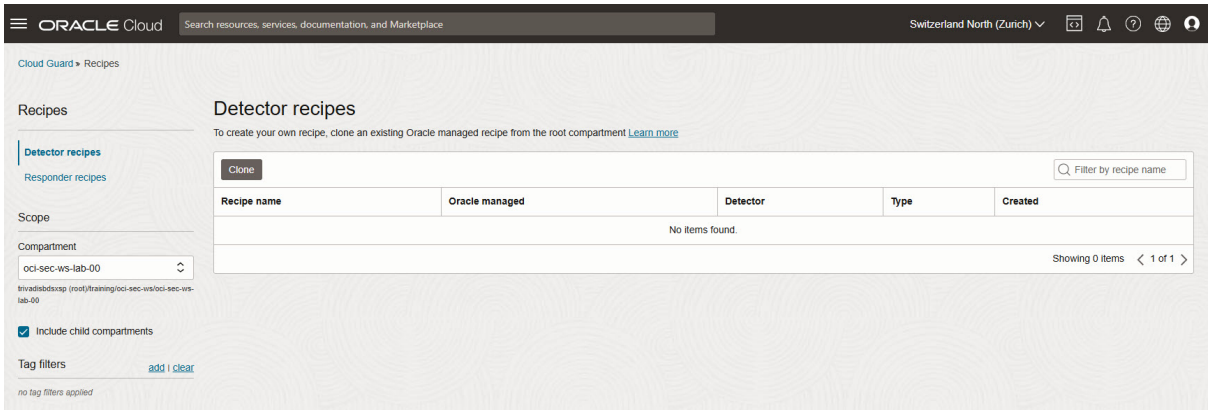


Figure 29: » step_1

5.1.2.1 Clone *Detector* recipes Cloud Guard -> Recipes -> Detector recipes

- Change compartment on top to trivadisbdsxsp (root).
- Select recipe **OCI Activity Detector Recipe (Oracle managed)**from dropdown list
- Set name for cloned recipe , as example **OCI Activity Detector Recipe comp-oci-ws-sec-ws-lab-00**.
- Ensure in section Compartment, your compartment is selected.

Copyright © 2024 Accenture. All rights reserved.

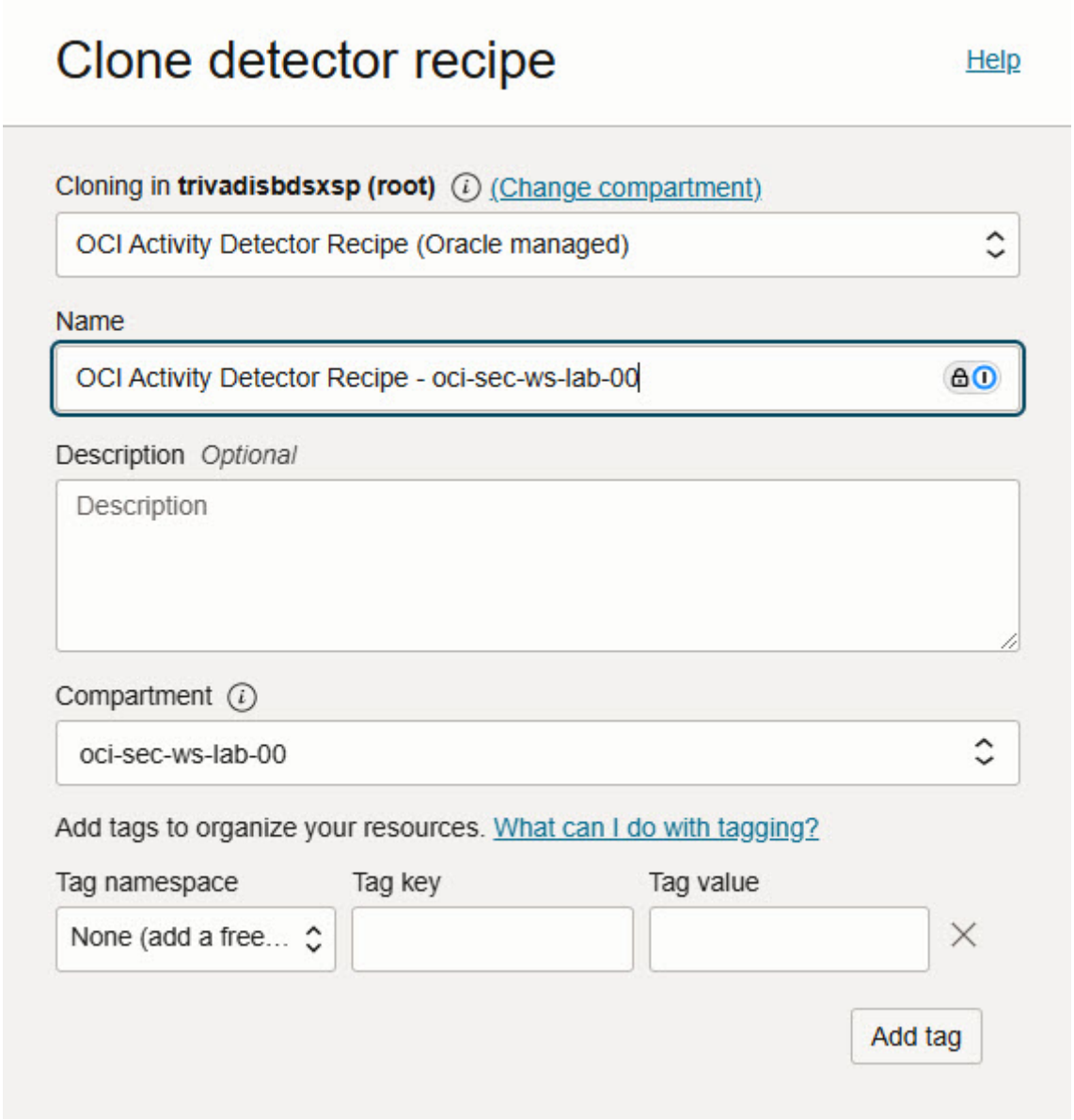


Figure 30: » step_2

Press *Clone* at the bottom.

Repeat the steps for the other Oracle managed detector recipes:

- OCI Configuration Detector Recipe (Oracle managed)
- OCI Instance Security Detector Recipe (Oracle managed)

After successful clone, you have recipes for Instance Security, Configuration and Activity.

5.1.2.2 Clone *Responder* recipes

Cloud Guard -> Recipes -> Responder recipes

- Ensure *Responder recipes* is select from left side menu.
- Change compartment on top to trivadisbdsxsp (root).

Copyright © 2024 Accenture. All rights reserved.

- Select recipe OCI Activity Detector Recipe (Oracle managed) from dropdown list
- Set name for cloned recipe , as example *OCI Activity Detector Recipe -*
- Ensure in section Compartment, your compartment is selected.

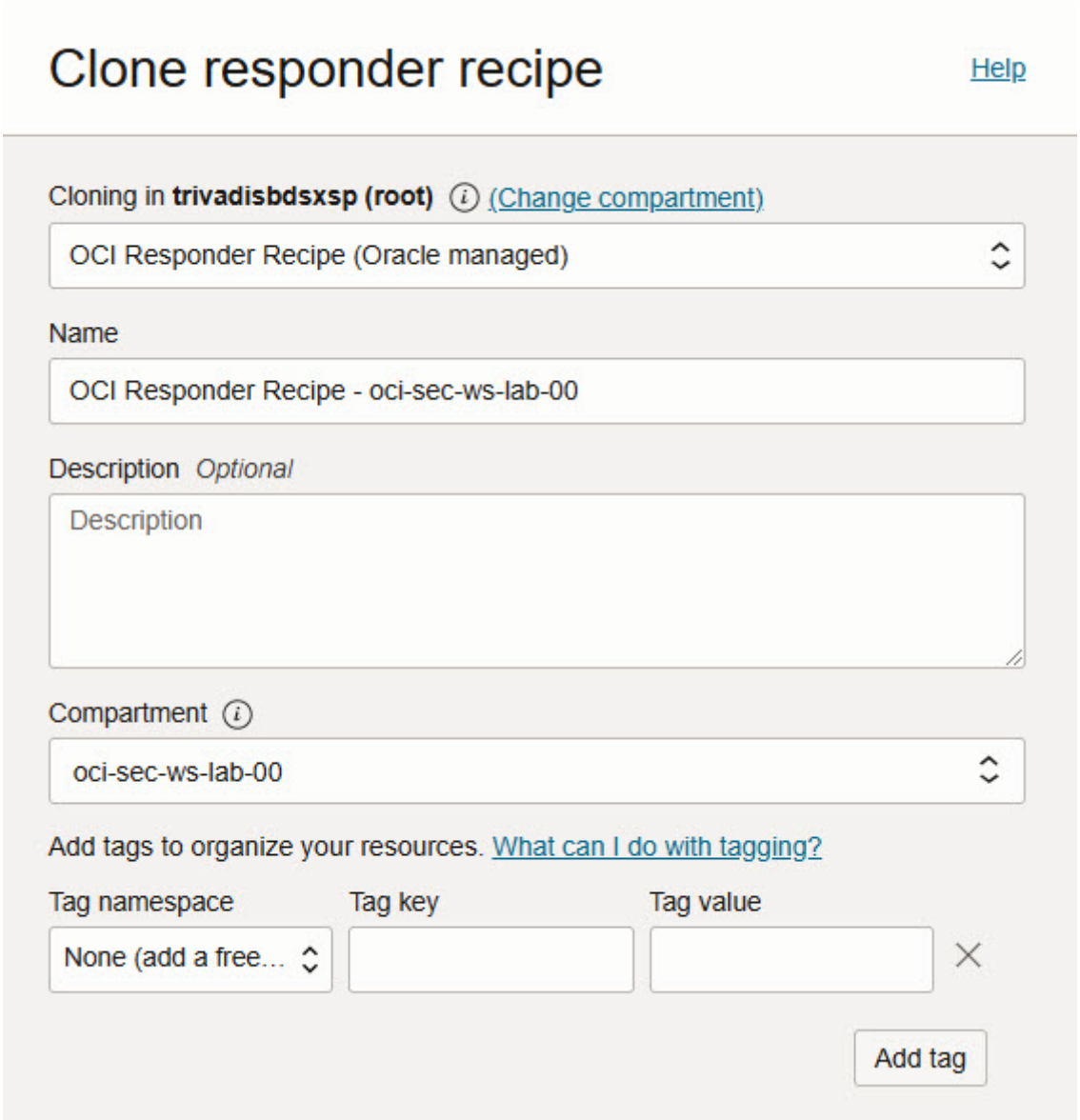


Figure 31: » step_3

Press *Clone* at the bottom.

5.1.3 Verify cloned recipes

After cloning, you must have three detector recipes and one responder recipes on your compartment.

Detector recipes:

Copyright © 2024 Accenture. All rights reserved.

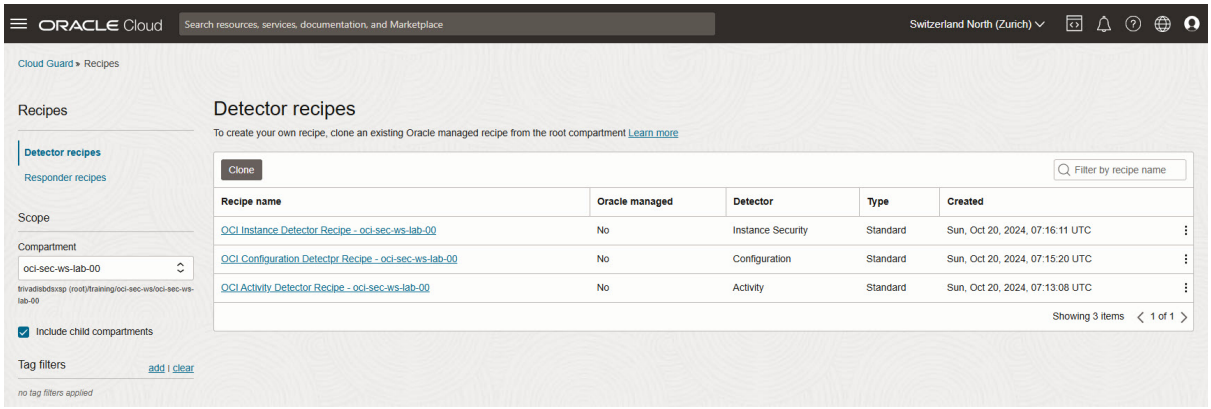


Figure 32: » step_4

Responder recipe:

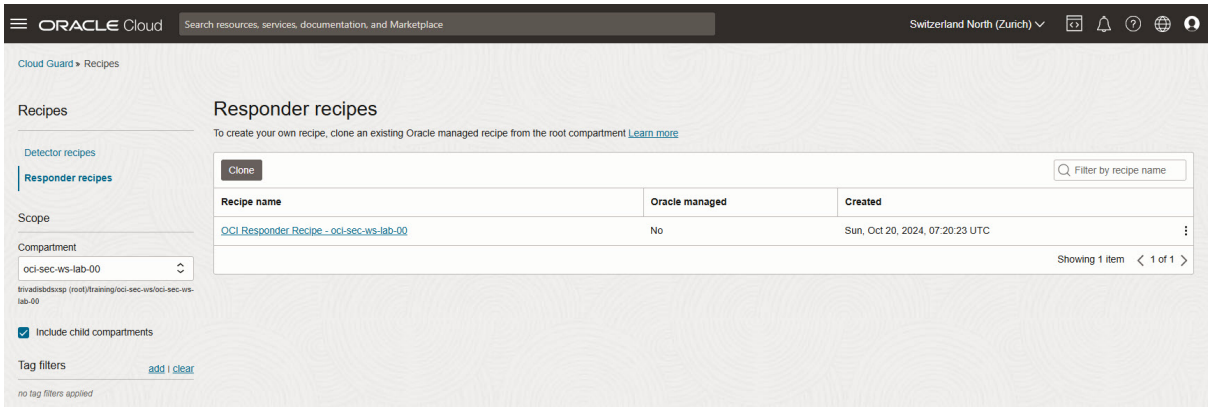


Figure 33: » step_5

5.1.4 Create a new target to observer your compartment objects

In this step, we create a target based in your compartment and add the recipes we created. Ensure, your compartment is selected in panel left.

Identity & Security -> Cloud Guard -> Configuration -> Targets -> Create Target

Copyright © 2024 Accenture. All rights reserved.

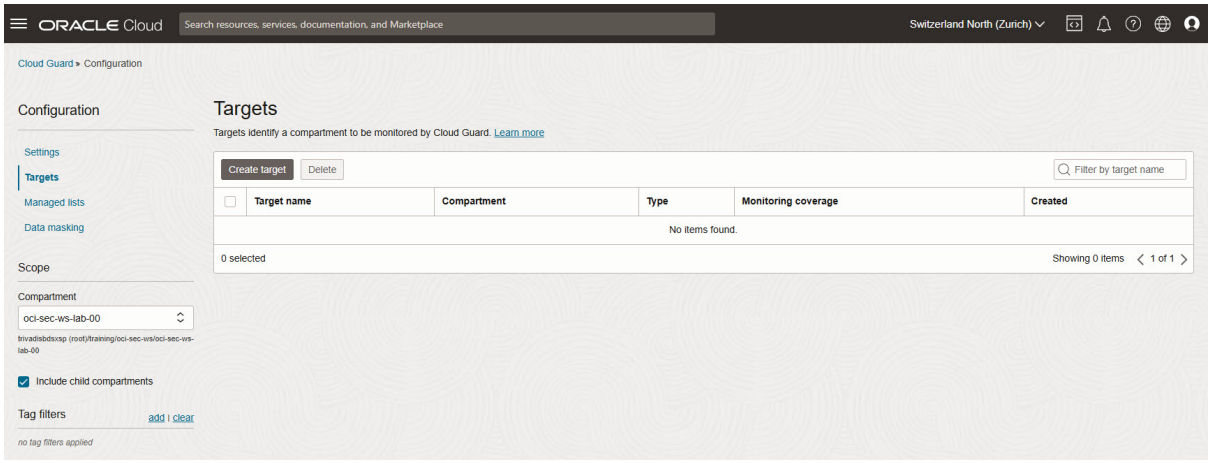


Figure 34: » targets_1

5.1.4.1 Basic Information Add basic information and description. Use the recipes you created for your compartment.

- Set target name according compartment, as example *cg-tgt-oci-sec-ws-lab-00*.
- Add description
- Verify compartment is correct according your work compartment.

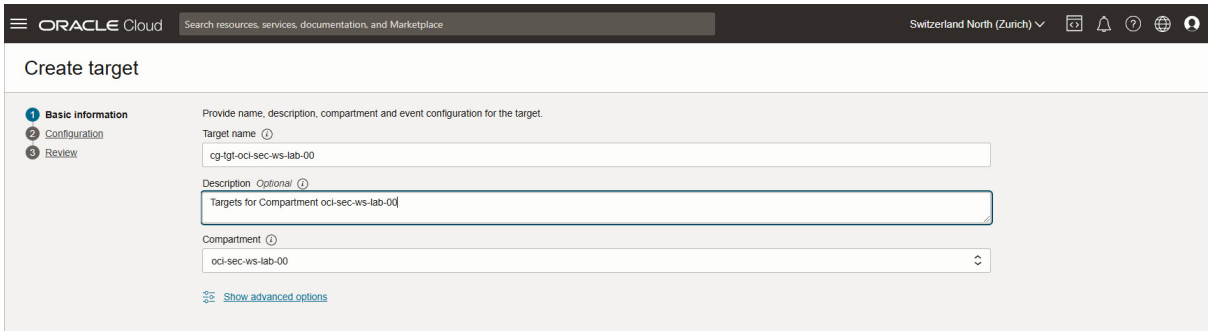


Figure 35: » targets_2

Press *Next* at the bottom.

5.1.4.2 Configuration Add basic information and description.

- In Posture and threat monitoring recipes, select the *OCI Configuration Detector Recipe* you created for your compartment.
- In Instance Security recipe, select the *OCI Instance Detector Recipe* you created for your compartment.
- Activate *All compute instances*.

Copyright © 2024 Accenture. All rights reserved.

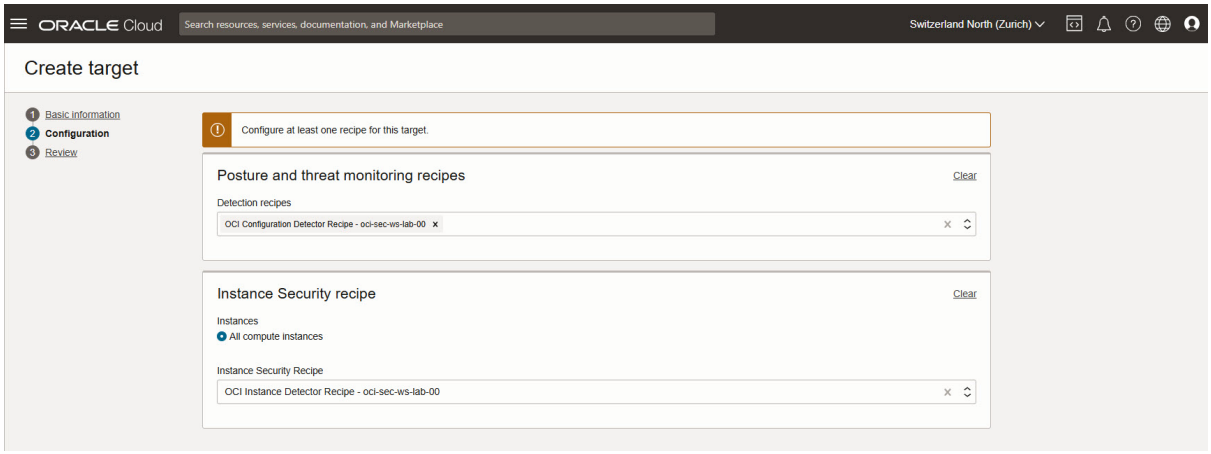


Figure 36: » targets_3

Press *Next* at the bottom.

5.1.4.3 Review Verify you select the proper recipes based on your compartment.

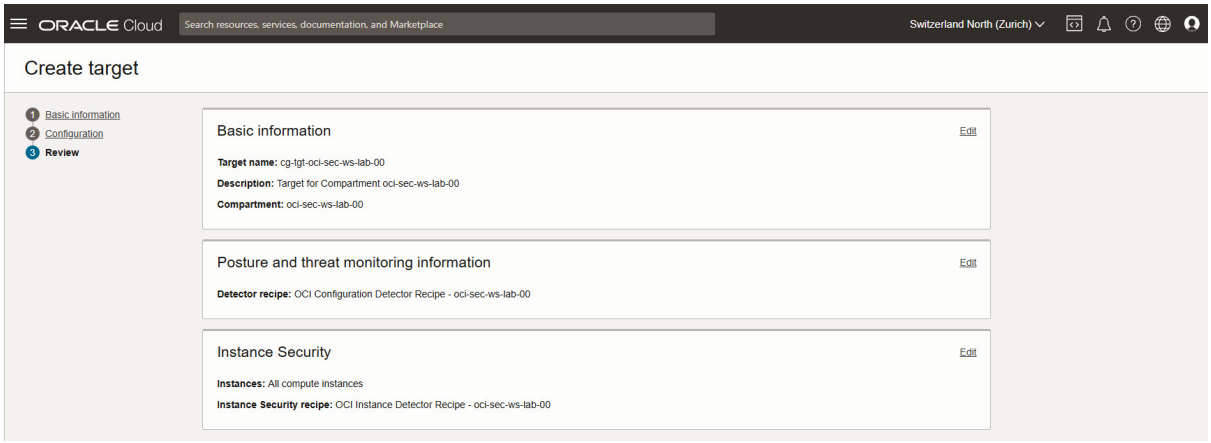


Figure 37: » targets_4

Press *Create* at the bottom. Go back to Cloud Guard Overview page.

5.1.5 Create a object storage bucket and change visibility to public

In this step, we create am Object Storage bucket and change visibility.

5.1.5.1 Create Bucket Add basic information and description. Ensure you are in the correct compartment. If not, select your compartment in left side dropdown menu.

Go to Storage -> Object Storage -> Buckets

Copyright © 2024 Accenture. All rights reserved.

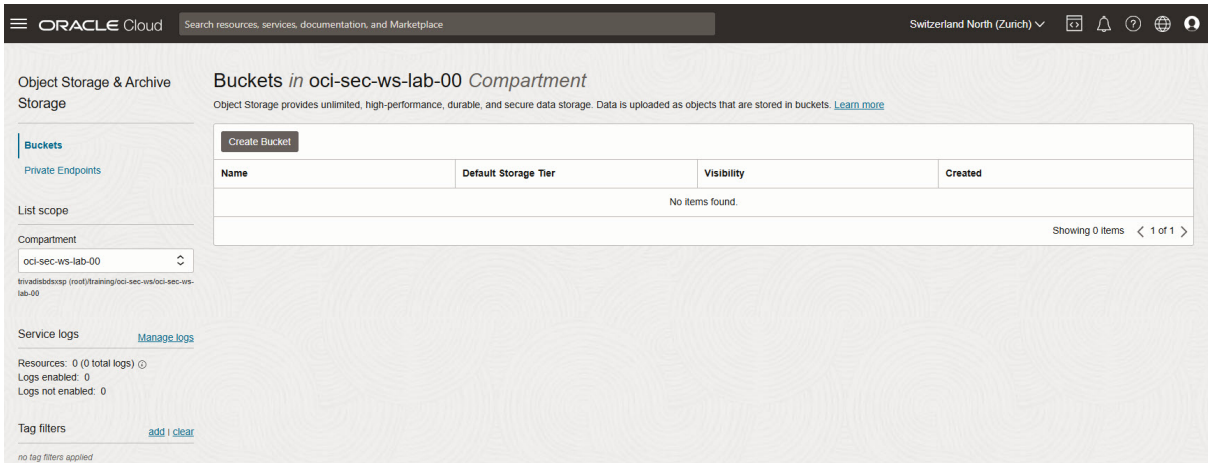


Figure 38: » bucket_1

Press *Create Bucket*.

- Set Bucket Name to *public-bucket* and let other settings as per default.

Copyright © 2024 Accenture. All rights reserved.

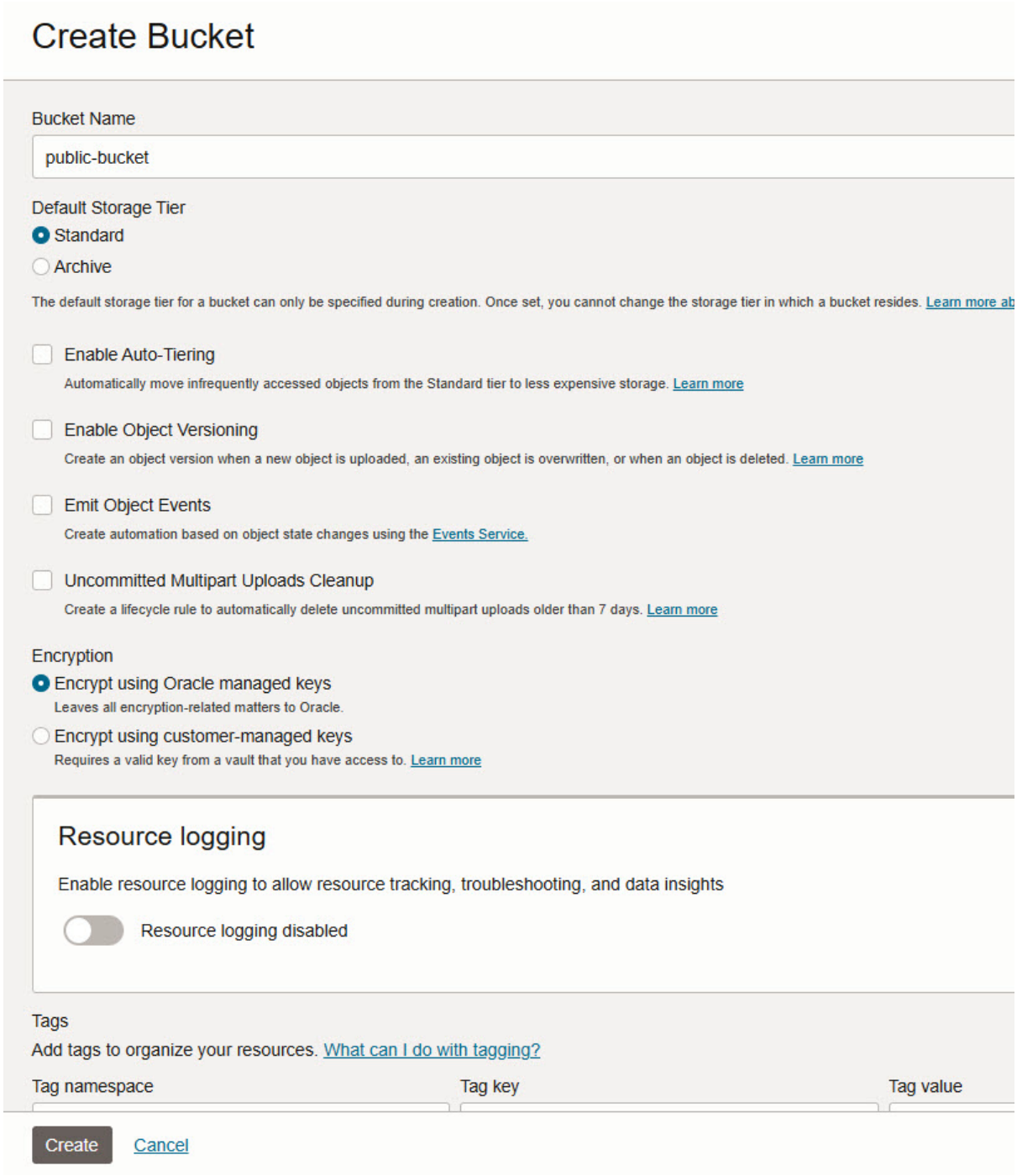


Figure 39: » bucket_2

Press *Create* at the bottom.

5.1.5.2 Edit Visibility Edit created bucket by click on the three dots -> Edit Visibility.

Copyright © 2024 Accenture. All rights reserved.

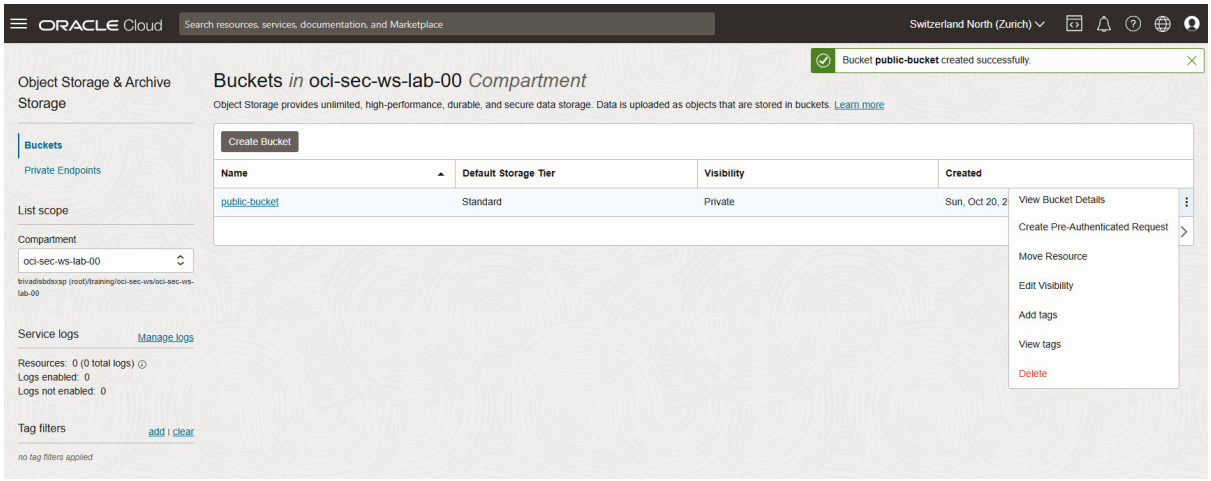


Figure 40: » bucket_3

Change visibility to Public. Let checkbox setting as per default.

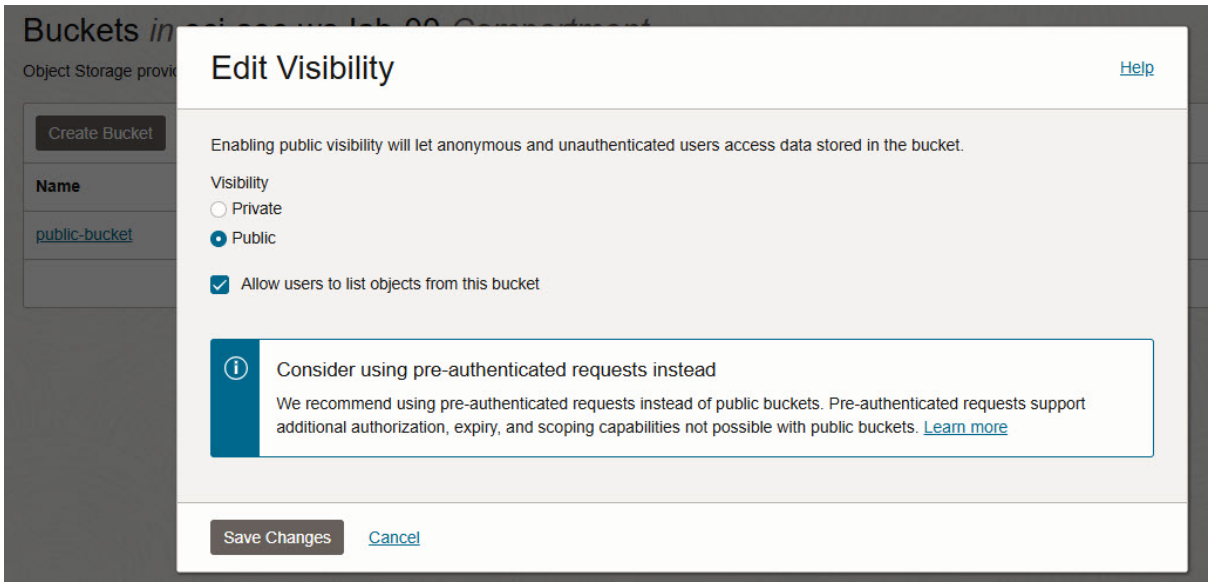


Figure 41: » bucket_4

Press *Save Changes* at the bottom.

5.1.5.3 Verification The bucket is set to public and marked by a yellow triangle.

Copyright © 2024 Accenture. All rights reserved.

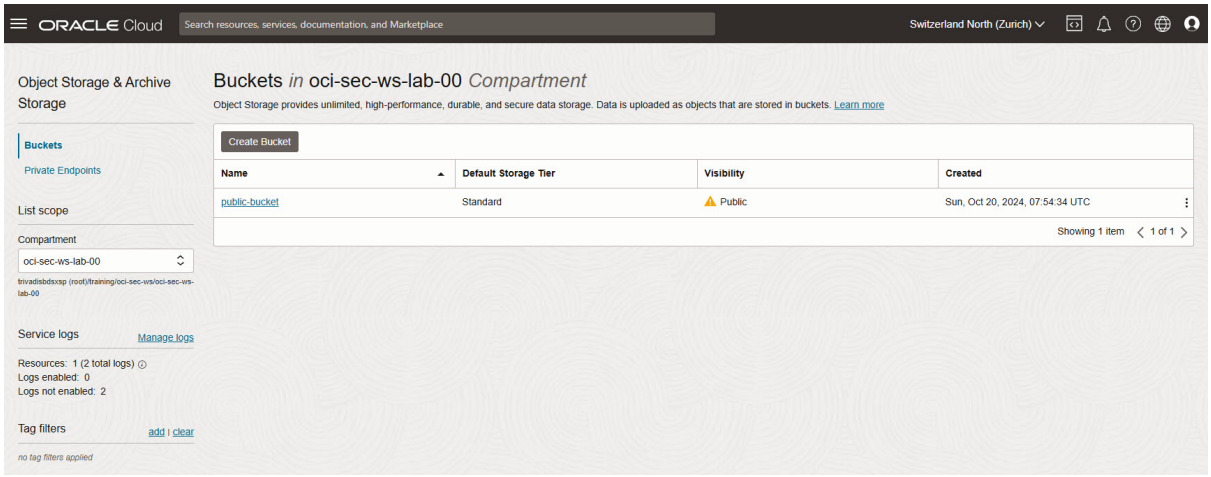


Figure 42: » bucket_5

5.1.6 Verify new Cloud Guard alert

Identity & Security -> Cloud Guard -> Alerts -> Problems

Verify if the public buckets is recognized by Cloud Guard. Yiu see an entry with risk level **Critical**.

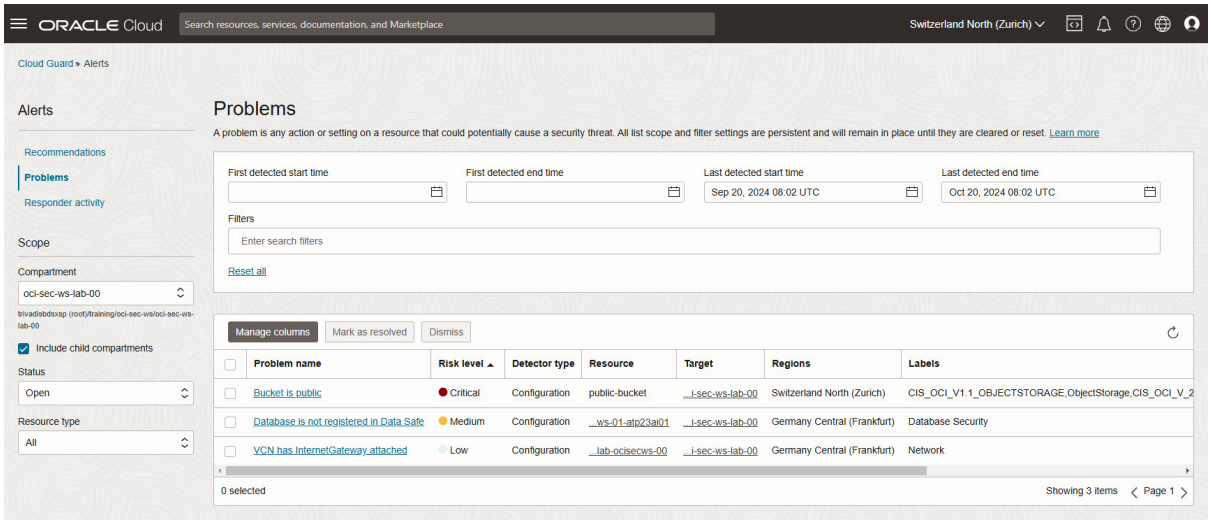


Figure 43: » alert_1

5.1.6.1 Remediation Select the alert entry by click on the bucket name to see the details and press *Remediate*.

Copyright © 2024 Accenture. All rights reserved.

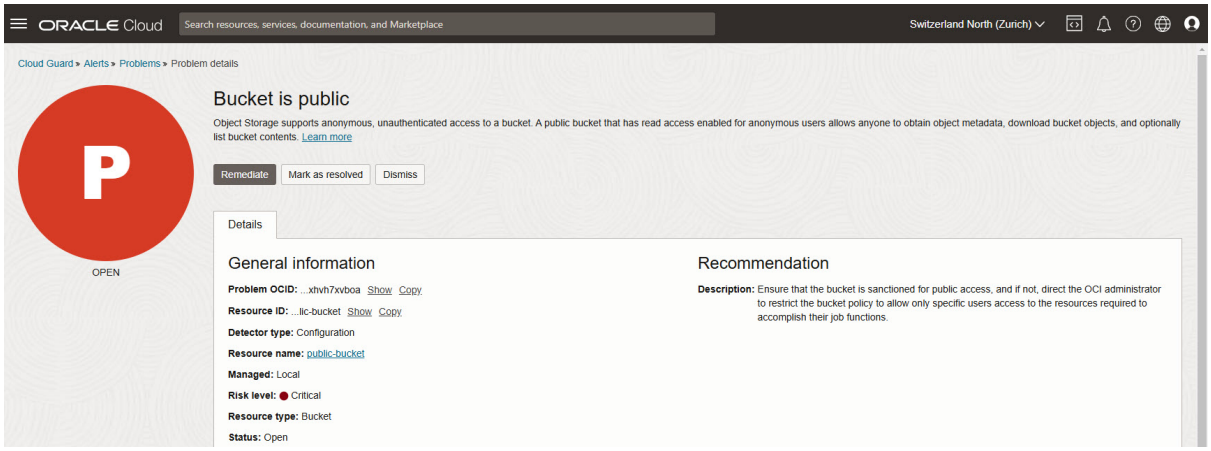


Figure 44: » alert_2

Ignore the warning ab out missing permissions as your OCI user is not able to see the policies created on top level compartment.

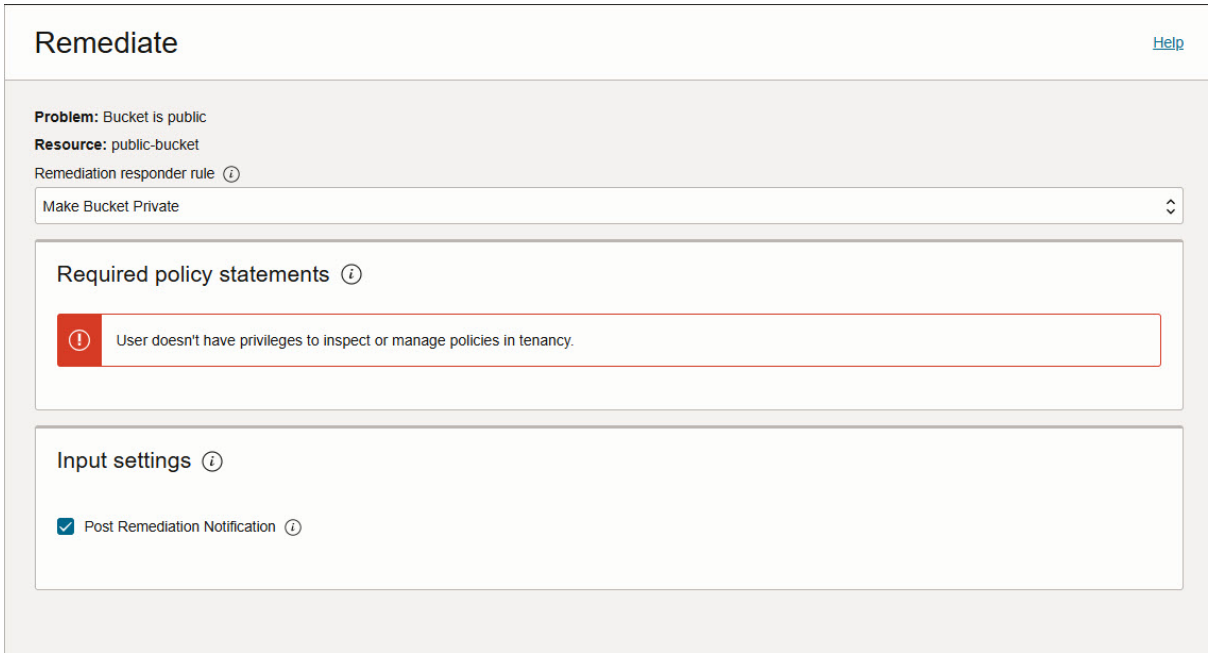


Figure 45: » alert_3

Confirm.

Copyright © 2024 Accenture. All rights reserved.

Figure 46: » alert_4

5.1.6.2 Verification After some seconds, the visibility for your created Object Storage bucket has changed back to *Private*.

Storage -> Object Storage -> Buckets

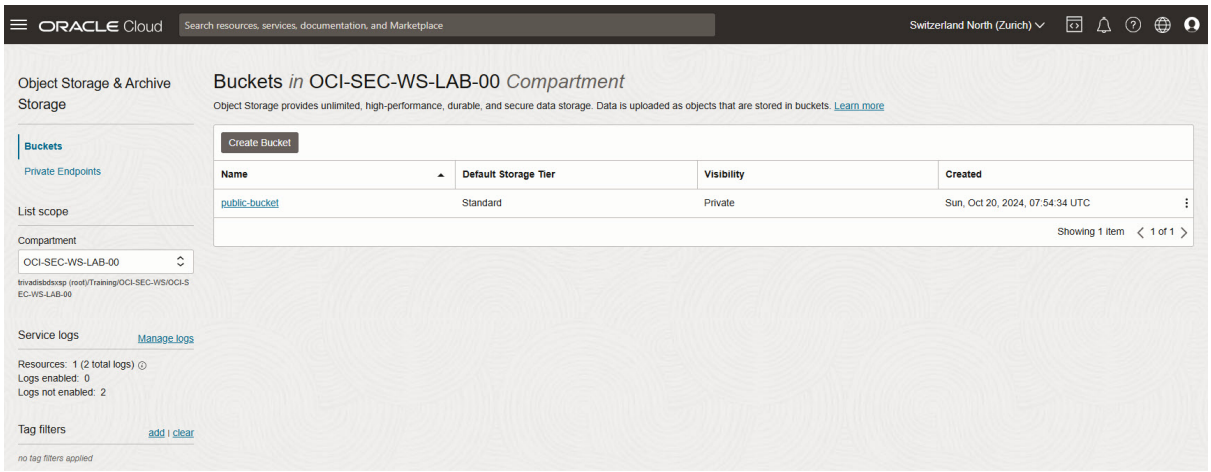


Figure 47: » alert_5

In Cloud Guard alert view, the state changes after a couple of seconds too.

The alert is not longer visible in alert list.

Summary

In this exercise, you:

- Cloned an Oracle-managed detector recipe in Cloud Guard.
- Created a new target to observe and monitor resources in your compartment.
- Configured an Object Storage bucket with public visibility.
- Verified that Cloud Guard generated an alert for the public bucket, indicating successful detection.

You are now ready to continue with the next exercise, where you will explore further Cloud Guard configurations.

Copyright © 2024 Accenture. All rights reserved.

- **Previous Exercise:** Exercise 01: Key Management
- **Next Exercise:** Exercise 03: Auto Remediation

5.2 Exercise 03: Auto Remediation

In this exercise, you will enable auto-remediation in Cloud Guard to automatically resolve issues with public Object Storage buckets. Building on the detector settings from the previous exercise, you will configure a responder recipe to change the visibility of public buckets to private automatically.

5.2.1 Objectives

- Add a responder recipe to the target.
- Enable auto-remediation to automatically resolve public bucket issues.
- Test the setup by creating a new bucket and setting its visibility to public,
- verifying that Cloud Guard automatically changes it to private.

Environment

Perform this exercise within the following environment:

- **Compartment:** `OCI-SEC-WS-LAB-nn`
- **Region:** Germany Central (Frankfurt)
- **OCI Console URL:** OCI Console Frankfurt - Login
- **OCI User:** *lab-oci-sec-ws**NN***
- **OCI Password:** *provided by trainer*

Ensure you are in the correct compartment and region. New resources, such as Cloud Shell configurations and ADB access settings, should be created within your designated compartment.

Solution

Login as User XYZ in OCI console and go to *Cloud Guard Overview*. Ensure you have select the proper compartment in from the dropdown list on left side.

Copyright © 2024 Accenture. All rights reserved.

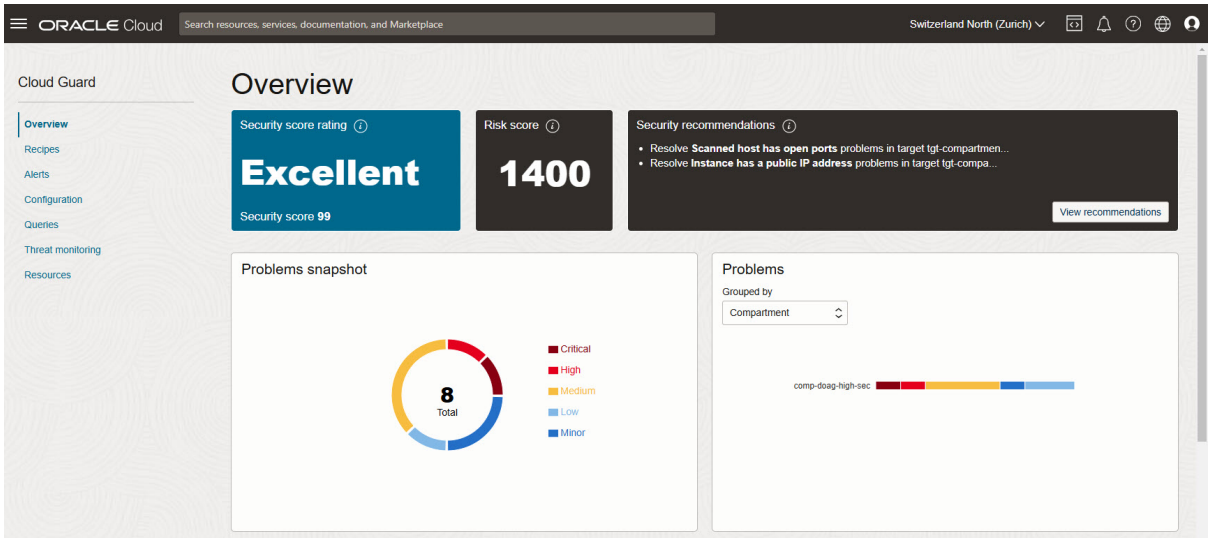


Figure 48: » overview

5.2.2 Enable Auto Resolve

5.2.2.1 Add Responder recipe to Target We must add the responder recipe to target configuration.

Identity & Security -> Cloud Guard -> Configuration -> Targets

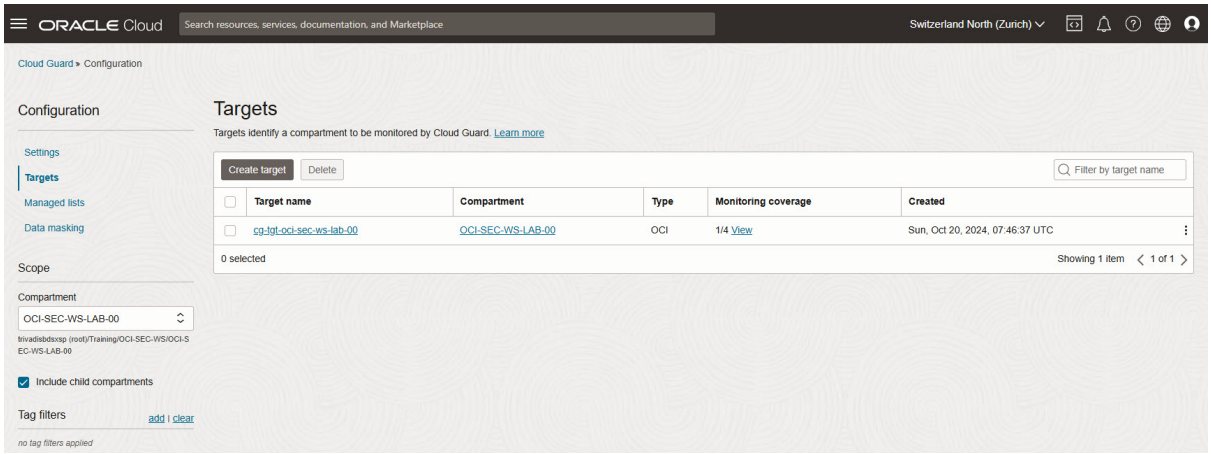


Figure 49: » step_1

Select your created target an scroll at the bottom.

Copyright © 2024 Accenture. All rights reserved.

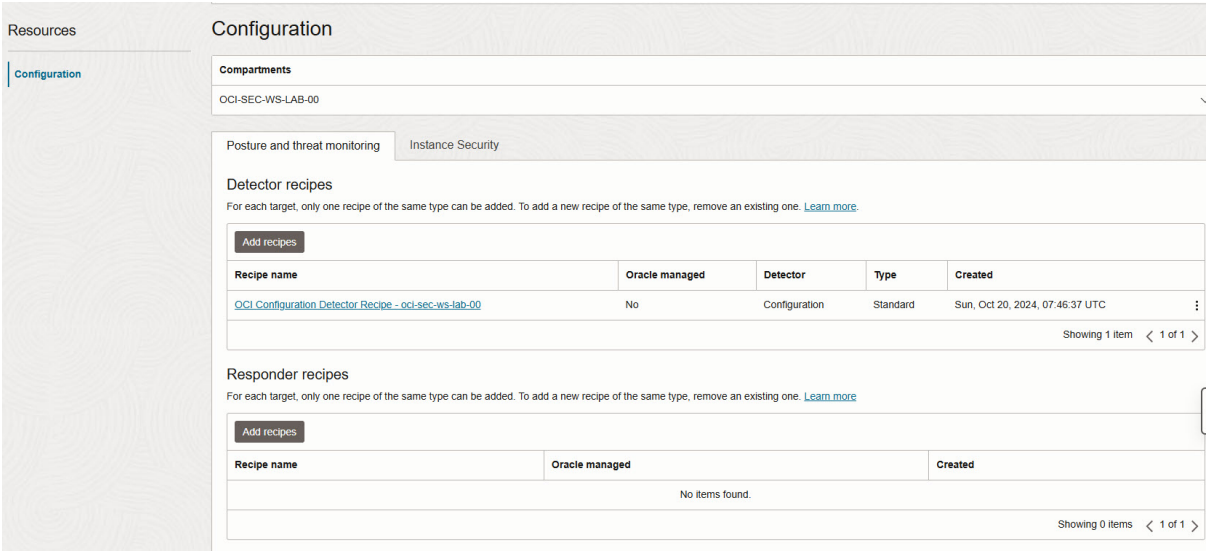


Figure 50: » step_2

In section *Configuration* und *Responder recipes*, add recipe. Select your responder recipe from dropdown list and press *Add recipes*. Do not select the Oracle managed recipe as you have no privileges there to change any settings.

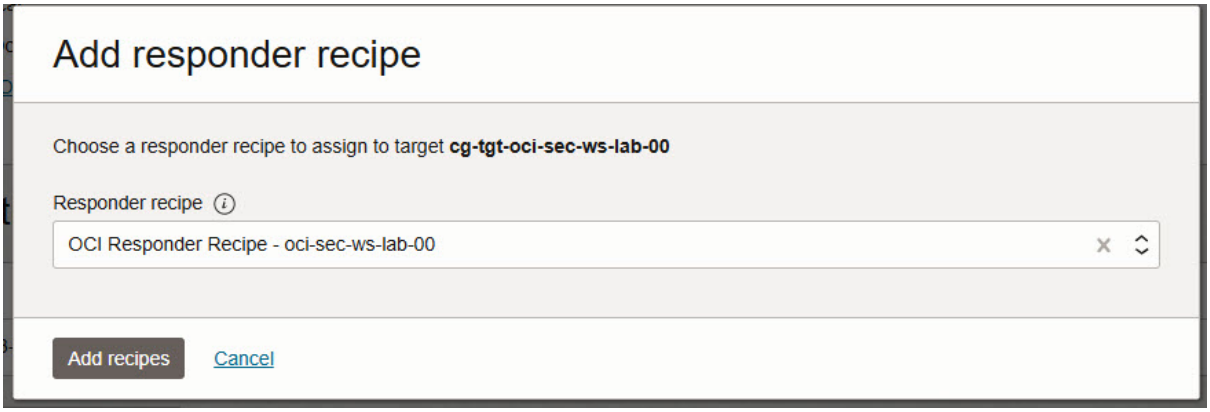


Figure 51: » step_3

5.2.2.2 Enable Auto resolve Select the fresh added Responder recipe. Edit the entry for *Make Bucket Private* by click on the three dots and *Edit*.

Copyright © 2024 Accenture. All rights reserved.

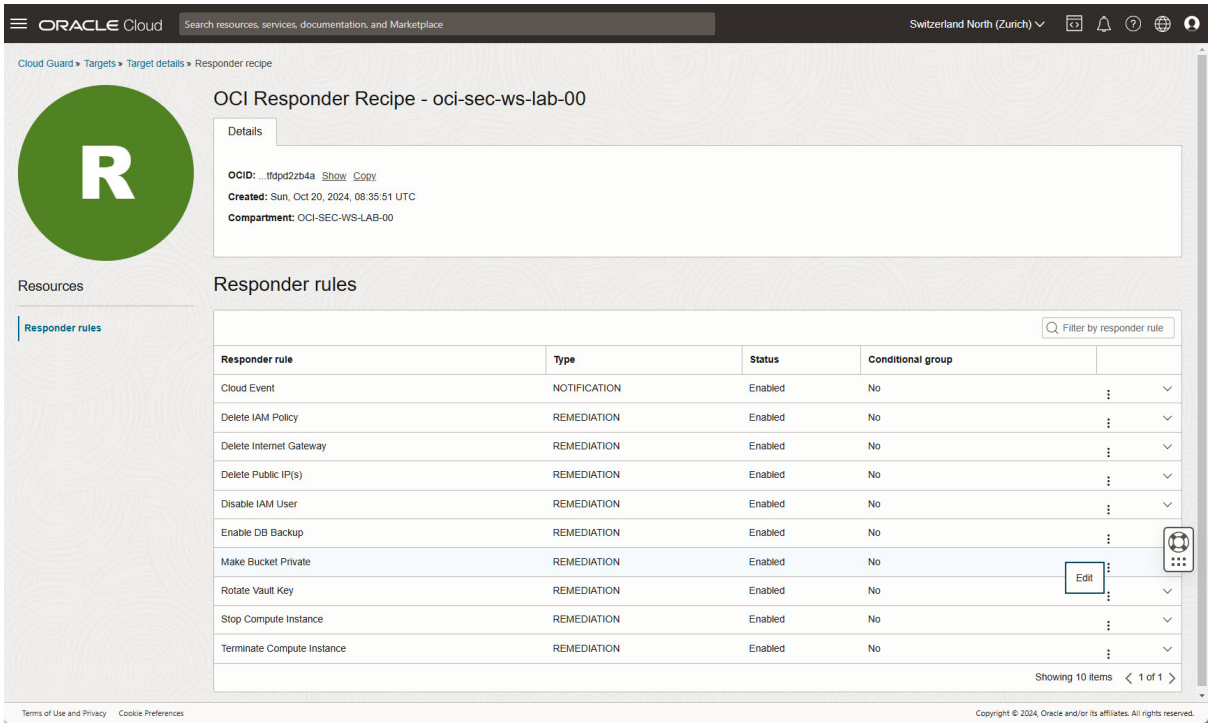


Figure 52: » step_4

You can ignore the alert about privileges as these settings are done on top compartment level. We set condition

- In section *Setting*, activated *Execute automatically*.
- Enable checkbox to confirm the execution.
- Set Conditional Group for parameter region to **eu-frankfurt-1**
- Parameter: Region
- Operator: In
- List: Custom List
- Value: eu-frankfurt-1

Copyright © 2024 Accenture. All rights reserved.

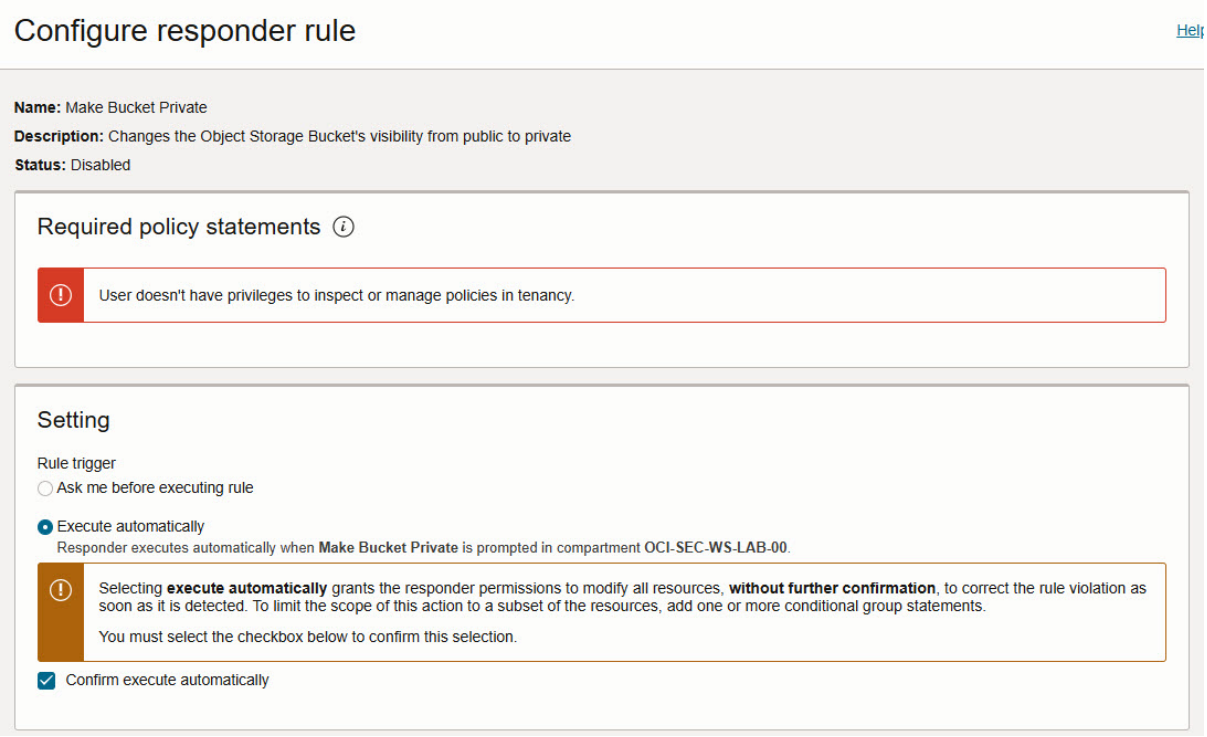


Figure 53: » step_5

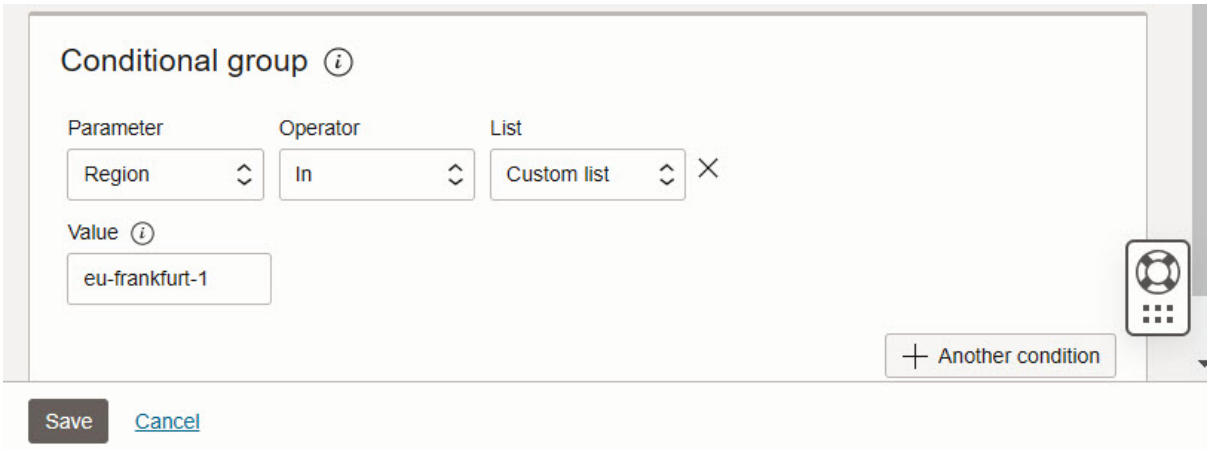


Figure 54: » step_6

Press *Save* at the bottom.

5.2.2.3 Verify Auto-Resolve by Creating a Public Bucket Repeat the steps from the previous lab to create a new bucket.

5.2.2.4 Create Bucket Add basic information and description. Call it *private_bucket*. Ensure you are in the correct compartment. If not, select your compartment in left side dropdown menu.

Copyright © 2024 Accenture. All rights reserved.

Go to Storage -> Object Storage & Archive Storage -> *Create Bucket*.

- Set Bucket Name to *private-bucket* and let other settings as per default.

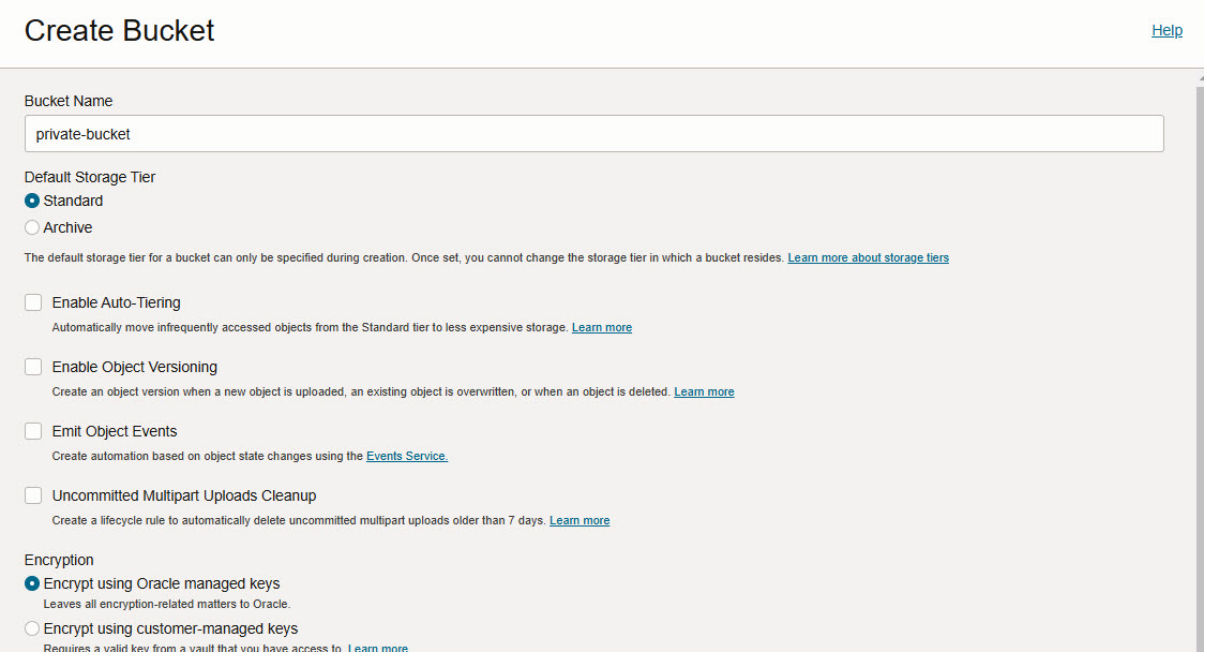


Figure 55: » step7

Press *Create* at the bottom.

5.2.2.5 Edit Visibility Edit created bucket from above by click on the three dots on bucket line -> Edit Visibility. Change it to public.

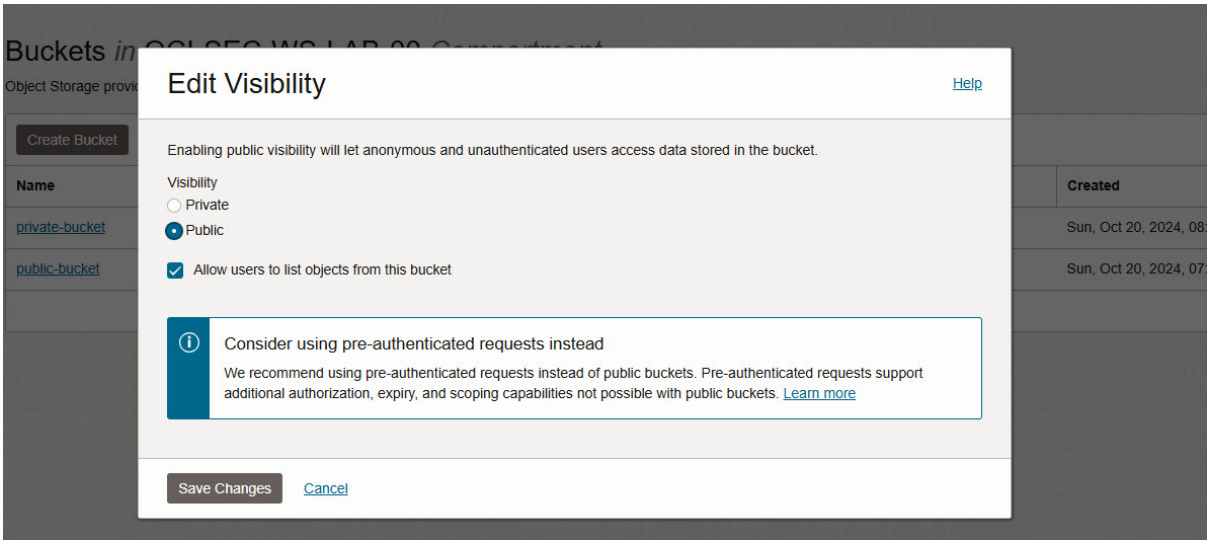


Figure 56: » step_8

Press *Save Changes* at the bottom.

Copyright © 2024 Accenture. All rights reserved.

5.2.2.6 Verification The bucket is set to public and marked by a yellow triangle.

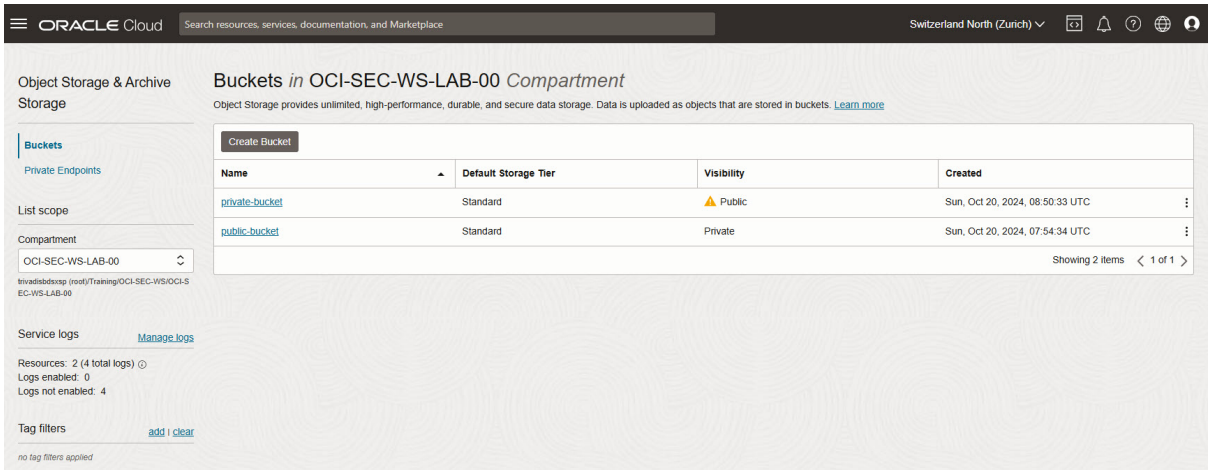


Figure 57: » step_9

5.2.2.7 Verify Auto Resolving After a couple of seconds, you can verify the Responder activity. There are two new entries to make the bucket private.

Identity & Security -> Cloud Guard -> Alerts -> Responder activity

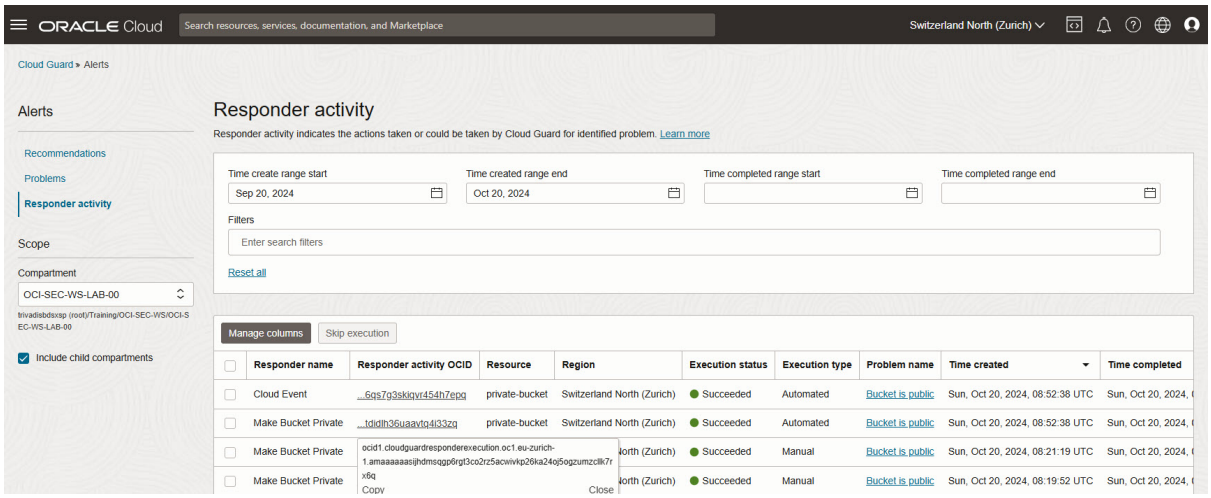


Figure 58: » step_10

5.2.2.8 Verification The visibility for your Object Storage bucket has automatically changed now to Private.

Storage -> Object Storage -> Buckets

Copyright © 2024 Accenture. All rights reserved.

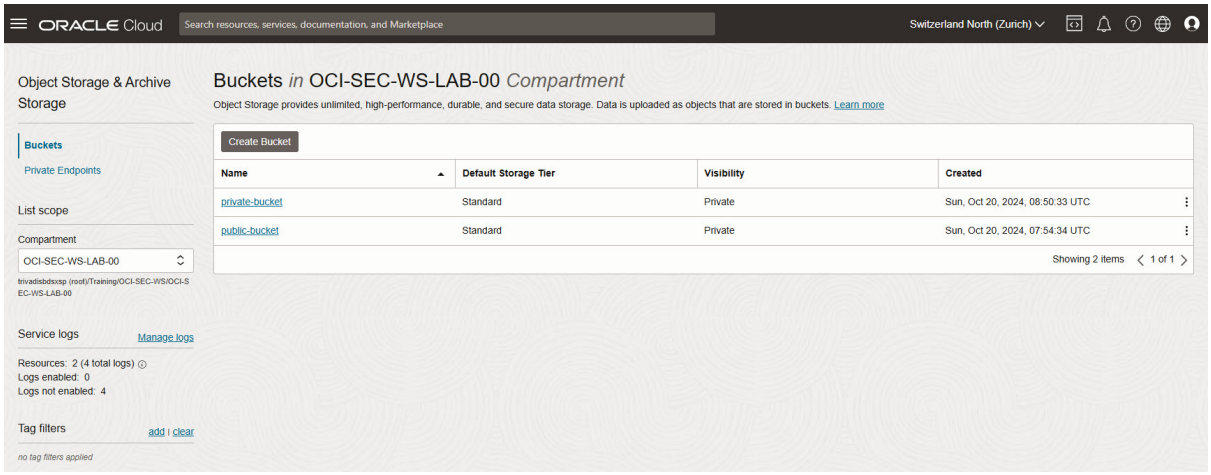


Figure 59: » step_11

Summary

In this exercise, you:

- Added a responder recipe to your Cloud Guard target.
- Enabled auto-remediation to handle public bucket visibility issues.
- Tested auto-remediation by creating a public bucket and verifying that Cloud Guard automatically set it to private.

You are now ready to continue with the next exercise, where you will configure Cloud Guard notifications for security alerts.

- **Previous Exercise:** Exercise 02: Manual Remediation
- **Next Exercise:** Exercise 04: Notification Setup

5.3 Exercise 04: Notification Setup

In this exercise, you will configure notifications in Cloud Guard to receive alerts about detected security issues. Using the existing detector settings, you'll set up notifications to be informed of any potential vulnerabilities or policy violations.

5.3.1 Objectives

- Create a notification topic and subscription.
- Set up a rule to trigger notifications.
- Test the notification by creating a public Object Storage bucket and verifying the alert.

Copyright © 2024 Accenture. All rights reserved.

Environment

Perform this exercise within the following environment:

- **Compartment:** `OCI-SEC-WS-LAB-nn`
- **Region:** Germany Central (Frankfurt)
- **OCI Console URL:** OCI Console Frankfurt - Login
- **OCI User:** *lab-oci-sec-ws**NN***
- **OCI Password:** *provided by trainer*

Ensure you are in the correct compartment and region. New resources, such as Cloud Shell configurations and ADB access settings, should be created within your designated compartment.

Solution

Login as User XYZ in OCI console. Ensure you have select the proper compartment in from the dropdown list on left side.

5.3.2 Enable Auto Resolve Notification by Topic

5.3.2.1 Create Topic, Subscription and Confirmation A topic and a subscription is required to enable the notification service based on events.

Developer Services -> Application Integration -> Notifications -> Create Topic

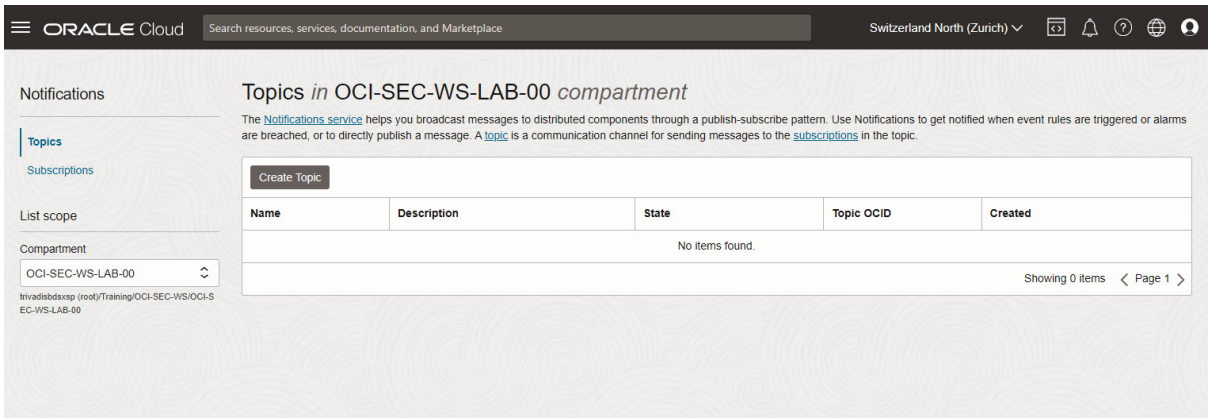


Figure 60: » step_1

Add details, *Create*.

Copyright © 2024 Accenture. All rights reserved.

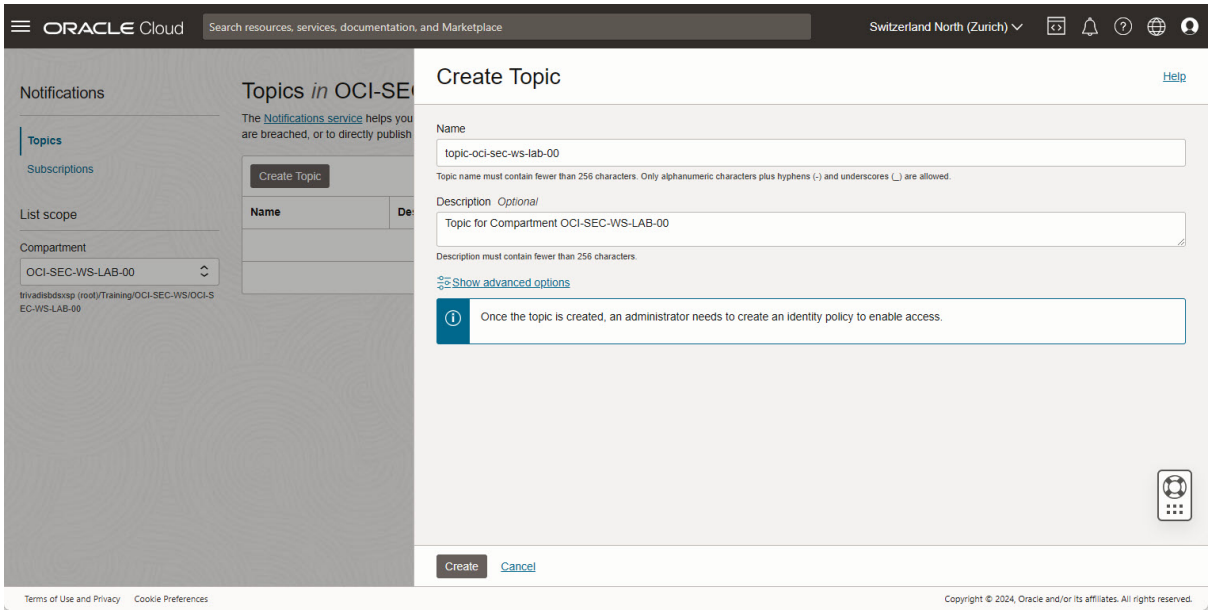


Figure 61: » step_2

The state of the new created topic is active.

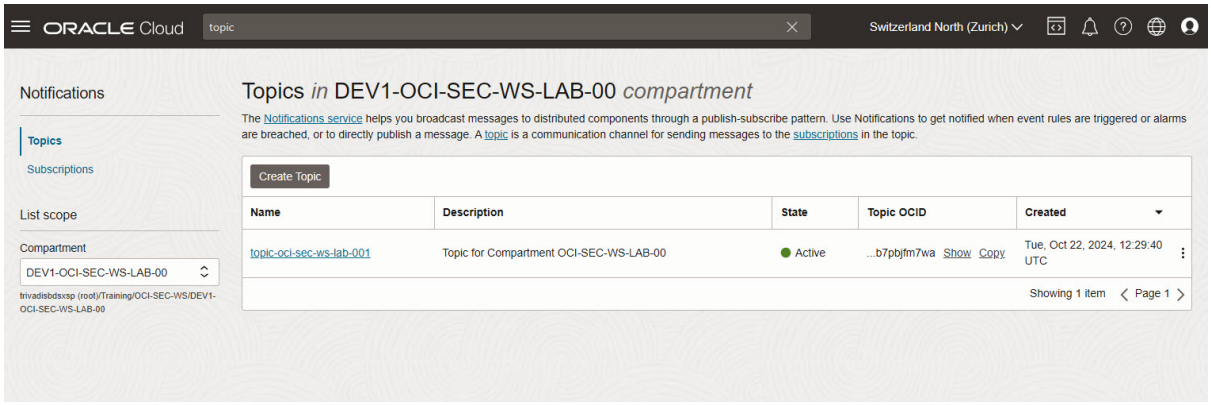


Figure 62: » step_3

View the details, click on topic name. Create a new Subscription: *Create Subscription*.

Copyright © 2024 Accenture. All rights reserved.

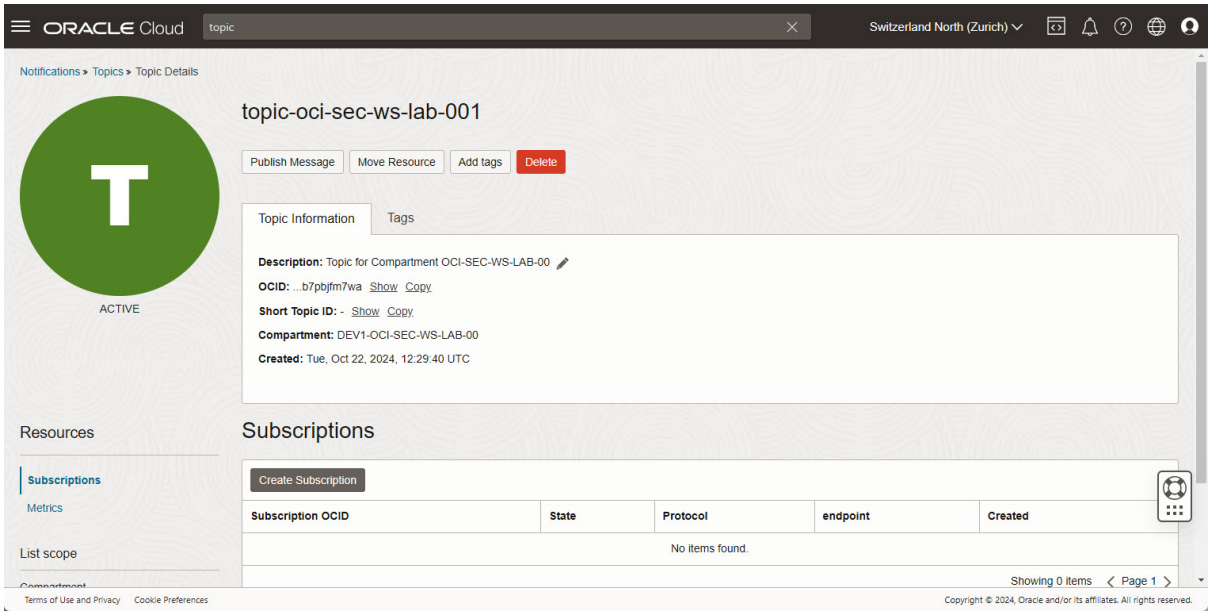


Figure 63: » step_4

Select:

- Protocol: Email
- Email: add your personal mail address, a mail address where you have immediate access for confirmation

Create the subscription and check your inbox.

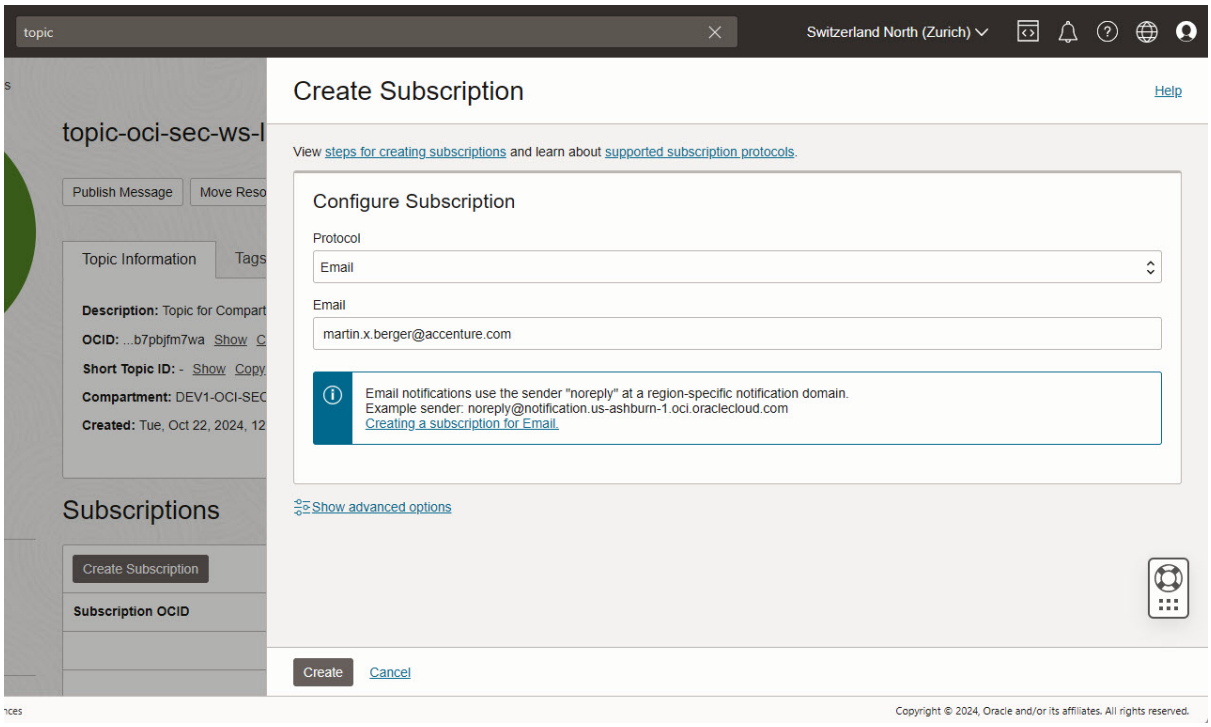


Figure 64: » step_5

Copyright © 2024 Accenture. All rights reserved.

Confirm the subscription

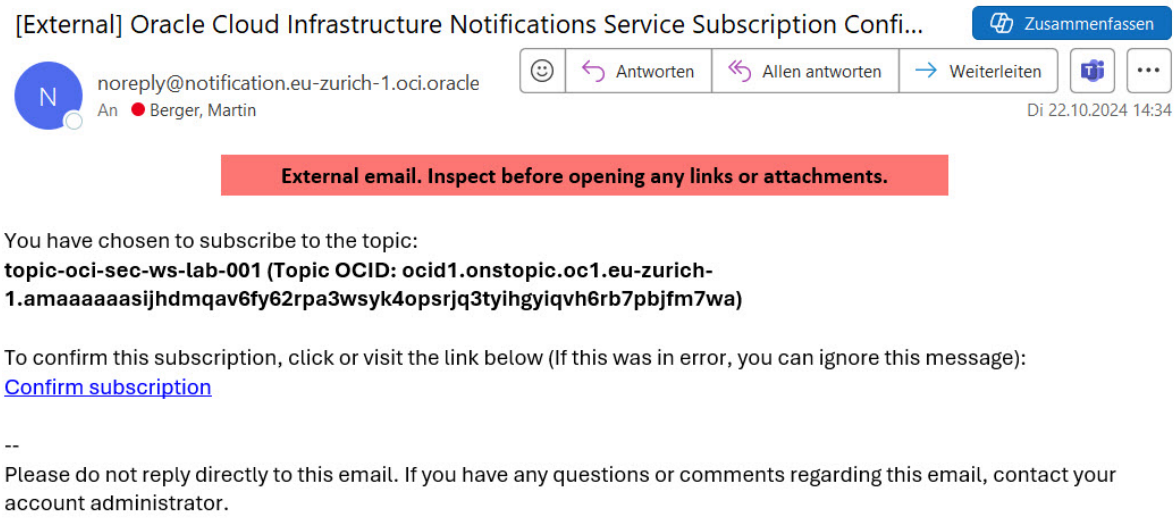


Figure 65: » step_6

Figure 66: » step_7

5.3.3 Create Rule

5.3.3.1 Create Topic, Subscription and Confirmation We create a rule based on Cloud Guard changes.

Observability & Management -> Events Service -> Rules -> *Create Rule*.

Set Display Name and Description, as example *rule-oci-sec-ws-lab-00-cloudguard*.

Copyright © 2024 Accenture. All rights reserved.

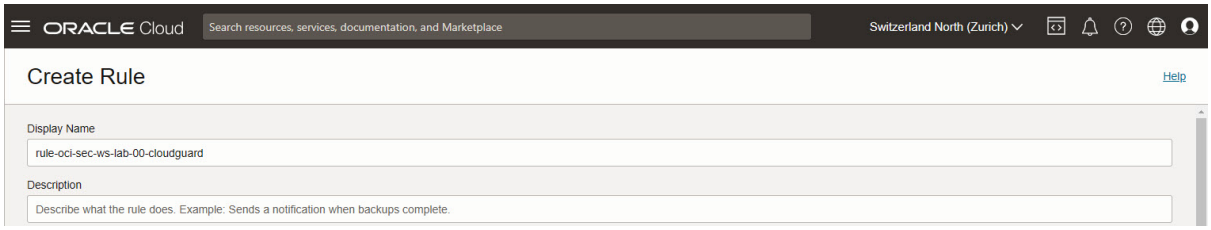


Figure 67: » step_1

Select Rule Condition.

In section *Rule Conditions*, select *Service Name* and *Event Type*. Select these event types:

- Detected - Problem
- Dismissed - Problem
- Remediated - Problem

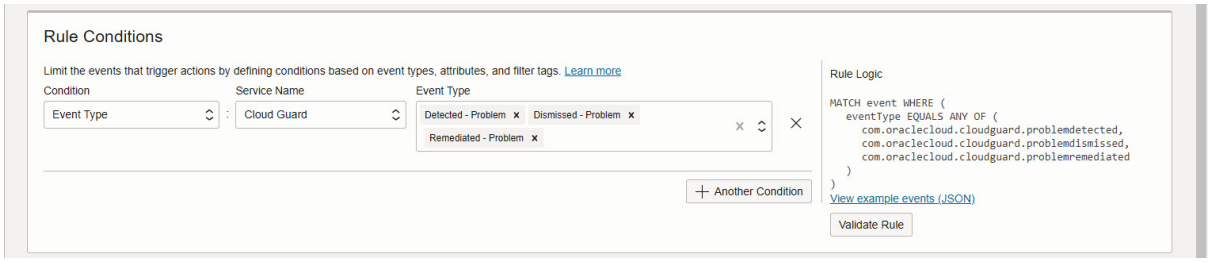


Figure 68: » step_2

Select Actions

- Action-Type: Notifications
- Notifications-Compartment: OCI-SEC-WS-LAB- (your compartment name)
- Topic: topic-oci-sec-ws-lab-001 (the topic you created)

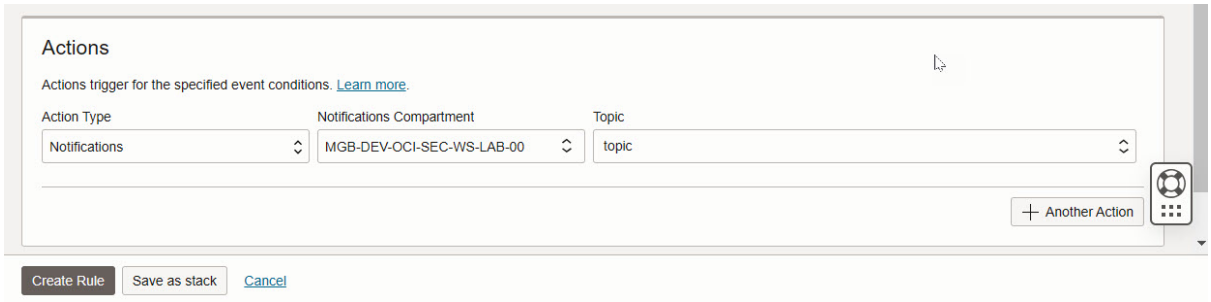


Figure 69: » step_3

5.3.4 Test

5.3.4.1 Change the visibility of an Object Storage bucket to public Storage -> Object Storage -> Buckets

Copyright © 2024 Accenture. All rights reserved.

Change the visibility and verify if you get a notification by mail.

Summary

In this exercise, you:

- Created a notification topic and subscription for Cloud Guard alerts.
- Configured a rule to send notifications based on specific detector findings.
- Verified the setup by creating a public bucket and receiving the corresponding alert.

You are now ready to continue with the next exercise to deepen your understanding of Data Safe configurations.

- **Previous Exercise:** Exercise 03: Auto Remediation
- **Next Exercise:** Exercise 05: Data Safe Configuration and Register ADB

Copyright © 2024 Accenture. All rights reserved.

6 Data Safe

6.1 Exercise 05: Configuration and Register ADB

In this exercise, you will set up Oracle Data Safe to enhance the security of an Autonomous Database (ADB). This process involves enabling monitoring and data protection features. You will first configure Oracle Data Safe and then register your ADB instance for secure management.

6.1.1 Objectives

- Set up Oracle Data Safe for your environment.
- Register an Autonomous Database (ADB) to integrate it with Data Safe.

Environment

Perform this exercise within the following environment:

- **Compartment:** `OCI-SEC-WS-LAB-nn`
- **Region:** Germany Central (Frankfurt)
- **OCI Console URL:** OCI Console Frankfurt - Login
- **OCI User:** *lab-oci-sec-ws**NN***
- **OCI Password:** *provided by trainer*

Ensure you are in the correct compartment and region. New resources, such as Cloud Shell configurations and ADB access settings, should be created within your designated compartment.

Solution

Log in to the OCI Console as User XYZ. Ensure you select the correct compartment from the dropdown menu on the left side.

Navigate to: **Oracle Database -> Data Safe -> Database Security -> Overview**

1. Navigate to the *Autonomous Database* registration wizard within the Data Safe section.

Copyright © 2024 Accenture. All rights reserved.

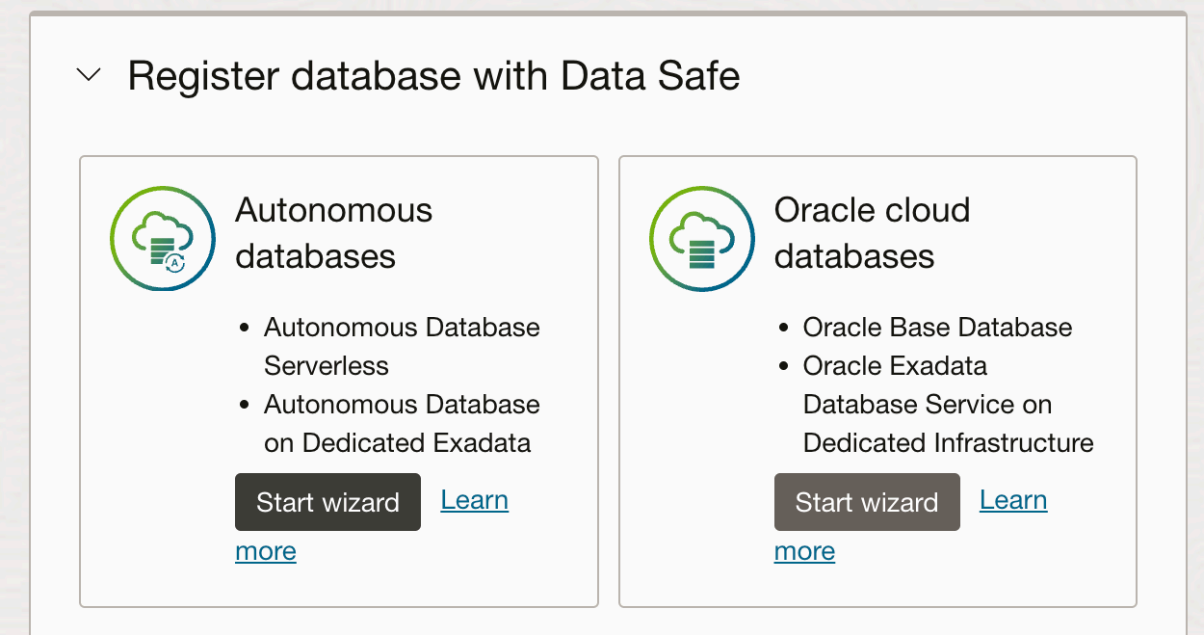


Figure 70: » step_1

2. Select the *Autonomous Database* in your designated compartment, for example, *SOE-DEV-OCI-SEC-WS-LAB-00*.

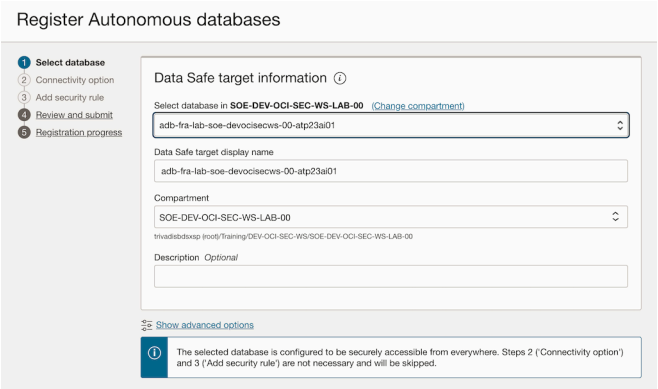


Figure 71: » step_2

3. Click **Next** to proceed and finalize the registration process.

Figure 72: » step_3

4. The registration process for the *Autonomous Database* may take some time.

Copyright © 2024 Accenture. All rights reserved.

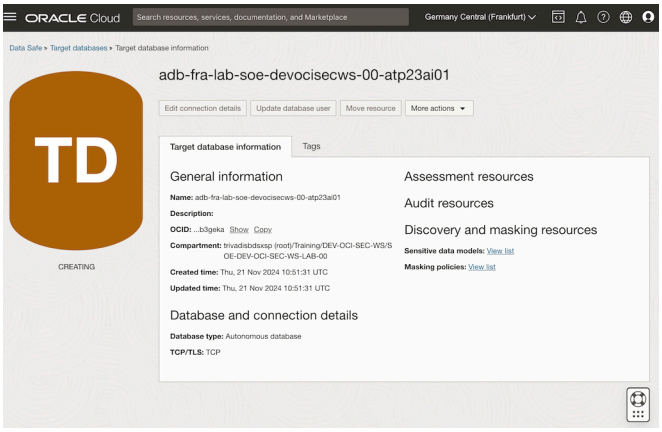


Figure 73: » step_4

5. Once the *Autonomous Database* is registered, it will appear in the Data Safe dashboard.

   Navigate to: **Oracle Database -> Data Safe -> Database Security -> Dashboard**

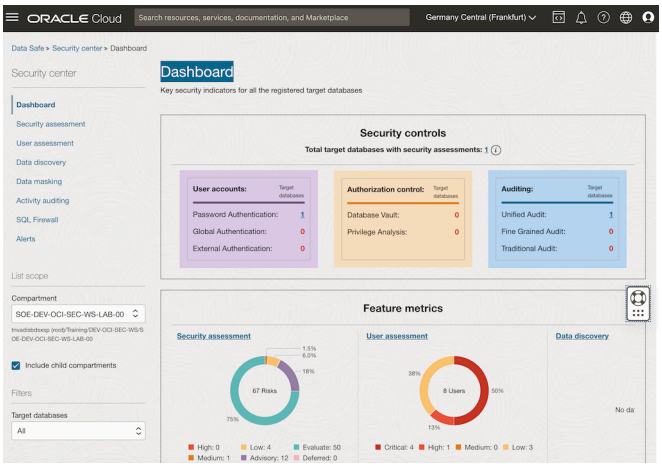


Figure 74: » step_5

Summary

In this exercise, you:

- Configured Oracle Data Safe to enable advanced security features for database monitoring and protection.
- Successfully registered an Autonomous Database (ADB) with Data Safe for secure management.

You are now ready to continue with the next exercise, where you will explore how to assess database configurations for compliance and best practices.

- **Previous Exercise:** Exercise 04: Notification Setup
- **Next Exercise:** Exercise 06: Assess Database Configurations

Copyright © 2024 Accenture. All rights reserved.

6.2 Exercise 06: Assess Database Configurations

In this exercise, you will use Oracle Data Safe to perform a configuration assessment on your Autonomous Database (ADB). This assessment checks the database settings for compliance with security best practices, helping to identify potential vulnerabilities and areas for improvement.

6.2.1 Objectives

- Run a configuration assessment using Oracle Data Safe.
- Identify security risks and areas for improvement based on database settings.

Environment

Perform this exercise within the following environment:

- **Compartment:** `OCI-SEC-WS-LAB-nn`
- **Region:** Germany Central (Frankfurt)
- **OCI Console URL:** OCI Console Frankfurt - Login
- **OCI User:** *lab-oci-sec-ws**NN***
- **OCI Password:** *provided by trainer*

Ensure you are in the correct compartment and region. New resources, such as Cloud Shell configurations and ADB access settings, should be created within your designated compartment.

Solution

6.2.2 Step 1: Explore Security Assessment

1. Navigate to the **Oracle Data Safe Dashboard** in the OCI Console.
    - Go to **Data Safe** -> **Security Assessments**.
2. View the overview of the Security Assessment for your Autonomous Database (ADB).
    - Select the target ADB you registered in the previous exercises.
    - Explore the summary metrics such as:
        - Total findings (e.g., high, medium, low risks).
        - Configuration compliance score.

Copyright © 2024 Accenture. All rights reserved.

Figure 75: » step_1

3. Go to the tab **Target summary** and click on the latest assessment report for the ADB to review the detailed findings.
    - Observe categories such as **Privileges and roles**, **Database configuration**, and **Auditing**.
    - Note any highlighted risks or warnings in the findings.

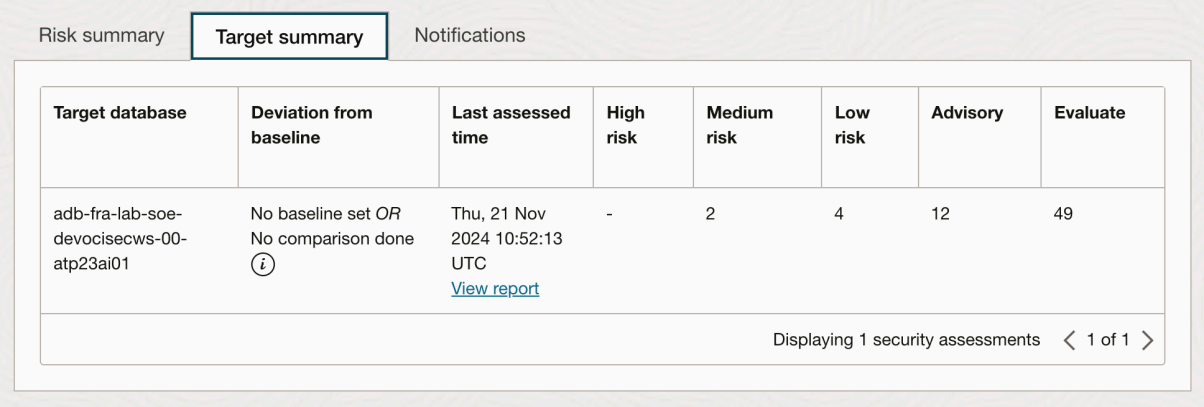


Figure 76: Target summary

Copyright © 2024 Accenture. All rights reserved.

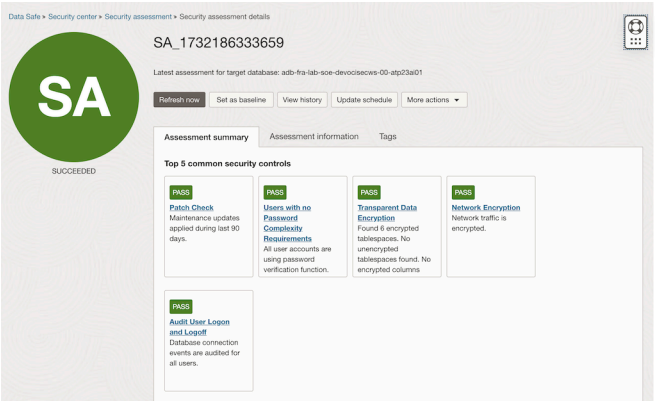


Figure 77: Security Assessment Details

6.2.3 Step 2: Adjust the Risk Level of a Risk Finding

1. From the **Security Assessment Report**, identify a **risk finding** that you want to adjust.
    - For example: *Users with Grant Option*
2. Click on the finding to view its details.
    - Note the current **risk level** (e.g., high, medium, or low).

Figure 78: Security Assessment Details

3. Adjust the **risk level**:
    - Click on **Edit Risk** or **Adjust Risk Level**.
    - Select a new risk level (e.g., from “Low” to “Medium”) and provide a justification for the change (e.g., “Compliance Requirement”).

Copyright © 2024 Accenture. All rights reserved.

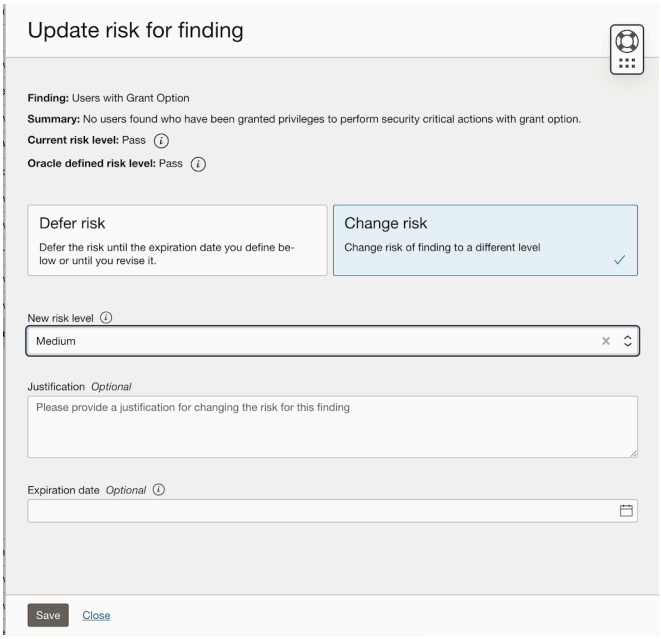


Figure 79: Adjust Risk Level for Users with Grant Option

4. Save the changes.

6.2.4 Step 3: Set Baseline

1. Go back to the top of the page of the latest assessment report for the ADB.

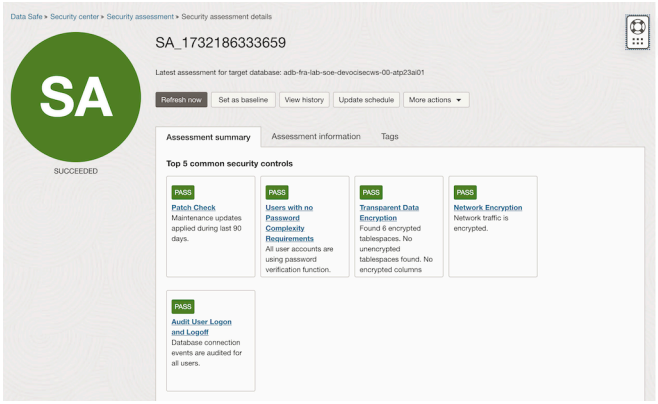


Figure 80: Security Assessment Details

2. Click on **Set Baseline**:
    - The baseline captures the current configuration and security settings as a reference point.
3. Confirm the baseline creation.
    - This baseline will be used for future comparisons to identify any deviations.

Copyright © 2024 Accenture. All rights reserved.

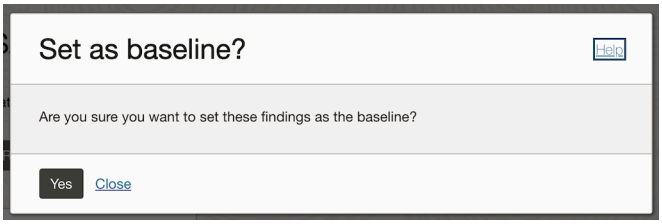


Figure 81: Set Security Assessment Baseline

6.2.5 Step 4: Create a Risk on the Target Database

1. Simulate a security risk by modifying a configuration on the target ADB.
2. Access the SQL worksheet in Database Actions. If your session has expired, sign in again as the ADMIN user.
3. If needed, clear the worksheet and the Script Output tab.
4. On the worksheet, enter the following command:

```
GRANT alter any role TO public;
CREATE USER scott IDENTIFIED BY NO AUTHENTICATION;
```

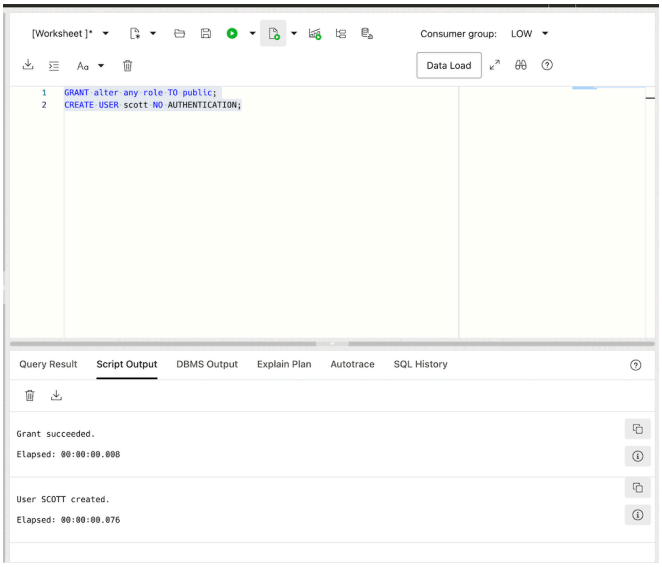


Figure 82: Create a Risk using SQL worksheet

6.2.6 Step 5: Refresh the Latest Security Assessment and Analyze the Results

1. Navigate back the top of the page of the latest assessment report for the ADB.
2. Click **Refresh Assessment**:
   - Wait for the assessment to complete.
   - The new assessment should reflect the risk you introduced in Step 4.

Copyright © 2024 Accenture. All rights reserved.

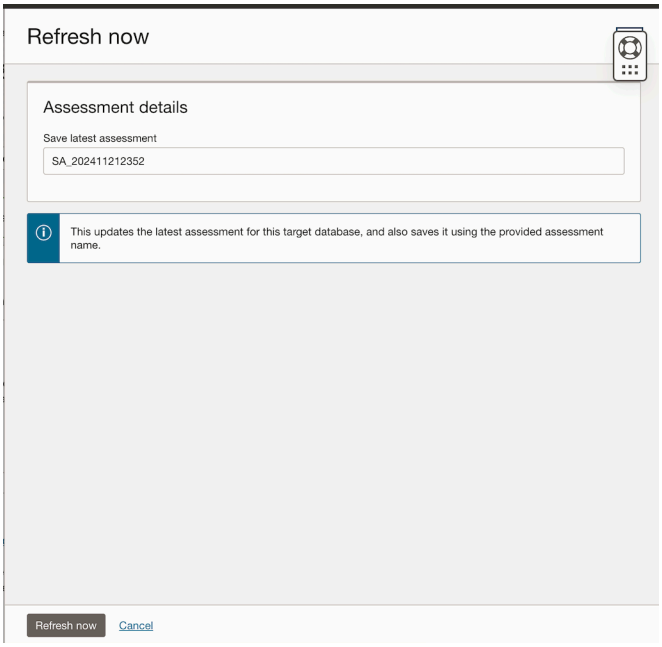


Figure 83: Refresh Security Assessment

3. Analyze the updated assessment report:
    - Look for the new risk findings created by your changes.
    - Review the affected areas and recommendations provided by Data Safe.

6.2.7 Step 6: Compare Your Assessment with the Baseline

1. From the Security Assessments page, select the **Baseline Comparison** option.
2. Compare the latest assessment results with the previously set baseline.
    - Identify any deviations or new risks.
    - Note changes such as:
        - Configuration setting differences.
        - Additional risk findings introduced in Step 4.
3. Document the results of the comparison:
    - Highlight any areas of concern that should be addressed.
    - Reset the baseline if the new state is acceptable and reflects the desired configuration.

Summary

In this exercise, you:

- Performed a configuration assessment with Oracle Data Safe to evaluate database settings.

Copyright © 2024 Accenture. All rights reserved.

- Identified potential vulnerabilities and areas to enhance security compliance.

You are now ready to continue with the next exercise, where you will assess database users to further strengthen your security posture.

- **Previous Exercise:** Exercise 05: Data Safe Configuration and Register ADB
- **Next Exercise:** Exercise 07: Assess Database Users

6.3 Exercise 07: Assess Database Users

In this exercise, you will use Oracle Data Safe to assess user accounts within your Autonomous Database (ADB). This assessment helps identify user roles, privileges, and potential security risks associated with database users, allowing for better security management and compliance.

6.3.1 Objectives

- Use Oracle Data Safe to assess and analyze database user accounts.
- Identify roles, privileges, and any potential security risks related to database users.

Environment

Perform this exercise within the following environment:

- **Compartment:** `OCI-SEC-WS-LAB-nn`
- **Region:** Germany Central (Frankfurt)
- **OCI Console URL:** OCI Console Frankfurt - Login
- **OCI User:** *lab-oci-sec-ws**NN***
- **OCI Password:** *provided by trainer*

Ensure you are in the correct compartment and region. New resources, such as Cloud Shell configurations and ADB access settings, should be created within your designated compartment.

Solution

6.3.2 Step 1: View the Overview Page for User Assessment

1. Navigate to the **Data Safe Dashboard** in the OCI Console.
    - Go to **Data Safe** **User Assessments**.
2. Select your target Autonomous Database (ADB).
3. View the **User Assessment Overview Page**:

Copyright © 2024 Accenture. All rights reserved.

- Review key metrics, including:
  - Total users.
  - Risk level distribution (e.g., High, Medium, Low).
  - User categories (e.g., Admin Users, Privileged Users).

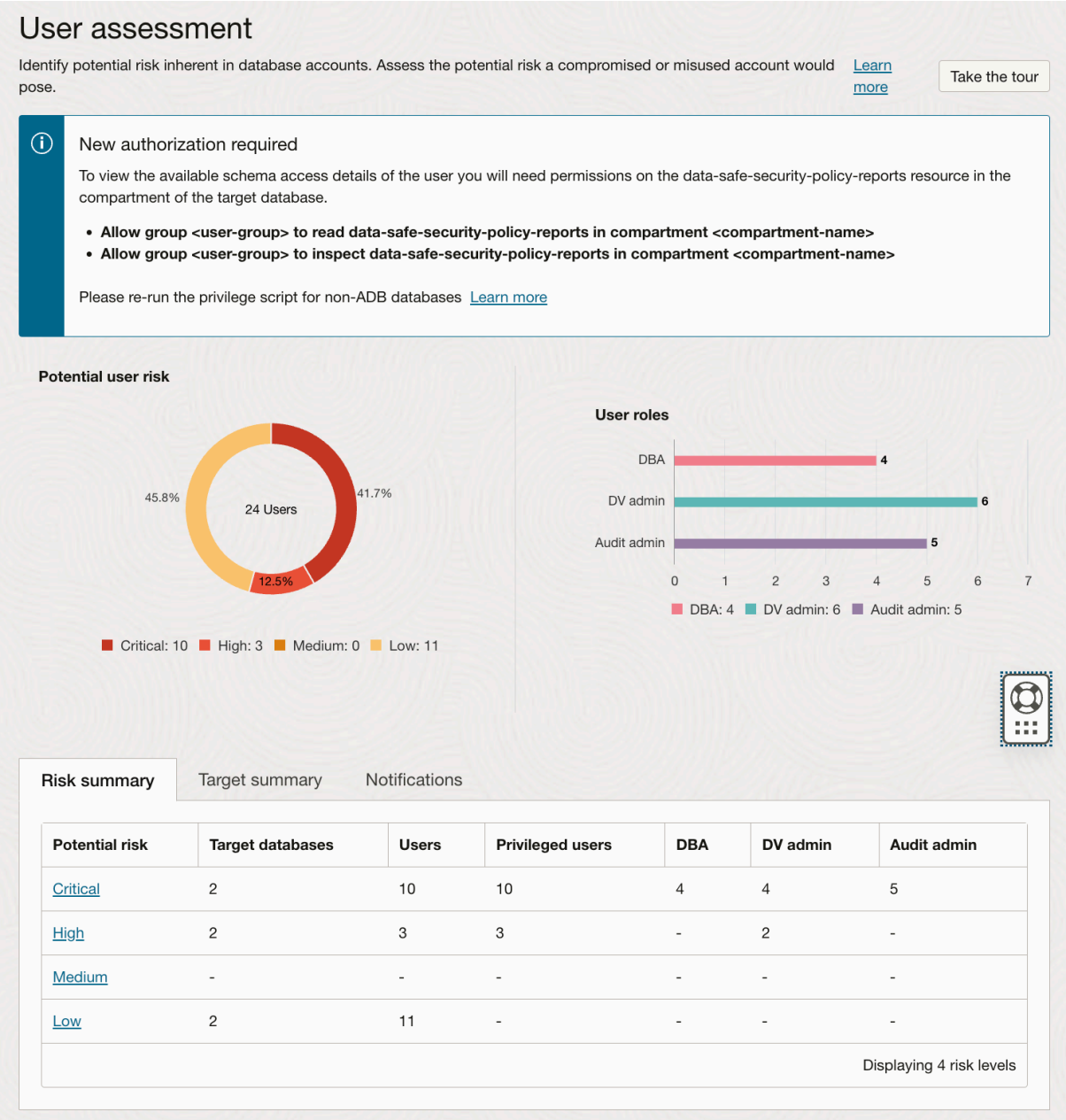


Figure 84: User Assessment

4. Note the summary of potential security risks related to user accounts.

6.3.3 Step 2: Analyze Users in the Latest User Assessment

1. Open the latest **User Assessment Report** for your target ADB.

Copyright © 2024 Accenture. All rights reserved.

2. Review the list of users and their associated risk levels:

    - Focus on users flagged with **High Risk** or **Medium Risk**.

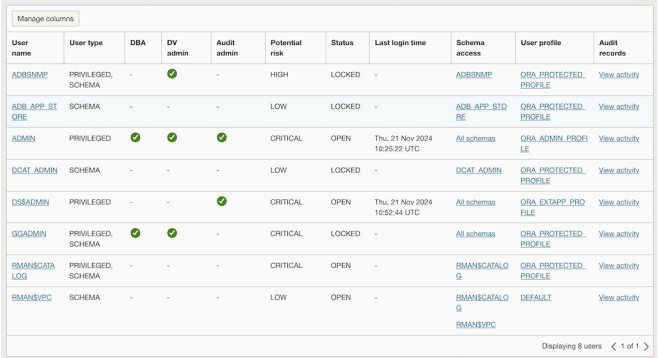


Figure 85: User Assessment Details

3. For each flagged user, analyze the following details:

    - **Privileges**: Review the specific roles and grants assigned to the user.
    - **Login Activity**: Check the last login time and ensure it aligns with expected usage.
    - **Account Status**: Identify users with default passwords, expired passwords, or locked accounts.

6.3.4 Step 3: Change Users and Entitlements on the Target Database

Either modify your target database via SQL worksheet, Cloud Shell or both.

1. Download and install HR sample schema using cloud shell

    - Download the Sample Schemas

```
cd $HOME
export TNS_ADMIN=$HOME/my_wallet
git clone https://github.com/oracle/db-sample-schemas.git
```

    - Set environment variable to connect to the ADB

```
export TNS_ADMIN=$HOME/my_wallet
export ADB_SERVICE=$(grep -o '^[^ ]*tpurgent' $HOME/my_wallet/tnsnames
    .ora)
```

    - Install **human_resources** demo Schema use the default LAB password

```
cd $HOME/db-sample-schemas/human_resources
sql admin@$ADB_SERVICE @hr_install.sql
```

2. Access your target database using a SQL worksheet and modify user accounts or privileges to simulate a change:

Copyright © 2024 Accenture. All rights reserved.

- Example 1: Grant an additional role to a user:

```
GRANT select any table TO hr;
```

- Example 2: Unlock a user account:

```
ALTER USER hr ACCOUNT UNLOCK;
```

- Example 3: Create a new test user with

```
CREATE USER test_user NO AUTHENTICATION;
GRANT CREATE SESSION TO test_user;
```

6.3.5 Step 4: Refresh the Latest User Assessment

1. Navigate back to **User Assessments** in the Data Safe Dashboard.
2. Click **Refresh Assessment** for your target database.
    - Wait for the refresh to complete.

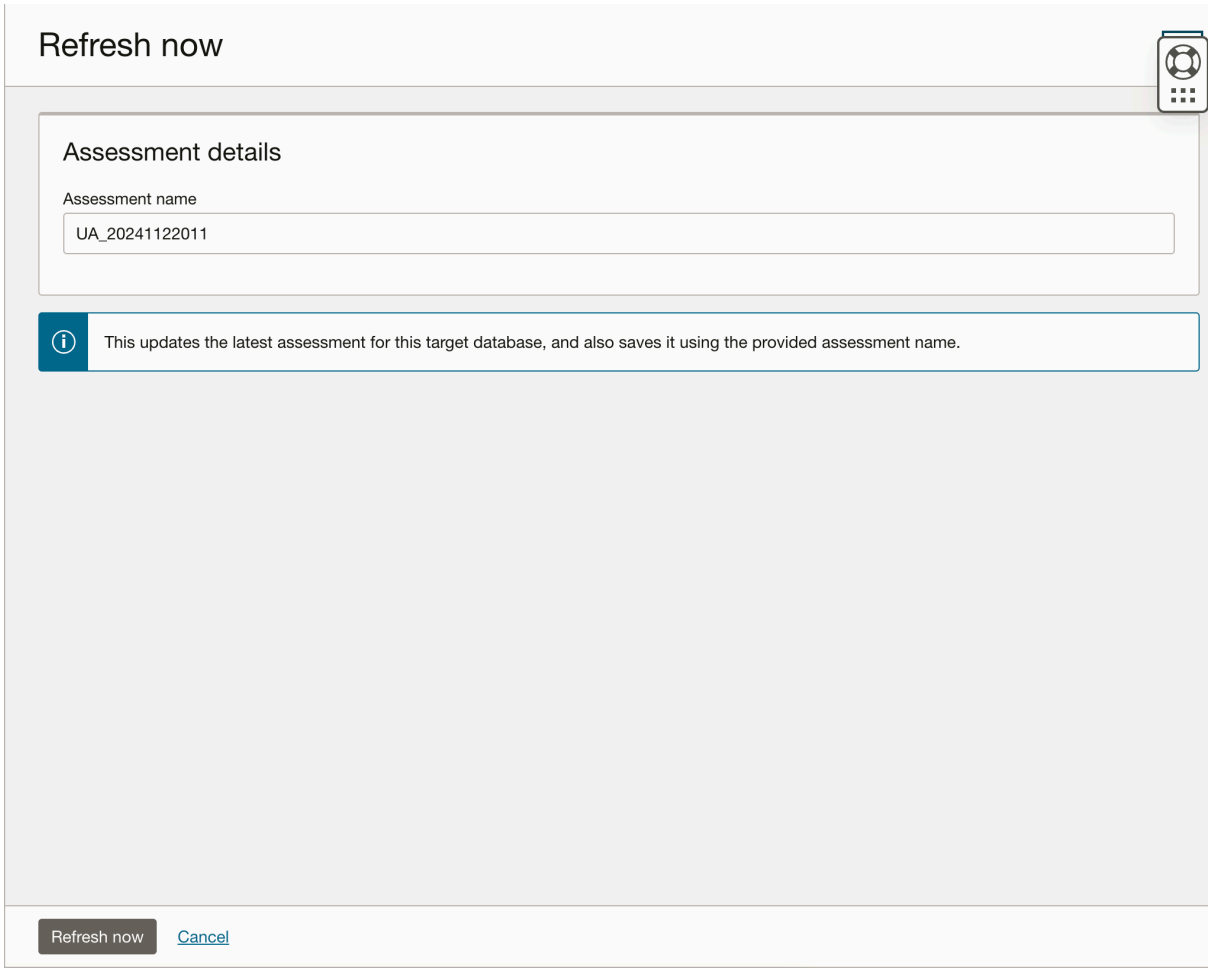


Figure 86: Refresh User Assessment

Copyright © 2024 Accenture. All rights reserved.

3. Review the updated User Assessment Report:
    - Ensure the changes made in Step 3 are reflected.
    - Check for any new findings or risks introduced by the changes.

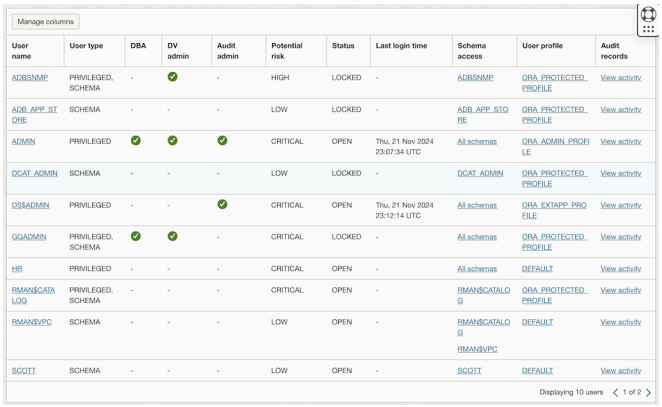


Figure 87: Review User Assessment Details

6.3.6 Step 5: Compare the Latest User Assessment with the Initial User Assessment

1. From the User Assessments page, select the **Comparison assessments** option.

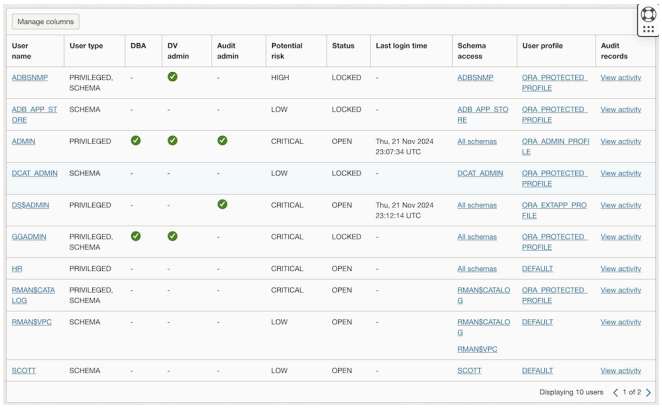


Figure 88: Compare User Assessment

2. Compare the latest assessment with the initial assessment:
    - Identify differences in:
        - New users added.
        - Changes in user privileges or roles.
        - Updated risk levels for existing users.
3. Document the comparison results:
    - Highlight any deviations or additional risks introduced by the changes.
    - Evaluate whether corrective actions are needed to mitigate risks.

Copyright © 2024 Accenture. All rights reserved.

Summary

In this exercise, you:

- Explored the User Assessment overview to review key metrics and user risk distributions.
- Analyzed the users and privileges in the latest user assessment report.
- Simulated changes to users and entitlements on the target database.
- Refreshed the user assessment to capture updates and identify new risks.
- Compared the latest user assessment with the initial assessment to evaluate deviations and ensure compliance.

You are now ready to continue with the next exercise, where you will learn how to audit database activity to enhance monitoring and security.

- **Previous Exercise:** Exercise 06: Assess Database Configurations
- **Next Exercise:** Exercise 08: Audit Database Activity

6.4 Exercise 08: Audit Database Activity

In this exercise, you will use Oracle Data Safe to audit database activity in your Autonomous Database (ADB). Auditing helps monitor actions performed within the database, providing insights into user activity and helping detect any suspicious or unauthorized actions.

6.4.1 Objectives

- Enable and configure auditing in Oracle Data Safe.
- Review and analyze database activity logs to monitor user actions.

Environment

Perform this exercise within the following environment:

- **Compartment:** `OCI-SEC-WS-LAB-nn`
- **Region:** Germany Central (Frankfurt)
- **OCI Console URL:** OCI Console Frankfurt - Login
- **OCI User:** *lab-oci-sec-ws**NN***
- **OCI Password:** *provided by trainer*

Ensure you are in the correct compartment and region. New resources, such as Cloud Shell configurations and ADB access settings, should be created within your designated compartment.

Copyright © 2024 Accenture. All rights reserved.

Solution

6.4.2 Step 1: Enable and Configure Auditing in Oracle Data Safe

1. **Access the Data Safe Dashboard**:
    - Navigate to **Data Safe** **Audit** in the OCI Console.
2. **Enable Auditing for the Target Database**:
    - Select the target Autonomous Database (ADB) from the list.
    - If auditing is not already enabled, follow these steps:
        - Click **Enable Auditing**.
        - Confirm that audit data collection is enabled for the selected database.
3. **Configure Audit Policies**:
    - Go to the **Audit Policies** tab in the Data Safe interface.
    - Enable specific audit policies for your ADB:
        - **Login/Logout Events**: Tracks user sessions.
        - **Privilege Usage**: Captures the use of system or object privileges.
        - **Data Manipulation (DML)**: Logs INSERT, UPDATE, and DELETE operations.
        - **Schema Changes**: Monitors CREATE, DROP, and ALTER statements.
4. **Save the Configuration**:
    - Ensure that the appropriate audit policies are applied to the database for logging key activities.

6.4.3 Step 2: Review and Analyze Database Activity Logs

1. **Access the Audit Reports**:
    - Navigate to **Data Safe** **Audit Reports**.
2. **Filter Logs by Criteria**:
    - Use the filters to view specific activities, such as:
        - **Time Period**: Specify a date and time range for recent activities.
        - **Users**: Focus on actions performed by specific users.
        - **Events**: Filter for particular event types, such as failed logins or schema changes.
3. **Analyze Audit Logs**:
    - Review details of the audit logs, including:
        - **Event Type**: Type of action performed (e.g., login, DML operations).
        - **User**: Who performed the action.
        - **Timestamp**: When the action occurred.

Copyright © 2024 Accenture. All rights reserved.

    - **Object Affected**: Database objects involved in the operation.

4. **Identify Suspicious Activities**:
    - Look for anomalies or risks, such as:
        - Unusual login attempts from unexpected IP addresses.
        - Privilege escalation events.
        - Unauthorized schema changes.

5. **Generate an Audit Report**:
    - Create a custom audit report for your findings:
        - Select specific events and users.
        - Export the report in PDF or CSV format for further analysis.

Summary

In this exercise, you:

- Enabled and configured auditing for your Autonomous Database in Oracle Data Safe.
- Applied audit policies to track key database activities, such as logins, privilege usage, and schema changes.
- Reviewed and analyzed database activity logs to monitor user actions and identify potential security risks.

You are now ready to proceed to the next exercise, where you will explore additional Oracle Data Safe features, such as generating alerts and notifications.

- **Previous Exercise:** Exercise 07: Assess Database Users
- **Next Exercise:** Exercise 09: Generate Alerts

6.5 Exercise 09: Generate Alerts

In this exercise, you will configure Oracle Data Safe to generate alerts for specific activities or events within your Autonomous Database (ADB). Setting up alerts helps you stay informed about critical actions, security incidents, and potential threats in real-time.

6.5.1 Objectives

- Configure alert settings in Oracle Data Safe.
- Set up rules to trigger alerts for specific database events.
- Test the alerting mechanism to ensure notifications are received for relevant actions.

Copyright © 2024 Accenture. All rights reserved.

Environment

Perform this exercise within the following environment:

- **Compartment:** `OCI-SEC-WS-LAB-nn`
- **Region:** Germany Central (Frankfurt)
- **OCI Console URL:** OCI Console Frankfurt - Login
- **OCI User:** *lab-oci-sec-ws**NN***
- **OCI Password:** *provided by trainer*

Ensure you are in the correct compartment and region. New resources, such as Cloud Shell configurations and ADB access settings, should be created within your designated compartment.

Solution

6.5.2 Step 1: Configure Alert Settings in Oracle Data Safe

1. **Access the Data Safe Dashboard**:
   - Navigate to **Data Safe** **Alerts** in the OCI Console.
2. **Enable Alerts for the Target Database**:
   - Select the target Autonomous Database (ADB) from the list.
   - If alerts are not already enabled, click **Enable Alerts** to activate the alerting mechanism for the database.
3. **Define Notification Settings**:
   - Navigate to the **Notification Settings** section.
   - Add or confirm the notification endpoint (e.g., email address or OCI Notification Service topic) where alerts will be sent.
   - Save your changes.

6.5.3 Step 2: Set Up Rules to Trigger Alerts for Specific Database Events

1. **Go to Alert Rules**:
   - In the **Alerts** section, navigate to the **Rules** tab.
2. **Create a New Alert Rule**:
   - Click **Create Rule** to define a custom alert.
   - Specify the following:
     - **Event Type**: Select the type of event to monitor, such as:
       * Failed logins.

Copyright © 2024 Accenture. All rights reserved.

        * Schema changes.
        * Privilege escalations.
    - **Severity Level**: Assign a severity (e.g., High, Medium, Low) for the alert.
    - **Description**: Provide a brief description of the rule for context.

3. **Save the Rule**:
    - Ensure the rule is active and associated with the target ADB.

6.5.4 Step 3: Test the Alerting Mechanism

1. **Simulate a Database Event**:
    - Perform an action on the target database that should trigger the alert.
        - Example 1: Attempt a failed login using an invalid user/password combination:

```
sqlplus invalid_user/invalid_password@your_database_alias
```

        - Example 2: Make a schema change such as creating a new table:

```
CREATE TABLE test_table (id NUMBER);
```

2. **Monitor for Alerts**:
    - Check the **Alert Logs** in the Data Safe Dashboard to ensure the event was captured.
    - Confirm that the alert was triggered based on your defined rule.
3. **Verify Notification Delivery**:
    - Check your email inbox or the notification endpoint for the alert message.
    - The notification should include details about the event, such as:
        - **Event Type**: Type of action that triggered the alert.
        - **Timestamp**: When the event occurred.
        - **Target Database**: The affected database.
4. **Troubleshoot if Necessary**:
    - If no alert or notification is received:
        - Verify that the rule is active and correctly configured.
        - Check the notification endpoint for proper setup.

Summary

In this exercise, you:

- Configured alert settings in Oracle Data Safe to monitor key database events.

Copyright © 2024 Accenture. All rights reserved.

- Defined custom alert rules to trigger notifications for specific actions, such as failed logins or schema changes.
- Tested the alerting mechanism by simulating database events and verifying notification delivery.

You are now ready to proceed to the next exercise, where you will explore data discovery and masking features in Oracle Data Safe.

- **Previous Exercise:** Exercise 08: Audit Database Activity
- **Next Exercise:** Exercise 10: Discover Sensitive Data

6.6 Exercise 10: Discover Sensitive Data

In this exercise, you will use Oracle Data Safe to identify and classify sensitive data within your Autonomous Database (ADB). This process helps ensure data privacy and compliance by discovering personally identifiable information (PII) and other sensitive data types.

6.6.1 Objectives

- Run a data discovery scan in Oracle Data Safe to locate sensitive data.
- Review the results to understand the types and locations of sensitive data within the database.

Environment

Perform this exercise within the following environment:

- **Compartment:** `OCI-SEC-WS-LAB-nn`
- **Region:** Germany Central (Frankfurt)
- **OCI Console URL:** OCI Console Frankfurt - Login
- **OCI User:** *lab-oci-sec-ws**NN***
- **OCI Password:** *provided by trainer*

Ensure you are in the correct compartment and region. New resources, such as Cloud Shell configurations and ADB access settings, should be created within your designated compartment.

Solution

6.6.2 Step 1: Run a Data Discovery Scan in Oracle Data Safe

1. **Access the Data Safe Dashboard**:

Copyright © 2024 Accenture. All rights reserved.

- Navigate to **Data Safe** **Data Discovery** in the OCI Console.

2. **Create a New Data Discovery Job**:
   - Click **Create Data Discovery Job** to initiate a new scan.
   - Select the target database (your registered ADB) from the list.
3. **Configure the Discovery Scan**:
   - Provide a meaningful name for the job, such as `Sensitive_Data_Discovery_Job`.
   - Select the scope of the scan:
     - **Schemas**: Choose specific schemas or scan all schemas.
     - **Columns**: Specify columns or allow automatic detection based on sensitive data models.
   - Enable **Include Predefined Sensitive Types** to use built-in data classifications (e.g., credit card numbers, social security numbers).
4. **Start the Scan**:
   - Review the job configuration and click **Start**.
   - Monitor the progress of the scan on the **Job Details** page.

6.6.3 Step 2: Review the Results

1. **Access the Completed Scan Report**:
   - Once the scan is complete, go to **Data Discovery** **Job Results**.
   - Select the completed job to view its details.
2. **Analyze the Sensitive Data Findings**:
   - Review the categorized results, such as:
     - **Sensitive Data Types**: Identify the types of sensitive data detected (e.g., Personally Identifiable Information, Financial Data).
     - **Locations**: View the schemas, tables, and columns where sensitive data is located.
3. **Understand the Risk Levels**:
   - Each finding is assigned a **Risk Level** (e.g., High, Medium, Low) based on the sensitivity and exposure of the data.
   - Focus on high-risk findings for immediate action.
4. **Export the Report** (Optional):
   - If required, export the discovery scan results in **PDF** or **CSV** format for further review or compliance reporting.

Copyright © 2024 Accenture. All rights reserved.

6.6.4 Optional: Plan for Data Protection

1. **Evaluate Data Masking**:
    - Based on the discovery results, consider applying **data masking** to protect sensitive data in non-production environments.
2. **Review User Access**:
    - Cross-reference sensitive data locations with user privileges to ensure only authorized users can access high-risk data.

Summary

In this exercise, you:

- Ran a data discovery scan in Oracle Data Safe to locate sensitive data in your Autonomous Database.
- Reviewed the results to identify sensitive data types and their locations within the database.
- Analyzed risk levels associated with sensitive data to understand potential vulnerabilities.

You are now ready to proceed to the next exercise, where you will explore additional data protection features, such as masking sensitive data.

- **Previous Exercise:** Exercise 09: Generate Alerts
- **Next Exercise:** Exercise 11: SQL Firewall

6.7 Exercise 11: SQL Firewall

In this exercise, you will configure the SQL Firewall in Oracle Data Safe to control and monitor SQL queries executed in your Autonomous Database (ADB). This feature helps enhance database security by defining rules that restrict unauthorized or potentially harmful SQL statements.

6.7.1 Objectives

- Set up the SQL Firewall in Oracle Data Safe.
- Define rules to allow or block specific SQL statements.
- Test the SQL Firewall by executing queries to verify that the rules are enforced.

Copyright © 2024 Accenture. All rights reserved.

Environment

Perform this exercise within the following environment:

- **Compartment:** `OCI-SEC-WS-LAB-nn`
- **Region:** Germany Central (Frankfurt)
- **OCI Console URL:** OCI Console Frankfurt - Login
- **OCI User:** *lab-oci-sec-ws**NN***
- **OCI Password:** *provided by trainer*

Ensure you are in the correct compartment and region. New resources, such as Cloud Shell configurations and ADB access settings, should be created within your designated compartment.

Solution

6.7.2 Step 1: Set Up the SQL Firewall in Oracle Data Safe

1. **Access the Data Safe Dashboard**:
    - Navigate to **Data Safe** **SQL Firewall** in the OCI Console.
2. **Enable SQL Firewall for the Target Database**:
    - Select the target database (your registered ADB) from the list.
    - If SQL Firewall is not already enabled, click **Enable SQL Firewall**.
    - Confirm the activation to enable SQL monitoring and protection.
3. **Define Initial SQL Activity Profile**:
    - Navigate to the **Activity Profiles** tab.
    - Click **Generate Profile** to create a baseline of SQL activity for the target database.
    - Select the duration for collecting SQL activity (e.g., 1 hour, 1 day).
    - Wait for the profile generation to complete.

6.7.3 Step 2: Define Rules to Allow or Block Specific SQL Statements

1. **Go to SQL Firewall Rules**:
    - Navigate to the **Rules** tab in the SQL Firewall section.
2. **Create a New Rule**:
    - Click **Create Rule** to define a custom SQL Firewall rule.
    - Specify the following:
        - **Rule Type**:

Copyright © 2024 Accenture. All rights reserved.

    - **Allow**: Permit specific SQL statements.
    - **Block**: Deny specific SQL statements.
  - **SQL Statement or Pattern**: Define the SQL statements or patterns to match (e.g., `SELECT * FROM sensitive_table` or `%DELETE%`).
  - **User or Role**: (Optional) Apply the rule to specific users or roles.

3. **Save the Rule**:
   - Ensure the rule is active and associated with the target database.

6.7.4 Step 3: Test the SQL Firewall by Executing Queries

1. **Connect to the Target Database**:
   - Use a SQL client (e.g., SQL*Plus or SQL Developer) or the OCI Cloud Shell to connect to the database:

```
sqlplus admin@your_database_alias
```

2. **Test Allowed Queries**:
   - Execute queries that are explicitly allowed by your SQL Firewall rules:

```
SELECT * FROM employees;
```

   - Confirm that these queries are executed successfully.

3. **Test Blocked Queries**:
   - Execute queries that should be blocked based on your rules:

```
DELETE FROM sensitive_table WHERE id = 1;
```

   - Verify that the query is blocked, and an error or log entry is generated.

4. **Verify Logs and Alerts**:
   - Return to the **SQL Firewall Dashboard** in Data Safe.
   - Review the logs to confirm that the blocked queries were recorded.
   - Check if any alerts were triggered for the blocked SQL statements.

Summary

In this exercise, you:

- Enabled and set up the SQL Firewall in Oracle Data Safe to monitor and protect SQL activity.
- Created rules to allow or block specific SQL statements based on security requirements.

Copyright © 2024 Accenture. All rights reserved.

- Tested the SQL Firewall by executing queries and verifying that the defined rules were enforced.

You have now completed the Data Safe exercises, enhancing your database security capabilities. Continue to explore other security features in Oracle Cloud Infrastructure.

- **Previous Exercise:** Exercise 10: Discover Sensitive Data
- **Next Exercise:** Exercise 12: Security Zones

Copyright © 2024 Accenture. All rights reserved.

7 Security Zones

7.1 Exercise 12: Create Security Zone

In this exercise, you will create a Security Zone in Oracle Cloud Infrastructure (OCI) to enforce security policies and explore the restrictions applied to resources created within the zone.

7.1.1 Objectives

- Set up a Security Zone in OCI.
- Test the Security Zone by creating an Object Storage bucket to observe enforced limitations.

Environment

Perform this exercise within the following environment:

- **Compartment:** `OCI-SEC-WS-LAB-nn`
- **Region:** Germany Central (Frankfurt)
- **OCI Console URL:** OCI Console Frankfurt - Login
- **OCI User:** *lab-oci-sec-ws**NN***
- **OCI Password:** *provided by trainer*

Ensure you are in the correct compartment and region. New resources, such as Cloud Shell configurations and ADB access settings, should be created within your designated compartment.

Solution

Login as User XYZ in OCI console and go to *Security & Identity -> Security Zones*. Ensure you have select the proper compartment in from the dropdown list on left side.

7.1.2 Create Security Zone

Identity & Security -> Security Zones

In dashboard, *Create Security Zone*.

Copyright © 2024 Accenture. All rights reserved.

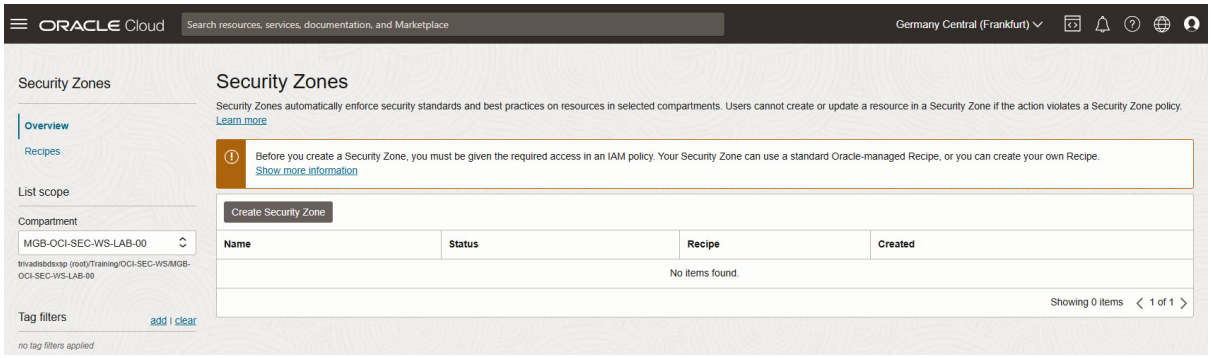


Figure 89: » step_1

Name the resource, as example in style: security-zone-. As example: security-zone-mbg-oci-sec-ws-lab-00. Add a description and click on **Create Security Zone**.

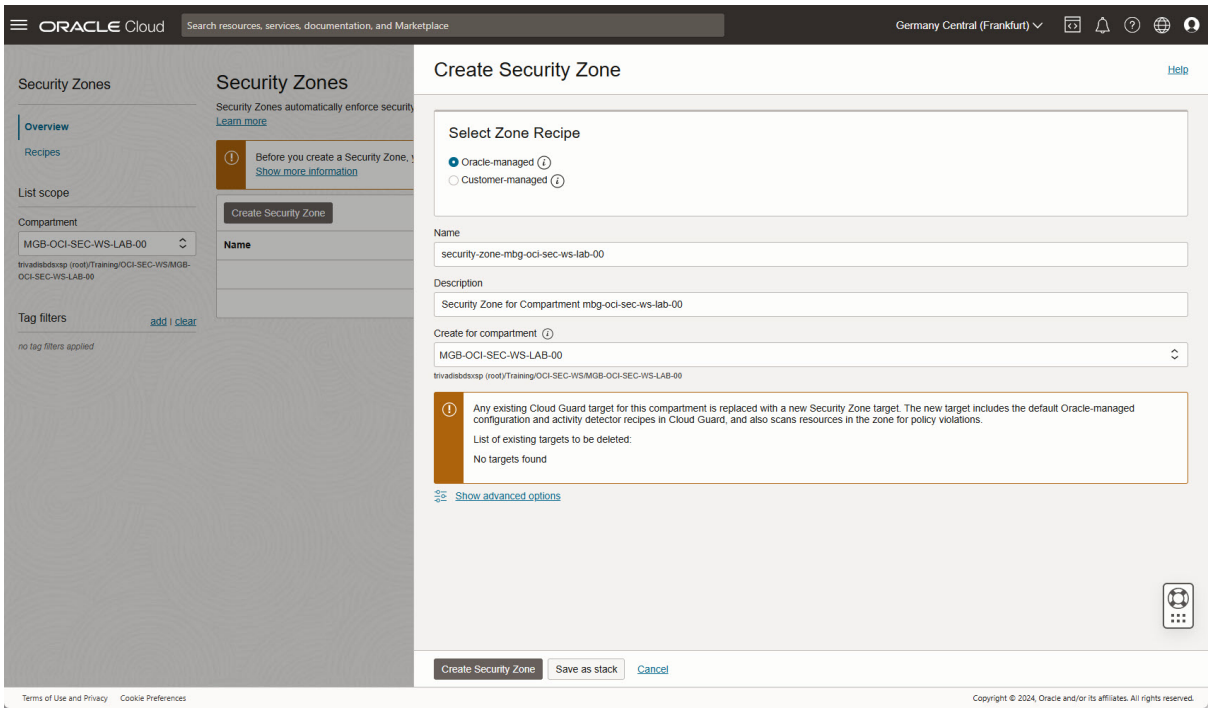


Figure 90: » step_2

Verify the new associated compartment.

Copyright © 2024 Accenture. All rights reserved.

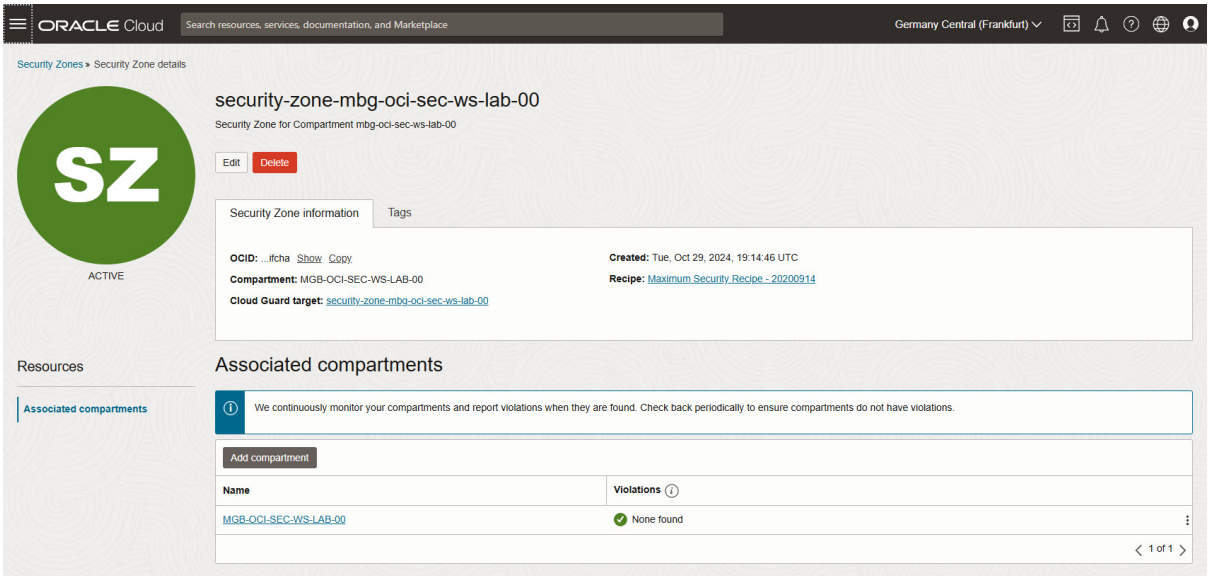


Figure 91: » step_3

In *Security Zones -> Recipes*, verify the associated Maximum Security Recipe automatically attached.

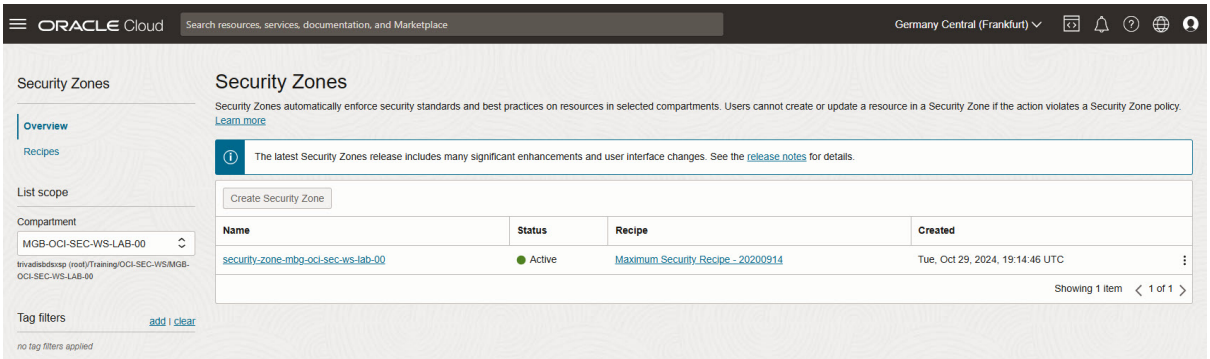


Figure 92: » step_4

7.1.3 Create an Object Storage bucket

Ensure you have select the proper compartment in from the dropdown list on left side to create a new Object Storage bucket. Verify the error.

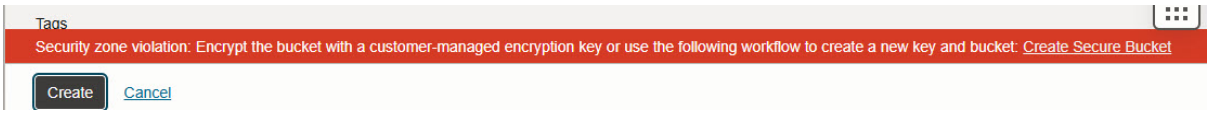


Figure 93: » step_5

Change and use the *Customer Managed Key* from exercise 01, as example my key called_mek-mbg-oci-sec-ws-lab-00_.

Copyright © 2024 Accenture. All rights reserved.

Figure 94: » step_6

Try to change visibility from the new created bucket to public. Verify the error message.

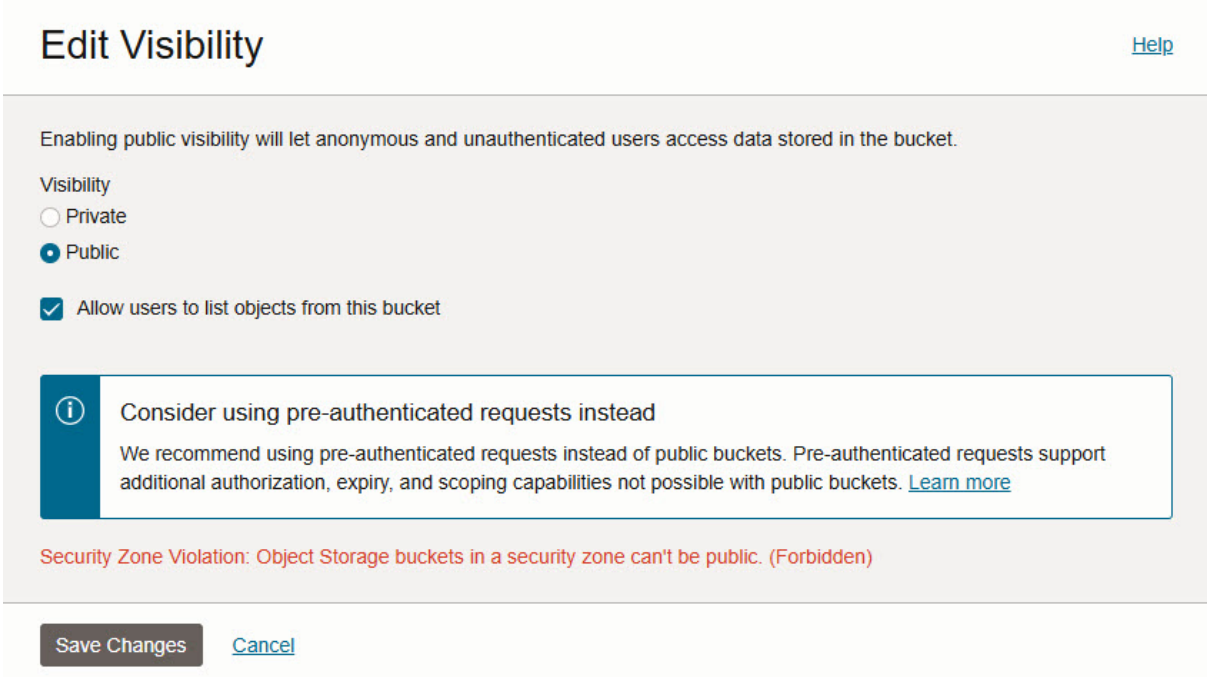


Figure 95: » step_7

7.1.4 Delete Security Zone

In *Security & Identity -> Security Zones*, select your security zone and delete it.

Copyright © 2024 Accenture. All rights reserved.

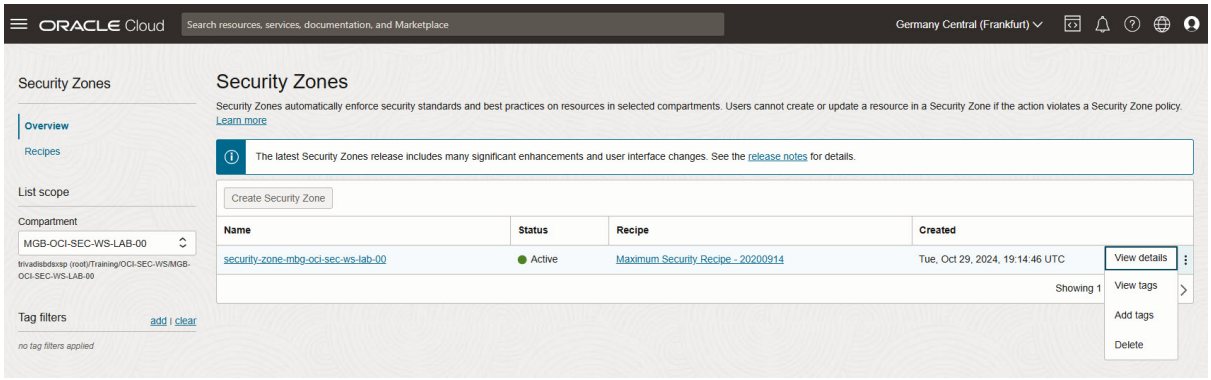


Figure 96: » step_8

7.1.5 Create a Public Object Storage

In Object Storage menu, change the visibility of created Object Storage bucket to *PUBLIC*. Verify the visibility - a yello triangle occurs.

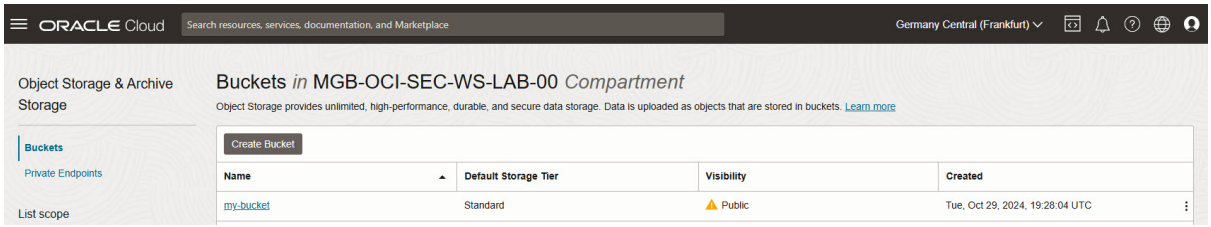


Figure 97: » step_9

7.1.6 Create Security Zone again

We repeat step 1, and create again the security zone in out compartment. Verify the Violations after successful creation. Is the public bucket detected? If not, grab a coffee and come back in a few minutes.

> step_10

Summary

In this exercise, you:

- Created a Security Zone to enforce OCI security policies.
- Attempted to create an Object Storage bucket within the Security Zone, observing any restrictions and limitations.

You are now ready to continue with the next exercise, where you will configure and test the Web Application Firewall (WAF) for enhanced application security.

Copyright © 2024 Accenture. All rights reserved.

- **Previous Exercise:** Exercise 11: SQL Firewall
- **Next Exercise:** Exercise 13: Web Application Firewall (WAF)

7.2 Exercise 13: Setup WAF for XSS Detection

In this exercise, you will configure a Web Application Firewall (WAF) in Oracle Cloud Infrastructure (OCI) to detect cross-site scripting (XSS) attacks. You will set up a Load Balancer and WAF to protect an HTTP server running on compute instances in a private network.

7.2.1 Objectives

- Configure Cloud Shell for access to the private network.
- Install an HTTP server on compute instances.
- Set up a public Load Balancer.
- Configure the Web Application Firewall (WAF).
- Test the WAF configuration to verify XSS detection.

Environment

Perform this exercise within the following environment:

- **Compartment:** `OCI-SEC-WS-LAB-nn`
- **Region:** Germany Central (Frankfurt)
- **OCI Console URL:** OCI Console Frankfurt - Login
- **OCI User:** *lab-oci-sec-ws**NN***
- **OCI Password:** *provided by trainer*

Ensure you are in the correct compartment and region. New resources, such as Cloud Shell configurations and ADB access settings, should be created within your designated compartment.

Solution

Login as User XYZ in OCI console. Ensure you have select the proper compartment in from the dropdown list on left side.

7.2.2 Setup Cloud Shell for private Network

In *Compute -> Instances*, note down the two private IP addresses of the compute instances. As example 10.0.0.75 and 10.0.0.76.

Copyright © 2024 Accenture. All rights reserved.

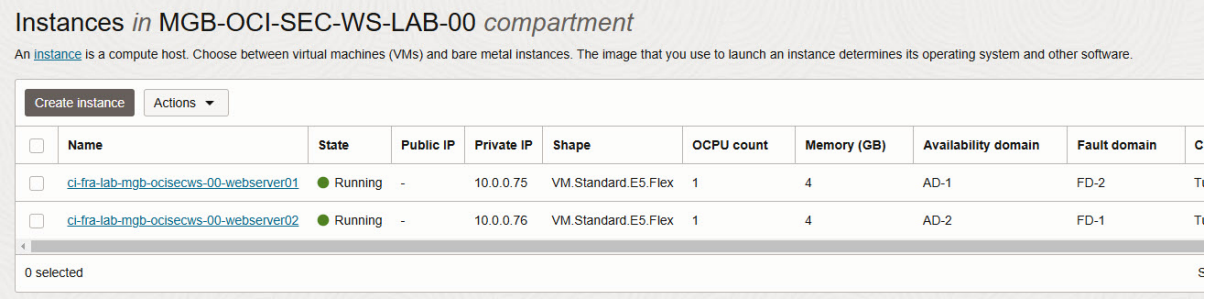


Figure 98: » step_1

On top of OCI Console, verify region is Germany Central (Frankfurt), open a Cloud Shell. Enusre private network from exercise 01 is activated.

In Cloud Shell, create a new directory and download Private SSH Key from OCI object storage.

```
-- create directory
mkdir ssh
cd ssh

--get key
wget https://objectstorage.eu-frankfurt-1.oraclecloud.com/p/Dec-
   iebNrGgpe_KhXMkugnekpAOQHl-jAUGJMlgpqngKmSP8iqMKdLXu8hT0Wsru/n/
   trivadisbdsxsp/b/DOAG-2024/o/id_rsa

-- set permissions
chmod 600 id_rsa
```

7.2.3 Install http Server on Compute Instances

Login in first compute instance webserver as user opc. Use the private key from above to connect.

```
--login as user opc
cd $HOME/ssh
ssh -i id_rsa opc@10.0.0.75
```

```
--http / php package installation
$ sudo dnf install httpd php -y
--start apache and php module
$ sudo apachectl start
$ sudo systemctl start php-fpm
--enable for server restart
$ sudo systemctl enable httpd
$ sudo systemctl enable php-fpm
--verify apache is running on port 80
$ sudo netstat -tulnp | grep http
--enable firewall
$ sudo firewall-cmd --permanent --zone=public --add-service=http
$ sudo firewall-cmd --reload
```

Create HTML Index Page and XSS PHP Page in /var/www/html

Copyright © 2024 Accenture. All rights reserved.

```
--create index.php file
$ sudo vi /var/www/html/index.php

--copy & paste the lines below to file

<?php
echo "OCI Hostname: " . gethostname();
?>
```

Save and close the file with

- esc
- :
- wq sequence.

```
--create xss demo file
$ sudo vi /var/www/html/xss_demo.php

--copy & paste the lines below to file

<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <title>XSS Demo</title>
</head>
<body>
    <h1>XSS Demo Page</h1>
    <form action="" method="get">
        <label for="name">Enter your name:</label>
        <input type="text" id="name" name="name">
        <input type="submit" value="Submit">
    </form>
    <?php
    if (isset($_GET['name'])) {
        $name = $_GET['name'];
        // This directly outputs user input without
        // sanitization, making it vulnerable to XSS
        echo "<p>Hello, $name</p>";
    }
    ?>
</body>
</html>
```

Save and close the file with

- esc
- :
- wq sequence.

Test running webserver. This command returns the hostname.

```
curl http://localhost
```

Repeat the steps for second webserver.

7.2.4 Setup Public Load Balancer

Create a Public Load Balancer in Public Subnet with the two webservers as backend, attention: health check must set to http (as https as per default). Verify that backend

Copyright © 2024 Accenture. All rights reserved.

checks run to green (ok) after a while.

Networking -> Load Balancer -> Create Load Balancer

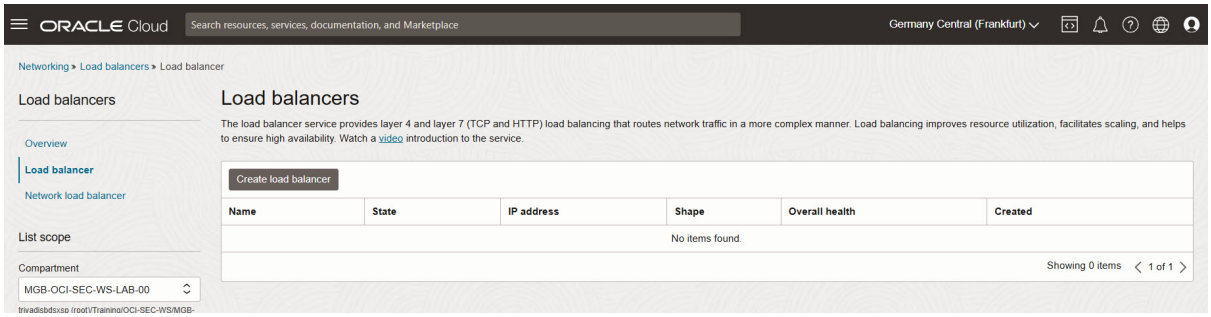


Figure 99: » step_6

Add details:

- set name
- let visibility type as PUBLIC

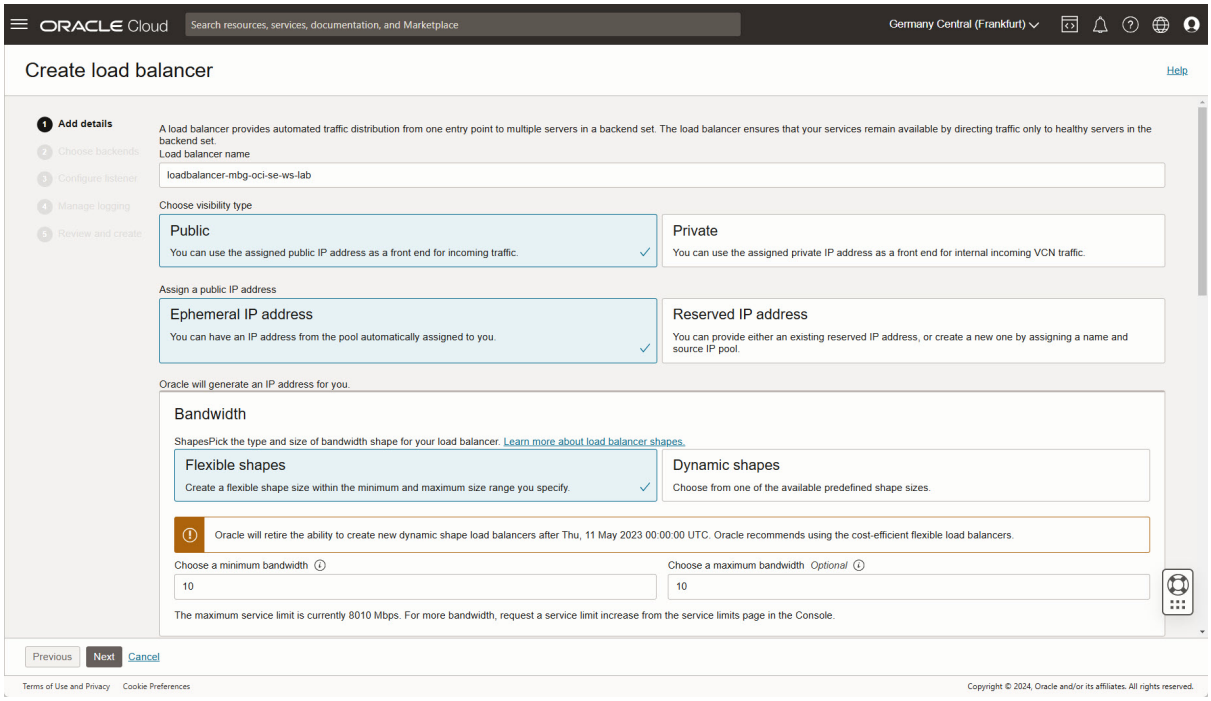


Figure 100: » step_7

Scroll down and set:

- Virtual Cloud network
- Your public subnet

Copyright © 2024 Accenture. All rights reserved.

Figure 101: » step_8

Next.

Choose backends:

- select backend servers and add your compute instances

Select your two webserver and add them to the list. Let port as is. Do ot change other settings.

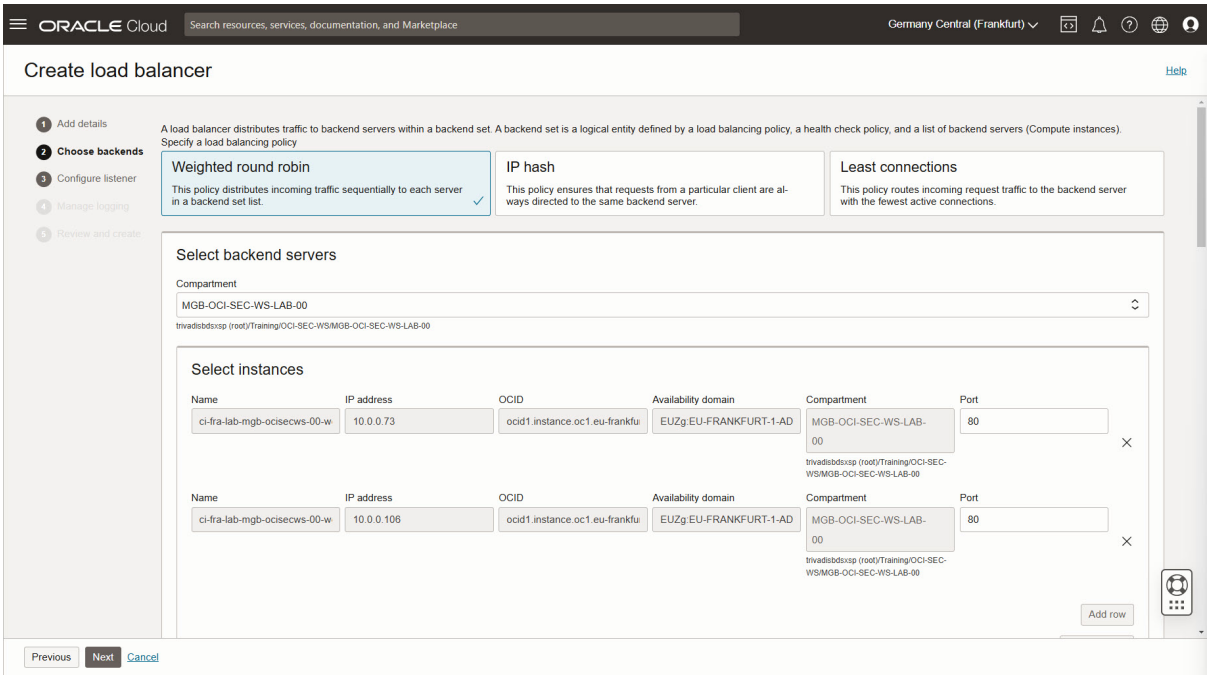


Figure 102: » step_9

Next.

Configure listener:

- Change type of traffic type to HTTP. Do not change other settings.Port is automatically changed to 80 now.

Copyright © 2024 Accenture. All rights reserved.

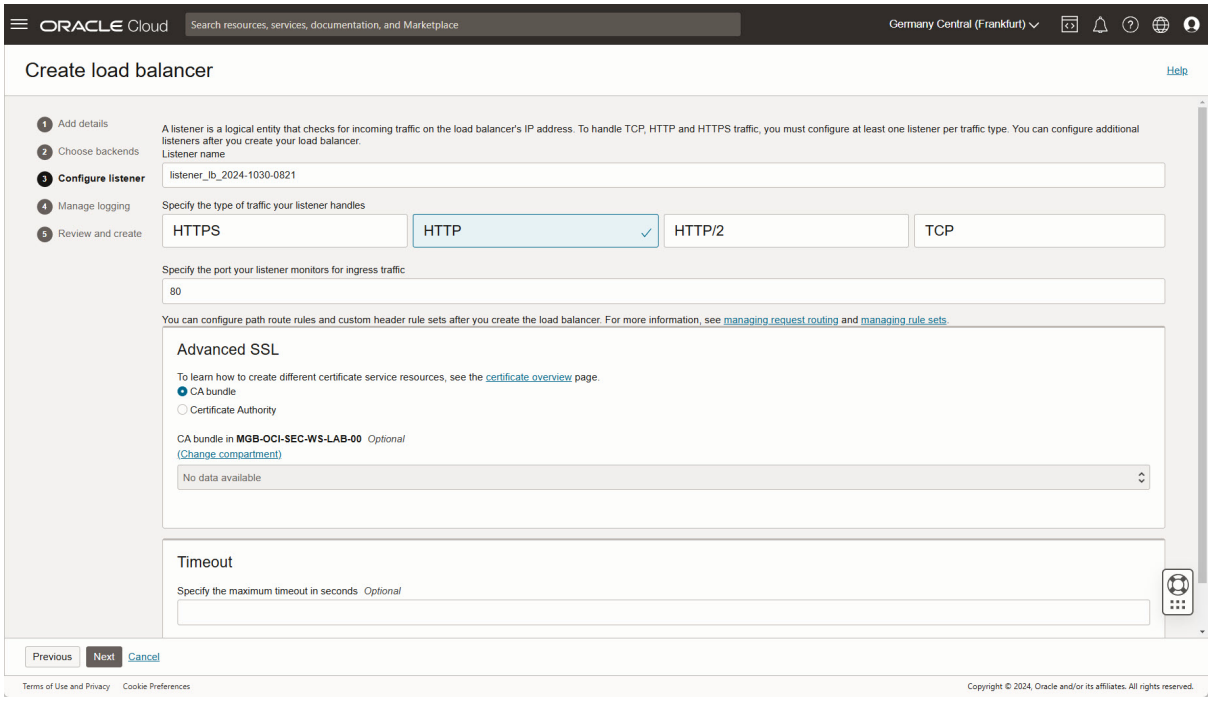


Figure 103: » step_10

Next.

Manage Logging:

- Do not change settings.
- Verify your compartment is selected in dropdown list

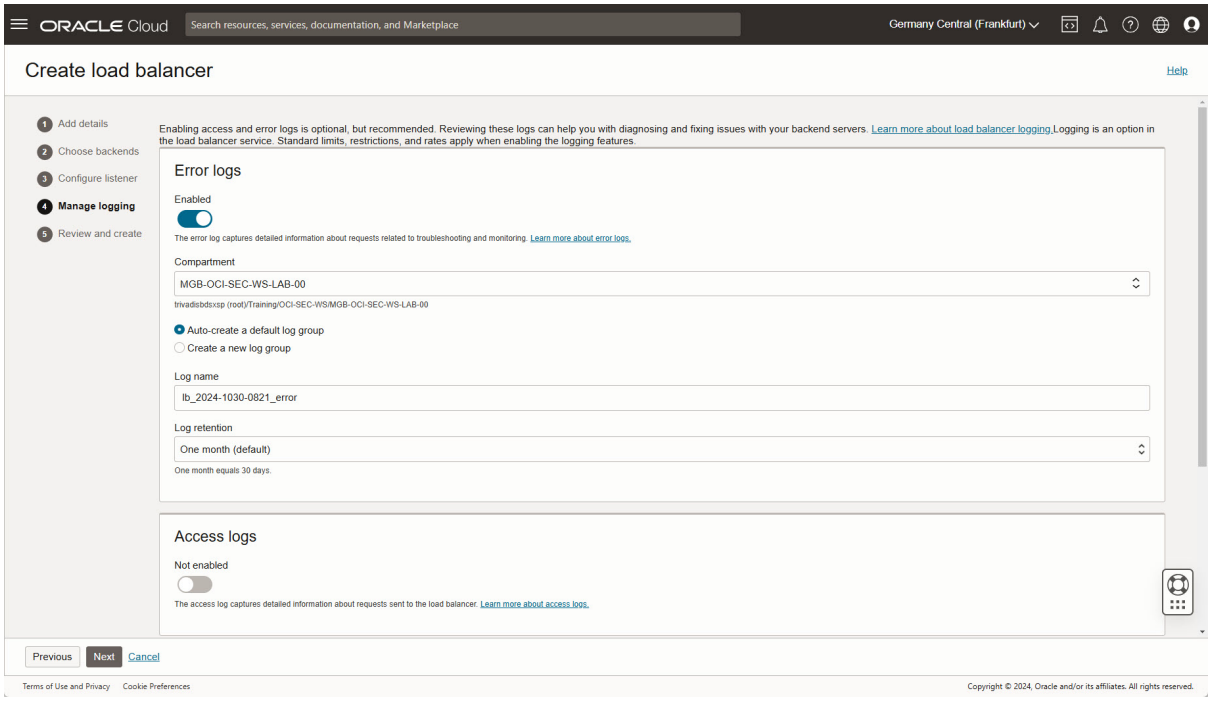


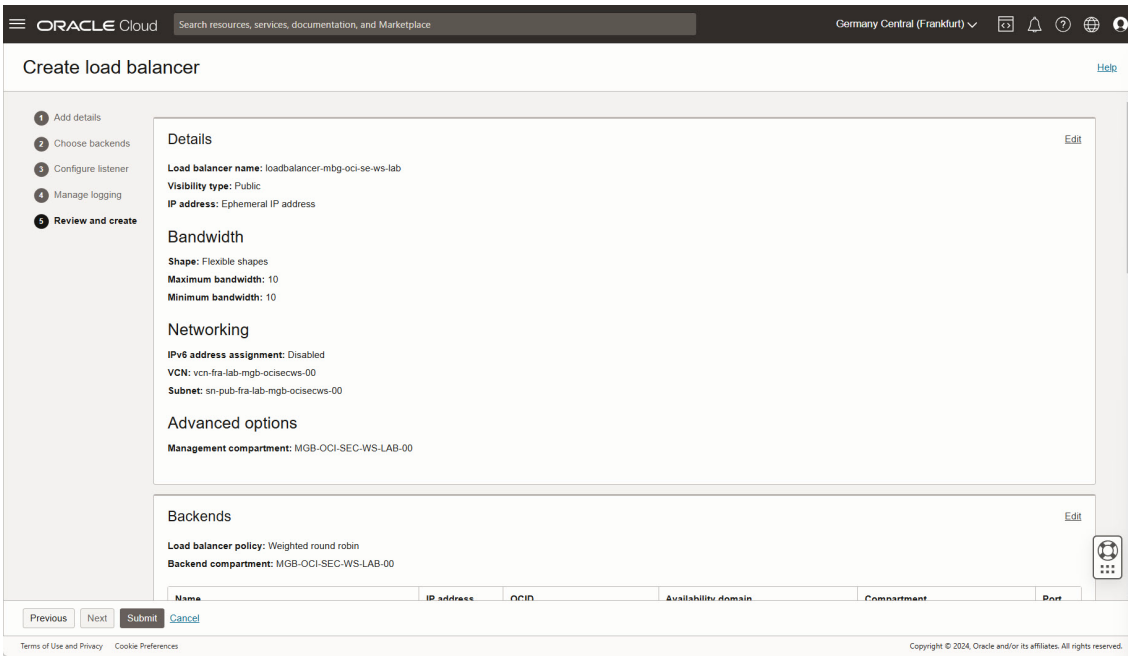
Figure 104: » step_11

Copyright © 2024 Accenture. All rights reserved.

Next.

Review and create:

- verify settings



Submit.

The load balancer is created, wait until completed. Now you can see the load balancer public IP in overview in section Load balancer information. The overall health changes to ok.

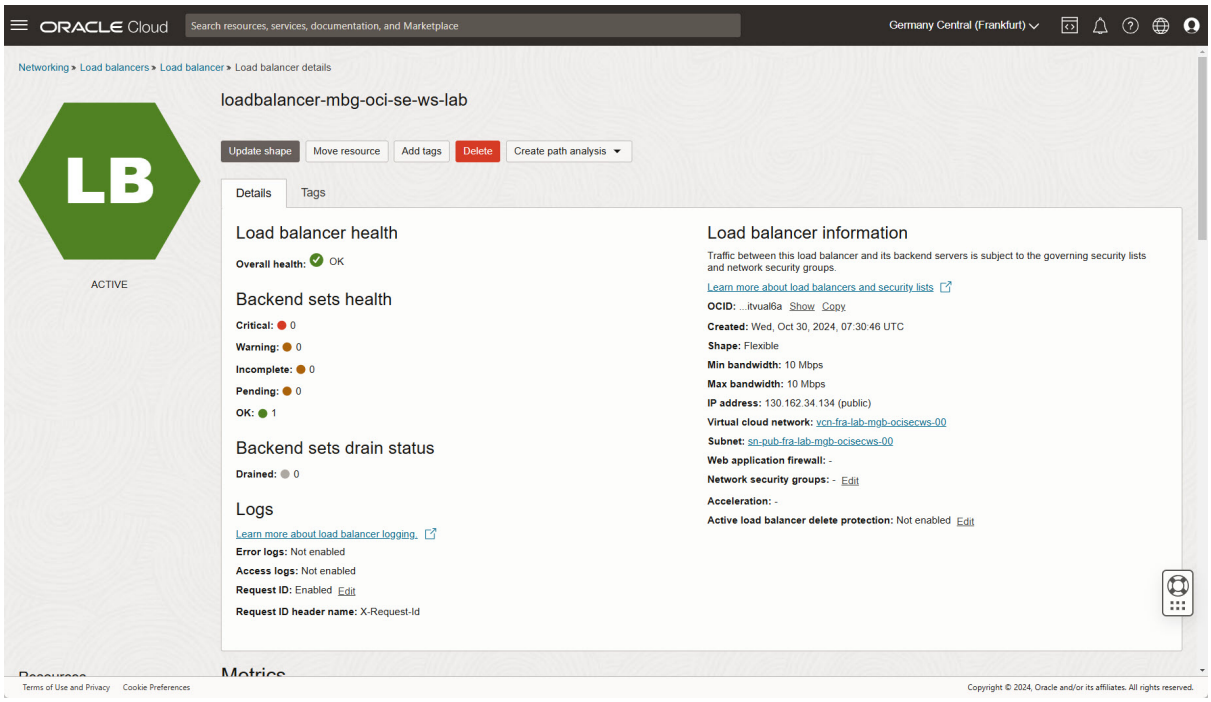


Figure 105: » step_13

Verify reachability in a new web browser window - URL: http://your public load bal-

Copyright © 2024 Accenture. All rights reserved.

ancer ip/index.php. Whenever the browser is refreshed, the webserver changes from webserver01 to webserver02 and vice versa.

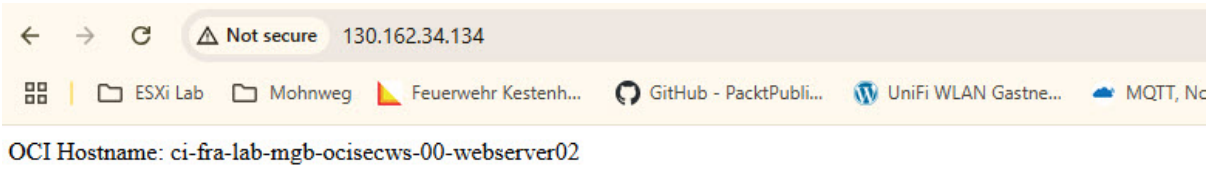


Figure 106: » step_14

Same when using xss_demo.php as target URL: http://your public load balancer ip/xss_demo-php.

Figure 107: » step_15

Test XSS-Injection by type in text box:

- or use the direct URL , as example http://129.159.106.151/xss_demo.php?name=
  .

A popup-window occurs. If there is no window, two possible reasons for:

- company network where such URLs are blocked by DNS
- popup-blocker enabled

Figure 108: » step_16

7.2.5 Setup Web Application Firewall

Identity & Security -> Web Application Firewall -> Create WAF policy.

Basic information: Set a name, do not change the actions.

Copyright © 2024 Accenture. All rights reserved.

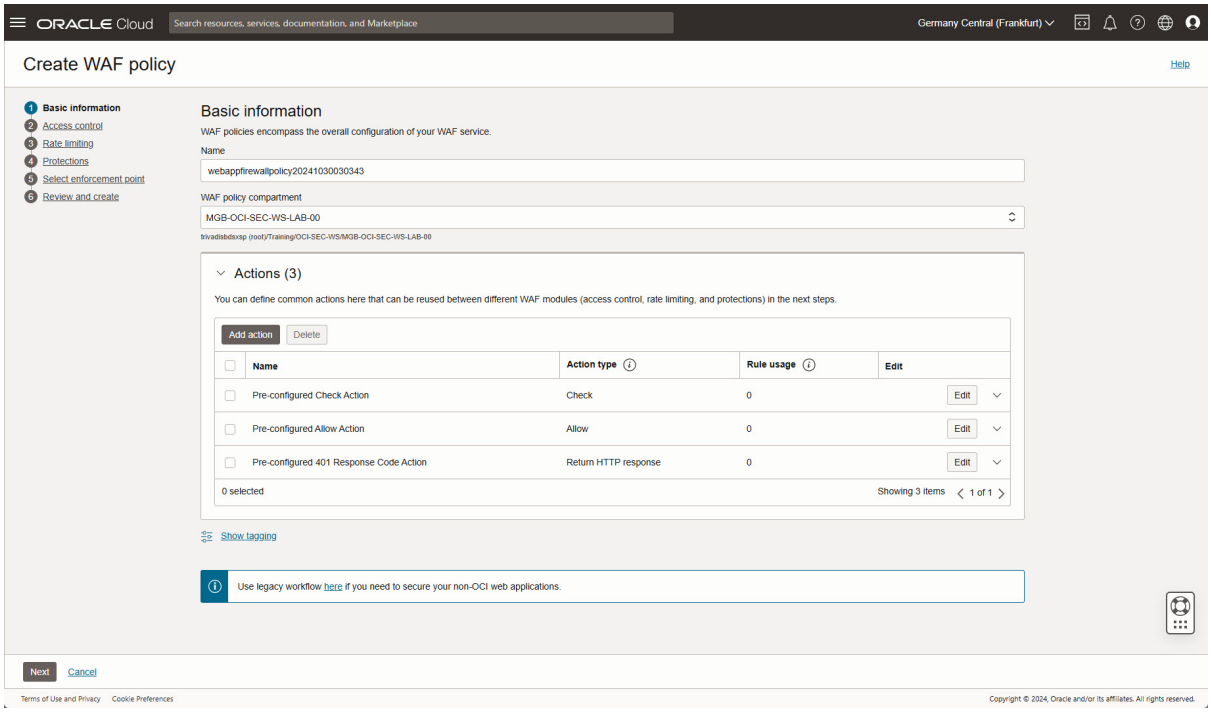


Figure 109: » step_1

Next.

Access control: Do NOT enable the checkbox.

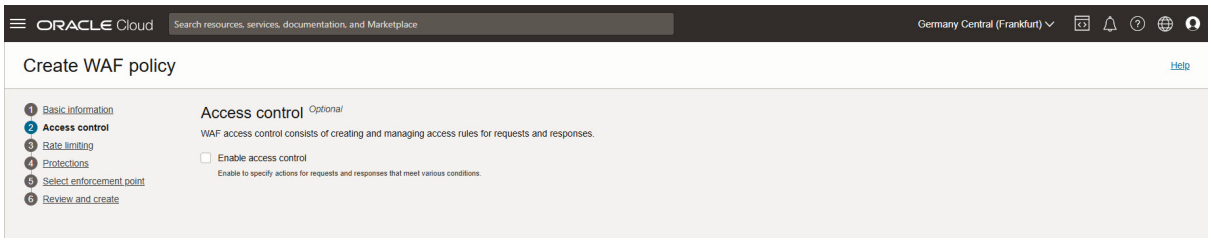


Figure 110: » step_2

Next.

Rate limiting: Do NOT enable the checkbox.

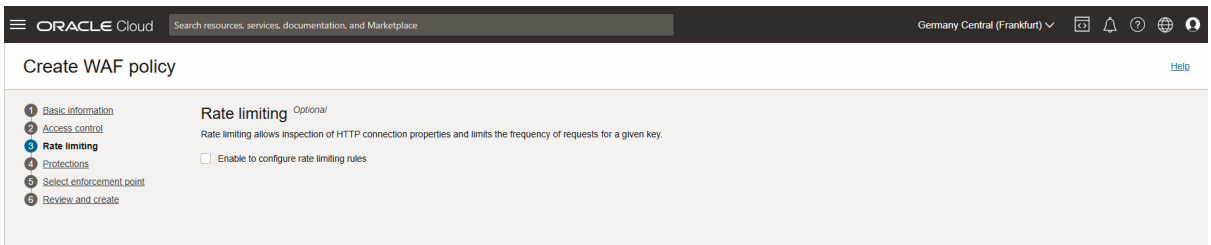


Figure 111: » step_3

Next.

Copyright © 2024 Accenture. All rights reserved.

Protections: Enable checkbox and *Add request protection rule*.

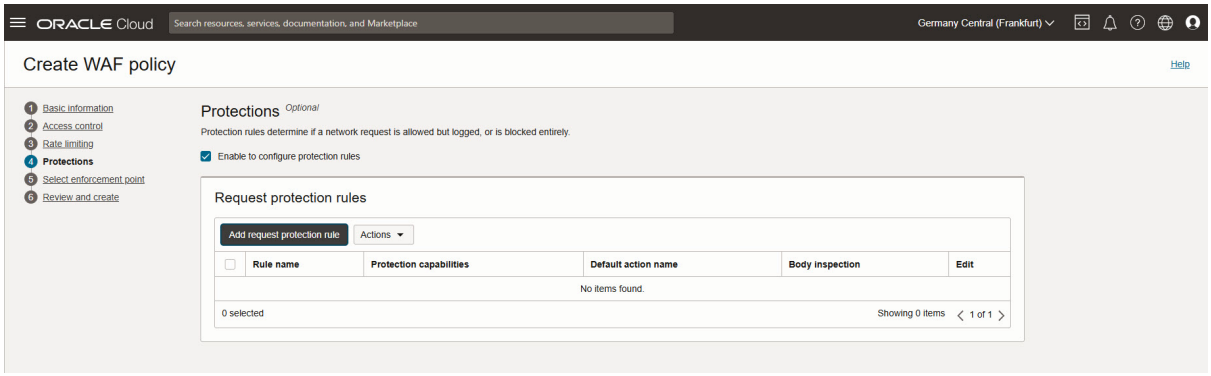


Figure 112: » step_4

Set a name for the rule, as action name select *Pre-configured 401 Response Code Action*.

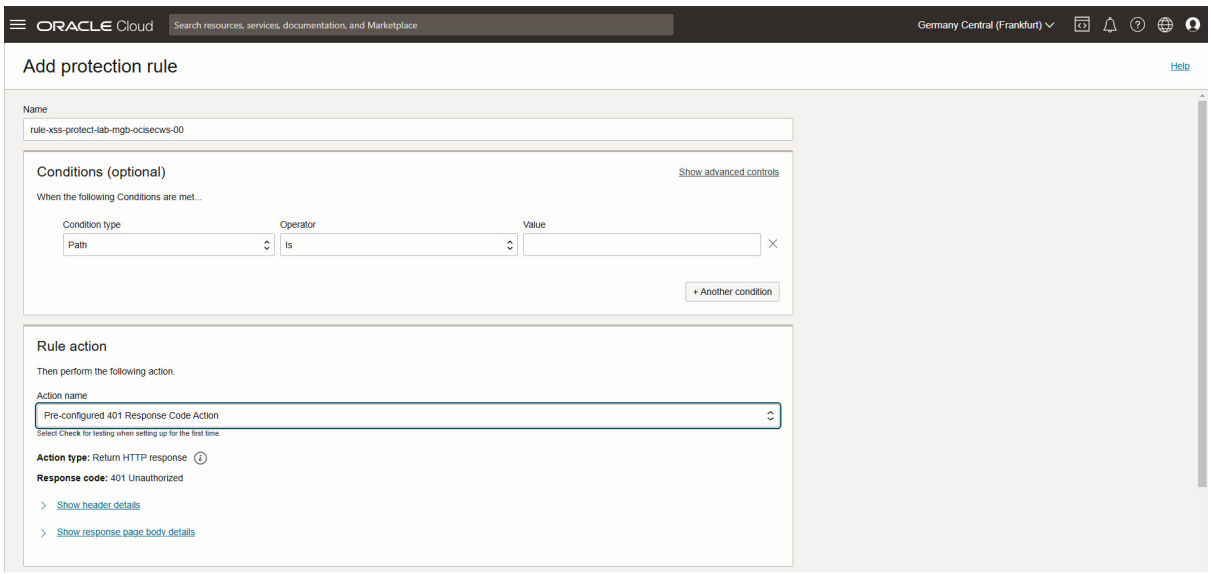


Figure 113: » step_5

Scroll down to section *Protection capabilities*, click on *Choose protection capabilities* to add XSS components.

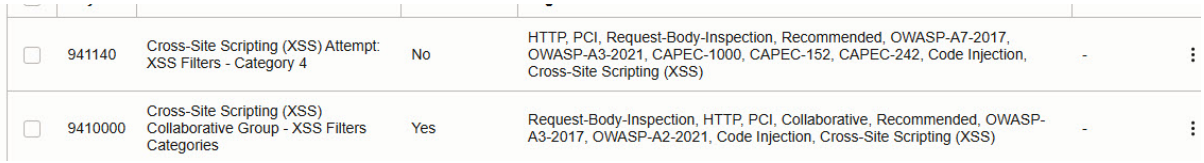


Figure 114: » step_6

Click on button *Add request protection rule* at the bottom to add selected rule action and protection capabilities.

Copyright © 2024 Accenture. All rights reserved.

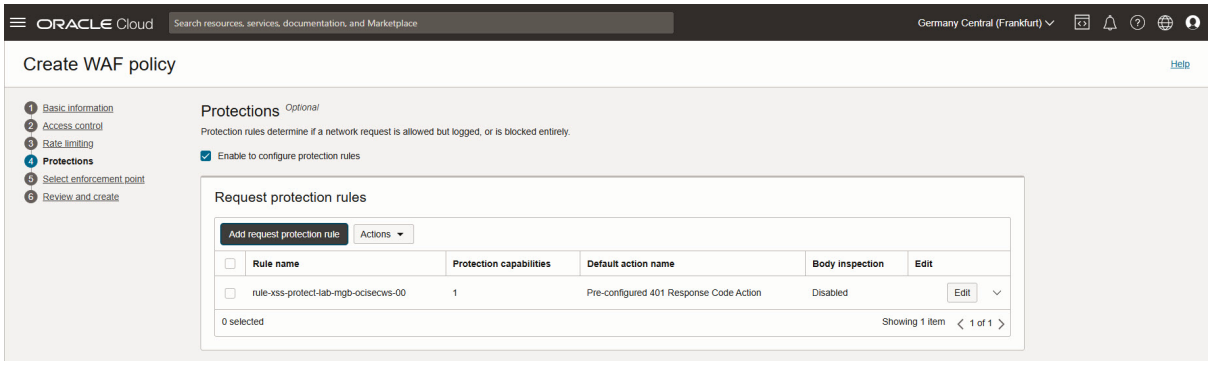


Figure 115: » step_7

Next.

Select enforcement point: select Load Balancer created above.

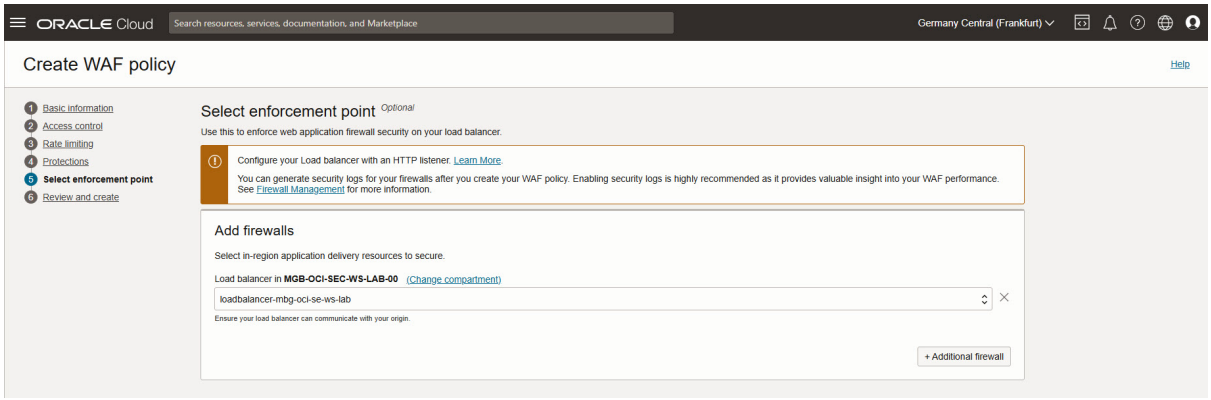


Figure 116: » step_8

Next.

Review and create: click on *Create WAF policy*. Wait a moment until policy and firewall rule are created.

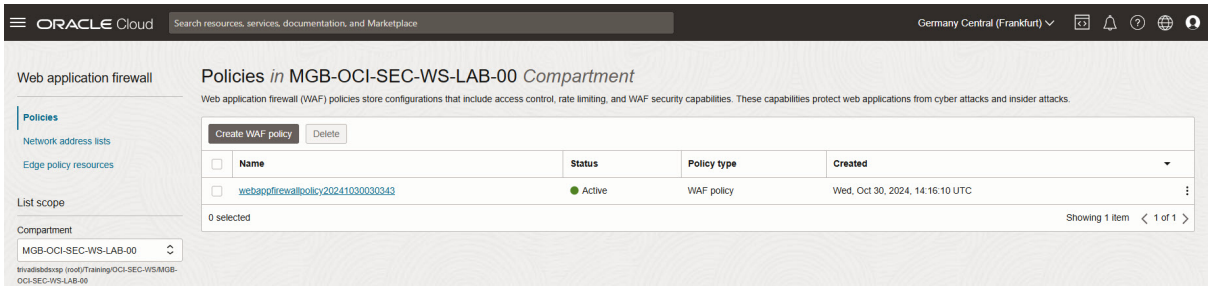


Figure 117: » step_9

Copyright © 2024 Accenture. All rights reserved.

7.2.6 Verify WAF

Open web browser with URL http:///xss_demo-php. Enter the code snippet into the text box nd click on *Submit*.

```
<script>alert('XSS');</script>
```

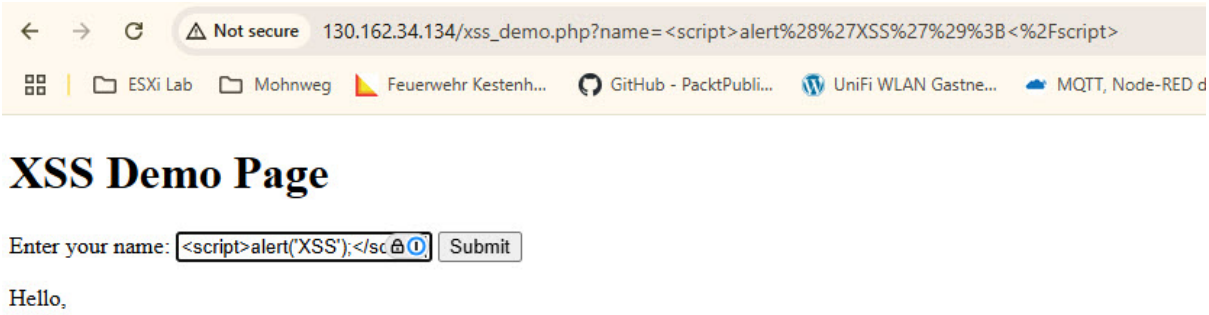


Figure 118: » step_10

An error occurs.

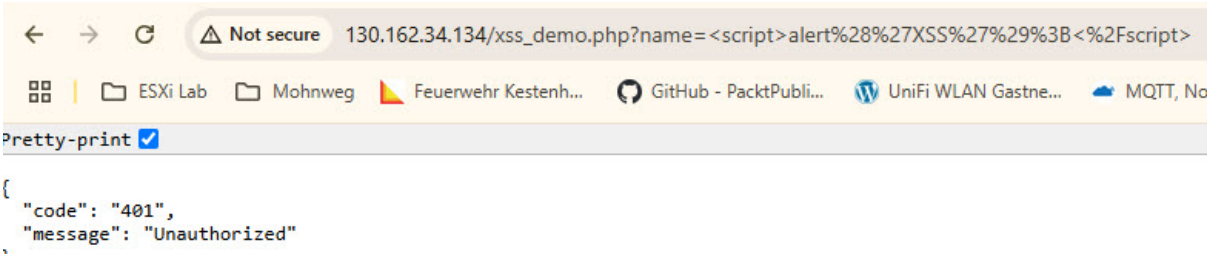


Figure 119: » step_11

Optional:

- try to change error message with a own text

Summary

In this exercise, you:

- Configured Cloud Shell to connect to the private network.
- Installed an HTTP server on compute instances.
- Set up a public Load Balancer to route traffic.
- Configured a Web Application Firewall (WAF) to detect and block XSS attacks.
- Verified that the WAF successfully detected XSS attempts.

You have now completed the WAF setup and are ready to continue exploring other security features in OCI.

Copyright © 2024 Accenture. All rights reserved.

- **Previous Exercise:** Exercise 12: Create Security Zone
- **Next Exercise:** Workshop Overview

Copyright © 2024 Accenture. All rights reserved.

8 Appendix E: Manual Lab Configuration

Copyright © 2024 Accenture. All rights reserved.

9 Appendix F: Oracle Cloud Infrastructure Users and Permissions

Copyright © 2024 Accenture. All rights reserved.