Oracle Cloud Infrastructure (OCI) Security Workshop

Laboratory and Exercise Guide

November 22, 2024, Version 0.14.1 Stefan Oehrli, Martin Berger



Table of Contents

1	Wo	rkshop Introduction	3
	1.1	Workshop Overview	3
	1.2	Learning Outcomes	3
2	Lab	Overview	4
	2.1	Oracle Cloud Infrastructure (OCI) Security Workshop Architecture	4
	2.2	Key Components of the Architecture	4
	2.3	Lab Exercise Focus Areas:	5
3	oc	Setup	6
	3.1	Exercise 00: Getting Started with OCI	6
4	Bas	ic OCI Security	18
	4.1	Exercise 01: Key Management	18
5	Clo	ud Guard	24
	5.1	Exercise 02: Manual Remediation	24
	5.2	Exercise 03: Auto Remediation	37
	5.3	Exercise 04: Notification Setup	44
6	Dat	a Safe	51
	6.1	Exercise 05: Configuration and Register ADB	51
	6.2	Exercise 06: Assess Database Configurations	54
	6.3	Exercise 07: Assess Database Users	60
	6.4	Exercise 08: Audit Database Activity	65
	6.5	Exercise 09: Generate Alerts	67
	6.6	Exercise 10: Discover Sensitive Data	70
	6.7	Exercise 11: SQL Firewall	72
7	Sec	urity Zones	76
	7.1	Exercise 12: Create Security Zone	76
	7.2	Exercise 13: Setup WAF for XSS Detection	81
8	Арр	pendix E: Manual Lab Configuration	94
9	App	endix F: Oracle Cloud Infrastructure Users and Permissions	95

List of Tables

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.

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.

- **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.

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-wsNN
- 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

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



Figure 2: Cloud Console

3.1.3 Step 2: Using the Cloud Shell

env |grep -i oci cs

- 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.
```

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.

 E ORACLE Cloud
 Search resources, services, doc
 Germany Central (Frankfurt) >
 Image: Cloud Shell Service network >

 Actions >
 Network: OCI service network >
 >
 Image: Cloud Shell Service network >
 Image: Cloud Shell Service network >
 Image: Cloud Shell Service network (Default)

 Vour Cloud Shell Private network definition list al (Frankfurt You are using
 Private network definition list directory. Your Cloud Shell (machine and home directory) are located in: Germany Centre user lab-mgb-dev-oci-sec-ws90

 Type 'help' for more info. lab_mgb_de@cloudshell:~ (eu-frankfurt-1)\$ []

Select Private network definition list.

Figure 3: Cloud Shell 01

Ω

මා

Click on Create private network definition.

Actions $$	Network: OCI service network	Private network definition list				
Cloud Shell						
Netcome to Ora Upgrade Notifi Your Cloud She al (Frankfurt) You are using Type `help` fo	cle Cloud Shell. cation: Cloud Shell will be upgrading ill machine comes with 568 of storage f Cloud Shell in tenancy trivadisbdsxsp r more info.	(i) You a You can have private networ	are using OCI service ne a maximum of 5 favorite rk list.	etwork.	ons. They are listed in the	
lab_mgb_de@clo	udshell:~ (eu-frankfurt-1)\$ 🛛	Create priv	vate network definition		Q Search by name	
		Favorite	Name	Subnet	Last used	
		No items found.				
				Sh	owing 0 items \langle 1 of 1 \rangle	
		Default no	etwork			
		Select defau	It network description			
		OCI servic	e network		\$	

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

Private n	etwork definitio	on list	Create private network definition	<u>Help</u>
(i) You are u	using OCI service network.	-		
/ou can have a m	aximum of 5 favorite private	network definitions. They	Name my-private-network	
Create private	network definition		VCN in MGB-DEV-OCI-SEC-WS-LAB-00 (Change con	npartment)
Eavorite N	Name	Subnet	vcn-fra-lab-mgb-devocisecws-00	\$
ravonte	Valle	No item	Subnet in MGB-DEV-OCI-SEC-WS-LAB-00 (Change compartment)	
			sn-prv-comp-fra-lab-mgb-devocisecws-00	\$
Select default netwo	etwork description		Network security groups (Optional Network security groups in No compartment selected (Change compartment) Select a virtual cloud network first + Anothe) C × r NSG
			Use as active network	
Close			Create <u>Cancel</u>	

Figure 5: Cloud Shell 03

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

You are using private Du can have a maximum of 5 Create private network defin Favorite Name	network " my-private-network ". favorite private network definitions. They are hition	listed in the private network list.	Q Search by name
u can have a maximum of 5 Create private network defin Favorite Name	favorite private network definitions. They are	listed in the private network list.	Q Search by name
Create private network defin	nition		O Search by name
Favorite Name	Subact		
	Subliet	Last used	
☆ my-private-ne	tworkcsg6axka <u>Sh</u>	<u> </u>	
			Showing 1 item < 1 of 1 >
Default network			
Select default network descri	סנוסח		
OCI service network			\$

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

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.

Autonomous Database de uman intervention while	Databa elivers fast peri the system is r	ASES <i>in</i> N formance and re running. <u>Learn r</u>	MGB-DE equires no datal	EV-OCI-SEC	C-WS-LAB-00 erforms all routine databas	compartmen	n t out
Create Autonomous D Display name	latabase	Compute	Storage	Workload type	Disaster recovery	Created	•
adb-fra-lab-mgb-devo- cisecws-00-atp23ai01 Developer	• Available	4 ECPUs	20 GB	Transaction Processing	_	Mon, Nov 18, 2024, 11:00:20 UTC	
					Displaying 1 Auto	onomous Database < 1	l of 1

Figure 8: ADB Connect 01

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

Resource allocation	Network		
ECPU count: 4	Mutual TLS (mTLS) authentication: Not required Edit		
Storage: 20 GB	Access type: Allow secure access from specified IPs and VCNs Access control list: Enabled Edit		
Associated services	Availability domain. EUZg.EU-FRANK		

Figure 9: ADB Connect 02

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

Edit access control list

Specify the IP addresses and VCNs allowed to access this database. You can use a comma-separated list to enter multiple IP addresses. An access control list blocks all IP addresses that are not in the list from accessing the database.

P notation type	Values
Virtual cloud network OCID	\$ ocid1.vcn.oc1.eu-frankfurt-1.amaaaaaasijhdmqaodduj2wi
	IP addresses or CIDRs Optional
	Add access control r

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.

		Add my IP address	Add access control rule
D	When you update a remote peer with separate acces updates from the primary database.	is control rules, it will no longer folic	w the access control rule

Figure 11: ADB Connect 04

Click on Save to store the settings.

Help

Edit access control list

Specify the IP addresses and VCNs allowed to access this database. You can use a comma-separated list to enter multiple IP addresses. An access control list blocks all IP addresses that are not in the list from accessing the database.

IP notation type	Values
Virtual cloud network OCID	cid1.vcn.oc1.eu-frankfurt-1.amaaaaaasijhdmqaodduj2wi
	IP addresses or CIDRs Optional ×
P notation type	Values
IP address	३ 138.2.168.154
	Add my IP address Add access control rule
updates from the primary database.	

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.

Create a new directory, change into this directory.

<u>Help</u>

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

Administrator password	Helo
Change your administrator's password.	
Username Read-only	
ADMIN	
Password	
Confirm password	
Change Cancel	

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.

Autonomous	Databa	ases <i>in</i> M	MGB-DE	EV-OCI-SEC	C-WS-LAB-00	compartment	t
Autonomous Database d human intervention while	elivers fast per the system is	formance and re running. <u>Learn r</u>	equires no data <u>nore</u> .	base administration. It p	erforms all routine database	e maintenance tasks witho	ut
Display name	State	Compute	Storage	Workload type	Disaster recovery	Created	•
adb-fra-lab-mgb-devo- cisecws-00-atp23ai01 Developer	Available	4 ECPUs	20 GB	Transaction Processing		Mon, Nov 18, 2024, 11:00:20 UTC	:
					Displaying 1 Auto	nomous Database < 1	of 1 >

Figure 15: ADB Connect 01

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.

		Search Database (ૠ+K)	Q ② 名 admin V
Navigator Files ③	[Worksheet]* 🕶 🕞 🍽 🛱 🗸 😽	년 🗐 Consumer group:	LOW -
ADMIN	🕹 🖂 🗛 🕶 🗊	Data Load	60 ③
All Objects	1 select-level-num 2 from-dual		_
Search	3 connect by level <= 10;		
\$1 DB100LS\$EXECUTION_HISTORY_SE	2		
	Query Results		
	Displays the results of the most recent Run Statement operation.		
	Right-click the grid to access advanced functionality such as manage and sort columns, count rows, view single records, and export data.		
	Query Result Script Output DBMS Output Explain Plan	Autotrace SQL History	0
	1 (i) (i) Download 🔻 Execution time: 0.004 seconds		
	NUM		
	1 1		
	2 2		
	4 4		
	5 5		
	a a		
(🗶 1 ⚠ 0 ξ§3 0 <u>9:25:07 PM - 10 rows total</u>			Powered by ORDS

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.

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

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-wsNN
- 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*.

Create Vault	<u>Help</u>
Vaults provide your growing data and application encryption with scalable key storage. You can start small, with as little as a single key, and grow to thousands of keys to support your growing cloud deployment. Create in Compartment	
OCI-SEC-WS-LAB-00	
trivadisbdsxsp (root)/Training/OCI-SEC-WS/OCI-SEC-WS-LAB-00	
Name	
vault-oci-sec-ws-lab-00	
Make it a virtual private vault Creates the vault as a dedicated partition on the HSM, sets pricing based on the maximum usage against key limits, and accommodates greater performance needs <u>Learn more</u>	

Figure 18: » step_1

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

				Switzerland North (Zurich) 🗸 🗔 🏠 💮 🖨 🧕
Key Management & Secret Management	Vaults in OCI-SEC-V Vauits let you centrally manage the encry Create Vauit	VS-LAB-00 Compartment	identials that you use to securely access resources. Learn	nore
Dedicated Key Management	Name	State	Virtual Private	Created -
External Key Management Private Endpoints	vault-oci-sec-ws-lab-00	Active	No	Wed, Oct 23, 2024, 12:30:30 UTC
List scope				Showing 1 item < 1 of 1 >
Compartment				
OCI-SEC-WS-LAB-00				
trivadisbdsxsp (root)/Training/OCI-SEC-WS/OCI-S EC-WS-LAB-00				
Tag filters add I clear				

Figure 19: » step_2

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

	Search resources, services, docur	mentation, and Marketplace			Switzerland North (Zurich) \checkmark	$\mathbf{\hat{o}}$	Δ (0	0
Key Management & Secret Managem	ent > Vault > Vault Details								Î
	vault-oci-sec	-ws-lab-00							
	Edit Name Replicate	e Vault Add tags Move Resource	Delete Vault						
	Vault Information	Tags							
	General infor	mation							8
	Compartment: trivadi	isbdsxsp (root)/Training/OCI-SEC-WS/OCI	I-SEC-WS-LAB-00	Virtual Private: No					
ACTIVE	OCID:nldgaq Show Created: Wed, Oct 23	<u>¥ Copy</u> 3, 2024, 12:30:30 UTC		Cryptographic Endpoint: https://fjtr3dfaa crypto.kms.eu- zurich-	fbe-				
				1.oraclecloud.co	<u>om</u> (i)				
				management Endpoint. <u>mito://jir.suiaan</u> management.km: zurich-	<u>s.eu-</u>				
				1.oraclecloud.cor	n (i)				1
Resources	Master Encry	ption Keys in OCI-SE	EC-WS-LAB-00 Compa	artment					
Master Encryption Keys	Create Key								
Secrets	Name	State	Protection Mode (i)	Algorithm	Created				
List scope			No iten	ns found.					
Compartment					SI	howing 0 i	tems <	1 of 1	>
OCI-SEC-WS-LAB-00								0	
trivadisbdsxsp (root)/Training/OCI-SEC-WS/OCI EC-WS-LAB-00	-5							Ŀ)

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.

E ORACLE Cloud	Search resources, services, documentation, and Marketp	lace	Switzerland North (Zurich) \vee	⊡ ↓ ⊘ ⊕ 9
Key Management & Secret Manager	nent » Vault » Vault Details	Create Key		<u>Help</u>
	vault-oci-sec-ws-lab-00	Create in Compartment		
	Edit Name Replicate Vault Add tags	OCI-SEC-WS-LAB-00	\$	
		trivadisbdsxsp (root)/Training/OCI-SEC-WS/OCI-SEC-WS-LAB-00		
	Vault Information Tags	Protection Mode ()		
		Software	\$	
	General information	Name		
	Compartment: trivadisbdsxsp (root)/Training	mek-oci-sec-ws-lab-00		
ACTIVE	OCID:nldgaq Show Copy	Key Shape: Algorithm ()	Key Shape: Length	
11/1/2 11/1/1/1/2025	Created: Wed, Oct 23, 2024, 12:30:30 UTC	AES (Symmetric key used for Encrypt and Decrypt)	256 bits	
111115-2019 [11] [12] [29]		Import External key		
		Create a new key by importing a wrapped file containing key data that matches the	e specified key shape. For more information, see Importing Keys.	
		Show advanced options		

Figure 21: » step_4

5. Verify Master Encryption Key is in State Enabled.

Master Encryption Key	s in OCI-SEC-WS-LA	B-00 Compartment			
Create Key					
Name	State	Protection Mode (i)	Algorithm	Created	
mek-oci-sec-ws-lab-00	Enabled	Software	AES	Wed, Oct 23, 2024, 12:38:46 UTC	;
				Showing 1 item < 1 of	12

Figure 22: » step_5

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).

Create Bucket	He
Bucket Name	
customer-managed-key-bucket	
Default Storage Tier	
O Standard	
The default storage tier for a bucket can only be specified during creation. Once set, you cannot change the storage tier in which a bucket resides. Learn more about storage tiers	
Enable Auto-Tiering	
Automatically move infrequently accessed objects from the Standard tier to less expensive storage. Learn more	
Enable Object Versioning	
Create an object version when a new object is uploaded, an existing object is overwritten, or when an object is deleted. Learn more	
Emit Object Evente	
Create automation based on object state changes using the Events Service.	
Uncommitted Multipart Uploads Cleanup Create a liferure rule to automatically delate uncommitted multipart unloads older than 7 days. Learn more	
oreare a mecycle rule to automaticany delete uncommitted monipart divided order than 7 days. <u>Learn more</u>	
Encryption	
Leaves all encryption-related matters to Oracle.	
Encrypt using customer-managed keys	
Requires a valid key from a vault that you have access to. Learn more	
Vault in OCI-SEC-WS-LAB-00 (Change compartment)	
vault-oci-sec-es-lab-00	\$
Master Encryption Key in OCI-SEC-WS-LAB-00 (Change compartment)	
mek-oci-sec-ws-lab-00	٢
	6

Figure 23: » step_6

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



Figure 24: » step_7

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.

Soot volume						
boot volume is a storage device that contains t	ne image that's use	ed to boot	a compute instance.			
Replace boot volume						
Boot volume name	State	Size	In-transit encryption	Created	Attached	Image
ci-fra-lab-ocisecws-00-webserver01 (Boot	Attached	150 GB	Enabled	Wed, Oct 23, 2024, 09:56:16 UTC	Thu, Oct 24, 2024, 05:02:52 UTC	Oracle-Linux-8.10-2024.0
volume)						

Figure 25: » step_8

Assign a new MEK.

Block Storage > Boot Volumes > Boot Volume Details Ci-fra-lab-ocisecws-00-webserver01 (Boot Volume) Image: Storage > Boot Volume Information Image: Storage > Boot Volume Information Image: Storage > Boot Volume Information Tags Availability domain: EUZ gEU-FRANKFURT-1-AD-1 Compartment: threatistassap (root)/Training/OCI-SEC-WSI-OCI-SEC	ORACLE Cloud	Search resources, services, documentation, and Marketplace	Germany Central (Frankfurt) 🗸	0	Δ (? €	• •
Ci-fra-lab-ocisecws-00-webserver01 (Boot Volume) Edit Create Instance Move resource Add tags Terminate Boot Volume Information Tags Availability domain: EUZg EU-FRANKFURT-1-AD-1 Compartment: threatisbdssxp (rootlyTraining/OCI-SEC-WSI-CAB-00 OCID:g625-g_Show Copy Volume group: None	Block Storage > Boot Volumes > Bo	ot Volume Details					Î
Edit Create Instance Move resource Add tags Terminate Boot Volume Information Tags Availability domain: EUZ gEU-FRANKFURT-1-AD-1 Hydrated: true Compartment: threatisbdsssp (root)/Training/OCI-SEC-WS/OCI-SEC-WS/LAB-00 Encryption key: Oracle-managed key Assign OCID:eg6z5q_Show_Copy Volume group: None		ci-fra-lab-ocisecws-00-webserver01 (Boot Volume)					2
Boot Volume Information Tegs Availability domain: EUZ gEU-FRANKFURT-1-AD-1 Availability domain: EUZ gEU-FRANKFURT-1-AD-1 Compartment: thrvalisbdsssp (root)/Training/OCI-SEC-WS/OCI-SEC-WS-LAB-00 Colp:eg6z5q_Show_Copy Volume group: None Volume group: None		Edit Create Instance Move resource Add tags Terminate					
Availability domain: EUZg/EU-FRANKFURT-1-AD-1 Hydrated: Irue Compartment: thradisbdsspp (root)/Training/OCL-SEC-WSI-CAB-00 Encryption key: Oracle-managed key Assign OCID:eg6z5q_Show_Copy Volume group: None	DV	Boot Volume Information Tags					
Compartment: trivadisbdsxsp (root)/Training/OCI-SEC-WS/OCI-SEC-WS-LAB-00 Encryption key: Oracle-managed key Assign OCID: ege25g Show Copy. Volume group: None		Availability domain: EUZg:EU-FRANKFURT-1-AD-1	Hydrated: true				8
OCID:eg6z5q Show Copy Volume group: None		Compartment: trivadisbdsxsp (root)/Training/OCI-SEC-WS/OCI-SEC-WS-LAB-00	Encryption key: Oracle-managed key Assign				
		OCID:eg6z5q Show Copy	Volume group: None				

Figure 26: » step_9

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

Assign master encryption key

ault Compartment		Vault	
OCI-SEC-WS-LAB-00	0	vault-oci-sec-es-lab-00	
vadisbdsxsp (root)/Training/OCI-SEC-WS/OCI-SEC-WS-L	AB-00	Master Encryption Key	
vadisbdsxsp (root)/Training/OCI-SEC-WS/OCI-SEC-WS-L laster Encryption Key Compartment	AB-00	Master Encryption Key	
vadisbdsxsp (root)/Training/OCI-SEC-WS/OCI-SEC-WS-L laster Encryption Key Compartment OCI-SEC-WS-LAB-00	AB-00	Master Encryption Key mek-oci-sec-ws-lab-00	

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

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-wsNN
- 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.

E ORACLE Cloud	Search resources, services, documentation, and Marketplace		Switzerland North (Zurich) 🗸 🕡 🌐 Q
Cloud Guard	Overview		
Overview Recipes Alerts Configuration	Security score rating () Excellent Security score 99	Risk score () 1400	Security recommendations ① Resolve Scanned host has open ports problems in target tgt-compartmen Resolve Instance has a public IP address problems in target tgt-compa View recommendations
Cuertes Threat monitoring Resources	Problems snapshot		Problems Grouped by Compartment
	8 Total	Ermical High Medium Low Minor	comp-doag-high-sec

Figure 28: » overview

5.1.2 Clone existing Oracle managed recipes

From left menu, select Recipes and Clone.

= ORACLE Cloud				Switzerland No	rth (Zurich) 🗸 👩 💭
Cloud Guard > Recipes					
Recipes	Detector recipes	e an existing Oracle managed recipe from the root compartmer	t Learn more		
Responder recipes	Clone				Q Filter by recipe name
	Recipe name	Oracle managed	Detector	Туре	Created
Scope			No items found.		
Compartment oci-sec-ws-lab-00					Showing 0 items < 1 of 1 >
trivadisbdsxsp (root)/training/oci-sec-ws/oci-sec- lab-00	N5-				
Include child compartments					
Tag filters add I cle	ear —				
the regiment of the					



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.

Clone detector recipe

	or Recipe (Oracle ma	naged)	0
Name			
OCI Activity Detecto	or Recipe - oci-sec-w	s-lab-00	80
Description Optional			
Description			
Compartment (i)			
			\$
oci-sec-ws-lab-00			
oci-sec-ws-lab-00 Add tags to organize	your resources. What	t can I do with tagging?	
oci-sec-ws-lab-00 Add tags to organize Tag namespace	your resources. <u>Wha</u> Tag key	<u>it can I do with tagging?</u> Tag value	

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).

- 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.

Cloning in trivadisbdsx	sp (root) () <u>(Cha</u>	nge compartment)	0
OCI Responder Recip	e (Oracle manageo	d)	0
lame			
OCI Responder Recip	e - oci-sec-ws-lab-	00	
Description Optional			
Description Optional			
Description Optional Description			
Description Optional Description			\$
Description Optional Description	ur resources. <u>Wha</u> t	t can I do with tagging?	\$
Description Optional Description			

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:

	ch resources, services, documentation, and Marketplace			Switz	erland North (Zurich) 🗸	0 L	1 (2)	• •
Cloud Guard > Recipes								
Recipes	Detector recipes To create your own recipe, clone an existing Oracle managed recipe from the root com	npartment Learn more						
Responder recipes	Clone					Q Filter by	y recipe nar	me
	Recipe name	Oracle managed	Detector	Туре	Created			
Scope	OCI Instance Detector Recipe - oci-sec-ws-lab-00	No	Instance Security	Standard	Sun, Oct 20, 2024, 07:16	5:11 UTC		:
Compartment	OCI Configuration Detectpr Recipe - oci-sec-ws-lab-00	No	Configuration	Standard	Sun, Oct 20, 2024, 07:15	5:20 UTC		
trivadisbdsxsp (root)/training/oci-sec-ws/oci-sec-ws-	OCI Activity Detector Recipe - oci-sec-ws-lab-00	No	Activity	Standard	Sun, Oct 20, 2024, 07:13	3:08 UTC		1
180-44						Showing 3 it	ems < 1	of 1 >
Include child compartments								
Tag filters add I clear								
no tag filters applied								

Figure 32: » step_4

Responder recipe:

			Switzerland North (Zurich) 🗸 🕢 💮
Cloud Guard » Recipes				
Recipes	Responder recipes To create your own recipe, clone an existing Oracle managed rec	ipe from the root compartment Learn more		
Responder recipes	Clone			Q Filter by recipe name
Same	Recipe name	Oracle managed	Created	
Compartment	OCI Responder Recipe - oci-sec-ws-lab-00	No	Sun, Oct 20, 2024, 07:20:23 UTC	1
oci-sec-ws-lab-00				Showing 1 item < 1 of 1 >
trivadisbdsxsp (root)/training/oci-sec-ws/oci-sec-w lab-00	а.			
Include child compartments				
Tag filters add cle	ar			

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

	irch resou	rces, services, documentation, and Marketp	lace			Switzerland North (Zuric	n)~ [5 <i>l</i>	¢ 0	۲	0
Cloud Guard > Configuration											
Configuration	Tar Target	gets is identify a compartment to be monitored by	y Cloud Guard. <u>Learn more</u>								
Settings Targets	Cr	eate target Delete					Q	Filter I	by target i	name	
Managed lists		Target name	Compartment	Туре	Monitoring coverage		Created				
Data masking				No items found	d.						
Scope	0 se	lected					Sho	wing 0	items <	(1 of 1	>
Compartment											
oci-sec-ws-lab-00											
trivadisbdsxsp (root)/training/oci-sec-ws/oci-sec-ws- lab-00											
Include child compartments											
Tag filters add I clear											

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.

	Search resources, services, documentation, and Marketplace	Switzerland North	(Zurich) 🗸 🤇	4	0	۲	0
Create target							
Basic information Configuration Review Review	Provide name, description, compartment and event configuration for the target. Target name ③ cg-tgt-oci-sec-ws-lab-00 Description Optional ④ Targets for Compartment oci-sec-ws-lab-00 Compartment ④ oci-sec-ws-lab-00						

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.

E ORACLE Cloud	Search resources, services, documentation, and Marketplace	Switzerland North (Zurich) 🗸 💿 🖨	0
Create target			
Basic information Configuration Review	Configure at least one recipe for this target.		
U LEILE	Posture and threat monitoring recipes	Clear	
	Detection recipes OCI Configuration Detector Recipe - od-sec-ws-lab-00 x	× 3	
	Instance Security recipe Instances All compute instances	Clear	
	Instance Security Recipe OCI Instance Detector Recipe - oci-sec-ws-lab-00	× 0	

Figure 36: » targets_3

Press Next at the bottom.

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

ORACLE Cloud	Search resources, services, documentation, and Marketplace	Switzerland North	(Zurich) 🗸 🖸	\$ ⊘	• •
Create target					
Basic information Configuration Review	Basic information Target name: cg-tgt-oci-sec-ws-lab-00 Description: Target for Compartment oci-sec-ws-lab-00 Compartment: oci-sec-ws-lab-00	EdB			
	Posture and threat monitoring information Detector recipe: OCI Configuration Detector Recipe - oci-sec-ws-lab-00	Edit			
	Instance Security Instances: All compute instances Instance Security recipe: OCI Instance Detector Recipe - oci-sec-ws-lab-00	Edt			

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

E ORACLE Cloud Sea	rch resources, services, documentatior	n, and Marketplace		Switzerland North (Zurich) 🗸 💿 🌐 🕻
Object Storage & Archive Storage	Buckets in oci-see	c-ws-lab-00 Compartment high-performance, durable, and secure data storage. Data is	uploaded as objects that are stored in buckets.	earn more
Buckets	Create Bucket			
Private Endpoints	Name	Default Storage Tier	Visibility	Created
List scope			No items found.	
Compartment				Showing 0 items 🛛 < 1 of 1 >
oci-sec-ws-lab-00				
trivadisbdsxsp (root)/training/oci-sec-ws/oci-sec-ws- lab-00				
Service logs Manage logs				
Resources: 0 (0 total logs) ③ Logs enabled: 0 Logs not enabled: 0				
Tag filters add clear				

Figure 38: » bucket_1

Press Create Bucket.

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

Create Bucket

public-bucket		
Default Storage Tier		
 Standard 		
Archive		
The default storage tier for a bucket can only	be specified during creation. Once set, you cannot change the storage tier in which a bucket resides	. Learn more
Enable Auto-Tiering		
Automatically move infrequently acces	ed objects from the Standard tier to less expensive storage. Learn more	
Enable Object Versioning		
Create an object version when a new of	ject is uploaded, an existing object is overwritten, or when an object is deleted. Learn more	
Emit Object Events		
Create automation based on object sta	e changes using the Events Service.	
Uncommitted Multipart Uploads	Cleanup	
Create a lifecycle rule to automatically	elete uncommitted multipart uploads older than 7 days. Learn more	
Encryption		
Encrypt using Oracle managed I	eys	
Leaves all encryption-related matters to	racle.	
 Encrypt using customer-manage Beguires a valid key from a yout that you 	I keys	
Requires a valid key nom a vault mat yo		
Resource logging		
Enable resource logging to allo	resource tracking troublesbooting and data insights	
Resource logging dis	abled	
Tags		
Add tags to organize your resource	s. What can I do with tagging?	
Tag namespace	Tag key Tag	value

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.

	ch resources, services, documentation,	and Marketplace		Switzerland North (Zu	ırich)∨ 🖸 🗘 곗 ⊕	0
Object Storage & Archive Storage	Buckets in oci-sec Object Storage provides unlimited, h	s-ws-lab-00 Compartment high-performance, durable, and secure data storage. Data is u	uploaded as objects that are stored in buckets.	Bucket public-bucket created success	sfully.	×
Buckets	Create Bucket					
Private Endpoints	Name	Default Storage Tier	Visibility	Created		
List scope	public-bucket	Standard	Private	Sun, Oct 20, 2	View Bucket Details	:
Compartment					Create Pre-Authenticated Request	>
oci-sec-ws-lab-00					Move Resource	
trivadisbdsxsp (roof)/training/oci-sec-ws/oci-sec-ws- lab-00					Edit Visibility	
					Add tags	
Service logs Manage logs					View tags	
Resources: 0 (0 total logs) ⓒ Logs enabled: 0 Logs not enabled: 0					Delete	
Tag filters add I clear						

Figure 40: » bucket_3

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

Object Storage provid	Edit Visibility	<u>Help</u>
Create Bucket Name public-bucket	Enabling public visibility will let anonymous and unauthenticated users access data stored in the bucket. Visibility Private Public Value Allow users to list objects from this bucket	
	Consider using pre-authenticated requests instead We recommend using pre-authenticated requests instead of public buckets. Pre-authenticated requests support additional authorization, expiry, and scoping capabilities not possible with public buckets. Learn more	
	Save Changes Cancel	

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.

	h resources, services, documentation, and Marketplace		Swit	zerland North (Zurich) 🗸 🤇	୭ 🌐 🛛
Object Storage & Archive Storage	Buckets in oci-sec-ws-lab-0 Object Storage provides unlimited, high-performance, o	00 Compartment durable, and secure data storage. Data is uploaded as ot	jects that are stored in buckets. Learn more		
Buckets	Create Bucket				
Private Endpoints	Name	Default Storage Tier	Visibility	Created	
List scope	public-bucket	Standard	A Public	Sun, Oct 20, 2024, 07:54:34 UTC	:
Compartment				Showing 1 item	< 1 of 1 >
oci-sec-ws-lab-00					
Service logs <u>Manage logs</u> Resources: 1 (2 total logs) () Logs enabled: 0 Logs not enabled: 2					
Tag filters add I clear					

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**.

	rch resources, services, documentation, and Marketpla	ю					Switzerlan	d North (Zurich) 🗸	$\overline{\mathbf{O}}$	4 0	2 🕀	0	
Cloud Guard > Alerts													
Alerts	Problems	at could potentia	lly cause a securit	v threat. All list scope :	und filter settings an	e nersistent and will remain in n	ace until they	are cleared or reset	earn moi	10			
Recommendations	First detected start time First detected end time Last detected end time												
Responder activity	[[8	E Sep 20, 2024 08:02 UTC			24 08:02 UTC		Oct 20, 2024 08:02 UTC					
Scope	Files Enlers search filters												
Compartment	Reset all												
oci-sec-ws-lab-00 🗘													
trivadisbdsxsp (root)/training/oci-sec-ws/oci-sec-ws- lab-00	Manage columns Mark as resolved Dismiss												
Include child compartments	Problem name	Risk level .	Detector type	Resource	Target	Regions	Labels						
Status		-	bettettet type		in get						antes meste	_	
Open 🗘	Bucket is public	 Critical 	Configuration	public-bucket	i-sec-ws-lab-00	Switzerland North (Zurich)	CIS_OCI_V	CIS_OCI_V1.1_OBJECTSTORAGE,ObjectStorage,CIS_OC					
Resource type	Database is not registered in Data Safe	Medium	Configuration	ws-01-atp23ai01	i-sec-ws-lab-00	Germany Central (Frankfurt)	Database Security						
All	VCN has InternetGateway attached	Low	Configuration	lab-ocisecws-00	i-sec-ws-lab-00	Germany Central (Frankfurt)	Network						
	O selected							s	nowing 3	items a	∠ Page 1	1 >	

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*.



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.

Remediate	<u>Help</u>
Problem: Bucket is public	
Remediation responder rule (i)	
Make Bucket Private	\$
Required policy statements (i) User doesn't have privileges to inspect or manage policies in tenancy.	
Input settings (i)	
✓ Post Remediation Notification ①	

Figure 45: » alert_3

Confirm.


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

	h resources, services, documentation, and Marketplace		Swi	tzerland North (Zurich) \checkmark		2	0
Object Storage & Archive Storage	Buckets in OCI-SEC-WS-LA Object Storage provides unlimited, high-performance, d	AB-00 Compartment lurable, and secure data storage. Data is uploaded as ot	jects that are stored in buckets. Learn more				
Buckets	Create Bucket						
Private Endpoints	Name	Default Storage Tier	Visibility	Created			
List scope	public-bucket	Standard	Private	Sun, Oct 20, 2024, 07:54:3	4 UTC		:
Compartment				5	Showing 1 item	< 1 of 1	>
OCI-SEC-WS-LAB-00 \$							
trivadisbdsxsp (root)/Training/OCI-SEC-WS/OCI-S EC-WS-LAB-00							
Service logs Manage logs							
Resources: 1 (2 total logs) () Logs enabled: 0 Logs not enabled: 2							
Tag filters add clear							

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.

- 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-wsNN
- 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.

= ORACLE Cloud	Search resources, services, documentation, and Marketplace		Switzerland North (Zurich) 🗸 💮 🌐 🔒
Cloud Guard	Overview		
Overview Recipes Alerts Configuration	Security score rating ① Excellent	Risk score (i)	Security recommendations ① • Resolve Scanned host has open ports problems in target (gf-compartmen • Resolve Instance has a public IP address problems in target (gf-compa
Queries Threat monitoring Resources	Problems snapshot		Problems Grouped by Compartment
	8 Total	E Critical High Medium Low Minor	comp-doag-high-sec

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

	earch resources, services, documentation, and Ma	irketplace			Switzerland North (Zurich)	× ⊡ ↓ ? ⊕ 9
Cloud Guard » Configuration						DINTIZ DININ
Configuration	Targets Targets identify a compartment to be monito	red by Cloud Guard. Learn more				
Settings Targets	Create target Delete					Q Filter by target name
Managed lists	Target name	Compartment	Туре	Monitoring coverage	Created	
Data masking	cg-tgt-oci-sec-ws-lab-00	OCI-SEC-WS-LAB-00	OCI	1/4 <u>View</u>	Sun, Oct 20, 2024, 07:46:37	UTC :
Scope	0 selected					Showing 1 item < 1 of 1 >
Compartment						
OCI-SEC-WS-LAB-00						
trivadisbdsxsp (root)/Training/OCI-SEC-WS/OCI-S EC-WS-LAB-00						
Include child compartments						
Tag filters add I clea	ī					

Figure 49: » step_1

Select your created target an scroll at the bottom.

Resources	Configuration							
Configuration	Compartments							
	OCI-SEC-WS-LAB-00							
	Posture and threat monitoring Instance Security							
	Detector recipes For each target, only one recipe of the same type can be added. To add a new recipe of the same type, remove an existing one. Learn more.							
	Add recipes							
	Recipe name		Oracle managed	Detector	Туре	Created		
	OCI Configuration Detector Recipe - oci-sec-ws-lab-00		No	Configuration	Standard	Sun, Oct 20, 2024, 07:46:37 UTC		
						Showing 1 item < 1 of 1 >		
	Responder recipes For each larget, only one recipe of the same type can be added. To add a new recipe of the same type, remove an existing one. Learn more Add recipes							
	Recipe name	Oracle mana	ged			Created		
			No items found.					
						Showing 0 items \langle 1 of 1 \rangle		

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.

Add responder recipe	
Choose a responder recipe to assign to target cg-tgt-oci-sec-ws-lab-00 Responder recipe (i)	
OCI Responder Recipe - oci-sec-ws-lab-00	× \$
Add recipes Cancel	

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*.

E ORACLE Cloud				Switzerland North (Zurich) 🗸 🕢 🖓	• •
Cloud Guard > Targets > Target deta	ils » Responder recipe					^
R	OCII Responder Recipe - oci Details OCID:Ifgpd22b4a <u>Show Copy</u> Create: Sun, Oci 20, 2024, 08:35:51 UTC Compartment: OCI-SEC-WS-LAB-00	sec-ws-lab-00				
Resources	Responder rules					
Responder rules					Q Filter by responder	rule
	Responder rule	Туре	Status	Conditional group		- 1
	Cloud Event	NOTIFICATION	Enabled	No	:	~
	Delete IAM Policy	REMEDIATION	Enabled	No	1	~
	Delete Internet Gateway	REMEDIATION	Enabled	No	:	~
	Delete Public IP(s)	REMEDIATION	Enabled	No	:	~
	Disable IAM User	REMEDIATION	Enabled	No	:	~
	Enable DB Backup	REMEDIATION	Enabled	No	:	6
	Make Bucket Private	REMEDIATION	Enabled	No		
	Rotate Vault Key	REMEDIATION	Enabled	No	Edit	~
	Stop Compute Instance	REMEDIATION	Enabled	No	:	~
	Terminate Compute Instance	REMEDIATION	Enabled	No	:	~
					Showing 10 items < 1	of 1 >
Terms of Use and Privacy Cookie Preference	ies .			Copyri	ght © 2024, Oracle and/or its affiliates. All ri	ghts 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

Configure responder rule

Name: Make Bucket Private
Description: Changes the Object Storage Bucket's visibility from public to private
Status: Disabled

	lired policy statements (i)
(!)	User doesn't have privileges to inspect or manage policies in tenancy.
Setti	ng
Rule trig	iger
Ask	me before executing rule
Exec	ute automatically
Resp	onder executes automatically when Make Bucket Private is prompted in compartment OCI-SEC-WS-LAB-00.
()	Selecting execute automatically grants the responder permissions to modify all resources, without further confirmation, to correct the rule violation as soon as it is detected. To limit the scope of this action to a subset of the resources, add one or more conditional group statements.

Figure 53: » step_5

Farameter	Operator	List		
Region	\$ In	\$ Custom list	\$ ×	
Value (i)				
ou frankfurt 1				ſ
eu-irankiun-i				



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.

Help

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

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

Create Bucket	<u>Help</u>
Bucket Name	
private-bucket	
Default Storage Tier	
Standard	
○ Archive	
The default storage tier for a bucket can only be specified during creation. Once set, you cannot change the storage tier in which a bucket resides. Learn more about storage tiers	
Enable Auto-Tiering	
Automatically move infrequently accessed objects from the Standard tier to less expensive storage. Learn more	
Enable Object Versioning	
Create an object version when a new object is uploaded, an existing object is overwritten, or when an object is deleted. Learn more	
Emit Object Events	
Create automation based on object state changes using the Events Service.	
Uncommitted Multipart Uploads Cleanup	
Create a lifecycle rule to automatically delete uncommitted multipart uploads older than 7 days. Learn more	
Encryption	
Encrypt using Oracle managed keys	
Leaves all encryption-related matters to Oracle.	
Encrypt using customer-managed keys	
Requires a valid key from a vauit that you have access to 1 earn more	

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.

Dbject Storage provid	Edit Visibility	<u>Help</u>	
Create Bucket	Enabling public visibility will let anonymous and unauthenticated users access data stored in the bucket.		
Name	Visibility		Created
private-bucket	Public		Sun, Oct 20, 2024, 08
public-bucket	✓ Allow users to list objects from this bucket		Sun, Oct 20, 2024, 07
	Consider using pre-authenticated requests instead We recommend using pre-authenticated requests instead of public buckets. Pre-authenticated requests support additional authorization, expiry, and scoping capabilities not possible with public buckets. Learn more		
	Save Changes Cancel		



Press Save Changes at the bottom.

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

	rch resources, services, documentation	n, and Marketplace		Switzerland North (Zurich) 🗸 🕡 🌐
Object Storage & Archive Storage	Buckets in OCI-S	EC-WS-LAB-00 Compartment high-performance, durable, and secure data storage. Data is	uploaded as objects that are stored in buckets. \underline{L}	eam more
Buckets	Create Bucket			
Private Endpoints	Name	Default Storage Tier	Visibility	Created
List scope	private-bucket	Standard	A Public	Sun, Oct 20, 2024, 08:50:33 UTC
Compartment	public-bucket	Standard	Private	Sun, Oct 20, 2024, 07:54:34 UTC
OCI-SEC-WS-LAB-00				Showing 2 items 🛛 < 1 of 1 🗲
trivadisbdsxsp (root)/Training/0CI-SEC-WS/0CI-S EC-WS-LAB-00				
Service logs <u>Manage logs</u> Resources: 2 (4 total logs) ⊙ Logs enabled: 0 Logs not enabled: 4				
Tag filters add clear				

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
------------------------	----------------	-------------	-----------	----------

	irch resour	ces, services, documenta	tion, and Marketplace					Switze	erland North (Zurich) 🗸	$\overline{\mathbf{O}}$	\$ ⊘	••
Cloud Guard > Alerts						利加加	JIIII A			Di	127	
Alerts	Respon	sponder activity indicates the	/ity e actions taken or could be t	aken by Cloud Gua	rd for identified problem. <u>Lear</u>	n more						
Recommendations	Tim	e create range start	-	Time created range	end	Time completed	range start		Time completed range end			
Responder activity	S	ep 20, 2024	8	Oct 20, 2024	8							8
(coponaci adanti)	Filte	ers										
Scope	E	Enter search filters										
Compartment	Res	set all										
OCI-SEC-WS-LAB-00 \$												
trivadisbdsxsp (root)/Training/OCI-SEC-WS/OCI-S EC-WS-LAB-00	Mai	nage columns Skip (execution									
Include child compartments		Responder name	Responder activity OCI	Resource	Region	Execution status	Execution type	Problem name	Time created	•	Time co	mpleted
		Cloud Event	6qs7g3skiqvr454h7epq	private-bucket	Switzerland North (Zurich)	Succeeded	Automated	Bucket is public	Sun, Oct 20, 2024, 08:53	2:38 UTC	Sun, Oc	:t 20, 2024, (
		Make Bucket Private	tdidlh36uaavtq4i33zq	private-bucket	Switzerland North (Zurich)	Succeeded	Automated	Bucket is public	Sun, Oct 20, 2024, 08:52	2:38 UTC	Sun, Oc	:t 20, 2024, (
		Make Bucket Private	ocid1.cloudguardrespondere 1.amaaaaaasijhdmsqgp6rgt3	xecution.oc1.eu-zurich co2rz5acwivkp26ka24	Horth (Zurich)	Succeeded	Manual	Bucket is public	Sun, Oct 20, 2024, 08:2	1:19 UTC	Sun, Oc	t 20, 2024, (
		Make Bucket Private	x6q Copy		Close lorth (Zurich)	Succeeded	Manual	Bucket is public	Sun, Oct 20, 2024, 08:19	52 UTC	Sun, Oc	:1 20, 2024, (

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

	ch resources, services, documentation, and Marketplace			Switzerland North (Zurich) 🗸 🖸 🌐 🧕
Object Storage & Archive Storage	Buckets in OCI-SEC-WS-L Object Storage provides unlimited, high-performance,	AB-00 Compartment	objects that are stored in buckets. Learn more	
Buckets	Create Bucket			
Private Endpoints	Name	Default Storage Tier	Visibility	Created
List scope	private-bucket	Standard	Private	Sun, Oct 20, 2024, 08:50:33 UTC
Compartment	public-bucket	Standard	Private	Sun, Oct 20, 2024, 07:54:34 UTC
OCI-SEC-WS-LAB-00 \$				Showing 2 items < 1 of 1 >
trivadisbdsxsp (root)/Training/OCI-SEC-WS/OCI-S EC-WS-LAB-00				
Service logs Manage logs				
Resources: 2 (4 total logs) () Logs enabled: 0 Logs not enabled: 4				
Tag filters add I clear				

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.

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-wsNN
- 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

Cloud S	iearch resources, services	s, documentation, and Marketplace		Switzerland N	lorth (Zurich) 🗸		¢ 0	@
Notifications	Topics in	OCI-SEC-WS-LAB-00	compartment	200200				
Topics	The <u>Notifications s</u> are breached, or to	service helps you broadcast messages to dis directly publish a message. A <u>topic</u> is a com	tributed components through a publish-s imunication channel for sending messag	subscribe pattern. Use Notifications to ge ges to the <u>subscriptions</u> in the topic.	et notified when eve	ent rules an	e triggered	or alarms
Subscriptions	Create Topic							
List scope	Name	Description	State	Topic OCID	Created			
Compartment			No items foun	ıd.				
OCI-SEC-WS-LAB-00					SI	howing 0 ite	ems < F	Page 1 >
thradibidasap (rool)/Training/OCI-SEC-WSIOCI- EC-WSLAB-00								

Figure 60: » step_1

Add details, Create.

	Search resources, services, documentation, a	and Marketplace	Switzerland North (Zurich) \checkmark	0 ¢	0
Notifications	Topics in OCI-SE	Create Topic			<u>Help</u>
Topics	The <u>Notifications service</u> helps you are breached, or to directly publish	Name			
Subscriptions	Create Topic	Topic name must contain fewer lihan 256 characters. Only alphanumeric characters plus hyphens (-) a	nd underscores (_) are allowed.		
List scope	Name De:	Description Optional Topic for Compartment OCI-SEC-WS-LAB-00			
Compartment OCI-SEC-WS-LAB-00		Description must contain fewer than 256 characters. So Show advanced options.			
trivadisbdsxsp (root)/Training/OCI-SEC-WS/OCI EC-WS-LAB-00	-5	① Once the topic is created, an administrator needs to create an identity p	policy to enable access.		
		Create <u>Cancel</u>			
Terms of Use and Privacy Cookie Preferences	5		Copyright © 2024, Ora	icle and/or its affiliate	es. All rights reserved.

Figure 61: » step_2

The state of the new created topic is active.

T				ETHIN ALL	
Notifications IO	pics in DEV1-0	JCI-SEC-WS-LAB-00 compartm	ent		
Topics are b	Notifications service helps yo preached, or to directly publis	u broadcast messages to distributed components through a publ h a message. A <u>topic</u> is a communication channel for sending me	lish-subscribe pattern. Use essages to the <u>subscriptio</u>	 Notifications to get notified when <u>ns</u> in the topic. 	event rules are triggered or alarms
Subscriptions	Create Topic				
List scope Na	me	Description	State	Topic OCID	Created -
Compartment top	ic-oci-sec-ws-lab-001	Topic for Compartment OCI-SEC-WS-LAB-00	Active	b7pbjfm7wa Show Copy	Tue, Oct 22, 2024, 12:29:40 UTC
DEV1-OCI-SEC-WS-LAB-00					
trivadisbdsxsp (root)/Training/OCI-SEC-WS/DEV1-					Showing 1 item < Page 1 >

Figure 62: » step_3

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

	ic				×	Switzerland North (Zurich)	~ 🖸	۵	? ∉	₿0
Notifications > Topics > Topic Details										Î
	topic-oci-sec-w	vs-lab-001								
	Publish Message Move	Resource Add tags Dele	ete							
	Topic Information	Tags								
	Description: Topic for Co	mpartment OCI-SEC-WS-LAB-00	0 /							2
	OCID:b7pbjfm7wa Sho	<u>ow Copy</u>								83
ACTIVE	Short Topic ID: - Show	<u>Copy</u>								22
	Compartment: DEV1-OC	I-SEC-WS-LAB-00								92
	Created: Tue, Oct 22, 202	24, 12:29:40 UTC								
Resources	Subscriptions									
Subscriptions	Create Subscription									
Metrics	Subscription OCID		State	Protocol	endpoin	nt Creat	ed			
List scope				No items found.						
Compartment						5	Showing 0 it	ems <	Page 1	- <1
Terms of Use and Privacy Cookie Preferences						Copyright © 2024	Oracle and/or	its affiliate	s. 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.

topi	c	\times Switzerland North (Zurich) \vee \bigodot \bigwedge	7 (?)	۲	0
S		Create Subscription		Hel	Þ
	topic-oci-sec-ws-l	View steps for creating subscriptions and learn about supported subscription protocols.			
	Publish Message Move Reso	Configure Subscription			
	Topic Information Tags	Protocol		\$	
	Description: Topic for Compart OCID:b7pbjfm7wa Show C	Email martin.x.berger@accenture.com			
	Short Topic ID: - Show Copy, Compartment: DEV1-OCI-SEC Created: Tue, Oct 22, 2024, 12	Email notifications use the sender "noreply" at a region-specific notification domain. Example sender: noreply@notification.us-ashburn-1.oci.oraclecloud.com <u>Creating a subscription for Email.</u>			
	Subscriptions	2 Show advanced options			
	Create Subscription			C	
	Subscription OCID			::	:
		Create Cancel			
nces		Copyright © 2024, Oracle and/or its aff	filiates. All ri	ghts reserv	/ed.

Figure 64: » step_5

Confirm the subscription

[Extern	nal] Oracle Cloud Infrastructure Notif	icatio	ons Service Su	ubscription Conf	🕼 Zusammenfassen
	noreply@notification.eu-zurich-1.oci.oracle	3	← Antworten) Allen antworten	\rightarrow Weiterleiten 🗊
	An Berger, Martin				Di 22.10.2024 14:34
	External email Inspect h	ofore	opening any lin	ke or attachmente	

You have chosen to subscribe to the topic: topic-oci-sec-ws-lab-001 (Topic OCID: ocid1.onstopic.oc1.eu-zurich-1.amaaaaaaasijhdmqav6fy62rpa3wsyk4opsrjq3tyihgyiqvh6rb7pbjfm7wa)

To confirm this subscription, click or visit the link below (If this was in error, you can ignore this message): <u>Confirm subscription</u>

--

Please do not reply directly to this email. If you have any questions or comments regarding this email, contact your account administrator.

Figure 65: » step_6



Subscription confirmed

Hi,

You have subscribed martin.x.berger@accenture.com to the topic: topic-oci-sec-ws-lab-001

 $Topic \ OCID: ocid 1. on stopic. oc 1. eu-zurich-1. amaaaaaaasijhdm qav 6fy 62rpa 3 wsyk 4 op srjq 3 tyih gyiq vh 6rb 7 pb jfm 7 was an amaaaaaa sijh dm qav 6fy 62rpa 3 wsyk 4 op srjq 3 tyih gyiq vh 6rb 7 pb jfm 7 was an amaaaaaa sijh dm qav 6fy 6 2 rpa 3 wsyk 4 op srjq 3 tyih gyiq vh 6rb 7 pb jfm 7 was an amaaaaaa sijh dm qav 6fy 6 2 rpa 3 wsyk 4 op srjq 3 tyih gyiq vh 6rb 7 pb jfm 7 was an amaaaaaaa sijh dm qav 6fy 6 2 rpa 3 wsyk 4 op srjq 3 tyih gyiq vh 6rb 7 pb jfm 7 was an amaaaaaa sijh dm qav 6fy 6 2 rpa 3 wsyk 4 op srjq 3 tyih gyiq vh 6rb 7 pb jfm 7 was an amaaaaaa sijh dm qav 6fy 6 2 rpa 3 wsyk 4 op srjq 3 tyih gyiq vh 6rb 7 pb jfm 7 was an amaaaaaaa sijh dm qav 6fy 6 2 rpa 3 wsyk 4 op srjq 3 tyih gyiq vh 6rb 7 pb jfm 7 was an amaaaaaa sijh dm qav 6fy 6 2 rpa 3 wsyk 4 op srjq 3 tyih gyiq vh 6rb 7 pb jfm 7 was an amaaaaaaa sijh dm qav 6fy 6 2 rpa 3 wsyk 4 op srjq 3 tyih gyiq vh 6rb 7 pb jfm 7 was an amaaaaaaa sijh dm qav 6fy 6 2 rpa 3 wsyk 4 op srjq 3 tyih gyiq vh 6rb 7 pb jfm 7 was an amaaaaaaa sijh dm qav 6fy 6 2 rpa 3 wsyk 4 op srjq 3 tyih gyiq vh 6rb 7 pb jfm 7 was an amaaaaaaa sijh dm qav 6fy 6 2 rpa 3 wsyk 4 op srjq 3 tyih gyiq vh 6rb 7 pb jfm 7 was an amaaaaaaa sijh dm qav 6fy 6 2 rpa 3 wsyk 4 op srjq 3 tyih gyiq vh 6rb 7 pb jfm 7 was an amaaaaaa sijh dm qav 6fy 6 2 rpa 3 wsyk 4 op srjq 3 tyih gyiq vh 6rb 7 pb jfm 7 was an amaaaaaa sijh dm qav 6fy 6 2 rpa 3 wsyk 4 op srjq 3 tyih gyiq vh 6rb 7 pb jfm 7 was an amaaaaaaa sijh dm qav 6fy 6 2 rpa 3 wsyk 4 op srjq 3 tyih gyiq vh 6rb 7 pb jfm 7 was an amaaaaaa sijh dm qav 6fy 6 2 rpa 3 wsyk 4 op srjq 3 tyih gyiq 4 tyih gyid 4 tyih gyiq 4 tyih gyiq 4 ty$

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.

ORACLE Cloud Search resources, services, documentation, and Marketplace	Switzerland North (Zurich) \checkmark	⊡ ↓ ? ⊕ 9
Create Rule		Help
Display Name		^ _
rule-oci-sec-ws-lab-00-cloudguard		
Description		
Describe what the rule does. Example: Sends a notification when backups complete.		

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

Rule Conditions					
Limit the events that trigger actions b	by defining conditions based on	event types, attributes, and filter tags. Learn more			Rule Logic
Condition	Service Name	Event Type			
Event Type 🗘	Cloud Guard	C Detected - Problem x Dismissed - Problem Remediated - Problem x	× × ≎	×	MATCH event WHERE (evenType EQUALS ANY OF (com.oraclecloud.cloudguand.problemdtected, com.oraclecloud.cloudguand.problemdismissed, com.oraclecloud.cloudguand.problemremediated
			+ Another Con	dition) ' <u>View example events (JSON)</u>
					Validate Rule



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)

ctions trigger for the specifie	d event conditio	ns. Learn more.		PAY	
ction Type		Notifications Compartment	Торіс		
Notifications	\$	MGB-DEV-OCI-SEC-WS-LAB-00 \$	topic		\$
				-	- Another Action



5.3.4 Test

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

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

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-wsNN
- 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.



Figure 70: » step_1

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

Register Auton	omous databases
Select database Connectivity option Connectivity option Act security rule Bediex.act.submit Bediex.act.submit Bediex.act.submit	Data Safe target information ③ Select diabase in S0E-DEV-OCI-SEC-WS-LAB-00 (Change compartment) adb-fra-lab-soe-devocisecvs-00-atp23a01 Data Safe target dipplay name adb-fra-lab-soe-devocisec-00-atp23a01 Compartment S0E-DEV-OCI-SEC-WS-LAB-00 ************************************
	E Show advanced options Image: The selected database is configured to be securely accessible from everywhere. Steps 2 (Connectivity option') and 3 (Add security rule) are not necessary and will be skipped.

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.



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





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

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-wsNN
- 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.

ecurity center	Security assessment		
Dashboard	Evaluate the security posture of your database	es and receive recommendations on how to mitigate the identified risks	s. <u>Learn more</u> Take the tour
Security assessment	Risk level	Risks by category	
Jser assessment	3.	0%	
Data discovery	-18	396 33%	
Data masking	67 Findings	6 Risks	R
Activity auditing		570/	
SQL Firewall	73%	6770	<u>.</u>
Alerts	High: 0 Low: 4 Eva	aluate: 49 User accounts: 4 DB configuration: 2	
elated resources	Advisory. 12 Der	eneu.u	
	Top 5 common security controls		
Assessment history	Patch compliance 1		
Schedules	Auditing 1		
	Password discipline		
	Encryption in-transit 1		
st scope	Encryption at-rest	2	
ompartment	Target database	5 5	
	Potential risk Advisory	erred	



- 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.

Target database	Deviation from baseline	Last assessed time	High risk	Medium risk	Low risk	Advisory	Evaluate
adb-fra-lab-soe- devocisecws-00- atp23ai01	No baseline set <i>OR</i> No comparison done (i)	Thu, 21 Nov 2024 10:52:13 UTC <u>View report</u>	-	2	4	12	49
				Disc	laving 1 sec	urity assessment	ts <1of1

Figure 76: Target summary



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).

✓ Users	with Grant Option
Limit propagat	ion of access rights
Status:	PASS
Summary:	No users found who have been granted privileges to perform security critical actions with grant option.
Remarks:	Account parmission to grant privileges within the database is an administrative function. Minimizing the number and privileges of administrative accounts reduces the chances of privileged account exploitation. User accounts that require WITH GRANT OFTIOR privileges backlo belong to sanctioned users who can propagata access rights to important objects. Limiting the propagation of access rights ensures that users can't continuously grant access to objects they don't own without restriction.
References:	Oracle Best Practice DISA STIG: V-219829, V-237715

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").

Update risk for finding		
Finding: Users with Grant Option Summary: No users found who have been granted privileges Current risk level: Pass () Oracle defined risk level: Pass ()	to perform security critical actions with grant option.	
Defer risk	Change risk	
Defer the risk until the expiration date you define be- low or until you revise it.	Change risk of finding to a different level	~
New risk level ① Medium Justification Optional		×≎
Please provide a justification for changing the risk for this fin	ding	le
Expiration date Optional		
		8
Save Close		

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.



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;

L E A _a ♥ ① Data Load e^{it} $\theta \theta$ ⑦ 1 GRANT alter any role TO public; 2 CREATE USER scott NO AUTHENTICATION;	-
1 GRANT alter any role 10 public; 2 CREATE USER scott NO AUTHENTICATION;	-
Query Result Script Output DBMS Output Explain Plan Autotrace SQL History (9
الله عن الله عن الله عن الله عن الله عن الله عن ال	
Grant succeeded.	Ū
Elapsed: 00:00.008	í
User SCOTT created.	6
Elapsed: 00:00:06.876	í

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.

Refresh	now	
Assessm	nent details	
Save latest a	ssessment	
SA_202411	212352	
(i) This up name.	dates the latest assessment for this target database, and also saves it using the provided assessment	

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.

• 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-wsNN
- 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:

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

	ierent in database accounts	. Assess the pot	ential risk a compromised of	or misused a	account would	Take the t			
		1000			<u> </u>				
New authori	zation required								
To view the ava	ailable schema access detai	Is of the user you	u will need permissions on	the data-safe	e-security-policy-	reports resource in the			
compartment of	of the target database.								
Allow grou	p <user-group> to read da</user-group>	ta-safe-security	y-policy-reports in compa	rtment <co< td=""><td>mpartment-name</td><td>3> me></td></co<>	mpartment-name	3> me>			
· Allow grou	p cuser-group> to inspect	uata-sale-secu	inty-policy-reports in con		comparament-ne				
Please re-run t	he privilege script for non-A	DB databases L	earn more						
-1010-00-0	3.111.111.111.111			022-1	11111111				
otential user risk									
			User role	s					
		4 70/	DBA	A		4			
45.8%	24 Users	.7%	DV admi	n		6			
			Audit admi	n		5			
	12.5%			0 1	2 3	4 5 6			
				BBA: 4	DV admin: 6	Audit admin: 5			
Critical: 1	0 📕 High: 3 📕 Medium: 0	Low: 11							
						c			
						L			
	Target summary	Notifications							
Risk summary	Targot Garminary								
Risk summary	larger barninary								
Risk summary Potential risk	Target databases	Users	Privileged users	DBA	DV admin	Audit admin			
Nisk summary Potential risk Critical	Target databases	Users 10	Privileged users	DBA	DV admin	Audit admin			
Nisk summary Potential risk Critical High	Target databases 2 2 2	Users 10 3	Privileged users 10 3	DBA 4	DV admin 4 2	Audit admin 5 -			
Nisk summary Potential risk Critical High Medium	Target databases 2 2 -	Users 10 3 -	Privileged users 10 3 -	DBA 4	DV admin 4 2 -	Audit admin 5 -			
Risk summary Potential risk Critical High Medium Low	Target databases 2 2 - 2 2	Users 10 3 - 11	Privileged users 10 3	DBA 4	DV admin 4 2	Audit admin 5			



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.

- 2. Review the list of users and their associated risk levels:
 - Status Last login time User name User type DBA DV Audit Potential risk Schema access User profile Audit records 0 LOCKED PRIVILEGED, SCHEMA нан ADB APP STO ORA PROT LOW Ø 0 IVILEGED 0 CRITICAL OPEN Thu, 21 Nov 2024 All schemas LOW LOCKED DCAT ADMIN 0 CRITICAL OPEN PRIVILEGED, Ø CRITICAL CRITICAL OPEN NSCATA PRIVILEGED, OPEN SCHEMA LOW ying 8 users < 1 of 1 >
 - 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

• 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:

• 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.

Refresh now	
Assessment details	
Assessment name	
UA_20241122011	
(i) This updates the latest assessment for this target database, and also saves it using the provided assessment name.	
Refresh now Cancel	

Figure 86: Refresh User Assessment

- 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.

User name	User type	DBA	DV admin	Audit admin	Potential risk	Status	Last login time	Schema access	User profile	Audit records
ADBSNMP	PRIVILEGED, SCHEMA		0		HIGH	LOCKED		ADBSNMP	ORA PROTECTED PROFILE	View activi
ADB APP_ST ORE	SCHEMA				LOW	LOCKED		ADB APP STO RE	ORA PROTECTED	View activi
ADMIN	PRIVILEGED	0	0	0	CRITICAL	OPEN	Thu, 21 Nov 2024 23:07:34 UTC	Al schemas	ORA ADMIN PROFI	View activi
XCAT ADMIN	SCHEMA	-	-	-	LOW	LOCKED		DCAT_ADMIN	ORA PROTECTED PROFILE	View activ
2S\$ADMIN	PRIVILEGED			0	CRITICAL	OPEN	Thu, 21 Nov 2024 23:12:14 UTC	All schemas	ORA EXTAPP PRO EILE	View activi
BGADMIN	PRIVILEGED, SCHEMA	0	0		CRITICAL	LOCKED		Allschemas	ORA PROTECTED PROFILE	View activ
1B	PRIVILEGED				CRITICAL	OPEN		Al schemas	DEFAULT	View activ
RMANSCATA .OG	PRIVILEGED, SCHEMA				CRITICAL	OPEN		RMANSCATALO G	ORA PROTECTED PROFILE	View activi
RMAN\$VPC	SCHEMA				LOW	OPEN		RMANSCATALO G	DEFAULT	View activ
								RMAN\$VPC		

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.

		admin	admin	risk	outus	cast rogin time	access	User prome	records
PRIVILEGED, SCHEMA		0		HIGH	LOCKED		ADBSNMP	ORA PROTECTED PROFILE	View acti
SCHEMA				LOW	LOCKED		ADB APP STO RE	ORA PROTECTED. PROFILE	View acti
PRIVILEGED	0	0	0	CRITICAL	OPEN	Thu, 21 Nov 2024 23:07:34 UTC	All schemas	ORA ADMIN PROFI	View.act
SCHEMA	-	-		LOW	LOCKED		DCAT_ADMIN	ORA PROTECTED PROFILE	View act
PRIVILEGED			0	CRITICAL	OPEN	Thu, 21 Nov 2024 23:12:14 UTC	All schemas	ORA EXTAPP PRO EILE	View act
PRIVILEGED, SCHEMA	0	0		CRITICAL	LOCKED		Allschemas	ORA PROTECTED PROFILE	View.act
PRIVILEGED				CRITICAL	OPEN		Allschemas	DEFAULT	View.act
PRIVILEGED, SCHEMA				CRITICAL	OPEN		RMANSCATALO G	ORA PROTECTED PROFILE	View act
SCHEMA				LOW	OPEN		RMANSCATALO G	DEFAULT	View act
							BMAN\$VPC		
	PRAILEGED, SCHEMA SCHEMA PRWILEGED SCHEMA PRWILEGED, SCHEMA SCHEMA SCHEMA	PRVNLEGED - SCHEMA - SCHEMA - PRVNLEGED Image: Comparison of the comparison	PRVLIGED · · · SCHEMA · · · SCHEMA · · · PRVLIGED · · · SCHEMA · · · SCHEMA · · · PRVLIGED · · · PRVLIGED · · · PRVLIGED · · · PRVLIGED · · · SCHEMA · · · SCHEMA · · · SCHEMA · · ·	PRVNLGGD · · · · SCHEMA · · · · SCHEMA · · · · PRVNLGGD · · · · SCHEMA · · · · PRVNLGGD · · · · SCHEMA · · · · SCHEMA · · · ·	Pervise Software ·	PRIVLEGED - - HGH LOCKED SCHEMA - - LOW LOCKED PRIVLEGED - - LOW LOCKED PRIVLEGED - - - LOW LOCKED PRIVLEGED - - LOW LOCKED PRIVLEGED - - LOW LOCKED PRIVLEGED - - - CRITCAL CRITCAL CRITCAL CRITCAL CRITCAL COCKED PRIVLEGED - - CRITCAL CRITCAL CRITCAL COCKED PRIVLEGED - - CRITCAL CRITCAL COCKED PRIVLEGED - - CRITCAL CRITCAL CRITCAL PRIVLEGED - - CRITCAL CRITCAL CRITCAL PRIVLEGED - - CRITCAL CRITCAL CRITCAL CRITCAL PRIVLEGED - - CRITCAL CRITCAL CRITCAL CRITCAL	PRIVILATION · · INGH LOCKED · SCHEAMA · · · LOCKED · · SCHEAMA · · · LOCKED · · PRIVILATION · · · LOCKED · · PRIVILATION · · · · LOCKED · · PRIVILATION · · · · LOCKED · · PRIVILATION · · · · LOCKED · <td>PRVNLEGIC · · HGH LOCKED · ADBBMA SCHEMA · · · LOW LOCKED · ADB SCHEMA · · · LOW LOCKED · ADB PNVLEGIC · · · ICM CPU CPU ADB ADB</td> <td>PENNLAGIO ··· HGH LOCRED ··· ADBSMM PRANLECTURD PRANLECTURD SCHEMA ·· ·· LOW LOW LOW ADB <</td>	PRVNLEGIC · · HGH LOCKED · ADBBMA SCHEMA · · · LOW LOCKED · ADB SCHEMA · · · LOW LOCKED · ADB PNVLEGIC · · · ICM CPU CPU ADB ADB	PENNLAGIO ··· HGH LOCRED ··· ADBSMM PRANLECTURD PRANLECTURD SCHEMA ·· ·· LOW LOW LOW ADB <

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.

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-wsNN
- 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

6.4.2 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.

- **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.

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-wsNN
- 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.

- * 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.

- 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-wsNN
- 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:

• 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.
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.

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-wsNN
- 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:

- * **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.

• 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

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-wsNN
- 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*.

E ORACLE Cloud Sea	rch resources, services, docum	ientation, and Marketplace		Germany Central (Frankfurt) 🗸	\bigcirc	A ()	Q		
Security Zones	Security Zone	28								
Overview	Security Zones automatica	Ily enforce security standards and best practices on resources	s in selected compartments. U	Jsers cannot create or update a	resource in a Security Zone if the action v	iolates a	Security 2	Zone poli	cy.	
Recipes	Before you create Show more inform	Before you create a Security Zone, you must be given the required access in an IAM policy. Your Security Zone can use a standard Oracle-managed Recipe, or you can create your own Recipe.								
List scope	Create Security Zone								۲	
Compartment										
MGB-OCI-SEC-WS-LAB-00	Name	Status	Recipe		Created					
trivadisbdsxsp (root)/Training/OCI-SEC-WS/MGB- OCI-SEC-WS-LAB-00			No items four	ıd.						
						Showing	0 items	< 1 of 1	1>	
Tag filters add I clear										
no tag filters applied										

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**.

E ORACLE Cloud Search		tplace Germany Central (Frankfurt) v 🔯 🛕 🧭	••
Security Zones	Security Zones	Create Security Zone	Help
Overview	Security Zones automatically enforce security Learn more	Select Zone Recipe	
Recipes	Before you create a Security Zone, Show more information	Oracle-managed () Customer-managed ()	
Compartment	Create Security Zone		
MGB-OCI-SEC-WS-LAB-00	Name	vame security-zone-mbg-oci-sec-ws-lab-00	
trivadisbdsxsp (root)/Training/OCI-SEC-WS/MGB- OCI-SEC-WS-LAB-00		Description	
Tag filters add clear		Security Zone for Compartment mbg-oci-sec-ws-lab-00	
no tag filters applied		Create for compartment ()	^
		MGB-0CI-SEC-WS-LAB-00 tivadiabdxxp (rod)/Training/0CI-SEC-WSM0B-0CI-SEC-WS-LAB-00	~
		Any existing Cloud Guard target for this compartment is replaced with a new Security Zone target. The new target includes the default Oracle-managed configuration and activity detector recipes in Cloud Guard, and also scans resources in the zone for policy violations. List of existing targets to be deleted: No targets found	
		ça <u>Show advanced options</u>	
	NUT IMPESSION	Create Security Zone Save as stack Cancel	
Terms of Use and Privacy Cookie Preferences		Copyright © 2024. Oracle and/or its affiliates. All ric	ahts reserved.

Figure 90: » step_2

Verify the new associated compartment.

Coracle Cloud	Search resources, services, documentation, an	d Marketplace		Germany Central (Frankfurt) 🗸	0	₽	? €	€ 9			
Security Zones » Security Zone deta	ils										
	security-zone-mbg-	oci-sec-ws-lab-00 cl-sec-ws-lab-00									
SZ	Edit Delete Security Zone information	Tags									
	OCID:ifcha Show Copy		Created: Tue, Oct 29, 2024, 19:14:46 UTC								
ACTIVE	Compartment: MGB-OCI-SEC-WS Cloud Guard target: <u>security-zone</u>	-LAB-00 -mbg-oci-sec-ws-lab-00	Recipe: Maximum Security Recipe - 20200914								
Resources	Associated compar	tments									
Associated compartments	We continuously monitor your	We continuously monitor your compartments and report violations when they are found. Check back periodically to ensure compartments do not have violations.									
	Add compartment										
	Name		Violations (i)								
	MGB-OCI-SEC-WS-LAB-00		None found					:			
							< 10	of 1 >			

Figure 91: » step_3

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

	arch resources, services, documentation, and Marketplace			Ge	rmany Central (Frankfurt) 🗸	\bigcirc	众	?	⊕ 0	
Security Zones	Security Zones Security Zones automatically enforce security standards and be Learn more	st practices on resource:	s in selected compartments.	Users cannot create or update a resource	in a Security Zone if the action v	iolates a	Securit	ty Zone	policy.	
Recipes	The latest Security Zones release includes many signit	The latest Security Zones release includes many significant enhancements and user interface changes. See the release notes for details.								
List scope	Create Security Zone									
Compartment	Name	Status	Recipe		Created					
trivadisbdsxsp (root)/Training/OCI-SEC-WS/MGB-	security-zone-mbg-oci-sec-ws-lab-00	Active	Maximum Security Recip	<u>be - 20200914</u>	Tue, Oct 29, 2024, 19:14:46 U	тс			:	
OCI-SEC-WS-LAB-00						Showin	g 1 item	<	1 of 1 >	
Tag filters add i clear										

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_.

Encryption	
Encrypt using Oracle managed keys	
Leaves all encryption-related matters to Oracle.	
Encrypt using customer-managed keys	
Requires a valid key from a vault that you have access to. Learn more	
Vault in MGB-OCI-SEC-WS-LAB-00 (Change compartment)	
vault-mbg-oci-sec-ws-lab-00	\$
Master Encryption Key in MGB-OCI-SEC-WS-LAB-00 (Change compartment)	
mek-mbg-oci-sec-ws-lab-00	<u>^</u>
	•

Figure 94: » step_6

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

Edit Visibility	<u>Help</u>
Enabling public visibility will let anonymous and unauthenticated users access data stored in the bucket. Visibility Private Public Allow users to list objects from this bucket	
(i) Consider using pre-authenticated requests instead We recommend using pre-authenticated requests instead of public buckets. Pre-authenticated requests support additional authorization, expiry, and scoping capabilities not possible with public buckets. Learn more	
Security Zone Violation: Object Storage buckets in a security zone can't be public. (Forbidden) Save Changes	

Figure 95: » step_7

7.1.4 Delete Security Zone

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

	ch resources, services, documentation, and Marketplace			Germany Central (Frankfurt) 🗸 🗔	\$ @ €	₽ 0		
Security Zones	Security Zones Security Zones automatically enforce security standards and Learn more	I best practices on resources	s in selected compartments. Users cannot create or up	pdate a resource in a Security Zone if the action violates a	Security Zone p	olicy.		
Recipes	The latest Security Zones release includes many significant enhancements and user interface changes. See the <u>release notes</u> for details.							
List scope	Create Security Zone							
Compartment	Name	Status	Recipe	Created				
trivadisbdsxsp (root)/Training/OCI-SEC-WS/MGB-	security-zone-mbg-oci-sec-ws-lab-00	Active	Maximum Security Recipe - 20200914	Tue, Oct 29, 2024, 19:14:46 UTC	View detai	ls :		
OCI-SEC-WS-LAB-00				Showing	1 View tags	>		
Tag filters add clear					Add tags			
no tag filters applied					Delete			

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 *PUB-LIC*. Verify the visibility - a yello triangle occurs.

	earch resources, services, documentat	ion, and Marketplace		—	Germany Central (Frankfurt) 🗸	0 A	?	٢	0
Object Storage & Archive Storage	Buckets in MGB	-OCI-SEC-	WS-LAB-00 Compartment furable, and secure data storage. Data is uploaded as	objects that are stored in buckets. Learn more					
Buckets	Create Bucket								
Private Endpoints	Name	•	Default Storage Tier	Visibility	Created				
List scope	my-bucket		Standard	A Public	Tue, Oct 29, 2024, 19:28	3:04 UTC			:



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.



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.

- 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-wsNN
- 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.

Cre	ate instance Actions -									
	Name	State	Public IP	Private IP	Shape	OCPU count	Memory (GB)	Availability domain	Fault domain	c
	ci-fra-lab-mgb-ocisecws-00-webserver01	Running		10.0.0.75	VM.Standard.E5.Flex	1	4	AD-1	FD-2	Т
	ci-fra-lab-mgb-ocisecws-00-webserver02	Running	-	10.0.0.76	VM.Standard.E5.Flex	1	4	AD-2	FD-1	т

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_KhXMkugnekpAOQH1-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

```
--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 "Hello, $name";
    }
    ?>
</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

checks run to green (ok) after a while.

Networking -> Load Balancer -> Create Load Balancer

Cloud	Search resources, services, o	documentation, and Marketplace			Germany Ce	entral (Frankfurt) 🗸	0	Δ (୭ 🌐	9 0
Networking > Load balancers > Load balan	alancer									
Load balancers Overview Load balancer	Load balancer se The load balancer se to ensure high availa	TCETS ervice provides layer 4 and layer 7 ibility. Watch a <u>video</u> introduction te	(TCP and HTTP) load balancing the o the service.	t routes network traffic in a more	complex manner. Load balancing impro	oves resource utilizatio	on, faciliti	ates scalir	ng, and h	elps
Network load balancer	Create load balar									
	Name	State	IP address	Shape	Overall health	Created				
List scope				No items found.						
Compartment							Showing	0 items	< 1 of	1 >
MGB-OCI-SEC-WS-LAB-00										
trivadisbdsxsp (root)/Training/OCI-SEC-WS/MGB										

Figure 99: » step_6

Add details:

- set name
- let visibility type as PUBLIC

	Search resources, services, documentation, and Marketplace		Germany Central (Frankfurt) 🗸 👩 🥼	⊕ 9
Create load ba	alancer			Help
 Add details Choose backends Configure listener 	A load balancer provides automated traffic distribution from one entry point to multiple servers in a backend set. Load balancer name loadbalancer.mbg-oci.se.ws-lab	The load balance	r ensures that your services remain available by directing traffic only to healthy servers in the	
	Choose visibility type Public You can use the assigned public IP address as a front end for incoming traffic. Assign a sublic IP address	Private You can use th	e assigned private IP address as a front end for internal incoming VCN traffic.	
	Passign a public in address Ephemeral IP address You can have an IP address from the pool automatically assigned to you.	Reserved You can provid source IP pool	IP address e either an existing reserved IP address, or create a new one by assigning a name and	
	Oracle will generate an IP address for you. Bandwidth ShapesPick the type and size of bandwidth shape for your load balancer Learn more about load balancer st	napes		
	Flexible shapes Create a flexible shape size within the minimum and maximum size range you specify.	Dynamic s Choose from o	hapes ne of the available predefined shape sizes.	
	Oracle will retire the ability to create new dynamic shape load balancers after Thu, 11 May 2023 00 Choose a minimum bandwidth	:00:00 UTC. Oracl Choose a maxin	e recommends using the cost-efficient flexible load balancers.	
	10 The maximum service limit is currently 8010 Mbps. For more bandwidth, request a service limit increase from	10 n the service limits	page in the Console.	
Previous Next Cance				

Figure 100: » step_7

Scroll down and set:

- Virtual Cloud network
- Your public subnet

Choose networking	
Virtual cloud network in MGB-OCI-SEC-WS-LAB-00 (Change compartment)	
vcn-fra-lab-mgb-ocisecws-00	\$
To create a public load balancer, specify a single regional subnet (recommended), or two availability domain-specific subnets in different availability domains. If backends have public IP addresses, configure a NAT gateway for connecting the public load balancers to its public IP address-based backends. Learn more about <u>configuring NAT gateway</u> . Subnet in MGB-OCI-SEC-WS-LAB-00 (Change compartment)	
sn-pub-fra-lab-mgb-ocisecws-00	\$
Use network security groups to control traffic ①	

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.

ate load bal	ancer							
Add details	A load balancer distributes traffic to back Specify a load balancing policy	kend servers within a backend se	. A backend set is a logical entity d	efined by a load balancing policy, a	a health check policy, and a list of t	backend servers (Comp	ute instances).	
Choose backends	Weighted round robin		IP hash		Least connection	s		
Configure listener This policy distributes incoming traffic sequentially to each server in a backend set list.			This policy ensures that reques ways directed to the same back	ts from a particular client are al- kend server.	This policy routes incomi with the fewest active co	ing request traffic to the nnections.	backend server	
Review and create								_
	Select backend servers							
	Compartment							
	MGB-OCI-SEC-WS-LAB-00						0	0
	trivadisbdsxsp (root)/Training/OCI-SEC-WS/M	GB-OCI-SEC-WS-LAB-00						
	Select instances							
	Select instances	IP address	OCID	Availability domain	Compartment	Port		
	Select instances Name ci-fra-lab-mgb-ocisecws-00-w	IP address	OCID ocid1.instance.oc1.eu-frankfu	Availability domain EUZg:EU-FRANKFURT-1-AD	Compartment MGB-OCI-SEC-WS-LAB-	Port 80		
	Select instances Name ci-fra-lab-mgb-ocisecws-00-w	IP address 10.0.0.73	OCID ocid1.instance.oc1.eu-frankfu	Availability domain	Compartment MGB-OCI-SEC-WS-LAB- 00	Port 80	×	
	Select instances Name cl-fra-lab-mgb-ocisecws-00-w	IP address 10.0.0.73	OCID ocid1.instance.oc1.eu-frankfu	Availability domain EUZg.EU-FRANKFURT-1-AD	Compartment MGB-OCI-SEC-WS-LAB- 00 Wixwadledsxsp (root)/Training/OCI-SEC- WS/MGB-OCI-SEC-WS-LAB-00	Port 80	×	
	Select instances Name ci-fra-lab-mgb-ocisecws-00-w Name	IP address	OCID ocid1.instance.oc1.eu-frankfu	Availability domain EUZg:EU-FRANKFURT-1-AD Availability domain	Compartment MGB-OCI-SEC-WS-LAB- 00 WSM0B-OCI-SEC-WS-LAB-00 Compartment	Port 80 Port	×	
	Select instances Name ci-fra-lab-mgb-ocisecws-00-w Name ci-fra-lab-mgb-ocisecws-00-w	IP address 10.0.0.73 IP address 10.0.0.106	OCID ocid1.instance.oc1.eu-frankfu OCID ocid1.instance.oc1.eu-frankfu	Availability domain EUZg EU-FRANKFURT-1-AD Availability domain EUZg EU-FRANKFURT-1-AD	Compartment MGB-OCI-SEC-WS-LAB- 00 triviatiosus (rod)/Tailing/OCI-SEC- WSM0B-OCI-SEC-WS-LAB- Compartment MGB-OCI-SEC-WS-LAB-	Port 80 Port 80	×	
	Select instances Name cl-fra-lab-mgb-ocisecws-00-w Name cl-fra-lab-mgb-ocisecws-00-w	IP address 10.0.0.73 IP address 10.0.0.106	OCID ocid1 instance oc1.eu-frankfu OCID ocid1 instance oc1.eu-frankfu	Availability domain EU2g EU-FRANKFURT-1-AD Availability domain EU2g EU-FRANKFURT-1-AD	Compartment MGB-OCI-SEC-WS-LAB- 00 trivedidation (indef)/Takinog/OCI-SEC- WS-MGB-OCI-SEC-WS-LAB- 00	Port 80 Port 80	×	
	Select instances Name ci-fra-lab-mgb-ocisecvs-00-w Name ci-fra-lab-mgb-ocisecvs-00-w	IP address 10.0.0.73 IP address 10.0.0.106	OCID ocid1.instance.oc1.eu-frankfu OCID ocid1.instance.oc1.eu-frankfu	Availability domain EUZg:EU-FRANKFURT-1-AD Availability domain EUZg:EU-FRANKFURT-1-AD	Compartment MGB-OCI-SEC-WS-LAB- 00 trivateladuse (root)/Training/OCI-SEC- WSMAB OCI-SEC-WS-LAB- 00 MGB-OCI-SEC-WS-LAB- 00 trivateladuse (root)/Training/OCI-SEC- WSMAB-OCI-SEC-WS-LAB-00	Port 80	×	

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.

= ORACLE Clou	JC Search resources, services, documentation, and M	arketplace	Ge	ermany Central (Frankfurt) 🗸	\bigcirc	\$ ∅		0				
Create load ba	llancer						Help	R				
 Add details Choose backends 	A listener is a logical entity that checks for incoming traff listeners after you create your load balancer. Listener name	ic on the load balancer's IP address. To handle TCP, H	ITTP and HTTPS traffic, you must configure at least on	e listener per traffic type. You can	configure	additional		*				
3 Configure listener		Seecify the type of traffic your listener handles										
Manage logging Review and create	HTTPS	HTTP 🗸	HTTP/2	ТСР								
Previous Next Gance	Specify the port your listener monitors for ingress traffic 80 You can configure path route rules and custom header in Advanced SSL To learn how to create different certificate service res • CA bundle • Certificate Authority CA bundle in MGB-OCI-SEC-WS-LAB-00 Optional (Change compartment) No data available	ipecify the port your listener monitors for ingress traffic 80 fou can configure path route rules and custom header rule sets after you create the load balancer. For more information, see <u>managing request routing and managing rule sets</u> . Advanced SSL To learn how to create different certificate service resources, see the <u>certificate overview</u> page. ● CA bundle Certificate Authority CAbundle in MGB-OCI-SEC-WS-LAB-00 Optional (Change compartment) No data available										
	Timeout Specify the maximum timeout in seconds Optional							P				

Figure 103: » step_10

Next.

Manage Logging:

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

E ORACLE Clou	Jd Search resources, services, documentation, and Marketplace	Germany Central (Frankfurt) 🗸 👩 🇘	୭ 🖶 9
Create load ba	lancer		Help
 Add details Choose backends Configure listener Manage logging Review and create 	Enabling access and error logs is optional, but recommended. Reviewing these logs can help you with diagnosing and fixing issue the load balancer service. Standard limits, restrictions, and rates apply when enabling the logging features. Error logs Enabled Enab	s with your backend servers. <u>Learn more about load balancer logging</u> Logging is an op	tion in
	Access logs Not enabled The access log captures detailed information about requests sent to the load balancer. Learn more about access logs.		Q
Previous Next Cance		Convicts © 2021 Carela undro its officients	All rights received

Figure 104: » step_11

Next.

Review and create:

	Cloud	Search resources, services, documentation, and Marketpla	зсе			Germany Central (Frankfurt) 🗸)	0
	Create load bala	ncer						Н	elp
	 Add details Choose backends Configure listener Manage logging Review and create 	Details Lead balancer name: loadbalancer.mbg.oci.se.ws-lab Visibility type: Public IP address: Ephemeral IP address Bandwidth Shape: Flexible shapes Maximum bandwidth: 10 Minimum bandwidth: 10 Networking UPV6 address assignment: Disabled VCN: vcn: fra-lab.mgb-ocisecws-00 Subnet: sn-pub-fra-lab.mgb-ocisecws-00 Subnet: sn-pub-fra-lab.mgb-ocisecws-00					E	Edit	
		Backends Load balancer policy: Weighted round robin Backend compartment: MGB-OCI-SEC-WS-LAB-00					E		D
	Previous Next Submit	Name	ID address	ocip	Availability domain	Compartment	Port		
settings	Terms of Use and Privacy Cookie Preferen	nces				Copyright © 2024, Oracl	e and/or its affiliates. All	l rights resi	erved.

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-

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

←	→ C	▲ Not secure 1	30.162.34.134			
	🗀 ESXi La	ab 🗀 Mohnweg	Feuerwehr Kestenh	O GitHub - PacktPubli	🔞 UniFi WLAN Gastne	🕋 MQTT, No
OCI Ho	ostname: ci	-fra-lab-mgb-oci	secws-00-webserver02			

Figure 106: » step_14

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

XSS Demo Page

Enter your name: Submit

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

-	130.162.34.134 says	
	XSS	
		ОК



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.

E ORACLE Cloud	Search resources, services, documentation, and Marketplace			Germany Central (Frankfurt)	× 🖸	\$?	• •
Create WAF policy	,						Help
Basic information Access control Access control Access control Access control Protections Select enforcement cont Review and create	Basic information Wat policies encompass the overall configuration of your WAF service. Name	fferent WAF modules (access control, rate limiting, a Action type ① Check Allow Return HTTP response web applications.	Ind protections) in the next steps.	€att €att			
Terms of Use and Privacy Cookie Preferences				Copyright © 202	4, Oracle and/or	its affiliates. 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.

		Germany Central (Frankfurt) ✓	$\overline{\mathbf{O}}$	۵	?	• •
Create WAF policy						Help
Basic information Access control Access control Rate limiting Protections Select conforcement point Beview and create	Rate limiting Optional Rate limiting allows inspection of HTTP connection properties and limits the frequency of requests for a given key.					

Figure 111: » step_3

Next.

Protections: Enable checkbox and Add request protection rule.

	arch resources, services, documentation,	and Marketplace		G	ermany Central (Frankfurt) 🗸		Ĵ ()	• •				
Create WAF policy								Help				
Basic Information Access control Bate Imiting Protections Select enforcement point Review and create	Protection S Optional Protection rules determine if a networ Protection rules determine fra networ Protection rule Request protection rule	rk request is allowed but logged, or is block les les Actions •	xed entirely.									
	Rule name	Protection capabilities	Default action name	Body inspection	Edit							
			No items found.									
	0 selected Showing 0 items < 1 or 1 >											

Figure 112: » step_4

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

ORACLE Cloud Search resources, services, documentation, and Marketplace	Germany Central (Frankfurt) 🗸 💿 🖨 🏮
Add protection rule	Help
Name rule-xss-protect-lab-mgb-ocisecws-00	·
Conditions (optional) Show advanced controls When the following Conditions are met	
Condition type Operator Value Path Operator Value	
+ Another condition	
Rule action	
Then perform the following action.	
Action name	
Pre-configured 401 Response Code Action	
Action type: Return HTTP response (i)	
Response code: 401 Unauthorized	
> Show header details	
> Show,resonse page body details	

Figure 113: » step_5

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

1.1.1					
941140	Cross-Site Scripting (XSS) Attempt: XSS Filters - Category 4	No	HTTP, PCI, Request-Body-Inspection, Recommended, OWASP-A7-2017, OWASP-A3-2021, CAPEC-1000, CAPEC-152, CAPEC-242, Code Injection, Cross-Site Scripting (XSS)	171	:
9410000	Cross-Site Scripting (XSS) Collaborative Group - XSS Filters Categories	Yes	Request-Body-Inspection, HTTP, PCI, Collaborative, Recommended, OWASP- A3-2017, OWASP-A2-2021, Code Injection, Cross-Site Scripting (XSS)	3 1 0	:

Figure 114: » step_6

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

	irch resources, services, documentation, and Marketplace				Germany Central (Frankfurt) 🗸	0	Δ (୭ €	€ 0
Create WAF policy									Help
Basic information Access control Bate innition Protections Sedic information point Sedic information point Beview and create	Protections Optional Protection rules determine if a network request is allowed by C Enable to configure protection rules Request protection rules Add request protection rule Rule name	ut logged, or is blocked entirely. Protection capabilities	Default action name	Body inspection	Edit				
	rule-xss-protect-lab-mgb-ocisecws-00	1	Pre-configured 401 Response Code Action	Disabled	Edit 🗸				
	0 selected			Show	ing 1 item < 1 of 1 >				

Figure 115: » step_7

Next.

Select enforcement point: select Load Balancer created above.

E ORACLE Cloud Sear	ch resources, services, documentation, and Marketplace Germany Centr	al (Frankfurt) 🗸	\bigcirc	Δ (? €	€ 0
Create WAF policy						<u>Help</u>
Basic Information Access control Rate limiting	Select enforcement point Optional Use this to enforce web application firewall security on your load balancer.					
Protections Select enforcement point Review and create	Configure your Load balancer with an HTTP listenet. Learn More. You can generate security logs for your frewaits after you create your WAF policy. Enabling security logs is highly recommended as it provides valuable insight into your WAF performance.					
	Add firewalls Select In-region application delivery resources to secure.					
	Load balancer in MGB-OCI-SEC-WS-LAB-09 (Change compatiment) Tool balancer mbg oci-se ws-lab Company to the balance an ommunicate why your orgin.	×				
	+ Additional fire	wall				

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

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*.



```
"code": "401",
"message": "Unauthorized"
```

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.

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

8 Appendix E: Manual Lab Configuration

9 Appendix F: Oracle Cloud Infrastructure Users and Permissions