



Security: Configure Security Zones Using Maximum Security Zones

Lab 7-1 Practices

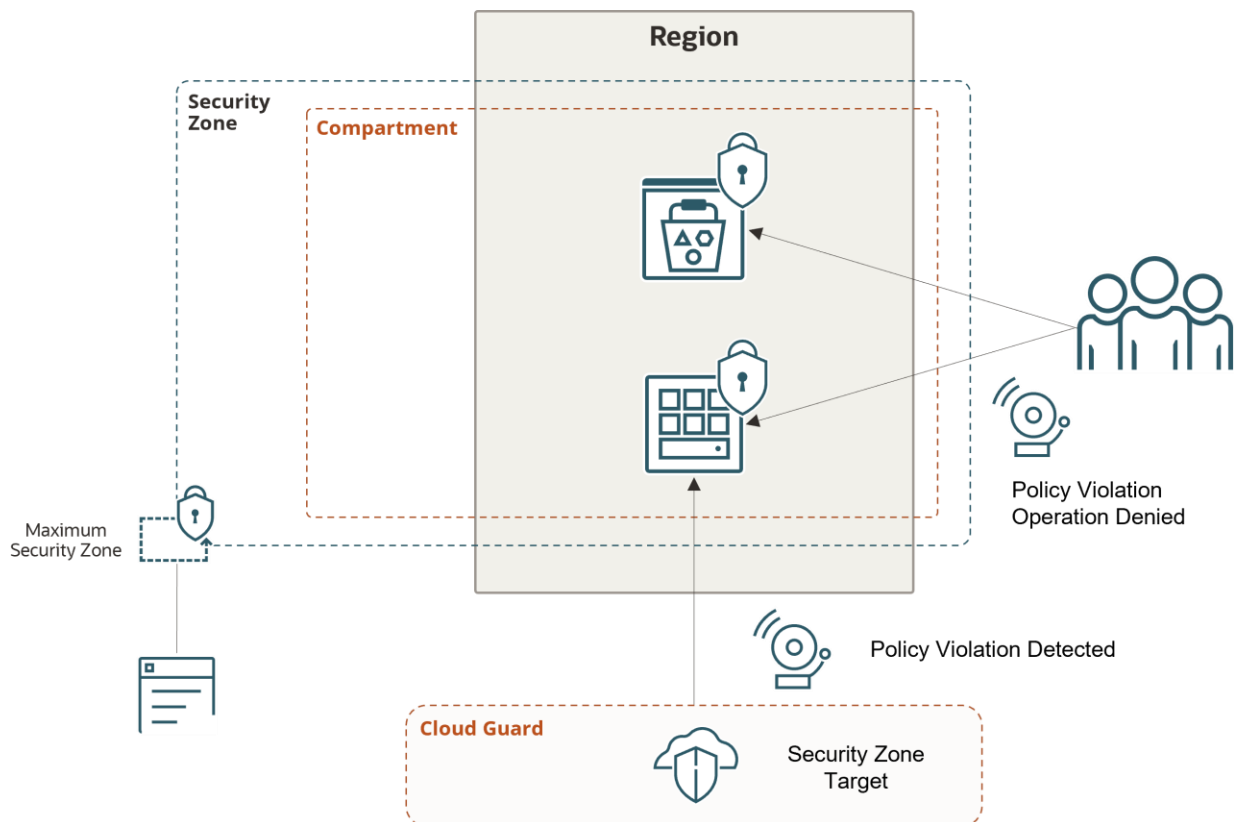
Get Started

Overview

Security zones enforce security posture on OCI cloud compartments and prevent actions that can compromise a customer's security posture. Security zone policies can be applied to various cloud infrastructure types (network, compute, storage, database, and so on) to guarantee cloud resources ensure security and to prevent potential misconfigurations.

In this lab, you will:

- Set up a security zone with Maximum Security Recipe
- View the security zone policies attached to a created security zone
- Test creating a bucket in an assigned compartment using an Oracle-managed key



Prerequisites

- You have access to the OCI Console.
- Your tenancy should have Cloud Guard enabled.

Assumptions

- In this lab, we are considering US East (Ashburn) (IAD) as your region.
- You must be familiar with navigating the OCI Console.

Set Up Security Zone with Maximum Security Recipe

You will create a security zone for an allocated compartment and check for any security zone policy violations.

Tasks

1. Sign in to the OCI Console.
2. In the Console ribbon at the top of the screen, click the **Region** icon to expand the menu. Ensure that you are in the correct region, **US East (Ashburn)**.
3. From the navigation menu, select **Identity & Security**. Navigate to **Security Zones**, and then click **Overview**.
4. In the left navigation pane, under **Scope**, select *<your assigned compartment>* from the drop-down menu.

Note: The compartment should not be associated with a security zone. By default, all sub-compartments are also in the same security zone.

5. Click **Create Security Zone**.
6. On the Create Security Zone page, enter the following values:
 - a. **Security Zone Recipe:** Select **Oracle-managed** to use Maximum Security Recipe.
 - b. **Name:** IAD-FA-LAB07-1-SZ-01
 - c. **Description:** My Security Zone
 - d. **Create for compartment:** *<your assigned compartment>*

7. Click **Create Security Zone**.

Note: When you create a security zone for a compartment, Cloud Guard does the following:

- Deletes any existing Cloud Guard target for the compartment and for any child compartments
- Creates a security zone target for the compartment
- Adds the default Oracle-managed detector recipes to the security zone target

View the Security Zone Policies Attached with a Created Security Zone

You will identify the recipe associated with the newly formed security zone, and then review its policies.

1. From the navigation menu, select **Identity & Security**. Navigate to **Security Zones**, and then click **Overview**.
2. In the left navigation pane, under Scope, select *<your assigned compartment>* from the drop-down menu.
3. Click the **IAD-FA-LAB07-1-SZ-01** security zone and view the Security Zone details page.
4. On the **Security Zone** information tab, locate the attached recipe and click the **Recipe** for this security zone: Maximum Security Recipe – 20200914.
5. View the Oracle-managed recipe attached to the Security Zone created on the **Recipe details** page.
6. View a few policy statements with associated Resource types:

```
deny public_subnets in VIRTUALNETWORK
deny public_buckets in OBJECTSTORAGE
deny buckets_without_vault_key in in OBJECTSTORAGE
```

Next, you will put a security zone to test by attempting to violate a few of its policies.

Verify Creating a Bucket in an Assigned Compartment Using a Oracle-Managed Key

You will test the security zone. Create a bucket to check if it is restricted in the security zone. As a reference, the security zone recipe has a policy that prohibits bucket creation without a customer-managed vault key.

To create a bucket to observe the security zone violations:

1. Open the navigation menu and click **Storage**. Navigate Object Storage, click **Buckets**.
2. In the left navigation pane, under **List Scope**, select the assigned compartment from the drop-down menu.
3. Click **Create Bucket**.
4. In the **Create Bucket** dialog box, specify the attributes of the bucket:
 - a. **Bucket Name:** IAD-FA-LAB07-1-BKT-01-<user-id>
Please specify your user ID in place of <user-id> to make it unique.
 - b. **Default Storage Tier:** Standard
 - c. **Encryption:** Encrypt using Oracle-managed keys.

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

5. Click **Create**.

You will receive an error indicating a security zone violation: “Encrypt the bucket with a customer-managed encryption key”.

6. Click **Cancel**.

The security zone recipe created earlier has a policy that prohibits bucket creation without a customer-managed key. You will need to create an OCI Vault and a master encryption key, using which you can create a bucket. This way the security zone recipes enforce security posture on OCI cloud compartments and prevent actions that could compromise the security posture of a customer.

Note: Please purge the Security Zone created for this lab.

Purge Security Zone

1. From the navigation menu, select **Identity & Security**. Navigate to **Security Zones** and click **Overview**.
2. Make sure you are in your given compartment.
3. From the list of Security Zones, locate your Security Zone and click its name: **IAD-FA-LAB07-1-SZ-01**.
4. Click **Delete**. Then click **Delete** in the Confirmation window.

