Security: Enable Cloud Guard

Lab 18-1 Practices

Get Started

Overview

Cloud Guard examines your Oracle Cloud Infrastructure resources for security weakness related to configuration, and your operators and users for risky activities. Upon detection, Cloud Guard can suggest, assist, or take corrective actions, based on your configuration.

In this lab, you will:

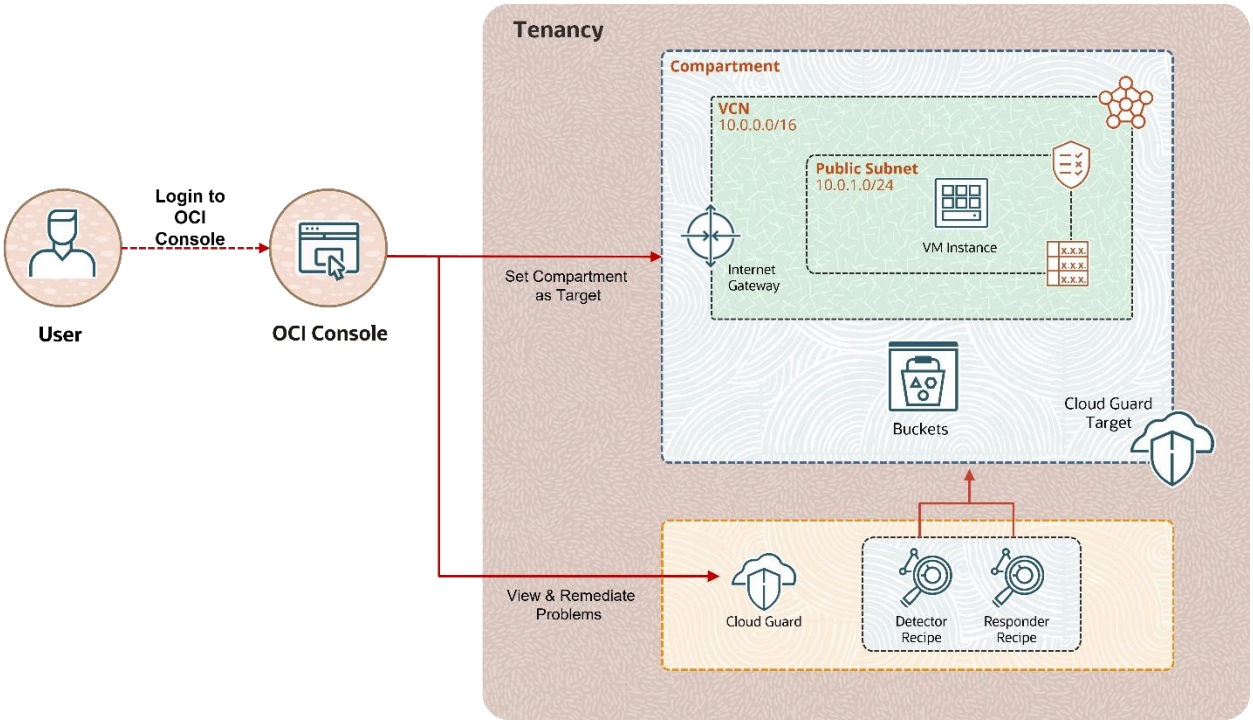
a. Create a Virtual Cloud Network

b. Explore Cloud Guard

c. Create a Cloud Guard target

d. Create a scenario to verify Cloud Guard monitoring

e. Remediate problems identified by Cloud Guard



Prerequisites

- You must have access to the OCI Console.

Create a Virtual Cloud Network

In this section, you will create a VCN by using the Start VCN Wizard tool.

Tasks

1. In the console ribbon at the top of the screen, click the **Regions menu** and select **UK South (London).**
2. Click the navigation menu, click **Networking**, and then click **Virtual Cloud Networks**.
3. Click **Start VCN Wizard**.
4. Select the **Create VCN with Internet Connectivity** option, and then click **Start VCN Wizard.**
5. Enter the following values:
   - **VCN Name:** `LHR-AA-LAB18-1-VCN-01`
   - **Compartment:** Select your assigned <*compartment name*>.
6. Leave the default values for the remaining fields. Click **Next**.
7. Review and understand the list of resources that the OCI VCN Wizard will create. Notice that the wizard will configure CIDR block ranges for VCN IP addresses, and for the public and private subnets. It will also set up security list rules and route table rules to enable basic access to the VCN.
8. Click **Create**.
9. When complete, click **View Virtual Cloud Network**.

Explore Cloud Guard

In this practice, you will explore Cloud Guard to obtain a unified view of your tenancy's cloud security posture. You will also explore detector recipes for monitoring targets and responder recipes for responding with any problems that occur.

Tasks

1. In the console ribbon at the top of the screen, from the **Regions menu**, select **US East (Ashburn).**
2. From the navigation menu, select **Identity & Security**, and then click **Cloud Guard**.

   Note: A dashboard with the current Cloud Guard observations is displayed. If the Guided Tour is displayed, go through the same to explore the various features. You can also click **Stop tour** if you are not interested in the tour. Once you are done with the tour, the dashboard with various options under Cloud Guard on the left side in the browser window is displayed.
3. In the left navigation pane, under **Cloud Guard**, click **Detector Recipes.**
4. In the left navigation pane, under **Scope**, select ***<Tenancy Name>*** **(root).**
5. Click **OCI Configuration Detector Recipe (Oracle managed)** and view the detector rules that are included in this recipe.
6. To view the details of a particular rule, click the **disclosure triangle,** a downward arrow located next to the three dots the right of the rule.
7. Click **Risk level** to organize rules by their risk level.
8. Click **Detector Recipes** from the breadcrumb list at the top left.
9. Click **OCI Activity Detector Recipe (Oracle managed)** and explore the rules that are within activity detector recipe. You also see that for the built-in, Oracle-Managed detector recipes, you can clone the recipe. You may clone an existing recipe and customize it to your needs.
10. Click **Detector recipes** from the breadcrumb list at the top left.
11. In the left navigation pane, under **Cloud Guard**, click **Responder Recipes.**

12. Click **OCI Responder Recipe (Oracle Managed)**.

    View the responder rules that are included in this recipe.

13. To view the details of a particular rule, click the **disclosure trx1iangle,** a downward arrow located next to the three dots to the right of the rule.

14. Click **Responder recipes** from the breadcrumb at the top left.

15. In the left navigation pane, under **Cloud Guard**, click **Managed lists**.

16. Click the **Oracle Cloud Guard CIDR Managed List**.

    Note: A managed list is a reusable list of parameters that makes it easier to set the scope for detector and responder rules. A managed list is a tool that can be used to apply certain configurations to detectors.

    Under **Entries,** observe the predefined list of trusted IP address ranges used by Oracle Cloud Infrastructure (OCI). Cloud Guard also lets you define your own managed lists as needed.

    For example, you can define lists of states or provinces, ZIP codes, OCIDs, or whatever else you may define. Click the **Managed Lists** breadcrumbs and you will see an option to create your own managed list.

17. In the left navigation pane, under **Cloud Guard**, click **Settings**.

    Note: Observe the reporting region listed. If you are in the home region of your tenancy, you will also see the option to **Disable Cloud Guard** (if it is already enabled). If you are in any other region, this button will be disabled.

Create a Cloud Guard Target

In this practice, you will learn to add target to set scope of resources that Cloud Guard monitors.

Note: Cloud Guard is enabled in your practice tenancy.

Tasks

1. In the console ribbon at the top of the screen, click the **Regions menu** and select **UK South (London).**
2. Click the navigation menu, click **Identity & Security**, and then click **Cloud Guard**.
3. In the left navigation pane, under **Cloud Guard**, click **Targets.**
4. In the left navigation pane, under **List Scope**, and select your assigned <*compartment name*>.

   Note: If you already have a specific target set for your compartment, delete it.
5. Click **Create New Target**.
6. Enter the following:
   - **Target Name:** `LHR-AA-LAB18-1-CG-01`
   - **Description:** Enter a description.
   - **Compartment:** Select your assigned <*compartment name*>
   - **Configuration detector recipe:** OCI Configuration Detector Recipe (Oracle managed)
   - **Threat detector recipe:** OCI Threat Detector Recipe (Oracle managed)
   - **Activity Detector Recipe:** Oracle Activity Detector Recipe (Oracle managed)
   - **Responder recipe:** OCI Responder Recipe (Oracle managed)
7. Click **Create**.

   Note: The detail page for the new target will be displayed.
8. In the left navigation pane, under **Resources**, click **Detector recipes** and view the detector recipes associated with the created target.

Create a Scenario to Verify Cloud Guard Monitoring

To identify a problem in the set target, you will create a bucket and make its visibility public.

1. In the console ribbon at the top of the screen, click the **Regions menu** and select **UK South (London).**

2. Click the navigation menu and click **Storage**. Under Object Storage, click **Buckets**.

3. In the left navigation pane, under **List Scope**, select your assigned *<compartment name>.*

4. Click **Create Bucket**.

5. In the **Create Bucket** dialog box, specify the attributes of the bucket:
   - **Bucket Name:** `LHR-AA-LAB18-1-BKT-01-<user-id>`

     Please specify your user ID in place of `<user-id>` to make it unique.
   - **Default Storage Tier:** Select Standard.

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

6. Click **Create**.

7. Click the three dots on the right to open the Actions menu and select **Edit Visibility**. Select **Public** and click **Save Changes**.

   Note: You have now created a bucket with public visibility in the assigned compartment. To assure cloud security posture, the detector recipe includes a configuration rule for **Bucket with a public visibility**.

   As a result, you must wait for Cloud Guard to evaluate your allocated detector configuration and list its observations on the set target. Wait 30-60 minutes before checking the Cloud Guard Dashboard to see if the problem has been identified and resolving it.

Remediate the Problems Identified by Cloud Guard

1. From the navigation menu, select **Identity & Security**. Click **Cloud Guard**.
2. In the left navigation pane, under **Cloud Guard**, click **Problems.**
3. In the left navigation pane, under **List Scope**, select your assigned *<compartment name>.*
4. View the list of problems Cloud Guard has identified with the resources in your assigned compartment based on your previous practices. The Problems page displays information about each problem, including:
   - Problem Name
   - Risk Level
   - Detector Type
   - Resource affected
   - Target
   - Region
   - Labels
   - First Detected
   - Last Detected

Follow this process to remediate the problem **Bucket is Public.**

1. In the breadcrumbs at the top left, click **Problems.**
2. In the left navigation pane, under **Resource type,** select **Bucket**.
3. Select "**Bucket is Public**" from the problem list.
4. Check problem details and problem history, before the actions are taken.

   Note: As per the problem details, you have the option to remediate (if there are any responder suggestions) or mark it as resolved or dismiss the problem.

   The problem specifies that Bucket has a public visibility, it is recommended to carefully assess whether public visibility is required for the mentioned resource and to act if it does not.
5. Click **Remediate** and confirm that you want to execute the responder to remediate the problem.

Note: After a couple of minutes, you will see that the problem is successfully resolved, and the problem icon turns green.

6. To verify, click **Buckets** under **Object storage**. Click the bucket **LHR-AA-LAB18-1-BKT-01-<User_Id>** . You will now see that the visibility is now Private.

   Similarly, Cloud Guard can remediate or resolve identified problems in your OCI tenancy, ensuring security posture.