OCI

Prepare Your OCI Account

Before you onboard an OCI tenant to Multicloud Defense, your OCI account needs to be properly set up. The following are the general steps required to prepare the tenant.

Note Multicloud Defense supports both Ingress and Egress/East-West protection for OCI. Inventory and traffic discovery are not supported.

In order to onboard the OCI tenant, you need to subscribe to the US West (San Jose) region. If this region is not subscribed, then the onboarding of the OCI tenant will result in an error.

In order to deploy a Multicloud Defense Gateway into OCI, the Terms and Conditions for the Multicloud Defense compute image **must** be accepted in each OCI compartment. Otherwise the deployment will error out with an unauthorized error.

The following procedure instructs how to prepare your OCI environment to successfully connect with Multicloud Defense; for OCI-specific documentation on how to accomplish these requirements, see OCI documentation.

Overview of Automated Steps

Multicloud Defense provides a script that automates the preparation of your OCI account. The automation does include the required group, policy, permissions, and user included in the manual procedure listed after.

1. Open your Oracle Cloud Shell or any linux-based shell prompt.
2. Enter and execute the following command:

```
bash <(curl -sSL
https://raw.githubusercontent.com/valtix-security/cli-oci-setup/main/oci_onboarding.sh)
```

3. Once successfully finished, continue to Connect the Oracle OCI Tenant to the Multicloud Defense Controller from the Multicloud Defense Dashboard, on page 2.

Overview of Manual Steps

Perform the following procedure to manually prepare your OCI account:

1. Create a Group.
2. Create a Policy. Note that the policy must have the `root` Compartment selected and the following permissions are included:

```
Allow group <group_name> to inspect instance-images in compartment <compartment_name>
Allow group <group_name> to read app-catalog-listing in compartment <compartment_name>
Allow group <group_name> to use volume-family in compartment <compartment_name>
Allow group <group_name> to use virtual-network-family in compartment <compartment_name>
Allow group <group_name> to manage volume-attachments in compartment <compartment_name>
Allow group <group_name> to manage instances in compartment <compartment_name>
Allow group <group_name> to {INSTANCE_IMAGE_READ} in compartment <compartment_name>
Allow group <group_name> to manage load-balancers in compartment <compartment_name>
Allow group <group_name> to read marketplace-listings in tenancy
Allow group <group_name> to read marketplace-community-listings in tenancy
Allow group <group_name> to inspect compartments in tenancy
Allow group <group_name> to manage app-catalog-listing in compartment <compartment_name>
Allow group <group_name> to read virtual-network-family in tenancy
Allow group <group_name> to read instance-family in tenancy
Allow group <group_name> to read load-balancers in tenancy
Allow group <controller-group> to manage cloudevents-rules in tenancy
Allow group <controller-group> to manage ons-family in tenancy
```

3. Create a User.
4. Add the User to the Group.
5. Create an API Key for the User.
6. Record the *user* and *tenancy* OCIDs.
7. Accept the Terms and Conditions.

What to do next:

Connect the OCI account to your Multicloud Defense using Connect the Oracle OCI Tenant to the Multicloud Defense Controller from the Multicloud Defense Dashboard, on page 2.

Connect the Oracle OCI Tenant to the Multicloud Defense Controller from the Multicloud Defense Dashboard

Before you begin

Review the requirements in Prepare Your OCI Account, on page 1.

Procedure

Step 1 In the Cloud Accounts pane, click **Add Account**.

Step 2 In the General Information page, select **OCI** in the Account Type list box.

Step 3 Click **Oracle Cloud Shell** to launch the native shell prompt.

Step 4 Copy the command provided in the Multicloud Defense Setup wizard and paste it into your cloud shell. Execute the command.

This command automates the process of creating an IAM policy, OCI group, and an OCI user that facilitate the communication between your OCI account and the Multicloud Defense.

Step 5 Fill in the following fields:

- **OCI Account Name**- Used to identify this OCI Tenant within the Multicloud Defense Controller.
- **Tenancy OCID** - Tenancy Oracle Cloud Identifier obtained from the OCI User.
- **User OCID** - User OCID obtained from the OCI User.
- **Private Key** - API private key that was assigned to the OCI User.

What to do next

Enable traffic visibility.