Onboarding Accounts in Multicloud Defense

Based on your provider that you use, ensure that you complete the prerequisites prior to onboarding your account.

Set up AWS Account

Before you begin

Before connecting your AWS cloud account to Multicloud Defense Controller you need to:

- Ensure you have an active Amazon Web Services (AWS) account.
- Ensure you have an Admin or Super Admin user role in your Security Cloud Control tenant.
- You must have Multicloud Defense enabled for your Security Cloud Control tenant.

For more information on the steps to prepare your AWS account for integration with Multicloud Defense using a CloudFormation template, see AWS Overview. You can watch a video on how to onboard an AWS Account here.

Procedure

Step 1 Set up your account using the easy setup wizard. For more details, see Connect AWS Account

Step 2 Connect and deploy to AWS Account from the Multicloud Defense Dashboard with a CloudFormation template, (which is part of the easy setup wizard). For more details, see Account Onboarding - AWS.

Step 3 Enable traffic visibility. For more details, see Enable traffic for AWS.

Step 4 Enable CloudFormation outputs. For more details, see CloudFormation Outputs.

Step 5 Create or add Controller, Gateway, and Inventory roles. You can set permissions for these roles based on your needs. For more details, see Roles Created by Multicloud Defense.

What to do next

- Secure your account using the easy setup wizard. For more details, see Secure Your Account.
- Monitor the traffic and manage policies and resources.

Set up Azure Account

Before you begin

Get your Azure account and subscriptions ready before you connect and onboard them to the Multicloud Defense Controller. For more details, see the steps outlined in Prepare your Azure account. You can watch a video on how to onboard an Azure account here.

Procedure

Step 1 Set up your account using the easy setup wizard. For more details, see Connect Azure Account.

Step 2 Connect and deploy your Azure Account. For more details, see Connect an Azure Subscription to the Multicloud Defense Controller from the Multicloud Defense Dashboard.

Step 3 Discover assets in your account using the easy setup wizard.

Step 4 Create a policy in the Azure portal.

Step 5 Enable traffic visibility. For more details, see Enable traffic visibility for Azure.

Step 6 (Optional) Based on your needs, you can configure:

a) VNet Route Tables for your Azure Subscription.
b) Post-Onboarding Procedures.
c) VNet Route Tables for your Azure Subscription.
d) Roles Created by Multicloud Defense.
e) Set up Azure VNet – Subnets, Security Groups, Launch ARM Template.

What to do next

- Secure your account using the easy setup wizard. For more details, see Secure Your Account.
- Monitor the traffic and manage policies and resources.

Set up GCP Account

Multicloud Defense supports both set up of accounts using GCP projects and GCP folders, although these components are supported separately. For more details, see GCP Overview. You can watch a video on how to onboard a GCP account here.

Before you begin

Ensure you have:

- An active project for GCP.
- Relevant permissions to create service accounts, VPC, subnets etc.
- Super Admin or Admin access in Security Cloud Control.
- Enabled your tenant for Multicloud Defense in Security Cloud Control.

Procedure

Step 1 Create a Controller Service Account.

Step 2 Create a GCP Firewall Service Account.

Step 3 Set up your account using the easy setup wizard. For more details, see Connect Google Cloud Platform Account.

Step 4 Connect and deploy a GCP Project. For more details, see Connect a GCP Project to the Multicloud Defense Controller from the Multicloud Defense Dashboard.

Step 5 Enable Traffic Visibility. For more details, see Enable Traffic for a GCP Project.

Step 6 (Optional) Set up roles and permissions based on your needs. For more details, see Roles Created by Multicloud Defense.

What to do next

- Secure your account using the easy setup wizard. For more details, see Secure Your Account.
- Monitor the traffic and manage policies and resources.

Set up OCI Account

Prepare your OCI environment using these steps to successfully connect with Multicloud Defense. For OCI-specific documentation on how to accomplish these requirements, see OCI documentation on oracle.com. Watch a video on how to onboard an OCI account here.

- You can use the automated method to prepare your OCI account. For more details, see Overview of Automated Steps.
- You can also use the manual method to prepare your OCI account. For more details, see Overview of Manual Steps.

Before you begin

Before you onboard an OCI tenant to Multicloud Defense, you need to set up your OCI account.

- Ensure you have an active OCI account.
- Ensure you have a Super Admin or Admin role in Security Cloud Control.
- Ensure that Multicloud Defense is enabled in Security Cloud Control.
- To onboard the OCI tenant, you need to subscribe to the US West (San Jose) region. If you do not subscribe to this region, 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 cause an unauthorized error.

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

Procedure

Step 1 Set up account using the easy setup wizard – Connect Oracle Acount.

Step 2 Connect and deploy the OCI account to your Multicloud Defense - Connect the Oracle OCI Tenant to the Multicloud Defense Controller from the the Multicloud Defense Dashboard.

Step 3 Enable traffic visibility using the easy setup wizard.

What to do next

- Secure your account using the easy setup wizard. For more details, see Secure Your Account.
- Monitor the traffic and manage policies and resources.

Discover Assets and Inventory

Once you onboard your accounts, you can get real-time visibility into the current resources deployed in any onboarded cloud accounts. In addition, it provides an interface into VPC flow logs and DNS logs to give a complete picture of your cloud deployment. The controller periodically crawls and keeps tabs on changes to maintain a fresh inventory model of the resources. In the **Discovery** tab, you can see the attributes of your resources and how they are interconnected. For more information about inventory, discovery, security insights, and rules and findings, see Assets and Inventory Discovery.