Azure

Azure Overview

Prepare and connect your Azure environment to Multicloud Defense Controller with the following steps:

- Acquire an Azure subscription. Ensure the subscription is assocaited to an Azure Active Directory.
- Connect an Azure Subscription to the Multicloud Defense Controller from the Multicloud Defense Dashboard, on page 1

If you find that you cannot use the automated script, see the alternative procedure to manually onboard your account here.

Connect an Azure Subscription to the Multicloud Defense Controller from the Multicloud Defense Dashboard

Once you prepared the Azure account and subscription as described in the previous sections, you can link it to the Multicloud Defense Controller.

Step 1 In the CDO menu bar, click Multicloud Defense.

Step 2 Click the Multicloud Defense Controller button.

Step 3 In the Cloud Accounts pane, click **Add Account**.

Step 4 On the General Information page, select Azure from the **Account Type** list box.

Step 5 In step 1, click the link to open an Azure Cloud Shell in bash mode.

Step 6 In step 2, click the **Copy** button.

Step 7 Run the onboarding script in the bash shell.

Note

- If there is another Azure subscription already connected to Multicloud Defense, this script may fail when creating an IAM role with the same existing name. There cannot be more than one IAM role. As a workaround, run the Bash script with the `-p` prefix.
- To support spoke VNet protection across subscriptions, onboard subscriptions using Active Directory app registrations.

Step 8 Provide a name for this Azure account. You can choose to name this the same as your Azure subscription name. This name is visible on the Multicloud Defense Controller accounts page only.

Step 9 (Optional) Provide a description for the subscription.

Step 10 Enter the **Directory ID**, also referred as the Tenant ID.

Step 11 Enter the **Subscription ID** for the subscription being onboarded.

Step 12 Enter the **Application ID**, also referred to as the Client ID, created by the onboarding script.

Step 13 Enter the **Client Secret**, also referred to as the Secret ID.

Step 14 Click **Save & Continue**.

The Azure subscription is onboarded and you are returned to the dashboard to see that the new device has been added.

What to do next

- Post-Onboarding Procedures, on page 2.
- Enable traffic visiblilty.

Post-Onboarding Procedures

Subnets

When configuring your gateway deployment, the Multicloud Defense Controller will prompt you for the **management** and **datapath** subnet information.

The **management** subnet is a public subnet that must be associated with the route table that has a default route to the Internet. The Multicloud Defense Gateway instance has an interface attached to this subnet that it uses to communicate with the Multicloud Defense Controller. This interface is used for policy pushes and other management and telemetry activities between the Multicloud Defense Controller and the Multicloud Defense Gateway instances. Customer application traffic **does not** flow through this interface and subnet. The interface is associated with the**management** security group, which is described in the Security Groups section below.

The **datapath** subnet is a public subnet that must be associated with the route table that has a default route to the Internet. The Multicloud Defense Controller creates a network load balancer (NLB) in this subnet. In addition, a Multicloud Defense Gateway instance has an interface attached to this subnet. The customer applications traffic **flows** through this interface. A security policy is applied to the trafficingressing through this interface. The interface is associated with the **datapath** security group, which is described in the Security Groups section.

Azure VNet Setup

This document describes the requirements and resources (subnets, security-groups) to be created in your VNet so that you can create Multicloud Defense Gateways in the VNet.

Security Groups

The management and datapath security groups are associated with the respective interfaces on the Multicloud Defense Gateway instance, as described in the subnets section above.

The **management** security group must allow outbound traffic that allows the gateway instance to communicate with the controller. Optionally, for inbound rules, enable port 22 (SSH) to allow SSH access to the gateway instance. SSH is not mandatory for the Multicloud Defense Gateway to function properly.

The **datapath** security group is attached to the datapath interface and allows traffic from the Internet to the Multicloud Defense Gateway. Currently the Multicloud Defense Controller does not manage this security group. An outbound rule must exist, allowing the traffic to egress this interface. Inbound ports must be opened for each port that is configured in the Multicloud Defense Controller security policy and used by the Multicloud Defense Gateway.

For example, if an application is running on port 3000 and is proxied by the Multicloud Defense Gateway on port 443, port 443 must be opened on the datapath security group. This example also implies that port 3000 is open on the security group attached to your application.

Launch ARM Template

Use the to create all of the resources described on this page.

This template creates a new VNet. This is very useful to get started on Multicloud Defense without touching your existing production environment.

The template creates the following resources:

- VNet.
- Management subnet.
- Datapath subnet.
- Management security group with outbound rules.
- Datapath security group with outbound rules and Inbound rules for port 443.

You can create additional subnets to run apps and create app-specific security groups, as needed.

Use the following steps to launch an ARM template:

Step 1 Log into your Azure account and Deploy a custom template.

Step 2 Click **Build your own template in the editor**.

Step 3 Copy the content from the ARM template and paste into the editor.

Step 4 Click **Save**.

Step 5 Select the *Subscription*, *Resource group*and the *Region*.

Step 6 Click **Review+ create**.

Step 7 Wait for a few minutes for all the resources to be created.