Azure

Prepare Your Azure Account

Prepare your Azure account and subscription(s) before you connect and onboard them to Multicloud Defense Controller with the following steps:

1. Acquire and register an Azure subscription. Ensure the subscription is associated to the Microsoft Entra ID. Review the list of **App Registrations** in your Azure portal to confirm whether the subscription is correctly linked to Multicloud Defense.
2. Create a custom role for your Azure subscription. This grants Multicloud Defense access to specific resources or actions that would otherwise be blocked.
3. Subscribe to the Azure Event Grid. This allows Multicloud Defense to receive real-time updates and can be configured to send events to subscribers (push) or subscribers can connect to Event Grid to read events (pull). See the "*Create event subscriptions*" chapter in the Azure User Guide for more information.
4. Connect an Azure Subscription to the Multicloud Defense Controller from the Multicloud Defense Dashboard, on page 4. Azure subscriptions encapslulate "technical" resources such as virtual machines. Complete this step to use any Azure-based VMs with Multicloud Defense gateways or any depoyment action.
5. Accept Marketplace Terms. If this is the first time your Azure account is being onboarded to Multicloud Defense, you must accept Cisco marketplace terms. Without this agreement you cannot complete the onboarding action.
6. (Optional) User-assigned Managed Identity for Key Vault and Blob Storage access. Configured in the Azure environment, the key vault and blob storage access is intended to give you more flexibility to use the same identity across different resources, maintaining consistent permissions and identities across services.

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

Note If you have more than one subscription you want to configure with Multicloud Defense, use the procedure in Connect an Azure Subscription to the Multicloud Defense Controller from the Multicloud Defense Dashboard, on page 4 for one subscription and then modify the policy in your Azure portal to add the other subscriptions. You must onboard these subscriptions individually, but you can associate them with Multicloud Defense in bulk.

Register Application in Microsoft Entra ID

Use the following procedure to register the Multicloud Defense application in your Entra ID.

Procedure

Step 1 From your Azure portal, navigate to **Microsoft Entra ID**.

Step 2 Select **App registrations**.

Step 3 Click **New registration**.

Step 4 Provide a name to reference the new app registration e.g. Multicloud Defense Controller In the *Supported account types* choose the second option *Accounts in any organizational directory*.

Step 5 Choose the option appropriate to your organization. Note that the **Redirect URI** is not needed for the creation of the App registration.

Step 6 Click **Register**.

Step 7 In the left navigation bar under the newly created application, click **Certificates & secrets**.

Step 8 Click **+ New client secret**, and then enter the required information in the *Add a client secret* dialog box

- **Description** - Add a description (e.g multicloud defense-controller-secret1)
- **Expires** - Choose **Never**. You can also make this selection at your convenience. You will need to create new secrets when the current one expires)

Step 9 Click **Add**. The client secret is populated under the **Value** column.

Step 10 Copy the **Client secret** into a notepad, as this is shown only once and is never displayed again.

Step 11 In the left navigation bar click **Overview**.

Step 12 Copy the **Application (client) ID** and **Directory (tenant) ID** into a notepad.

Create a custom role to assign to the Application

The CloudFormation template creates a **custom role** that will be assigned to the application created for the Multicloud Defense Controller. The custom role gives the application permissions to read inventory information and create resources (e.g., VMs, load balancers, etc.)

There are multiple ways to create a custom role but we recommend the following procedure:

Procedure

Step 1 Navigate to **Subscription** and click **Access Control (IAM)**.

Step 2 Click on **Roles** and on the top menu bar navigate to click **+Add** > **Add Custom Role**.

Step 3 Give a name to the custom role (e.g., `multicloud defense-controller-role`).

Step 4 Keep clicking **Next** until you get to the JSON editing screen.

Step 5 Click **Edit** on the screen and in the JSON text, under the **permissions > actions** section, copy and paste the following content between the square brackets (no need to maintain the indentation):

```
"Microsoft.ApiManagement/service/*",
"Microsoft.Compute/disks/*",
"Microsoft.Compute/images/read",
"Microsoft.Compute/sshPublicKeys/read",
"Microsoft.Compute/virtualMachines/*",
"Microsoft.ManagedIdentity/userAssignedIdentities/read",
"Microsoft.ManagedIdentity/userAssignedIdentities/assign/action",
"Microsoft.Network/loadBalancers/*",
"Microsoft.Network/natGateways/*",
"Microsoft.Network/networkinterfaces/*",
"Microsoft.Network/networkSecurityGroups/*",
"Microsoft.Network/publicIPAddresses/*",
"Microsoft.Network/routeTables/*",
"Microsoft.Network/virtualNetworks/*",
"Microsoft.Network/virtualNetworks/subnets/*",
"Microsoft.Resources/subscriptions/resourcegroups/*",
"Microsoft.Storage/storageAccounts/blobServices/*",
"Microsoft.Storage/storageAccounts/listkeys/action",
"Microsoft.Network/networkWatchers/*",
"Microsoft.Network/applicationSecurityGroups/*",
"Microsoft.Compute/diskEncryptionSets/read",
"Microsoft.Insights/Metrics/Read"
```

Step 6 **Optional** - If you plan to use multiple subscriptions with Multicloud Defense, you must edit the JSON at `assignableScopes` to add another subscription line or change it to ***** (star) so the custom role can be used with all subscriptions.

Step 7 Click **Save** at the top of the text box.

Step 8 Click **Review + Create** and create the role.

Step 9 Once the custom role is created return to **Access Control (IAM).**

Step 10 On the top menu bar, click **Add** > **Add role assignment**.

Step 11 In the **Role** dropdown, select the custom role created above.

Step 12 In the **Assign access to** dropdown leave it as the default (Azure AD user, group, service principal).

Step 13 In the **Select** text box, type in the name of the application created earlier (e.g. `multicloud defensecontrollerapp`) and click **Save**.

Step 14 In the **Subscription** page, click on the **Overview** in the left menu bar and copy the subscription ID to the notepad.

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.

Procedure

Step 1 In the Multicloud Defense Controller dashboard, click **Add Account** in the Cloud Accounts pane.

Step 2 On the General Information page, select **Azure** from the **Account Type** list box.

Step 3 In step 1, follow the instructions to open an Azure Cloud Shell in bash mode.

Step 4 In step 2, click the **Copy** button.

Step 5 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 6 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 7 (Optional) Provide a description for the subscription.

Step 8 Enter the **Directory ID**, also referred as the Tenant ID.

Step 9 Enter the **Subscription ID** for the subscription being onboarded.

Step 10 Enter the **Application ID**, also referred to as the Client ID, created by the onboarding script.

Step 11 Enter the **Client Secret**, also referred to as the Secret ID.

Step 12 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

- Create a policy in the Azure portal.
- VNet Route Tables for your Azure Subscription, on page 6
- Post-Onboarding Procedures, on page 7.
- Enable traffic visiblilty.

Accept Marketplace Terms

Multicloud Defense Controller creates Gateway instances using a Multicloud Defense virtual machine (VM) image from the Azure marketplace. The Terms and Conditions must be accepted for each subscription. Open the Azure cloud shell from the Azure portal website (on the top menubar towards the right side). Choose or switch to bash shell and execute the following command (replace the subscription-id with your subscription id copied in the previous section):

```
az vm image terms accept --subscription $sub_id --publisher valtix --offer datapath --plan
 valtix_dp_image
```

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.

Procedure

Step 1 In the Multicloud Defense Controller dashboard, click **Add Account** in the Cloud Accounts pane.

Step 2 On the General Information page, select **Azure** from the **Account Type** list box.

Step 3 In step 1, follow the instructions to open an Azure Cloud Shell in bash mode.

Step 4 In step 2, click the **Copy** button.

Step 5 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 6 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 7 (Optional) Provide a description for the subscription.

Step 8 Enter the **Directory ID**, also referred as the Tenant ID.

Step 9 Enter the **Subscription ID** for the subscription being onboarded.

Step 10 Enter the **Application ID**, also referred to as the Client ID, created by the onboarding script.

Step 11 Enter the **Client Secret**, also referred to as the Secret ID.

Step 12 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

- Create a policy in the Azure portal.
- VNet Route Tables for your Azure Subscription, on page 6
- Post-Onboarding Procedures, on page 7.
- Enable traffic visiblilty.

VNet Route Tables for your Azure Subscription

For egress deployments, you may need to create a user-defined routing (UDR) table to manually specify the direction for the spoke network. By default, both Azure and has the ability to automatically identify the routing values because of a private information exchange between the peers. This setup is ideal for ingress gateways; however, it is not suitable for egress gateways.

To override these values or the subnet routing table as a whole for your egress deployment, you must reassign the values in the Azure portal. See Azure documentation for more information.

What Kind of Routing Table Is My Gateway Using?

To determine if your routing table is based on a peer device's VNet or not, view the gateway assigned to your subscription in **Infrastructure** > **Gateways** > **Gateways** and click **View Details**. From this window navigate to the **Troubleshooting** > **Datapath Subnet** tab. If there is no routing table visible, then your subscription is utilizing the default routing table pulled from your peer device.

Roles Created by Multicloud Defense

When you onboard a cloud service account to Multicloud Defense Controller with the provided script, user roles are created within the parameters of the cloud service provider to ensure that communication between the services are protected. Depending on the cloud service provider, different roles and permissions are created.

The following roles are created when you onboard an account.

Azure IAM Roles

You need to create a custom role that will be assigned to the application created for the Multicloud Defense Controller. The custom role gives the application permissions to read inventory information and create resources such as VMs, load balancers. The custom role can be created in multiple ways. One of the easiest ways is to navigate to your subscription and click Access Control (IAM).

When you add a custom role, you need to name the role and edit the JSON file. This file addresses all of the permissions required to allow communication and data transfer between the sbuscription and the Multicloud Defense Controller. The following list are all the required permissions for this:

```
"Microsoft.ApiManagement/service/*",
"Microsoft.Compute/disks/*",
"Microsoft.Compute/images/read",
"Microsoft.Compute/sshPublicKeys/read",
"Microsoft.Compute/virtualMachines/*",
"Microsoft.ManagedIdentity/userAssignedIdentities/read",
"Microsoft.ManagedIdentity/userAssignedIdentities/assign/action",
"Microsoft.Network/loadBalancers/*",
"Microsoft.Network/natGateways/*",
"Microsoft.Network/networkinterfaces/*",
```

```
"Microsoft.Network/networkSecurityGroups/*",
"Microsoft.Network/publicIPAddresses/*",
"Microsoft.Network/routeTables/*",
"Microsoft.Network/virtualNetworks/*",
"Microsoft.Network/virtualNetworks/subnets/*",
"Microsoft.Resources/subscriptions/resourcegroups/*",
"Microsoft.Storage/storageAccounts/blobServices/*",
"Microsoft.Storage/storageAccounts/listkeys/action",
"Microsoft.Network/networkWatchers/*",
"Microsoft.Network/applicationSecurityGroups/*",
"Microsoft.Compute/diskEncryptionSets/read",
"Microsoft.Insights/Metrics/Read"
```

Post-Onboarding Procedures

Use the following procedures to wrap up and secure your Azure account with Multicloud Defense.

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.

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.

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 provided template 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 provided template will create 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:

Procedure

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.