AWS

AWS Overview

Multicloud Defense has created a CloudFormation template that you use when connecting an AWS account to the Multicloud Defense Controller.

To prepare cloud account for integration with Multicloud Defense Controller, there are certain steps that need to be performed in the cloud account. Below are the prerequisite steps you need to perform before connecting your AWS cloud account to Multicloud Defense Controller. This is intended to provide an overview of the operation and not intended to be performed manually. In CloudFormation section, there are details of deployments and parameters information.

Overview of steps

1. Create a cross account IAM role that's used by the Multicloud Defense Controller to manage your cloud account.
2. Create an IAM role that is assigned to the Multicloud Defense Gateway EC2 instances that run in your account.
3. Create a CloudWatch event rule that transfers the management events to the Multicloud Defense Controller.
4. Create an IAM role that is used by the above CloudWatch event rule that gives it the permissions to do the transfer of the management events.
5. Optionally create a S3 bucket in your account to store CloudTrail Events, Route53 DNS query logs and VPC Flow Logs.
6. Enable Route53 DNS Query Logging with the destination as the S3 Bucket created above and select the VPCs for which query logging must be enabled.
7. Enable CloudTrail to log all the management events to the S3 Bucket created above.
8. Enable VPC Flow Logs with destination as the S3 Bucket created above.

Connect AWS Account to Multicloud Defense Controller from The Multicloud Defense Dashboard

Multicloud Defense has created a CloudFormation template that makes it easy to connect an AWS account to the Multicloud Defense Controller.

Before you begin

You must have requested a Multicloud Defense Controller for your CDO tenant before you begin.

Note Multicloud Defense Controller version 23.10 defaults to IMDSv2 in the AWS EC2 instance when using Multicloud Defense Gateway version 23.04 or newer. For more information about the difference beween IMDSv1 and IMDSv2, see AWS documentation.

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

Step 2 Click Multicloud Defense Controller.

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

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

Step 5 Click **Launch Stack** to download and deploy our CloudFormation template. This should open up another tab to deploy the template. Login to AWS is required.

Step 6 Acknowledge that the AWS CloudFormation might create IAM resources with custom names.

Step 7 Fill in these values:

- **AWS Account Number**: Enter the AWS account number of the account you wish to secure. This number can be found in the output value CurrentAccount of the CloudFormation Template.
- **Account Name**: Enter the name you want to give your account once it has been onboarded.
- **Description:**(Optional) Enter an account description.
- **External ID**: A random string for IAM role's trust policy. This value will be used in the controller IAM role created. You can edit or regenerate the External ID.
- **Controller IAM Role**: This is the IAM role created for theMulticloud Defense Controller during CloudFormation Template (CFT) deployment. Look for the output value MCDControllerRoleArn in CFT stack. It should be something similar to this: `arn:aws:iam::<Acc Number>:role/ciscomcdcontrollerrole`.
- **Inventory Monitor Role**: This is the IAM role created for Multicould Defense Inventory during CFT deployment. Look for the output value MCDInventoryRoleArn in CFT stack. Should be something similar to this: `arn:aws:iam::<Acc Number>:role/ciscomcdinventoryrole`.

Step 8 Click **Save and Continue**.
You are returned to the Multicloud Defense dashboard where you will see that the you have a new AWS cloud account recorded.

What to do next

Enable traffic visibility.

CloudFormation Outputs

From the **Outputs** tab, copy and paste the following informationin to a text editor:

- CurrentAccount (This is your AWS Account ID where applications run and Multicloud Defense Gateways will be deployed)
    - MCDControllerRoleArn
    - MCDGatewayRoleName
    - MCDInventoryRoleArn
    - MCDS3BucketArn
    - MCDBucketName