Deploy Secure Dynamic Attribute Connector in FMC

Contents

Introduction

This document describes about Cisco Secure Dynamic Attribute Connector In FMC.

Background – Problem

CSDAC (Cisco Secure Dynamic Attributes Connector) can be integrated into FMC (Firepower Management Center), providing the same level of functionality as the standalone CSDAC application and CSDAC in CDO. For standalone CSDAC, it relieves customers from the overhead of administering and maintaining a separate machine for CSDAC. As a Network Admin, I want the programmatic interfaces to be easy to integrate and keep up to date with changes to external dynamic environment providers. This integration solves the problem of gathering attributes from dynamically changing cloud environments without deploying a policy.

Solution (Summary)

CSDAC can now be configured in FMC to fetch tag attributes from Azure, vCenter, AWS, GCP, Office 365, and Azure Service Tags, providing feature parity with the standalone CSDAC and CSDAC in CDO.

- You can now choose to use
  - CSDAC in FMC (or)
  - CSDAC in CDO (or)
  - Standalone CSDAC
- Target Market: Enterprise, Service Provider

Dynamic Attributes Connector in FMC Summary

FMC Dynamic Attributes Connector:

- **Dashboard** screen to build and operate the Dynamic Attribute Connector features.
- FMC UI to configure Source workload **Connectors** (AWS, Azure, vCenter, Office 365, GCP)
- FMC UI to define dynamic attribute **filters** to create Dynamic Objects

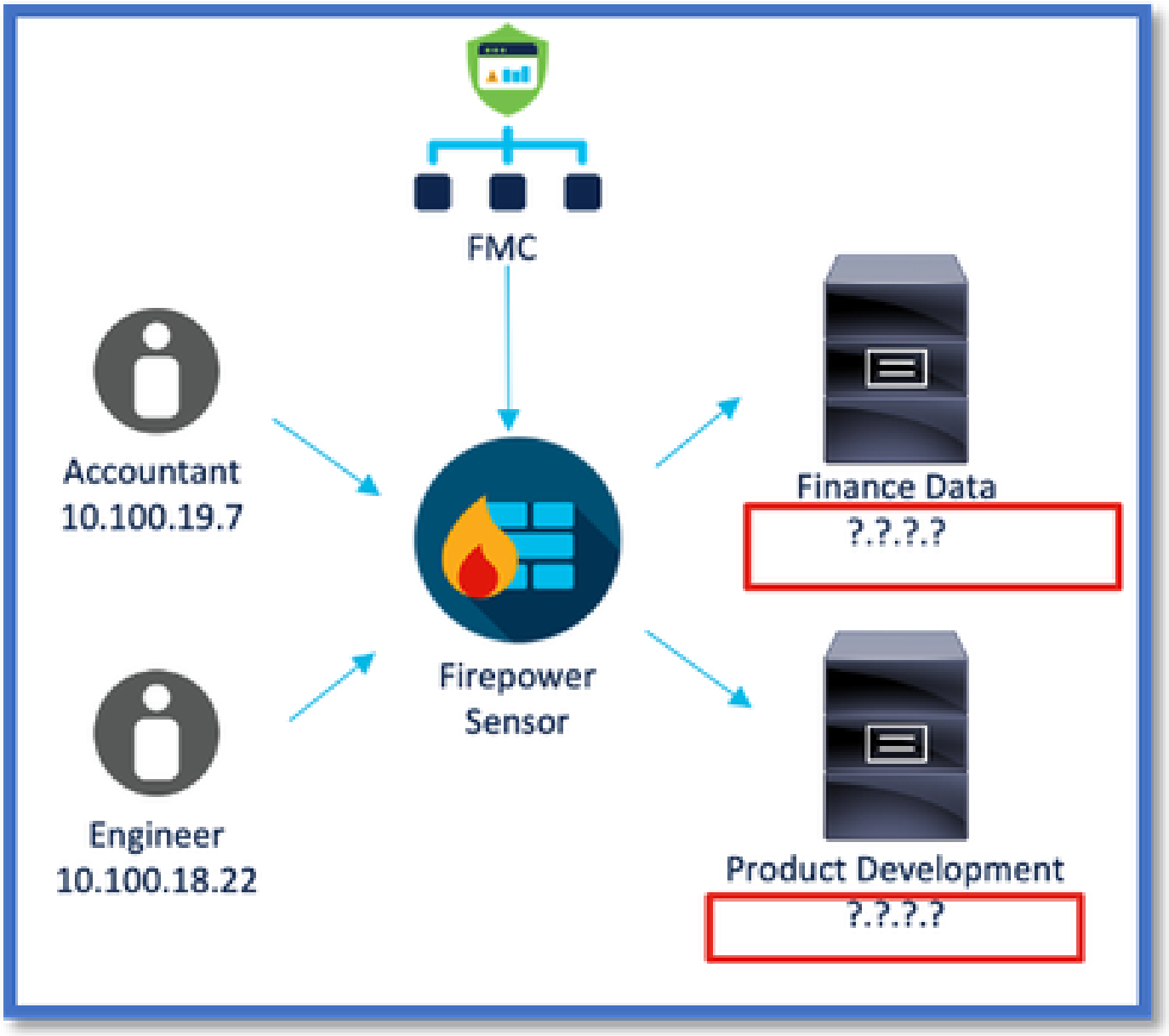
Deployment Examples

On-Prem CSDAC

Last year, I deployed a dedicated VM for CSDAC to collect attributes from my AWS and Azure Accounts.

The Problem

Now, my organization has moved to Cloud, and I cannot deploy and manage a dedicated Virtual Machine for CSDAC in my environment.



Option 1: Use Dynamic Attributes Connector built inside FMC

You can fix the problem by using Dynamic Attributes Connector built inside FMC. The dynamic objects created by it can be used in Access Policy.

Option 2: Use cloud-delivered Dynamic Attributes Connector in CDO

You can fix the problem by using Dynamic Attributes Connector in CDO. The dynamic objects created by it can be used in

- CDO cloud-delivered FMC
- CDO on-prem FMC

Prerequisites, Supported Platforms, Licensing

Minimum Supported Software & Hardware Platforms

Min Supported Manager Version	Managed Devices	Min Supported Managed Device Version Required	Notes
FMC 7.4	Any FTD Supported	Any 7.0+ FTD	

** Dynamic Attributes Connector is not supported on FDM-Managed Devices*

Components Used

The information in this document is based on these software and hardware versions:
• Cisco Firewall Management Center running 7.4
• Cisco Firepower Threat Defense running 7.4 or higher.
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Feature Details

Standalone CSDAC Overview (Currently released - 7.4)

The Cisco Secure Dynamic Attributes Connector enables you to use tags from various cloud service platforms in Firewall Management Center (FMC) access control rules.

On-Prem CSDAC is installable on a Linux Machine, supports getting attributes from:

- AWS,Azure,VMware vCenter and NSX-T,Office 365,Azure Service Tags,GCP,GitHub.

CSDAC in CDO Overview (Currently released - 7.4)

Supports the same functionality as On-Prem CSDAC with no need to install and maintain a dedicated application.

vCenter connector is not currently supported in CDO.

Supports sending the received attributes to cloud-delivered FMC and On-Prem FMC in CDO.

CSDAC in FMC

Supports the same functionality as Standalone CSDAC with no need to install and maintain a dedicated application.

CSDAC in FMC supports getting attributes from:

- AWS,Azure,VMware vCenter and NSX-T,Office 365,Azure Service Tags,GCP,GitHub

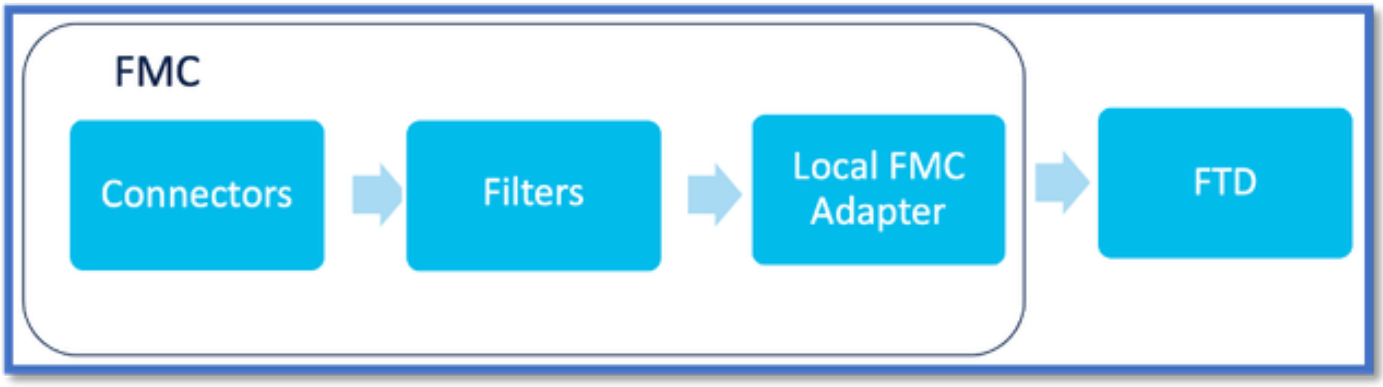
There is no explicit adapter configuration here as it is local to FMC.

How It Works

Connectors are used to get attributes from AWS, Azure, o365, vCenter.

Local Adapter is then used to save these streamlined attributes and its IP mappings in FMC as dynamic objects.

FMC sends the mapping real time to FTD (without deploy).



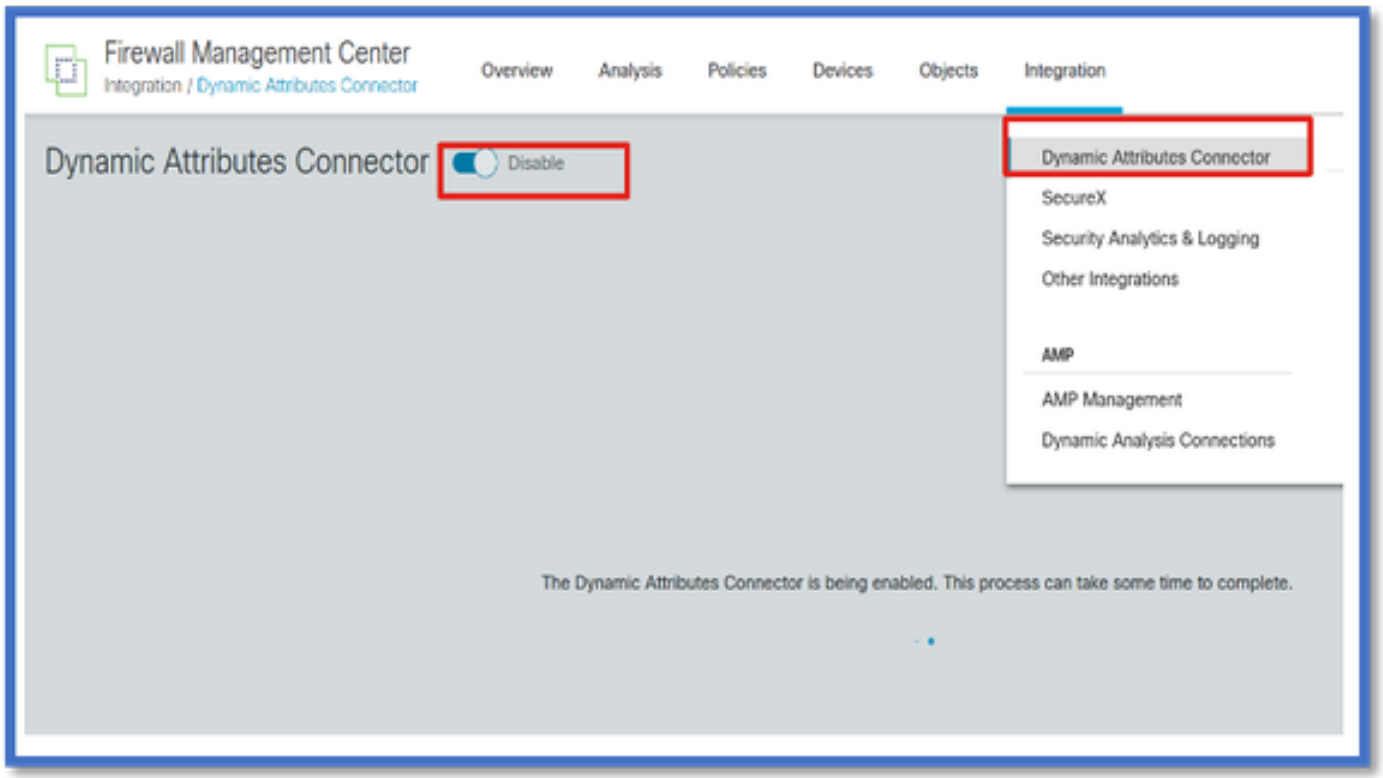
Enable CSDAC in FMC

Navigate to Integration > Dynamic Attributes Connector.

Use Toggle button to enable the connector.

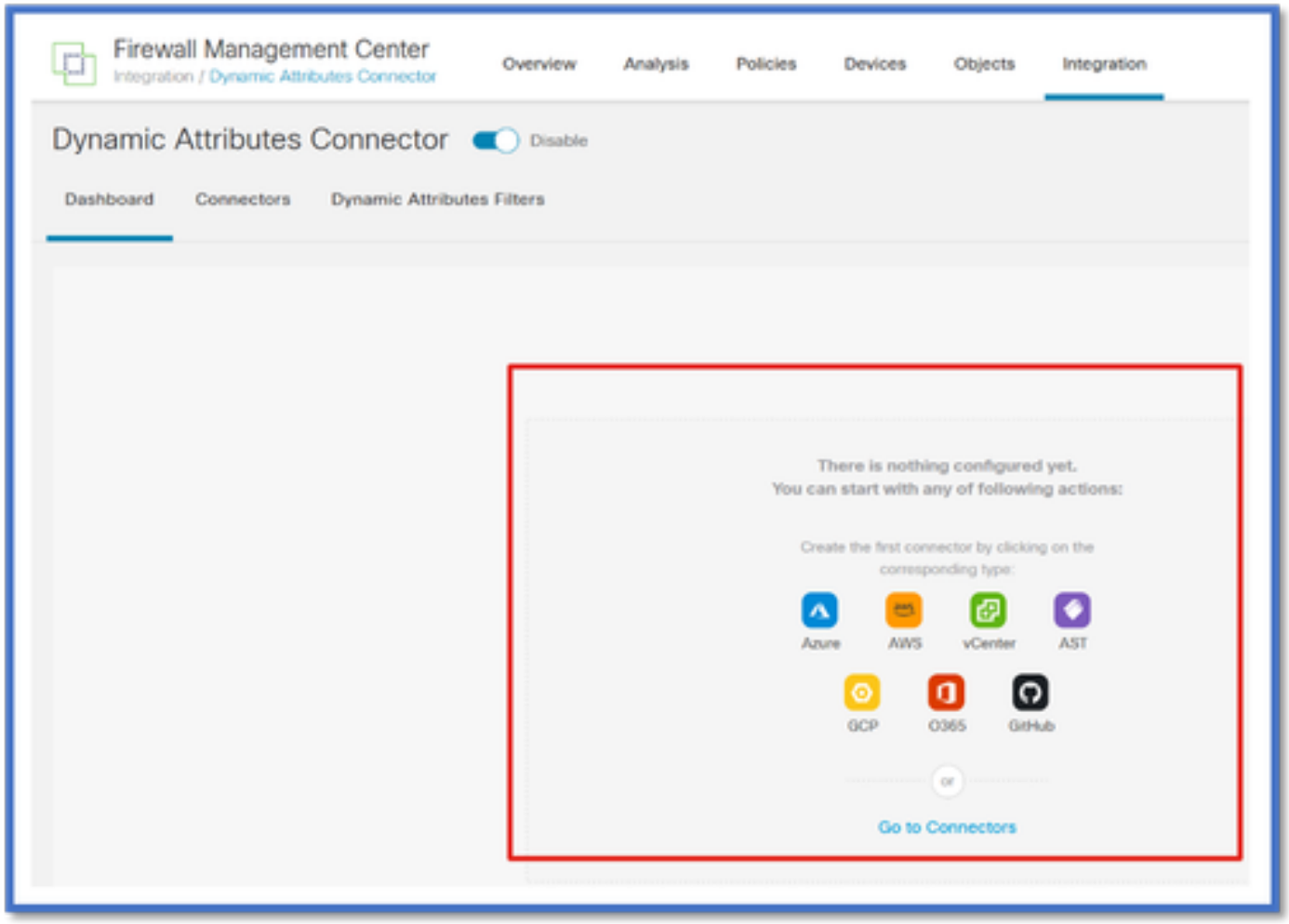
FMC takes a few minutes to download and bring up the docker images and containers.

This can only be configured in FMC global domain.



CSDAC Dashboard

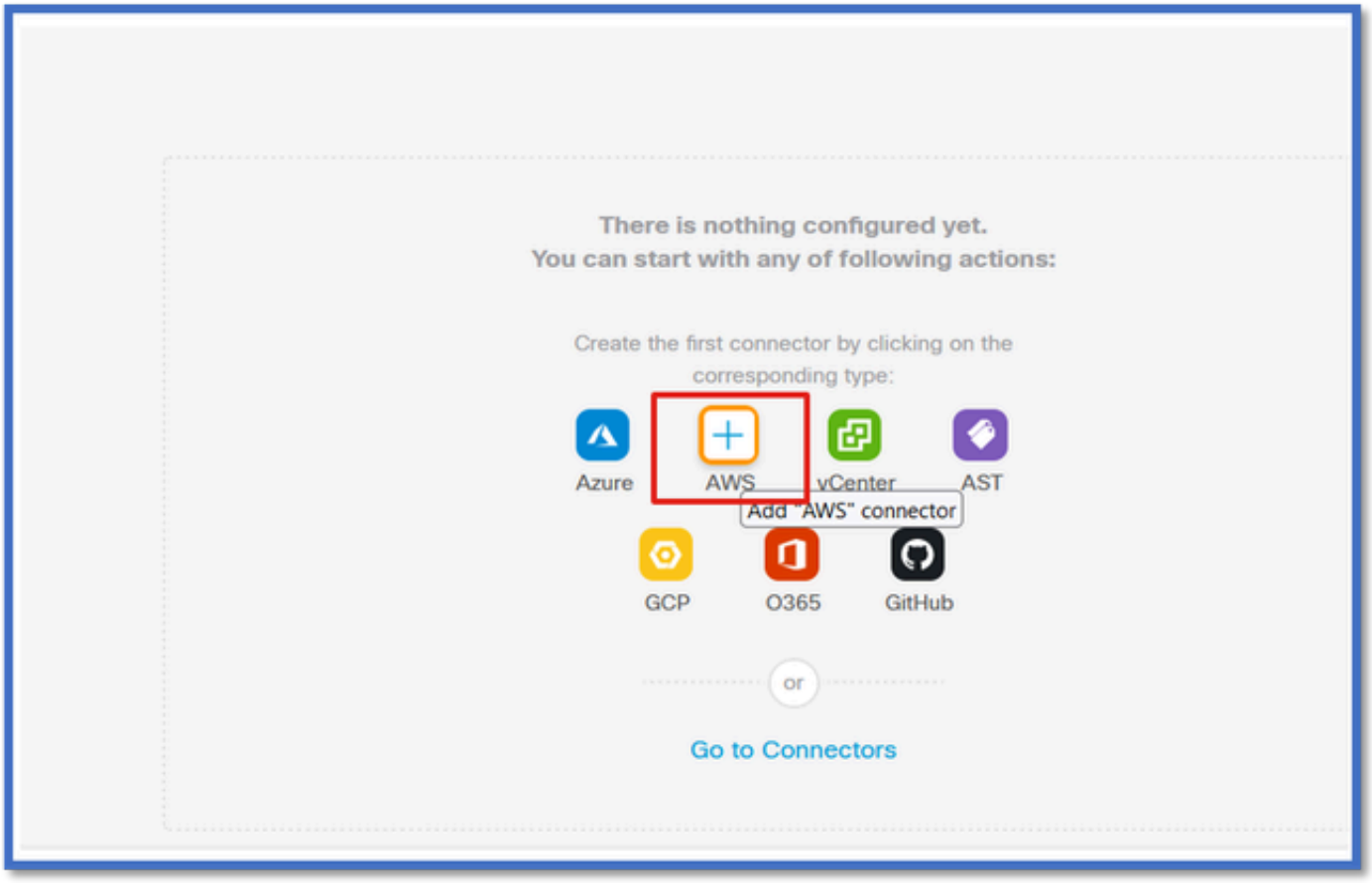
After enabling CSDAC, user is presented with CSDAC Dashboard page. Dashboard is used to both configure and view consolidated connectors and filter.



Configure Connectors

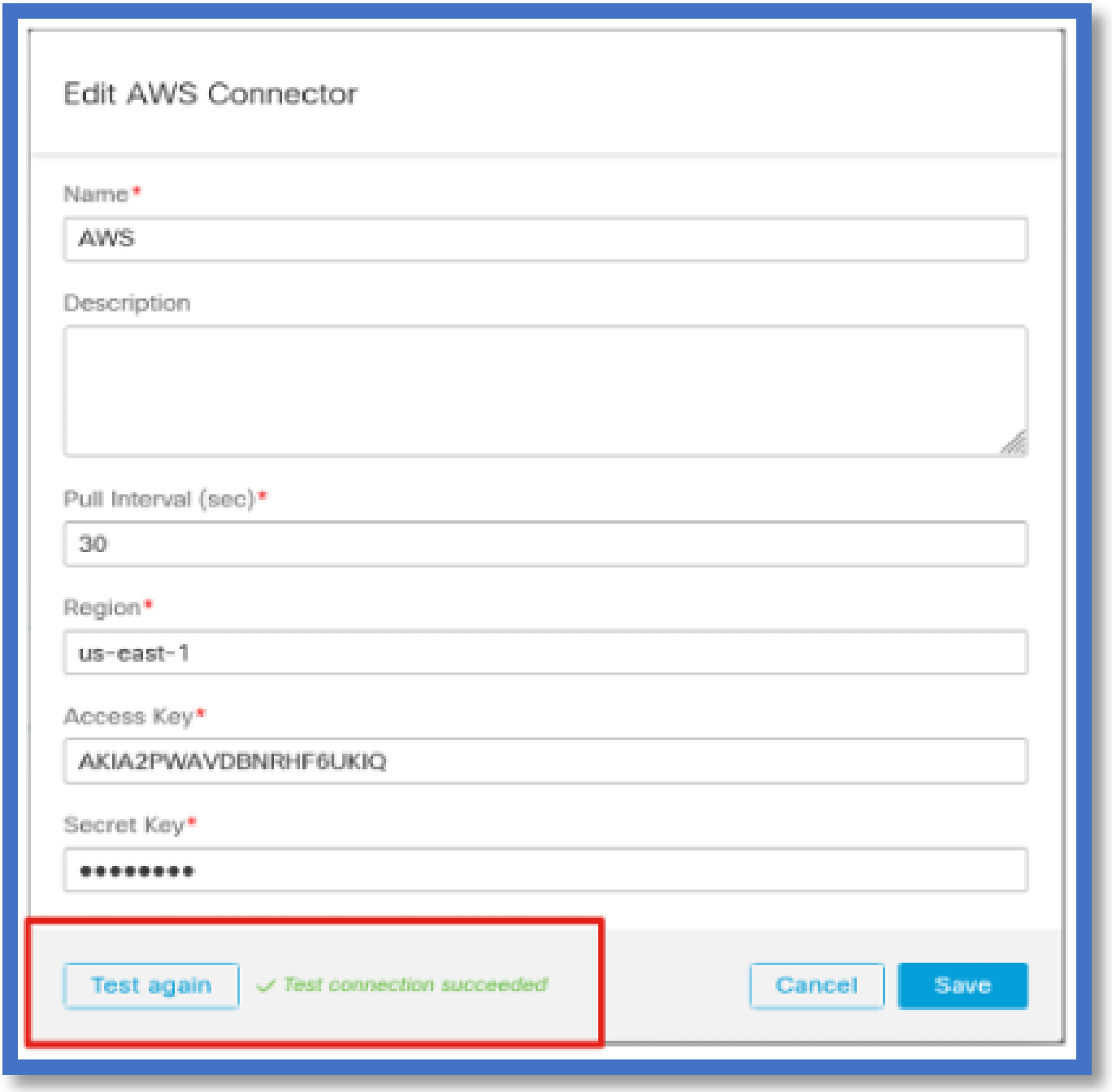
Add Connectors from Dashboard

On the Dashboard, click on the icon for the desired connector to add it.



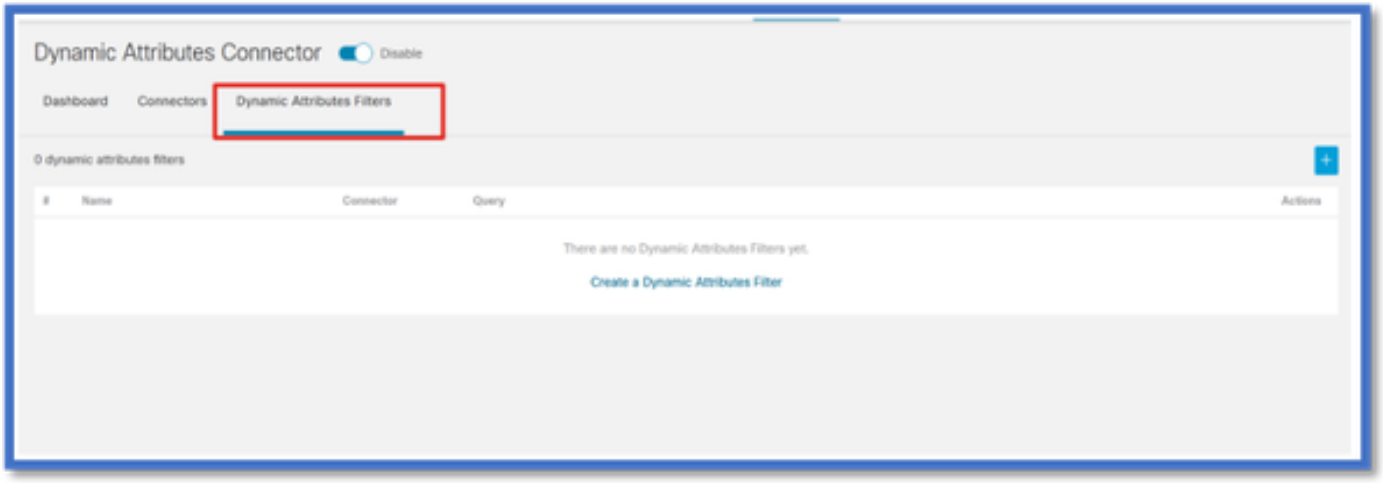
Configure a time interval (in the Pull Interval field) so that the connectors can pull information from providers with the configured periodicity.

Enter the provider credentials to get the tag attributes. Once you have configured the connector, you can test the connector by clicking on the Test Button.



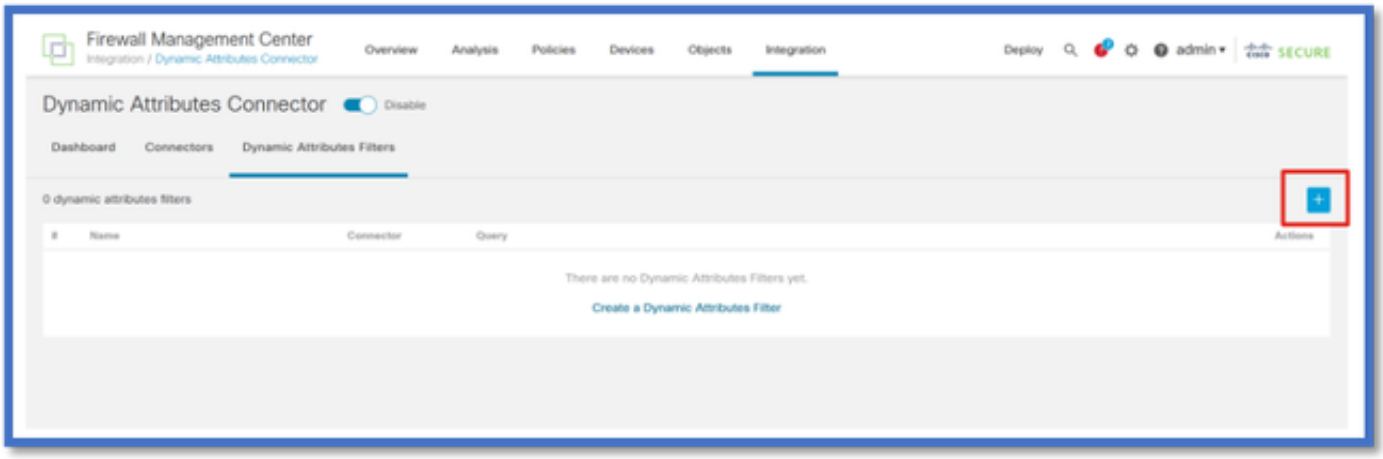
Configure Filters

Click on the “Dynamic Attribute Filters” tab in the “Dynamic Attributes Connector” menu to go to the Dynamic Attributes Filters page.



Adding Filters

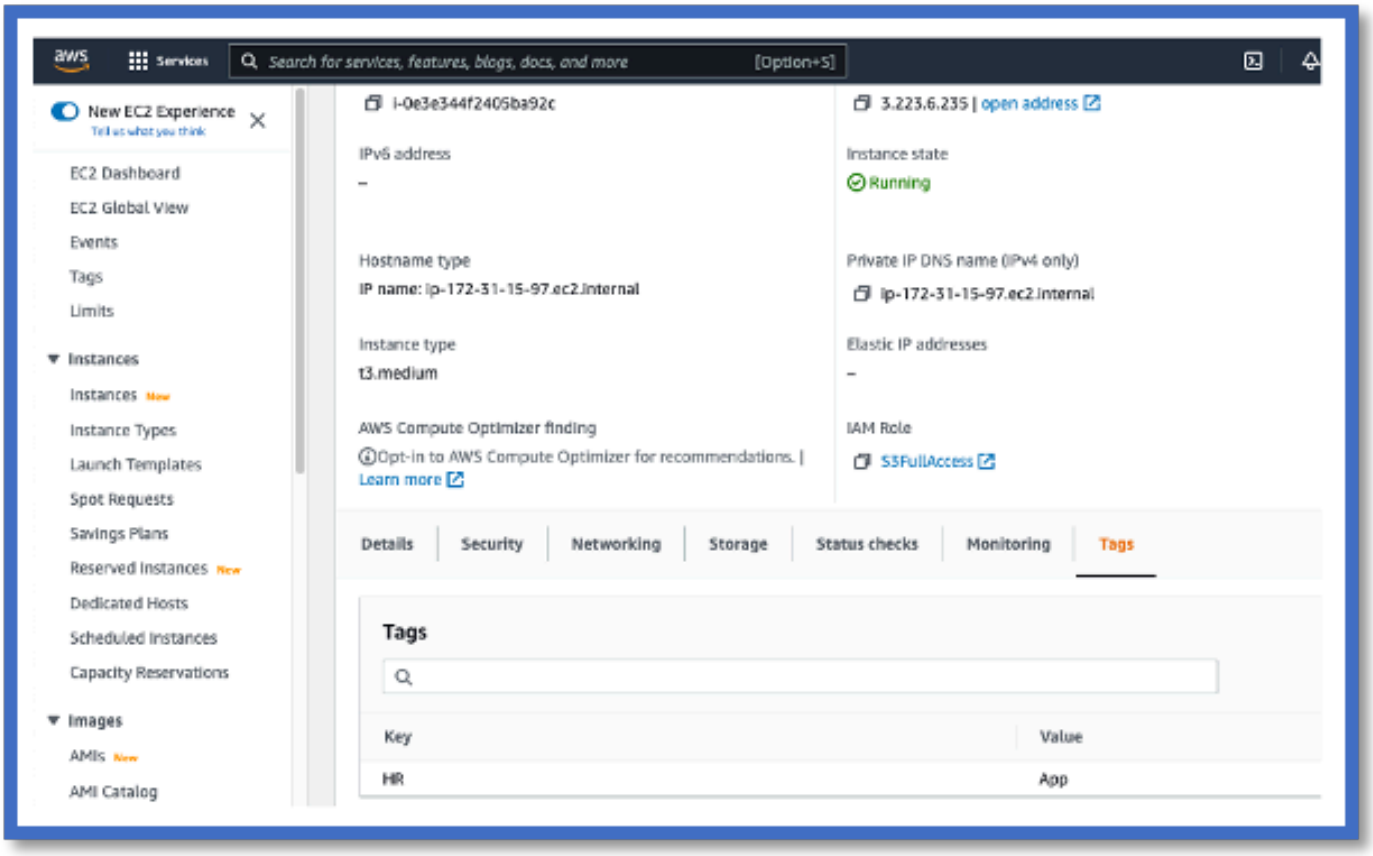
Click on the + button to create a filter for attribute connectors.



Add AWS tags

For example, we can assume you are interested in the key ‘HR’ and value ‘App’ in AWS workloads.

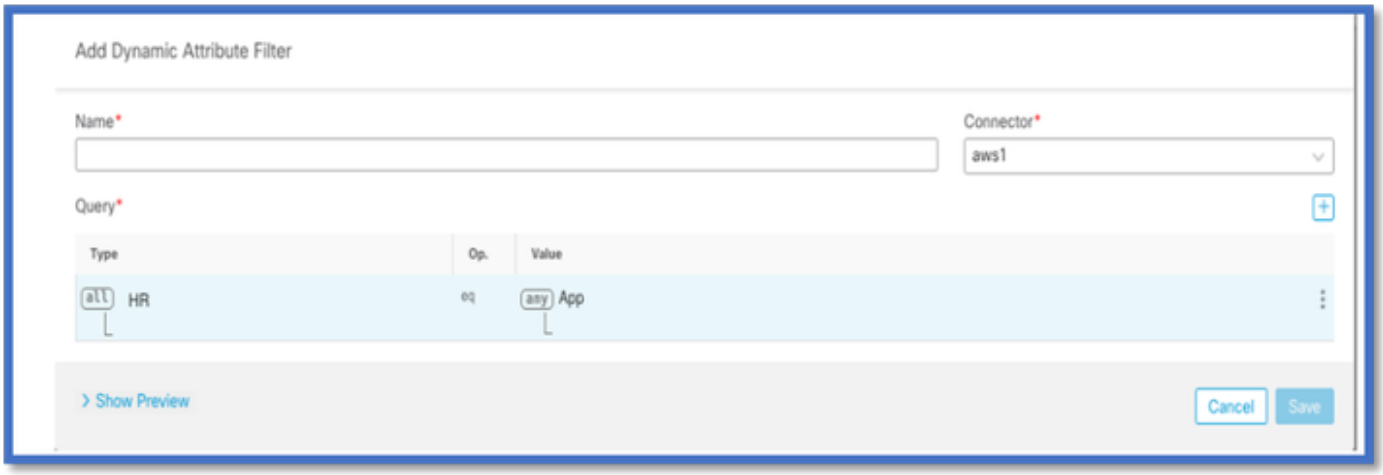
This is what it would look like in AWS.



CSDAC in FMC

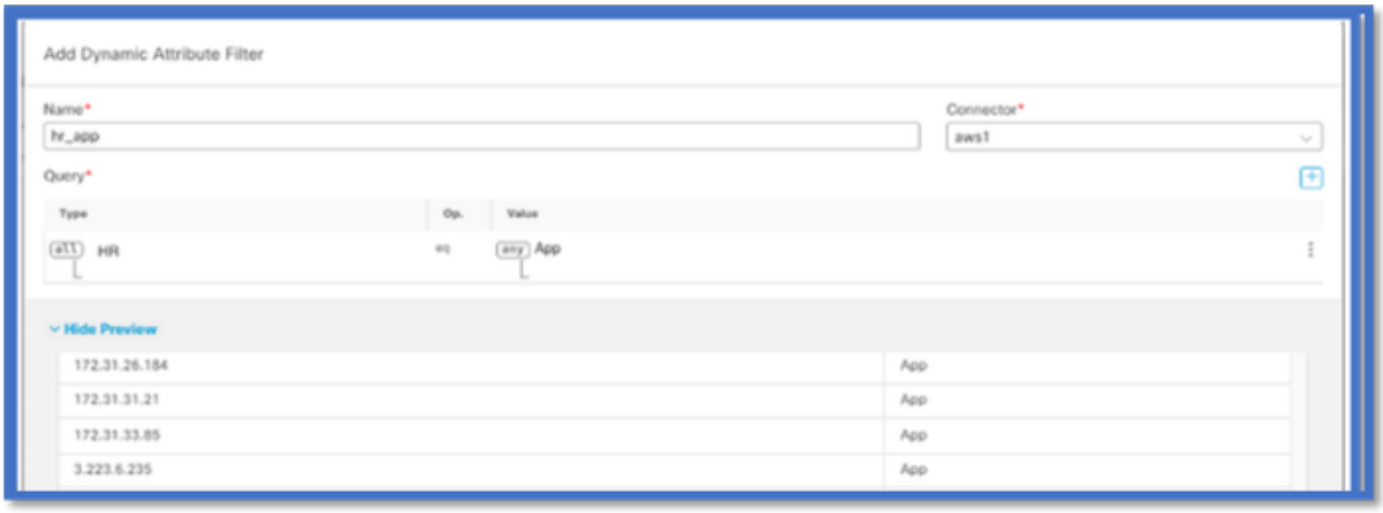
You can create a ‘HR equals App’ rule by clicking on the + button.

The local FMC adapter would send the matching IP addresses as dynamic object mappings to FMC



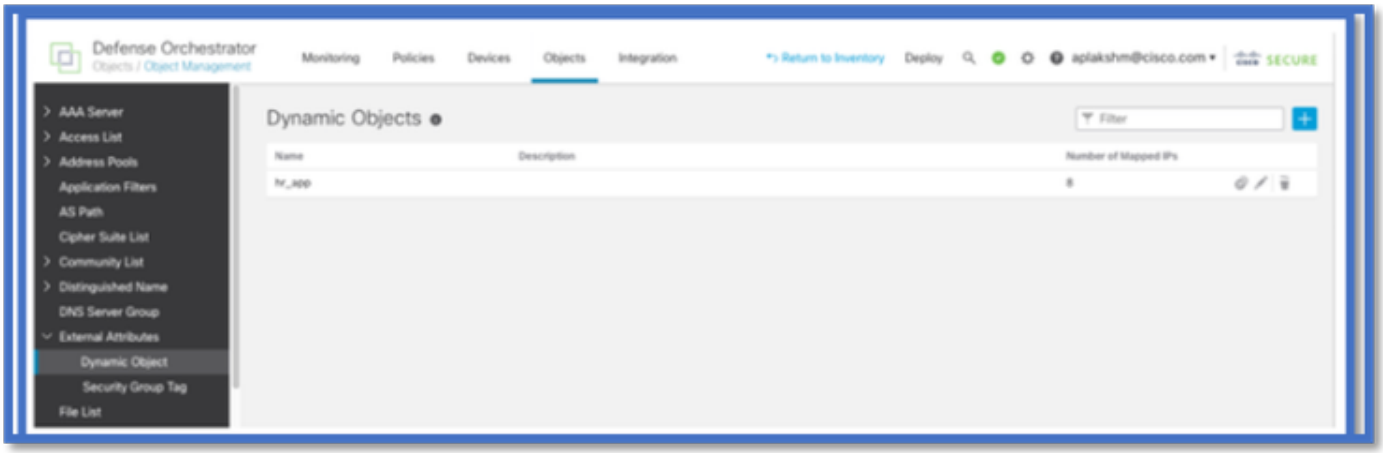
Preview

You can also view the matching IP addresses of a particular attribute rule by clicking the ‘Show | Hide Preview’ button.



Dynamic Objects

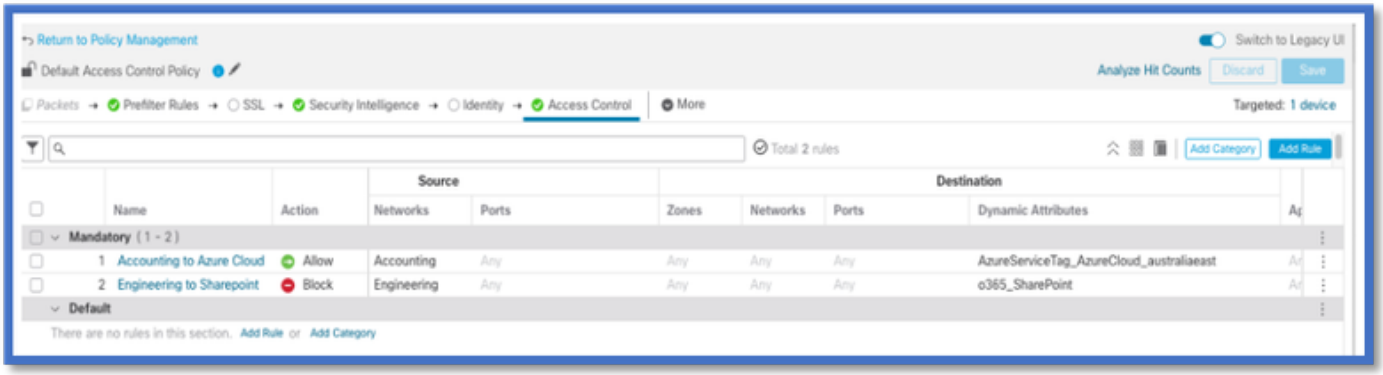
View the Dynamic objects created by CSDAC in Objects > External Attributes, Dynamic Object in FMC



AC Policy

Configuration: Access Policy

In FMC, add access policy to allow or block the received dynamic objects from Dynamic Attribute Connector.



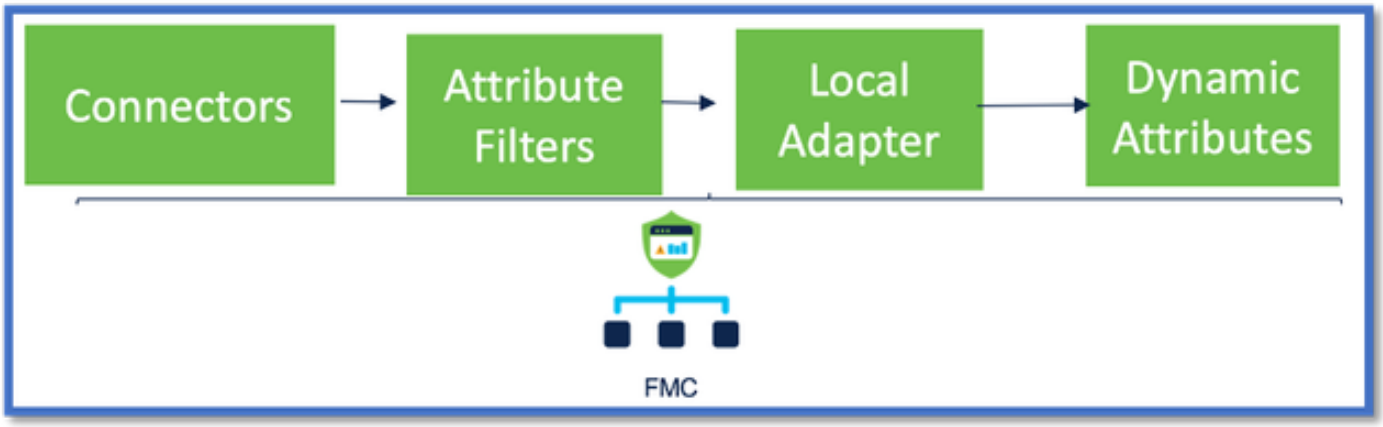
Platform Limits

- Connector limits are based on available FMC memory.
- vFMC would need an extra 1GB memory to support 5 connectors
- Azure AD realm is also included in the limit, as it is also a CSDAC container.

Models	**No of Connectors Supported**	**Platforms**	**Limit based on Memory**
Basic	Only Azure AD	1600	32GB
Small	5	vFMC	> 32 GB
Medium	10	vFMC 300, 2600	>= 64 GB
Large	20	4600	>= 128 GB

Troubleshooting / Diagnostics

Troubleshooting is best performed by tracing dynamic object(s) from CSDAC Connectors to Dynamics Attributes in FMC.Many internal logs refer to this feature as ‘muster’. You can peek into system state along the broadcast chain to isolate problems. CSDAC uses Docker containers. Messages and names of logs and other files must be referred to as “docker”



Check the Connectors

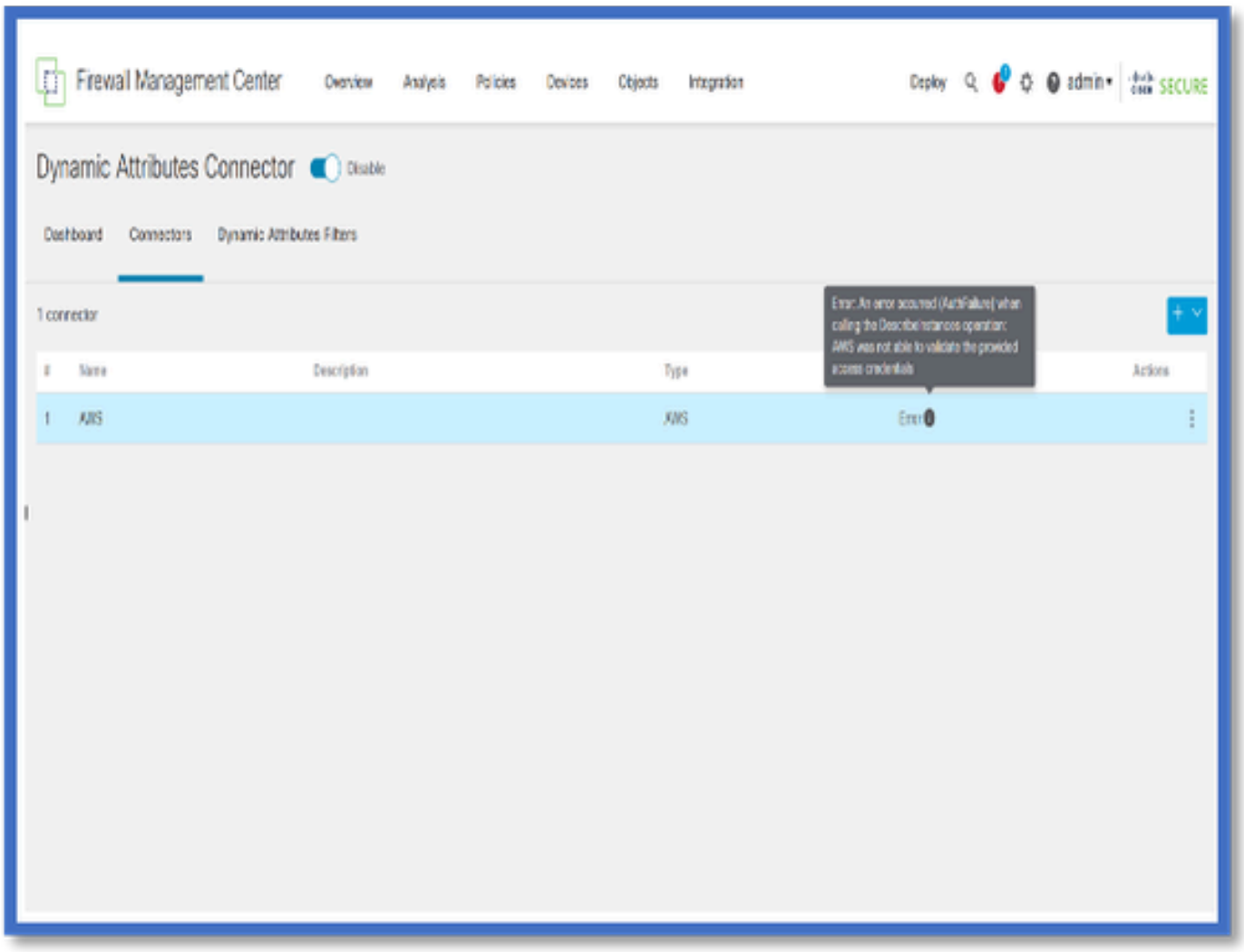
First make sure Connectors can connect to vCenter, AWS, or Azure servers.

If Connectors are not configured correctly, then downstream processes cannot obtain tag information.

View Connectors from the Connectors Tab

Connector status is displayed in status field and updated every 15 seconds.

Here, we see that connector was unable to authenticate using the provided credentials.



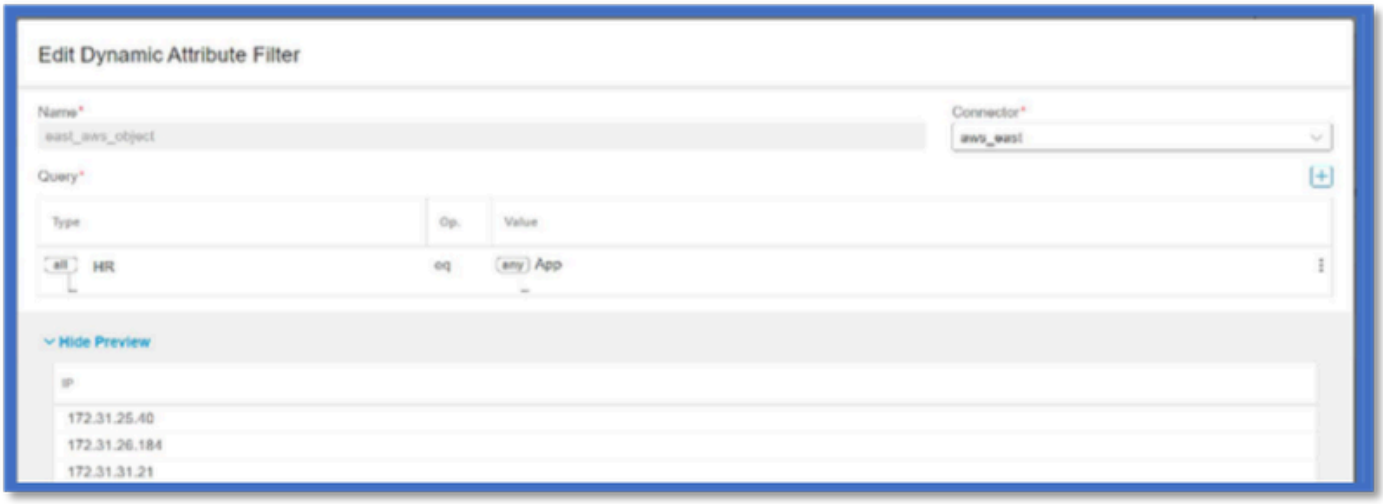
Check the Attribute Filters

Make sure the Rule preview shows the matching IP addresses for your query condition.

If there are no matching IP addresses, then FMC cannot get the dynamic object mappings.

Checking the Attribute Filters

Check that Dynamic Attribute IP mappings are available in Preview. Show preview button is available on Dynamic Attribute Filter edit popup.



Check the Dynamic Objects in FMC UI

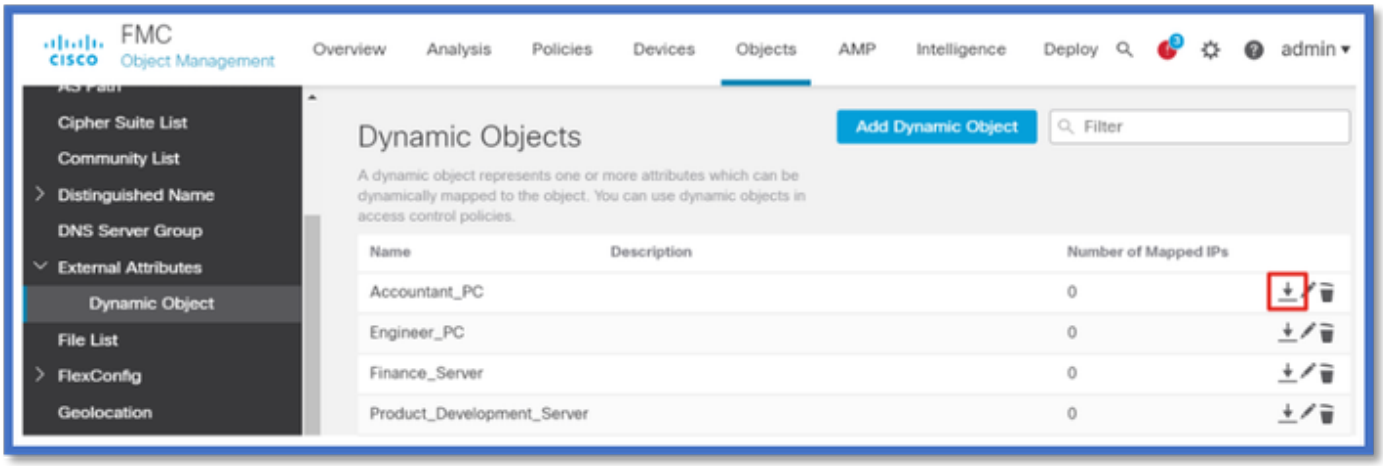
First, make sure FMC server contains the bindings you expect.

- Look under Object Management, External Objects tab, check Dynamic Objects for bindings.
- If FMC does not get the bindings, then FTD cannot get them.

Check FMC Health Monitor and Notifications for CSDAC Health Alerts.

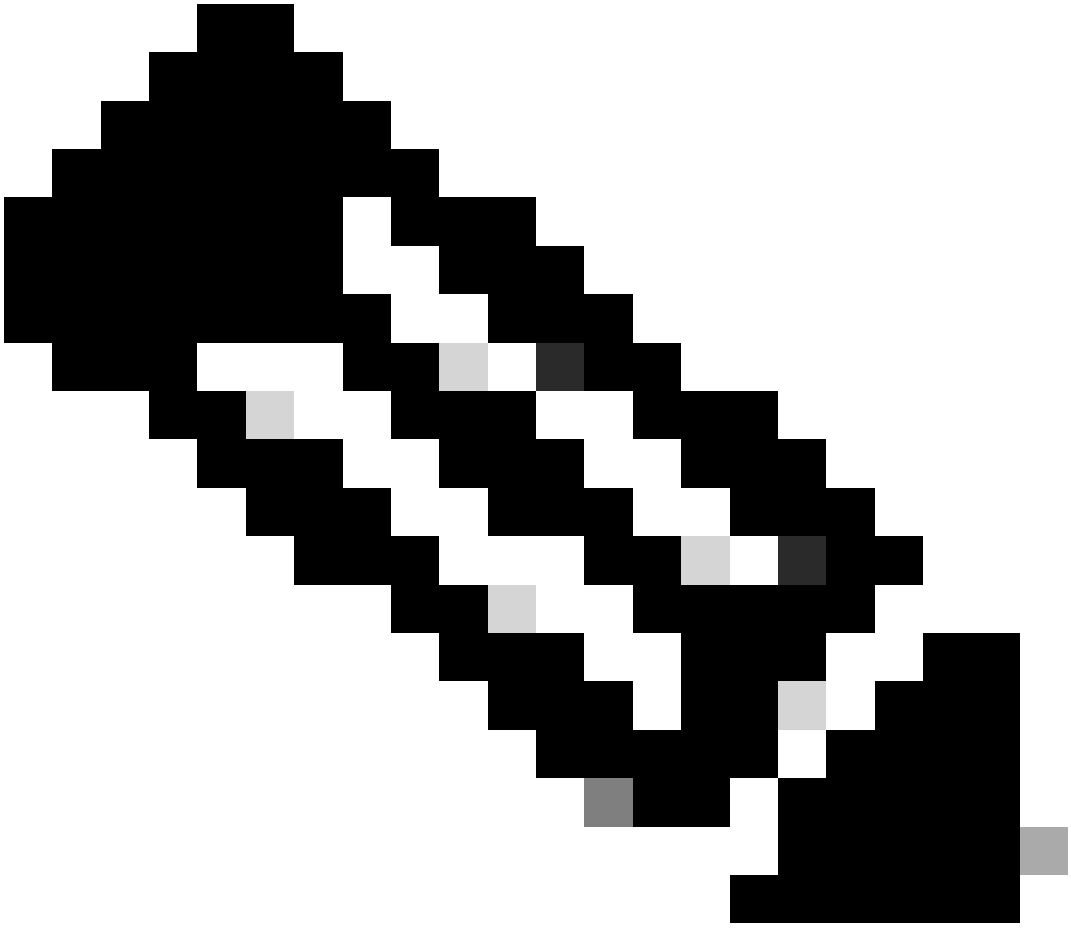
Checking Dynamic Objects

FMC Object Manager allows you to download current Dynamic Object IP addresses.

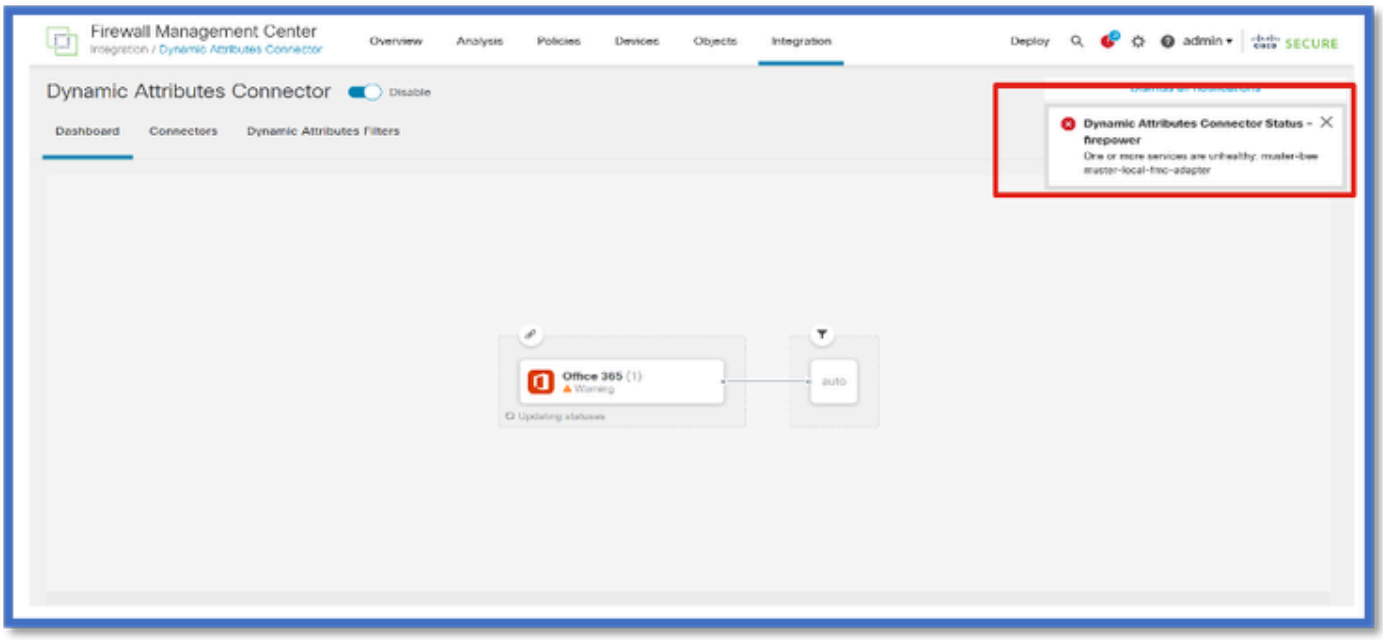


CSDAC Health Alerts

FMC's Task Manager displays Health Alerts if any core service, including the Dynamic Attributes Connector, is down. The Alert contains information regarding service name and status.

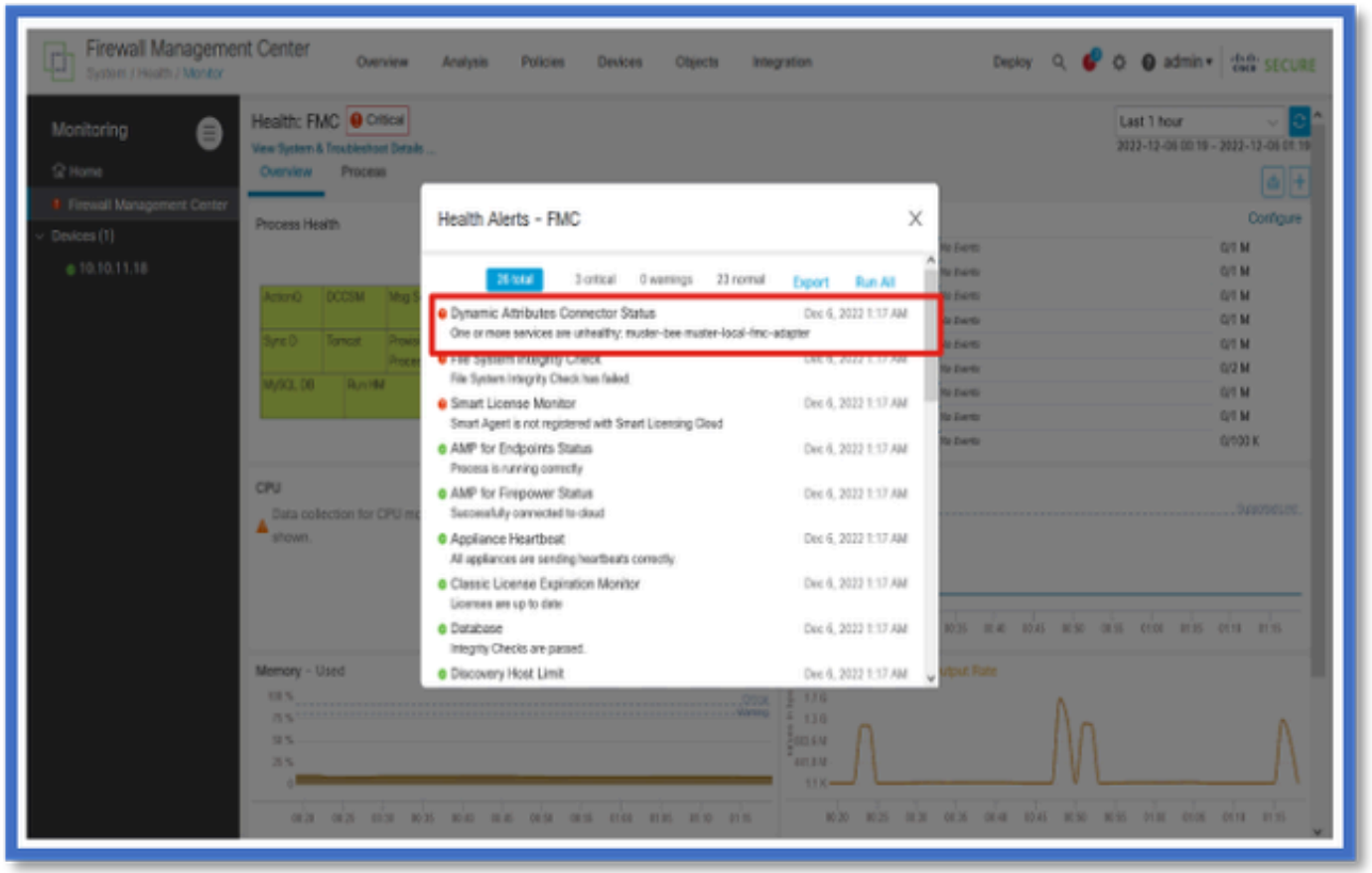


Note: We still have the “muster” naming in several notifications and it is required here to provide service name for detailed information.



Here we see that muster-bee and muster-local-fmc-adapter are “unhealthy”.

If error indicates any of the core services, then troubleshoot logs need to be collected for debug.



CSDAC in Troubleshoots

Generating a CSDAC Troubleshoot

- CSDAC logs are automatically collected during FMC Troubleshoot generation.The bundle contains

Docker status, logs, and data needed to debug the problem offline.
- Good practice is to enabling CSDAC debug mode before reproducing error for which troubleshoot logs are collected .

From /usr/local/sf/csdac call ./muster-cli debug-on

Find the CSDAC logs in untarred Troubleshoot in these folders:

/results-XX/command-outputs/csdac_troubleshoot/info

This contains the data stored in the etcd database.

/results-XX/command-outputs/csdac_troubleshoot /log

This contains the logs from the docker containers.

/results-XX/command-outputs/csdac_troubleshoot/status.log

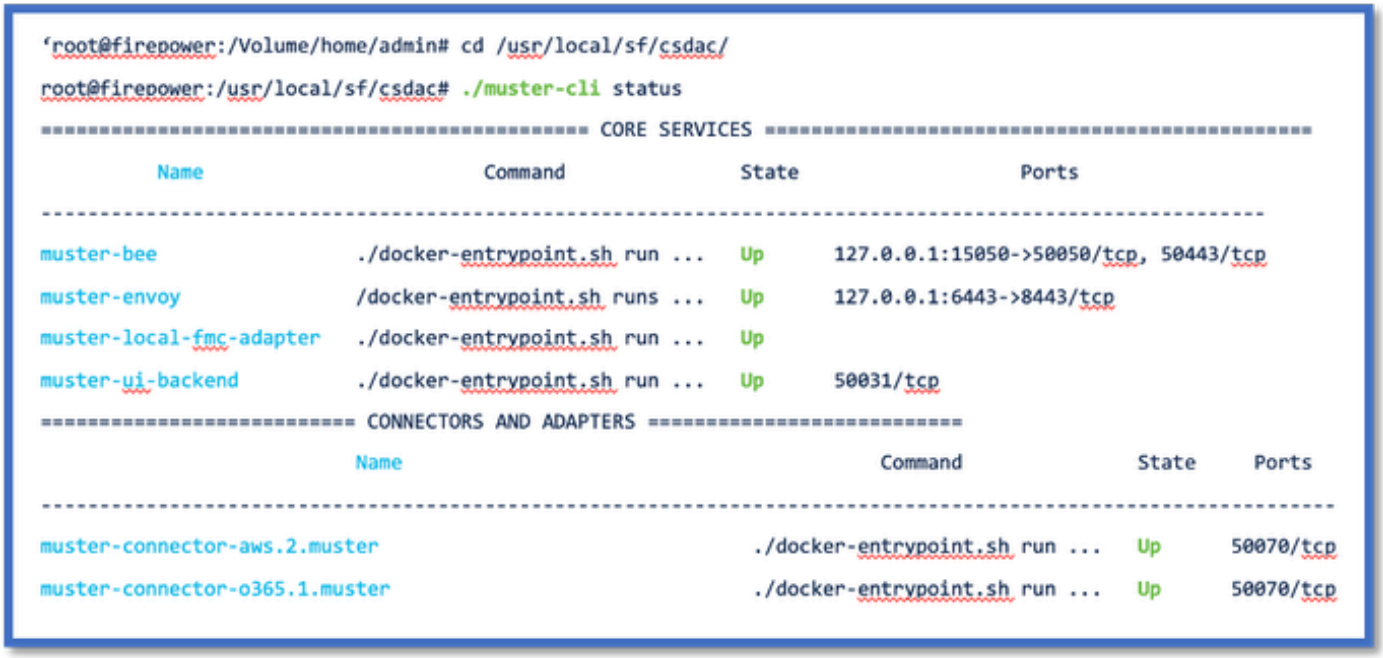
This shows the container status, versions and docker image details.

CLI Troubleshooting

muster-cli script can be used to check the status of CSDAC from FMC CLI.

If the status for any service is “Exited” or otherwise different from “Up”, then start by checking logs for that container.

The container Name is needed for getting logs; it can be obtained from the output.



CSDAC Debug Mode

‘muster-cli’ script can be used to turn on and off the debug logs.By default, the containers are logged at the INFO level.INFO and DEBUG are the only supported levels.

To enable DEBUG level user: **./muster-cli debug-on.**

This would provide more information for troubleshoot generation and help with debug.This option must be enabled while reproducing an issue.

To return to INFO level use: **./muster-cli debug-off.**

<#root>

```
root@firepower:/usr/local/sf/csdac# ./muster-cli debug-on


Recreating muster-bee ...
Recreating muster-bee ... done
Recreating muster-user-analysis     ... done
Recreating muster-local-fmc-adapter ... done
Recreating muster-ui-backend        ... done
```

Logged messages with Debug

When debug mode is enabled all docker container logs would also contain debug messages

Obtain logs in real time using docker commands: **docker logs -f <container_name>**

In the example below, the debug message shows what triggered a **gRPC error**

<#root>

```
2022-12-12 14:33:29,649 [status_storage] DEBUG: Loading status from /app/status/aws.1_status.json...
2022-12-12 14:33:29,650 [status_storage] DEBUG: Loading status from /app/status/gcp.1_status.json...
2022-12-12 14:33:29,651 [status_storage] DEBUG: Loading status from /app/status/github.1_status.json...
2022-12-12 14:33:29,651 [status_storage] DEBUG: Loading status from /app/status/o365.1_status.json...
2022-12-12 14:33:43,279 [server] DEBUG: Got health status request.

2022-12-12 14:33:43,280 [bee_api] WARNING: Got gRPC error from BEE: StatusCode.UNAVAILABLE failed to cor
```

Sample Problem with Troubleshooting Walkthrough

Problem and Troubleshooting Overview

Problem:

Most common problem we encounter is that FMC does not receive all dynamic object mappings.

Troubleshooting:

To troubleshoot the problem, we

- Enable debug mode from "muster-cli"
- Generated Troubleshoot file from FMC UI
- Checked the CSDAC AWS Connector logs in collected the Troubleshoot.
- Found out that CSDAC AWS Connector only queried for first IP in the AWS instances.

Prepare troubleshot bundle

- From FMC CLI we enabled debug mode using ./muster-cli debug-on. muster-cli tool is available in /usr/local/sf/csdac.
- Recreated the problem by waiting for the connector to have status OK and then checking the Dynamic Attribute Filters.
- Collected the troubleshoot logs from FMC UI and extracted them.Checked the AWS Connector logs for contents of snapshot

Look at the tag attributes for an IP

The tag attributes for a given IP is logged in the Troubleshoot logs. For AWS Connector, we looked at muster-connector-aws.1.muster-docker.log.gz

Summary of Checks

Does the Connector and Adapter status look good?

Check the statuses in the corresponding Connector, Adapter pages.

Did the Connectors get all the mappings?

Check the rule preview for matching IP addresses.

Check the Connector docker logs to see if it is querying the mappings correctly.

Did the REST Server receive dynamic tag mappings from connector?

Check the FMC dynamic objects page.

Check the USMS logs (in /opt/CSCOpx/MDC/log/operation/usmsharedsvcs.log) to see if the FMC REST server processed the API request from CSDAC correctly.

Q&A

Q: What version of on-premises CSDAC supports an ISE connector, I also do not see such a connector in Version 7.4.0 (build 1494)?

A: This is in Standalone CSDAC and not in FMC or in CDO. you would need a CSDAC ansible package to test this.

Q: When released, what on-premises CSDAC version would it be?

A: Likely 2.1.0.

Q: A screen with a gear that has API laid over it has been shown. I think it is CSDAC; what does that mean?

A: API explorer is inbuilt in this CSDAC, you can make API calls to CSDAC from that page.