在FMC中部署安全动态属性连接器

目录

简介

本文档介绍FMC中的Cisco安全动态属性连接器。

背景-问题

CSDAC（思科安全动态属性连接器）可集成到FMC（Firepower管理中心）中，提供与独立CSDAC应用和CDO中的CSDAC相同级别的功能。对于独立CSDAC，它可免除客户管理和维护CSDAC独立计算机的开销。作为网络管理员，我希望编程接口能够轻松集成并及时了解外部动态环境提供商的变化。此集成解决了从动态变化的云环境中收集属性而不部署策略的问题。

解决方案（摘要）

现在，可以在FMC中配置CSDAC，以便从Azure、vCenter、AWS、GCP、Office 365和Azure服务标签获取标签属性，从而提供与CDO中的独立CSDAC和CSDAC相同的功能。

- 您现在可以选择使用
  - FMC中的CSDAC（或）
  - CDO中的CSDAC（或）
  - 独立CSDAC
- 目标市场：企业、服务提供商

FMC摘要中的动态属性连接器

FMC动态属性连接器：

- 控制面板屏幕，用于构建和操作动态属性连接器功能。
- 用于配置源工作负载连接器(AWS、Azure、vCenter、Office 365、GCP)的FMC UI
- 用于定义动态属性过滤器以创建动态对象的FMC UI

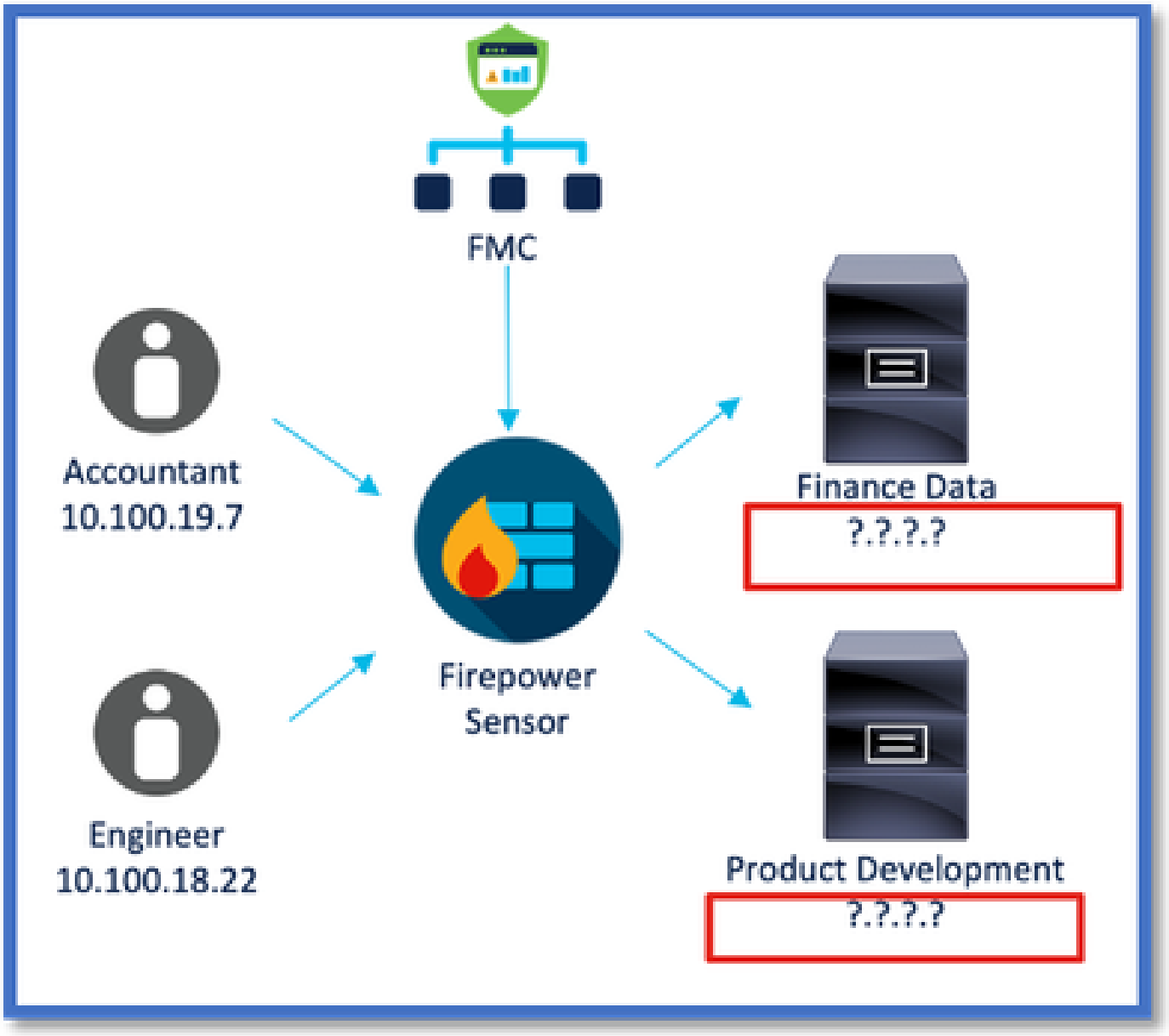
部署示例

内部部署CSDAC

去年，我为CSDAC部署了专用虚拟机，以便从AWS和Azure帐户收集属性。

问题

现在，我的组织已迁移到云，我无法在我的环境中为CSDAC部署和管理专用虚拟机。



选项1：使用FMC内部构建的动态属性连接器

您可以通过使用FMC内部构建的动态属性连接器来解决问题。由它创建的动态对象可用于访问策略中。

选项2：在CDO中使用云交付的动态属性连接器

您可以在CDO中使用动态属性连接器来解决问题。由它创建的动态对象可用于

- CDO云交付的FMC
- CDO内部FMC

必备条件、支持的平台、许可

支持的最低软件和硬件平台

支持的最低管理器版本	受管设备	需要支持的最低受管设备版本	备注
FMC 7.4	支持的任何FTD	任何7.0+ FTD	

* FDM管理的设备不支持动态属性连接器

使用的组件

本文档中的信息基于以下软件和硬件版本：
· 运行7.4的思科防火墙管理中心
· 运行7.4或更高版本的Cisco Firepower威胁防御。
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

功能详细信息

独立CSDAC概述（当前版本- 7.4）

思科安全动态属性连接器使您能够在防火墙管理中心(FMC)访问控制规则中使用来自各种云服务平台的标记。

本地CSDAC可安装在Linux计算机上，支持从以下位置获取属性：

- AWS，Azure，VMware vCenter和NSX-T，Office 365，Azure服务标签，GCP，GitHub。

CDO中的CSDAC概述（当前发布- 7.4）

支持与本地CSDAC相同的功能，无需安装和维护专用应用。

CDO中当前不支持vCenter连接器。

支持将收到的属性发送到CDO中云交付的FMC和内部FMC。

FMC中的CSDAC

支持与独立CSDAC相同的功能，无需安装和维护专用应用。

FMC中的CSDAC支持从以下位置获取属性：

- AWS，Azure，VMware vCenter和NSX-T，Office 365，Azure服务标签，GCP，GitHub

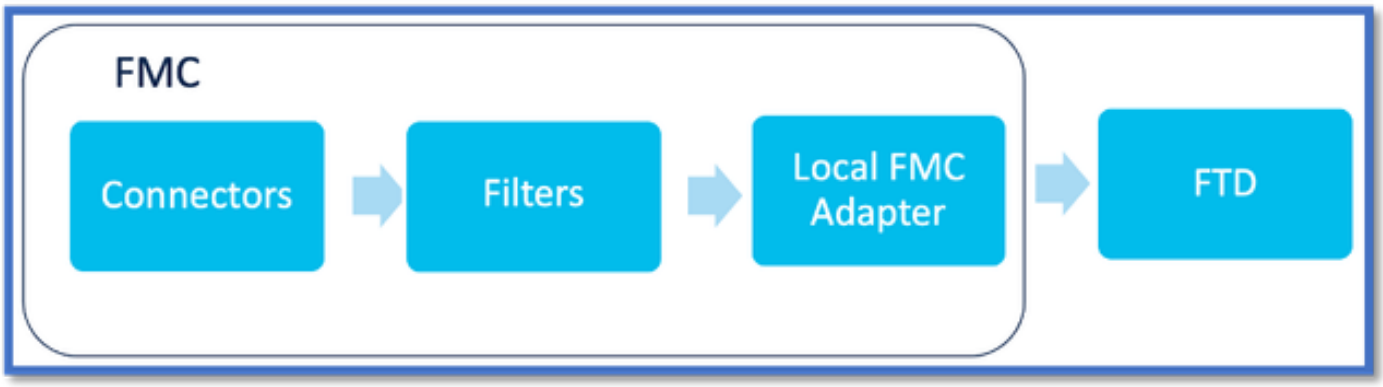
此处没有显式适配器配置，因为它是FMC的本地配置。

工作原理

连接器用于从AWS、Azure、o365、vCenter获取属性。

然后使用本地适配器将这些简化属性及其IP映射保存在FMC中作为动态对象。

FMC将映射实时发送到FTD（无需部署）。



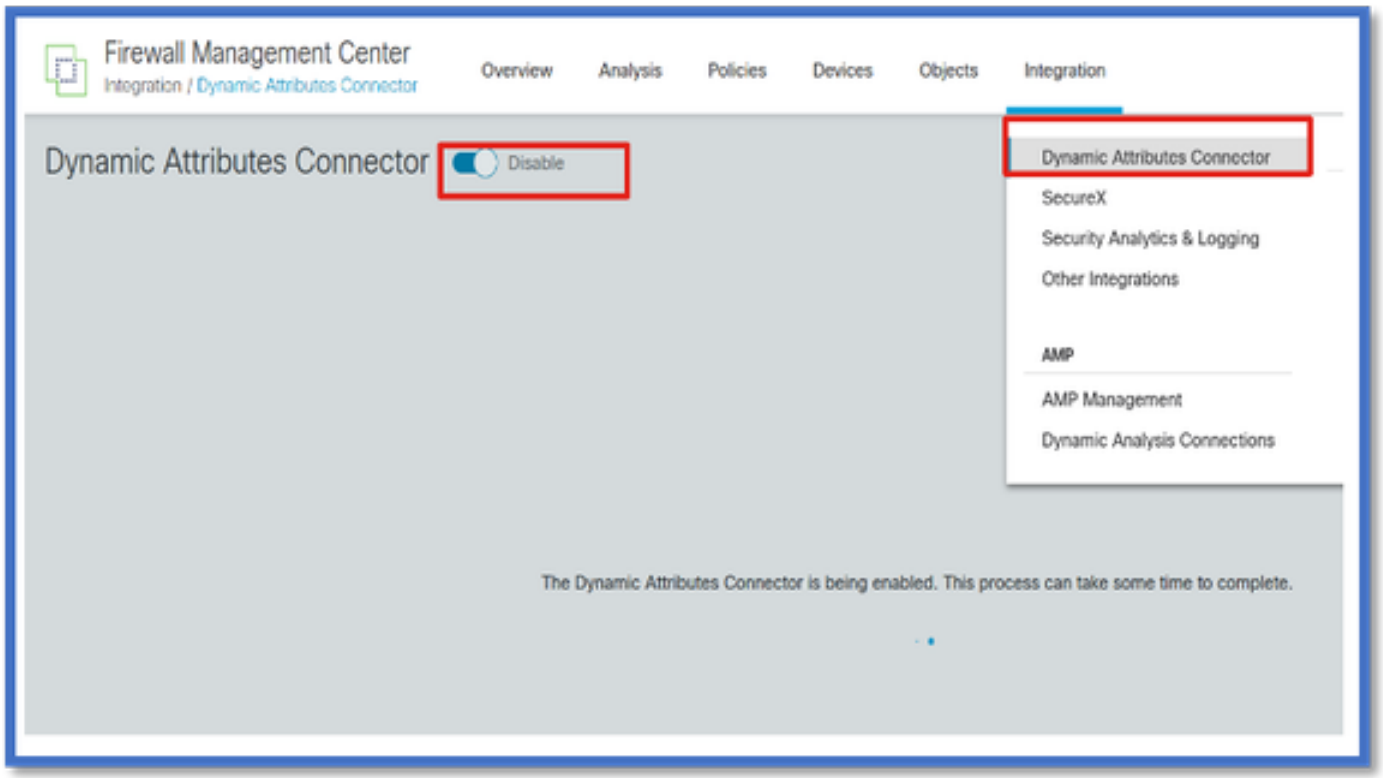
在FMC中启用CSDAC

导航到Integration > Dynamic Attributes Connector。

使用“切换”按钮启用连接器。

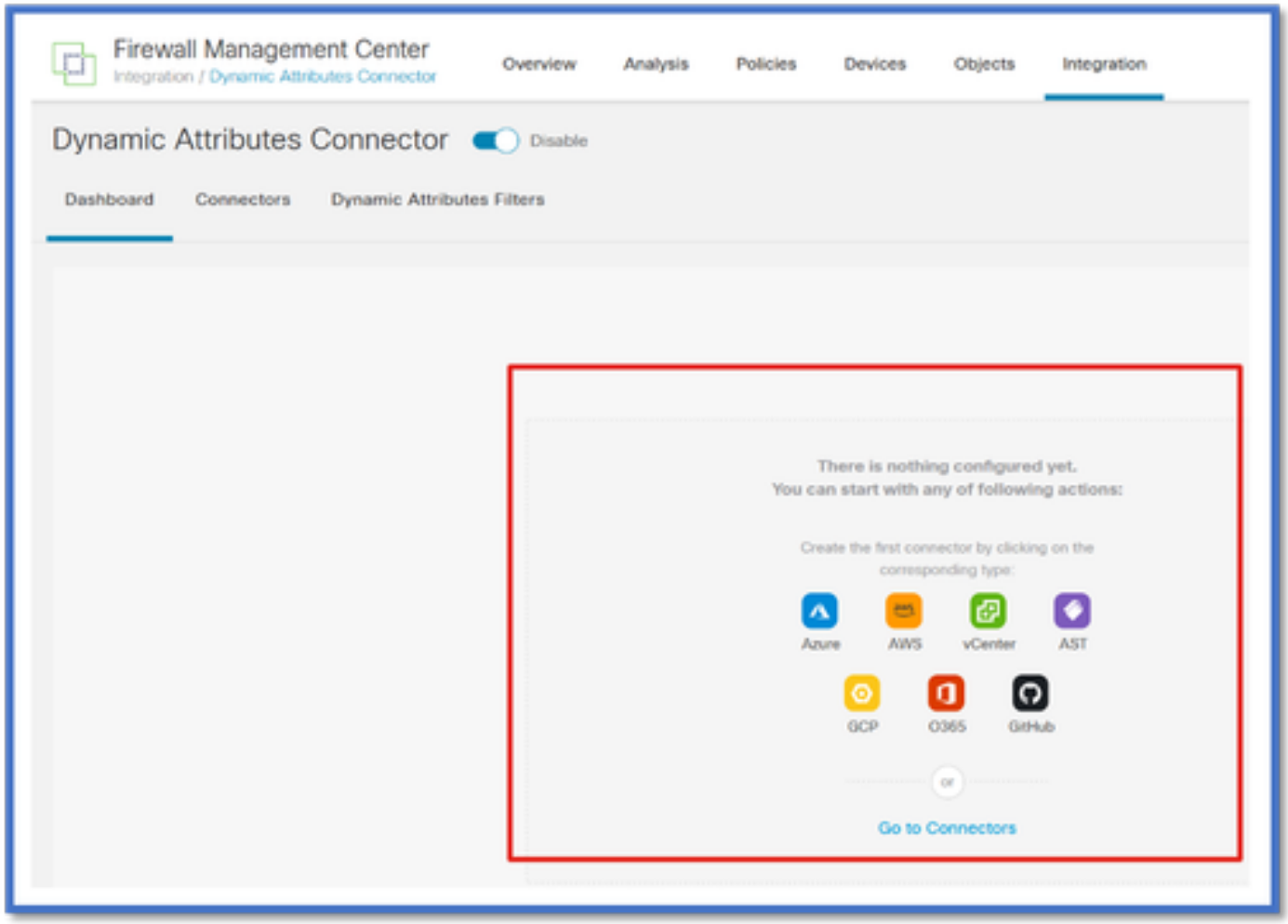
FMC需要几分钟时间来下载和启动docker映像和容器。

这只能在FMC全局域中配置。



CSDAC控制面板

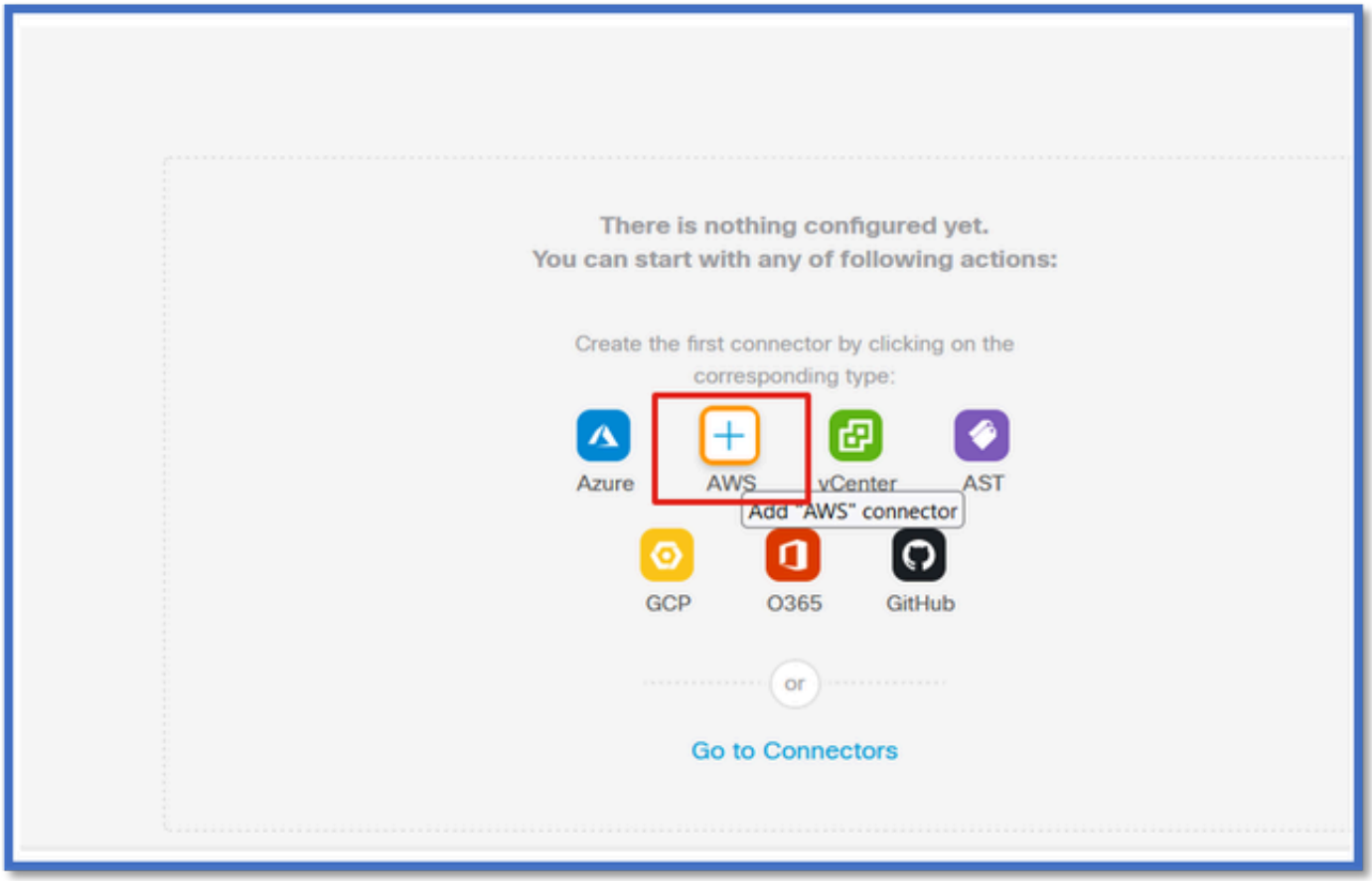
启用CSDAC后，用户会看到CSDAC控制面板页面。控制面板用于配置和查看统一连接器和过滤器。



配置连接器

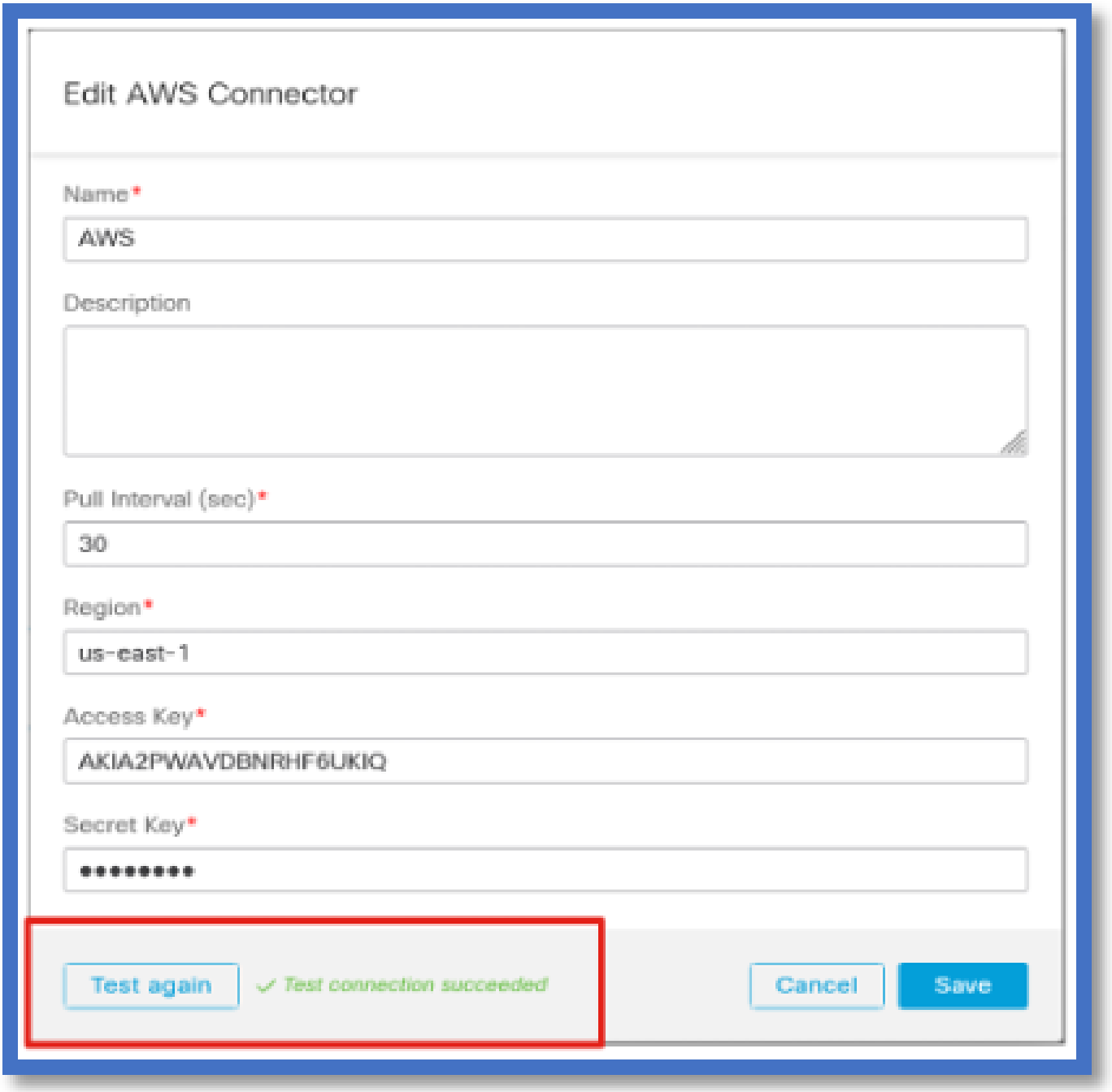
从仪表板添加连接器

在控制面板上，点击所需连接器的图标进行添加。



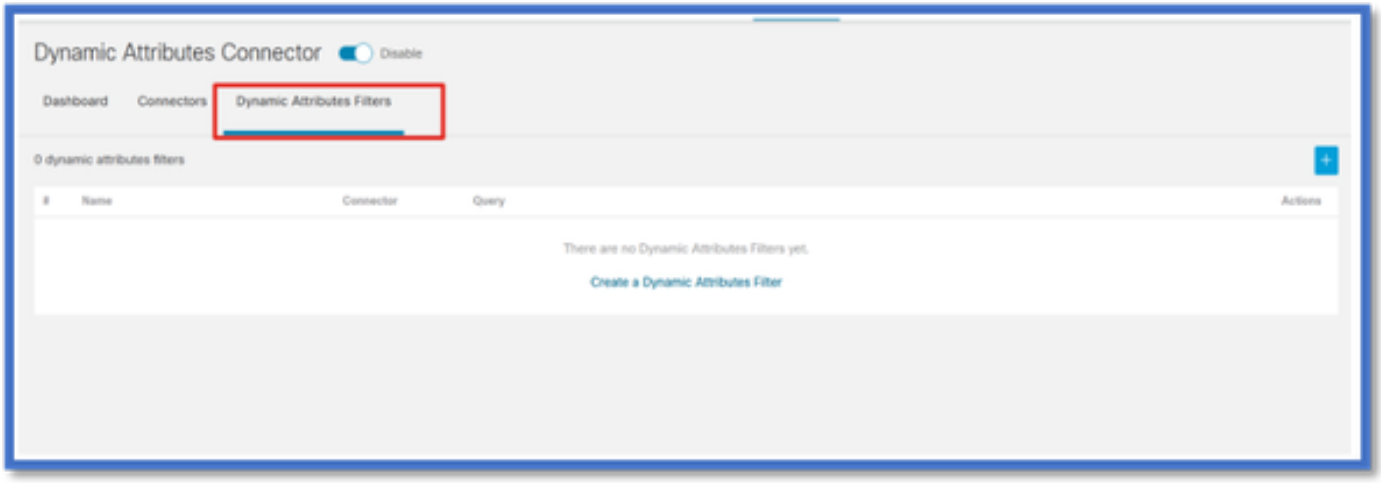
配置时间间隔（在Pull Interval字段中），以便连接器可以按照配置的周期从提供程序中提取信息。

输入提供程序凭据以获取标记属性。配置连接器后，可以点击Test Button测试连接器。



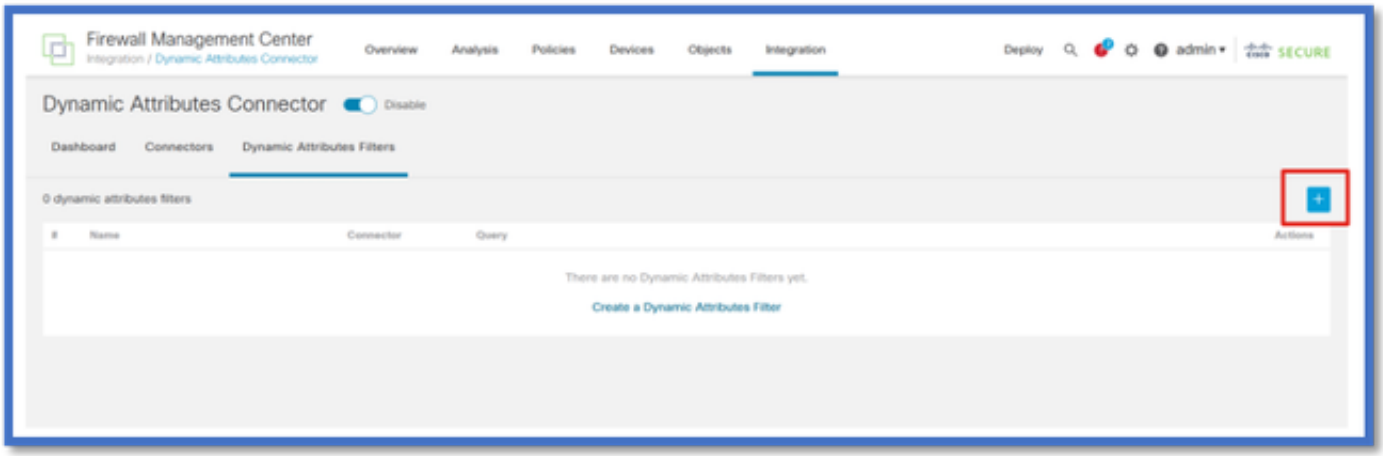
配置过滤器

单击“动态属性连接器”(Dynamic Attributes Connector)菜单中的“动态属性过滤器”(Dynamic Attribute Filters)选项卡，转到“动态属性过滤器”(Dynamic Attributes Filters)页面。



添加过滤器

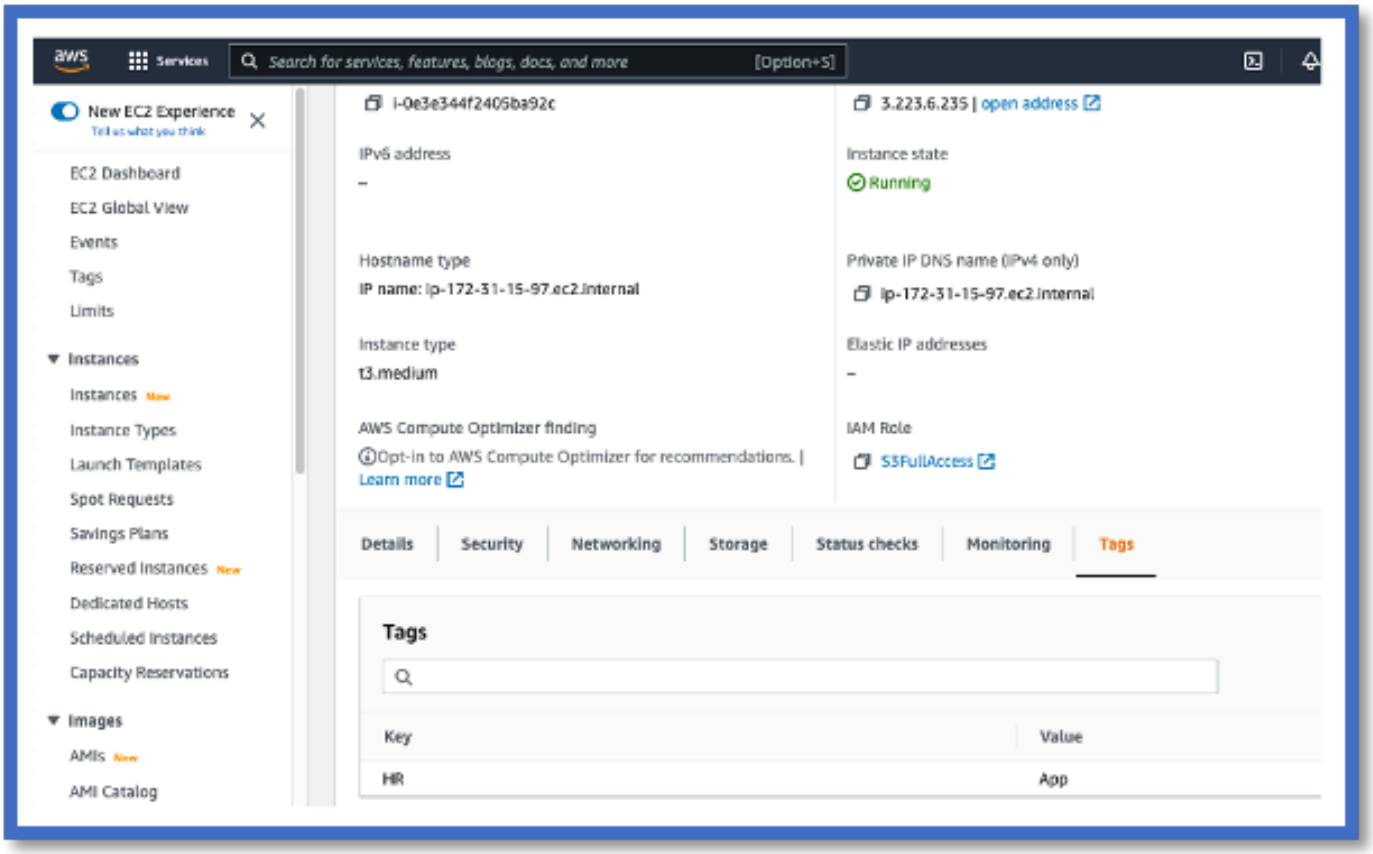
点击+按钮，为属性连接器创建过滤器。



添加AWS标记

例如，我们可以假设您对AWS工作负载中的关键“HR”和价值“App”感兴趣。

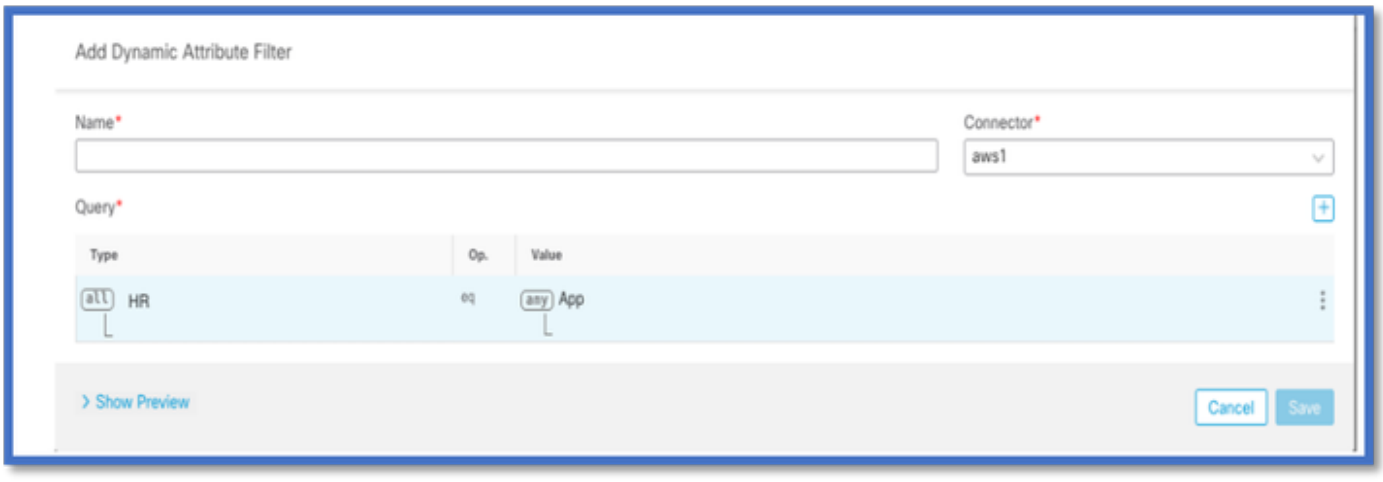
这是AWS中的情况。



FMC中的CSDAC

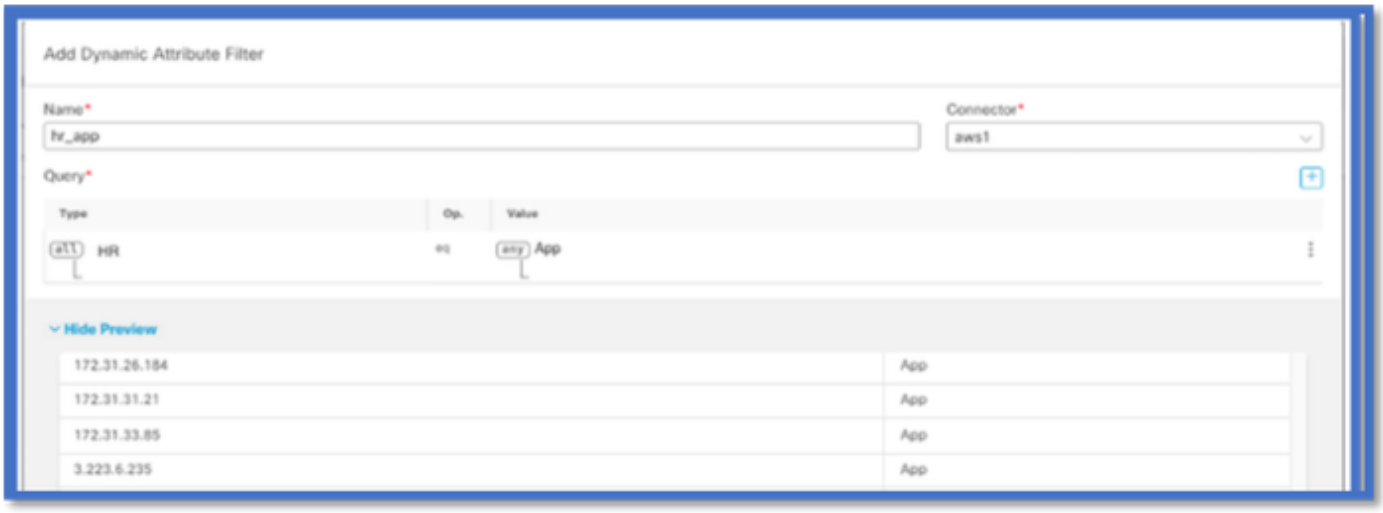
您可以通过点击+按钮创建“HR等于App”规则。

本地FMC适配器会将匹配的IP地址作为动态对象映射发送到FMC



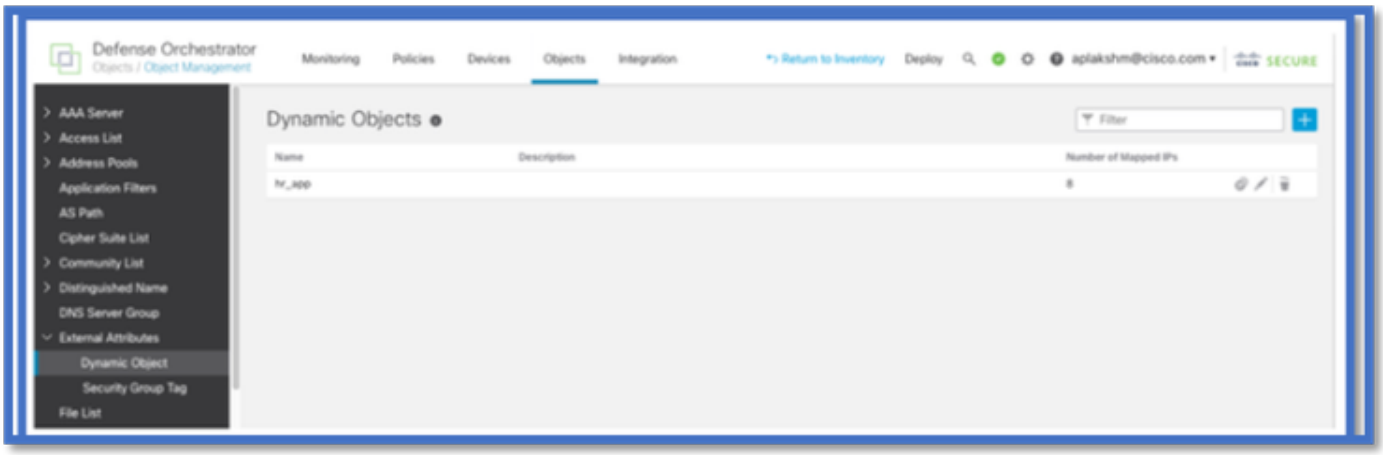
预览

您还可以通过点击“显示”(Show)查看特定属性规则的匹配IP地址 | 隐藏预览”按钮。



动态对象

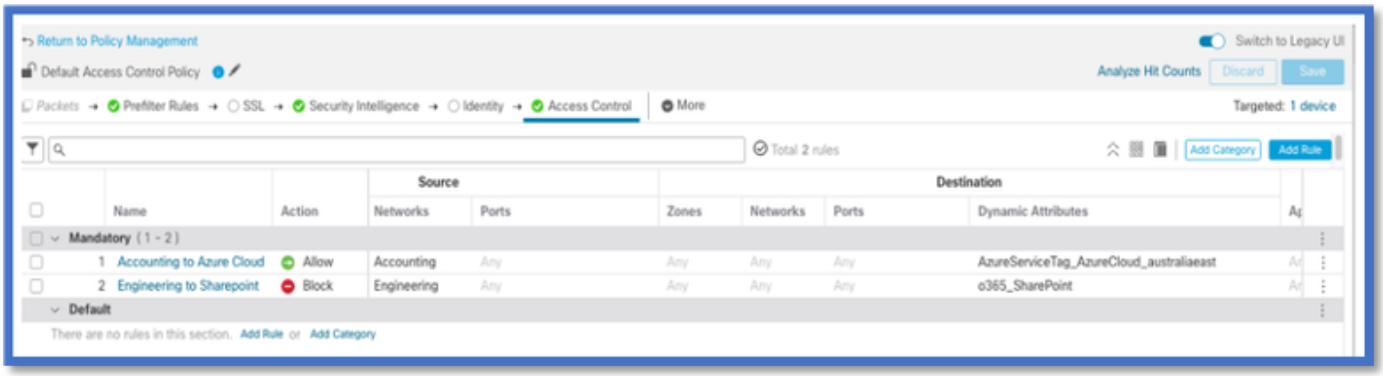
在“对象”>“外部属性”中查看CSDAC创建的动态对象，在FMC中查看动态对象



AC策略

配置：访问策略

在FMC中，添加访问策略以允许或阻止从动态属性连接器接收的动态对象。



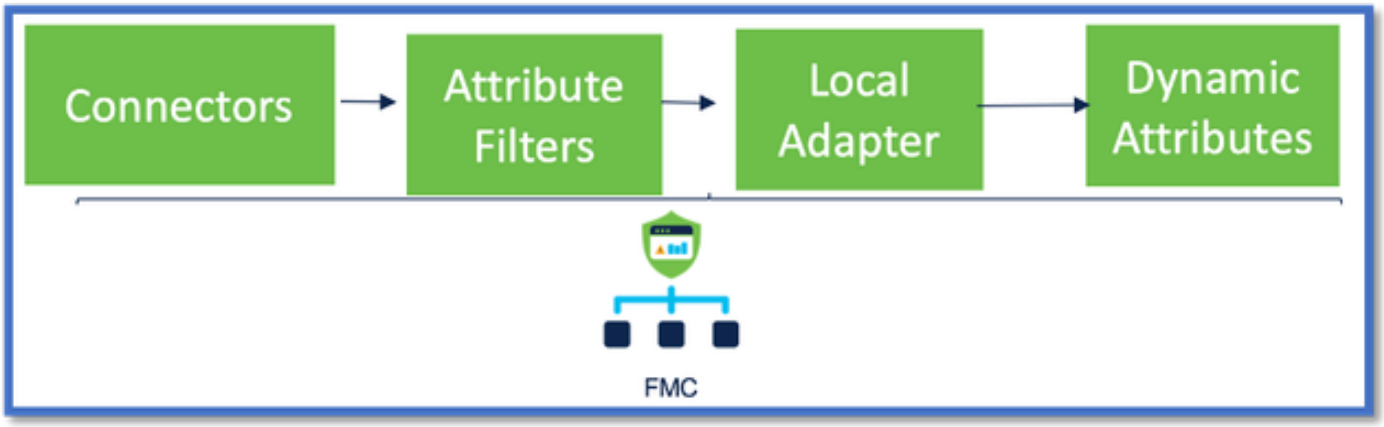
平台限制

- 连接器限制基于可用的FMC内存。
- vFMC需要额外的1GB内存来支持5个连接器
- Azure AD领域也包含在限制中，因为它也是CSDAC容器。

型号	支持的连接器数	平台	基于内存的限制
基本	仅Azure AD	1600	32GB
小型	5	vFMC	> 32 GB
中	10	vFMC 300、2600	>= 64 GB
大型	20	4600	>= 128 GB

故障排除/诊断

故障排除最好通过从CSDAC连接器跟踪动态对象到FMC中的动态属性来执行。许多内部日志将此功能称为“集”。您可以沿广播链窥探系统状态以隔离问题。CSDAC使用Docker容器。 日志和其他文件的消息和名称必须称为“docker”



检查连接器

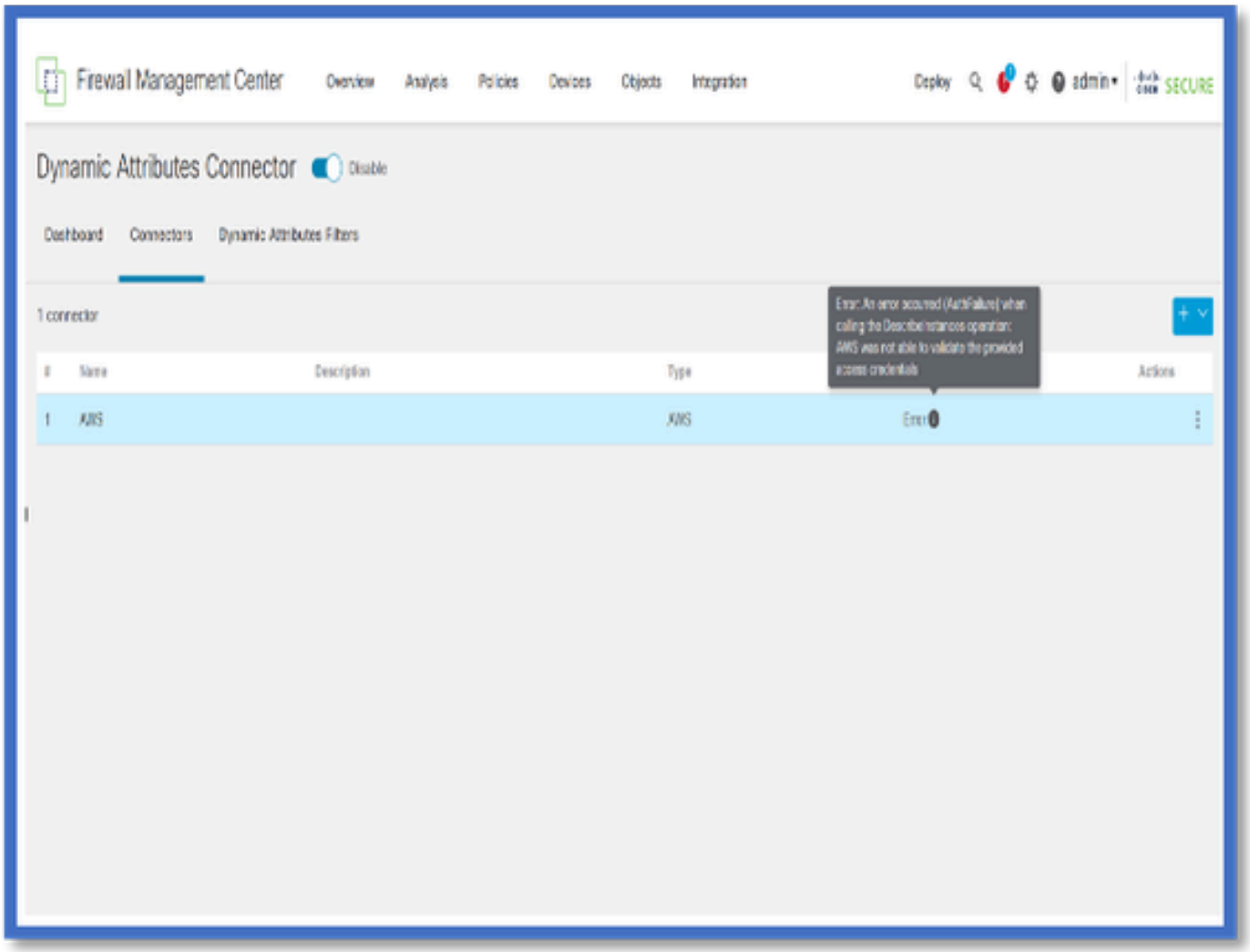
首先确保连接器可以连接到vCenter、AWS或Azure服务器。

如果连接器配置不正确，则下游进程无法获得标记信息。

从“连接器”选项卡查看连接器

连接器状态显示在状态字段中，每15秒更新一次。

在此，我们看到连接器无法使用提供的凭证进行身份验证。



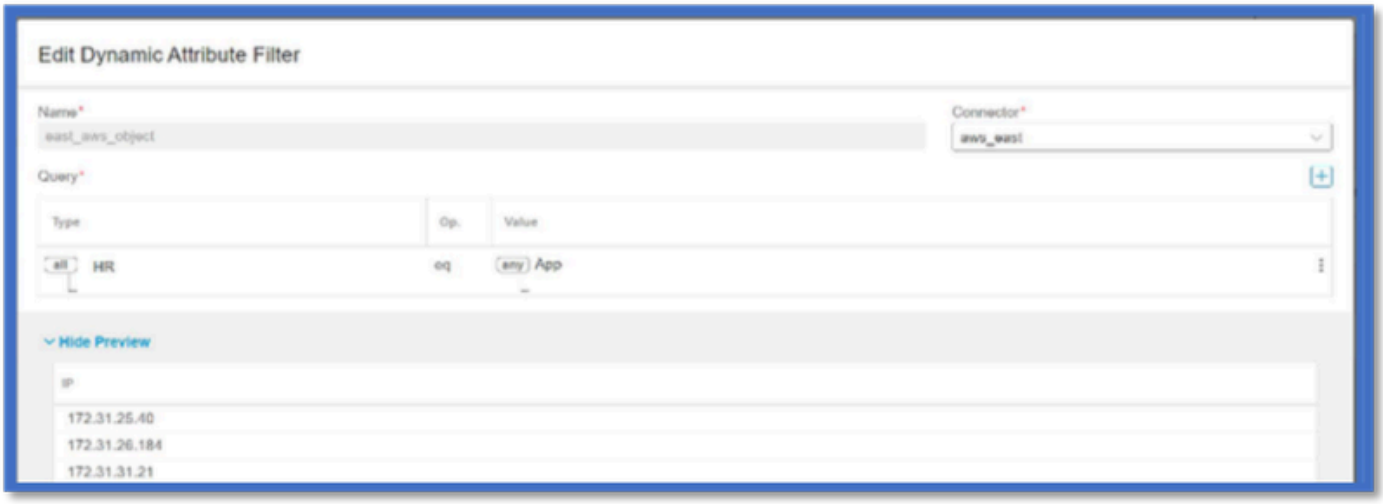
检查属性过滤器

确保规则预览显示查询条件的匹配IP地址。

如果没有匹配的IP地址，则FMC无法获取动态对象映射。

检查属性过滤器

检查动态属性IP映射在预览中是否可用。“显示预览”按钮在动态属性过滤器编辑弹出窗口中可用。



检查FMC UI中的动态对象

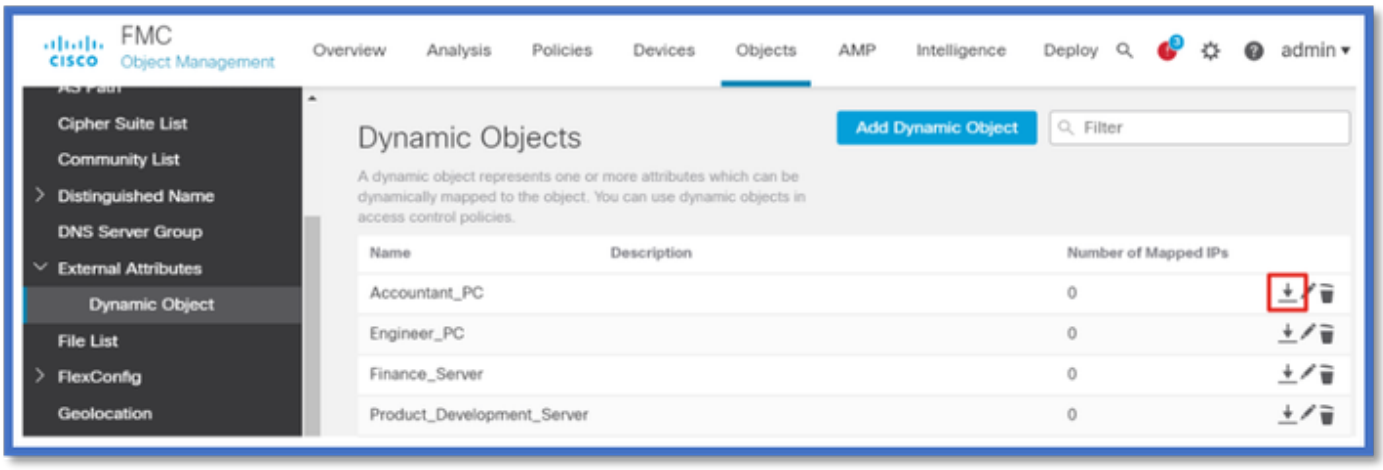
首先，确保FMC服务器包含您期望的绑定。

- 在“对象管理”、“外部对象”选项卡下，选中“动态对象”进行绑定。
- 如果FMC未获取绑定，则FTD无法获取绑定。

检查FMC运行状况监视器和CSDAC运行状况警报通知。

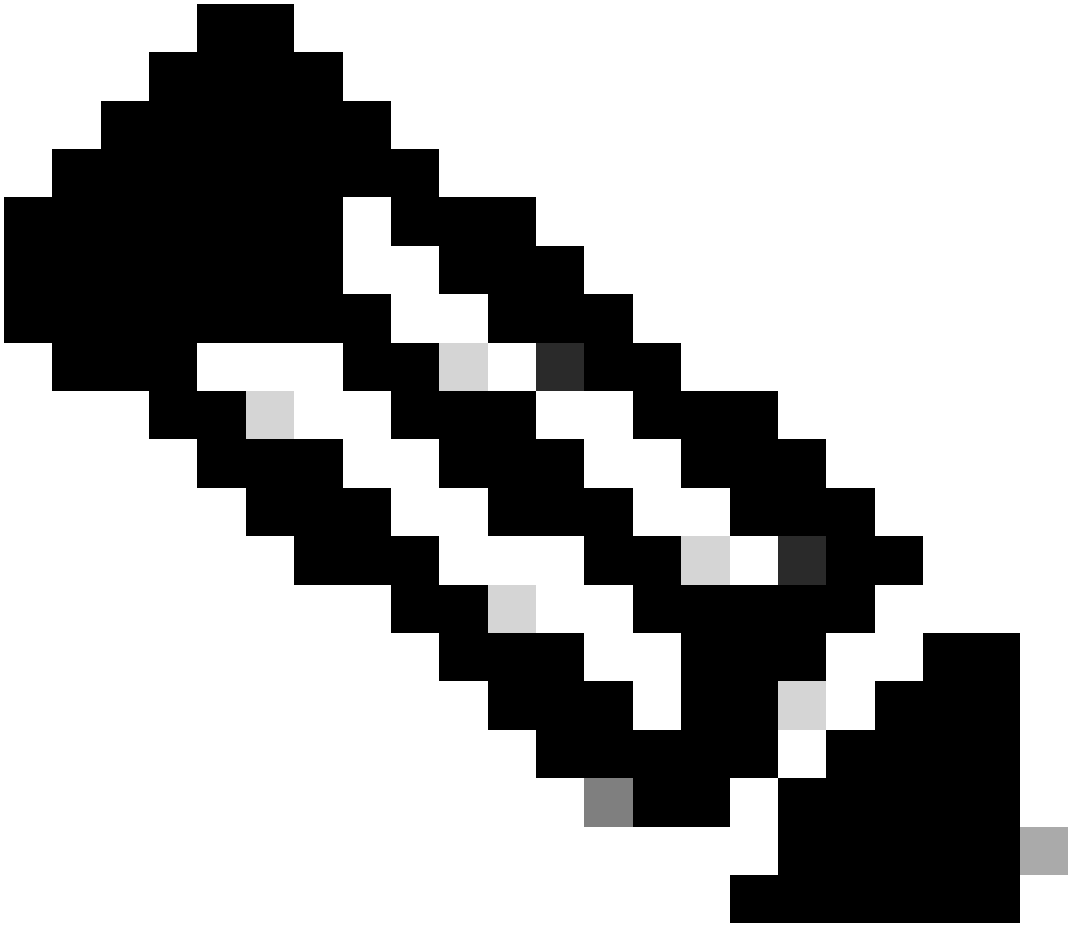
检查动态对象

FMC对象管理器允许您下载当前动态对象IP地址。

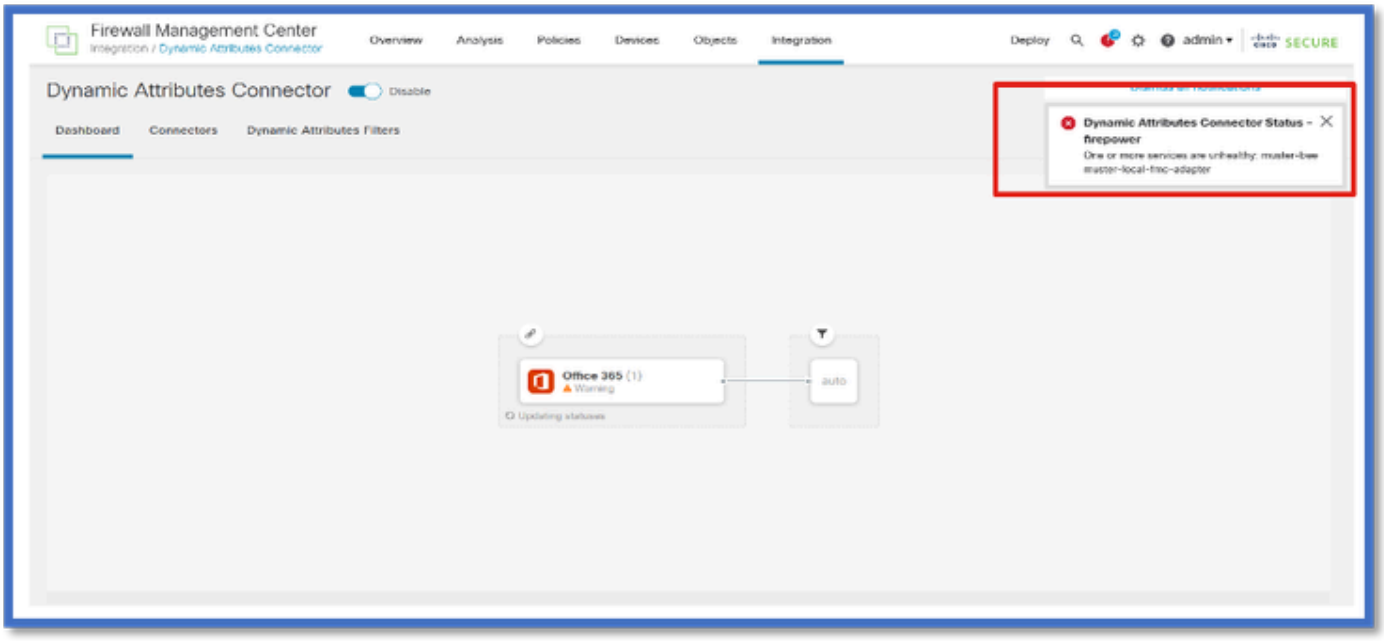


CSDAC运行状况警报

如果任何核心服务（包括动态属性连接器）发生故障，FMC的任务管理器会显示运行状况警报。警报包含有关服务名称和状态的信息。

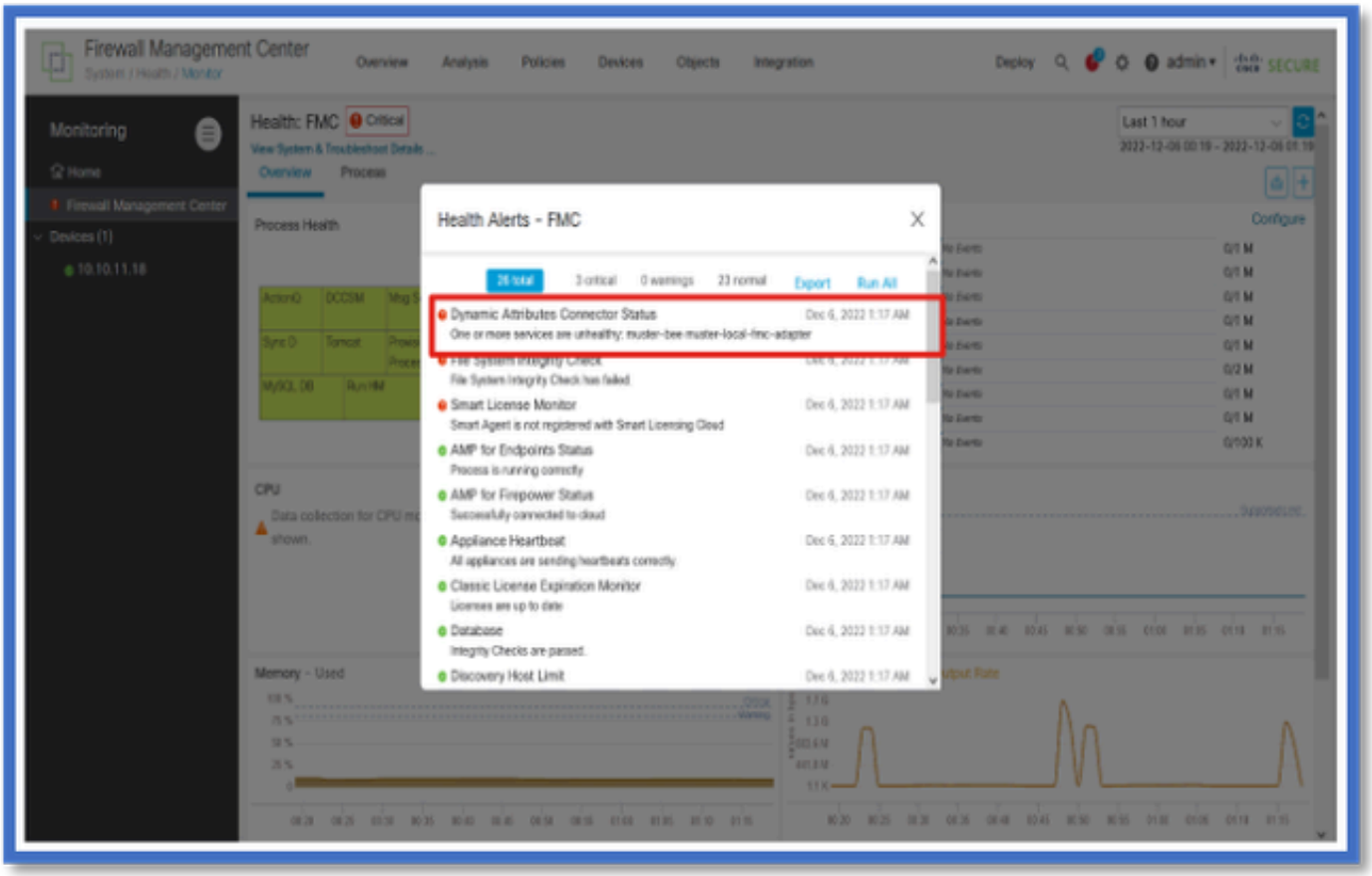


注意：我们在多个通知中仍有“汇总”命名，此处需要提供服务名称以获取详细信息。



此处我们看到muster-bee和muster-local-fmc-adapter“不正常”。

如果错误指示任何核心服务，则需要收集故障排除日志以进行调试。



CSDAC进行故障排除

生成CSDAC故障排除

- CSDAC日志在FMC故障排除生成期间自动收集。捆绑包包含Docker状态、日志和离线调试问题所需的数据。
- 比较好的做法是在重现错误之前启用CSDAC调试模式，针对此错误收集了故障排除日志。

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

在以下文件夹中查找CSDAC日志“Troubleshoot”（非跟踪故障排除）：

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

它包含etcd数据库中存储的数据。

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

这包含docker容器中的日志。

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

这将显示容器状态、版本和docker映像详细信息。

CLI故障排除

muster-cli脚本可用于从FMC CLI检查CSDAC的状态。

如果任何服务的状态为“已退出”或不同于“启动”，则首先检查该容器的日志。

获取日志需要容器名称；可以从输出中获取。

```
'root@firepower:/Volume/home/admin# cd /usr/local/sf/csdac/
root@firepower:/usr/local/sf/csdac# ./muster-cli status
============================================ CORE SERVICES ============================================
          Name                          Command              State                  Ports
-------------------------------------------------------------------------------------------------------
muster-bee                 ./docker-entrypoint.sh run ...   Up      127.0.0.1:15050->50050/tcp, 50443/tcp
muster-envoy               /docker-entrypoint.sh runs ...   Up      127.0.0.1:6443->8443/tcp
muster-local-fmc-adapter   ./docker-entrypoint.sh run ...   Up
muster-ui-backend          ./docker-entrypoint.sh run ...   Up      50031/tcp
========================== CONNECTORS AND ADAPTERS ==========================
                          Name                                    Command               State     Ports
-------------------------------------------------------------------------------------------------------------
muster-connector-aws.2.muster                          ./docker-entrypoint.sh run ...   Up      50070/tcp
muster-connector-o365.1.muster                         ./docker-entrypoint.sh run ...   Up      50070/tcp
```

CSDAC调试模式

“muster-cli”脚本可用于打开和关闭调试日志。默认情况下，容器记录在INFO level.INFO中，DEBUG是唯一受支持的级别。

要启用调试级别用户，请执行以下操作：./muster-cli debug-on。

这将为生成故障排除提供更多信息并帮助debug。再现问题时必须启用此选项。

要返回INFO（信息）级别，使用：./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
```

带调试的已记录消息

启用调试模式后，所有docker容器日志也将包含调试消息

使用docker命令实时获取日志：docker logs -f <container_name>

在下面的示例中，调试消息显示触发gRPC错误的内容

<#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
```

故障排除演练中的问题示例

问题和故障排除概述

问题：

我们遇到的最常见问题是FMC无法接收所有动态对象映射。

故障排除：

要排除故障，我们需要

- 从“muster-cli”启用调试模式
- 从FMC UI生成的故障排除文件
- 已检查收集的“故障排除”中的CSDAC AWS连接器日志。
- 发现CSDAC AWS Connector仅查询AWS实例中的第一个IP。

准备故障排除捆绑包

- 在FMC CLI中，我们使用。/muster-cli debug-on启用调试模式。muster-cli工具在/usr/local/sf/csdac中可用。
- 已重新创建问题，方法是等待连接器的状态变为OK，然后检查动态属性过滤器。
- 从FMC UI收集并提取了故障排除日志。已检查AWS Connector日志以获取快照内容

查看IP的标记属性

给定IP的标记属性记录在故障排除日志中。对于AWS Connector，我们查看了muster-connector-aws.1.muster-docker.log.gz

检查摘要

连接器和适配器状态是否正常？

检查相应“连接器”、“适配器”页中的状态。

连接器是否获得了所有映射？

检查规则预览是否匹配IP地址。

检查连接器docker日志，查看其是否正确查询映射。

REST服务器是否从连接器收到动态标记映射？

检查FMC动态对象页面。

检查USMS日志(在/opt/CSCOpx/MDC/log/operation/usmsharedsvcs.log中)以查看FMC REST服务器是否正确处理来自CSDAC的API请求。

问题解答

问：哪种版本的本地CSDAC支持ISE连接器？在版本7.4.0（内部版本1494）中我也看不到此类连接器。

答：这位于独立CSDAC中，而不是FMC或CDO中。您需要一个CSDAC可解析软件包来测试此功能。

问：发布时，本地CSDAC版本是什么？

答：可能是2.1.0。

问：显示了一个屏幕，上面有放置了API的齿轮。我认为是CSDAC，这是什么意思？

答：此CSDAC中内置了API资源管理器，您可以从该页面对CSDAC进行API调用。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。