在FMC中部署安全動態屬性聯結器

目錄

簡介

本文檔介紹有關FMC中的Cisco Secure Dynamic Attribute Connector。

背景-問題

CSDAC（思科安全動態屬性聯結器）可整合到FMC（Firepower管理中心）中，提供與獨立CSDAC應用和CDO中的CSDAC相同級別的功能。對於獨立CSDAC，它減輕了客戶管理和維護CSDAC獨立機器的開銷。身為網路管理員，我希望程式介面能夠輕鬆整合，並隨時瞭解外部動態環境提供者的變更。此整合可解決從動態變化的雲環境中收集屬性而不部署策略的問題。

解決方案（摘要）

現在，可以在FMC中配置CSDAC以從Azure、vCenter、AWS、GCP、Office 365和Azure服務標籤獲取標籤屬性，從而提供與CDO中的獨立CSDAC和CSDAC的功能同位。

- 您現在可以選擇使用
  - FMC中的CSDAC（或）
  - CDO中的CSDAC （或）
  - 獨立CSDAC
- 目標市場：企業、服務提供商

FMC摘要中的動態屬性聯結器

FMC動態屬性聯結器：

- 儀表板畫面可建立並操作動態屬性聯結器功能。
- 用於配置源工作負載聯結器(AWS、Azure、vCenter、Office 365、GCP)的FMC UI
- FMC UI：定義動態屬性篩選器以建立動態物件

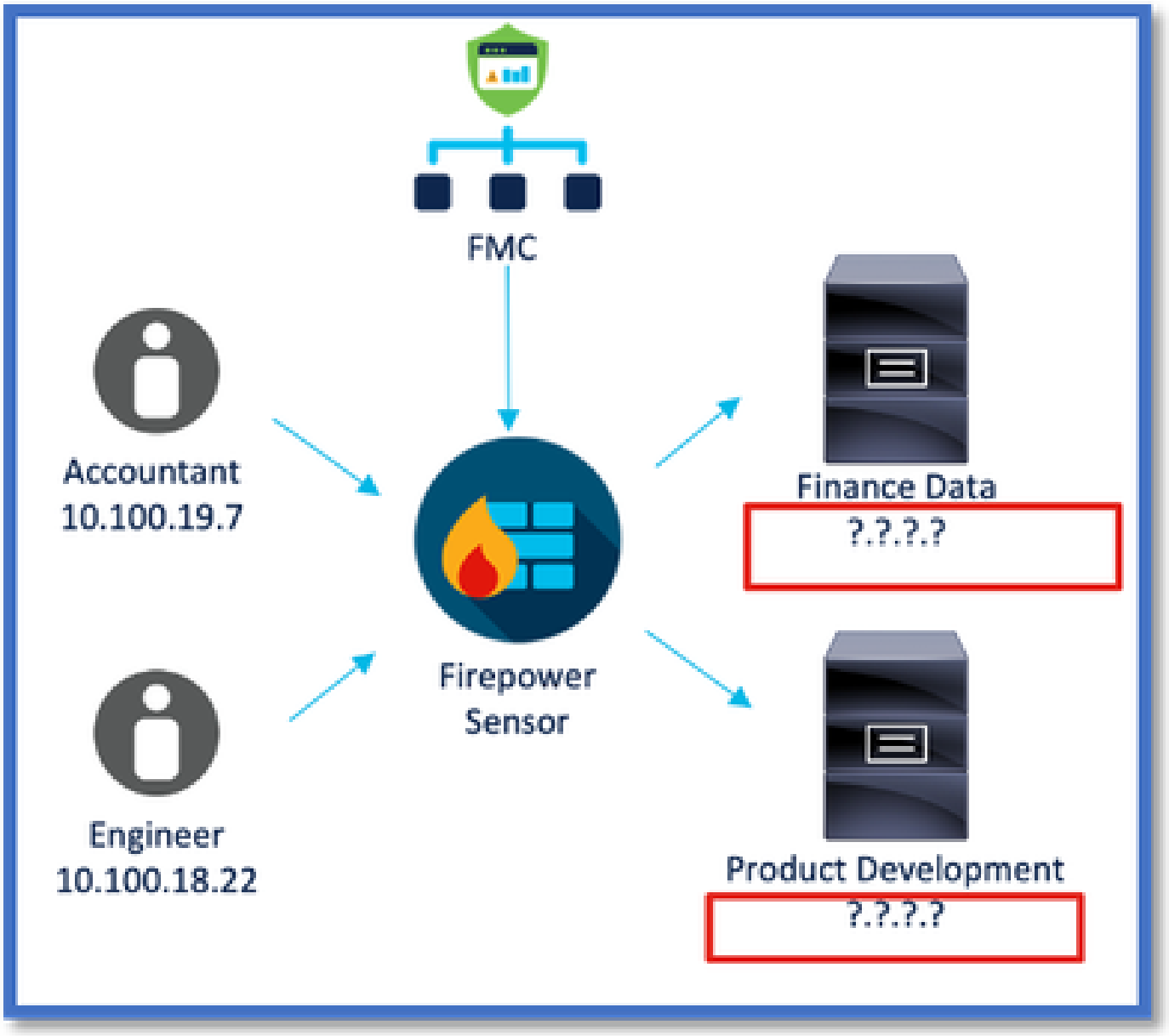
部署範例

內建CSDAC

去年，我為CSDAC部署了專用虛擬機器，以便從AWS和Azure帳戶收集屬性。

問題

現在，我的組織已遷移至雲，我不能在我的環境中為CSDAC部署和管理專用虛擬機器。



選項1：使用FMC內建的動態屬性聯結器

您可以使用FMC內建的動態屬性聯結器來修正此問題。由它建立的動態對象可用於訪問策略中。

選項2：在CDO中使用雲交付的動態屬性聯結器

您可以在CDO中使用「動態屬性聯結器」來修正問題。由它建立的動態物件可用於

- CDO雲交付的FMC
- CDO內部部署FMC

必要條件、支援的平台、授權

最低支援的軟體和硬體平台

支援的管理員最低版本	受管裝置	需要支援的最低受管裝置版本	備註
FMC 7.4	支援的任何FTD	任何7.0+ FTD	

* FDM管理的裝置不支援動態屬性聯結器

採用元件

本文中的資訊係根據以下軟體和硬體版本：
· 運行7.4的思科防火牆管理中心
· 運行7.4或更高版本的Cisco Firepower威脅防禦。
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

功能詳細資料

獨立CSDAC概述（當前版本- 7.4）

思科安全動態屬性聯結器使您能夠在防火牆管理中心(FMC)訪問控制規則中使用來自各種雲服務平台的標籤。

內建CSDAC可在Linux機器上安裝，支援從下列專案取得屬性：

- AWS、Azure、VMware vCenter和NSX-T、Office 365、Azure服務標籤、GCP、GitHub。

CDO中的CSDAC概述（當前版本- 7.4）

支援與本地CSDAC相同的功能，無需安裝和維護專用應用程式。

CDO目前不支援vCenter聯結器。

支援將收到的屬性傳送到CDO中雲交付的FMC和內部FMC。

FMC中的CSDAC

支援與獨立CSDAC相同的功能，無需安裝和維護專用應用程式。

FMC中的CSDAC支援從下列專案取得屬性：

- AWS、Azure、VMware vCenter和NSX-T、Office 365、Azure服務標籤、GCP、GitHub

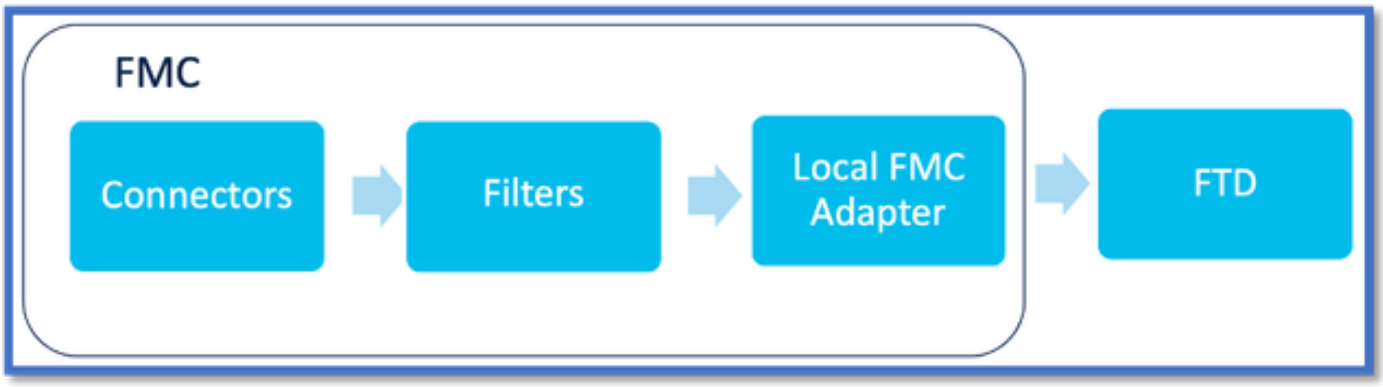
此處沒有明確的介面卡組態，因為它是FMC的本機。

運作方式

聯結器用於從AWS、Azure、o365、vCenter獲取屬性。

然後使用本機介面卡將這些簡化屬性及其IP對映儲存到FMC中，作為動態物件。

FMC會即時將對應傳送到FTD（不含部署）。



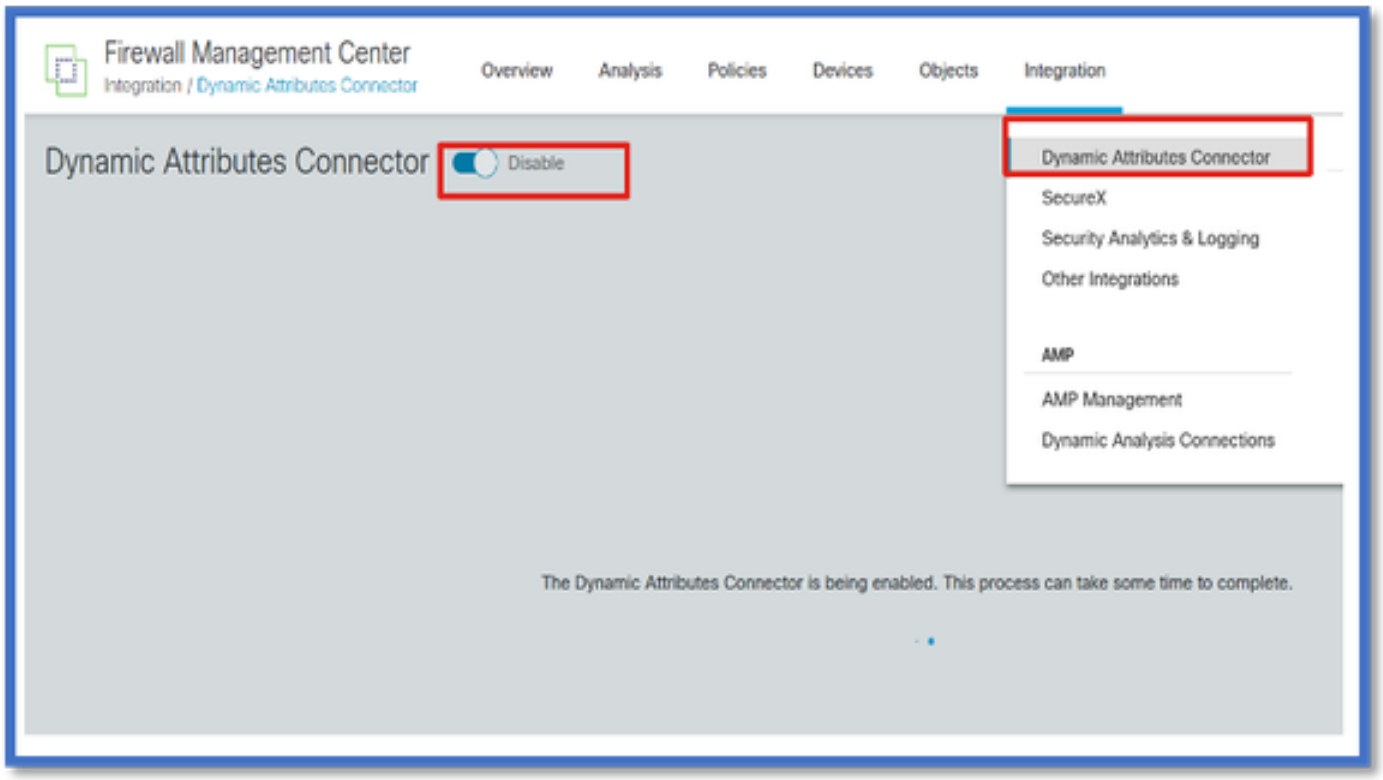
在FMC中啟用CSDAC

導航到「整合」>「動態屬性聯結器」。

使用「切換」按鈕來啟用聯結器。

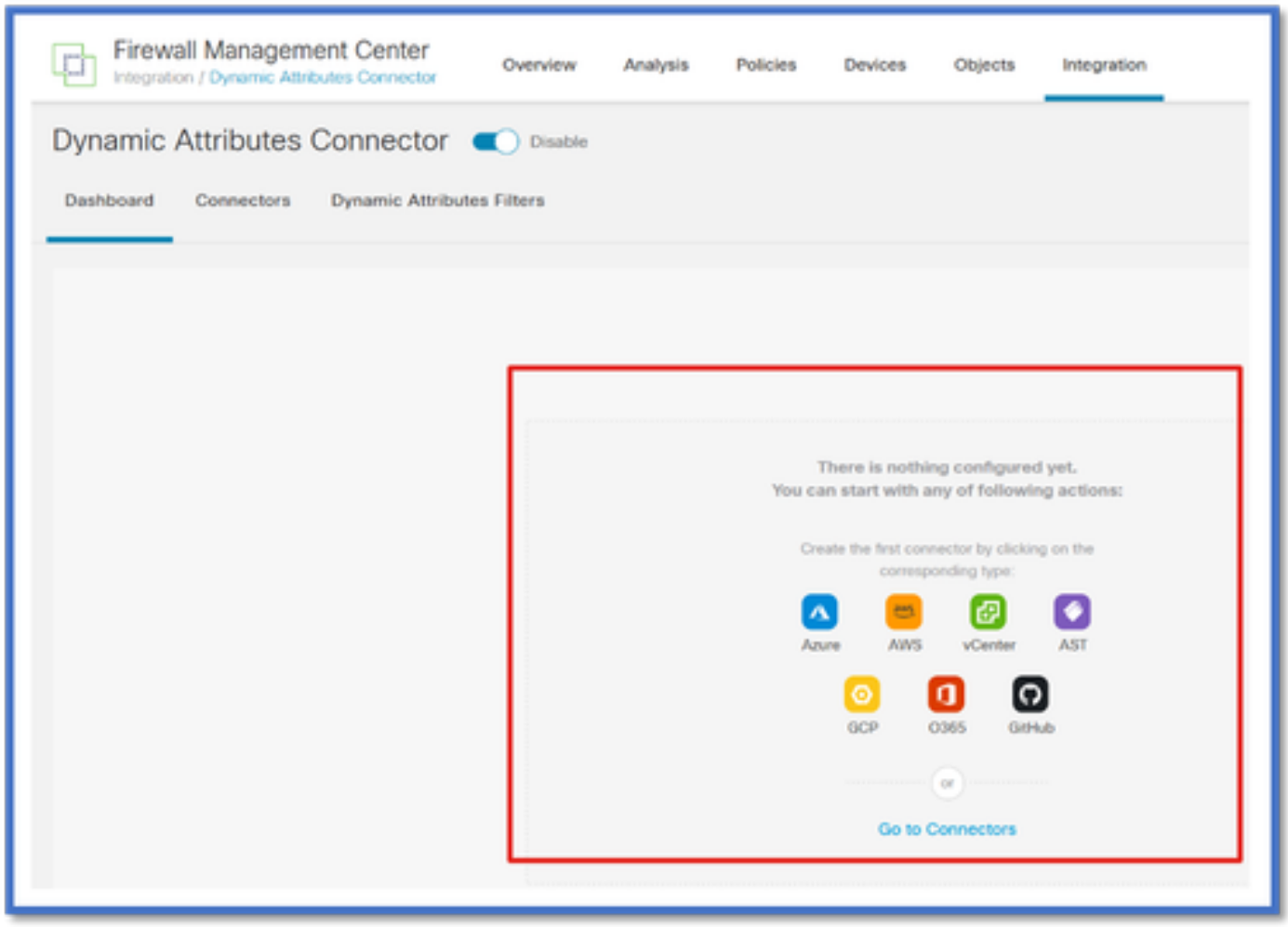
FMC需要幾分鐘的時間來下載並顯示docker映像和容器。

這只能在FMC全局域中進行配置。



CSDAC儀表板

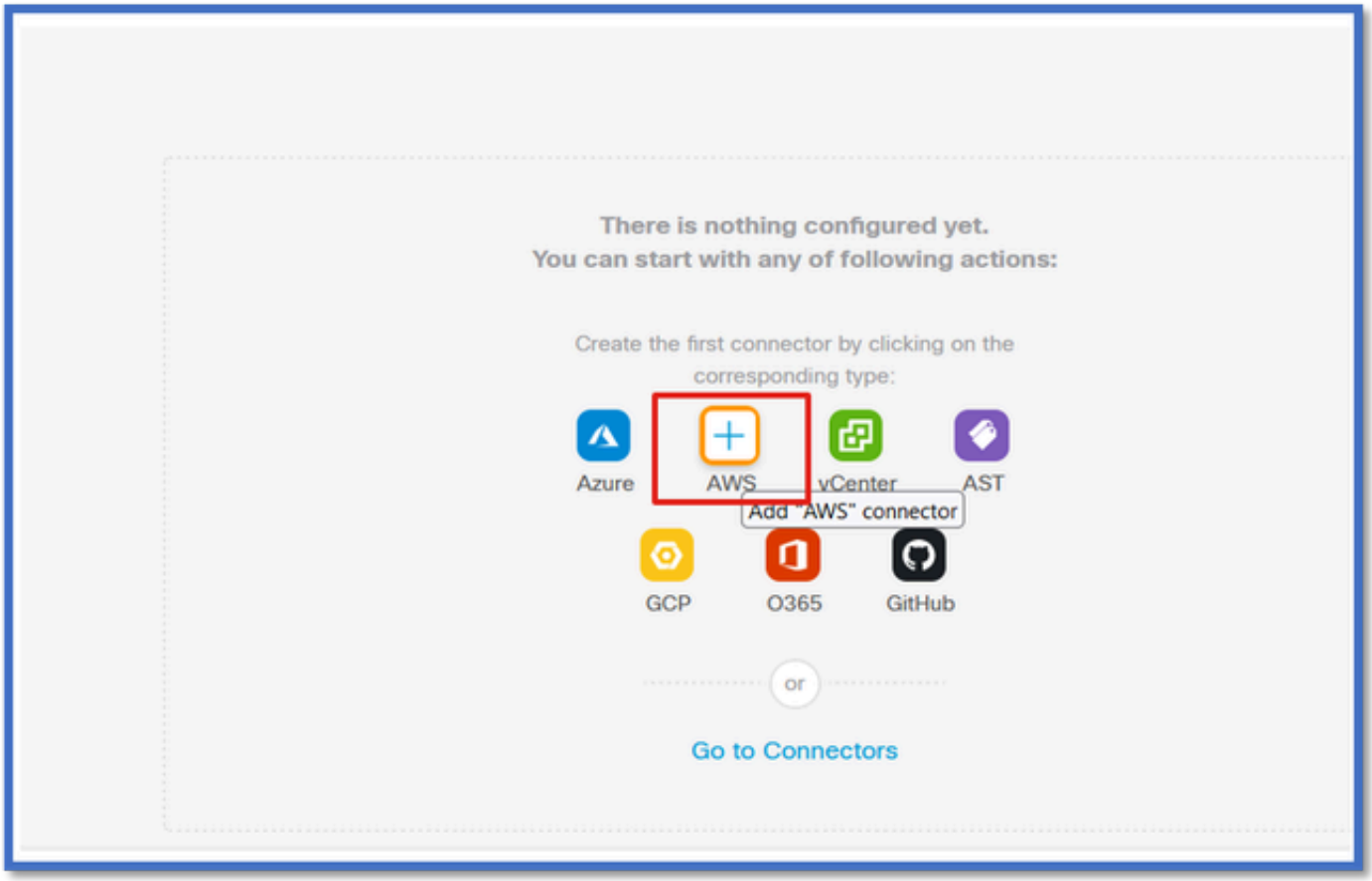
啟用CSDAC後，使用者會看到CSDAC控制台頁面。控制台用於配置和檢視統一聯結器和過濾器。



設定聯結器

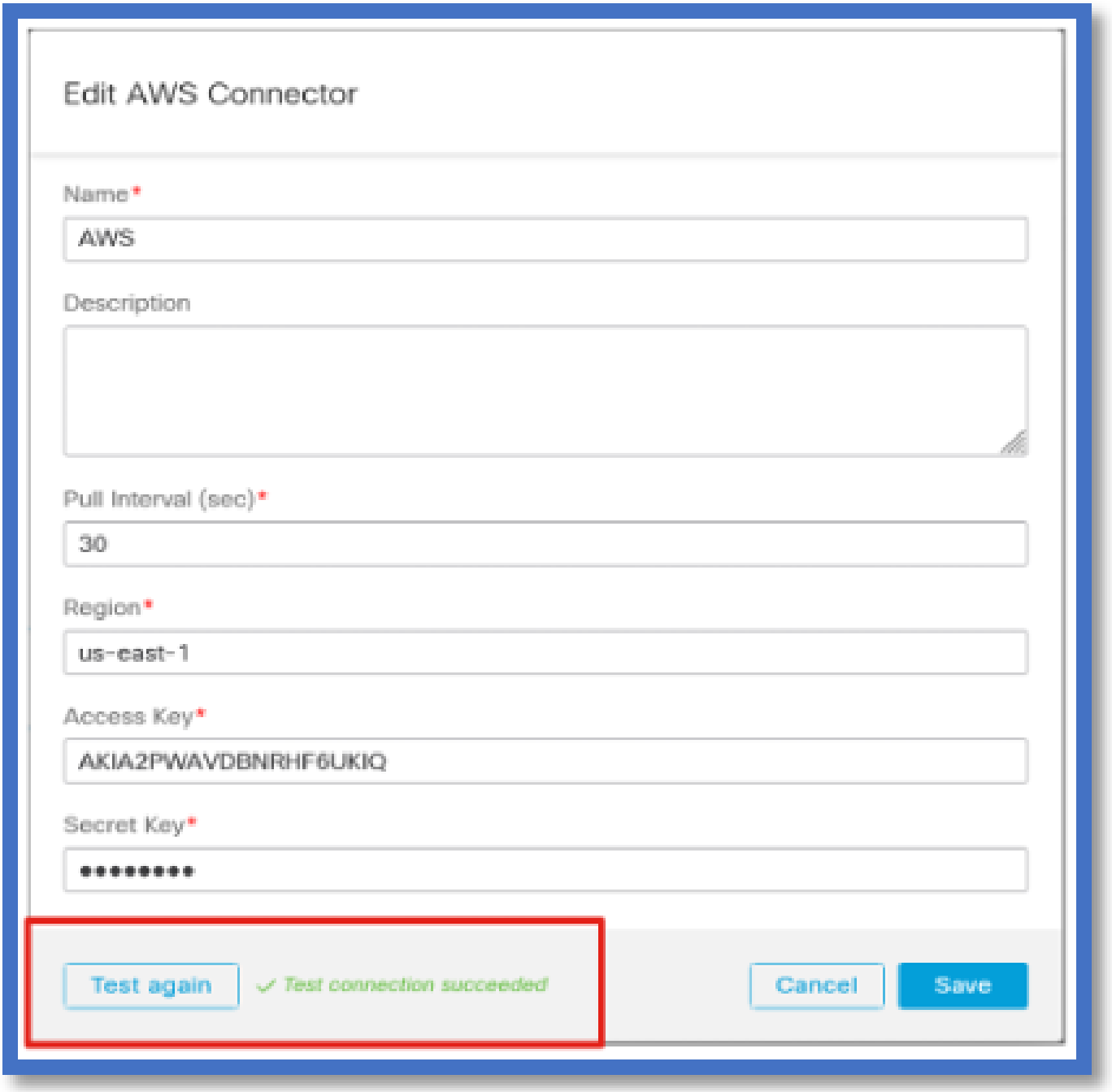
從儀表板新增聯結器

在「圖示板」上，按一下所需聯結器的圖示以新增它。



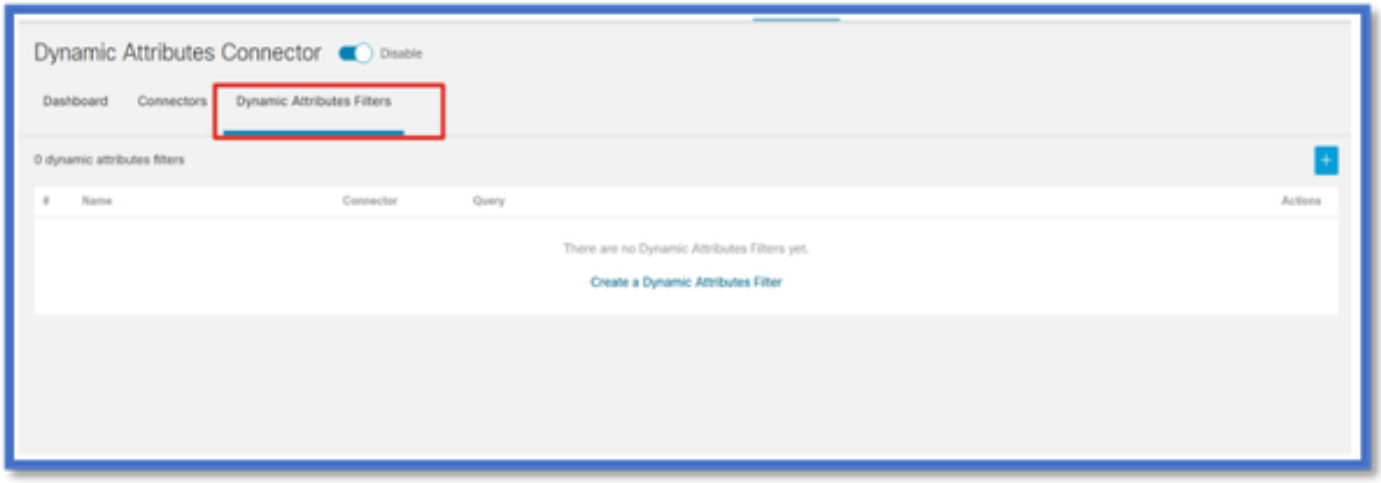
配置時間間隔(在「提取間隔」(Pull Interval)欄位中)，以便聯結器可以按照配置的週期從提供程式提取資訊。

輸入提供者證明資料以取得標籤屬性。設定好聯結器之後，您可以按一下「測試」按鈕來測試聯結器。



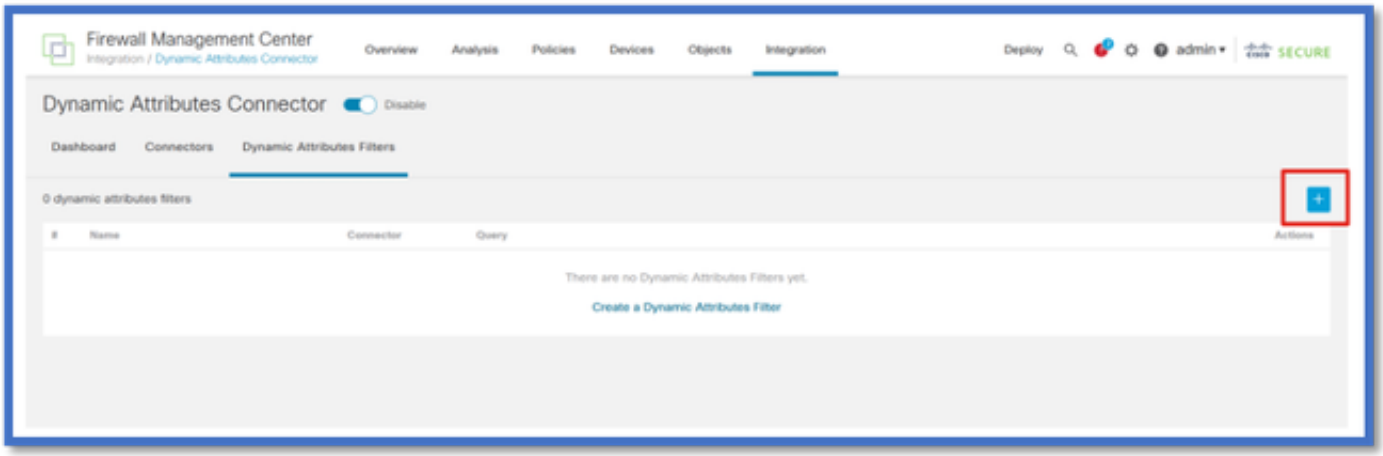
配置過濾器

按一下「動態屬性聯結器」功能表中的「動態屬性篩選」標籤，即可移至「動態屬性篩選」頁面。



新增篩選條件

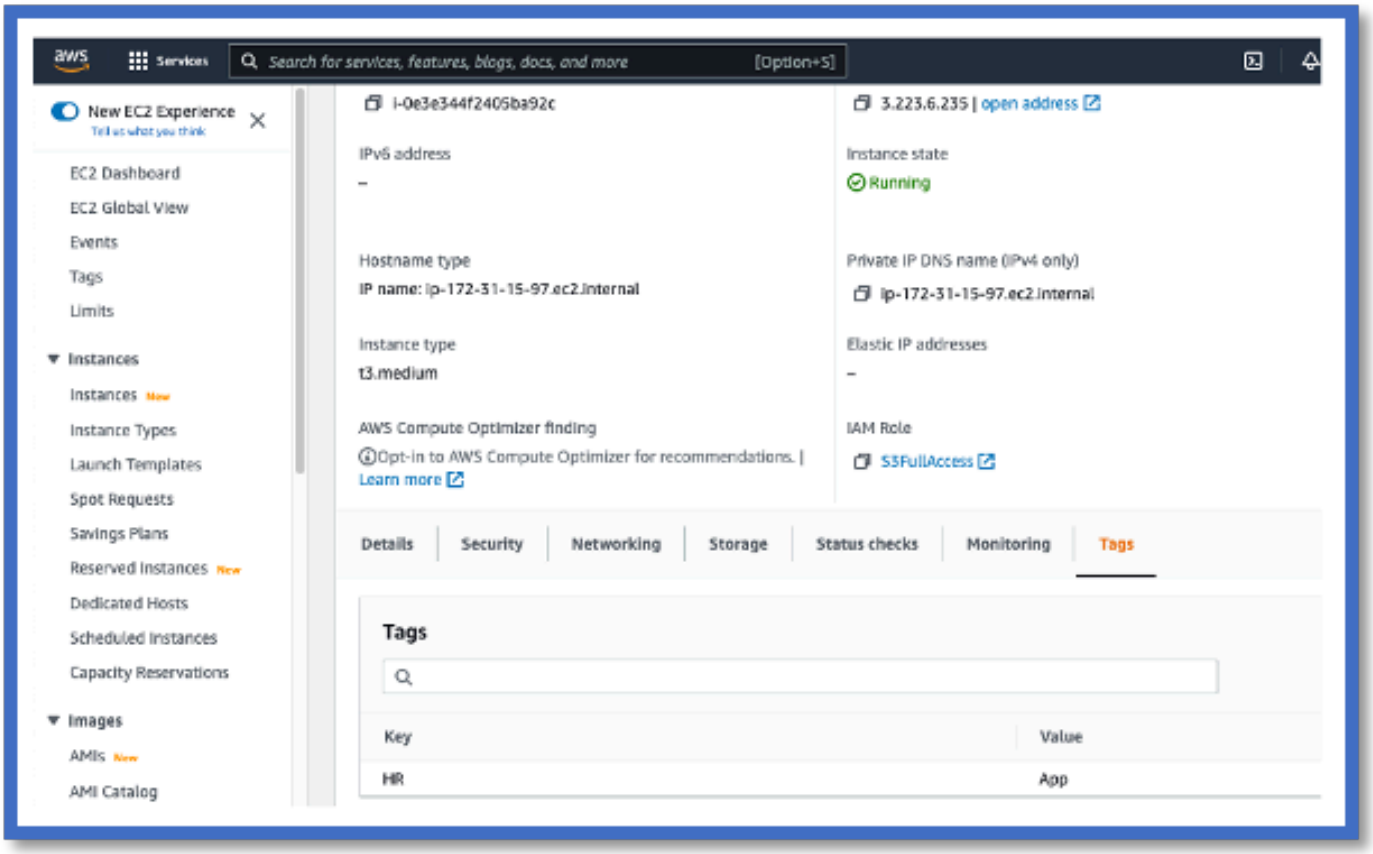
按一下+按鈕，建立屬性聯結器的篩選條件。



增加AWS標籤

例如，我們可以假設您對AWS工作負載中的關鍵「HR」和價值「App」感興趣。

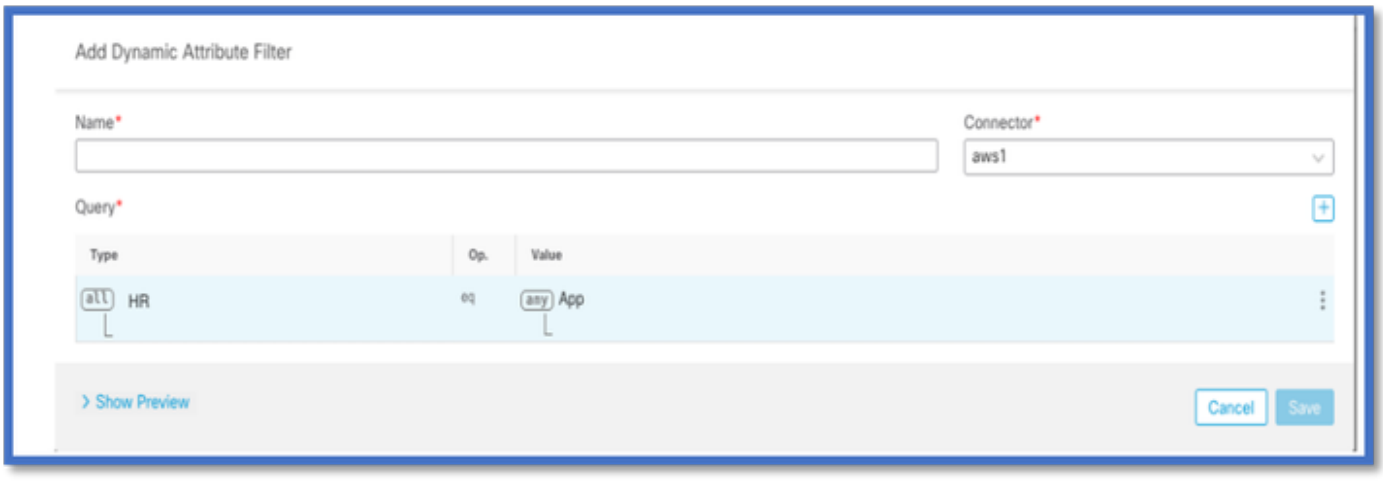
這在AWS中將是這樣。



FMC中的CSDAC

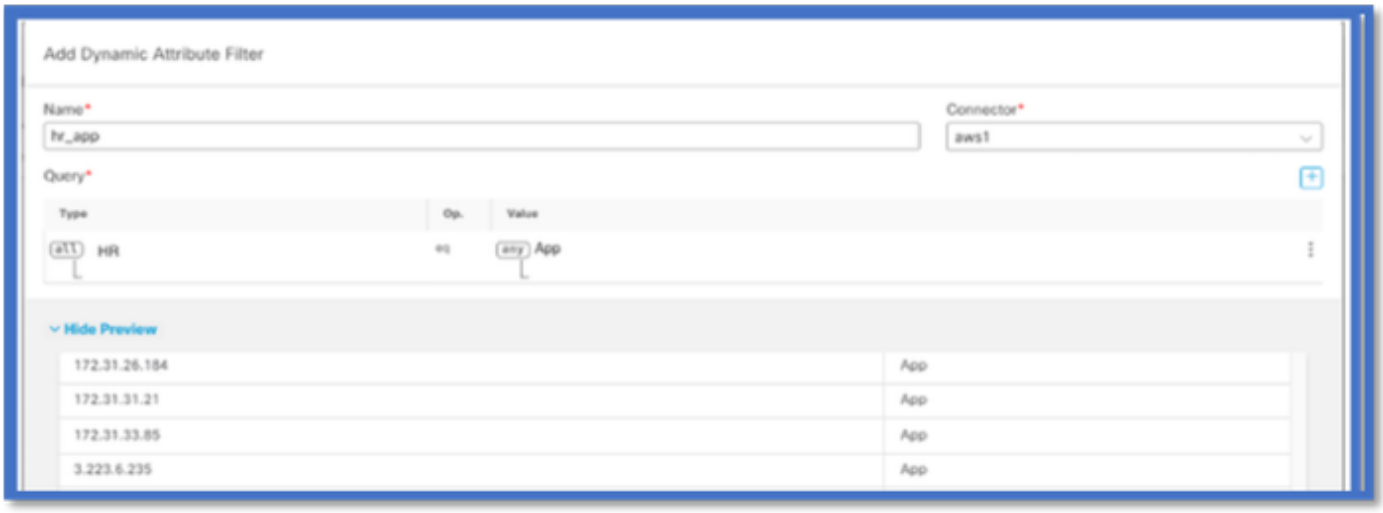
您可以按一下+按鈕來建立「HR等於應用程式」規則。

本地FMC介面卡會將匹配的IP地址作為動態對象對映傳送到FMC



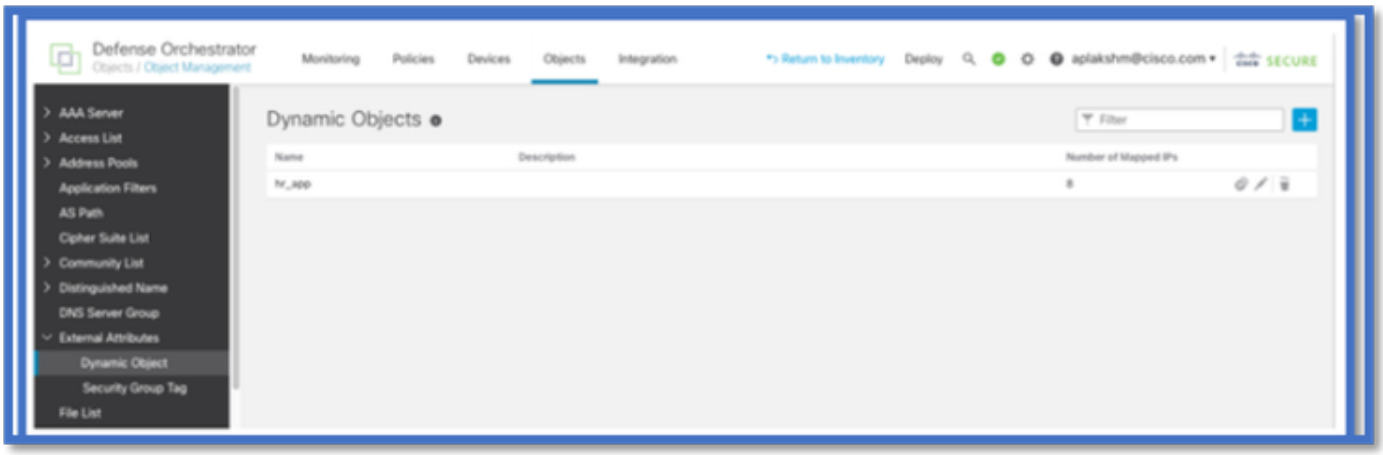
預覽

您也可以按一下「顯示」來檢視特定屬性規則的相符的IP位址 | 隱藏預覽按鈕。



動態物件

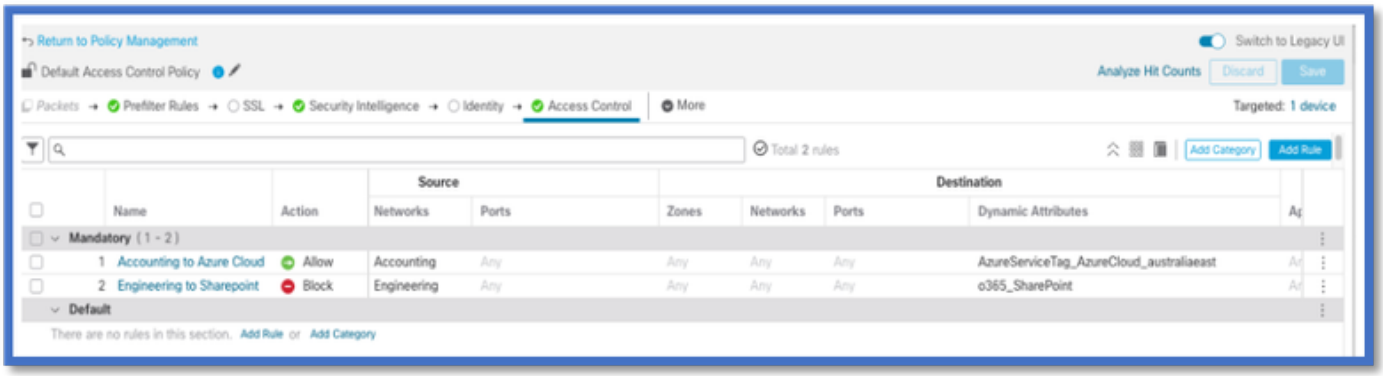
在「物件>外部屬性，在FMC中檢視CSDAC建立的動態物件」



AC策略

配置：訪問策略

在FMC中，增加訪問策略以允許或阻止從動態屬性聯結器接收的動態對象。



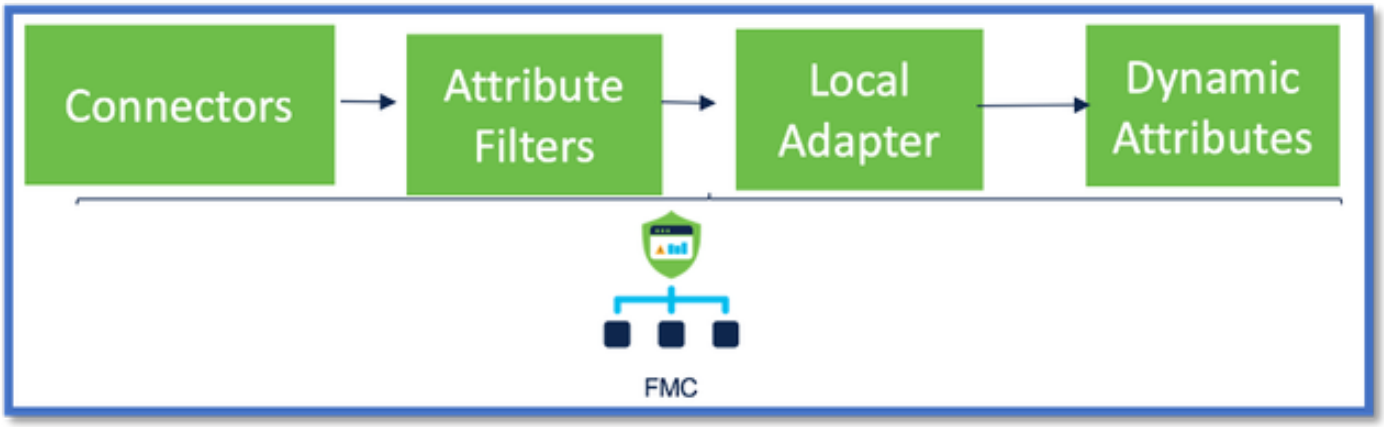
平台限制

- 聯結器限制取決於可用的FMC記憶體。
- vFMC需要額外的1GB記憶體以支援5個聯結器
- Azure AD領域也包含在限制中，因為它也是CSDAC容器。

型號	支援的聯結器數目	平台	基於記憶體的限制
基本	僅Azure AD	1600	32GB
小型	5	vFMC	> 32 GB
中	10	vFMC 300、2600	>= 64 GB
大型	20	4600	>= 128 GB

疑難排解/診斷

疑難排解的最佳方式是從CSDAC聯結器追蹤動態物件至FMC中的Dynamics屬性。許多內部記錄會將此功能稱為「彙總程式」。您可以透過廣播鏈進入系統狀態以隔離問題。CSDAC使用Docker容器。 日誌和其他檔案的消息和名稱必須稱為「docker」



檢查聯結器

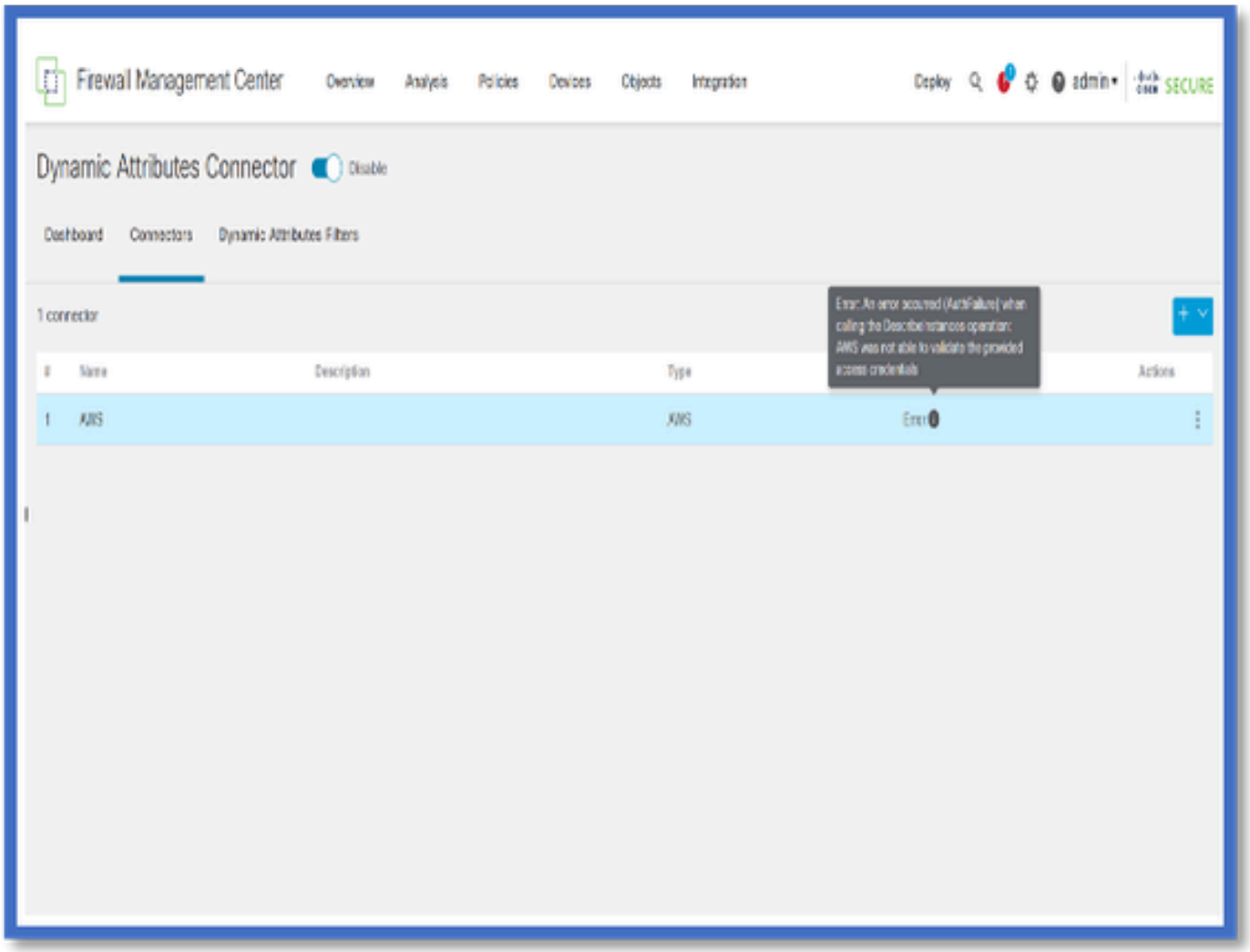
首先確保Connectors可以連線到vCenter、AWS或Azure伺服器。

如果未正確配置聯結器，則下游進程無法獲得標籤資訊。

從聯結器標籤檢視聯結器

聯結器狀態顯示在狀態列位中，每15秒更新一次。

在此，我們看到聯結器無法使用提供的憑據進行身份驗證。



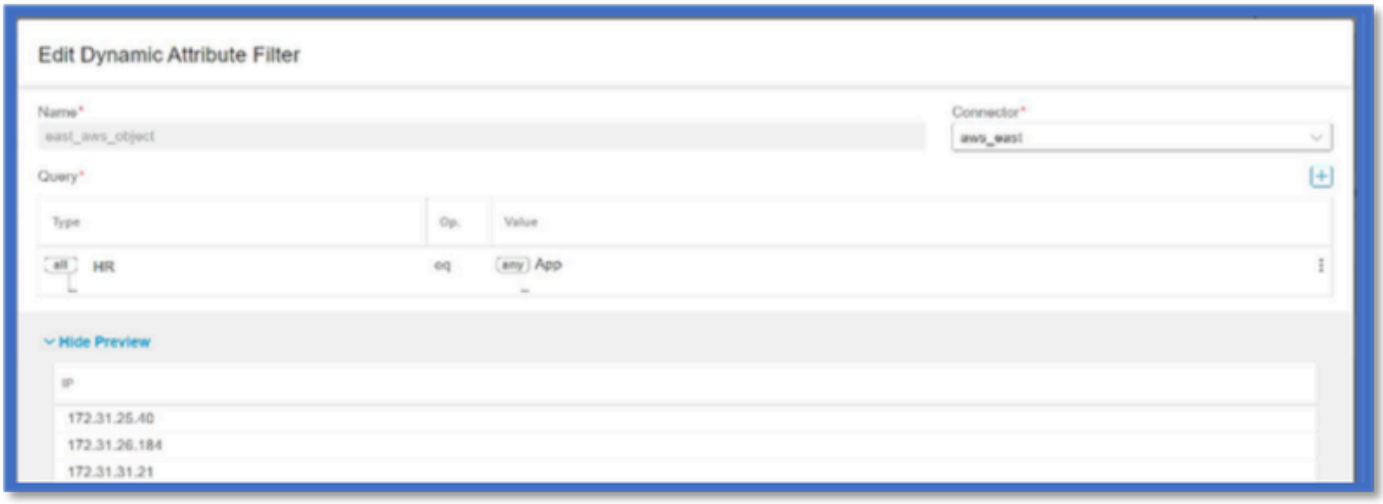
檢查屬性篩選器

確保規則預覽顯示查詢條件的匹配IP地址。

如果沒有匹配的IP地址，則FMC無法獲取動態對象對映。

檢查屬性篩選器

檢查動態屬性IP對映在預覽中是否可用。「顯示預覽」按鈕可在「動態屬性篩選」編輯快顯功能表上使用。



檢查FMC UI中的動態對象

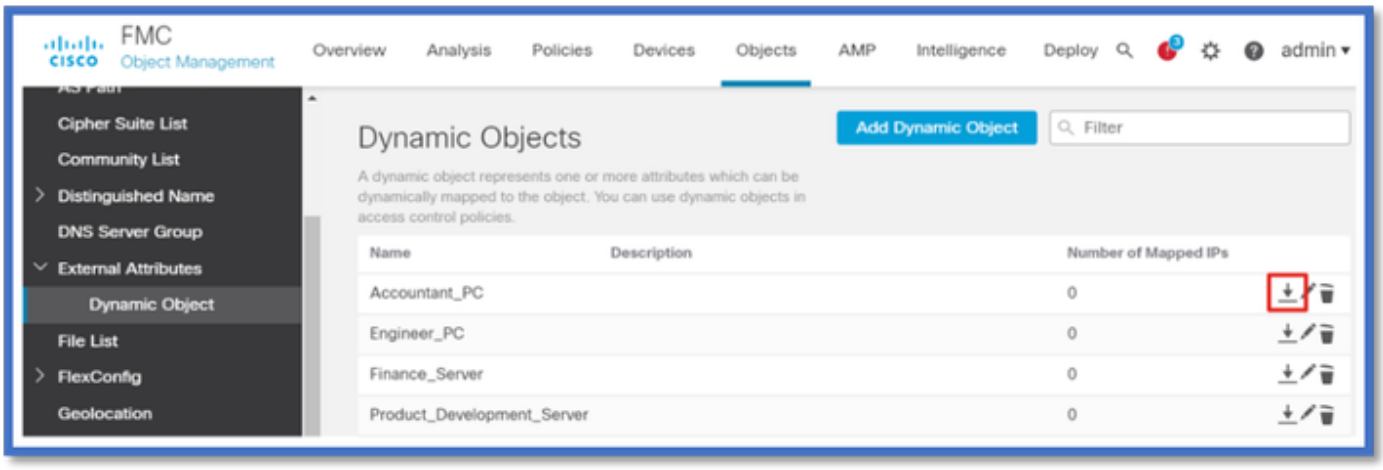
首先，請確定FMC伺服器包含您預期的繫結。

- 在物件管理、外部物件標籤下，檢查動態物件是否有繫結。
- 如果FMC沒有取得連結，則FTD無法取得連結。

檢查FMC運行狀況監控器和通知，以獲取CSDAC運行狀況警報。

檢查動態物件

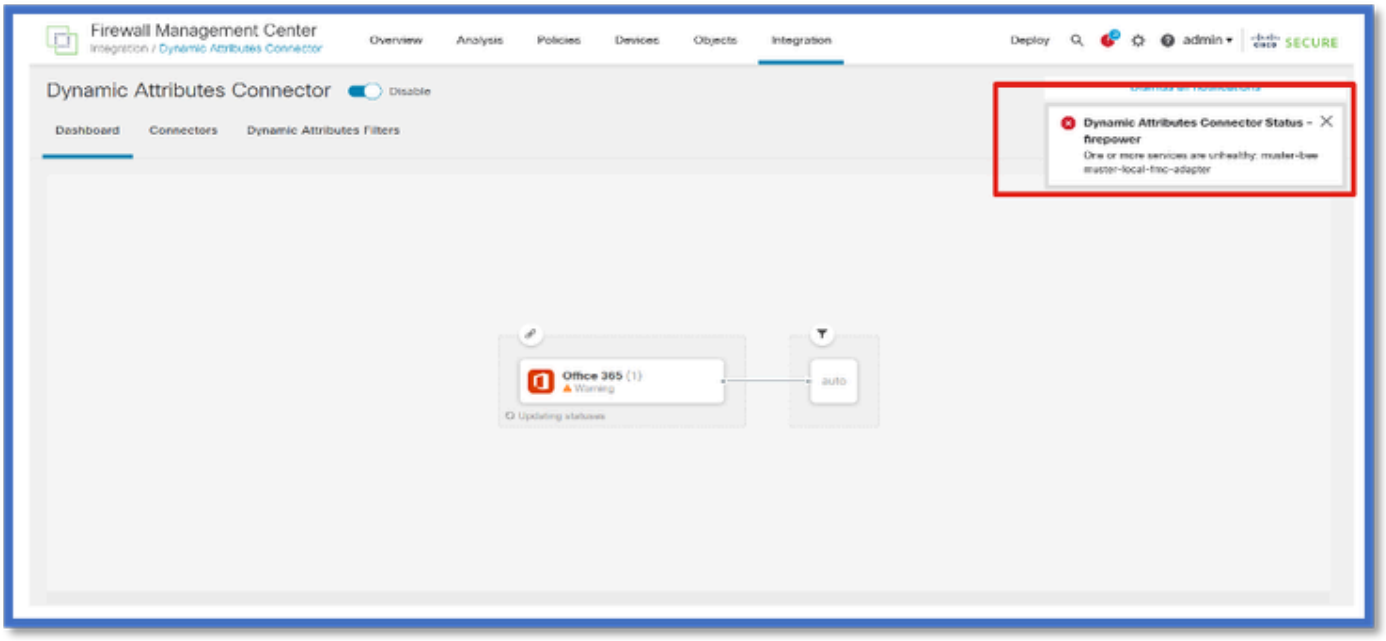
FMC對象管理器允許您下載當前動態對象IP地址。



CSDAC健康警示

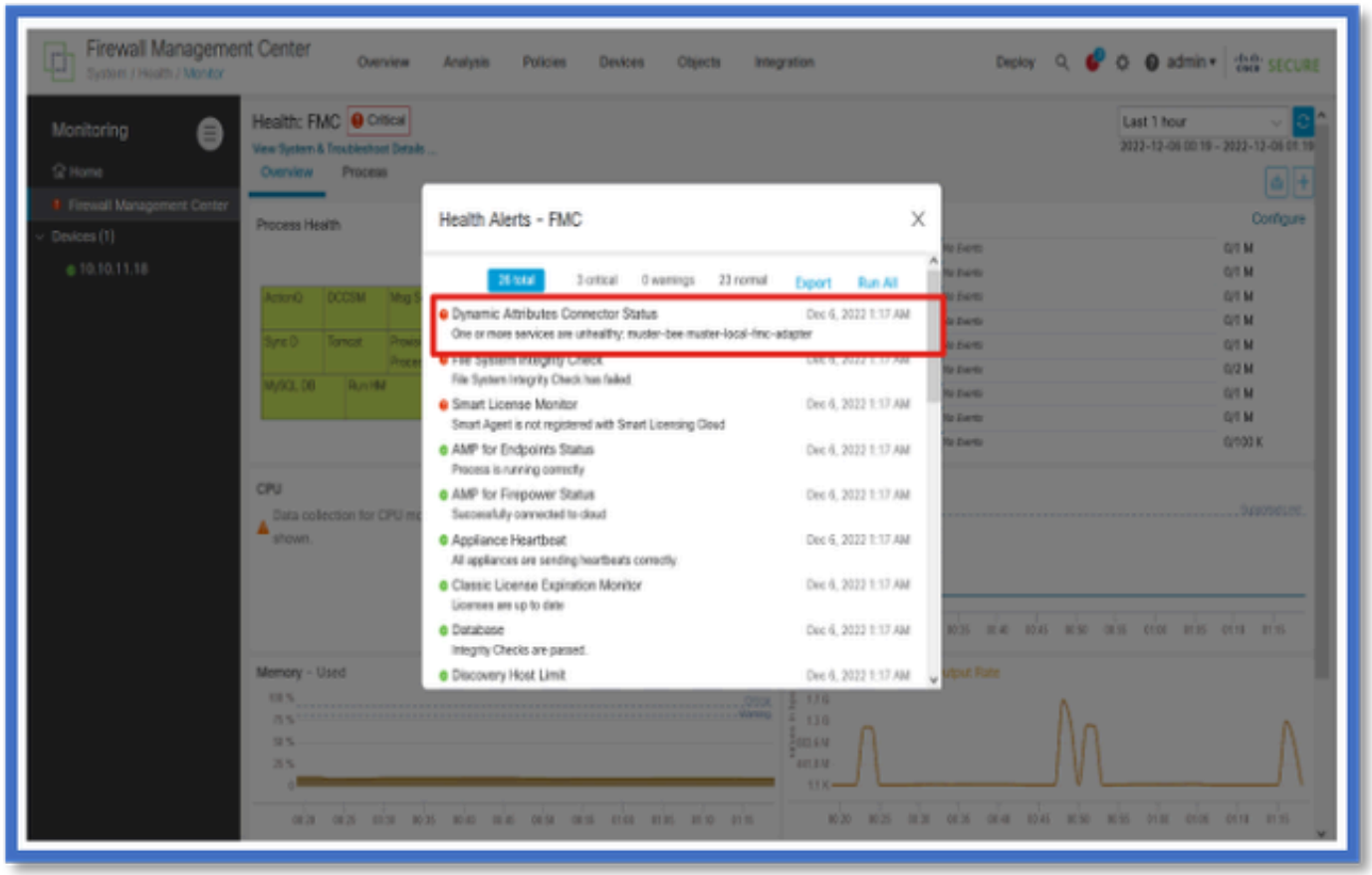
如果任何核心服務（包括動態屬性聯結器）發生故障，FMC的工作管理員將顯示運行狀況警報。該警報包含有關服務名稱和狀態的資訊。

注意：我們仍有「集」命名出現在多個通知中，此處需要提供服務名稱以獲取詳細資訊。



這裡，我們看到火蜂和火蜂本土FMC介面卡是「不健康的」。

如果錯誤指示任何核心服務，則需要收集故障排除日誌以進行調試。



CSDAC的故障排除

生成CSDAC故障排除

- CSDAC日誌在FMC故障排除生成期間自動收集。捆綁包包含Docker狀態、日誌和離線問題調試所需的資料。
- 在重現錯誤之前啟用CSDAC調試模式是好的做法，針對該錯誤收集了故障排除日誌。

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

在下列資料夾中，尋找Untared Troubleshoot中的CSDAC記錄：

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

這包含儲存在etcd資料庫中的資料。

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

這包含docker容器中的日誌。

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

這會顯示容器狀態、版本和docker映像詳細資訊。

CLI故障排除

muster-cli script可用於從FMC CLI檢查CSDAC的狀態。

如果任何服務的狀態為「已退出」或不同於「啟動」，則首先檢查該容器的日誌。

獲取日誌需要容器Name；可以從輸出中獲取。

```
'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調試模式

可以使用「muster-cli」指令碼打開和關閉調試日誌。預設情況下，容器記錄在INFO level.INFO中，僅支援DEBUG級別。

啟用調試級別使用者：./muster-cli debug-on.

這將提供用於產生疑難排解的更多資訊，並協助進行偵錯。在重現問題時，必須啟用此選項。

要返回到INFO級別，請使用：./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
```

使用Debug記錄的消息

啟用除錯模式時，所有docker容器日誌也會包含除錯訊息

使用docker命令即時獲取日誌： docker logs -f <container_name>

在下面的示例中，調試消息顯示觸發gRPC錯誤的原因

<#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
```

疑難排解逐步解的問題範例

問題和疑難排解概述

問題:

我們遇到的最常見問題是FMC無法接收所有動態對象對映。

疑難排解:

若要疑難排解問題，我們

- 從「muster-cli」啟用調試模式
- 從FMC UI生成的故障排除檔案
- 已檢查收集的「故障排除」中的CSDAC AWS Connector日誌。
- 發現CSDAC AWS Connector僅查詢AWS例項中的第一個IP。

準備疑難排解套件

- 在FMC CLI中，我們使用。/muster-cli debug-on啟用調試模式。muster-cli工具位於 /usr/local/sf/csdac。
- 已重新建立問題，方法是等待聯結器的狀態變為「正常」，然後檢查「動態屬性篩選」。
- 從FMC UI收集故障排除日誌並提取它們。已檢查AWS Connector日誌中是否有快照內容

檢視IP的標籤屬性

給定IP的標籤屬性記錄在故障排除日誌中。對於AWS Connector，我們檢視了muster-connector-aws.1.muster-docker.log.gz

檢查摘要

接頭和介面卡狀態是否正常？

檢查對應的「聯結器」、「介面卡」頁中的狀態。

聯結器是否獲得了所有對映？

檢查規則預覽是否匹配IP地址。

檢查「聯結器」檔案處理程式記錄檔，檢視其是否正確查詢對應。

REST伺服器是否從聯結器接收動態標籤對映？

檢查FMC動態物件頁面。

檢查USMS日誌(位於/opt/CSCOpx/MDC/log/operation/usmsharedsvcs.log)，檢視FMC REST伺服器是否正確處理來自CSDAC的API請求。

問答

問：什麼版本的內部部署CSDAC支援ISE聯結器？我在7.4.0版（內部版本1494）中也沒有看到這樣的聯結器。

答：這是獨立的CSDAC，而不是FMC或CDO。您需要一個CSDAC Ansible套件來測試它。

問：發佈時，會採用什麼本地CSDAC版本？

答：可能是2.1.0。

問：顯示了一個上面放置了API的裝置的螢幕。我認為是CSDAC，這是什麼意思？

答：此CSDAC中內建了API瀏覽器，您可以從該頁面對CSDAC進行API呼叫。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。