FMCでのセキュアなダイナミック属性コネクタの展開

内容

はじめに

このドキュメントでは、FMCのCisco Secure Dynamic Attribute Connector(DAC)について説明します。

背景 – 問題

CSDAC(Cisco Secure Dynamic Attributes Connector)をFMC(Firepower Management Center)に統合すると、スタンドアロンのCSDACアプリケーションおよびCDOのCSDACと同じレベルの機能を提供できます。スタンドアロンCSDACでは、CSDAC用の個別マシンの管理と保守のオーバーヘッドから顧客を解放します。ネットワーク管理者として、プログラマチックインターフェイスを統合し、外部のダイナミック環境プロバイダーの変更に合わせて最新の状態を維持しやすくしたいと考えています。この統合により、ポリシーを導入することなく、動的に変化するクラウド環境から属性を収集するという問題が解決されます。

ソリューション（概要）

CSDACをFMCで構成して、Azure、vCenter、AWS、GCP、Office 365、およびAzure Service Tagからタグ属性を取得できるようになりました。これにより、CDOのスタンドアロンCSDACおよびCSDACと同等の機能が提供されます。

- を使用する方法を選択できます
  - FMCのCSDAC（または）
  - CDOのCSDAC（または）
  - スタンドアロンCSDAC
- ターゲット市場：エンタープライズ、サービスプロバイダー

FMCでのダイナミック属性コネクタの概要

FMCダイナミック属性コネクタ：

- 動的属性コネクタ機能を構築および操作するためのダッシュボード画面。
- ソースワークロードコネクタ(AWS、Azure、vCenter、Office 365、GCP)を構成するためのFMC UI
- ダイナミックオブジェクトを作成するダイナミック属性フィルタを定義するFMC UI

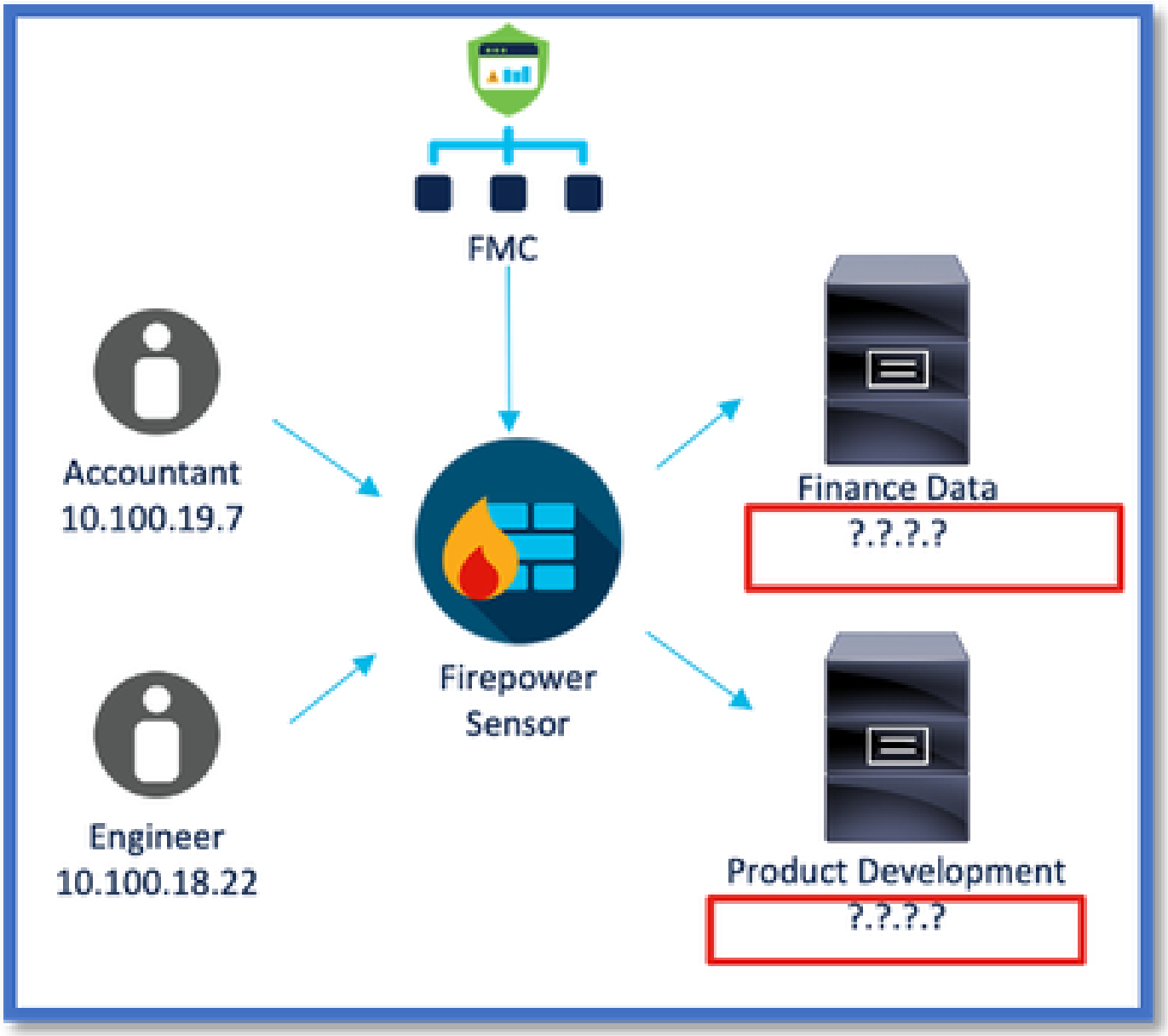
導入例

オンプレミスCSDAC

昨年、AWSおよびAzureアカウントから属性を収集するために、CSDAC専用のVMをデプロイしました。

問題

現在、組織がクラウドに移行したため、自分の環境にCSDAC専用の仮想マシンを導入して管理することができません。



オプション1:FMC内に構築されたダイナミック属性コネクタを使用する

この問題は、FMC内に組み込まれたダイナミック属性コネクタを使用して修正できます。これによって作成されたダイナミックオブジェクトは、アクセスポリシーで使用できます。

オプション2：クラウド提供のダイナミック属性コネクタをCDOで使用する

この問題は、CDOのダイナミック属性コネクタを使用して修正できます。作成された動的オブジ

ェクトは、

- CDOクラウド提供FMC
- CDOオンプレミスFMC

前提条件、サポート対象プラットフォーム、ライセンス

サポートされる最低限のソフトウェアおよびハードウェアプラットフォーム

サポートされるManagerの最小バージョン	管理対象デバイス	サポートされる管理対象デバイスの最小バージョンが必要	注意事項
FMC 7.4	サポートされる任意のFTD	任意の7.0以降のFTD	

* 動的属性コネクタは、FDM管理対象デバイスではサポートされません

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。
・ 7.4を実行するCisco Firewall Management Center
・ 7.4以降を実行するCisco Firepower Threat Defense
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

機能の詳細

スタンドアロンCSDACの概要（現在リリースされている – 7.4）

Cisco Secure Dynamic Attributes Connectorを使用すると、Firewall Management Center(FMC)アクセスコントロールルールのさまざまなクラウドサービスプラットフォームのタグを使用できます。

オンプレミスCSDACはLinuxマシンにインストール可能で、次の場所からの属性の取得をサポートします。

- AWS、Azure、VMware vCenterおよびNSX-T、Office 365、Azureサービスタグ、GCP、GitHub。

CDOでのCSDACの概要（現在リリースされている – 7.4）

専用アプリケーションをインストールしてメンテナンスする必要がなく、オンプレミスのCSDACと同じ機能をサポート

vCenterコネクタは、現在CDOではサポートされていません。

CDOのクラウド配信FMCとオンプレミスFMCへの受信属性の送信をサポート

FMCでのCSDAC

スタンドアロンCSDACと同じ機能をサポートし、専用アプリケーションをインストールして維持する必要はありません。

FMCのCSDACは次からの属性の取得をサポートしています：

- AWS、Azure、VMware vCenterおよびNSX-T、Office 365、Azureサービスタグ、GCP、GitHub

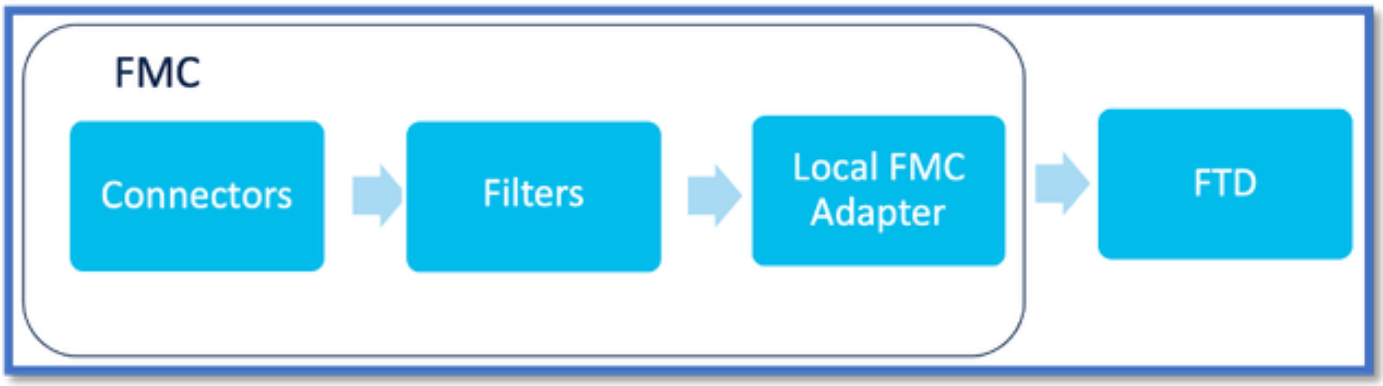
FMCに対してローカルであるため、明示的なアダプタ設定はありません。

仕組み

コネクタは、AWS、Azure、o365、vCenterから属性を取得するために使用されます。

次に、ローカルアダプタを使用して、これらの合理化された属性とそのIPマッピングをFMCにダイナミックオブジェクトとして保存します。

FMCはマッピングをリアルタイムでFTDに送信します（展開なし）。



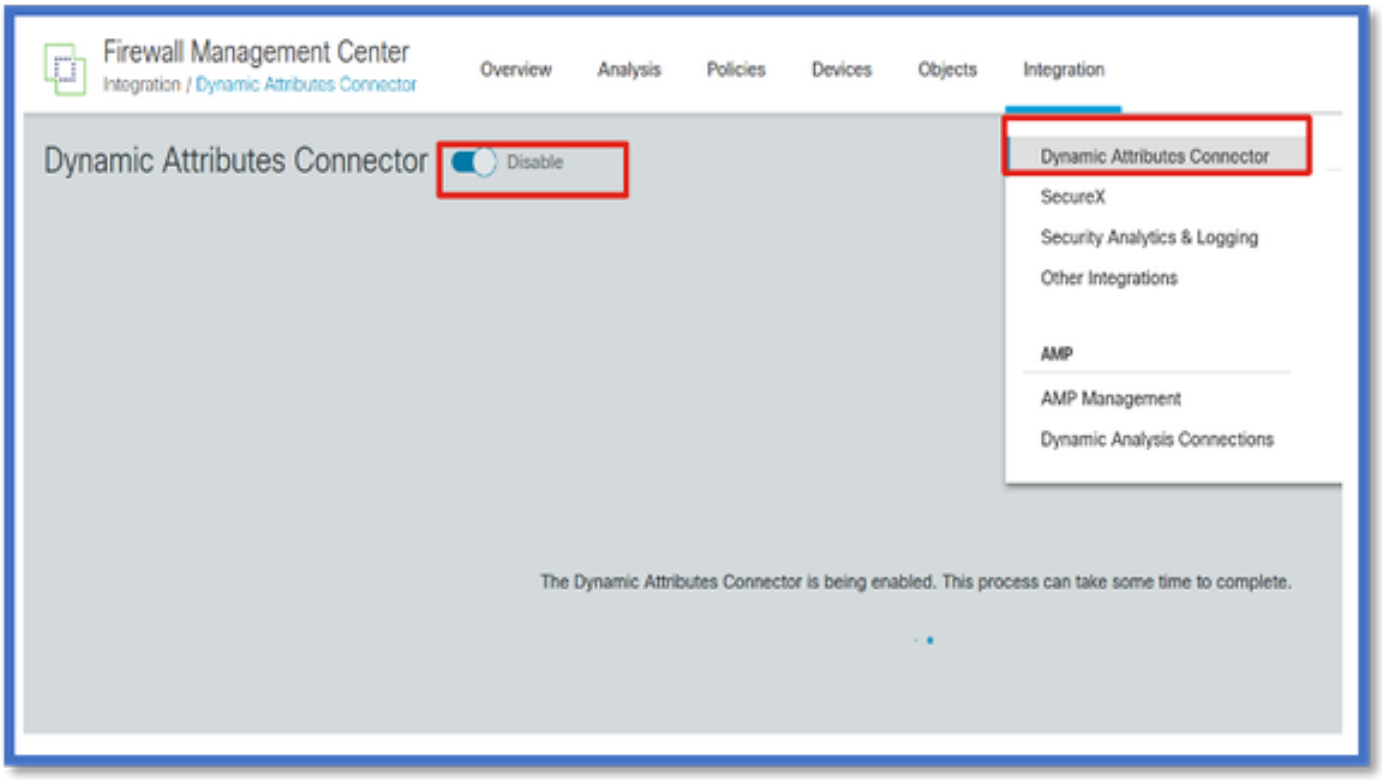
FMCでCSDACを有効にします

「統合」>「動的属性コネクタ」にナビゲートします。

[切り替え]ボタンを使用して、コネクタを有効にします。

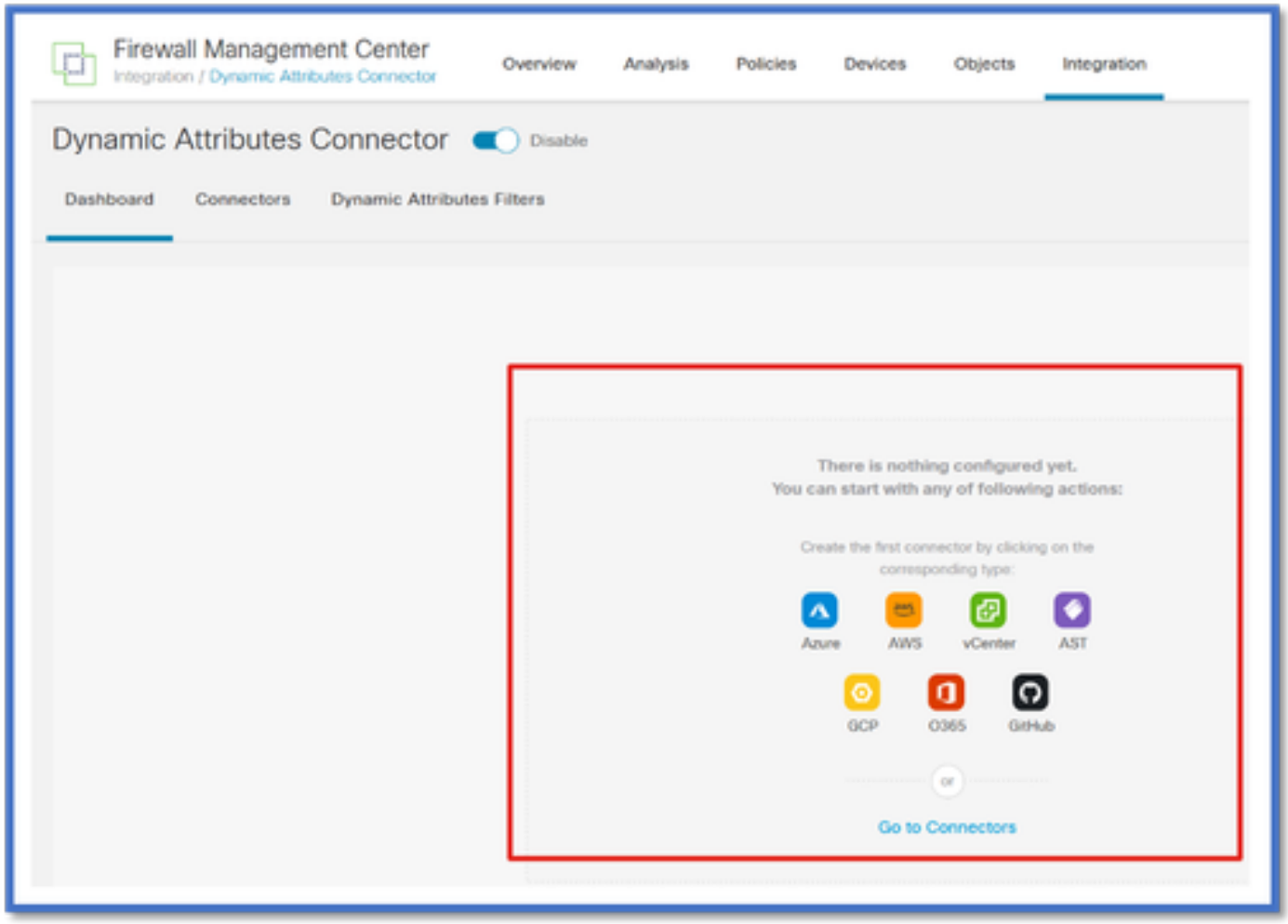
FMCでは、Dockerイメージとコンテナをダウンロードして起動するのに数分かかります。

これは、FMCグローバルドメインでのみ設定できます。



CSDACダッシュボード

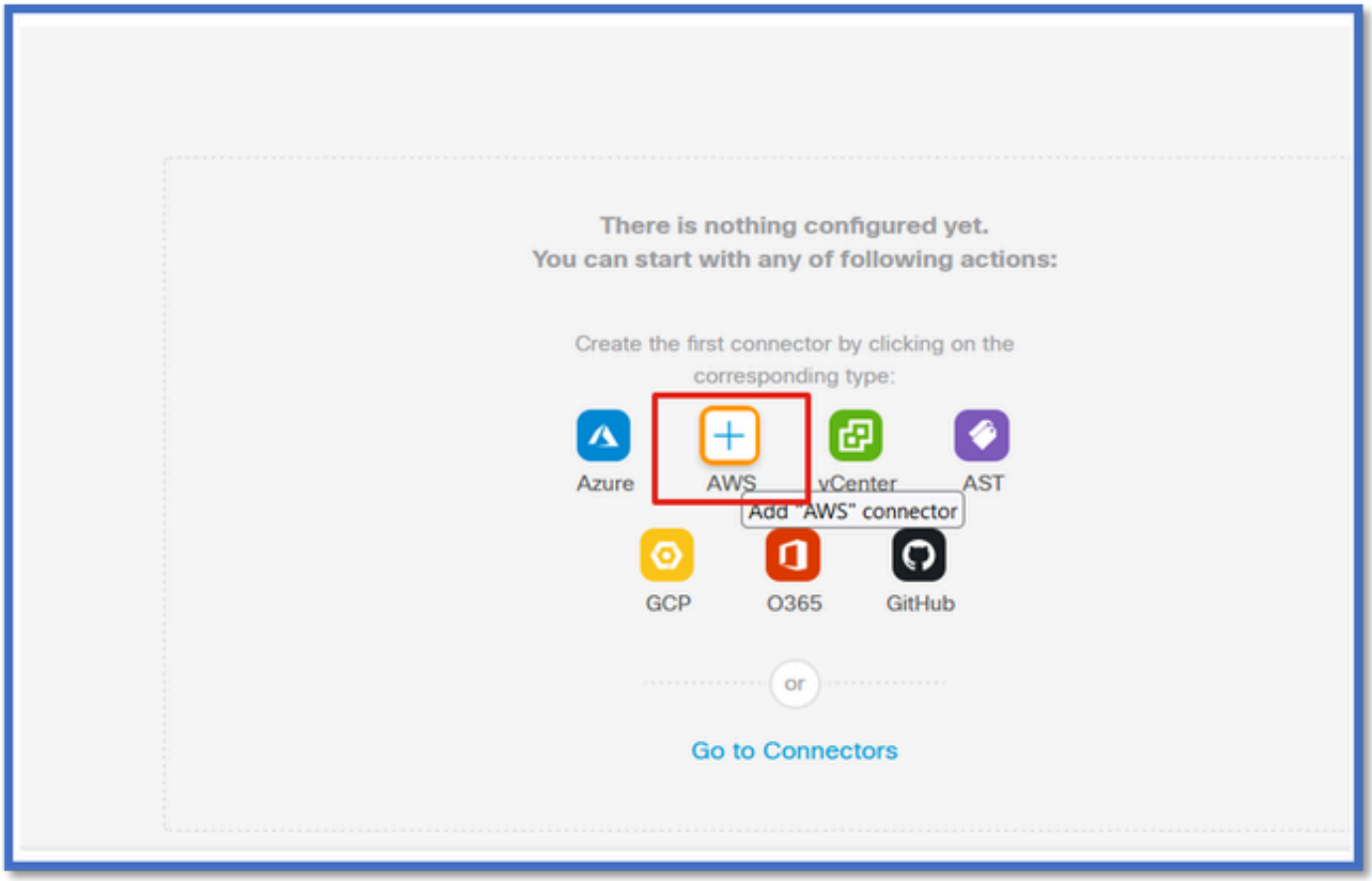
CSDACを有効にすると、CSDACダッシュボードページが表示されます。ダッシュボードは、統合コネクタとフィルタの設定と表示の両方に使用されます。



コネクタの設定

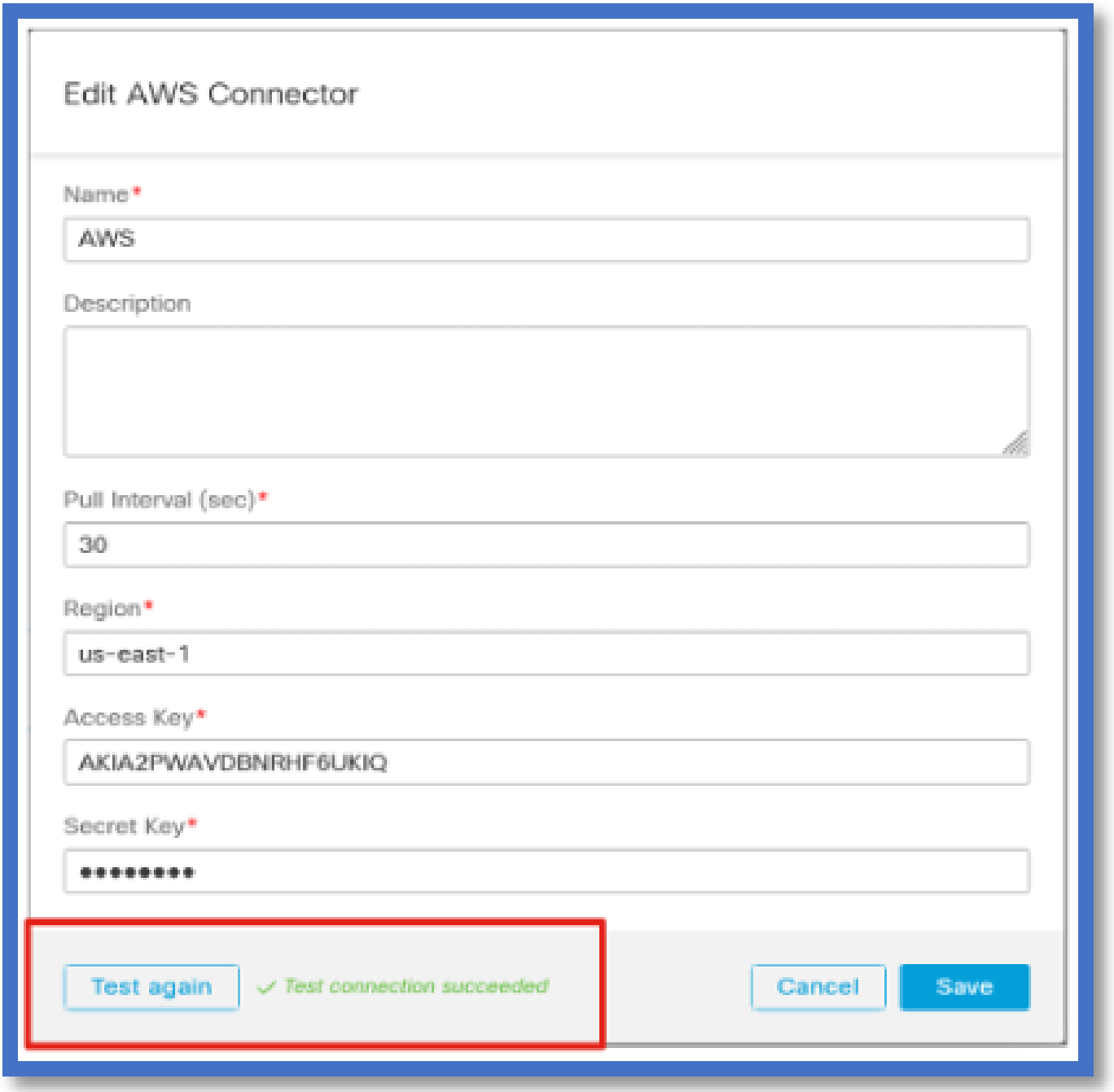
ダッシュボードからコネクタを追加

ダッシュボードで、追加するコネクタのアイコンをクリックします。



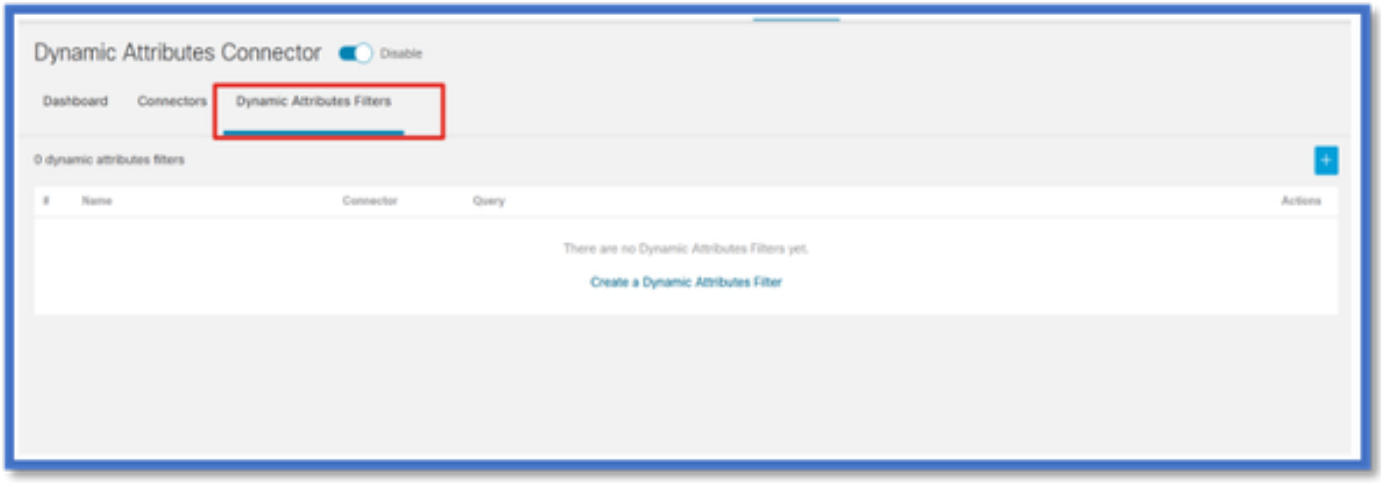
コネクタが設定された周期性を持つプロバイダから情報をプルできるように、時間間隔 (「プル間隔」フィールド) を設定します。

プロバイダーの資格情報を入力して、タグ属性を取得します。コネクタを設定したら、「テスト」ボタンをクリックしてコネクタをテストできます。



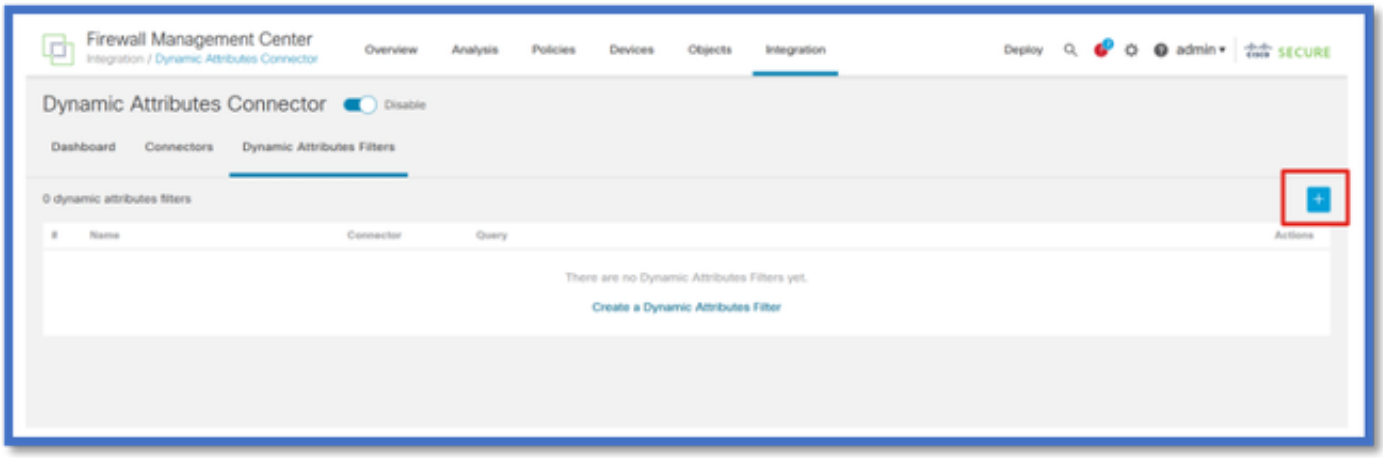
フィルタの設定

「動的属性コネクタ」メニューの「動的属性フィルタ」タブをクリックして、「動的属性フィルタ」ページに移動します。



フィルタの追加

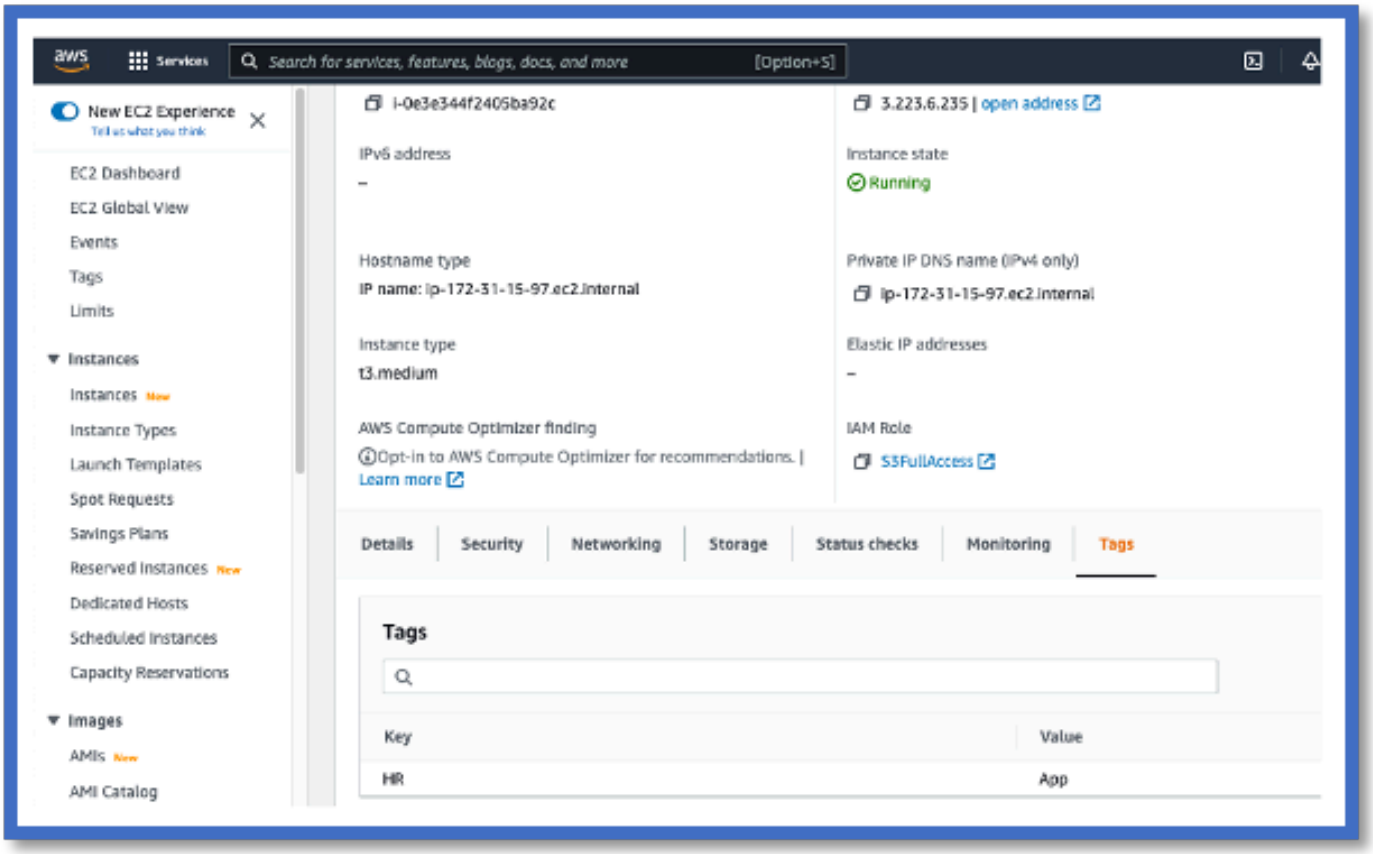
+ボタンをクリックして、属性コネクタのフィルタを作成します。



AWSタグの追加

たとえば、AWSワークロードのキー「HR」と値「App」に関心があると仮定できます。

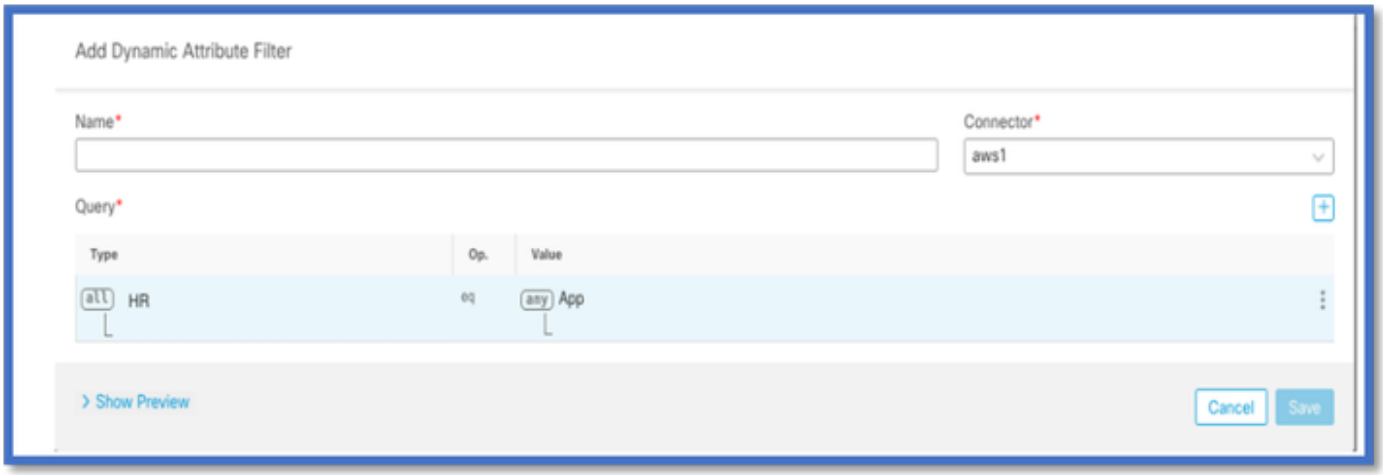
これはAWSで表示される内容です。



FMCでのCSDAC

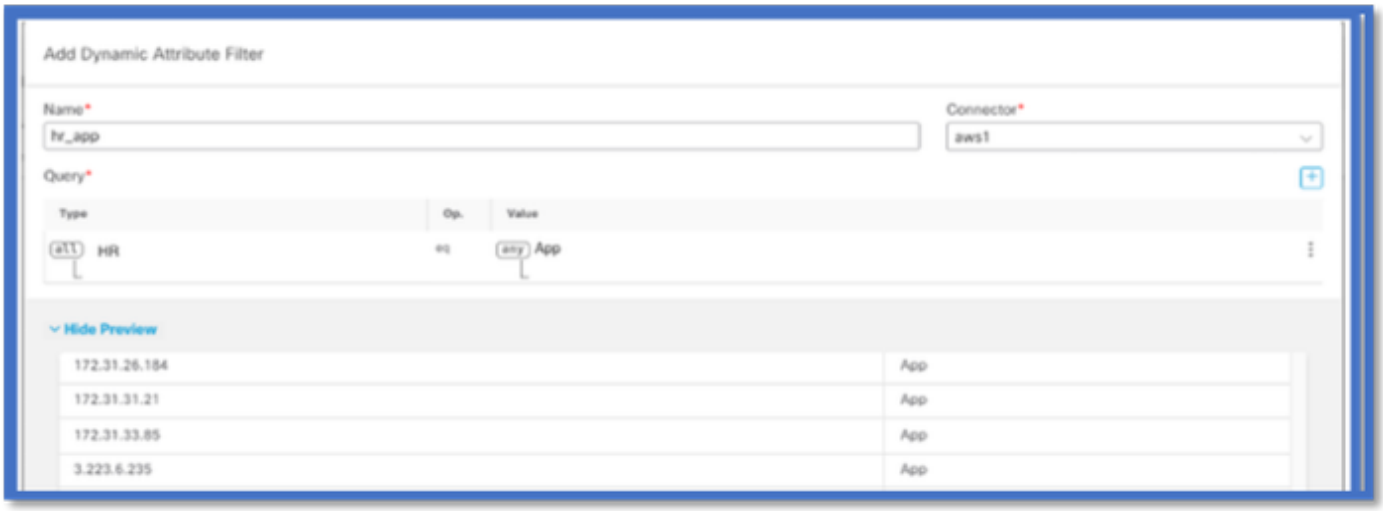
+ボタンをクリックすると、「HR equals App」ルールを作成できます。

ローカルFMCアダプタは、一致するIPアドレスをダイナミックオブジェクトマッピングとしてFMCに送信します



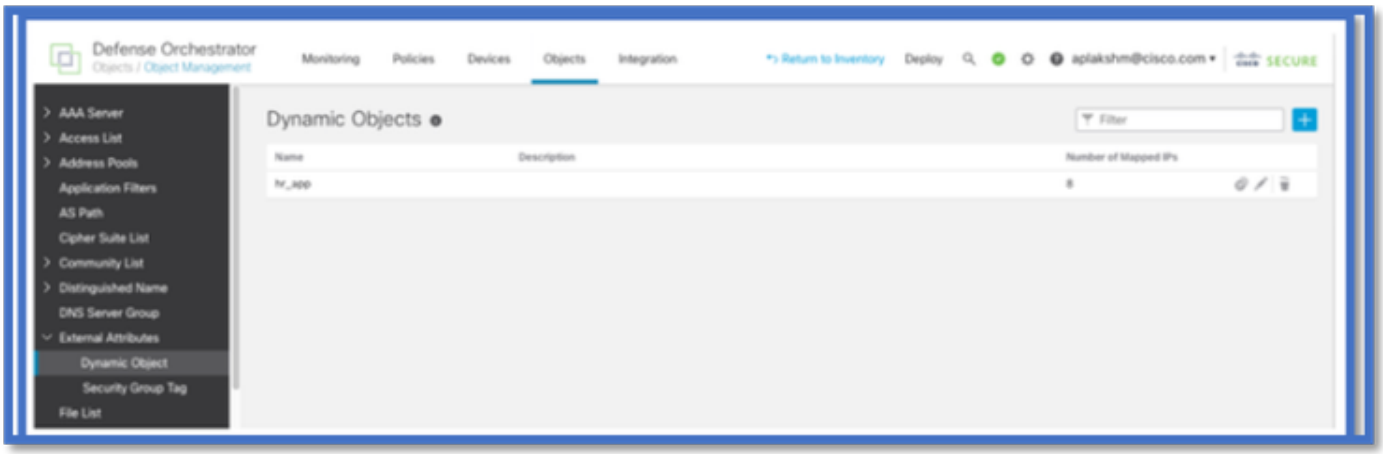
プレビュー

特定の属性ルールに一致するIPアドレスを表示するには、 | [プレビューを表示しない]ボタン



動的オブジェクト

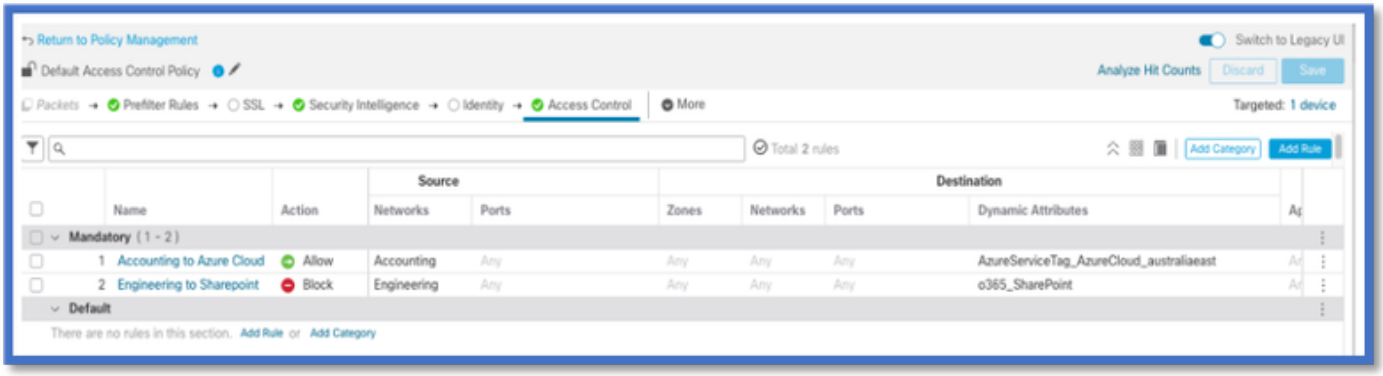
FMCのObjects > External Attributes, Dynamic ObjectでCSDACによって作成された動的オブジェクトを表示します



ACポリシー

設定：アクセスポリシー

FMCで、ダイナミック属性コネクタから受信したダイナミックオブジェクトを許可またはブロックするアクセスポリシーを追加します。



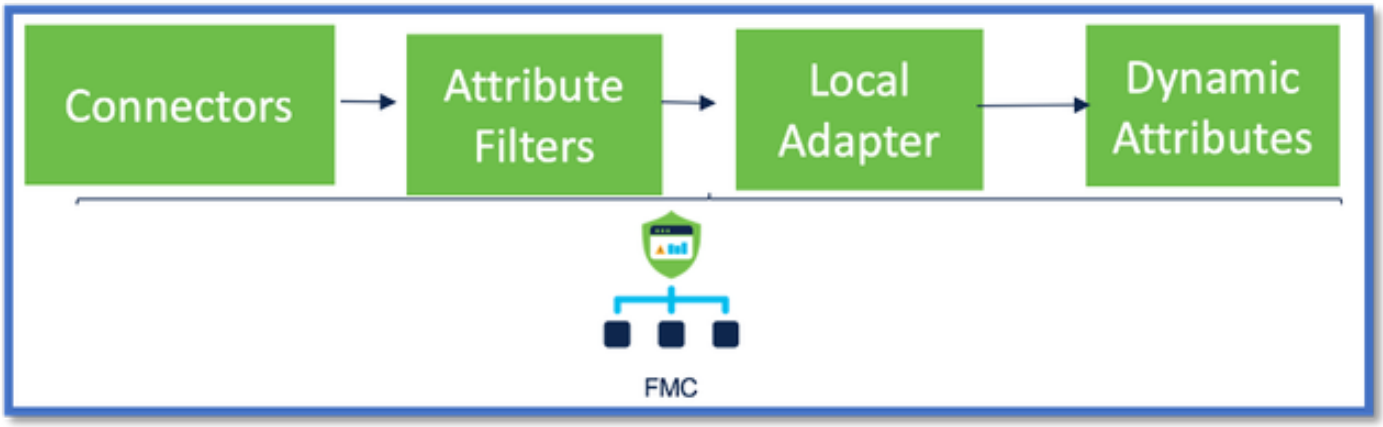
プラットフォームの制限

- コネクタの制限は、使用可能なFMCメモリに基づいています。
- vFMCでは、5つのコネクタをサポートするために追加の1 GBメモリが必要です
- Azure ADレルムもCSDACコンテナーであるため、制限に含まれています。

モデル	サポートされるコネクタの数	プラットフォーム	メモリに基づく制限
基本	Azure ADのみ	1600	32 GB
小	5	vFMC	32 GB超
中	10	vFMC 300、2600	>= 64 GB
大	20	4600	128 GB以上

トラブルシューティング/診断

トラブルシューティングは、FMCでCSDACコネクタからDynamics属性に対する動的オブジェクトをトレースすることによって実行するのが最適です。多くの内部ログでは、この機能を「マスター」と呼んでいます。ブロードキャストチェーンに沿ってシステム状態を確認し、問題を切り分けることができます。CSDACはDockerコンテナを使用します。 ログやその他のファイルのメッセージと名前は「docker」と呼ぶ必要があります。



コネクタの確認

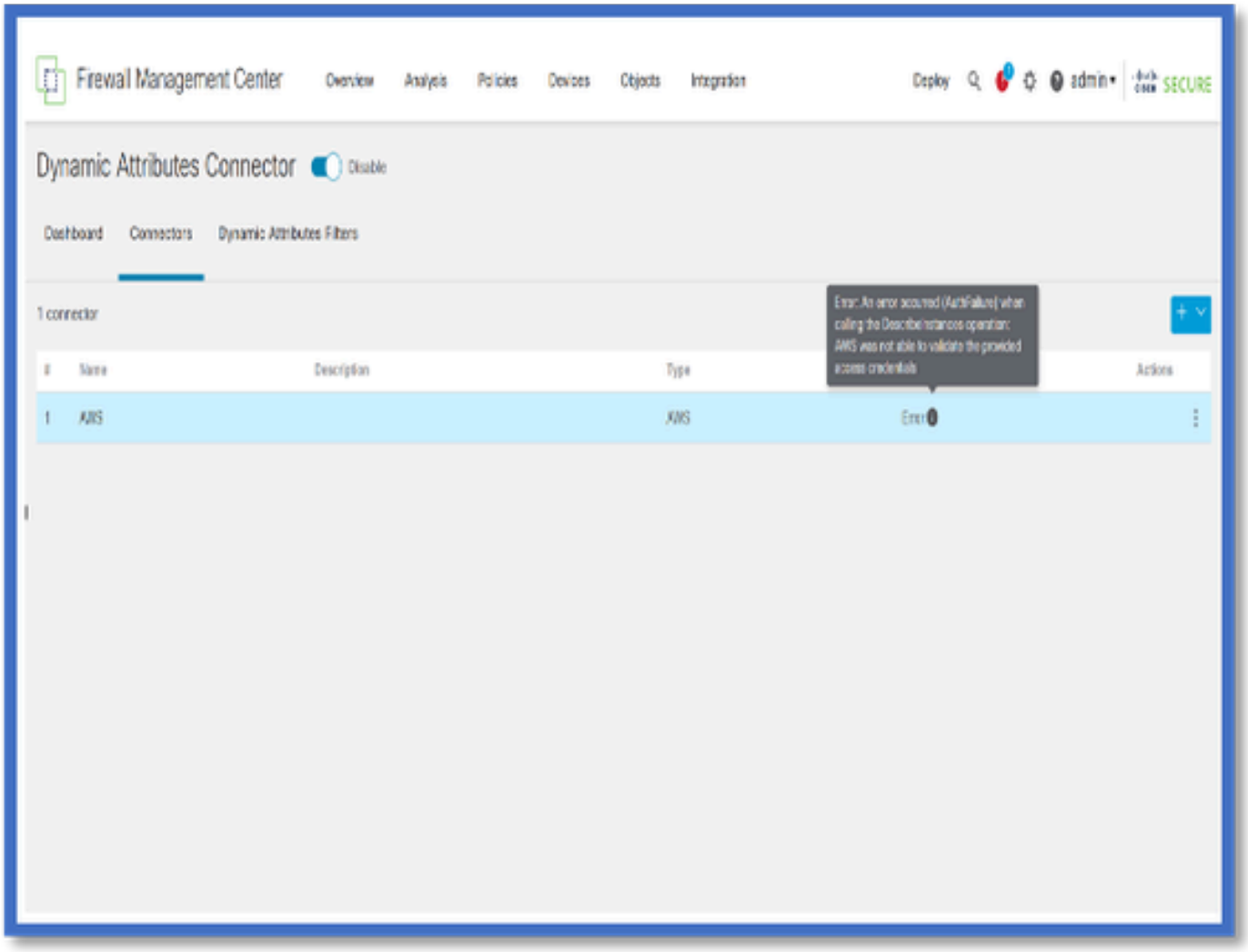
最初に、コネクタがvCenter、AWS、またはAzureサーバーに接続できることを確認します。

コネクタが正しく設定されていない場合、ダウンストリームプロセスはタグ情報を取得できません。

コネクタタブからのコネクタの表示

コネクタステータスはステータスフィールドに表示され、15秒ごとに更新されます。

ここで、コネクタが指定された資格情報を使用して認証できなかったことがわかります。



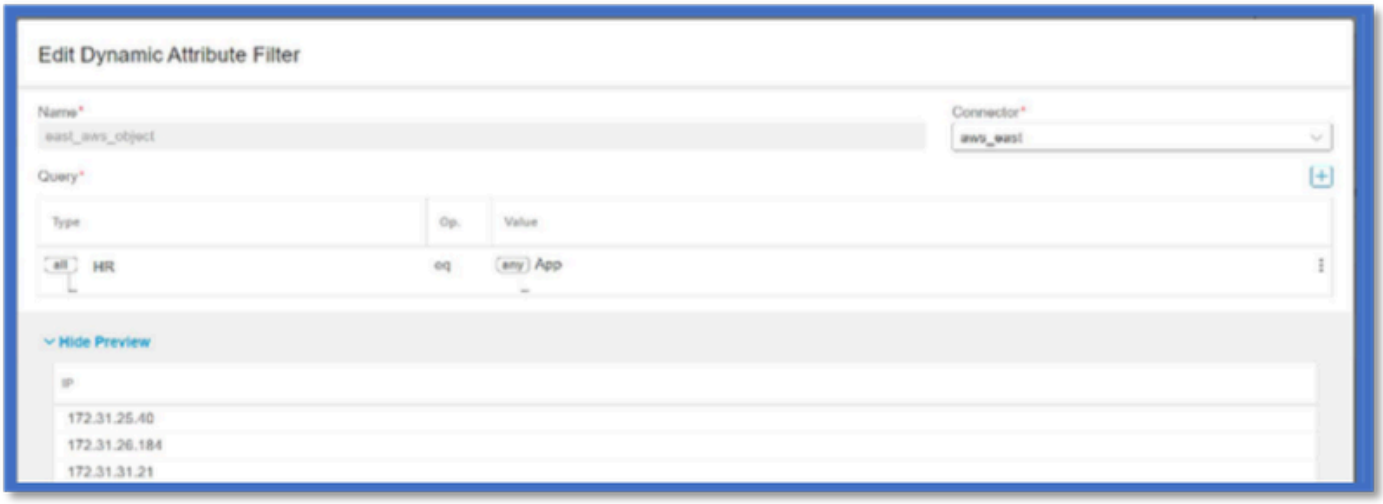
属性フィルタの確認

ルールのプレビューに、クエリ条件に一致するIPアドレスが表示されていることを確認します。

一致するIPアドレスがない場合、FMCはダイナミックオブジェクトマッピングを取得できません。

属性フィルタのチェック

ダイナミック属性IPマッピングがプレビューで使用できることを確認します。[プレビューを表示]ボタンは、[ダイナミックアトリビュートフィルタ]編集ポップアップで使用できます。



FMCのUIでダイナミックオブジェクトを確認する

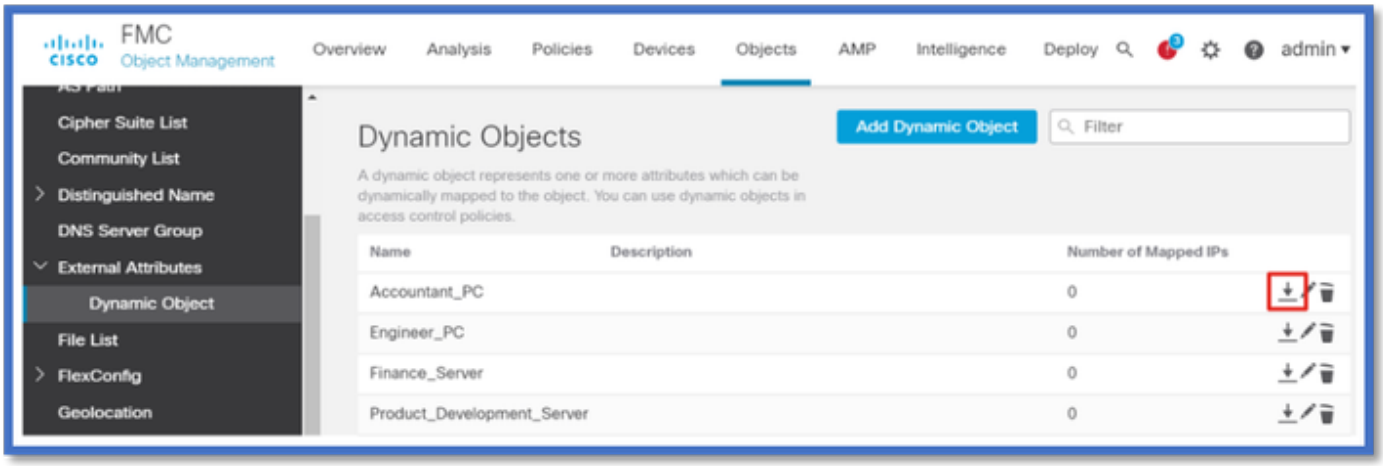
最初に、FMCサーバに必要なバインディングが含まれていることを確認します。

- [オブジェクト管理]の[外部オブジェクト]タブで、[ダイナミックオブジェクト]の[バインド]をオンにします。
- FMCがバインディングを取得しない場合、FTDはバインディングを取得できません。

FMCヘルスモニタとCSDACヘルスアラート通知を確認します。

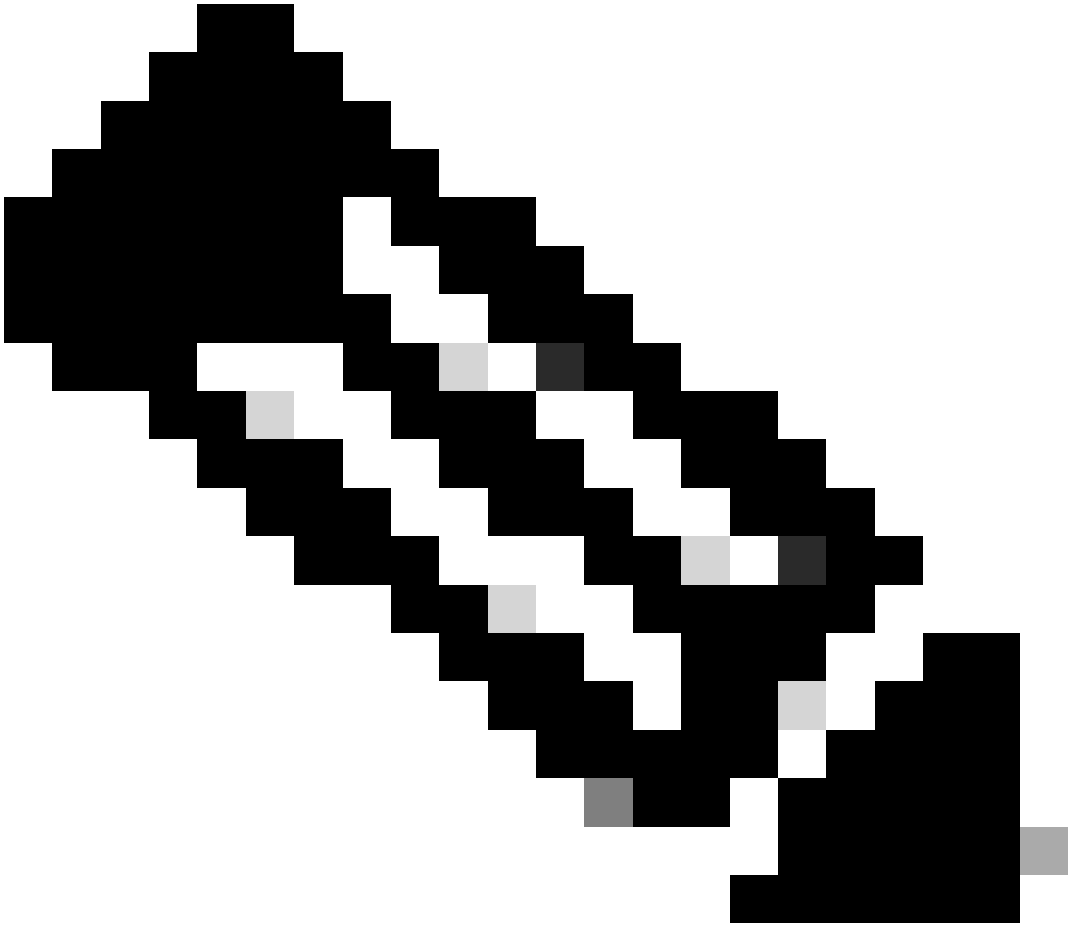
動的オブジェクトのチェック

FMC Object Managerを使用すると、現在のDynamic Object IPアドレスをダウンロードできます。

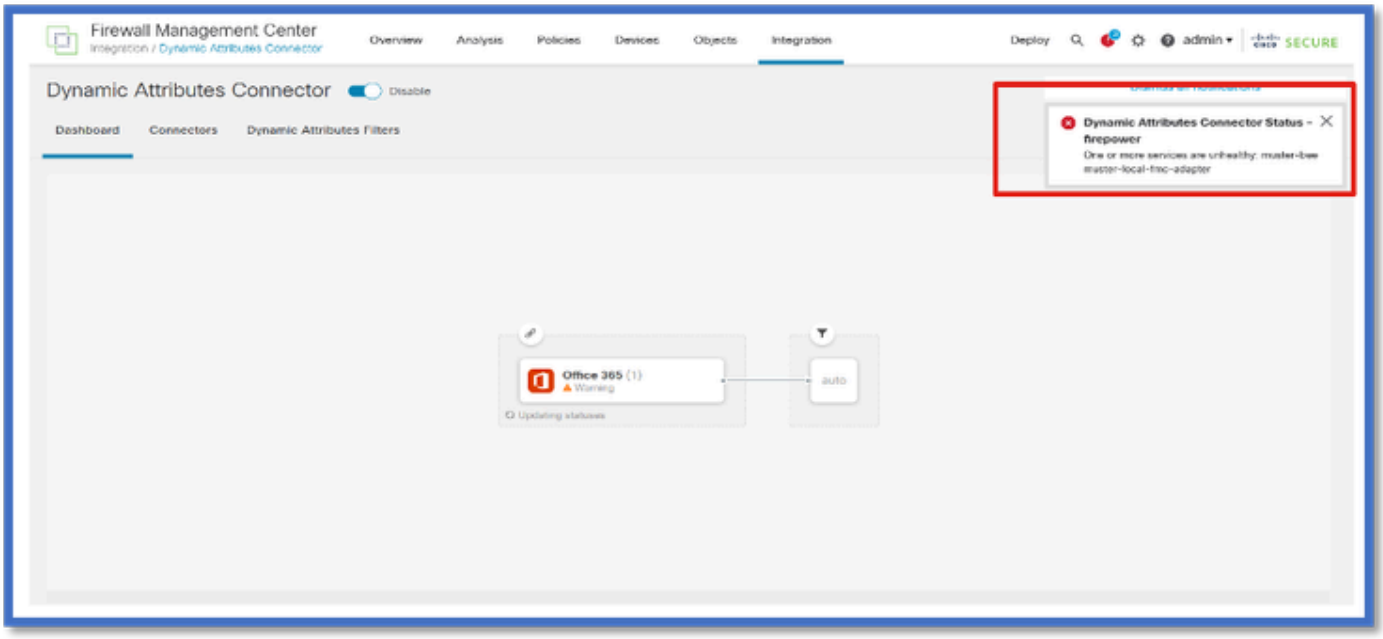


CSDACヘルスアラート

ダイナミック属性コネクタなどのコアサービスがダウンした場合、FMCのタスクマネージャにヘルスアラートが表示されます。 アラートには、サービス名とステータスに関する情報が含まれます。

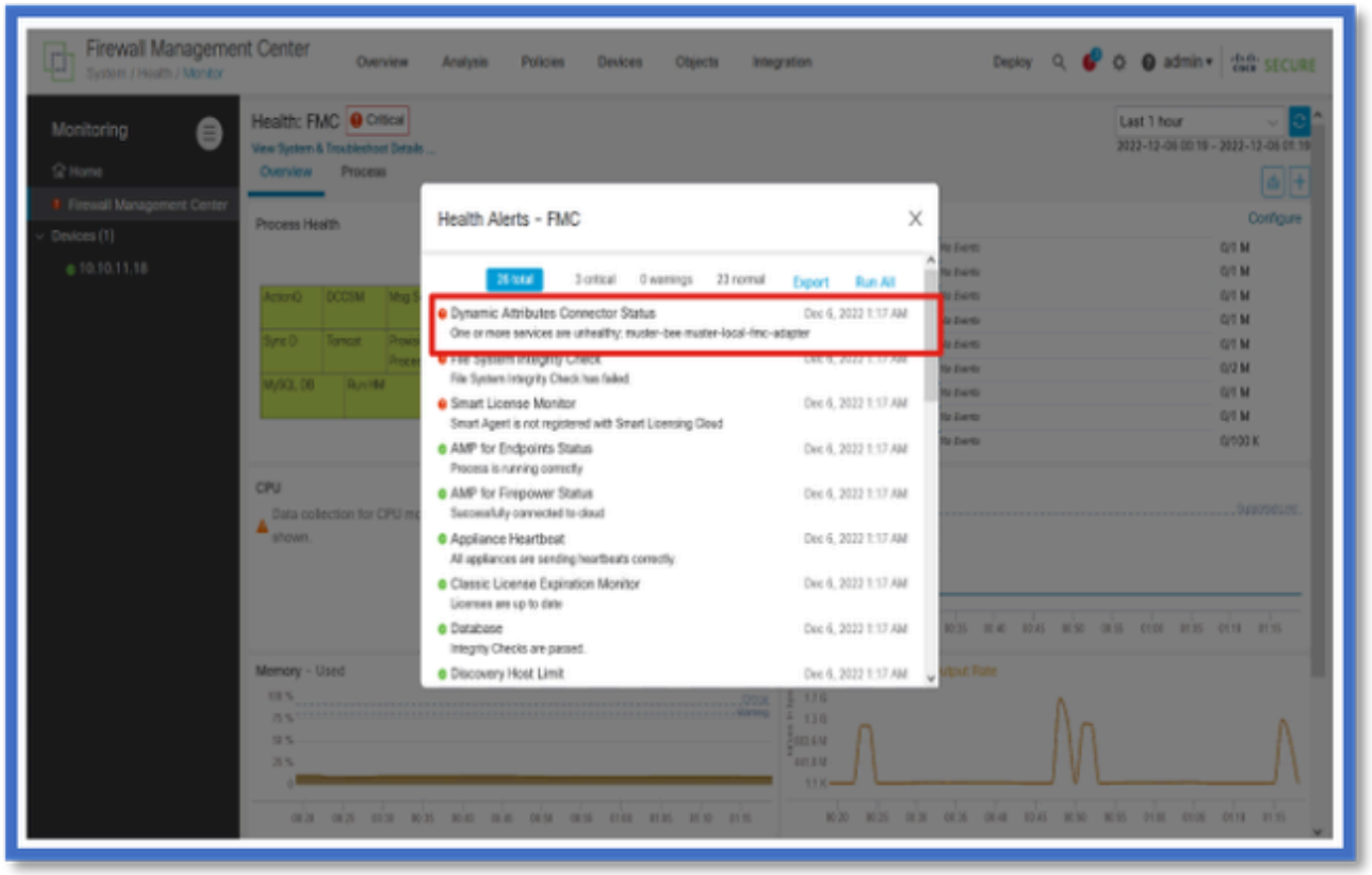


注：いくつかの通知には「マスター」という名前が残っています。ここでは、詳細情報を提供するサービス名を指定する必要があります。



ここでは、muster-beeとmuster-local-fmc-adapterが「異常」であることが確認できます。

errorがコアサービスのいずれかを示している場合は、デバッグ用にトラブルシューティングログを収集する必要があります。



トラブルシューティングのCSDAC

CSDACの生成のトラブルシューティング

- FMCのトラブルシューティングの生成中に、CSDACログが自動的に収集されます。バンドルには、Dockerのステータス、ログ、および問題をオフラインでデバッグするために必要なデータが含まれています。
- トラブルシューティングログが収集されるエラーを再現する前に、CSDACデバッグモードを有効にすることを推奨します（推奨）。

/usr/local/sf/csdacから。/mster-cli debug-onを呼び出します。

次のフォルダでuntarredのCSDACログを探し、Troubleshootします。

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

これには、etcdデータベースに保存されているデータが含まれます。

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

これには、Dockerコンテナからのログが含まれます。

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

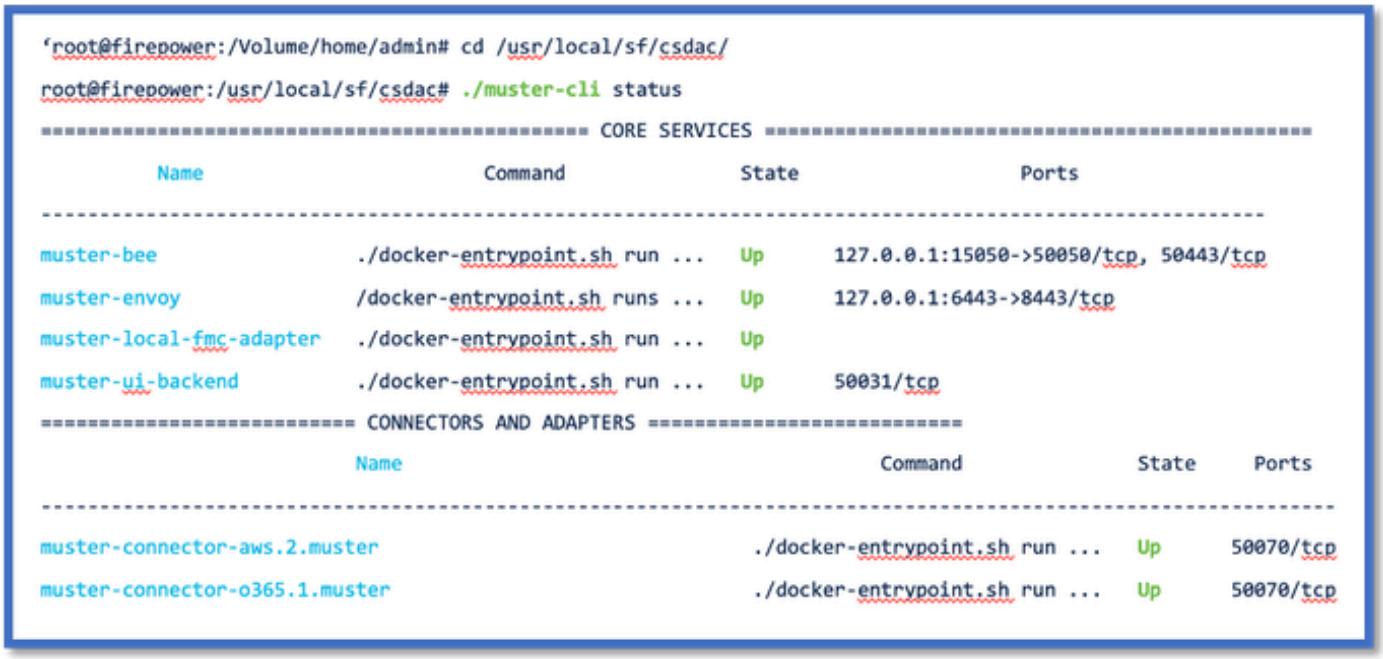
コンテナのステータス、バージョン、およびDockerイメージの詳細が表示されます。

CLIのトラブルシューティング

muster-cliスクリプトを使用して、FMC CLIからCSDACのステータスを確認できます。

サービスのステータスが「Exited」であるか、または「Up」と異なる場合は、まずそのコンテナのログをチェックします。

ログを取得するにはコンテナ名が必要です。出力から取得できます。



CSDACデバッグモード

デバッグログのオンとオフを切り替えるには、「muster-cli」スクリプトを使用できます。デフォルトでは、コンテナはINFO level.INFOに記録され、DEBUGのみがサポートされているレベルです。

デバッグレベルのユーザを有効にするには、./moster-cli debug-onを実行します。

これにより、トラブルシューティングの生成とデバッグのヘルプに関する詳細情報が提供されます。このオプションは、問題を再現するときに有効にする必要があります。

INFOレベルに戻るには、./muster-cli debug-offを使用します。

<#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
```

デバッグ付きログメッセージ

デバッグモードを有効にすると、すべてのDockerコンテナログにもデバッグメッセージが含まれます

dockerコマンドを使用してリアルタイムでログを取得する：docker logs -f <container_name>

次の例では、デバッグメッセージによってgRPCエラーがトリガーされたことが示されています

<#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
```

トラブルシューティングのウォークスルーの問題例

問題とトラブルシューティングの概要

問題：

発生する最も一般的な問題は、FMCがすべてのダイナミックオブジェクトマッピングを受信しないことです。

トラブルシューティング：

この問題をトラブルシューティングするために、

- 「muster-cli」からのデバッグモードの有効化
- FMC UIから生成されたトラブルシューティングファイル
- トラブルシューティングで収集したCSDAC AWS Connectorのログを確認。
- CSDAC AWS ConnectorがAWSインスタンスの最初のIPのみを照会したことが判明しました。

トラブルシューティングバンドルの準備

- FMCのCLIから、./moster-cli debug-onを使用してデバッグモードを有効にしました。muster-cliツールは、/usr/local/sf/csdacにあります。
- コネクタのステータスがOKになるのを待ってから、ダイナミックアトリビュートフィルタをチェックして、問題を再現。
- FMC UIからトラブルシューティングログを収集し、それらを抽出しました。スナップショットの内容についてAWS Connectorログを確認しました。

IPのタグ属性を確認します

特定のIPのタグ属性は、トラブルシューティングログに記録されます。AWS Connectorについては、muster-connector-aws.1.muster-docker.log.gzを参照しました。

チェックの概要

コネクタとアダプタのステータスは良好ですか。

　対応する「コネクタ」、「アダプタ」の各ページでステータスを確認します。

コネクタはすべてのマッピングを取得しましたか。

一致するIPアドレスのルールプレビューを確認します。

コネクタDockerログを調べて、マッピングを正しく照会しているかどうかを確認します。

RESTサーバはコネクタから動的なタグマッピングを受信しましたか。

FMCのダイナミックオブジェクトページをチェックします。

USMSログ(/opt/CSCOpx/MDC/log/operation/usmsharedsvcs.log内)をチェックして、FMC RESTサーバがCSDACからのAPI要求を正しく処理したかどうかを確認します。

Q&A

Q:ISEコネクタをサポートするオンプレミスCSDACのバージョンを教えてください。バージョン7.4.0（ビルド1494）でもそのようなコネクタは表示されません。

A：これはスタンドアロンCSDACであり、FMCまたはCDOにはありません。これをテストするには、CSDAC対応パッケージが必要です。

Q：リリース時のオンプレミスCSDACのバージョンを教えてください。

A：おそらく2.1.0。

Q:APIを重ねたギアの画面が表示されています。CSDACだと思いますが、これはどういう意味ですか。

A：このCSDACにはAPIエクスプローラが組み込まれているため、そのページからCSDACをAPI呼び出すことができます。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。