Dynamic Attributes Connector

次のトピックでは、Dynamic Attributes Connector を設定および使用する方法について説明します。

Dynamic Attributes Connector について

dynamic attributes connector を使用すると、アクセス コントロールポリシーが、パブリック クラウド ワークロード、プライベート クラウド ワークロードおよびビジネスに重要な Software as a Service（SaaS）アプリケーションの変更にリアルタイムで順応できるようになります。面倒な手動更新やポリシーのデプロイメントを行うことなく、ルールを最新の状態に保つことで、ポリシー管理が簡素化されます。お客様は、IP アドレスや VLAN が変更されてもファイアウォールポリシーが持続するように、VM 名やセキュリティグループなどの非ネットワーク構造に基づいてポリシールールを定義する必要があります。

サポートされるコネクタ

現在、次をサポートしています。

表 *1 : dynamic attributes connector* バージョンおよびプラットフォーム でサポートされているコネクタのリスト

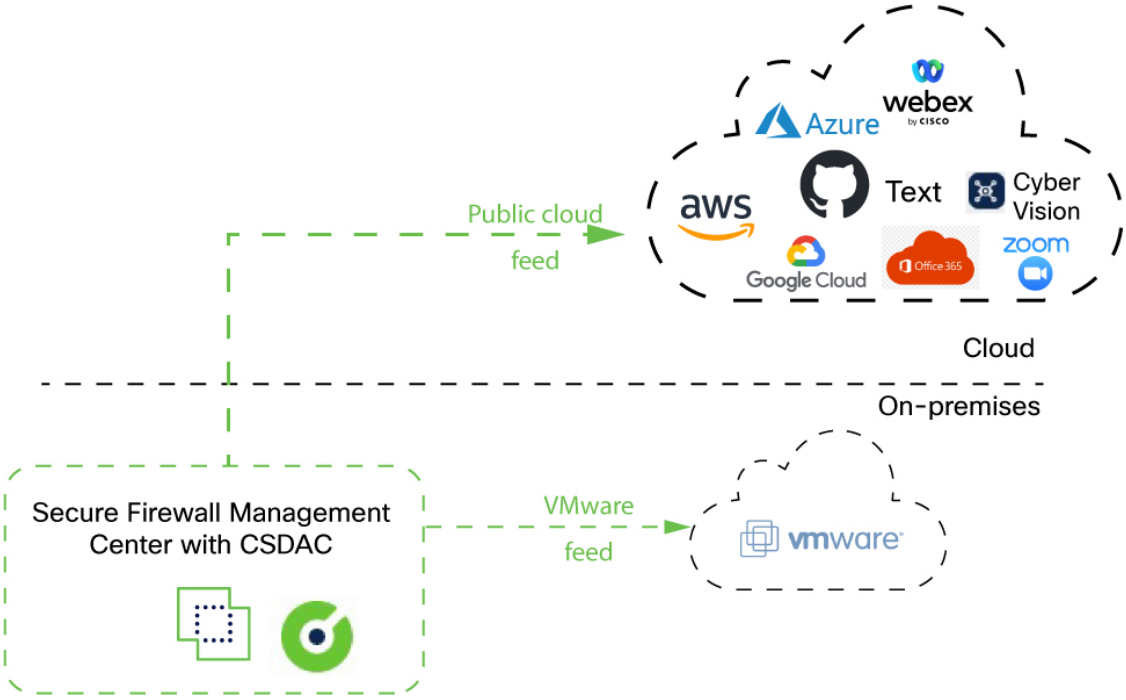
CSDAC バージョン	AWS	AWS セキュリティグループ	AWS サービスタグ	Azure	Azure サービスタグ	Cisco APIC	Cisco Cyber Vision	Cisco Multicl. Defense	汎用テキスト	GitHub	Google クラウド	Microsoft Office 365	Tenable	vCenter	Webex	Zoom
バージョン 1.1（オンプレミス）	はい	いいえ	非対応	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ	非対応	はい	いいえ	はい	いいえ	非対応
バージョン 2.0（オンプレミス）	はい	いいえ	非対応	はい	はい	いいえ	いいえ	いいえ	いいえ	非対応	はい	はい	いいえ	はい	いいえ	非対応
バージョン 2.2（オンプレミス）	はい	いいえ	非対応	はい	はい	いいえ	いいえ	いいえ	非対応	はい	はい	はい	いいえ	はい	いいえ	非対応
バージョン 2.3（オンプレミス）	はい	いいえ	非対応	はい	はい	いいえ	いいえ	いいえ	非対応	はい	はい	はい	いいえ	はい	はい	はい
バージョン 3.0（オンプレミス）	はい	はい	はい	はい	はい	いいえ	はい	いいえ	はい	はい	はい	はい	いいえ	はい	はい	はい
バージョン 3.1（オンプレミス）	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	いいえ	はい	はい	はい
クラウド提供型（Security Cloud Control）	はい	いいえ	非対応	はい	はい	いいえ	非対応	はい	いいえ	はい	はい	はい	はい	いいえ	いいえ	非対応
Secure Firewall Management Center 7.4.1	はい	いいえ	非対応	はい	はい	いいえ	いいえ	非対応	はい	はい	はい	はい	いいえ	はい	はい	はい
Secure Firewall Management Center 7.6	はい	はい	はい	はい	はい	いいえ	はい	いいえ	はい	はい	はい	はい	いいえ	はい	はい	はい
Secure Firewall Management Center 7.7	はい	はい	はい	はい	はい	いいえ	はい	いいえ	はい	はい	はい	はい	いいえ	はい	はい	はい

機能の仕組み

dynamic attributes connector を使用すると、アクセス コントロールポリシーが、パブリック クラウド ワークロード、プライベート クラウド ワークロードおよびビジネスに重要な Software as a Service（SaaS）アプリケーションの変更にリアルタイムで順応できるようになります。面倒な手動更新やポリシーのデプロイメントを行うことなく、ルールを最新の状態に保つことで、ポリシー管理が簡素化されます。お客様は、IP アドレスや VLAN が変更されてもファイ

アウォールポリシーが持続するように、VM名やセキュリティグループなどの非ネットワーク構造に基づいてポリシールールを定義する必要があります。

次の図は、システムが高レベルでどのように機能するかを示しています。



- システムは、特定のパブリック クラウド プロバイダーをサポートします。

  このトピックでは、サポートされているコネクタ（これらのプロバイダーへの接続）について説明します。

- dynamic attributes connector は Secure Firewall Management Centerとともに提供されます。

関連項目

- dynamic attributes connector の有効化 （5 ページ）
- ダッシュボードについて （8 ページ）

Dynamic Attributes Connector の履歴

機能	Minimum Firewall Management Center	Minimum Firewall Threat Defense	詳細
新しいコネクタ	7.6	7.6	AWS セキュリティグループ、AWS サービスタグ、および Cisco Cyber Vision これらのコネクタは、Security Cloud Control と同様に、オンプレミスの Secure Firewall Management Center ダイナミックオブジェクトを送信できます。 オンプレミスの dynamic attributes connector からダイナミックオブジェクトを受信するには、オンプレミスのダイナミック属性コネクタのバージョン 3.0 が必要です。
Dynamic Attributes Connector	7.4.0	7.4.0	この機能が導入されます。 Dynamic Attributes Connector が Secure Firewall Management Center に含まれるようになりました。dynamic attributes connector を使用すると、管理対象デバイスに展開することなく、アクセス制御ルールでMicrosoft Azure などのクラウドベースのプラットフォームから IP アドレスを取得できます。 詳細情報： • この製品に含まれる dynamic attributes connector：Dynamic Attributes Connector について （1 ページ） • スタンドアロン dynamic attributes connector：*Cisco Secure Dynamic Attributes Connector Configuration Guide* 新規/変更された画面：**Integration** > **Dynamic Attributes Connector**

Dynamic Attributes Connector のシステム要件

Dynamic Attributes Connector には、以下のメモリ要件があります。

FMCv：RAM の容量	Secure Firewall Management Center ハードウェアモデル	最大数（コネクタ + Azure AD レルム）
32 GB 以上	Firepower 1000、Firepower 1600、vFMC	10
64 GB 以上	Firepower 2500、Firepower 2600、vFMC 300	20
128 GB 以上	Firepower 4500、Firepower 4600	30

上記の制限は、仮想マシンと物理マシンの両方に適用されます。

展開の問題が発生する可能性があるため、システムによって前述の制限を超えることが阻止されます。

dynamic attributes connector の有効化

このタスクでは、Secure Firewall Management Center で Dynamic Attributes Connector を有効にする方法について説明します。dynamic attributes connectorは、クラウドネットワーキング製品のオブジェクトを Firewall Management Center のアクセス制御 のルールで使用できるようにする統合です。

手順

ステップ 1 Secure Firewall Management Center にログインしていない場合は、ログインします。

ステップ 2 **Integration** > **Dynamic Attributes Connector** をクリックします。

ステップ 3 [有効（Enabled）] にスライドします。

ステップ 4 dynamic attributes connector が有効になっている間、メッセージが表示されます。

エラーが発生した場合は、再試行してください。エラーが続く場合には、Cisco TAC に連絡してください。

Docker コンテナのネットワークとサブネットの設定

Dynamic Attributes Connector は、Docker コンテナを使用して Secure Firewall Management Center 内のコネクタデータを取得します。Secure Firewall Management Center 管理インターフェイスおよびネットワークで使用されているその他の IP アドレスとの競合を回避するために、このセクションで説明されているコマンドを使用して、Docker IP アドレスと範囲を変更することもできます。

Docker ネットワークについて

dynamic attributes connector で使用される Docker デーモンには、次のネットワークが必要です。

- Docker デーモンによって内部で使用される `docker0`。
- `veth`*`number`* という名前の一連の IPv6 ネットワーク。

  これらは、dynamic attributes connector によって使用される内部ブリッジネットワークです。
- `br-`*`number`* という名前の dynamic attributes connector コネクタで使用される Docker ブリッジネットワーク。

dynamic attributes connectorを有効にする前は、172.18.0.1/16 に設定された `docker0` という名前の Docker インターフェイスが 1 つだけあります（Secure Firewall Management Center Virtualの場合。オンプレミスのマネージャは異なる IP アドレス範囲を使用します）。詳細については、「例」セクションの表を参照してください。

Docker ネットワークとサブネットの変更

まず dynamic attributes connector を有効にします（dynamic attributes connector の有効化 （5 ページ）を参照）。

Docker ネットワークとサブネットを変更するには、ルート権限を持つユーザーとして `/usr/local/sf/bin/change_docker_subnet.sh -b CIDR-network -s address-pool-size` を実行します。

- `-b CIDR-network` は、CIDR 表記でネットワーク ベース アドレス プールを設定します。
- `-s address-pool-size` は、ネットワークベースアドレスのネットマスクを設定します。このオプションを使用して、ネットワーク範囲が既存のネットワーク範囲と重複する場合に、ベースアドレス範囲内のアドレス数を制限できます。特に、Secure Firewall Management Center モデルには特定の `-s` 値を使用して、マシンで利用可能な RAM を超えないようにすることをお勧めします（Docker コンテナは dynamic attributes connector コネクタで使用され、それらの制限は Dynamic Attributes Connector のシステム要件 （4 ページ）に示されています）。

重要 Docker に割り当てるネットワークは、内部ネットワークの範囲内にある必要があり、Secure Firewall Management Center または内部ネットワーク内の他のデバイスで使用されるネットワークと競合しないようにする必要があります。

例

次の表に例を示します。

Secure Firewall Management Center モデル	推奨される -s 値	-b 値の例	使用される Dynamic Attributes Connector コンテナアドレス
Firepower 1000、Firepower 1600、vFMC	27（ネットマスク 255.255.255.224）	172.19.0.0/16	30 個の IP アドレス `docker0`：172.19.0.1 ブリッジネットワークの `br-` 番号ゲートウェイ `172.19.0.33` とサブネット `172.19.0.32/27` `172.19.0.38/27`、`172.19.0.39/27` などのネットワークで作成されたコネクタ

Secure Firewall Management Center モデル	推奨される -s 値	-b 値の例	使用される Dynamic Attributes Connector コンテナアドレス
Firepower 2500、Firepower 2600、vFMC 300	26 （ネットマスク 255.255.255.192）	192.168.0.0/16	62 個の IP アドレス `docker0`：192.168.1.1 ブリッジネットワークの `br-` 番号ゲートウェイ `192.168.1.65` とサブネット `192.168.1.64/26` `192.168.1.71/26`、`192.168.1.72/26` などのネットワークで作成されたコネクタ
Firepower 4500、Firepower 4600	25 （ネットマスク 255.255.255.128）	192.168.0.0/16	126 個の IP アドレス `docker0`：192.168.1.1 ブリッジネットワーク `br-` 番号ゲートウェイ `192.168.1.129` とサブネット `192.168.1.128/25` `192.168.1.136/25`、`192.168.1.135/25` などのネットワークで作成されたコネクタ

完全なコマンドは以下のとおりです。

```
sudo /usr/local/sf/bin/change_docker_subnet.sh -b 172.19.0.0/16 -s 27
sudo /usr/local/sf/bin/change_docker_subnet.sh -b 192.168.0.0/16 -s 26
sudo /usr/local/sf/bin/change_docker_subnet.sh -b 192.168.0.0/16 -s 25
```

ネットワークの確認

ネットワーク設定を確認するには、`sudo docker network inspect muster-net` と入力します。コマンドの結果は JSON 形式で表示されます。

トラブルシューティング

以下に、このコマンドを使用して発生する可能性のある一般的なエラーの解決策の一部を示します。

エラー：**プルサブネット値はサイズより大きくすることはできません**

解決策：`-s` の値を変更して、CIDR ネットワーク値よりも小さくします。

次に例を示します。

誤：`sudo /usr/local/sf/bin/change_docker_subnet.sh -b 172.19.0.0/16 -s8`

正：`sudo /usr/local/sf/bin/change_docker_subnet.sh -b172.19.0.0/16-s 20`

エラー：**コマンドの実行後、Docker ネットワークが正しくありません。**

解決策：Docker デーモンを再起動します：`sudo pmtool restartbyid docker`

エラー：`unix:///var/run/docker.sock の Docker デーモンに接続できません。Docker デーモンは実行されていますか？`

解決策：Docker を再起動します：`pmtool restartbyid docker`

エラー：**入力を空にすることはできません**

`-s` パラメータは必須です。

エラー：**プルサイズ - 32（32 よりも大きくするか、0 未満にすることはできません）**

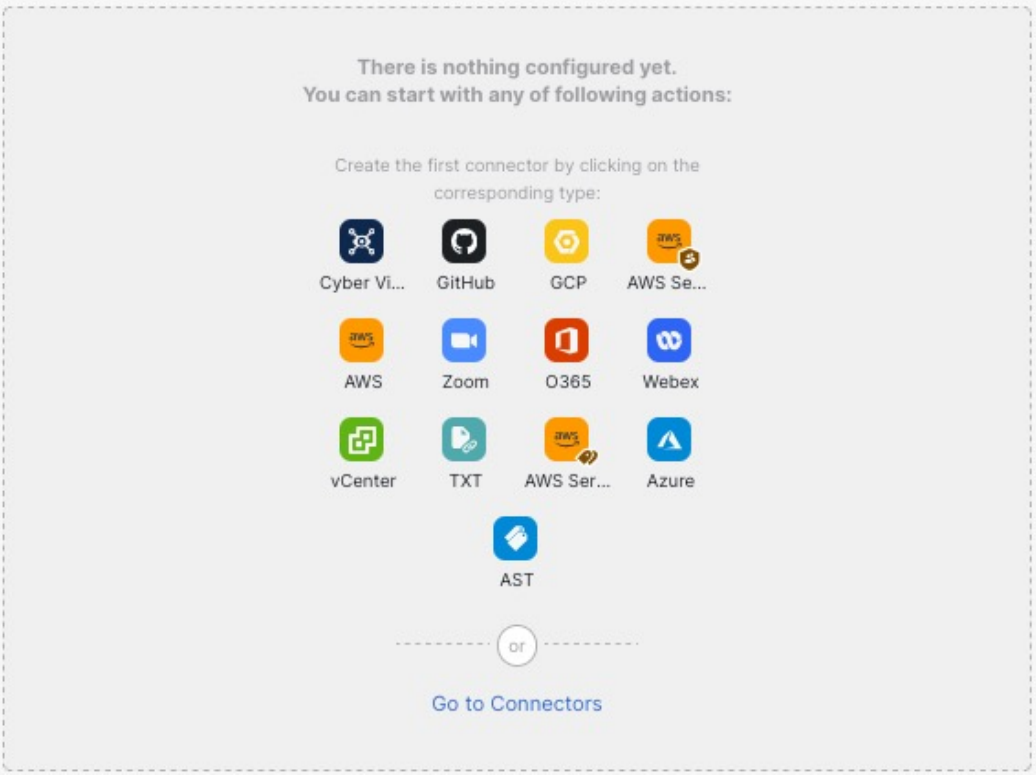
解決策：`-s` の値を変更して、0 より大きく、かつ 32 未満になるようにします。

ダッシュボードについて

dynamic attributes connector ダッシュボードにアクセスするには、Cisco Secure Firewall Manager にログインし、ページの上部にある [**Integration** > **Dynamic Attributes Connector**] をクリックします

dynamic attributes connector が有効になっていない場合は、スライダを動かして有効にします。このプロセスの完了には数分かかる場合があります。

dynamic attributes connector ダッシュボードページには、コネクタ、アダプタ、およびフィルタの状態が一目でわかるように表示されます。以下に、未設定のシステムのダッシュボードの例を示します。



ダッシュボードでできることは以下のとおりです。

- コネクタ動的属性フィルタ、およびを追加、編集、および削除します。

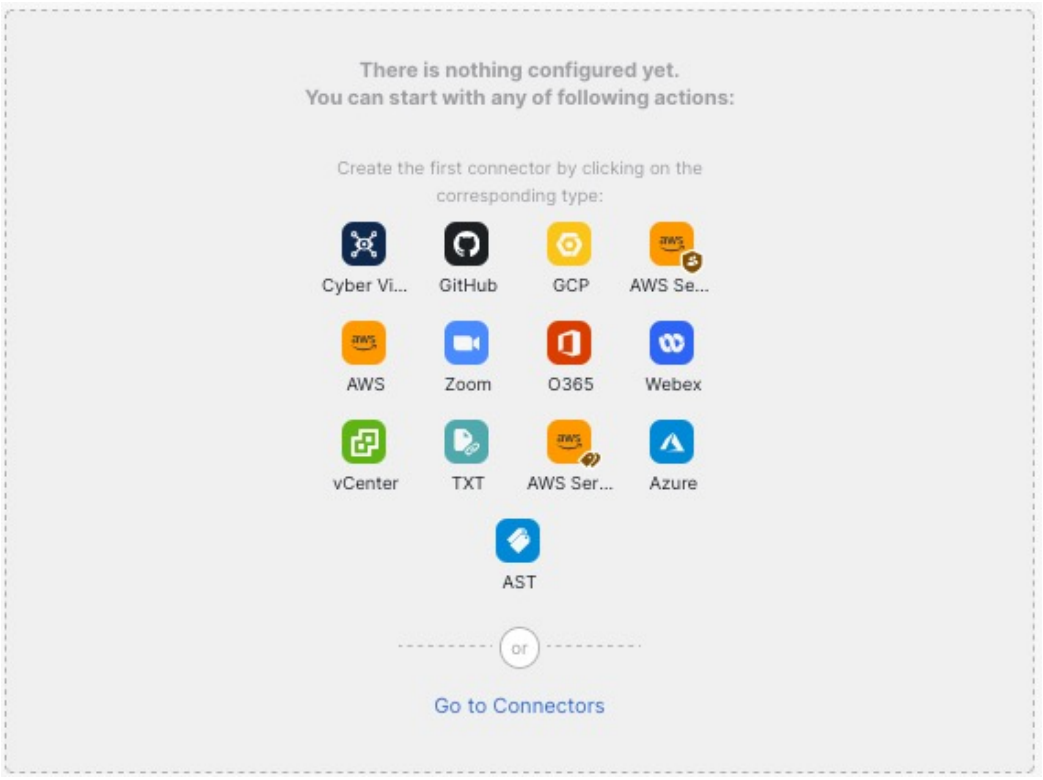
- コネクタ動的属性フィルタ 、 および の相互関係を確認します。
- 警告およびエラーを表示します。

関連項目

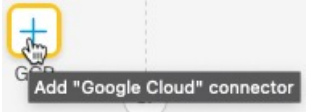
- 構成されていないシステムのダッシュボード （9 ページ）
- 構成済みシステムのダッシュボード （10 ページ）
- コネクタを追加、編集、削除する （11 ページ）
- ダイナミック属性フィルタを追加、編集または削除する （13 ページ）

構成されていないシステムのダッシュボード

設定されていないシステムの dynamic attributes connector ダッシュボードページの例



[ダッシュボード（Dashboard）]には、システムに設定できるすべてのタイプのコネクタが最初に表示されます次のいずれかの操作を実行できます。

- コネクタの上にマウスポインタを合わせ、 

をクリックして新しいアダプタを作成します。

- [コネクタに移動（Go to Connectors）] をクリックして、コネクタを追加、編集、または削除します（複数のコネクタを同時に作成、編集、または削除する場合に適しています）。

  詳細については、「コネクタを作成する （15 ページ）」を参照してください。

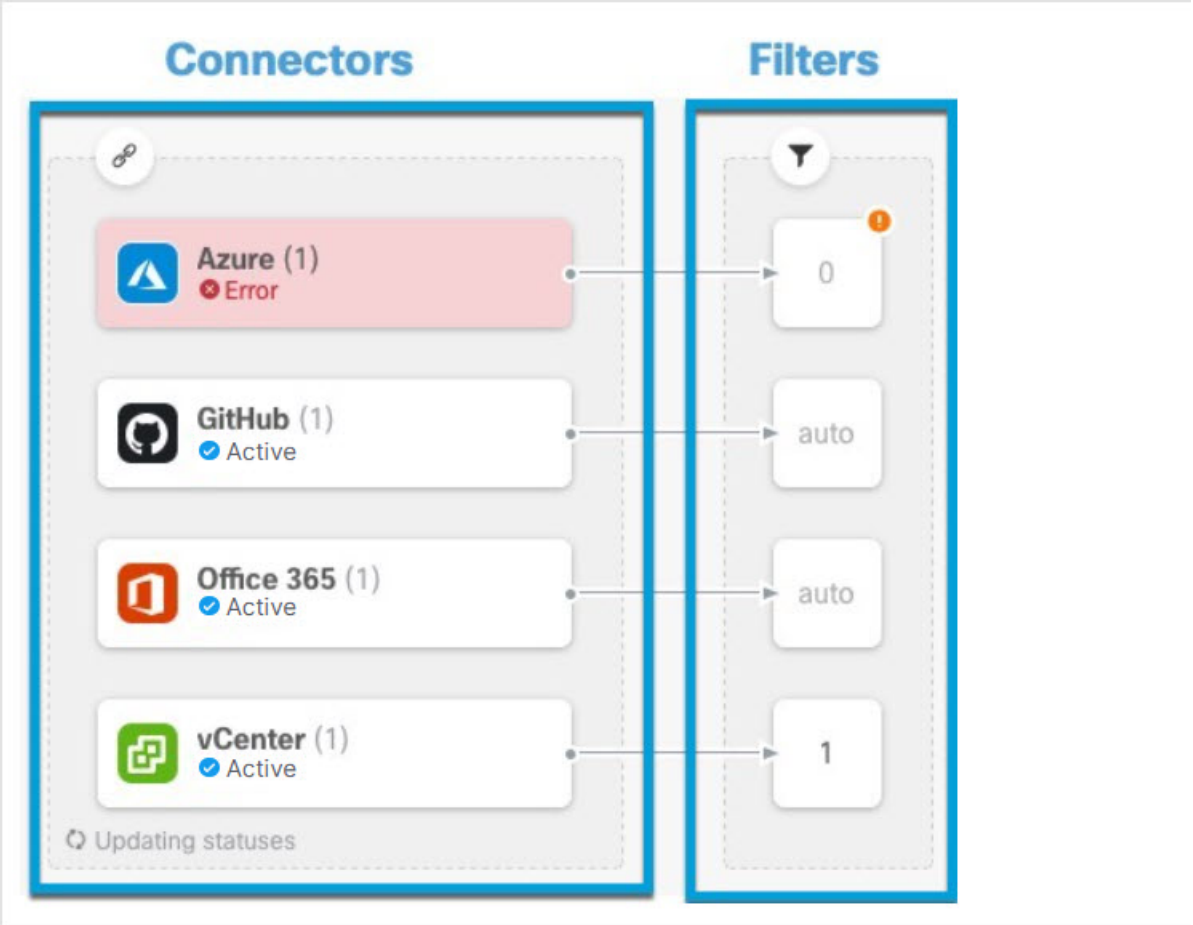
関連トピック：

- 構成済みシステムのダッシュボード （10 ページ）
- コネクタを追加、編集、削除する （11 ページ）
- ダイナミック属性フィルタを追加、編集または削除する （13 ページ）

構成済みシステムのダッシュボード

設定済みシステムの dynamic attributes connector ダッシュボードページの例：

図の任意のエリアをクリックして詳細を確認するか、図の下のリンクのいずれかをクリックしてください。



1 コネクタを作成する （15 ページ）

2 ダイナミック属性フィルタを作成する （43 ページ）

ダッシュボードには、次が示されます（左から右）。

コネクタ列	フィルタ列
構成されている各タイプの数を示す数値付きのコネクタのリスト。コネクタは、Cisco Secure Firewall Manager に送信できる動的属性を収集します。動的属性フィルタは、送信されるデータを指定します。 設定済みのすべてのコネクタの詳細を表示するには、 をクリックします。コネクタの名前をクリックして、コネクタを追加、編集、または削除するか、それらに関する詳細情報を表示できます。詳細については、コネクタを追加、編集、削除する （11 ページ）を参照してください。	コネクタに関連付けられている各フィルタの数を示す数値と、各コネクタに関連付けられた動的属性フィルタのリスト。 設定済みのすべてのフィルタの詳細を表示するには、 をクリックします。フィルタの名前をクリックして、フィルタを追加、編集、または削除するか、それらに関する詳細情報を表示できます。詳細については、「ダイナミック属性フィルタを追加、編集または削除する （13 ページ）」を参照してください。

（注） Outlook 365 や Azure サービスタグなどの一部のコネクタは、動的属性フィルタを必要とせずに、使用可能なダイナミックオブジェクトを自動的にプルします。これらのコネクタは、 列に [自動（Auto）] と表示されます。

ダッシュボードは、オブジェクトが利用可能かどうかを示します。[ダッシュボード（Dashboard）] ページは 15 秒ごとに更新されますが、ページの上部にある **Refresh** ( ) をクリックすると、いつでもすぐに更新できます問題が解決しない場合は、ネットワーク接続を確認してください。

関連トピック：

- コネクタを追加、編集、削除する （11 ページ）
- ダイナミック属性フィルタを追加、編集または削除する （13 ページ）

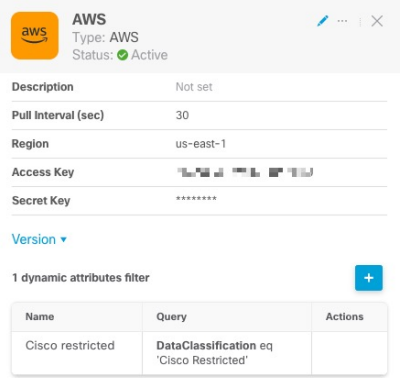
コネクタを追加、編集、削除する

ダッシュボードでは、コネクタを表示または編集できます。コネクタの名前をクリックしてそのコネクタのすべてのインスタンスを表示するか、 をクリックして次の追加オプションを選択できます。

- すべてのコネクタを同時に表示するには、[コネクタに移動（Go to Connectors）] を選択します。そこからコネクタを追加、編集、削除できます。

- **[コネクタタイプ > の追加（Add Connector type）]** をクリックして、指定したタイプのコネクタを追加します。

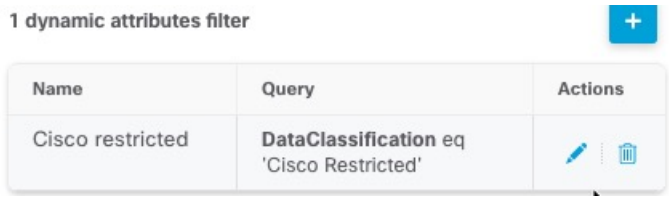
コネクタ列のコネクタ（ ）をクリックすると、そのコネクタに関する詳細情報が表示されます。以下に例を示します。



次の選択肢があります。

- Edit icon ( ) をクリックしてこのコネクタを編集する。
- More icon ( ) をクリックして追加のオプションを表示する。
- をクリックしてパネルを閉じる。
- [バージョン（Version）] をクリックしてバージョンを表示する。Cisco TAC で使用するために、必要に応じてバージョンをクリップボードにコピーできます。

パネルの下部にあるテーブルでは、動的属性フィルタを追加できます。または、コネクタを編集または dynamic attributes connector 削除できます。以下に例を示します。



Add icon ( ) をクリックして、このコネクタの動的属性フィルタを追加します。詳細については、「ダイナミック属性フィルタを作成する （43 ページ）」を参照してください。

指定されたコネクタを編集または削除するには、[アクション（Actions）] 列にマウスポインタを合わせます。

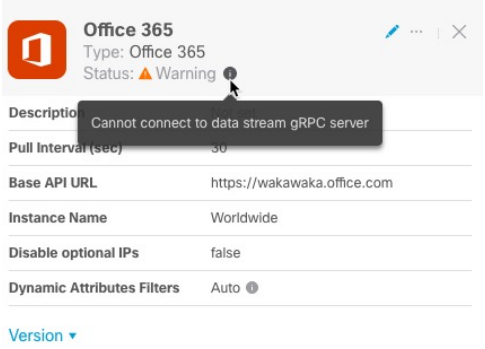
エラー情報の表示

コネクタのエラー情報を表示するには、以下の手順を実行します。

1. ダッシュボードで、エラーを表示しているコネクタの名前をクリックします。

2. 右側のペインで **Information** ( ) をクリックします。

   次に例を示します。



3. この問題を解決するには、Office 365 コネクタを作成する （35 ページ） の説明に従ってコネクタ設定を編集します。
4. 問題を解決できない場合は、[バージョン（Version）] をクリックし、バージョンをテキストファイルにコピーします。
5. このすべての情報を Cisco TAC に提供します。

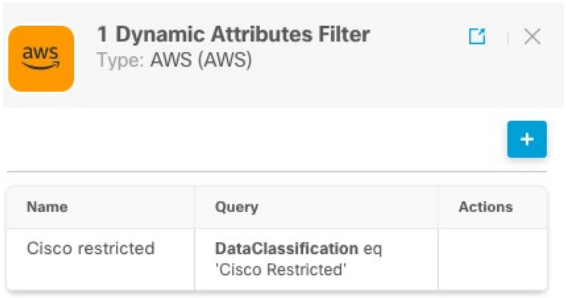
ダイナミック属性フィルタを追加、編集または削除する

ダッシュボードでは、ダイナミック属性フィルタを追加、編集または削除できます。フィルタの名前をクリックしてそのフィルタのすべてのインスタンスを表示するか、 をクリックして以下の追加オプションを選択できます。

- 設定されているすべての動的属性フィルタを表示するには、[動的属性フィルタ（Dynamic Attributes Filters）] に移動し ます。そこから動的属性フィルタを追加、編集、または削除できます。
- [動的属性フィルタの追加（Add Dynamic Attributes Filters）] をクリックしてフィルタを追加します。

動的属性フィルタの追加の詳細については、ダイナミック属性フィルタを作成する （43 ページ） を参照してください。

次に例を示します。



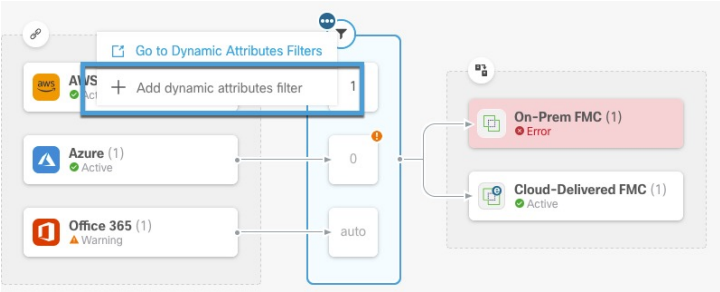
（注） Outlook 365 や Azure サービスタグなどの一部のコネクタは、動的属性フィルタを必要とせずに、使用可能なダイナミックオブジェクトを自動的にプルします。これらのコネクタは、 列に [自動（Auto）] と表示されます。

次の選択肢があります。

- フィルタインスタンスをクリックすると、コネクタに関連付けられている動的属性フィルタに関する概要情報が表示されます。
- Add icon ( ) をクリックして、新しい動的属性フィルタを追加します。

  詳細については、「ダイナミック属性フィルタを作成する （43 ページ）」を参照してください。
- フィルタ列（ ）の をクリックします。これは、指定されたコネクタに動的属性フィルタが関連付けられていないことを示します。関連付けられたフィルタがない場合、コネクタは Firewall Management Center に何も送信できません。

  この問題を解決する方法の 1 つは、フィルタ列の をクリックし、[動的属性フィルタの追加（Add Dynamic Attributes Filter）] をクリックすることです。次に例を示します。



- をクリックして、フィルタを追加、編集、または削除する。
- をクリックしてパネルを閉じる。

コネクタを作成する

コネクタは、クラウドサービスでのインターフェイスです。コネクタは、クラウドサービスからネットワーク情報を取得するので、Secure Firewall Management Center のポリシーでネットワーク情報を使用できます。

次がサポートされています。

表 *2 : dynamic attributes connector* バージョンおよびプラットフォーム でサポートされているコネクタのリスト

CSDAC バージョン	AWS	AWS セキュリティグループ	AWS サービスタグ	Azure	Azure サービスタグ	Cisco APIC	Cisco Cyber Vision	Cisco Multicl. Defense	汎用テキスト	GitHub	Google クラウド	Microsoft Office 365	Tenable	vCenter	Webex	Zoom
バージョン 1.1（オンプレミス）	はい	いいえ	非対応	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ	非対応	はい	いいえ	はい	いいえ	非対応
バージョン 2.0（オンプレミス）	はい	いいえ	非対応	はい	はい	いいえ	いいえ	いいえ	いいえ	非対応	はい	はい	いいえ	はい	いいえ	非対応
バージョン 2.2（オンプレミス）	はい	いいえ	非対応	はい	はい	いいえ	いいえ	いいえ	非対応	はい	はい	はい	いいえ	はい	いいえ	非対応
バージョン 2.3（オンプレミス）	はい	いいえ	非対応	はい	はい	いいえ	いいえ	いいえ	非対応	はい	はい	はい	いいえ	はい	はい	はい
バージョン 3.0（オンプレミス）	はい	はい	はい	はい	はい	いいえ	はい	いいえ	はい	はい	はい	はい	いいえ	はい	はい	はい
バージョン 3.1（オンプレミス）	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	いいえ	はい	はい	はい
クラウド提供型（Security Cloud Control）	はい	いいえ	非対応	はい	はい	いいえ	非対応	はい	いいえ	はい	はい	はい	はい	いいえ	いいえ	非対応
Secure Firewall Management Center 7.4.1	はい	いいえ	非対応	はい	はい	いいえ	いいえ	非対応	はい	はい	はい	はい	いいえ	はい	はい	はい
Secure Firewall Management Center 7.6	はい	はい	はい	はい	はい	いいえ	はい	いいえ	はい	はい	はい	はい	いいえ	はい	はい	はい
Secure Firewall Management Center 7.7	はい	はい	はい	はい	はい	いいえ	はい	いいえ	はい	はい	はい	はい	いいえ	はい	はい	はい

Amazon Web Services コネクタ：ユーザー権限とインポートされたデータについて

dynamic attributes connector は、ポリシーで使用するために AWS から Secure Firewall Management Center へ動的属性をインポートします。

インポートされた動的属性

AWS から次の動的属性をインポートします。

- タグ：AWS EC2 リソースを整理するために使用できるユーザー定義のキーと値のペア。

  詳細については、AWS ドキュメントの「Tag your EC2 Resources」を参照してください

- AWS 内の仮想マシンの *IP* アドレス。

必要な最小限の権限

dynamic attributes connector には、少なくとも、`ec2:DescribeTags`、`ec2:DescribeVpcs`、および `ec2:DescribeInstances` に動的属性のインポートを許可するポリシーを持つユーザーが必要です。

dynamic attributes connector に対して最小限の権限を持つ AWS ユーザーを作成します。

このタスクでは、動的属性を Secure Firewall Management Center に送信するための最小限の権限を持つサービスアカウントを設定する方法について説明します。これらの属性のリストについては、Amazon Web Services コネクタ：ユーザー権限とインポートされたデータについて （16 ページ）を参照してください。

始める前に

Amazon Web Services（AWS）アカウントがすでに設定されている必要があります。これを行う方法の詳細については、AWS ドキュメントのこの記事を参照してください。

手順

ステップ 1 管理者ロールを持つユーザーとして AWS コンソールにログインします。

ステップ 2 ダッシュボードから、**[セキュリティ、アイデンティティおよび遵守（Security, Identity & Compliance）]** > **[IAM]**をクリックします。

ステップ 3 **[アクセス管理（Access Management）]** > **[ユーザー（Users）]**をクリックします。

ステップ 4 [ユーザの追加（Add Users）] をクリックします。

ステップ 5 [ユーザー名（User Name）] フィールドに、ユーザーを識別するための名前を入力します。

ステップ 6 [アクセスキー - プログラムによるアクセス（Access Key - Programmatic Access）] をクリックします。

ステップ 7 [権限の設定（Set permissions）]ページで、ユーザーに何もアクセスを許可せずに**[次へ（Next）]**をクリックします。後からユーザーにアクセス権を付与できます。

ステップ 8 必要に応じて、ユーザーにタグを追加します。

ステップ 9 [ユーザーの作成（Create User）] をクリックします。

ステップ 10 [.csvをダウンロード（Download.csv）]をクリックして、ユーザーのキーをコンピューターにダウンロードします。

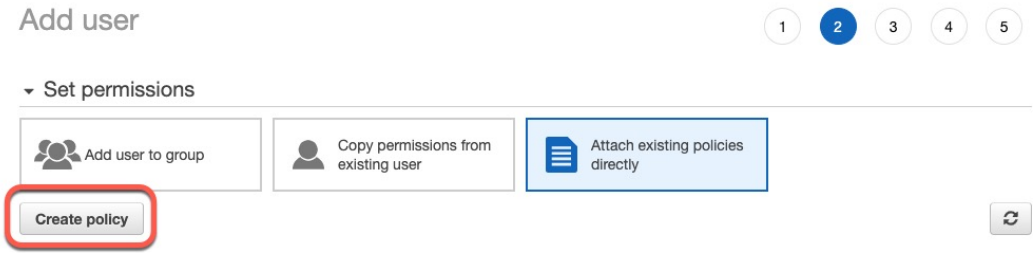
（注）
これが、ユーザーのキーを取得する必要がある唯一の機会です。

ステップ 11 [閉じる（Close）] をクリックします。

ステップ 12 左側の列の[アイデンティティとアクセス管理（IAM）（Identity and Access Management (IAM)）]ページで、**[アクセス管理（Access Management）]**>**[ポリシー（Policies）]**をクリックします。

ステップ 13 [ポリシーの作成（Create Policy）] をクリックします。

ステップ 14 [ポリシーの作成（Create Policy）] ページで、[JSON] をクリックします。



ステップ 15 フィールドに次のポリシーを入力します。

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "ec2:DescribeTags",
    "ec2:DescribeInstances",
    "ec2:DescribeVpcs"
   ],
   "Resource": "*"
  }
 ]
}
```

ステップ 16 [次へ（Next）] をクリックします。

ステップ 17 [レビュー（Review）] をクリックします。

ステップ 18 [ポリシーの確認（Review Policy）] ページで、必要な情報を入力し、[ポリシーの作成（Create Policy）] をクリックします。

ステップ 19 [ポリシー（Policies）]ページで、検索フィールドにポリシー名のすべてまたは一部を入力し、Enter キーを押します。

ステップ 20 作成したポリシーをクリックします。

ステップ 21 **[アクション（Actions）]**>**[アタッチ（Attach）]**をクリックします。

ステップ 22 必要に応じて、検索フィールドにユーザー名の全部または一部を入力し、Enter キーを押します。

ステップ 23 [ポリシーをアタッチ（Attach policy）] をクリックします。

次のタスク

AWS コネクタの作成 （18 ページ）。

AWS コネクタの作成

このタスクでは、ポリシーで使用するため、AWS から Secure Firewall Management Center にデータを送信するコネクタを構成する方法について説明します。

始める前に

dynamic attributes connector に対して最小限の権限を持つ AWS ユーザーを作成します。 （16 ページ） で説明した権限以上のユーザーを作成します。

手順

ステップ 1 Secure Firewall Management Center にログインします。

ステップ 2 **Integration** > **Dynamic Attributes Connector** > **Connectors** をクリックします。

ステップ 3 次のいずれかを実行します。

- 新しいコネクタの追加：Add icon ( ) をクリックしてから、コネクタの名前をクリックします。
- コネクタの編集または削除：**More** ( ) をクリックしてから、行の末尾にある [編集（Edit）] または [削除（Delete）] をクリックします。

ステップ 4 次の情報を入力します。

値	説明
名前（Name）	（必須）このコネクタを一意に識別する名前を入力します。
説明（Description）	説明（オプション）。
プル間隔（Pull Interval）	（デフォルトは 30 秒）AWS から IP マッピングを取得する間隔です。
リージョン（Region）	（必須）AWS リージョンコードを入力します。
アクセスキー（Access Key）	（必須）アクセスキーを入力します。
秘密キー（Secret Key）	（必須）秘密鍵を入力します。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 [ステータス（Status）] 列に [OK] が表示されていることを確認します。

Amazon Web Services セキュリティ グループ コネクタ：ユーザー権限

dynamic attributes connector は、ポリシーで使用するために AWS から Secure Firewall Management Center へ動的属性をインポートします。

必要な最小限の権限

dynamic attributes connector には、少なくとも、`ec2:DescribeTags`、`ec2:DescribeVpcs`、および `ec2:DescribeInstances` に動的属性のインポートを許可するポリシーを持つユーザーが必要です。

dynamic attributes connector に対して最小限の権限を持つ AWS ユーザーを作成します。

このタスクでは、動的属性を Secure Firewall Management Center に送信するための最小限の権限を持つサービスアカウントを設定する方法について説明します。これらの属性のリストについては、Amazon Web Services コネクタ：ユーザー権限とインポートされたデータについて （16 ページ）を参照してください。

始める前に

Amazon Web Services（AWS）アカウントがすでに設定されている必要があります。これを行う方法の詳細については、AWS ドキュメントのこの記事を参照してください。

手順

ステップ 1 管理者ロールを持つユーザーとして AWS コンソールにログインします。

ステップ 2 ダッシュボードから、**[セキュリティ、アイデンティティおよび遵守（Security, Identity & Compliance）] > [IAM]**をクリックします。

ステップ 3 **[アクセス管理（Access Management）] > [ユーザー（Users）]**をクリックします。

ステップ 4 [ユーザの追加（Add Users）] をクリックします。

ステップ 5 [ユーザー名（User Name）] フィールドに、ユーザーを識別するための名前を入力します。

ステップ 6 [アクセスキー - プログラムによるアクセス（Access Key - Programmatic Access）] をクリックします。

ステップ 7 [権限の設定（Set permissions）] ページで、ユーザーに何もアクセスを許可せずに**[次へ（Next）]** をクリックします。後からユーザーにアクセス権を付与できます。

ステップ 8 必要に応じて、ユーザーにタグを追加します。

ステップ 9 [ユーザーの作成（Create User）] をクリックします。

ステップ 10 [.csvをダウンロード（Download.csv）] をクリックして、ユーザーのキーをコンピューターにダウンロードします。

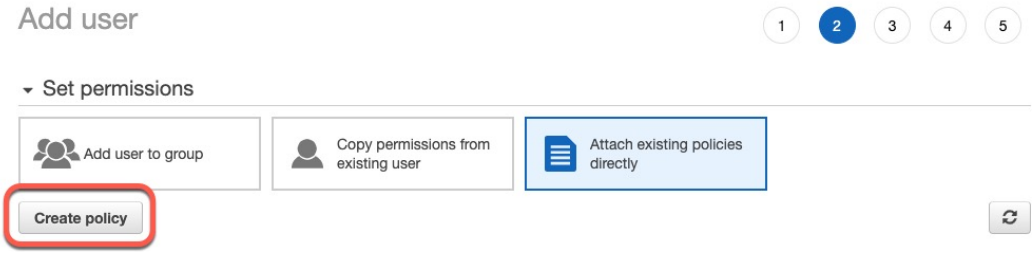
（注）
これが、ユーザーのキーを取得する必要がある唯一の機会です。

ステップ 11 [閉じる（Close）] をクリックします。

ステップ 12 左側の列の [アイデンティティとアクセス管理（IAM）（Identity and Access Management (IAM)）] ページで、**[アクセス管理（Access Management）] > [ポリシー（Policies）]**をクリックします。

ステップ 13 [ポリシーの作成（Create Policy）] をクリックします。

ステップ 14 [ポリシーの作成（Create Policy）] ページで、[JSON] をクリックします。



ステップ 15 フィールドに次のポリシーを入力します。

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "ec2:DescribeTags",
    "ec2:DescribeInstances",
    "ec2:DescribeVpcs"
   ],
   "Resource": "*"
  }
 ]
}
```

ステップ 16 [次へ（Next）] をクリックします。

ステップ 17 [レビュー（Review）] をクリックします。

ステップ 18 [ポリシーの確認（Review Policy）] ページで、必要な情報を入力し、[ポリシーの作成（Create Policy）] をクリックします。

ステップ 19 [ポリシー（Policies）]ページで、検索フィールドにポリシー名のすべてまたは一部を入力し、Enter キーを押します。

ステップ 20 作成したポリシーをクリックします。

ステップ 21 **[アクション（Actions）] > [アタッチ（Attach）]**をクリックします。

ステップ 22 必要に応じて、検索フィールドにユーザー名の全部または一部を入力し、Enter キーを押します。

ステップ 23 [ポリシーをアタッチ（Attach policy）] をクリックします。

次のタスク

AWS コネクタの作成 （18 ページ）。

AWS セキュリティ グループ コネクタの作成

このタスクでは、ポリシーで使用するために AWS セキュリティグループから Secure Firewall Management Center にデータを送信するコネクタを構成する方法について説明します。

始める前に

次のことをすべて行います。

- AWS ドキュメントサイトの「セキュリティグループの操作」に記載された手順で、AWS セキュリティグループを作成します。
- dynamic attributes connector に対して最小限の権限を持つ AWS ユーザーを作成します。（16 ページ） で説明した権限以上のユーザーを作成します。

手順

ステップ 1 Secure Firewall Management Center にログインします。

ステップ 2 **Integration** > **Dynamic Attributes Connector** > **Connectors** をクリックします。

ステップ 3 次のいずれかを実行します。

- 新しいコネクタの追加：Add icon ( ) をクリックしてから、コネクタの名前をクリックします。
- コネクタの編集または削除：**More** ( ) をクリックしてから、行の末尾にある [編集（Edit）] または [削除（Delete）] をクリックします。

ステップ 4 次の情報を入力します。

値	説明
名前（Name）	（必須）このコネクタを一意に識別する名前を入力します。
説明（Description）	説明（オプション）。
プル間隔（Pull Interval）	（デフォルトは 30 秒）AWS から IP マッピングを取得する間隔です。 [プル間隔（Pull Interval）] の最小値は 1 秒です。最大は任意の値に設定できます。最小値を低い値に設定することはお勧めしません。これは、大量のトラフィックが生成される可能性があり、該当する場合、それらのトラフィックに関する請求が発生する可能性があるためです。

値	説明
リージョン（**Region**）	（必須）AWS リージョンコードを入力します。
AWS Access Key	（必須）アクセスキーを入力します。
AWS 秘密鍵	（必須）秘密鍵を入力します。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 [ステータス（Status）] 列に [OK] が表示されていることを確認します。

AWS サービスタグコネクタを作成する

このトピックでは、ポリシーで使用する Secure Firewall Management Center への Amazon Web Services（AWS）サービス タグのコネクタを作成する方法について説明します。

詳細については、次のような AWS ドキュメントサイトのリソースを参照してください。

- What are tags?
- AWS IP address ranges
- Tagging your AWS resources
- Guidance for Tagging on AWS
- AWS service points

手順

ステップ 1 Secure Firewall Management Center にログインします。

ステップ 2 **Integration** > **Dynamic Attributes Connector** > **Connectors** をクリックします。

ステップ 3 次のいずれかを実行します。

- 新しいコネクタの追加：Add icon ( ) をクリックしてから、コネクタの名前をクリックします。
- コネクタの編集または削除：**More** ( ) をクリックしてから、行の末尾にある [編集（Edit）] または [削除（Delete）] をクリックします。

ステップ 4 次の情報を入力します。

値	説明
名前（**Name**）	（必須）このコネクタを一意に識別する名前を入力します。

値	説明
説明（**Description**）	説明（オプション）。
URL	（必須）推奨されていない限り、URL を変更しないでください。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 [ステータス（Status）] 列に [OK] が表示されていることを確認します。

Azure コネクタ：ユーザー権限とインポートされたデータについて

dynamic attributes connector は、ポリシーで使用するために Azure から Secure Firewall Management Center へ動的属性をインポートします。

インポートされた動的属性

Azure から次の動的属性をインポートします。

- タグ：リソース、リソースグループ、およびサブスクリプションに関連付けられたキーと値のペア。

  詳細については、Microsoft ドキュメントのこのページを参照してください。

- Azure 内の仮想マシンの *IP* アドレス。

必要な最小限の権限

dynamic attributes connector で、動的属性をインポートするには、少なくとも**リーダー**権限を持つユーザーが必要です。

dynamic attributes connector に対する最小限の権限を持つ Azure ユーザーの作成

このタスクでは、動的属性を Secure Firewall Management Center に送信するための最小限の権限を持つサービスアカウントを設定する方法について説明します。これらの属性のリストについては、Azure コネクタ：ユーザー権限とインポートされたデータについて （23 ページ）を参照してください。

始める前に

Microsoft Azure アカウントを既に持っている必要があります。設定するには、Azure ドキュメントサイトのこのページを参照してください。

手順

ステップ 1 サブスクリプションの所有者として Azure Portal にログインします。

ステップ 2 **[Azure Active Directory]** をクリックします。

ステップ 3 設定するアプリケーションの Azure Active Directory のインスタンスを見つけます。

ステップ 4 **[追加（Add）]** > **[アプリケーションの登録（App registration）]** をクリックします。

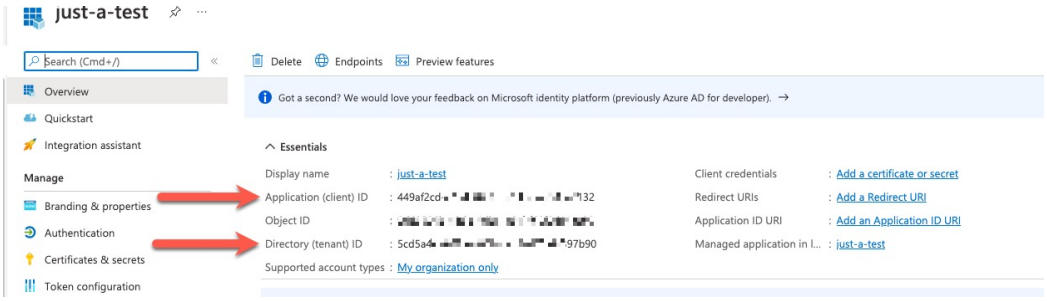
ステップ 5 [名前（Name）] フィールドに、このアプリケーションを識別するための名前を入力します。

ステップ 6 組織の必要に応じて、このページにその他の情報を入力します。

ステップ 7 [登録（Register）] をクリックします。

ステップ 8 次のページで、クライアント ID (アプリケーション *ID* とも呼ばれる) とテナント ID (ディレクトリ *ID* とも呼ばれる) を書き留めまたは、コピーします。

次に例を示します。

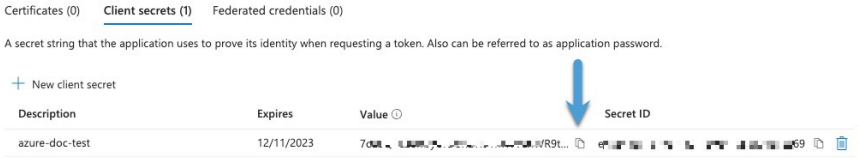


ステップ 9 [クライアントクレデンシャル（Client Credentials）] の横にある [証明書またはシークレットの追加（Add a certificate or secret）] をクリックします。

ステップ 10 [新しいクライアントシークレット（New Client Secret）] をクリックします。

ステップ 11 要求された情報を入力し、[追加（Add）] をクリックします。

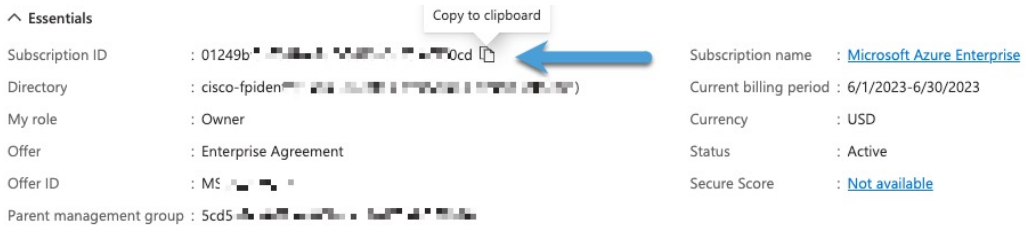
ステップ 12 [値（Value）] フィールドの値をクリップボードにコピーします。[シークレットID（Secret ID）] ではなく、この値がクライアントシークレットです。



ステップ 13 Azure Portal のメインページに戻り、[サブスクリプション（Subscriptions）] をクリックします。

ステップ 14 サブスクリプションの名前をクリックします。

ステップ 15 クリップボードにサブスクリプション ID をコピーします。



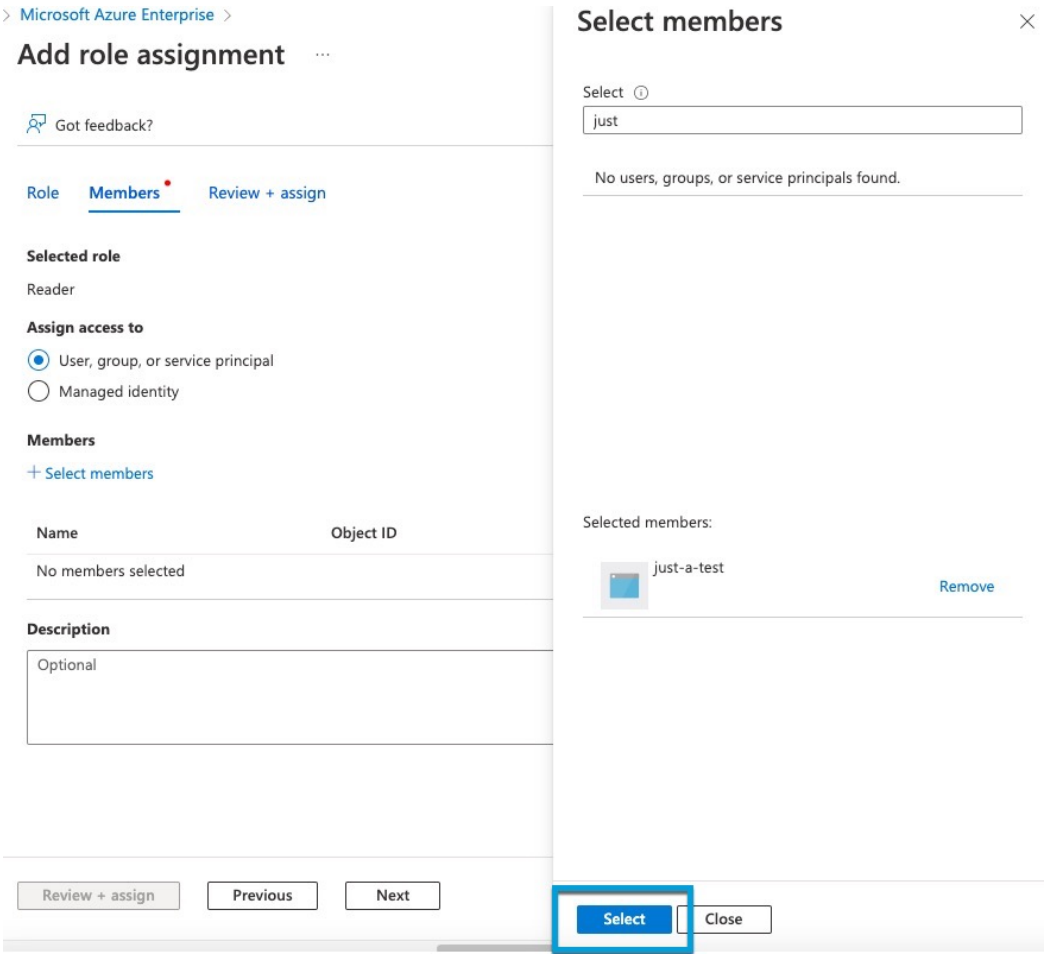
ステップ 16 [アクセス制御（IAM）（Access Control (IAM)）] をクリックします。

ステップ 17 **[追加（Add）] > [ロール割り当ての追加（Add role assignment）]**をクリックします。

ステップ 18 [リーダー（Reader）] をクリックし、[次へ（Next）] をクリックします。

ステップ 19 [メンバーの選択（Select Members）]をクリックします。

ステップ 20 ページの右側で、登録したアプリケーションの名前をクリックし、[選択（Select）] をクリックします。



ステップ 21 [確認と割り当て（Review + Assign）] をクリックし、プロンプトに従って操作を完了します。

次のタスク

「Azure コネクタの作成 （26 ページ）」を参照してください。

Azure コネクタの作成

このタスクでは、ポリシーで使用するために Azure から Secure Firewall Management Center にデータを送信するコネクタを作成する方法について説明します。

始める前に

dynamic attributes connector に対する最小限の権限を持つ Azure ユーザーの作成 （23 ページ）で説明した権限以上の Azure ユーザーを作成します。

手順

ステップ 1 Secure Firewall Management Center にログインします。

ステップ 2 **Integration** > **Dynamic Attributes Connector** > **Connectors** をクリックします。

ステップ 3 次のいずれかを実行します。

- 新しいコネクタの追加：Add icon ( ) をクリックしてから、コネクタの名前をクリックします。
- コネクタの編集または削除：**More** ( ) をクリックしてから、行の末尾にある [編集（Edit）] または [削除（Delete）] をクリックします。

ステップ 4 次の情報を入力します。

値	説明
名前（Name）	（必須）このコネクタを一意に識別する名前を入力します。
説明（Description）	説明（オプション）。
プル間隔（Pull Interval）	（デフォルトは 30 秒）Azure から IP マッピングを取得する間隔です。 [プル間隔（Pull Interval）] の最小値は 1 秒です。最大は任意の値に設定できます。最小値を低い値に設定することはお勧めしません。これは、大量のトラフィックが生成される可能性があり、該当する場合、それらのトラフィックに関する請求が発生する可能性があるためです。
サブスクリプションID（Subscription Id）	（必須）Azure サブスクリプション ID を入力します。
テナントID（Tenant Id）	（必須）テナント ID を入力します。

値	説明
クライアント ID（Client Id）	（必須）クライアント ID を入力します。
クライアントのシークレット（Client Secret）	（必須）クライアントのシークレットを入力します。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 [ステータス（Status）] 列に [OK] が表示されていることを確認します。

Azure サービス タグ コネクタの作成

このトピックでは、ポリシーで使用する Secure Firewall Management Center への Azure サービス タグのコネクタを作成する方法について説明します。これらのタグに関連付けられた IP アドレスは、Microsoft によって毎週更新されます。

詳細については、Microsoft TechNet の「仮想ネットワーク サービス タグ」を参照してください。

手順

ステップ 1 Secure Firewall Management Center にログインします。

ステップ 2 **Integration** > **Dynamic Attributes Connector** > **Connectors** をクリックします。

ステップ 3 次のいずれかを実行します。

- 新しいコネクタの追加：Add icon ( ) をクリックしてから、コネクタの名前をクリックします。
- コネクタの編集または削除：**More** ( ) をクリックしてから、行の末尾にある [編集（Edit）] または [削除（Delete）] をクリックします。

ステップ 4 次の情報を入力します。

値	説明
名前（Name）	（必須）このコネクタを一意に識別する名前を入力します。
説明（Description）	説明（オプション）。

値	説明
プル間隔（**Pull Interval**）	（デフォルトは 30 秒）Azure から IP マッピングを取得する間隔です。 [プル間隔（Pull Interval）] の最小値は 1 秒です。最大は任意の値に設定できます。最小値を低い値に設定することはお勧めしません。これは、大量のトラフィックが生成される可能性があり、該当する場合、それらのトラフィックに関する請求が発生する可能性があるためです。
サブスクリプションID（**Subscription Id**）	（必須）Azure サブスクリプション ID を入力します。
テナントID（**Tenant Id**）	（必須）テナント ID を入力します。
クライアント ID（**Client Id**）	（必須）クライアント ID を入力します。
クライアントのシークレット（**Client Secret**）	（必須）クライアントのシークレットを入力します。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 [ステータス（Status）] 列に [OK] が表示されていることを確認します。

Cisco Cyber Vision コネクタを作成する

このタスクでは、Cisco Cyber Vision から Secure Firewall Management Center にデータを送信する方法について説明します。

始める前に

Cisco Cyber Vision は、dynamic attributes connector が実行されているマシンから到達できる必要があります。IP アドレス、ポート、および API キーを把握している必要があります。

Cyber Vision 管理コンソールで API キーを見つけるには、**[管理（Admin）]** > **[API]** > **[トークン（Token）]** をクリックしてから、[表示（Show）] をクリックしてトークンを表示し、  をクリックしてトークンをクリップボードにコピーします。

手順

ステップ 1 Secure Firewall Management Center にログインします。

ステップ 2 **Integration** > **Dynamic Attributes Connector** > **Connectors** をクリックします。

ステップ 3 次のいずれかを実行します。

- 新しいコネクタの追加：Add icon () をクリックしてから、コネクタの名前をクリックします。
- コネクタの編集または削除：**More** (⋮) をクリックしてから、行の末尾にある [編集（Edit）] または [削除（Delete）] をクリックします。

ステップ 4 次の情報を入力します。

値	説明
名前（Name）	（必須）このコネクタを一意に識別する名前を入力します。
説明（Description）	説明（オプション）。
Cyber Visionプレフィックス（Cyber Vision Prefix）	オブジェクトが Secure Firewall Management Center に送信されるときに、この Cyber Vision の IP アドレスからダイナミックオブジェクトを識別するための英数字の文字列を入力します。 1 つの Cyber Vision IP アドレスがある場合は、**1** などの任意の値を入力できます。
プル間隔（Pull Interval）	（デフォルトは 60 秒です）。Cyber Vision からデータマッピングを取得する間隔。 [プル間隔（Pull Interval）] の最小値は 1 秒です。最大は任意の値に設定できます。最小値を低い値に設定することはお勧めしません。これは、大量のトラフィックが生成される可能性があり、該当する場合、それらのトラフィックに関する請求が発生する可能性があるためです。
ホスト（Host）	（必須）Cyber Vision の完全修飾ホスト名または IP アドレスを入力します。
ポート（Port）	（必須）Cyber Vision のリッスンポートを入力します。
トークン	（必須）API トークンを入力します。

ステップ 5 コネクタを保存する前に、[テスト（Test）] をクリックして、テストが成功することを確認します。

ステップ 6 [保存（Save）] をクリックします。

ステップ 7 [ステータス（Status）] 列に [OK] が表示されていることを確認します。

汎用テキストコネクタを作成する

このタスクでは、手動で維持するIPアドレスのアドホックリストを作成し、選択した間隔（デフォルトでは30秒）で取得する方法について説明します。アドレスのリストは必要なときにいつでも更新できます。

始める前に

IPアドレスを含むテキストファイルを作成し、Secure Firewall Management Centerからアクセス可能なWebサーバーに配置します。IPアドレスにはCIDR表記を含めることができます。テキストファイルには、1行につき1つのIPアドレスのみを含める必要があります。

たとえば、アクセス制御ルールの「許可リスト」用のIPアドレスのリストと、アクセス制御ルールの「ブロックリスト」用の別のIPアドレスのリストが存在する場合があります。

テキストファイルごとに最大10,000個のIPアドレスを指定できます。

手順

ステップ1 Secure Firewall Management Centerにログインします。

ステップ2 **Integration** > **Dynamic Attributes Connector** > **Connectors** をクリックします。

ステップ3 次のいずれかを実行します。

- 新しいコネクタの追加：Add icon ( ) をクリックしてから、コネクタの名前をクリックします。
- コネクタの編集または削除：**More** ( ) をクリックしてから、行の末尾にある[編集（Edit）]または[削除（Delete）]をクリックします。

ステップ4 次の情報を入力します。

項目	説明
名前（Name）	名前を入力して、コネクタを特定します。
説明	（オプション）説明を入力
プル間隔（Pull Interval）	ダイナミック属性コネクタが、テキストファイルからIPアドレスを取得する頻度を秒単位で変更します。デフォルトは30秒です。 [プル間隔（Pull Interval）]の最小値は1秒です。最大は任意の値に設定できます。最小値を低い値に設定することはお勧めしません。これは、大量のトラフィックが生成される可能性があり、該当する場合、それらのトラフィックに関する請求が発生する可能性があるためです。
URL	IPアドレスを取得するためにURLを入力します。

項目	説明
別のURLの追加	（オプション）既存のリストにさらにURLを追加するには、リンクをクリックします。
証明書	（任意）Web サーバーへのセキュアな接続に証明書チェーンが必要な場合は、次のオプションがあります。 • **[証明書を取得（Get Certificate）]** > **[取得（Fetch）]**をクリックして証明書を自動的に取得するか、それが不可能な場合は、認証局 (CA) チェーンを手動で取得する （46 ページ） で説明されているように手動で証明書を取得します。 • **[証明書を取得（Get Certificate）]** > **[ファイルから参照（Browse from file）]**をクリックして、以前にダウンロードした証明書チェーンをアップロードします。

ステップ 5 コネクタを保存する前に、[テスト（Test）] をクリックして、テストが成功することを確認します。

ステップ 6 [保存（Save）] をクリックします。

ステップ 7 [ステータス（Status）] 列に [OK] が表示されていることを確認します。

GitHub コネクタを作成する

このセクションでは、ポリシーで使用するためにデータを Secure Firewall Management Center に送信する GitHub コネクタを作成する方法について説明します。これらのタグに関連付けられている IP アドレスは、GitHub によって管理されています。動的属性フィルタを作成する必要はありません。

詳細については、「GitHub の IP アドレスについて」を参照してください。

（注） IP アドレスの取得に失敗するため、URL は変更しないでください。

手順

ステップ 1 Secure Firewall Management Center にログインします。

ステップ 2 **Integration** > **Dynamic Attributes Connector** > **Connectors** をクリックします。

ステップ 3 次のいずれかを実行します。

- 新しいコネクタの追加：Add icon ( ) をクリックしてから、コネクタの名前をクリックします。

- コネクタの編集または削除：**More** をクリックしてから、行の末尾にある [編集（Edit）] または [削除（Delete）] をクリックします。

ステップ 4 [名前（Name）] とオプションの [説明（Description）]を入力します。

ステップ 5 （オプション）[プル間隔（Pull Interval）] フィールドで、動的属性コネクタが GitHub から IP アドレスを取得する頻度を秒単位で変更します。デフォルトは 21,600 秒（6 時間）です。

ステップ 6 [保存（Save）] をクリックします。

ステップ 7 [ステータス（Status）] 列に [OK] が表示されていることを確認します。

Google Cloud コネクタ：ユーザー権限とインポートされたデータについて

dynamic attributes connector は、ポリシーで使用するために、Google Cloud から Secure Firewall Management Center へ動的属性をインポートします。

インポートされた動的属性

次の動的属性を Google Cloud からインポートします。

- ラベル：Google Cloud リソースを整理するために使用できるキーと値のペア。

  詳細については、Google Cloud ドキュメントの「ラベルの作成と管理」を参照してください。

- ネットワークタグ：組織、フォルダー、またはプロジェクトに関連付けられたキーと値のペア。

  詳細については、Google Cloud ドキュメントの「タグの作成と管理」を参照してください。

- Google Cloud 内の仮想マシンの *IP* アドレス。

必要最小限の権限

dynamic attributes connector では、少なくとも、動的属性をインポートできる基本閲覧者（Basic Viewer）権限を持つユーザーが必要です。 >

dynamic attributes connector に対して最小限の権限を持つ Google Cloud ユーザーを作成します。

このタスクでは、動的属性を Secure Firewall Management Center に送信するための最小限の権限を持つサービスアカウントを設定する方法について説明します。これらの属性のリストについては、Google Cloud コネクタ：ユーザー権限とインポートされたデータについて （32 ページ）を参照してください。

始める前に

Google Cloud アカウントがすでに設定されている必要があります。設定方法に関する詳細情報については、 Google Cloud ドキュメントの「環境設定」を参照してください。

手順

ステップ 1 所有者ロールを持つユーザーとして Google Cloud アカウントにログインします。

ステップ 2 **[IAMおよび管理者（IAM & Admin）] > [サービスアカウント（Service Accounts）] > [サービスアカウントの作成（Create Service Account）]** をクリックします。

ステップ 3 次の情報を入力します。

- サービスアカウント名（Service account name）：このアカウントを識別するための名前。たとえば、**CSDAC**。
- サービスアカウントID（Service account ID）：サービスアカウント名を入力した後、一意の値を入力する必要があります。
- サービスアカウントの説明（Service account description）： オプションの説明を入力します。

サービスアカウントの詳細については、Google Cloud ドキュメントの「サービスアカウントについて」を参照してください。

ステップ 4 [作成して続行（Create and Continue）] をクリックします。

ステップ 5 [このサービスアカウントへのアクセスをユーザーに許可する（Grant users access to this service account）] セクションが表示されるまで、画面の指示に従います。

ステップ 6 ユーザーに基本閲覧者（Basic Viewer）ロールを付与します。 >

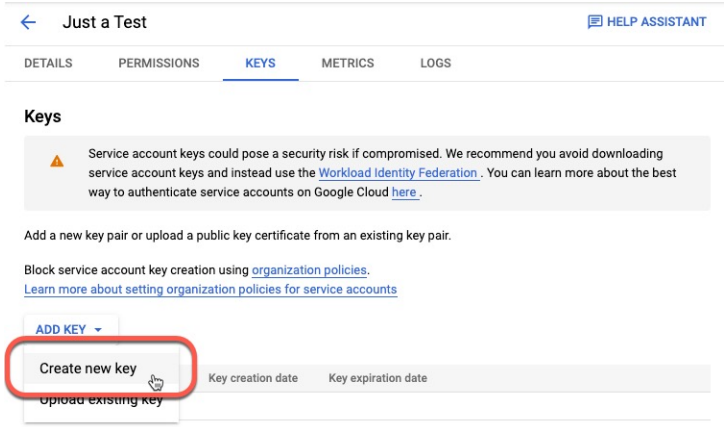
ステップ 7 [完了（Done）] をクリックします。

サービスアカウントのリストが表示されます。

ステップ 8 作成したサービスアカウントの行の末尾にある **More** (⋮) をクリックします。

ステップ 9 [キーの管理（Manage Keys）] をクリックします。

ステップ 10 **[キーの追加（ADD KEY）] > [新しいキーの作成（Create New Key）]**をクリックします。



ステップ 11 [JSON] をクリックします。

ステップ 12 [作成（Create）] をクリックします。

JSON キーがコンピュータにダウンロードされます。

ステップ 13 GCP コネクタを構成するときは、キーを手元に置いておいてください。

次のタスク

「Google Cloud コネクタの作成 （34 ページ）」を参照してください。

Google Cloud コネクタの作成

始める前に

Google Cloud JSON 形式のサービスアカウントデータを準備します。コネクタの設定に必要です。

手順

ステップ 1 Secure Firewall Management Center にログインします。

ステップ 2 **Integration** > **Dynamic Attributes Connector** > **Connectors** をクリックします。

ステップ 3 次のいずれかを実行します。

- 新しいコネクタの追加：Add icon ( ) をクリックしてから、コネクタの名前をクリックします。
- コネクタの編集または削除：**More** ( ) をクリックしてから、行の末尾にある [編集（Edit）] または [削除（Delete）] をクリックします。

ステップ 4 次の情報を入力します。

値	説明
名前（**Name**）	（必須）このコネクタを一意に識別する名前を入力します。
説明（**Description**）	説明（オプション）。
プル間隔（**Pull Interval**）	（デフォルトは 30 秒）AWS から IP マッピングを取得する間隔です。 [プル間隔（Pull Interval）] の最小値は 1 秒です。最大は任意の値に設定できます。最小値を低い値に設定することはお勧めしません。これは、大量のトラフィックが生成される可能性があり、該当する場合、それらのトラフィックに関する請求が発生する可能性があるためです。
GCP リージョン（**GCP region**）	（必須）Google Cloud が配置されている GCP リージョンを入力します。詳細については、Google Cloud のドキュメント「リージョンとゾーン」を参照してください。
サービス アカウント	Google Cloud サービスアカウントの JSON コードを貼り付けます。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 [ステータス（Status）] 列に [OK] が表示されていることを確認します。

Office 365 コネクタを作成する

このタスクでは、ポリシーで使用するためのデータを Secure Firewall Management Center に送信する、Office 365 タグのコネクタを作成する方法について説明します。これらのタグに関連付けられた IP アドレスは、Microsoft によって毎週更新されます。データを使用するために動的属性フィルタを作成する必要はありません。

詳細については、docs.microsoft.com の「Office 365 URL および IP アドレス範囲」を参照してください。

手順

ステップ 1 Secure Firewall Management Center にログインします。

ステップ 2 **Integration** > **Dynamic Attributes Connector** > **Connectors** をクリックします。

ステップ 3 次のいずれかを実行します。

- 新しいコネクタの追加：Add icon ( ) をクリックしてから、コネクタの名前をクリックします。

- コネクタの編集または削除：**More** をクリックしてから、行の末尾にある [編集（Edit）] または [削除（Delete）] をクリックします。

ステップ 4 次の情報を入力します。

値	説明
名前（Name）	（必須）このコネクタを一意に識別する名前を入力します。
説明（Description）	説明（オプション）。
プル間隔（Pull Interval）	（デフォルトは 30 秒）Azure から IP マッピングを取得する間隔です。 [プル間隔（Pull Interval）] の最小値は 1 秒です。最大は任意の値に設定できます。最小値を低い値に設定することはお勧めしません。これは、大量のトラフィックが生成される可能性があり、該当する場合、それらのトラフィックに関する請求が発生する可能性があるためです。
ベース API URL（Base API URL）	（必須）デフォルトと異なる場合は、Office 365 情報を取得する URL を入力します。詳細については、Microsoft ドキュメントサイトの「Office 365 IP アドレスと URL の Web サービス」を参照してください。
インスタンス名（Instance name）	（必須）リストからインスタンス名をクリックします。詳細については、Microsoft ドキュメントサイトの「Office 365 IP アドレスと URL の Web サービス」を参照してください。
オプションの IP を無効にする	（必須）**true**または**false**の入力。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 [ステータス（Status）] 列に [OK] が表示されていることを確認します。

vCenter コネクタ：ユーザー権限とインポートされたデータについて

Dynamic Attributes Connector は、ポリシーで使用するために vCenter から Secure Firewall Management Center へ動的属性をインポートします。

インポートされた動的属性

vCenter から次の動的属性をインポートします。

- オペレーティング システム
- *MAC* アドレス

- *IP* アドレス
- *NSX* タグ

必要最小限の権限

Dynamic Attributes Connector では、少なくとも、動的属性をインポートできる**読み取り専用**権限を持つユーザーが必要です。

dynamic attributes connector に対して最小限の権限を持つ vCenter ユーザーの作成

このタスクでは、動的属性を Secure Firewall Management Center に送信するための最小限の権限を持つサービスアカウントを設定する方法について説明します。これらの属性のリストについては、vCenter コネクタ：ユーザー権限とインポートされたデータについて （36 ページ）を参照してください。

始める前に

vCenter Server アカウントがすでに設定されている必要があります。設定方法の詳細については、vCenter ドキュメントの vCenter Server のインストールとセットアップに関する説明を参照してください。

手順

ステップ 1 vCenter に管理者としてログインします。

ステップ 2 **[メニュー（Menu）]** > **[管理（Administration）]** をクリックします。

ステップ 3 左側のペインで、**[シングルサインオン（Single Sign On）]** > **[ユーザーとグループ（Users and Groups）]** をクリックします。

ステップ 4 [ドメイン（Domain）] リストから、ユーザーを追加するドメインの名前をクリックします。

ステップ 5 [ユーザの追加（Add User）] をクリックします。

ステップ 6 要求された情報を入力し、[追加（Add）] をクリックします。

ステップ 7 左側のペインで、**[アクセス制御（Access Control）]** > **[グローバル権限（Global Permissions）]** をクリックします。

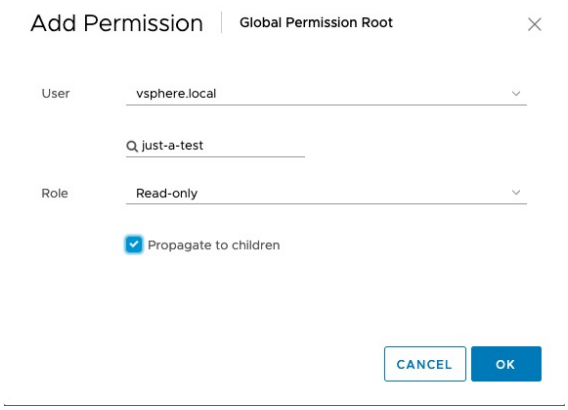
ステップ 8 **[追加（Add）]**（＋）をクリックします。

ステップ 9 [ユーザー（User）] フィールドで、ユーザーを作成した vCenter ドメインの名前をクリックします。

ステップ 10 検索フィールドに、ユーザーの名前の一部を入力します。

ステップ 11 [ロール（Role）] リストから、[読み取り専用（Read-only）] をクリックします。

ステップ 12 [子への伝播（Propagate to children）] チェックボックスをオンにします。



ステップ 13 [OK] をクリックします。

次のタスク

「vCenter コネクタの作成 （38 ページ）」を参照してください。

vCenter コネクタの作成

このタスクでは、ポリシーで使用するためにデータを Secure Firewall Management Center に送信する VMware vCenter のコネクタを作成する方法について説明します。

始める前に

信頼されていない証明書を使用して vCenter と通信する場合は、認証局 (CA) チェーンを手動で取得する （46 ページ）を参照してください。

手順

ステップ 1 Secure Firewall Management Center にログインします。

ステップ 2 **Integration** > **Dynamic Attributes Connector** > **Connectors** をクリックします。

ステップ 3 次のいずれかを実行します。

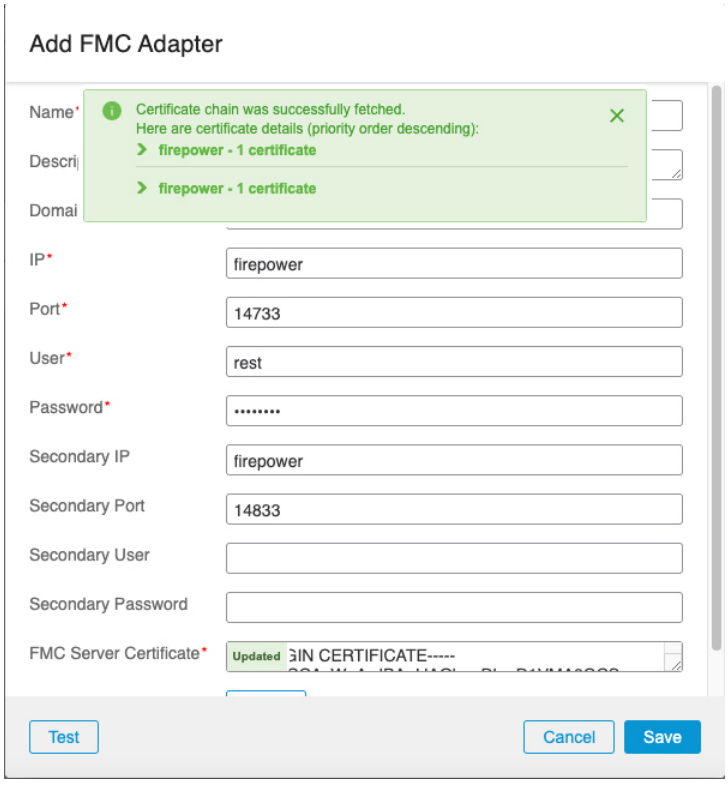
- 新しいコネクタの追加：Add icon ( ) をクリックしてから、コネクタの名前をクリックします。
- コネクタの編集または削除：**More** ( ) をクリックしてから、行の末尾にある [編集（Edit）] または [削除（Delete）] をクリックします。

ステップ 4 次の情報を入力します。

値	説明
名前（Name）	（必須）このコネクタを一意に識別する名前を入力します。
説明（Description）	任意で説明を入力します。
プル間隔（Pull Interval）	（デフォルトは30秒）vCenterからIPマッピングを取得する間隔です。 [プル間隔（Pull Interval）] の最小値は1秒です。最大は任意の値に設定できます。最小値を低い値に設定することはお勧めしません。これは、大量のトラフィックが生成される可能性があり、該当する場合、それらのトラフィックに関する請求が発生する可能性があるためです。
ホスト（Host）	（必須）次のいずれかを入力します。 • vCenterの完全修飾ホスト名 • vCenterのIPアドレス •（オプション）ポート スキーム（**`https://`**など）または末尾のスラッシュを入力しないでください。 たとえば、**`myvcenter.example.com`**または**`192.0.2.100:9090`**
ユーザー（User）	（必須）最低限でも読み取り専用ロールを持つユーザーのユーザー名を入力します。ユーザ名は大文字/小文字を区別します。
パスワード（Password）	（必須）ユーザーのパスワードを入力します。
NSX IP	vCenter Network Security Visualization（NSX）を使用する場合は、そのIPアドレスを入力します。
NSXユーザー（NSX User）	最低限でも監査人ロールを持つNSXユーザーのユーザー名を入力します。
NSXタイプ（NSX Type）	**NSX-T** を入力します。
NSXパスワード（NSX Password）	NSXユーザーのパスワードを入力します。

値	説明
vCenter証明書（vCenter Certificate）	次の選択肢があります。 • 認証局 (CA) チェーンを手動で取得する （46 ページ）で説明したように、取得した認証局（CA）チェーンを貼り付けます。 • [取得（Fetch）] をクリックして証明書を自動的に取得するか、それが不可能な場合は、認証局 (CA) チェーンを手動で取得する （46 ページ）で説明されているように手動で証明書を取得します。 • **[証明書を取得（Get Certificate）] > [取得（Fetch）]**をクリックして証明書を自動的に取得するか、それが不可能な場合は、認証局 (CA) チェーンを手動で取得する （46 ページ） で説明されているように手動で証明書を取得します。 • **[証明書を取得（Get Certificate）] > [ファイルから参照（Browse from file）]**をクリックして、以前にダウンロードした証明書チェーンをアップロードします。

次に、証明書チェーンを正常に取得する例を示します。



ダイアログボックスの上部にある証明書CAチェーンを展開すると、次のような証明書が表示されます。

この方法で証明書を取得できない場合は、認証局 (CA) チェーンを手動で取得する （46 ページ）で説明されているように、証明書チェーンを手動で取得できます。

ステップ 5 **[保存（Save）]** をクリックします。

Webex コネクタを作成する

このセクションでは、ポリシーで使用するためにデータを Secure Firewall Management Center に送信する Webex コネクタを作成する方法について説明します。これらのタグに関連付けられている IP アドレスは、Webex によって管理されています。動的属性フィルタを作成する必要はありません。

詳細については、「Port Reference for Webex Calling」を参照してください。

手順

ステップ 1 Secure Firewall Management Center にログインします。

ステップ 2 **Integration** > **Dynamic Attributes Connector** > **Connectors** をクリックします。

ステップ 3 次のいずれかを実行します。

- 新しいコネクタの追加：Add icon ( ) をクリックしてから、コネクタの名前をクリックします。
- コネクタの編集または削除：**More** ( ) をクリックしてから、行の末尾にある [編集（Edit）] または [削除（Delete）] をクリックします。

ステップ 4 次の情報を入力します。

値	説明
名前（Name）	（必須）このコネクタを一意に識別する名前を入力します。
説明（Description）	説明（オプション）。

値	説明
プル間隔（**Pull Interval**）	（デフォルトは 30 秒）Webex から IP マッピングを取得する間隔です。 [プル間隔（Pull Interval）] の最小値は 1 秒です。最大は任意の値に設定できます。最小値を低い値に設定することはお勧めしません。これは、大量のトラフィックが生成される可能性があり、該当する場合、それらのトラフィックに関する請求が発生する可能性があるためです。
[プロバイダーの予約済みIP（Provider Reserved IPs）]	（必須）（必須）予約済み IP アドレスを取得するには、[有効（Enabled）] にスライドします。

ステップ 5 コネクタを保存する前に、[テスト（Test）] をクリックして、テストが成功することを確認します。

ステップ 6 [保存（Save）] をクリックします。

ステップ 7 [ステータス（Status）] 列に [OK] が表示されていることを確認します。

Zoom コネクタの作成

このセクションでは、ポリシーで使用するためにデータを Secure Firewall Management Center に送信する Zoom コネクタを作成する方法について説明します。これらのタグに関連付けられている IP アドレスは、Zoom によって管理されています。動的属性フィルタを作成する必要はありません。

詳細については、「Zoom network firewall or proxy server settings」[英語] を参照してください。

手順

ステップ 1 Secure Firewall Management Center にログインします。

ステップ 2 **Integration** > **Dynamic Attributes Connector** > **Connectors** をクリックします。

ステップ 3 次のいずれかを実行します。

- 新しいコネクタの追加：Add icon ( ) をクリックしてから、コネクタの名前をクリックします。
- コネクタの編集または削除：**More** ( ) をクリックしてから、行の末尾にある [編集（Edit）] または [削除（Delete）] をクリックします。

ステップ 4 次の情報を入力します。

値	説明
名前（Name）	（必須）このコネクタを一意に識別する名前を入力します。
説明（Description）	説明（オプション）。
プル間隔（Pull Interval）	（デフォルトは 30 秒）Zoom から IP マッピングを取得する間隔です。 [プル間隔（Pull Interval）] の最小値は 1 秒です。最大は任意の値に設定できます。最小値を低い値に設定することはお勧めしません。これは、大量のトラフィックが生成される可能性があり、該当する場合、それらのトラフィックに関する請求が発生する可能性があるためです。
[プロバイダーの予約済みIP（Provider Reserved IPs）]	（必須）予約済み IP アドレスを取得するには、[有効（Enabled）] にスライドします。

ステップ 5 コネクタを保存する前に、[テスト（Test）] をクリックして、テストが成功することを確認します。

ステップ 6 [保存（Save）] をクリックします。

ステップ 7 [ステータス（Status）] 列に [OK] が表示されていることを確認します。

ダイナミック属性フィルタを作成する

Dynamic Attributes Connectorを使用して定義する動的属性フィルタは、アクセス コントロール ポリシーで使用できるダイナミックオブジェクトとして Secure Firewall Management Center で公開されます。たとえば、財務部門の AWS サーバーへのアクセスを、Microsoft Active Directory（AD）で定義された財務グループのメンバーのみに制限できます。

（注） 汎用テキスト、Office 365、Azure サービスタグ、Webex または Zoom では動的属性フィルタを作成できません。これらのタイプのクラウドオブジェクトは、独自の IP アドレスを提供します。

アクセスコントロールの詳細については、「ダイナミック属性フィルタを使用してアクセスコントロールルールを作成する （52 ページ）」を参照してください。

始める前に

コネクタを作成する （15 ページ）

手順

ステップ 1 Secure Firewall Management Center にログインします。

ステップ 2 **Integration** > **Dynamic Attributes Connector** > **Dynamic Attributes Filters** をクリックします。

ステップ 3 次のいずれかを実行します。

- 新しいフィルタの追加：**Add** ( ) をクリックします。
- フィルタの編集または削除：**More** ( ) をクリックしてから、行の末尾にある [編集（Edit）] または [削除（Delete）] をクリックします。

ステップ 4 次の情報を入力します。

項目	説明
名前（Name）	ポリシーおよび Secure Firewall Management Center オブジェクト マネージャ（**外部属性** > **ダイナミック オブジェクト**）において、ダイナミック フィルタを（ダイナミック オブジェクトとして）識別するための一意の名前。
コネクタ（Connector）	リストから、使用するコネクタの名前をクリックします。
[Query（クエリ）]	Add をクリックします。

ステップ 5 クエリを追加または編集するには、次の情報を入力します。

項目	説明
キー（Key）	リストからキーをクリックします。キーはコネクタから取得されます。
操作（Operation）	次のいずれかをクリックします。 • キーを値に正確に一致させるには、[等しい（Equals）]。 • 値のいずれかの部分が一致する場合に、キーを値に一致させるには、[含む（Contains）]。
値（Value）	[任意（Any）] または [すべて（All）] をクリックし、リストから 1 つ以上の値をクリックします。[別の値を追加（Add another value）] をクリックして、クエリに値を追加します。

ステップ 6 [プレビューを表示（Show Preview）] をクリックして、クエリによって返されたネットワークまたは IP アドレスのリストを表示します。

ステップ 7 完了したら、[保存（Save）] をクリックします。

ステップ 8 （オプション）Secure Firewall Management Center のダイナミックオブジェクトを確認します。

a) 最低限でもネットワーク管理者ロールを持つユーザーとして Secure Firewall Management Center にログインします。

b) **Objects** > **Object Management** > **External Attributes** > **Dynamic Object** をクリックします。

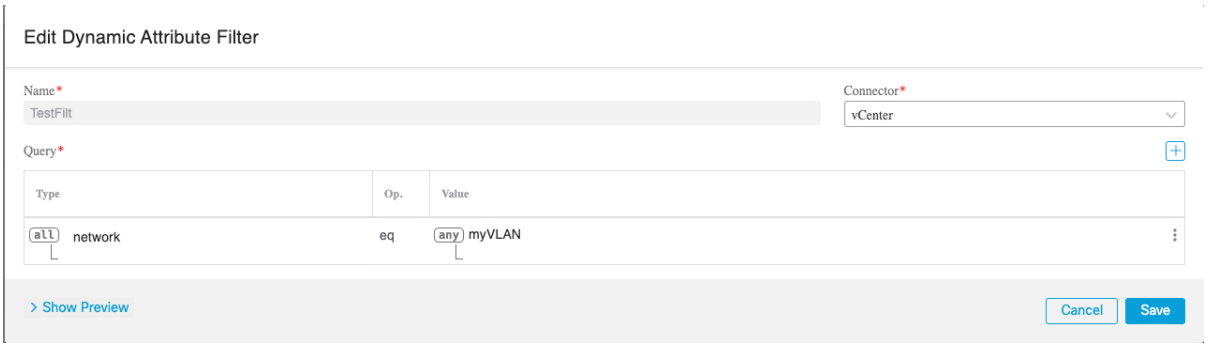
作成した動的属性クエリは、ダイナミックオブジェクトとして表示されます。

動的属性フィルタの例

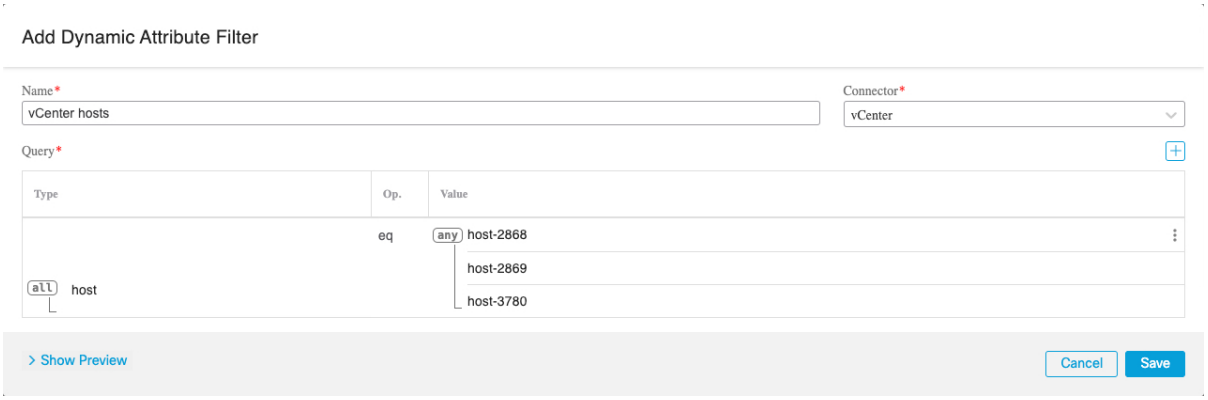
このトピックでは、動的属性フィルタの設定例をいくつか示します。

例：vCenter

次の例は、1 つの基準を示しています：VLAN。

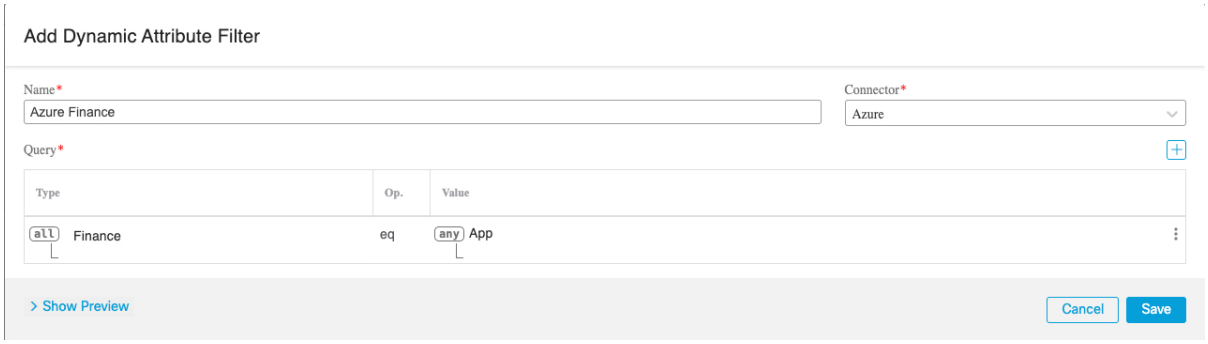


次の例は、OR で結合された 3 つの条件を示しています。クエリは 3 つのホストのいずれかに一致します。



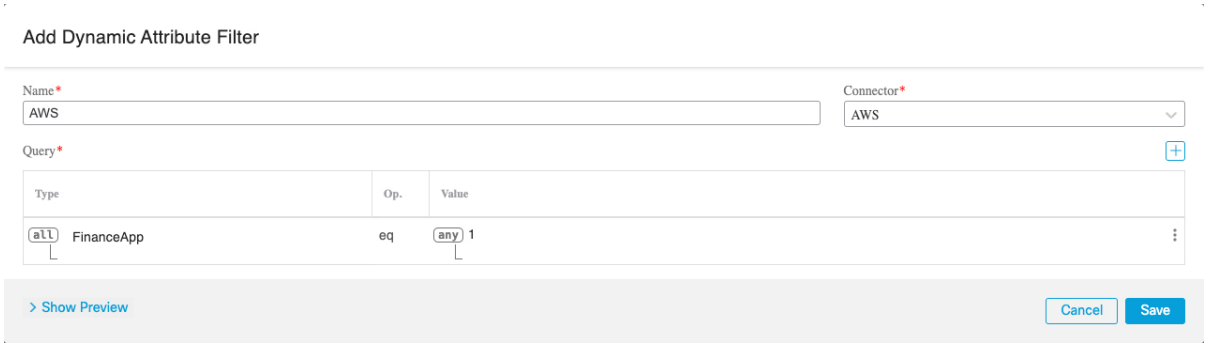
例：Azure

次の例は 1 つの条件を示しています：サーバーが財務アプリケーションとしてタグ付けされる。



例：AWS

次の例は、1 つの基準を示しています：値が 1 の FinanceApp。



認証局 (CA) チェーンを手動で取得する

認証局チェーンを自動的に取得できない場合は、次のブラウザ固有の手順のいずれかを使用して、vCenter または Firewall Management Center にセキュアに接続するための証明書チェーンを取得します。

証明書チェーンは、ルート証明書とすべての下位証明書です。

必要に応じて、これらの手順のいずれかを使用して次に接続できます。

- vCenter または NSX
- Firewall Management Center

証明書チェーンの取得：Mac（Chrome および Firefox）

Mac OS で Chrome および Firefox ブラウザを使用して証明書チェーンを取得するには、この手順を使用します。

1. ターミナル ウィンドウを開きます。
2. 次のコマンドを入力します。

   ```
   security verify-cert -P url[:port]
   ```

   ここでの、*url* は、vCenterr または Firewall Management Center への（スキームを含む）URL です。例：

   ```
   security verify-cert -P https://myvcenter.example.com
   ```

   NAT または PAT を使用して、vCenter または Firewall Management Center にアクセスする場合、次のようにポートを追加できます。

   ```
   security verify-cert -P https://myvcenter.example.com:12345
   ```

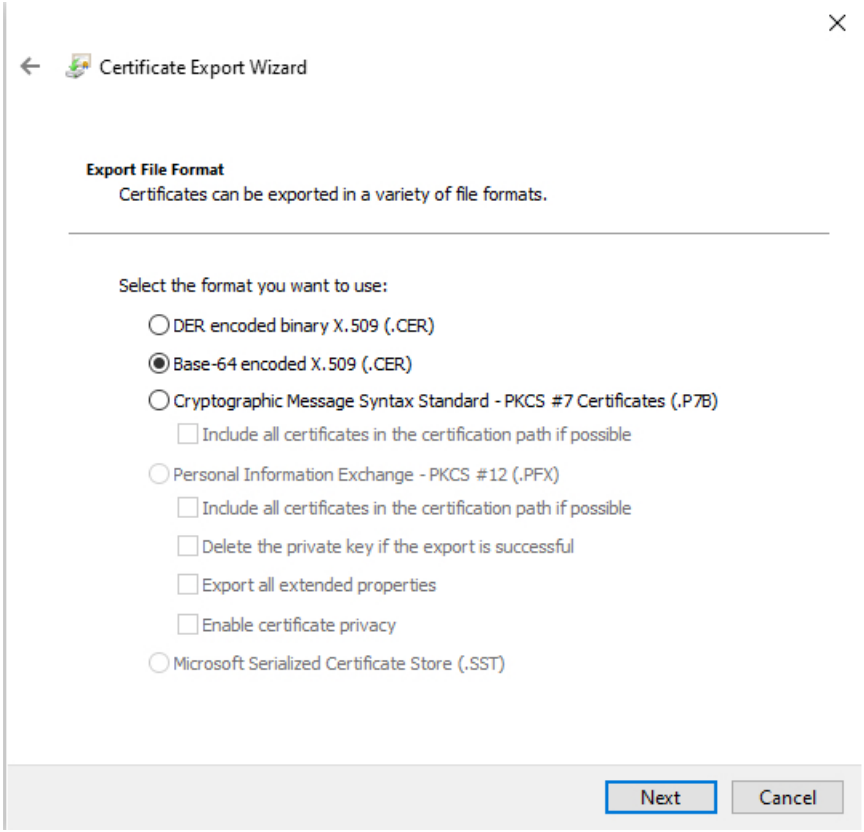
3. 証明書チェーン全体をプレーンテキストファイルに保存します。
   - すべての `-----BEGIN CERTIFICATE-----` および `-----END CERTIFICATE-----` 区切り文字を含めます。
   - 無関係なテキスト（たとえば、証明書の名前、山かっこ（<および>）に含まれるテキスト、および山かっこ自体を除外します。
4. vCenter Firewall Management Center、Cisco APIC、 に対してこれらのタスクを繰り返します。

証明書チェーンの取得：Windows Chrome

Windows で Chrome ブラウザを使用して証明書チェーンを取得するには、この手順を使用します。

1. Chrome を使用して vCenter または Firewall Management Center にログインします。
2. ブラウザのアドレスバーで、ホスト名の左側にあるロックをクリックします。
3. [証明書（Certificate）] をクリックします。
4. [証明のパス（Certification Path）] タブをクリックします。
5. チェーンの最上位（つまり、最初）の証明書をクリックします。
6. **証明書の表示**をクリックします。
7. [詳細（Details）] タブをクリックします。
8. [ファイルにコピーする（Copy to File）] をクリックします。
9. プロンプトに従って、証明書チェーン全体を含むCER形式の証明書ファイルを作成します。

   エクスポートファイル形式の選択を求められたら、次の図に示すように、[Base 64 エンコード X.509（.CER）（Base 64-Encoded X.509 (.CER)）] をクリックします。



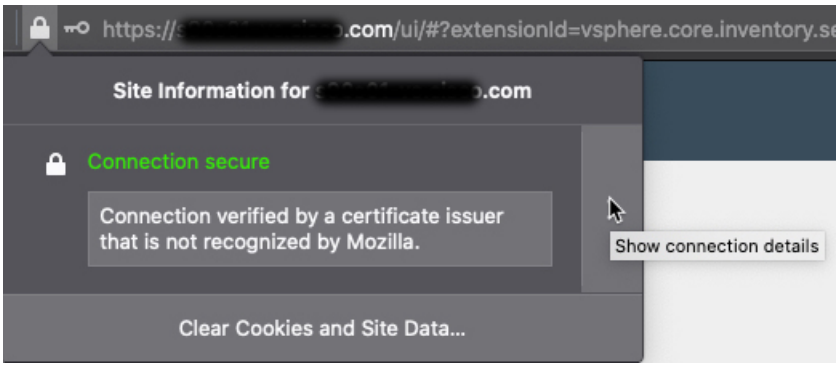
10. 指示に従ってエクスポートを完了します。
11. 証明書をテキストエディタで開きます。
12. チェーン内のすべての証明書に対してこのプロセスを繰り返します。

    テキストエディタに各証明書を最初から最後まで順番に貼り付ける必要があります。
13. vCenter または Firewall Management Center に対してこれらのタスクを繰り返します。

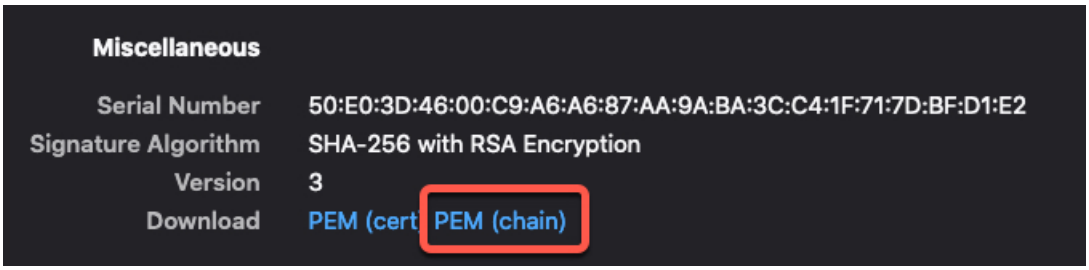
証明書チェーンの取得：Windows Firefox

Windows または Mac OS で Firefox ブラウザの証明書チェーンを取得するには、次の手順を使用します。

1. Firefox を使用して vCenter または Firewall Management Center にログインします。
2. ホスト名の左側にあるロックをクリックします。
3. 右矢印（[接続の詳細を表示（Show connection details）]）をクリックします。次の図は例を示しています。



4. [詳細（More Information）] をクリックします。
5. **証明書の表示**をクリックします。
6. 結果のダイアログボックスにタブページがある場合は、最上位 CA に対応するタブページをクリックします。
7. [その他（Miscellaneous）] セクションまでスクロールします。
8. [ダウンロード（Miscellaneous）] 行の [PEM（チェーン）（PEM (chain)）] をクリックします。次の図は例を示しています。



9. ファイルを保存します。
10. vCenter または Firewall Management Center に対してこれらのタスクを繰り返します。

アクセス制御ポリシーでのダイナミックオブジェクトの使用

dynamic attributes connectorでは、で動的オブジェクトとして Secure Firewall Management Center で表示される 動的属性フィルタを設定できます。

アクセス制御ルール ルールのダイナミック オブジェクトについて

コネクタを作成し、動的属性フィルタを作成してそのコネクタに保存すると、ダイナミックオブジェクトが dynamic attributes connectorから定義済み Cisco Secure Firewall に自動的にプッシュされます。

これらのダイナミック オブジェクトは、アクセス制御ルールまたは、の **[動的属性（Dynamic Attributes）]** タブページで使用できます。送信元属性または接続先属性としてダイナミックオブジェクトを追加できます。たとえば、アクセス制御ブロックルールでは、ルール内の他の基準に一致するオブジェクトによって財務サーバーへのアクセスをブロックする接続先属性として財務ダイナミックオブジェクトを追加できます。

（注） 汎用テキスト、Office 365、Azure サービスタグ、Webex または Zoom では動的属性フィルタを作成できません。これらのタイプのクラウドオブジェクトは、独自の IP アドレスを提供します。

ダイナミック属性フィルタを作成する

Dynamic Attributes Connectorを使用して定義する動的属性フィルタは、アクセス コントロール ポリシーで使用できるダイナミックオブジェクトとして Secure Firewall Management Center で公開されます。たとえば、財務部門の AWS サーバーへのアクセスを、Microsoft Active Directory（AD）で定義された財務グループのメンバーのみに制限できます。

（注） 汎用テキスト、Office 365、Azure サービスタグ、Webex または Zoom では動的属性フィルタを作成できません。これらのタイプのクラウドオブジェクトは、独自の IP アドレスを提供します。

アクセスコントロールの詳細については、「ダイナミック属性フィルタを使用してアクセスコントロールルールを作成する （52 ページ）」を参照してください。

始める前に

コネクタを作成する （15 ページ）

手順

ステップ 1 Secure Firewall Management Center にログインします。

ステップ 2 **Integration** > **Dynamic Attributes Connector** > **Dynamic Attributes Filters** をクリックします。

ステップ 3 次のいずれかを実行します。

- 新しいフィルタの追加：**Add** ( ) をクリックします。

- フィルタの編集または削除：**More** をクリックしてから、行の末尾にある [編集（Edit）] または [削除（Delete）] をクリックします。

ステップ 4 次の情報を入力します。

項目	説明
名前（Name）	ポリシーおよび Secure Firewall Management Center オブジェクト マネージャ（**外部属性** > **ダイナミック オブジェクト**）において、ダイナミック フィルタを（ダイナミック オブジェクトとして）識別するための一意の名前。
コネクタ（Connector）	リストから、使用するコネクタの名前をクリックします。
[Query（クエリ）]	Add をクリックします。

ステップ 5 クエリを追加または編集するには、次の情報を入力します。

項目	説明
キー（Key）	リストからキーをクリックします。キーはコネクタから取得されます。
操作（Operation）	次のいずれかをクリックします。 • キーを値に正確に一致させるには、[等しい（Equals）]。 • 値のいずれかの部分が一致する場合に、キーを値に一致させるには、[含む（Contains）]。
値（Value）	[任意（Any）] または [すべて（All）] をクリックし、リストから 1 つ以上の値をクリックします。[別の値を追加（Add another value）] をクリックして、クエリに値を追加します。

ステップ 6 [プレビューを表示（Show Preview）] をクリックして、クエリによって返されたネットワークまたは IP アドレスのリストを表示します。

ステップ 7 完了したら、[保存（Save）] をクリックします。

ステップ 8 （オプション）Secure Firewall Management Center のダイナミックオブジェクトを確認します。

a) 最低限でもネットワーク管理者ロールを持つユーザーとして Secure Firewall Management Center にログインします。

b) **Objects** > **Object Management** > **External Attributes** > **Dynamic Object** をクリックします。

作成した動的属性クエリは、ダイナミックオブジェクトとして表示されます。

ダイナミック属性ルールの条件

ダイナミック属性には次のものがあります。

- （送信元または宛先）。ダイナミックオブジェクト（dynamic attributes connector からのものなど）

  dynamic attributes connector では、クラウドプロバイダーからデータ（ネットワークや IP アドレスなど）を収集し、それを Secure Firewall Management Center に送信して、アクセス制御ルールで使用できるようにします。

  dynamic attributes connector の詳細については、「Dynamic Attributes Connector について」を参照してください。

- （送信元のみ）。SGT オブジェクトは、手動で定義したタグ、または ISE が定義したタグを含みます。詳細については、送信元および宛先セキュリティグループタグ（SGT）の照合 および セキュリティグループタグを参照してください。
- （送信元のみ）。Cisco ISE が定義したロケーション IP オブジェクト
- （送信元のみ）。Cisco ISE が定義したデバイスタイプオブジェクト（エンドポイント プロファイル オブジェクトとも呼ばれます）

ダイナミック属性は、アクセスコントロールルールの送信元基準および接続先基準として使用できます。次の注意事項に従ってください。

- 異なるタイプのオブジェクトは AND 結合される
- 同様のタイプのオブジェクトは OR 結合される

たとえば、送信元と宛先の基準 SGT 1、SGT 2、およびデバイスタイプ 1 を選択した場合、デバイスタイプ 1 が SGT 1 または SGT 2 で検出された場合、ルールが一致します。別の例として、セキュリティグループタグと、IP アドレスをリストするダイナミックオブジェクトの両方を選択した場合、タグを持つトラフィックがそれらの IP アドレスのいずれかを発信元（または宛先）とする場合にルールが一致します。

ダイナミック属性フィルタを使用してアクセスコントロールルールを作成する

このトピックでは、ダイナミックオブジェクトを使用してアクセス制御ルールを作成する方法について説明します（これらのダイナミックオブジェクトは、前に作成した動的属性フィルタにちなんで命名されます）。

ダイナミック属性フィルタを DNS ポリシーに追加するには、「基本的な DNS ポリシーの作成」を参照してください。

始める前に

「ダイナミック属性フィルタを作成する （43 ページ）」で説明されているように、これらのダイナミック属性フィルタを編集または置換できます。

（注） 汎用テキスト、Office 365、Azure サービスタグ、Webex または Zoom では動的属性フィルタを作成できません。これらのタイプのクラウドオブジェクトは、独自の IP アドレスを提供します。

手順

ステップ 1 Secure Firewall Management Centerへのログイン

ステップ 2 **Policies** > **Access Control heading** > **Access Control** をクリックします。

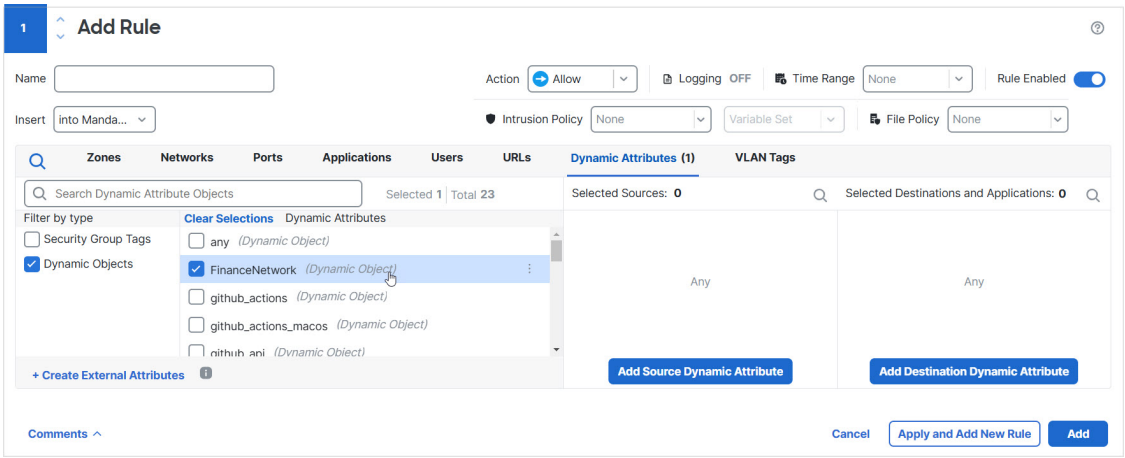
ステップ 3 アクセス コントロール ポリシーの横にある **Edit** ( ) をクリックします。

ステップ 4 [ルールの追加（Add Rule）] をクリックします。

ステップ 5 [動的属性（Dynamic Attributes）] タブをクリックします。

ステップ 6 [使用可能な属性（Available Attributes）] セクションで、リストから [ダイナミックオブジェクト（Dynamic Objects）] をクリックします。

次の図は例を示しています。



例は、dynamic attributes connector で作成されたダイナミック属性フィルタに対応する `APIC ダイナミック属性`という名前のダイナミック オブジェクトを示しています。

ステップ 7 目的のオブジェクトを送信元または接続先属性に追加します。

ステップ 8 必要に応じて、ルールに他の条件を追加します。

次のタスク

「ダイナミック属性ルールの条件 （52 ページ）」を参照してください。

Dynamic Attributes Connector の無効化

クラウドソースからダイナミックオブジェクトを収集する必要がなくなった場合は、次のタスクで説明するように、Secure Firewall Management Center の Dynamic Attributes Connector を無効にすることができます。

手順

ステップ 1 Secure Firewall Management Center にログインしていない場合は、ログインします。

ステップ 2 **Integration** > **Dynamic Attributes Connector** をクリックします。

ステップ 3 [無効（Disabled）] にスライドします。

Secure Firewall Management Centerを使用したトラブルシューティング

このタスクでは、Secure Firewall Management Center のトラブルシューティング ファイルを生成する方法について説明します。

手順

ステップ 1 Secure Firewall Management Center にログインします。

ステップ 2 **System** (⚙) > **Health** > **Monitor** をクリックします。

ステップ 3 左側のペインで、[Firewall Management Center（Firewall Management Center）] をクリックします。

ステップ 4 上部にある [システムとトラブルシューティングの詳細（System and Troubleshooting Details）] をクリックします。

ステップ 5 [トラブルシューティング ファイルの生成（Generate Troubleshooting Files）] をクリックします。

ステップ 6 Cisco TAC またはベータコーディネータにファイルを提供します。

認証局 (CA) チェーンを手動で取得する

認証局チェーンを自動的に取得できない場合は、次のブラウザ固有の手順のいずれかを使用して、vCenter または Firewall Management Center にセキュアに接続するための証明書チェーンを取得します。

証明書チェーンは、ルート証明書とすべての下位証明書です。

必要に応じて、これらの手順のいずれかを使用して次に接続できます。

- vCenter または NSX
- Firewall Management Center

証明書チェーンの取得：Mac（Chrome および Firefox）

Mac OS で Chrome および Firefox ブラウザを使用して証明書チェーンを取得するには、この手順を使用します。

1. ターミナル ウィンドウを開きます。
2. 次のコマンドを入力します。

   ```
   security verify-cert -P url[:port]
   ```

   ここでの、*url* は、vCenterr または Firewall Management Center への（スキームを含む）URL です。例：

   ```
   security verify-cert -P https://myvcenter.example.com
   ```

   NAT または PAT を使用して、vCenter または Firewall Management Center にアクセスする場合、次のようにポートを追加できます。

   ```
   security verify-cert -P https://myvcenter.example.com:12345
   ```

3. 証明書チェーン全体をプレーンテキストファイルに保存します。
   - すべての `-----BEGIN CERTIFICATE-----` および `-----END CERTIFICATE-----` 区切り文字を含めます。
   - 無関係なテキスト（たとえば、証明書の名前、山かっこ（<および>）に含まれるテキスト、および山かっこ自体を除外します。
4. vCenter Firewall Management Center、Cisco APIC、 に対してこれらのタスクを繰り返します。

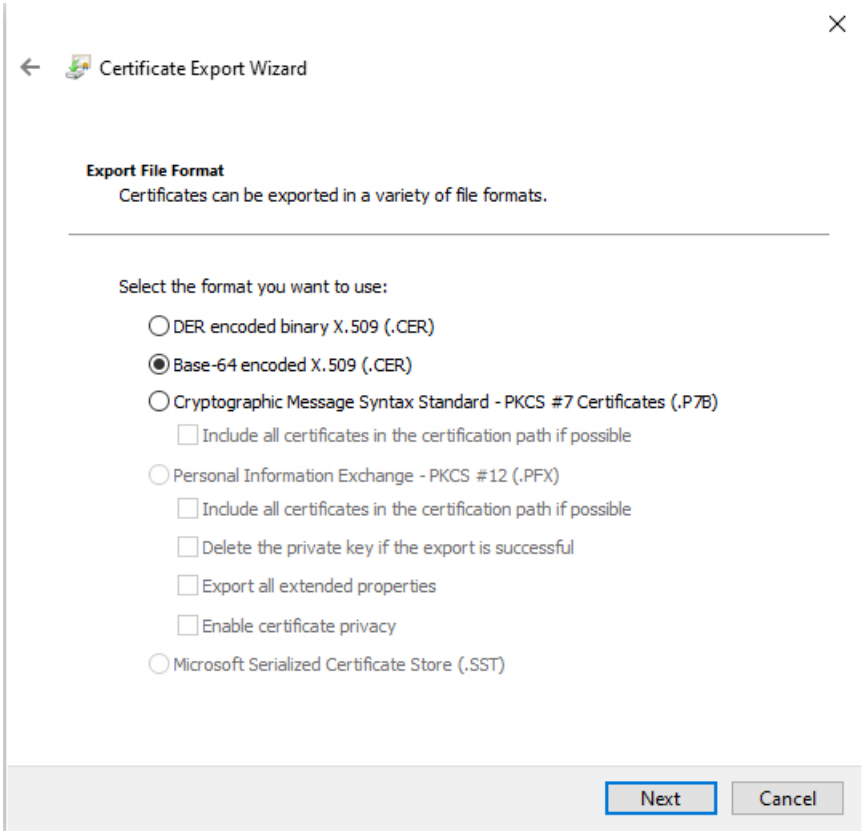
証明書チェーンの取得：Windows Chrome

Windows で Chrome ブラウザを使用して証明書チェーンを取得するには、この手順を使用します。

1. Chrome を使用して vCenter または Firewall Management Center にログインします。

2. ブラウザのアドレスバーで、ホスト名の左側にあるロックをクリックします。
3. [証明書（Certificate）] をクリックします。
4. [証明のパス（Certification Path）] タブをクリックします。
5. チェーンの最上位（つまり、最初）の証明書をクリックします。
6. **証明書の表示**をクリックします。
7. [詳細（Details）] タブをクリックします。
8. [ファイルにコピーする（Copy to File）] をクリックします。
9. プロンプトに従って、証明書チェーン全体を含むCER形式の証明書ファイルを作成します。

   エクスポートファイル形式の選択を求められたら、次の図に示すように、[Base 64 エンコード X.509（.CER）（Base 64-Encoded X.509 (.CER)）] をクリックします。



10. 指示に従ってエクスポートを完了します。
11. 証明書をテキストエディタで開きます。
12. チェーン内のすべての証明書に対してこのプロセスを繰り返します。

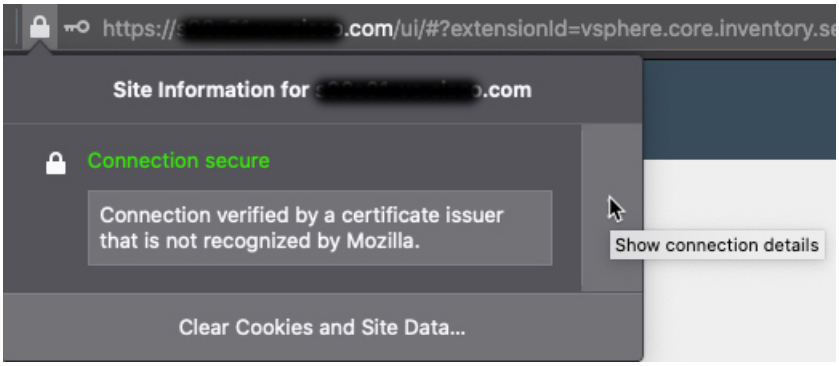
    テキストエディタに各証明書を最初から最後まで順番に貼り付ける必要があります。

13. vCenter または Firewall Management Center に対してこれらのタスクを繰り返します。

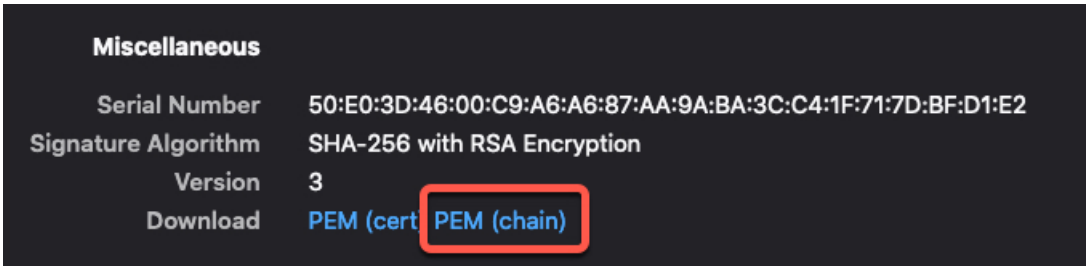
証明書チェーンの取得：Windows Firefox

Windows または Mac OS で Firefox ブラウザの証明書チェーンを取得するには、次の手順を使用します。

1. Firefox を使用して vCenter または Firewall Management Center にログインします。
2. ホスト名の左側にあるロックをクリックします。
3. 右矢印（[接続の詳細を表示（Show connection details）]）をクリックします。次の図は例を示しています。



4. [詳細（More Information）] をクリックします。
5. **証明書の表示**をクリックします。
6. 結果のダイアログボックスにタブページがある場合は、最上位 CA に対応するタブページをクリックします。
7. [その他（Miscellaneous）] セクションまでスクロールします。
8. [ダウンロード（Miscellaneous）] 行の [PEM（チェーン）（PEM (chain)）] をクリックします。次の図は例を示しています。



9. ファイルを保存します。
10. vCenter または Firewall Management Center に対してこれらのタスクを繰り返します。

セキュリティ要件

dynamic attributes connectorを保護するには、保護された内部ネットワークにそれをインストールしてください。dynamic attributes connectorは、使用可能なサービスとポートのうち必要なもののみを持つように設定されていますが、攻撃が到達できないように確保する必要があります。

dynamic attributes connector と Secure Firewall Management Center が同じネットワーク上に存在している場合は、Secure Firewall Management Center を dynamic attributes connector と同じ保護された内部ネットワークに接続することができます。

アプライアンスの展開方法に関係なく、システム間通信は暗号化されます。それでも、分散型サービス拒否（DDoS）や中間者攻撃などの手段でアプライアンス間の通信が中断、ブロック、または改ざんされないよう何らかの対策を講じる必要があります。

インターネット アクセス要件

デフォルトでは、dynamic attributes connector は、ポート 443/tcp（HTTPS）で HTTPS を使用してインターネット経由で Firepower システムと通信するように構成されています。dynamic attributes connector がインターネットに直接アクセスしないようにするために、プロキシサーバーを構成できます。

次の情報により、Secure Firewall Management Center および外部サーバーとの通信に dynamic attributes connector が使用する URL が通知されます。

表 *3 : Dynamic Attributes Connector* アクセス要件

URL	理由
https://*fmc-ip*/**api/fmc_platform/v1/auth/generatetoken**	認証
https://*fmc-ip*/**api/fmc_config/v1/domain/***domain-id*/**object/dynamicobjects**	GET および POST ダイナミックオブジェクト
https://*fmc-ip*/**api/fmc_config/ v1/domain/***domain-id*/**object/dynamicobjects/***object-id*/**mappings?action=add**	マッピングを追加します
https://*fmc-ip*/**api/fmc_config/v1/domain/***domain-id* **/object/dynamicobjects/***object-id*/**mappings?action=remove**	マッピングを削除します

表 *4 : Dynamic Attributes Connector vCenter* アクセス要件

URL	理由
https://*vcenter-ip*/**rest/com/vmware/cis/session**	認証

URL	理由
https://*vcenter-ip***/rest/vcenter/vm**	VM 情報を取得します
https://*nsx-ip***/api/v1/fabric/virtual-machines/***vm-id***	仮想マシンに関連付けられた NSX-T タグを取得します

DockerHub から Amazon ECR への移行

Dynamic Attributes Connector の Docker イメージは、Docker Hub [英語] から Amazon Elastic Container Registry（Amazon ECR）に移行されています。

新しいフィールドパッケージを使用するには、ファイアウォールまたはプロキシから次のすべての URL へのアクセスを許可する必要があります。

- https://public.ecr.aws
- https://csdac-cosign.s3.us-west-1.amazonaws.com
- https://d2glxqk2uabbnd.cloudfront.net
- https://d5l0dvt14r5h8.cloudfront.net

  Amazon CloudFront URL の詳細については、 EKS Anywhere の ドキュメントを参照してください。

Dynamic Attributes Connector Azure のアクセス要件

dynamic attributes connector は、組み込みの SDK メソッドを呼び出してインスタンス情報を取得します。これらのメソッドは、https://login.microsoft.com（認証用）と https://management.azure.com（インスタンス情報の取得用）を内部的に呼び出します。

Dynamic Attributes Connector の履歴

機能	Minimum Firewall Management Center	Minimum Firewall Threat Defense	詳細
新しいコネクタ	7.6	7.6	AWS セキュリティグループ、AWS サービスタグ、および Cisco Cyber Vision これらのコネクタは、Security Cloud Control と同様に、オンプレミスの Secure Firewall Management Center ダイナミックオブジェクトを送信できます。 オンプレミスの dynamic attributes connector からダイナミックオブジェクトを受信するには、オンプレミスのダイナミック属性コネクタのバージョン 3.0 が必要です。

機能	Minimum Firewall Management Center	Minimum Firewall Threat Defense	詳細
Dynamic Attributes Connector	7.4.0	7.4.0	この機能が導入されます。 Dynamic Attributes Connector が Secure Firewall Management Center に含まれるようになりました。dynamic attributes connector を使用すると、管理対象デバイスに展開することなく、アクセス制御ルールでMicrosoft Azure などのクラウドベースのプラットフォームから IP アドレスを取得できます。 詳細情報： • この製品に含まれる dynamic attributes connector：Dynamic Attributes Connector について （1 ページ） • スタンドアロン dynamic attributes connector：*Cisco Secure Dynamic Attributes Connector Configuration Guide* 新規/変更された画面：**Integration** > **Dynamic Attributes Connector**

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。