Cisco Secure 動的属性コネクタ

次のトピックでは、Cisco Secure 動的属性コネクタ を設定および使用する方法について説明します。

Cisco Secure 動的属性コネクタ について

動的属性コネクタ により、さまざまなクラウド サービス プラットフォームのサービスタグとカテゴリを Secure Firewall Management Center アクセス制御ルールで使用できます。

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 : Cisco Secure* 動的属性コネクタ 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/プラットフォーム	AWS	Azure	Azure サービスタグ	Cyber Vision	汎用テキスト	GitHub	Google クラウド	Microsoft Office 365	vCenter	Webex	Zoom
バージョン 1.1（オンプレミス）	対応	対応	対応	×	×	×	×	対応	対応	×	×
バージョン 2.0（オンプレミス）	対応	対応	対応	×	×	×	対応	対応	対応	×	×
バージョン 2.2（オンプレミス）	対応	対応	対応	×	×	対応	対応	対応	対応	×	×
バージョン 2.3（オンプレミス）	対応	対応	対応	×	×	対応	対応	対応	対応	対応	対応
クラウド提供型（Cisco Defense Orchestrator）	対応	対応	対応	×	×	対応	対応	対応	×	×	×
Secure Firewall Management Center 7.4.1	対応	対応	対応	×	対応	対応	対応	対応	対応	対応	対応

コネクタの詳細は次のとおりです。

- Amazon Web Services（AWS）

  詳細については、Amazon ドキュメントサイトの「AWS リソースのタグ付け」などのリソースを参照してください。

  「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 （16 ページ）」を参照してください。

- Microsoft Azure

  詳細については、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。

  「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 （19 ページ）」を参照してください。

- Microsoft Azure サービスタグ

詳細については、Microsoft TechNet の「仮想ネットワークサービスタグ」などのリソースを参照してください。

- 指定した IP アドレスの汎用テキストリスト。

  詳細については、汎用テキストコネクタの作成 （25 ページ）を参照してください。

- Google クラウド

  詳細については、 Google Cloud ドキュメントの「環境設定」を参照してください。

- Office 365 の IP アドレス

  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。

- vCenter と NSX-T によって管理される VMware のカテゴリとタグ

  詳細については、VMware ドキュメントサイトの「vSphere タグと属性」などのリソースを参照してください。

- Webex の IP アドレス

  詳細については、Webex コネクタの作成 （34 ページ）を参照してください。

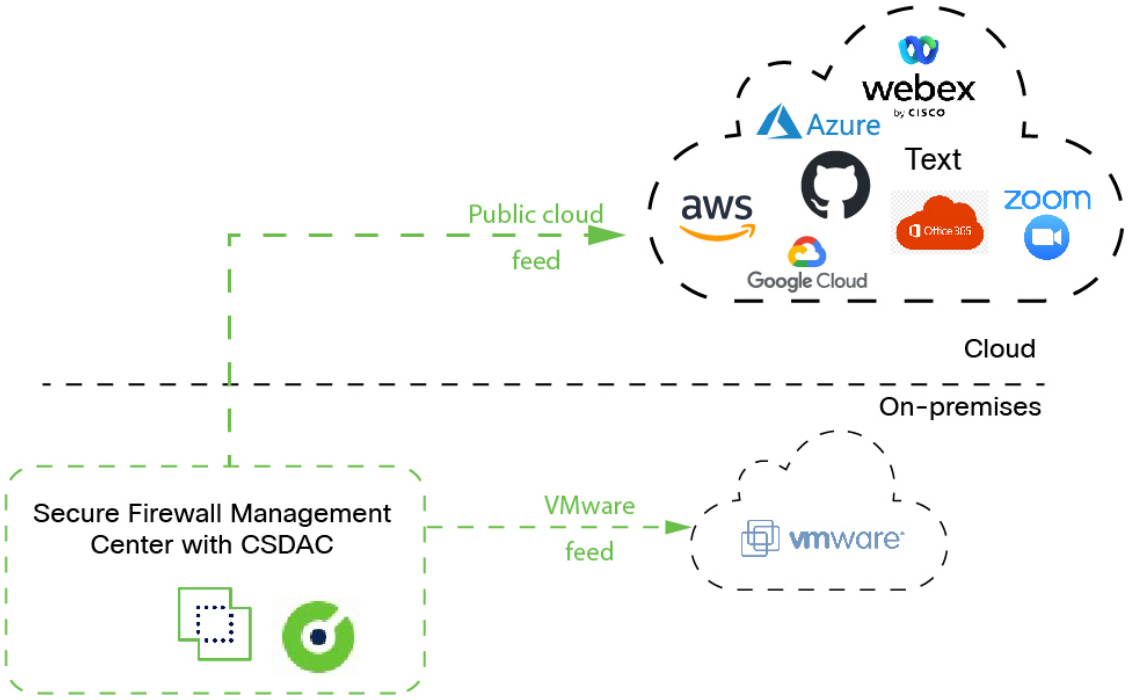
- Zoom の IP アドレス

  詳細については、Zoom コネクタの作成 （35 ページ）を参照してください。

機能の仕組み

ワークロードの動的な性質とIPアドレスの重複の必然性により、IPアドレスなどのネットワーク構造は、仮想、クラウド、およびコンテナ環境では信頼できません。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。

関連項目

- Cisco Secure 動的属性コネクタ の有効化 （5 ページ）
- ダッシュボードについて （9 ページ）

Cisco Secure 動的属性コネクタ の履歴

機能	最小 Management Center	最小 Threat Defense	詳細

機能	最小 Management Center	最小 Threat Defense	詳細
Cisco Secure 動的属性コネクタ	7.4.0	7.4.0	この機能が導入されます。 Cisco Secure 動的属性コネクタ が Secure Firewall Management Center に含まれるようになりました。動的属性コネクタを使用すると、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 動的属性コネクタ：Cisco Secure 動的属性コネクタ について （1 ページ） • スタンドアロン 動的属性コネクタ：Cisco Secure 動的属性コネクタ コンフィギュレーション ガイド 新規/変更された画面：**[統合（Integration）] > [Cisco動的属性コネクタ（Cisco Dynamic Attributes Connector）]**

Cisco Secure 動的属性コネクタ のシステム要件

Cisco Secure 動的属性コネクタ 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）
32GB 以上	Firepower 1000、Firepower 1600、vFMC	10
64GB 以上	Firepower 2500、Firepower 2600、vFMC 300	20
128GB 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。

Cisco Secure 動的属性コネクタ の有効化

このタスクでは、Secure Firewall Management Center で Cisco Secure 動的属性コネクタ を有効にする方法について説明します。動的属性コネクタ は、クラウドネットワーキング製品のオブジェクトを Management Center アクセスコントロール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 **[統合（Integration）] > [Cisco動的属性コネクタ（Cisco 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 動的属性コネクタ 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

Cisco Secure 動的属性コネクタ 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

動的属性コネクタ 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、動的属性コネクタ 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 動的属性コネクタ コネクタで使用される Docker ブリッジネットワーク。

動的属性コネクタ を有効にする前は、172.18.0.1/16 に設定されている `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。

Docker ネットワークとサブネットの変更

まず 動的属性コネクタ を有効にします（Cisco Secure 動的属性コネクタ 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 動的属性コネクタ コネクタで使用され、それらの制限は Cisco Secure 動的属性コネクタ のシステム要件 （5 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 Cisco Secure 動的属性コネクタ 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
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

Secure Firewall Management Center モデル	推奨される -s 値	-b 値の例	使用される Cisco Secure 動的属性コネクタ コンテナアドレス
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）**

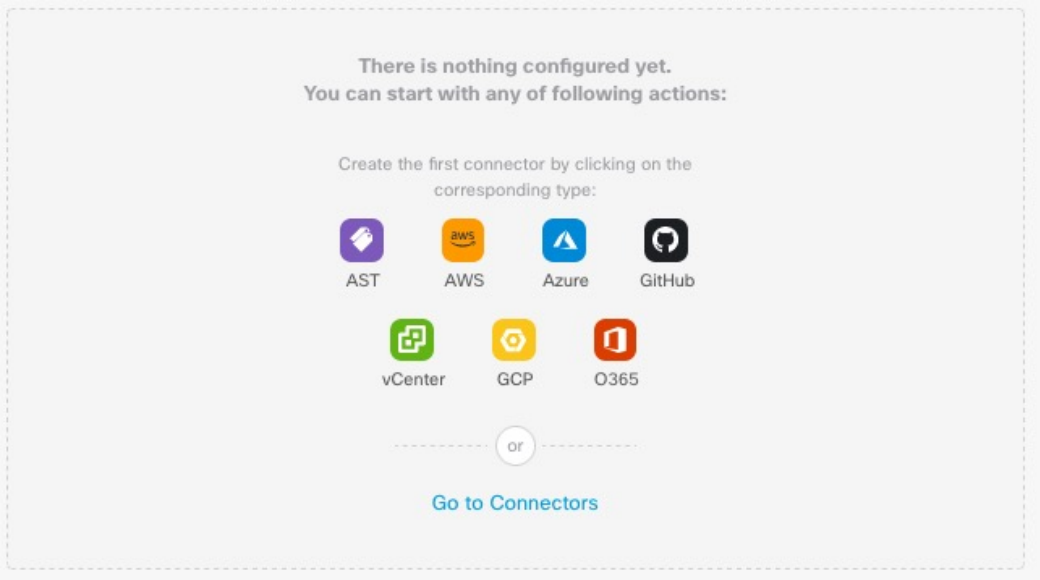
解決策：`-s` の値を変更して、0 より大きく、かつ 32 未満になるようにします。

ダッシュボードについて

Cisco Secure 動的属性コネクタ ダッシュボードにアクセスするには、Cisco Secure Firewall マネージャにログインし、ページの上部にある **[統合（Integration）]** > **[Cisco動的属性コネクタ（Cisco Dynamic Attributes Connector）]** をクリックします

Cisco Secure 動的属性コネクタ 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。

Cisco Secure 動的属性コネクタ 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。

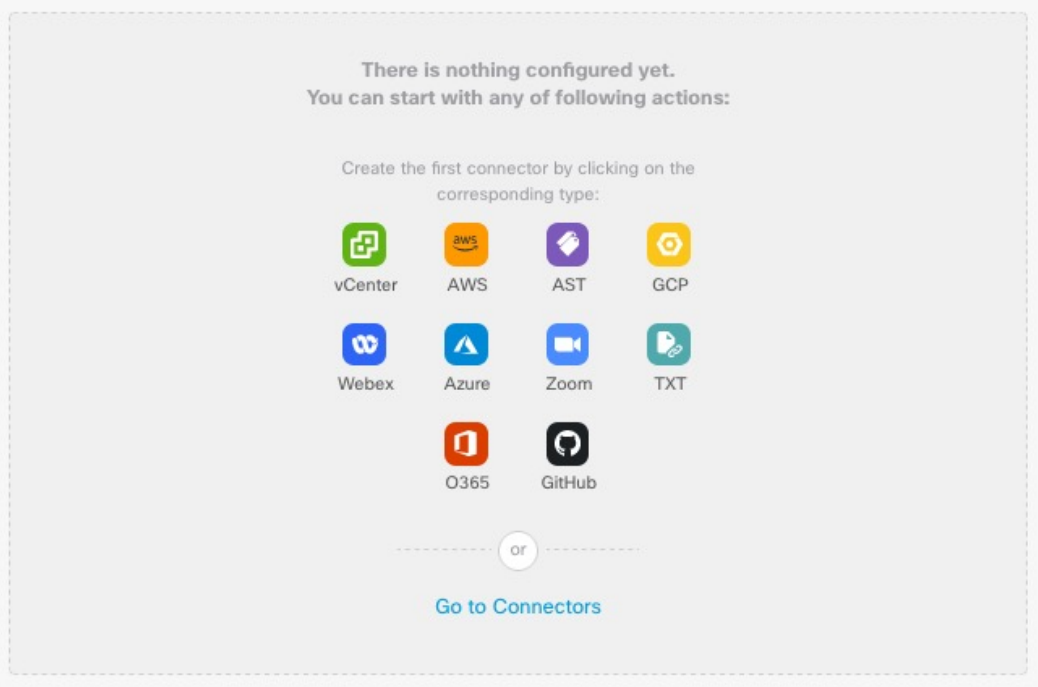
- コネクタ動的属性フィルタ、およびを追加、編集、および削除します。
- コネクタ動的属性フィルタ 、 および の相互関係を確認します。
- 警告およびエラーを表示します。

関連項目

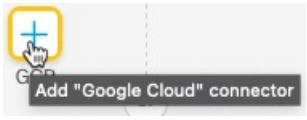
- 設定されていないシステムのダッシュボード （10 ページ）
- 設定済みシステムのダッシュボード （10 ページ）
- コネクタの追加、編集、削除 （12 ページ）
- 動的属性フィルタの追加、編集、削除 （14 ページ）

設定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 Cisco Secure 動的属性コネクタ 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、「コネクタの作成 （15 ページ）」を参照してください。

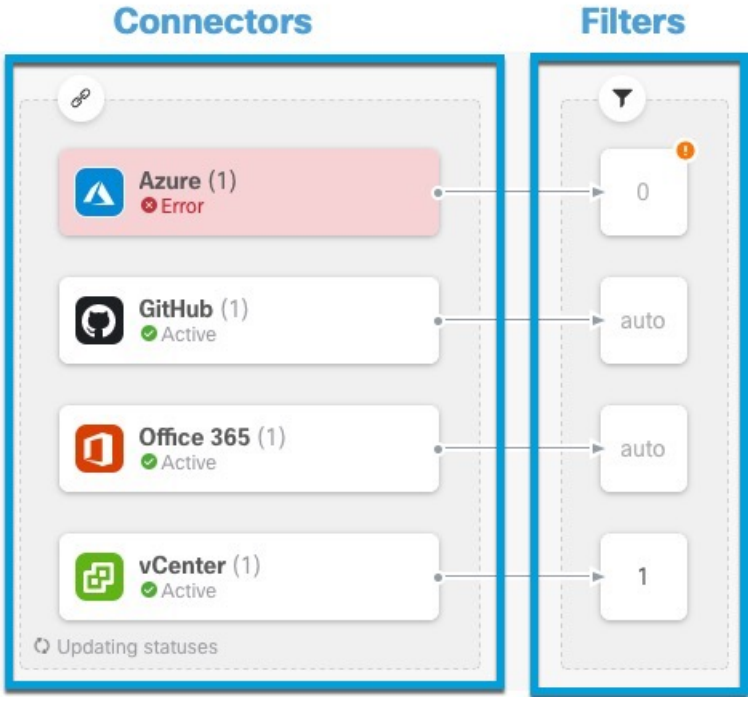
関連トピック：

- 設定済みシステムのダッシュボード （10 ページ）
- コネクタの追加、編集、削除 （12 ページ）
- 動的属性フィルタの追加、編集、削除 （14 ページ）

設定済みシステムのダッシュボード

設定済みシステムの Cisco Secure 動的属性コネクタ 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 コネクタの作成 （15 ページ）
2 動的属性フィルタの作成 （36 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、コネクタの追加、編集、削除 （12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、「動的属性フィルタの追加、編集、削除 （14 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 **[更新（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：

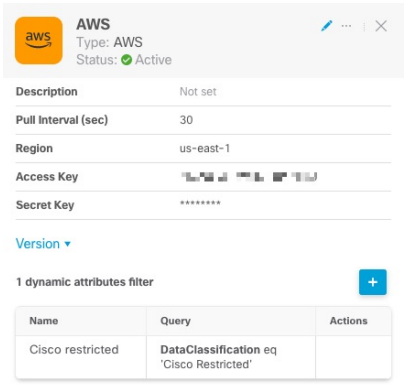
- コネクタの追加、編集、削除 （12 ページ）
- 動的属性フィルタの追加、編集、削除 （14 ページ）

コネクタの追加、編集、削除

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。

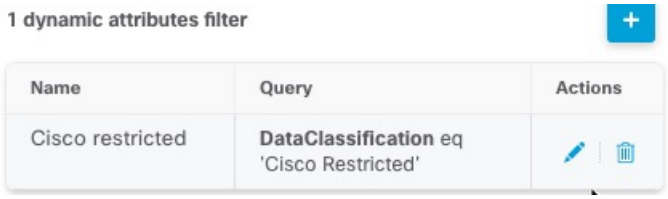
コネクタ列のコネクタ（）をクリックすると、そのコネクタに関する詳細情報が表示されます。以下に例を示します。



次の選択肢があります。

- [Edit] アイコン（ ）をクリックしてこのコネクタを編集する。
- [詳細情報（More）] アイコン（ アイコン）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 動的属性コネクタ 削除できます。以下に例を示します。



[追加（Add）] アイコン（ ）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、「動的属性フィルタの作成 （36 ページ）」を参照してください。

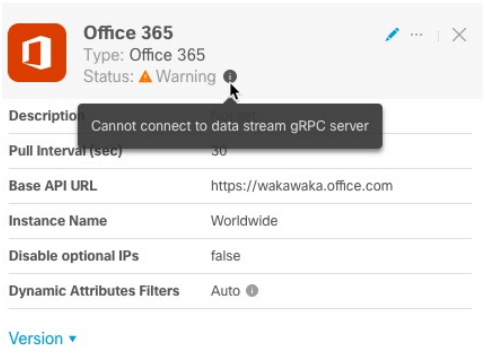
指定されたコネクタを編集または削除するには、[アクション（Actions）] 列にマウスポインタを合わせます。

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 **[情報（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 コネクタの作成 （30 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。

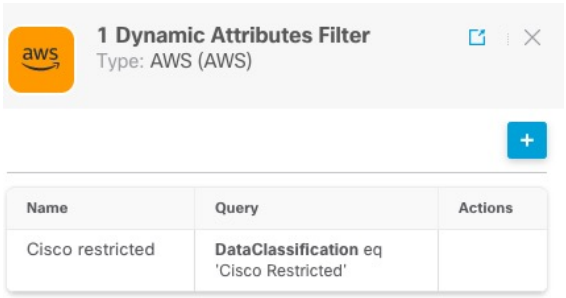
動的属性フィルタの追加、編集、削除

ダッシュボードでは、動的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、動的属性フィルタの作成 （36 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。

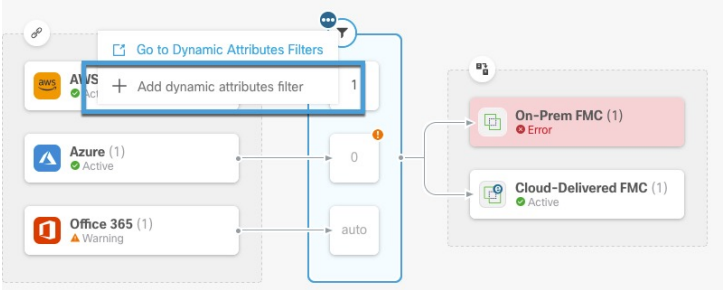
次の選択肢があります。

- 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。
- [追加（Add）] アイコン（  ） 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、「動的属性フィルタの作成 （36 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 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。

コネクタの作成

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ため、management center のアクセス コントロール 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 : Cisco Secure* 動的属性コネクタ 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/プラットフォーム	AWS	Azure	Azure サービスタグ	Cyber Vision	汎用テキスト	GitHub	Google クラウド	Microsoft Office 365	vCenter	Webex	Zoom
バージョン 1.1（オンプレミス）	対応	対応	対応	×	×	×	×	対応	対応	×	×
バージョン 2.0（オンプレミス）	対応	対応	対応	×	×	×	対応	対応	対応	×	×

CSDAC バージョン/プラットフォーム	AWS	Azure	Azure サービスタグ	Cyber Vision	汎用テキスト	GitHub	Google クラウド	Microsoft Office 365	vCenter	Webex	Zoom
バージョン 2.2（オンプレミス）	対応	対応	対応	×	×	対応	対応	対応	対応	×	×
バージョン 2.3（オンプレミス）	対応	対応	対応	×	×	対応	対応	対応	対応	対応	対応
クラウド提供型（Cisco Defense Orchestrator）	対応	対応	対応	×	×	対応	対応	対応	×	×	×
Secure Firewall Management Center 7.4.1	対応	対応	対応	×	対応	対応	対応	対応	対応	対応	対応

詳細については、次の項を参照してください。

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

Cisco Secure 動的属性コネクタ は、アクセス コントロール ポリシーで使用するために AWS から management center に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

Cisco Secure 動的属性コネクタ 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。

Cisco Secure 動的属性コネクタ 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 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。これは後で行います。

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。

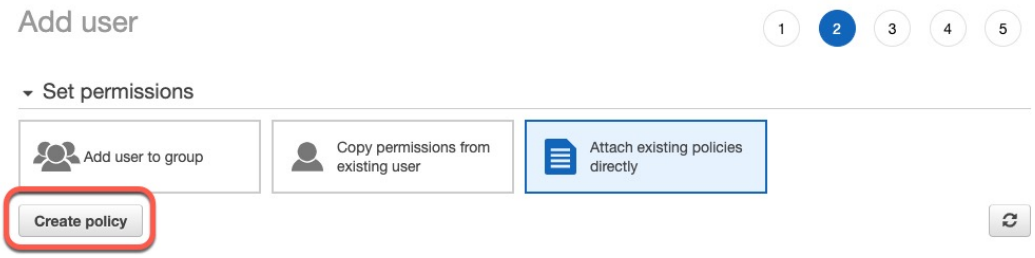
（注） これが、ユーザーのキーを取得する必要がある唯一の機会です。

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、アクセス コントロール ポリシーで使用するため、AWS から management center にデータを送信するコネクタを設定する方法について説明します。

始める前に

Cisco Secure 動的属性コネクタ に対して最小限の権限を持つ AWS ユーザーを作成します。（17 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 management center にログインします。

ステップ 2 **[統合（Integration）]** > **[Cisco動的属性コネクタ（Cisco Dynamic Attributes Connector）]** をクリックします。

ステップ 3 [コネクタ（Connectors）] をクリックします。

ステップ 4 次のいずれかを実行します。

- 新しいコネクタの追加：[追加（Add）] アイコン（ ） 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：**その他** （ ） 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 5 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 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。

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

Cisco Secure 動的属性コネクタ は、アクセス コントロール ポリシーで使用するために、Azure から 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

Cisco Secure 動的属性コネクタ 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。

Cisco Secure 動的属性コネクタ 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 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 （19 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。

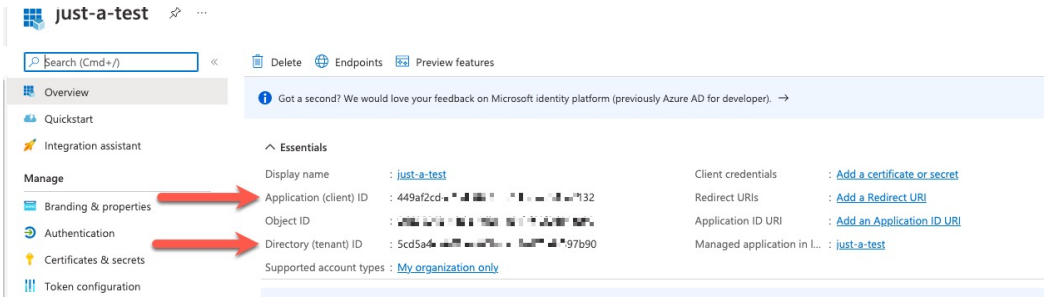
ステップ 5 [名前（Name）] フィールドに、このアプリケーションを識別するための名前を入力します。

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。

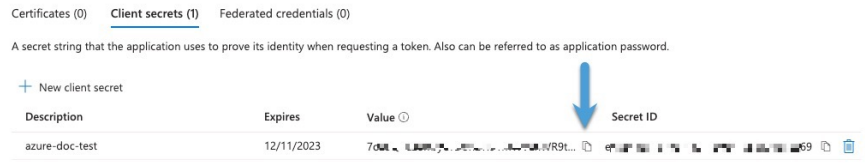


ステップ 9 [クライアントクレデンシャル（Client Credentials）] の横にある [証明書またはシークレットの追加（Add a certificate or secret）] をクリックします。

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。

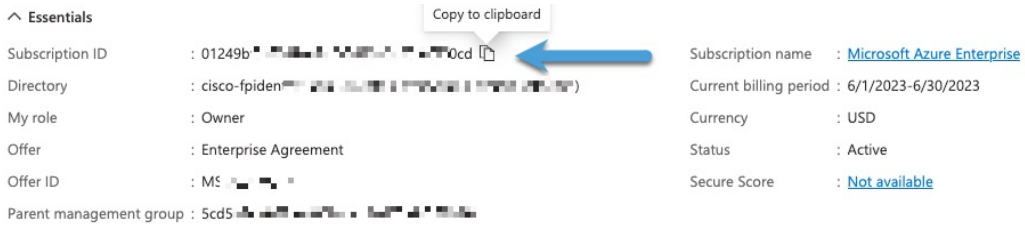
ステップ 12 [値（Value）] フィールドの値をクリップボードにコピーします。[シークレットID（Secret ID）] ではなく、この値がクライアントシークレットです。



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。



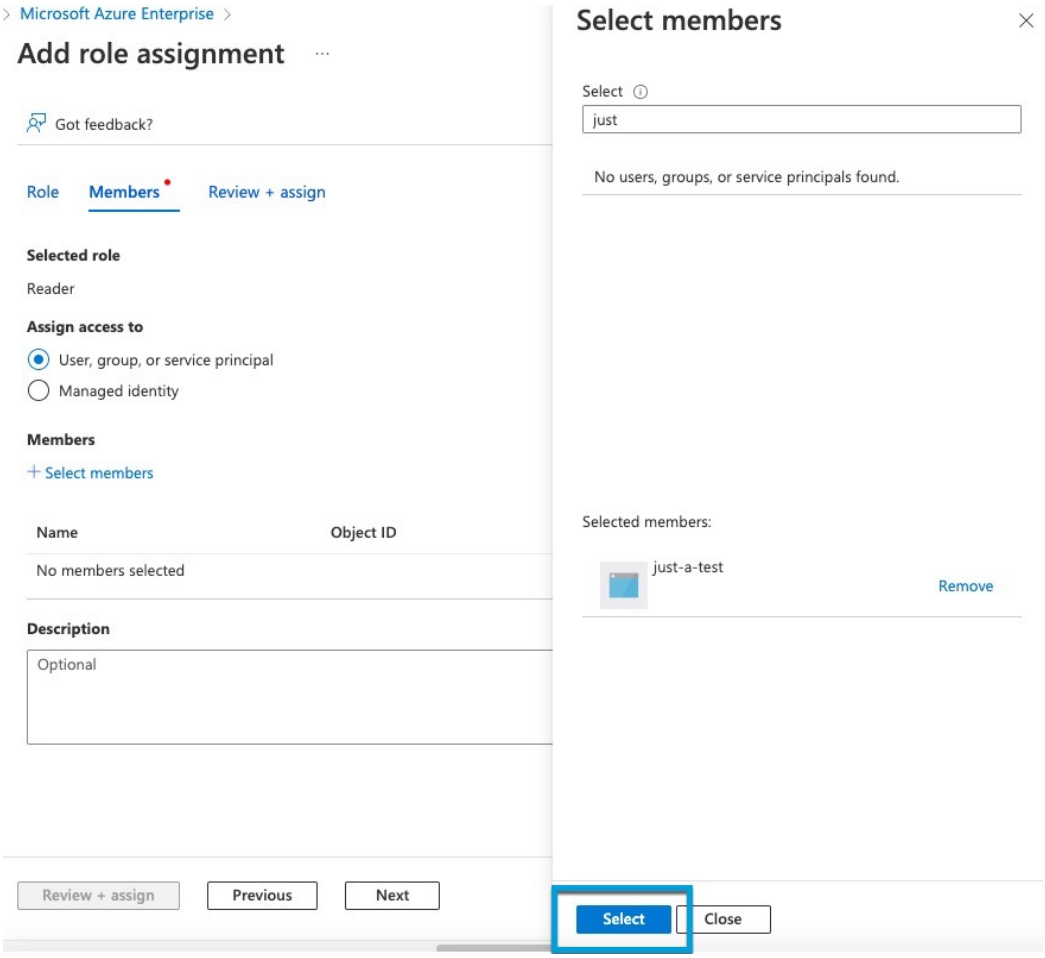
ステップ 16 [アクセス制御（IAM）（Access Control (IAM)）] をクリックします。

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 （22 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、アクセス コントロール ポリシーで使用するために Azure から 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

Cisco Secure 動的属性コネクタ に対する最小限の権限を持つ Azure ユーザーの作成 （20 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 management center にログインします。

ステップ 2 **[統合（Integration）]** > **[Cisco動的属性コネクタ（Cisco Dynamic Attributes Connector）]** をクリックします。

ステップ 3 [コネクタ（Connectors）] をクリックします。

ステップ 4 次のいずれかを実行します。

- 新しいコネクタの追加：[追加（Add）] アイコン（ ） 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：**その他**（ ） 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 5 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。
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 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。

Azure サービスタグコネクタの作成

このトピックでは、アクセス コントロール ポリシーで使用する 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 management center にログインします。

ステップ 2 **[統合（Integration）] > [Cisco動的属性コネクタ（Cisco Dynamic Attributes Connector）]** をクリックします。

ステップ 3 [コネクタ（Connectors）] をクリックします。

ステップ 4 次のいずれかを実行します。

- 新しいコネクタの追加：[追加（Add）] アイコン（ ） 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：**その他**（ ） 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 5 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。
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 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の作成

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、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。

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。

（注） IP アドレスにスキーム（**http://** または **https://**）を含めないでください。

手順

ステップ 1 management center にログインします。

ステップ 2 **[統合（Integration）] > [Cisco動的属性コネクタ（Cisco Dynamic Attributes Connector）]** をクリックします。

ステップ 3 [コネクタ（Connectors）] をクリックします。

ステップ 4 次のいずれかを実行します。

- 新しいコネクタの追加：[追加（Add）] アイコン（ ） 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：**その他**（ ） 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 5 [名前（Name）] とオプションの [説明（Description）]を入力します。

ステップ 6 （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 30 秒です。

ステップ 7 [URL（URL）] フィールドに、IP アドレスを取得する各 URL を 1 行に 1 つずつ入力します。

ステップ 8 （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) チェーンの手動での取得 （39 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 9 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 10 [保存（Save）] をクリックします。

ステップ 11 [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 コネクタの作成

このセクションでは、アクセス コントロール ポリシーで使用するためにデータを 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 management center にログインします。

ステップ 2 **[統合（Integration）] > [Cisco動的属性コネクタ（Cisco Dynamic Attributes Connector）]** をクリックします。

ステップ 3 [コネクタ（Connectors）] をクリックします。

ステップ 4 次のいずれかを実行します。

- 新しいコネクタの追加：[追加（Add）] アイコン（ ） 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：**その他**（ ） 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 5 [名前（Name）] とオプションの [説明（Description）]を入力します。

ステップ 6 （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 7 [保存（Save）] をクリックします。

ステップ 8 [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

Cisco Secure 動的属性コネクタは、アクセス コントロール ポリシーで使用するために、Google Cloud から 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

Cisco Secure 動的属性コネクタ 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。 >

Cisco Secure 動的属性コネクタ 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 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 （27 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。 >

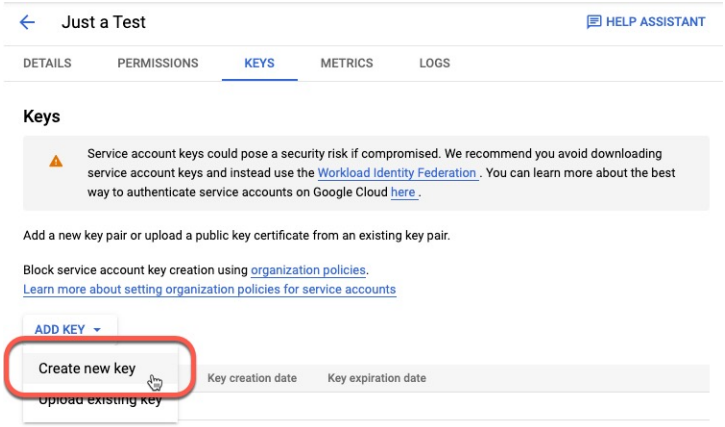
ステップ 7 [完了（Done）] をクリックします。

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 **その他**（⋮） 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 （29 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 management center にログインします。

ステップ 2 **[統合（Integration）]** > **[Cisco動的属性コネクタ（Cisco Dynamic Attributes Connector）]** をクリックします。

ステップ 3 [コネクタ（Connectors）] をクリックします。

ステップ 4 次のいずれかを実行します。

- 新しいコネクタの追加：[追加（Add）] アイコン（ ） 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：**その他**（ ） 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 5 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。
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 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。

Office 365 コネクタの作成

このタスクでは、アクセス コントロール ポリシーで使用するためのデータを 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 management center にログインします。

ステップ 2 **[統合（Integration）] > [Cisco動的属性コネクタ（Cisco Dynamic Attributes Connector）]** をクリックします。

ステップ 3 [コネクタ（Connectors）] をクリックします。

ステップ 4 次のいずれかを実行します。

- 新しいコネクタの追加：[追加（Add）] アイコン（ ） 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：**その他**（ ） 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 5 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。
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 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。

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

Cisco Secure 動的属性コネクタは、アクセス コントロール ポリシーで使用するために、vCenter から 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

Cisco Secure 動的属性コネクタ 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。

vCenter コネクタの作成

このタスクでは、アクセス コントロール ポリシーで使用するためにデータを 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。

手順

ステップ 1 management center にログインします。

ステップ 2 **[統合（Integration）]** > **[Cisco動的属性コネクタ（Cisco Dynamic Attributes Connector）]** 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。

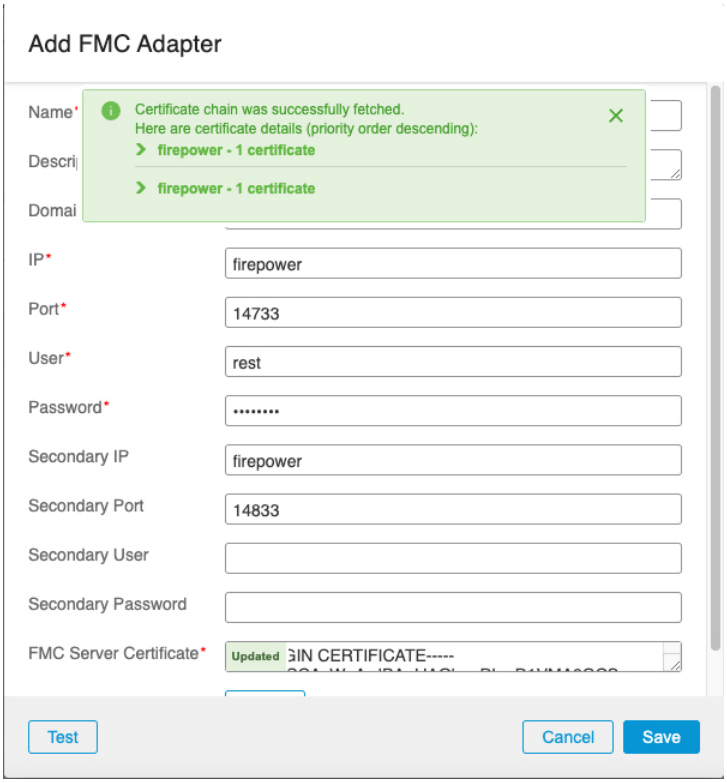
- 新しいコネクタの追加：[追加（Add）] アイコン（ ） をクリックしてから、コネクタの名前をクリックします。
- コネクタの編集または削除：**その他**（ ） をクリックしてから、行の末尾にある [編集（Edit）] または [削除（Delete）] をクリックします。

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。
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) チェーンの手動での取得 （39 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) チェーンの手動での取得 （39 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) チェーンの手動での取得 （39 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) チェーンの手動での取得 （39 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 コネクタの作成

このセクションでは、アクセス コントロール ポリシーで使用するためにデータを 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 management center にログインします。

ステップ 2 **[統合（Integration）] > [Cisco動的属性コネクタ（Cisco Dynamic Attributes Connector）]** をクリックします。

ステップ 3 [コネクタ（Connectors）] をクリックします。

ステップ 4 次のいずれかを実行します。

- 新しいコネクタの追加：[追加（Add）] アイコン（ ） 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：**その他**（ ） 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 5 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）Webex から IP マッピングを取得する間隔です。

値	説明
[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 6 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 7 [保存（Save）] をクリックします。

ステップ 8 [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、アクセス コントロール ポリシーで使用するためにデータを 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 management center にログインします。

ステップ 2 **[統合（Integration）] > [Cisco動的属性コネクタ（Cisco Dynamic Attributes Connector）]** をクリックします。

ステップ 3 [コネクタ（Connectors）] をクリックします。

ステップ 4 次のいずれかを実行します。

- 新しいコネクタの追加：[追加（Add）] アイコン（ ） 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：**その他**（ ） 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 5 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。

値	説明
[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 6 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 7 [保存（Save）] をクリックします。

ステップ 8 [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。

動的属性フィルタの作成

Cisco Secure 動的属性コネクタ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 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 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。

アクセス制御ルールの詳細については、動的属性フィルタを使用したアクセス制御ルールの作成 （43 ページ）を参照してください。

始める前に

コネクタの作成 （15 ページ）

手順

ステップ 1 management center にログインします。

ステップ 2 **[統合（Integration）] > [Cisco動的属性コネクタ（Cisco Dynamic Attributes Connector）]** をクリックします。

ステップ 3 [Dynamic Attributes Filters（ダイナミック属性フィルタ）] をクリックします。

- 新しいコネクタの追加：[追加（Add）] アイコン（ ） 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：**その他**（ ） 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）	アクセス コントロール ポリシーおよび management center オブジェクトマネージャ（**[外部属性（External Attributes）]** > **[ダイナミックオブジェクト（Dynamic Object）]**）で動的フィルタを(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。
クエリ（Query）	• 新しいフィルタの追加：[追加（Add）]アイコン（）をクリックします。 • フィルタの編集または削除：**その他**（）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 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）management center のダイナミックオブジェクトを確認します。

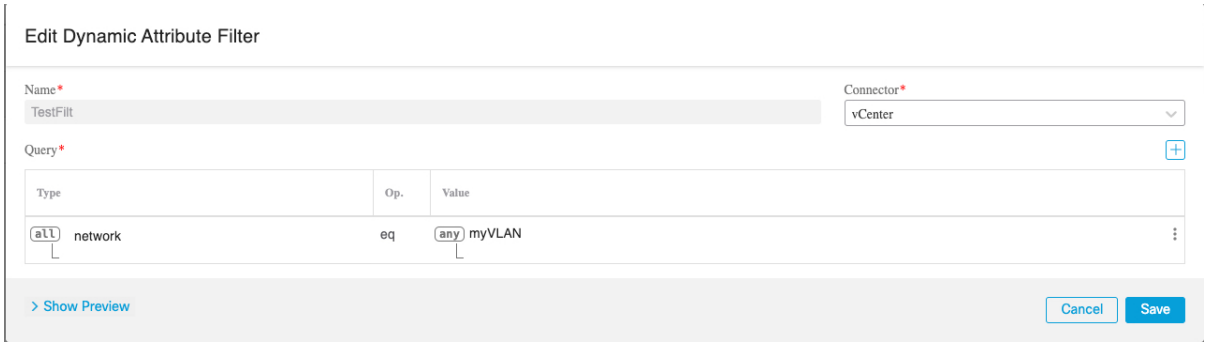
a) 最低限でもネットワーク管理者ロールを持つユーザとして management center にログインします。
b) **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]** をクリックします。
c) 左側のペインで、**[外部属性（External Attributes）] > [ダイナミックオブジェクト（Dynamic Object）]** をクリックします。
作成した動的属性クエリは、ダイナミックオブジェクトとして表示されます。

動的属性フィルタの例

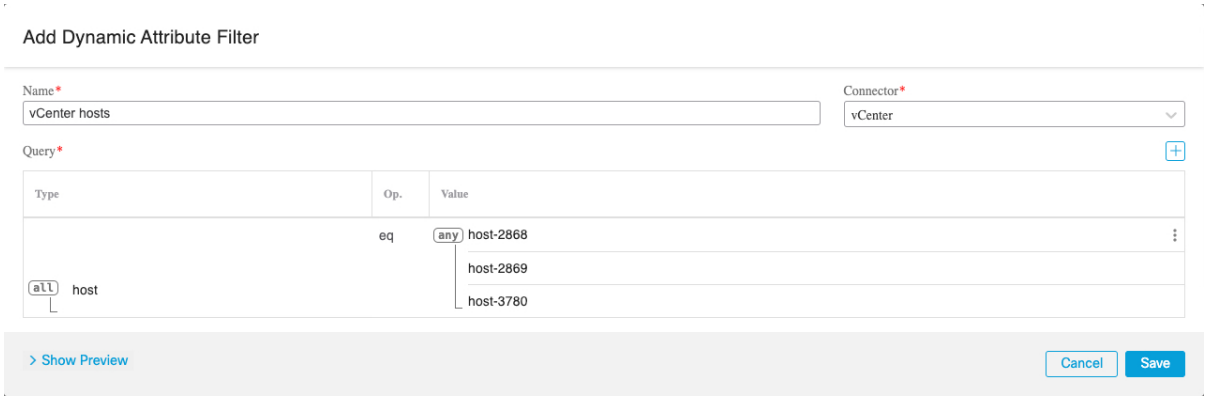
このトピックでは、動的属性フィルタの設定例をいくつか示します。

例：vCenter

次の例は、1 つの基準を示しています：VLAN。

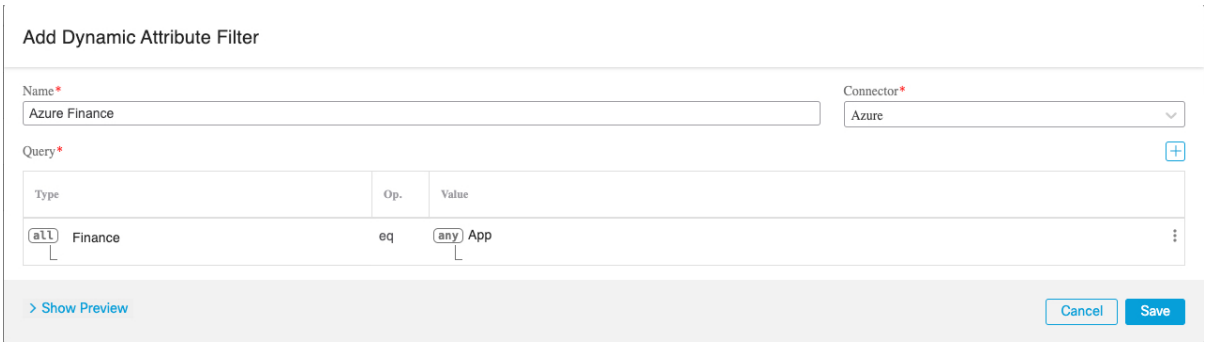


次の例は、OR で結合された 3 つの条件を示しています。クエリは 3 つのホストのいずれかに一致します。



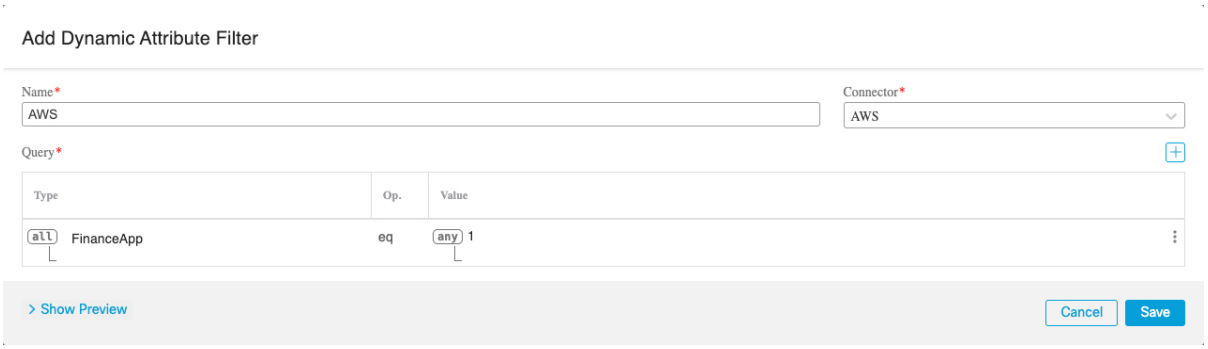
例：Azure

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) チェーンの手動での取得

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、NSX、または Management Center に安全に接続するために使用される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。

次に接続するには、これらの手順のいずれかを使用する必要があります。

- vCenter または NSX

  Azure または AWS に接続するために証明書チェーンを取得する必要はありません。

- 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、url は vCenter または Management Center への URL（スキームを含む）です。次に例を示します。

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

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

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

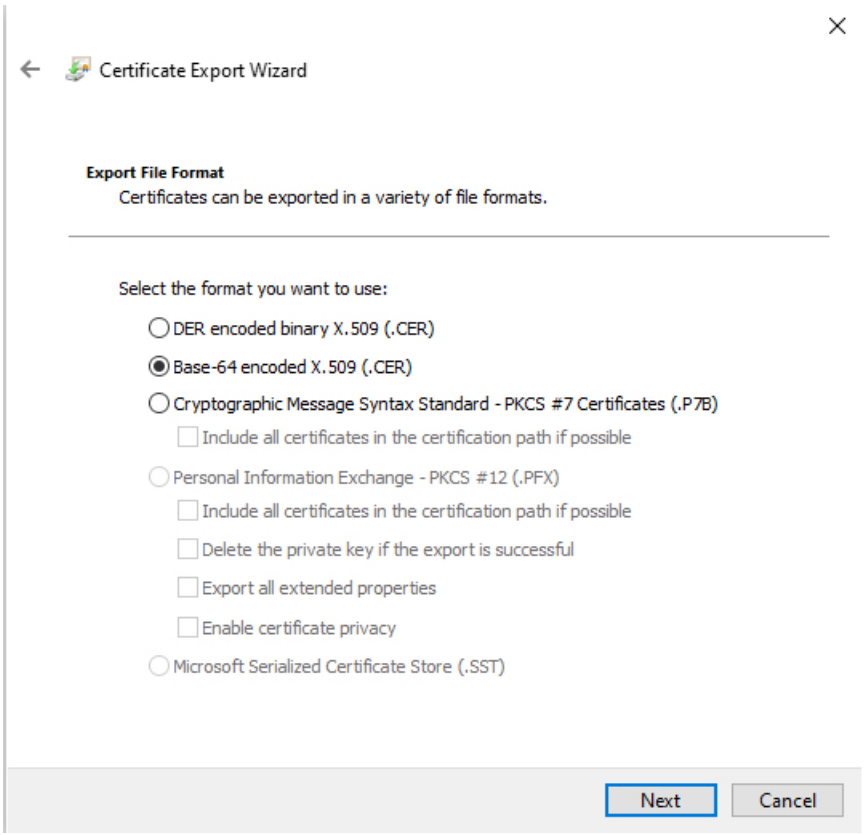
3. 証明書チェーン全体をプレーンテキストファイルに保存します。
   - すべての `-----BEGIN CERTIFICATE-----` および `-----END CERTIFICATE-----` 区切り文字を含めます。
   - 無関係なテキスト（たとえば、証明書の名前、山かっこ（<および>）に含まれるテキスト、および山かっこ自体を除外します。
4. vCenter と Management Center の両方で、これらのタスクを繰り返します。

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



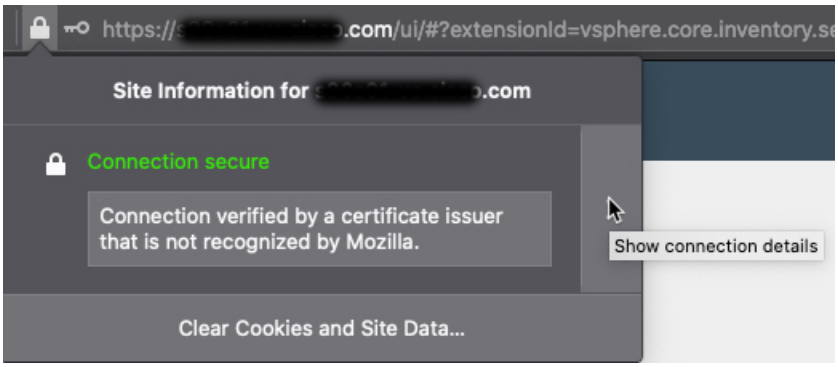
10. 指示に従ってエクスポートを完了します。
11. 証明書をテキストエディタで開きます。
12. チェーン内のすべての証明書に対してこのプロセスを繰り返します。

    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 と FMC の両方でこれらのタスクを繰り返します。

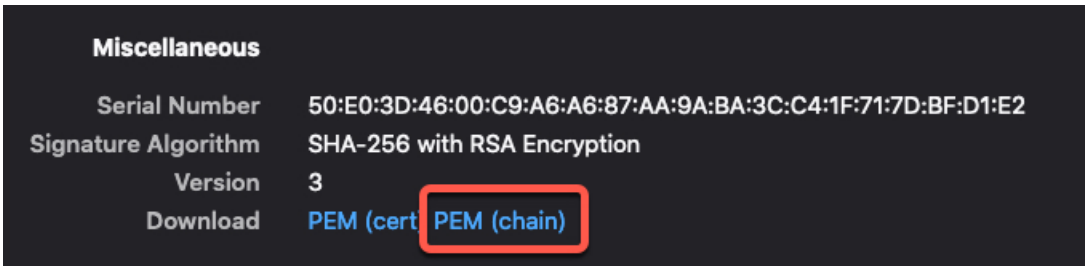
証明書チェーンの取得：Windows Firefox

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 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 と Management Center の両方で、これらのタスクを繰り返します。

アクセス コントロール ポリシーでのダイナミックオブジェクトの使用

動的属性コネクタ では、アクセス制御ルールで、ダイナミックオブジェクトとして management center に表示されるダイナミックフィルタを構成できます。

アクセス制御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 動的属性コネクタから定義済み Cisco Secure Firewall に自動的にプッシュされます。

ダイナミックオブジェクトは、セキュリティグループタグ（SGT）の使用方法と同様に、アクセス制御ルールの [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。

動的属性フィルタを使用したアクセス制御ルールの作成

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。

始める前に

動的属性フィルタの作成 （36 ページ）で説明されているように、動的属性フィルタを作成します。

（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 management center にログインします。

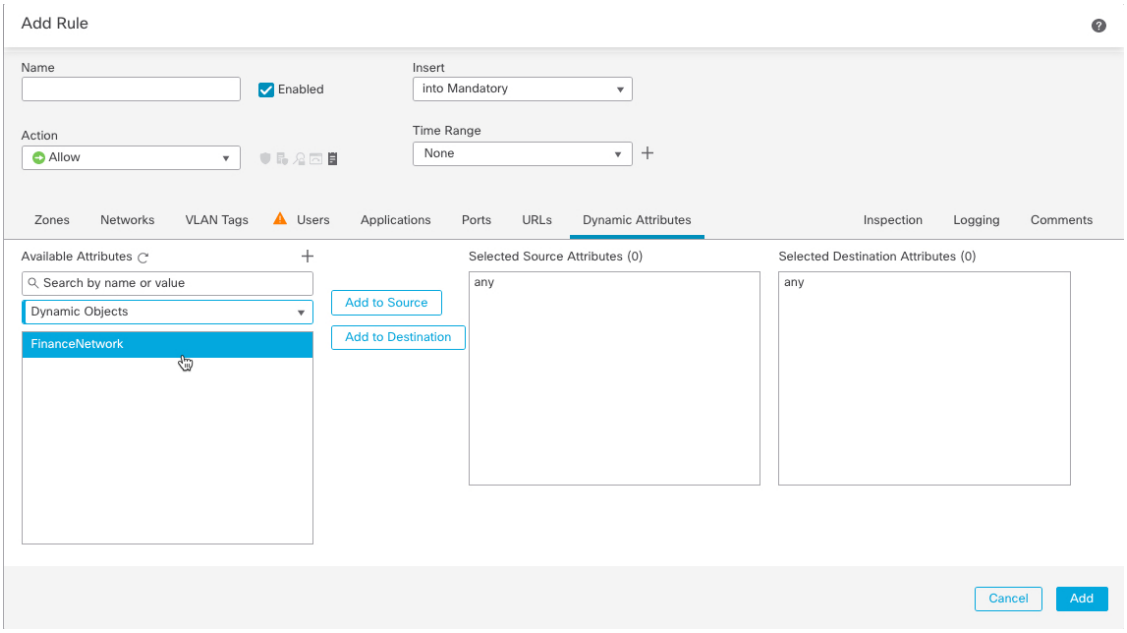
ステップ 2 アクセス コントロール ポリシーの横にある [編集（Edit）]（✎） をクリックします。

ステップ 3 [ルールの追加（Add Rule）] をクリックします。

ステップ 4 [動的属性（Dynamic Attributes）] タブをクリックします。

ステップ 5 [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。



前の例は、Cisco Secure 動的属性コネクタ で作成された動的属性フィルタに対応する `FinanceNetwork` 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 6 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 7 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

『*Cisco Secure Firewall Management Center* デバイス構成ガイド』の「アクセス制御」の章（章へのリンク）

Cisco Secure Dynamic Attributes コネクタの無効化

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 Cisco Secure 動的属性コネクタ 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 **[統合（Integration）] > [Cisco動的属性コネクタ（Cisco 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。

コマンドラインを使用したトラブルシューティング

高度なトラブルシューティングとCisco TACとの連携を支援するために、次のトラブルシューティング ツールを提供しています。これらのツールを使用するには、動的属性コネクタ が実行されているUbuntuホストに任意のユーザーとしてログインします。

コンテナステータスの確認

動的属性コネクタDockerコンテナのステータスを確認するには、次のコマンドを入力します。

```
cd /usr/local/sf/csdac
sudo ./muster-cli status
```

出力例を次に示します。

```
================================================ CORE SERVICES
================================================
          Name                          Command               State                    Ports

-------------------------------------------------------------------------------------------------------------
muster-bee                  /bin/sh -c /app/bee              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

muster-user-analysis        ./docker-entrypoint.sh run ...   Up      50070/tcp

============================ CONNECTORS AND ADAPTERS ============================
             Name                                Command               State     Ports
-------------------------------------------------------------------------------------
muster-connector-o365.1.muster   ./docker-entrypoint.sh run ...   Up      50070/tcp
```

動的属性コネクタ Docker コンテナの停止、起動、または再起動

./muster-cli status がコンテナが停止していることを示している場合、または問題が発生したときにコンテナを再起動するには、次のコマンドを入力できます。

停止と再起動：

```
cd ~/csdac/app
sudo ./muster-cli stop
sudo ./muster-cli start
```

起動のみ：

```
cd ~/csdac/app
sudo ./muster-cli start
```

アプリケーション デバッグ ロギングの有効化とトラブルシューティング ファイルの生成

Cisco TACから推奨された場合は、デバッグロギングを有効にして、次のようにトラブルシューティング ファイルを生成します。

```
cd ~/csdac/app
sudo ./muster-cli debug-on
sudo ./muster-cli ts-gen
```

トラブルシューティング ファイル名は **ts-bundle-***timestamp***.tar** で、同じディレクトリに作成されます。

次の表は、トラブルシューティング ファイルとトラブルシューティング ファイル内のログの場所を示しています。

ロケーション	内容
/csdac/app/ts-bundle-*timestamp***/info**	etcd データベース格納ファイル
/csdac/app/ts-bundle-*timestamp***/logs**	コンテナログファイル
/csdac/app/ts-bundle-*timestamp***/status.log**	コンテナのステータス、バージョン、およびイメージのステータス

コンテナのデバッグの有効化

次のように、最初にコンテナの名前を取得する場合は、オプションで個々のコンテナのデバッグを有効にすることができます。

```
cd /usr/local/sf/csdac
sudo ./muster-cli versions
```

出力例を次に示します。

```
CSDAC version: 1.0.0
CONTAINERS VERSIONS
CONTAINER                       | APP VERSION          | COMMIT
================================================================================
muster-bee                      | fmc7.4-13            |
944d50c6c384567693d6ecc5a31420de57f6ce2f
muster-envoy                    | fmc7.4-25            |
5e5f6d83164a4acbef5b106aa39e2e3f68fa738f
muster-local-fmc-adapter        | fmc7.4-17            |
c5902f818baa8e27d7c0b8027490dcacc28c0168
muster-ui-backend               | fmc7.4-64            |
165a1f5f0d763aa75829a30b5ffbddf0012682b6
muster-user-analysis            | fmc7.4-43            |
63cd64e29a92599908c3eb684d91e9f685d8c740
muster-connector-o365.1.muster | fmc7.4-8             |
28f075d315c8867f667b828970c9fbad35fa89cc
```

たとえば、Office 365 コネクタのデバッグを有効にするには、次のコマンドを入力します。

```
sudo ./muster-cli container-debug-on muster-connector-o365.1.muster
```

そのコネクタのデバッグを無効にするには、次のコマンドを入力します。

```
sudo ./muster-cli container-debug-off muster-connector-o365.1.muster
```

ダイナミックオブジェクトの確認

コネクタが management center でオブジェクトを作成していることを確認するには、management center で管理者として次のコマンドを使用します。

```
sudo tail f /var/opt/CSCOpx/MDC/log/operation/usmsharedsvcs.log
```

例：成功したオブジェクトの作成

```
26-Aug-2021 12:41:35.912,[INFO],(DefenseCenterServiceImpl.java:1442)
com.cisco.nm.vms.api.dc.DefenseCenterServiceImpl, ajp-nio-127.0.0.1-9009-exec-10
** REST Request [ CSM ]
** ID : 18b25356-fd6b-4cc4-8d27-bbccb52a6275
** URL: POST /audit
{
  "version": "7.1.0",
  "requestId": "18b25356-fd6b-4cc4-8d27-bbccb52a6275",
  "data": {
    "userName": "csdac-centos7",
    "subsystem": "API",
    "message": "POST
https://myfmc.example.com/api/fmc_config/v1/domain/e276abec-e0f2-11e3-8169-6d9ed49b625f
/object/dynamicobjects Created (201) - The request has been fulfilled and resulted in a
 new resource being created",
    "sourceIP": "192.0.2.103",
    "domainUuid": "e276abec-e0f2-11e3-8169-6d9ed49b625f",
    "time": "1629981695431"
  },
  "deleteList": []
}
```

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。

始める前に

トラブルシューティングの詳細については、『Cisco Secure Firewall Management Center アドミニストレーション ガイド』のトラブルシューティングの章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 **システム**（⚙）> **[正常性（Health）]** > **[モニタ（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) チェーンの手動での取得

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、NSX、またはManagement Centerに安全に接続するために使用される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。

次に接続するには、これらの手順のいずれかを使用する必要があります。

- vCenter または NSX

  Azure または AWS に接続するために証明書チェーンを取得する必要はありません。

- 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、url は vCenter または Management Center への URL（スキームを含む）です。次に例を示します。

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

   NAT または PAT を使用して vCenter または Management Center にアクセスする場合は、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 と Management Center の両方で、これらのタスクを繰り返します。

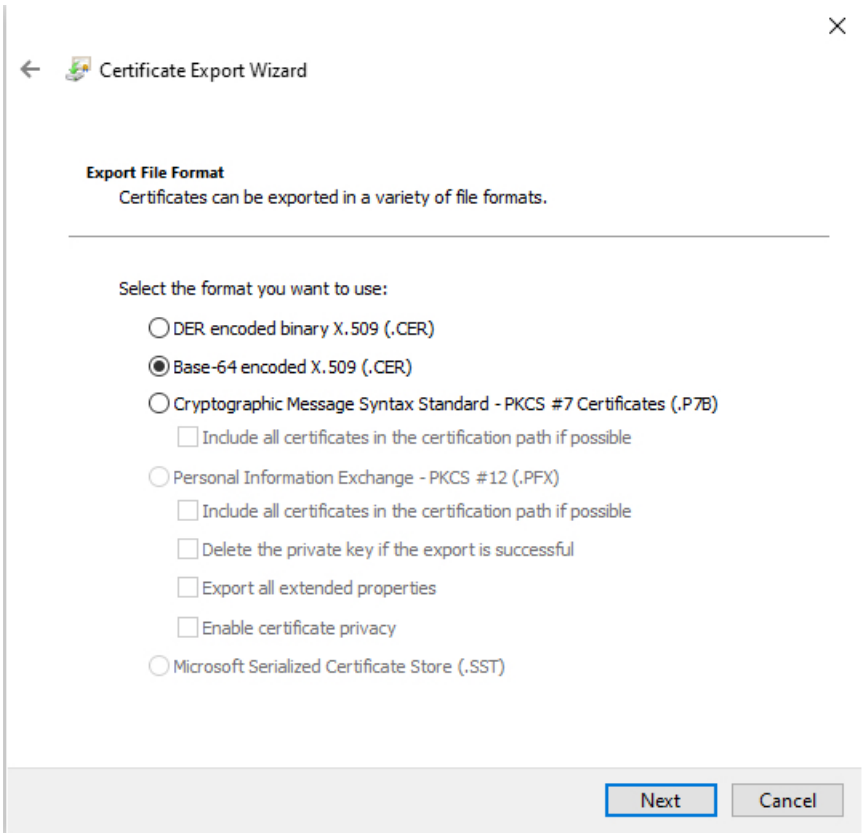
証明書チェーンの取得：Windows Chrome

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

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。

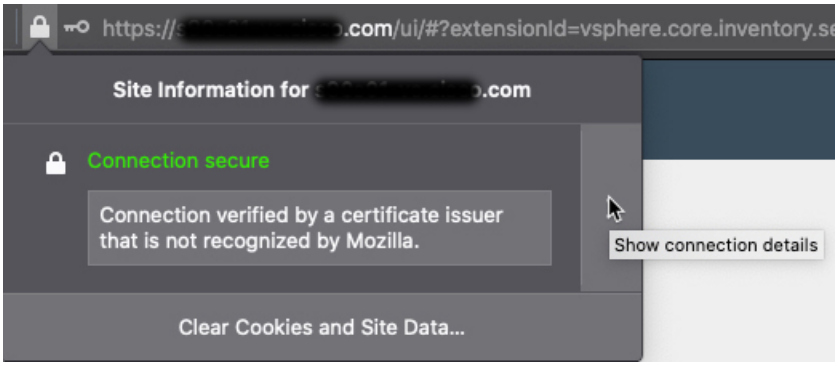
    テキストエディタに各証明書を最初から最後まで順番に貼り付ける必要があります。

13. vCenter と FMC の両方でこれらのタスクを繰り返します。

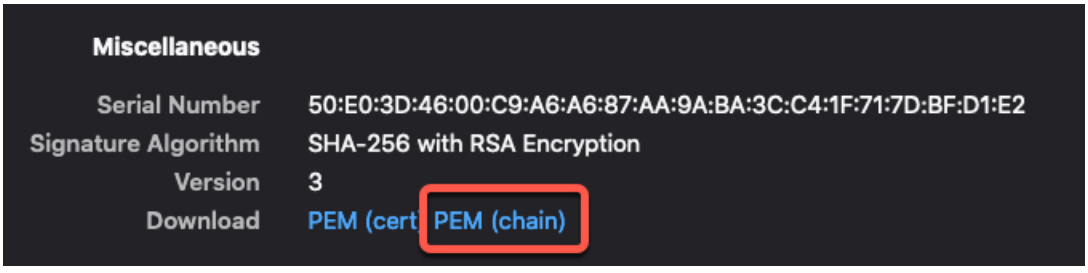
証明書チェーンの取得：Windows Firefox

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 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 と Management Center の両方で、これらのタスクを繰り返します。

セキュリティ要件

Cisco Secure 動的属性コネクタを保護するには、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。動的属性コネクタは、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。

動的属性コネクタと management center が同じネットワーク上に存在している場合は、management center を 動的属性コネクタ 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、動的属性コネクタ 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。動的属性コネクタ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、management center および外部サーバーとの通信に 動的属性コネクタ が使用する URL が通知されます。

表 *3*：動的属性コネクタ *management center* 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*：動的属性コネクタ *vCenter* アクセス要件

URL	理由
https://*vcenter-ip***/rest/com/vmware/cis/session**	認証
https://*vcenter-ip***/rest/vcenter/vm**	VM 情報を取得します

URL	理由
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

Cisco Secure 動的属性コネクタ 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

動的属性コネクタ Azure のアクセス要件

動的属性コネクタは、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。

Cisco Secure 動的属性コネクタ の履歴

機能	最小 Management Center	最小 Threat Defense	詳細
Cisco Secure 動的属性コネクタ	7.4.0	7.4.0	この機能が導入されます。 Cisco Secure 動的属性コネクタ が Secure Firewall Management Center に含まれるようになりました。動的属性コネクタを使用すると、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 動的属性コネクタ：Cisco Secure 動的属性コネクタ について （1 ページ） • スタンドアロン 動的属性コネクタ：Cisco Secure 動的属性コネクタ コンフィギュレーション ガイド 新規/変更された画面：**[統合（Integration）] > [Cisco動的属性コネクタ（Cisco 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。