



Cisco Secure 動的属性コネクタ の設定

動的属性コネクタをインストールして、コネクタ、動的属性フィルタ、アダプタを構成し、アクセス制御ルールで使用できるダイナミック ネットワーク データを management center に提供します。

動的属性コネクタにより、コネクタを構成して、アクセス制御ルールで使用できるダイナミック ネットワーク データを management center に提供できます。

詳細については、次のトピックを参照してください。

- [コネクタの作成 \(1 ページ\)](#)
- [アダプタの作成 \(17 ページ\)](#)
- [動的属性フィルタの作成 \(26 ページ\)](#)
- [認証局 \(CA\) チェーンの手動での取得 \(30 ページ\)](#)

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 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	GitHub	Google クラウド	Azure	Azure サービススタグ	Microsoft Office 365	vCenter
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	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

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「[Amazon EC2 リソースのタグ付け](#)」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` 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 \(2 ページ\)](#) を参照してください。

始める前に

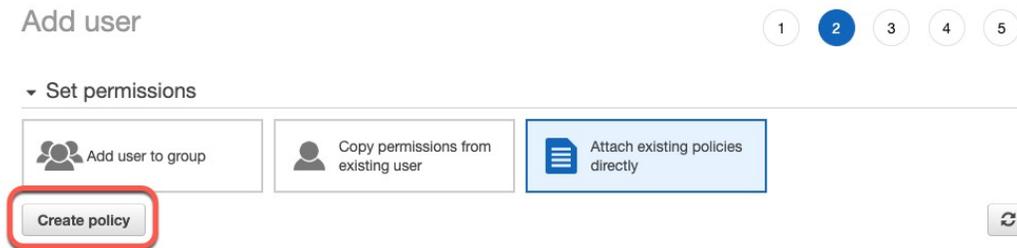
Amazon Web Services (AWS) アカウントがすでに設定されている必要があります。これを行う方法の詳細については、AWS ドキュメントの[この記事](#)を参照してください。

-
- 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** [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** [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"
      ],
      "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 \(4 ページ\)](#)。

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。
(2 ページ) で説明した権限以上のユーザーを作成します。

ステップ 1 動的属性コネクタにログインします。

ステップ 2 [コネクタ (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 : [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)	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 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。

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。

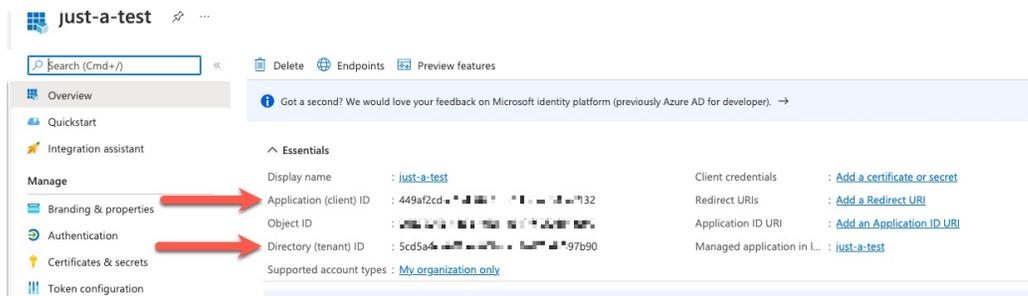
Cisco Secure 動的属性コネクタ に対する最小限の権限を持つ Azure ユーザーの作成

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 \(5 ページ\)](#) 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。

-
- 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 と呼ばれる) とテナント ID (ディレクトリ ID と呼ばれる) 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。

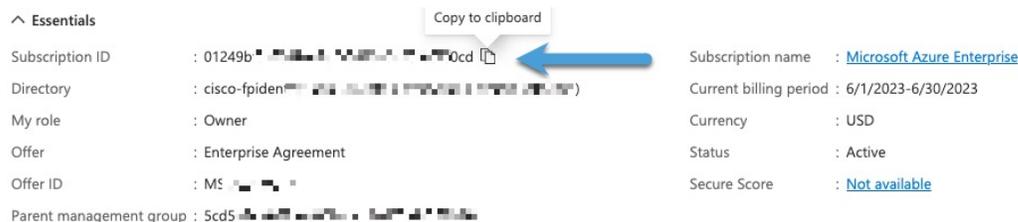
ステップ 12 [値 (Value)]フィールドの値をクリップボードにコピーします。[シークレットID (Secret ID)]ではなく、この値がクライアントシークレットです。



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。

> Microsoft Azure Enterprise >

Add role assignment

Got feedback?

Role **Members** Review + assign

Selected role
Reader

Assign access to
 User, group, or service principal
 Managed identity

Members
+ Select members

Name	Object ID
No members selected	

Description
Optional

Review + assign Previous Next **Select** Close

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 \(7 ページ\)](#) 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 \(5 ページ\)](#) で説明した権限以上の Azure ユーザーを作成します。

ステップ 1 動的属性コネクタにログインします。

ステップ2 [コネクタ (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：[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)	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5 コネクタを保存する前に、[テスト (Test)] をクリックして、**Test connection succeeded** が表示され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。

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。

ステップ1 動的属性コネクタにログインします。

ステップ2 [コネクタ (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 : [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)	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 5 コネクタを保存する前に、[テスト (Test)]をクリックして、**Test connection succeeded** が表示され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。

ステップ 1 動的属性コネクタ にログインします。

ステップ 2 [コネクタ (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 : [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 [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 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。

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。 >

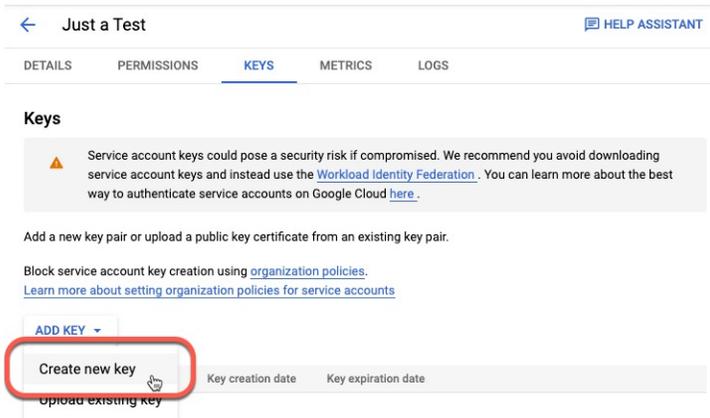
Cisco Secure 動的属性コネクタ に対して最小限の権限を持つ Google Cloud ユーザーを作成します。

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（10 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。

-
- 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 \(12 ページ\)](#) 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。

ステップ 1 動的属性コネクタにログインします。

ステップ 2 [コネクタ (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 : [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。

値	説明
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 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。

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。

ステップ 1 動的属性コネクタにログインします。

ステップ 2 [コネクタ (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: [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)	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。

値	説明
ベース APIURL (Base APIURL)	(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 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。

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。

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 \(CA\) チェーンの手動での取得 \(23 ページ\)](#) を参照してください。

ステップ 1 動的属性コネクタにログインします。

ステップ 2 [コネクタ (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: [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。 <ul style="list-style-type: none"> • 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。ユーザー名は大文字/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。

値	説明
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。
vCenter証明書 (vCenter Certificate)	次の選択肢があります。 <ul style="list-style-type: none"> • [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 (23 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 \(23 ページ\)](#) 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 コネクタを保存する前に、[テスト (Test)] をクリックして、**Test connection succeeded** が表示され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。

次のタスク

[アダプタの作成 \(17 ページ\)](#)

アダプタの作成

アダプタは、アクセスコントロールポリシーで使用するためにクラウドオブジェクトからネットワーク情報をプッシュする Management Center への安全な接続です。

まず、オプションで認証局チェーンを取得できます。これは、management center に安全に接続するために必要です。

認証局チェーンの取得に必要なものは、management center ホスト名のみです。アダプタを作成するには、ユーザー名、パスワード、およびその他の情報が必要です。

動的属性コネクタの Secure Firewall Management Center ユーザーの作成

動的属性コネクタ アダプタ用に専用の management center ユーザーを作成することを推奨します。専用 management center ユーザーを作成すると、management center からの予期しないログアウトなどの問題を回避できます。これは、動的属性コネクタが REST API を使用して定期的にログインし、新規および更新されたダイナミックオブジェクトで management center を更新するためです。

management center ユーザーには、最低限でもアクセス管理者 (Access Admin) 権限が必要です。

ステップ 1 まだ 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 システム (⚙️) > [ユーザー (Users)] をクリックします。

ステップ 3 [ユーザの作成 (Create User)] をクリックします。

ステップ 4 ユーザーを作成するために必要な情報を入力します。

ステップ 5 [ユーザーロールの構成 (User Role Configuration)] で、次のデフォルトロールのいずれか、または同じ権限レベルのカスタムロールをチェックします。

- 管理者 (Administrator)

- アクセス管理者
- ネットワーク管理者

次の図は例を示しています。

User Configuration

User Name	<input type="text" value="csdac-sample"/>
Real Name	<input type="text" value="csdac-sample"/>
Authentication	<input type="checkbox"/> Use External Authentication Method
Password	<input type="password" value="....."/>
Confirm Password	<input type="password" value="..... "/>
Maximum Number of Failed Logins	<input type="text" value="5"/> (0 = Unlimited)
Minimum Password Length	<input type="text" value="8"/>
Days Until Password Expiration	<input type="text" value="0"/> (0 = Unlimited)
Days Before Password Expiration Warning	<input type="text" value="0"/>
Options	<input type="checkbox"/> Force Password Reset on Login <input type="checkbox"/> Check Password Strength <input type="checkbox"/> Exempt from Browser Session Timeout

User Role Configuration

Default User Roles	<input type="checkbox"/> Administrator <input type="checkbox"/> External Database User (Read Only) <input type="checkbox"/> Security Analyst <input type="checkbox"/> Security Analyst (Read Only) <input type="checkbox"/> Security Approver <input type="checkbox"/> Intrusion Admin <input checked="" type="checkbox"/> Access Admin <input type="checkbox"/> Network Admin <input type="checkbox"/> Maintenance User <input type="checkbox"/> Discovery Admin <input type="checkbox"/> Threat Intelligence Director (TID) User
--------------------	--

RESTアクションを許可するために十分な権限を持つカスタムロール、または十分な権限を持つ別のデフォルトロールを選択することもできます。デフォルトロールの詳細については、ユーザーアカウントに関する章の「ユーザーロール」セクションを参照してください。

次のタスク

[アダプタの作成 \(17 ページ\)](#)

オンプレミス Firewall Management Center アダプタを作成する方法

このトピックでは、ダイナミックオブジェクトを動的属性コネクタ から management center にプッシュするアダプタを作成する方法について説明します。

始める前に

動的属性コネクタの [Secure Firewall Management Center ユーザーの作成 \(17 ページ\)](#) を参照してください。

ステップ 1 動的属性コネクタにログインします。

ステップ 2 [アダプタ (Adapters)] 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) このアダプタを識別するための一意の名前を入力します。
説明	オプションのアダプタの説明。
ドメイン (Domain)	ダイナミックオブジェクトを作成する Secure Firewall Management Center Virtual ドメインを入力します。グローバルドメインにダイナミックオブジェクトを作成するには、フィールドを空白のままにします。 例 : Global/MySubdomain
IP	(必須) Secure Firewall Management Center Virtual のホスト名または IP アドレスを入力します。 入力するホスト名または IP は、安全に接続するために使用される CA 証明書の共通名と完全に一致している必要があります。
ポート (Port)	(必須) Secure Firewall Management Center Virtual が使用する TLS ポートを入力します。
ユーザー (User)	(必須) 最低限でもネットワーク管理者ロールを持つ Secure Firewall Management Center Virtual ユーザーの名前を入力します。
パスワード (Password)	(必須) ユーザーのパスワードを入力します。

値	説明
セカンダリ IP (Secondary IP)	<p>(高可用性のみ。) セカンダリ Secure Firewall Management Center Virtual のホスト名または IP アドレスを入力します。</p> <p>入力するホスト名または IP は、安全に接続するために使用される CA 証明書の共通名と完全に一致している必要があります。</p>
セカンダリポート (Secondary Port)	<p>(高可用性のみ。) セカンダリ Secure Firewall Management Center Virtual が使用する TLS ポートを入力します。</p>
セカンダリユーザー (Secondary User)	<p>(高可用性のみ。) 最低限でもネットワーク管理者ロールを持つセカンダリ Secure Firewall Management Center Virtual ユーザーの名前を入力します。</p>
セカンダリ パスワード (Secondary Password)	<p>(高可用性のみ。) ユーザーのパスワードを入力します。</p>
サーバー証明書	<p>次の選択肢があります。</p> <ul style="list-style-type: none"> • [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 (23 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 \(23 ページ\)](#) 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 アダプタを保存する前に、[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。

クラウド提供型 Firewall Management Center アダプタの作成

このトピックでは、Cisco Defense Orchestrator で管理される管理センターに、動的属性コネクタからダイナミックオブジェクトをプッシュするアダプタを作成する方法について説明します。

クラウド提供型 Firewall Management Center を作成する前に、次の [ベース URL と API トークンの取得 \(22 ページ\)](#) の情報を取得してください。

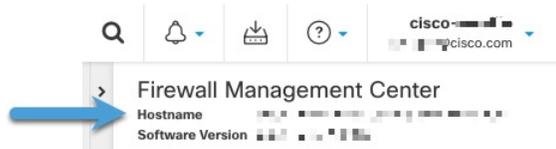
ベース URL と API トークンの取得

このタスクでは、クラウド提供型 Firewall Management Center アダプタの作成に必要な URL と API トークンを CDO から取得する方法について説明します。

始める前に

このセクションで説明するタスクを完了するには、CDO のスーパー管理者である必要があります。

- ステップ 1 ネットワーク管理者ロールを持つユーザーとして CDO にログインします。
- ステップ 2 ページの右上隅で、[設定 (Settings)] をクリックします。
- ステップ 3 [全般設定 (General Settings)] をクリックします。
- ステップ 4 [API トークン (API Token)] の横にある [更新 (Refresh)] をクリックします。
- ステップ 5 後で使用するために、API トークンをテキストファイルにコピーします。
- ステップ 6 [ツールとサービス (Tools & Services)] > [Firewall Management Center] をクリックします。
- ステップ 7 動的属性コネクタ データを送信する管理センターの名前をクリックします。
- ステップ 8 [https://] で始まる [ホスト名 (Hostname)] の値は、ベース URL です。
次に例を示します。



次のタスク

[クラウド提供型 Firewall Management Center アダプタを作成する方法 \(22 ページ\)](#)。

クラウド提供型 Firewall Management Center アダプタを作成する方法

このタスクでは、CDO によって管理されているデバイスに動的属性コネクタ からデータを送信するクラウド提供型 Firewall Management Center アダプタを作成する方法について説明します。

始める前に

このタスクを完了する前に、管理センターのベース URL と API トークンを CDO から取得する必要があります。詳細については、[ベース URL と API トークンの取得 \(22 ページ\)](#) を参照してください。

- ステップ 1 動的属性コネクタにログインします。
- ステップ 2 [アダプタ (Adapters)] 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) このアダプタを識別するための一意の名前を入力します。
説明	オプションのアダプタの説明。
[ベースURL (Base URL)]	(必須) ベース URL と API トークンの取得 (22 ページ) で見つけたベース URL を使用します。
[API Token]	(必須) ベース URL と API トークンの取得 (22 ページ) で見つけた API トークンを使用します。

ステップ 5 アダプタを保存する前に、[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。

次のタスク

[動的属性フィルタの作成 \(26 ページ\)](#)。

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

この手順を使用する前に、次の認証局チェーンの自動取得に関するセクションを参照してください。

- [vCenter コネクタの作成 \(14 ページ\)](#)

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
```

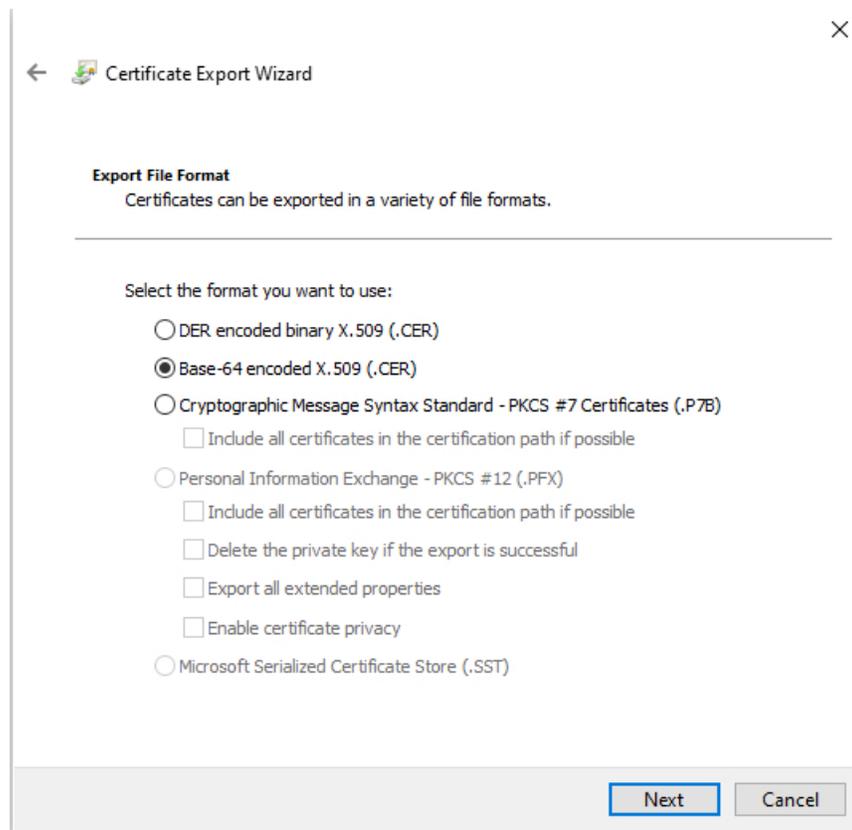
3. 証明書チェーン全体をプレーンテキストファイルに保存します。
 - すべての -----BEGIN CERTIFICATE----- および -----END CERTIFICATE----- 区切り文字を含めます。
 - 無関係なテキスト (たとえば、証明書の名前、山かっこ (<および>) に含まれるテキスト、および山かっこ自体を除外します。
4. vCenter と Management Center の両方で、これらのタスクを繰り返します。

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。

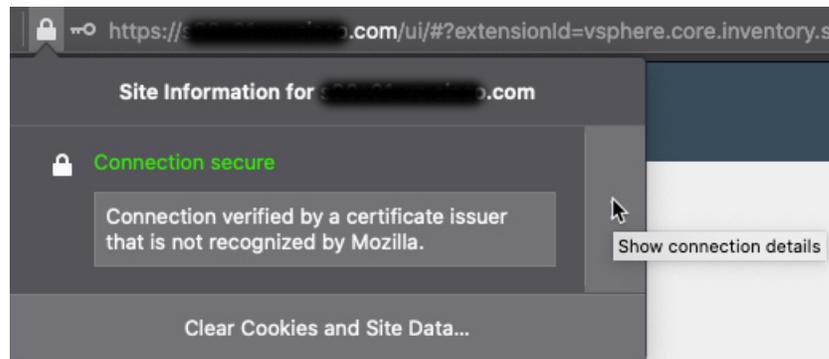


10. 指示に従ってエクスポートを完了します。
11. 証明書をテキストエディタで開きます。
12. チェーン内のすべての証明書に対してこのプロセスを繰り返します。
テキストエディタに各証明書を最初から最後まで順番に貼り付ける必要があります。
13. vCenter と FMC の両方でこれらのタスクを繰り返します。

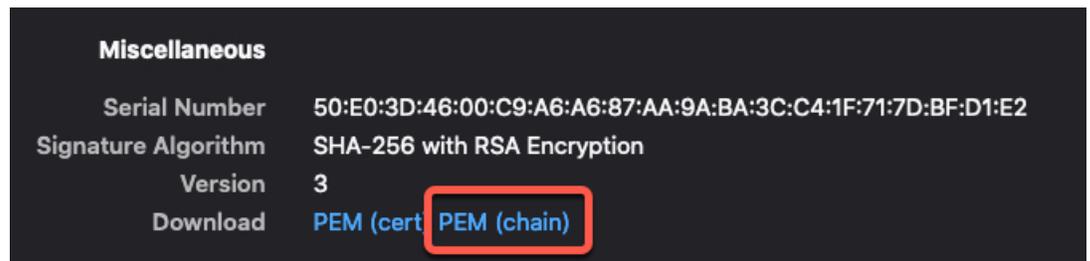
証明書チェーンの取得 : Windows Firefox

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。

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) GitHub、Office 365、Azure サービスタグ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](#)を参照してください。

始める前に

[コネクタの作成 \(1 ページ\)](#)

ステップ 1 動的属性コネクタにログインします。

ステップ 2 [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 3 次の情報を入力します。

項目	説明
名前	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	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	<ul style="list-style-type: none"> • 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 4 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	<p>次のいずれかをクリックします。</p> <ul style="list-style-type: none"> • キーを値に正確に一致させるには、[等しい (Equals)]。

項目	説明
	<ul style="list-style-type: none"> 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	[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 5 [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 6 完了したら、[保存 (Save)] をクリックします。

ステップ 7 (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。

- 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。
- [オブジェクト (Objects)] > [オブジェクトマネージャ (Object Manager)] をクリックします。
- 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。

The screenshot shows the 'Edit Dynamic Attribute Filter' interface. The 'Name' field contains 'TestFilt' and the 'Connector' dropdown is set to 'vCenter'. Below, the 'Query' section is a table with three columns: 'Type', 'Op.', and 'Value'. The first row has 'all' in the Type column, 'network' in the Op. column, and 'eq any myVLAN' in the Value column. A '+ Show Preview' link is located below the table. At the bottom right, there are 'Cancel' and 'Save' buttons.

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。

Add Dynamic Attribute Filter

Name* Connector*

Query* +

Type	Op.	Value
<input type="checkbox"/> all host	eq	<input type="checkbox"/> any host-2868 host-2869 host-3780

[> Show Preview](#)

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。

Add Dynamic Attribute Filter

Name* Connector*

Query* +

Type	Op.	Value
<input type="checkbox"/> all Finance	eq	<input type="checkbox"/> any App

[> Show Preview](#)

例 : AWS

次の例は、1 つの基準を示しています : 値が 1 の FinanceApp。

Add Dynamic Attribute Filter

Name* Connector*

Query* +

Type	Op.	Value
<input type="checkbox"/> all FinanceApp	eq	<input type="checkbox"/> any 1

[> Show Preview](#)

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

この手順を使用する前に、次の認証局チェーンの自動取得に関するセクションを参照してください。

- [vCenter コネクタの作成 \(14 ページ\)](#)

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
```

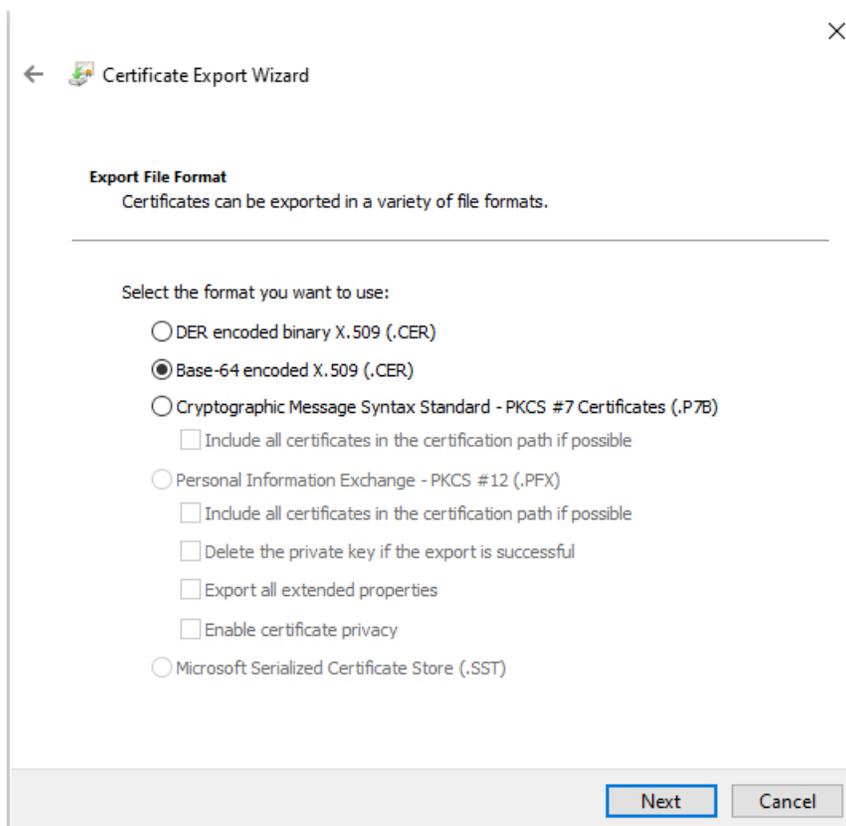
3. 証明書チェーン全体をプレーンテキストファイルに保存します。
 - すべての -----BEGIN CERTIFICATE----- および -----END CERTIFICATE----- 区切り文字を含めます。
 - 無関係なテキスト (たとえば、証明書の名前、山かっこ (<および>) に含まれるテキスト、および山かっこ自体を除外します。
4. vCenter と Management Center の両方で、これらのタスクを繰り返します。

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。

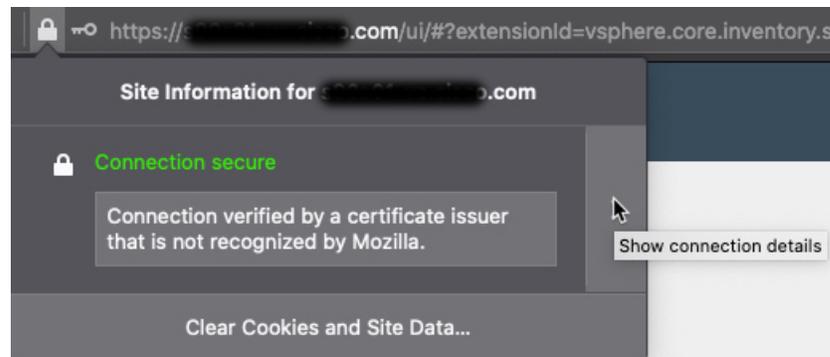


10. 指示に従ってエクスポートを完了します。
11. 証明書をテキストエディタで開きます。
12. チェーン内のすべての証明書に対してこのプロセスを繰り返します。
テキストエディタに各証明書を最初から最後まで順番に貼り付ける必要があります。
13. vCenter と FMC の両方でこれらのタスクを繰り返します。

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。

Miscellaneous	
Serial Number	50:E0:3D:46:00:C9:A6:A6:87:AA:9A:BA:3C:C4:1F:71:7D:BF:D1:E2
Signature Algorithm	SHA-256 with RSA Encryption
Version	3
Download	PEM (cert) PEM (chain)

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。

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。