Cisco Secure Dynamic Attributes Connector 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 FMC に提供します。

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

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、FMC 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 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/プラットフォーム	AWS	Git-Hub	Google クラウド	Azure	Azure サービスタグ	Microsoft Office 365	VMware vCenter
バージョン 1.1（オンプレミス）	対応	非対応	非対応	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
クラウド提供型（Cisco Defense Orchestrator）	対応	対応	対応	対応	対応	対応	非対応

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 Dynamic Attributes Connector 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 FMC 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 Dynamic Attributes Connector 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 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 FMC 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。

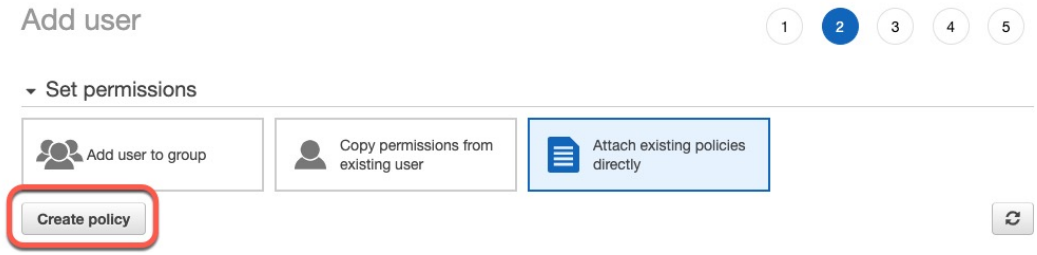
（注） これが、ユーザーのキーを取得する必要がある唯一の機会です。

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 FMC 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 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。 （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：**Add** (＋) 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 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。

次のタスク

アダプタの作成 （14 ページ）

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 Dynamic Attributes Connector 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 FMC 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 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。

Cisco Secure 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 FMC 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。

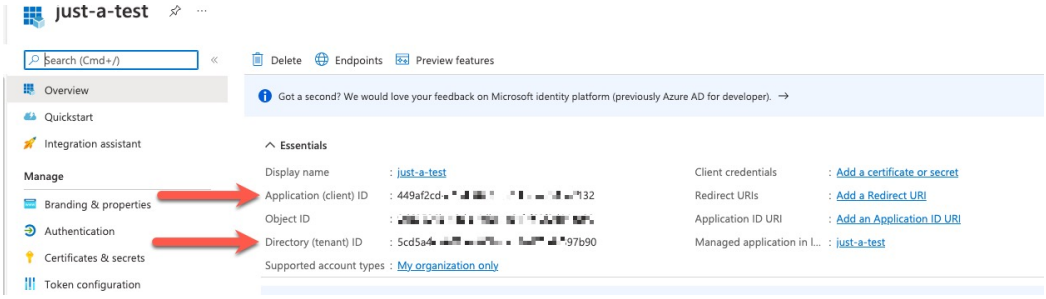
ステップ 5 [名前（Name）] フィールドに、このアプリケーションを識別するための名前を入力します。

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 [証明書またはシークレットを追加（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 Azure コネクタの設定に必要になるため、クライアント**値**をクリップボードにコピーします。

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 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 15 サブスクリプションページで、サブスクリプションの名前をクリックします。

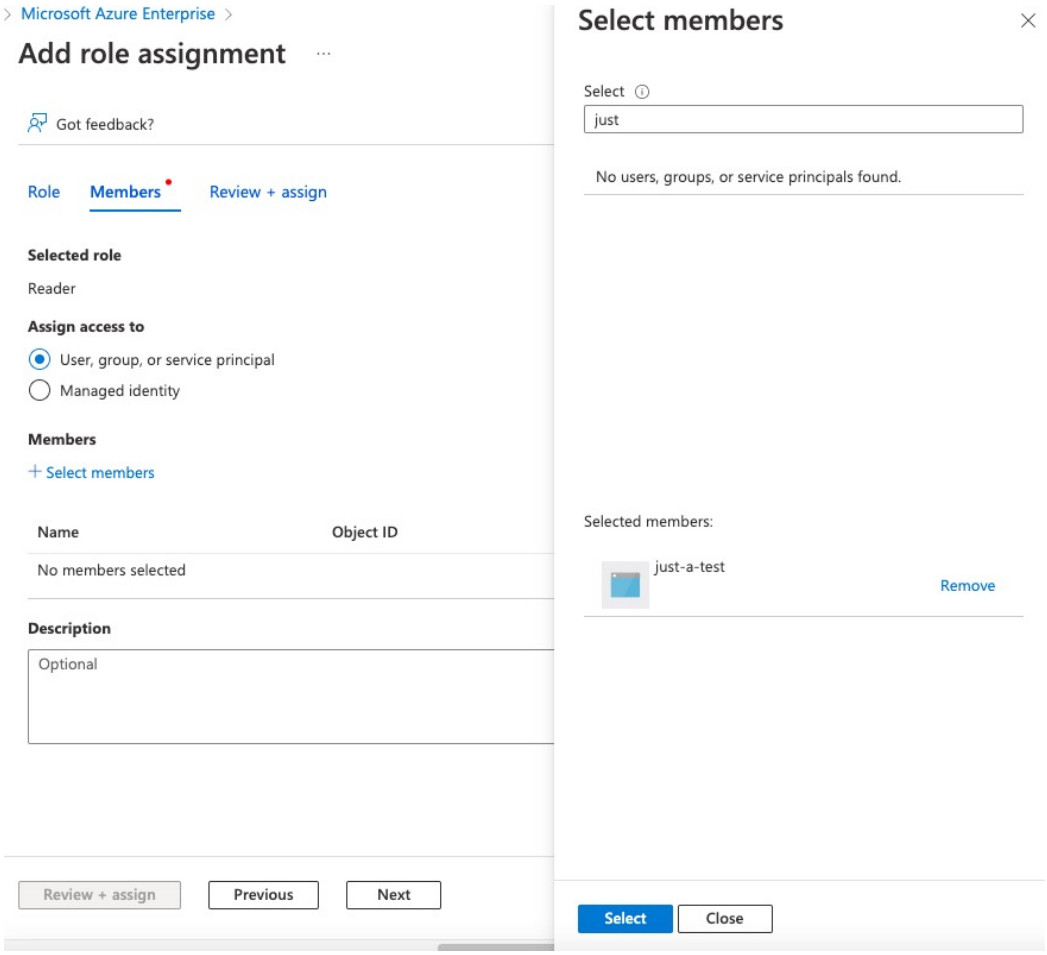
ステップ 16 [アクセス制御（IAM）（Access Control (IAM)）] をクリックします。

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 （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 FMC 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 Dynamic Attributes Connector 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：**Add** (+) 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。
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。

次のタスク

アダプタの作成 （14 ページ）

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 FMC 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：**Add** (+) 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。
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。

次のタスク

アダプタの作成 （14 ページ）

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 FMC 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：**Add** (+) 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。
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。

次のタスク

アダプタの作成 （14 ページ）

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 Dynamic Attributes Connector 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 FMC 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 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。

vCenter コネクタの認証局 (CA) チェーンの取得

このトピックでは、コネクタまたはアダプタの認証局チェーンを自動的に取得する方法について説明します。認証局チェーンは、ルート証明書とすべての下位証明書です。 vCenter または に安全に接続する必要があります。FMC

動的属性コネクタにより、認証局チェーンを自動的に取得できますが、何らかの理由でこの手順が機能しない場合は、認証局 (CA) チェーンの手動での取得 （16 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 次のいずれかを実行します。

a) vCenter CA チェーンを取得するには、[コネクタ（Connectors）] をクリックします。

b) FMC アダプタ CA チェーンを取得するには、[アダプタ（Adapters）] をクリックします。

c) **Add** (+) をクリックします。

ステップ 3 [名前（Name）] フィールドに、コネクタまたはアダプタを識別するための名前を入力します。

ステップ 4 [ホスト（Host）] フィールドに、コネクタまたはアダプタのホスト名または IP アドレスをスキーム (**https://** など）なしで入力します。

たとえば、**`myvcenter.example.com`** または **`192.0.2.100:9090`**

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。

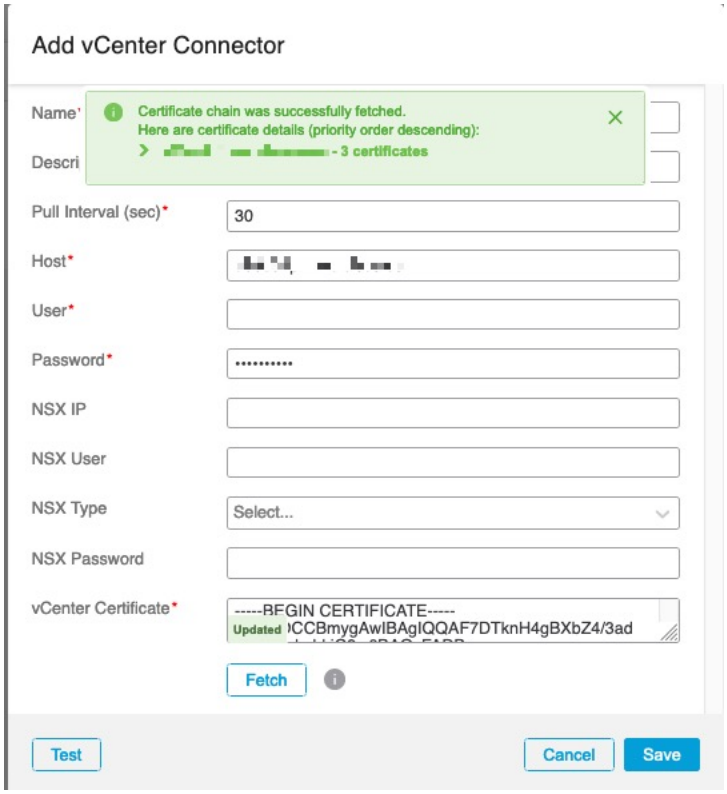
証明書 CA チェーンを取得するために、他の情報は必要ありません。

ステップ 5 [Fetch] をクリックします。

ステップ 6 （オプション）証明書 CA チェーンの証明書を展開して検証します。

例

次に、vCenter コネクタの証明書 CA の取得に成功した例を示します。



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。

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 FMC 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 （16 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：**Add (+)** 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	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。
vCenter証明書（vCenter Certificate）	

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 [Save] をクリックします。

次のタスク

アダプタの作成 （14 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 FMC 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、FMC 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、FMC 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 Firepower Management Center ユーザーの作成

dynamic attributes connector アダプタ用に専用の FMC ユーザーを作成することを推奨します。専用 FMC ユーザーを作成すると、FMC 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、dynamic attributes connector 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 FMC を更新するためです。

FMC 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 FMC 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 **System** (⚙) > **Users** をクリックします。

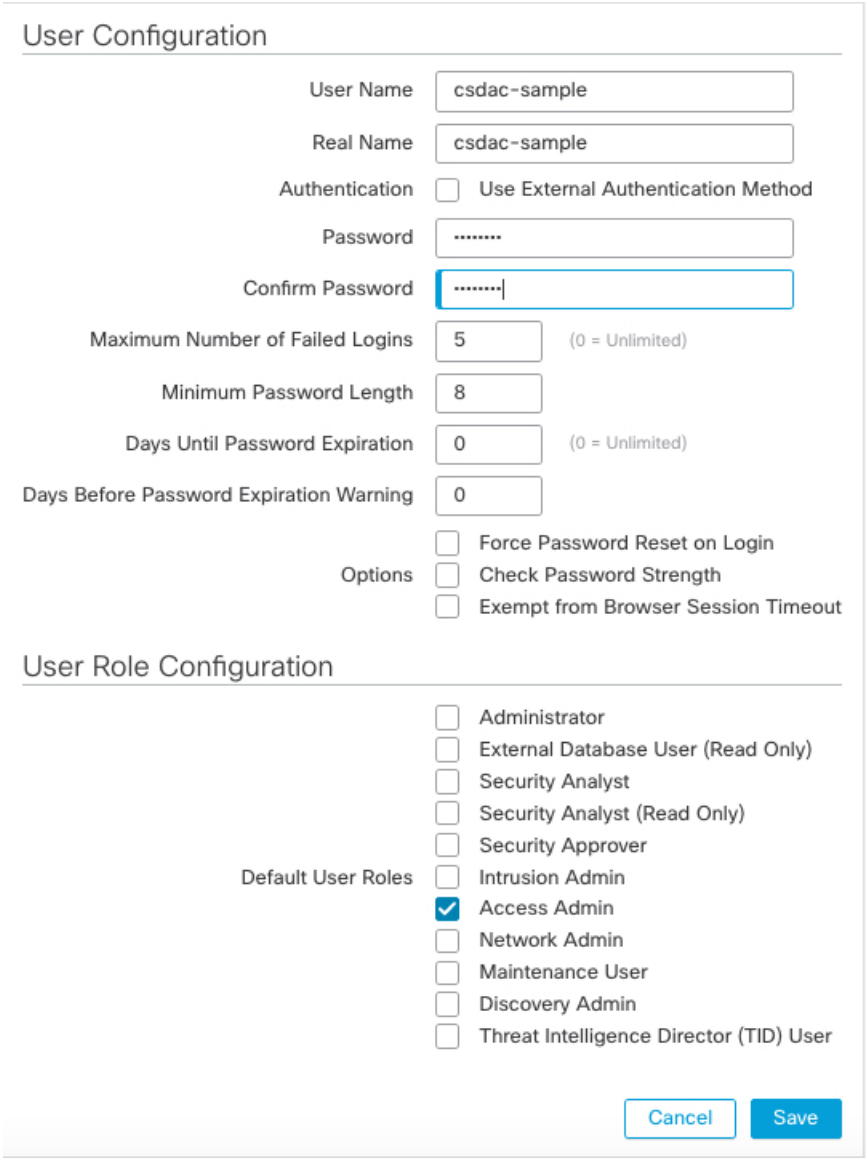
ステップ 3 [ユーザの作成（Create User）] をクリックします。

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。



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 （14 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 FMC 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。

- FMC

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 （12 ページ）
- アダプタの作成 （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 FMC 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 FMC 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。

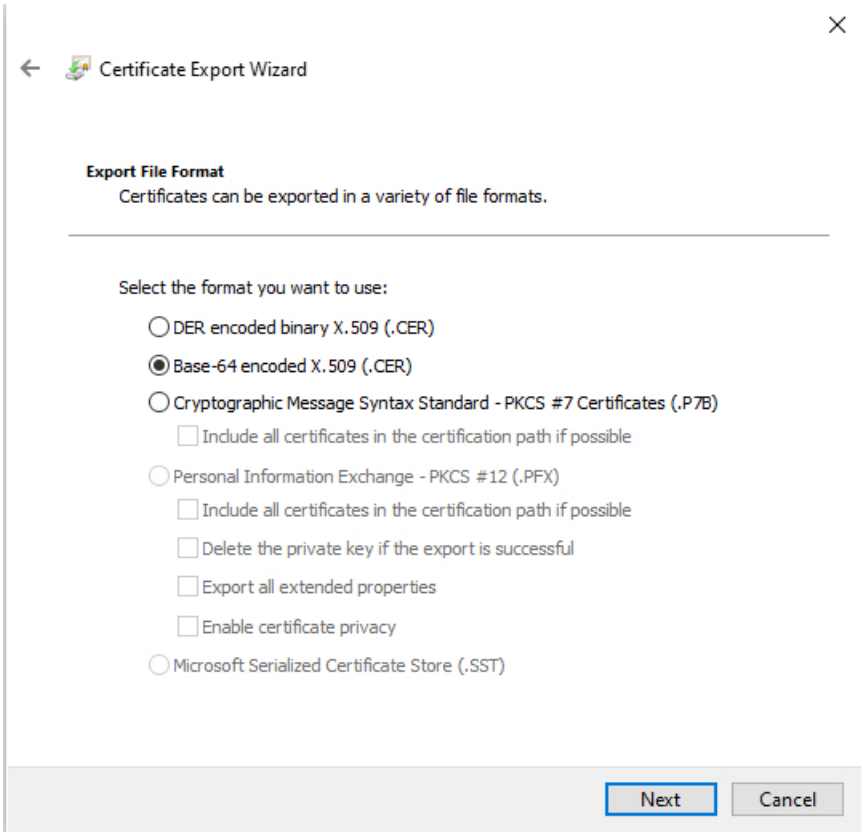
4. vCenter と FMC の両方で、これらのタスクを繰り返します。

証明書チェーンの取得：Windows 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。FMC
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。



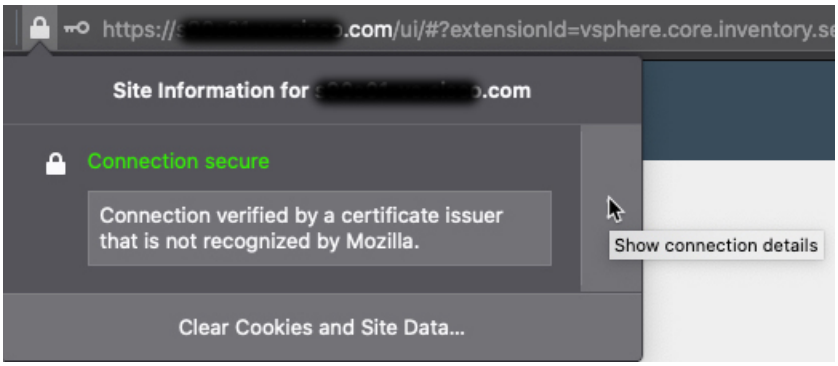
10. 指示に従ってエクスポートを完了します。
11. 証明書をテキストエディタで開きます。
12. チェーン内のすべての証明書に対してこのプロセスを繰り返します。

    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。

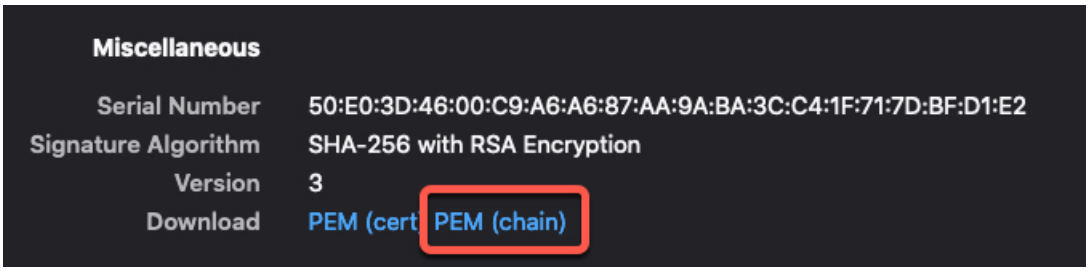
証明書チェーンの取得：Windows Firefox

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 FMC 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 FMC の両方で、これらのタスクを繰り返します。

FMC アダプタの認証局 (CA) チェーンの取得

このトピックでは、コネクタまたはアダプタの認証局チェーンを自動的に取得する方法について説明します。認証局チェーンは、ルート証明書とすべての下位証明書です。 vCenter または に安全に接続する必要があります。FMC

動的属性コネクタにより、認証局チェーンを自動的に取得できますが、何らかの理由でこの手順が機能しない場合は、認証局 (CA) チェーンの手動での取得 （16 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 次のいずれかを実行します。

a) vCenter CA チェーンを取得するには、[コネクタ（Connectors）] をクリックします。
b) FMC アダプタ CA チェーンを取得するには、[アダプタ（Adapters）] をクリックします。
c) **Add** (+) をクリックします。

ステップ 3 [名前（Name）] フィールドに、コネクタまたはアダプタを識別するための名前を入力します。

ステップ 4 [ホスト（Host）] フィールドに、コネクタまたはアダプタのホスト名または IP アドレスをスキーム (**https://** など）なしで入力します。

たとえば、`myvcenter.example.com` または `192.0.2.100:9090`

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。

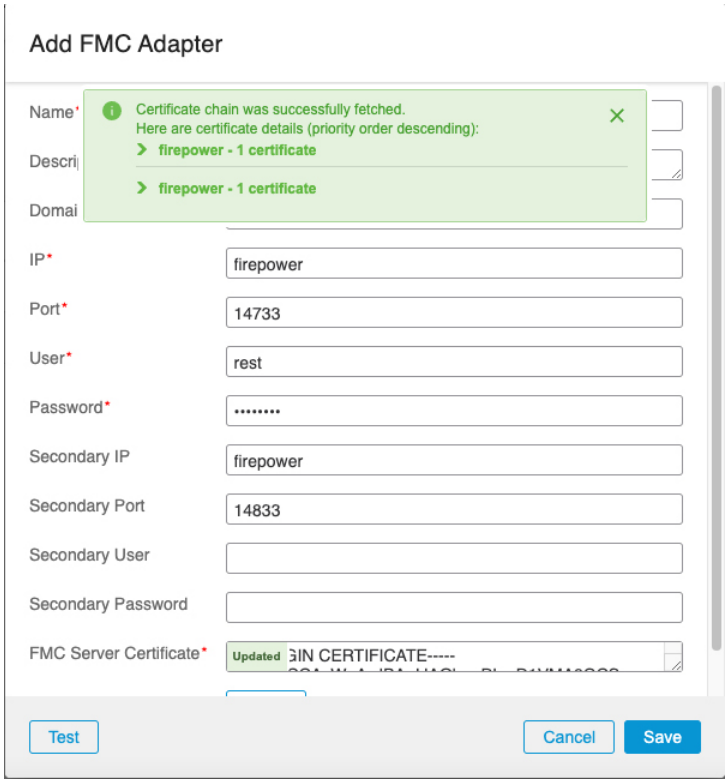
証明書 CA チェーンを取得するために、他の情報は必要ありません。

ステップ 5 [Fetch] をクリックします。

ステップ 6 （オプション）証明書 CA チェーンの証明書を展開して検証します。

例

次に、vCenter コネクタの証明書 CA の取得に成功した例を示します。



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。

FMC 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 dynamic attributes connector から FMC 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 Firepower Management Center ユーザーの作成 （14 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。

- 新しいアダプタを追加します。**Add** (+) をクリックして、FMC をクリックします。
- アダプタを編集または削除します。**More** (⋮) をクリックして、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 Firepower 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）Firepower 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）Firepower 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 Firepower 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。
セカンダリ IP（Secondary IP）	（高可用性のみ。）セカンダリ Firepower 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。
セカンダリポート（Secondary Port）	（高可用性のみ。）セカンダリ Firepower Management Center Virtual が使用する TLS ポートを入力します。
セカンダリユーザー（Secondary User）	（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 Firepower Management Center Virtual ユーザーの名前を入力します。

値	説明
セカンダリ パスワード（Secondary Password）	（高可用性のみ。）ユーザーのパスワードを入力します。
FMC サーバー証明書	[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 （16 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。

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 [Save] をクリックします。

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 FMC 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） Office 365、または 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

次のタスクをすべて完了します。

- 前提条件ソフトウェアのインストール
- コネクタの作成 （1 ページ）
- アダプタの作成 （14 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。

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	アクセス コントロール ポリシーおよび FMC 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	• 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 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	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	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	[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）FMC 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 FMC にログインします。

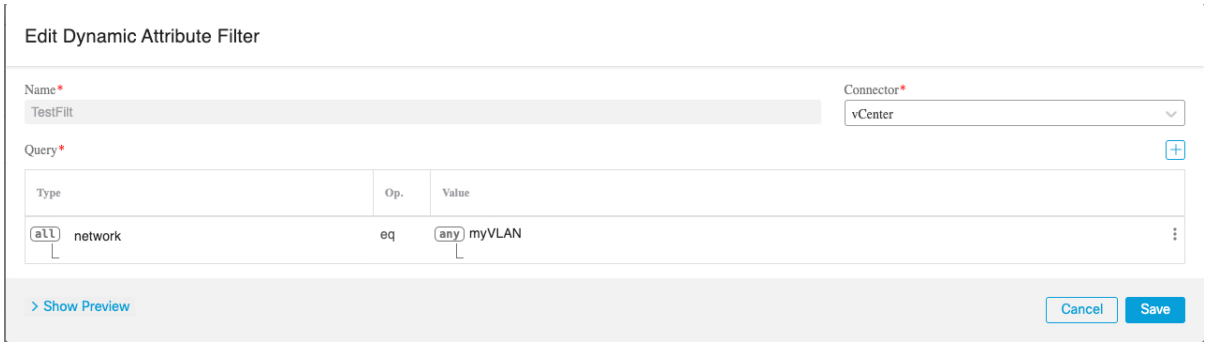
b) **[オブジェクト（Objects）]** > **[オブジェクトマネージャ（Object Manager）]** をクリックします。
c) 左側のペインで、**[外部属性（External Attributes）]** > **[ダイナミックオブジェクト（Dynamic Object）]** をクリックします。
作成した動的属性クエリは、ダイナミックオブジェクトとして表示されます。

動的属性フィルタの例

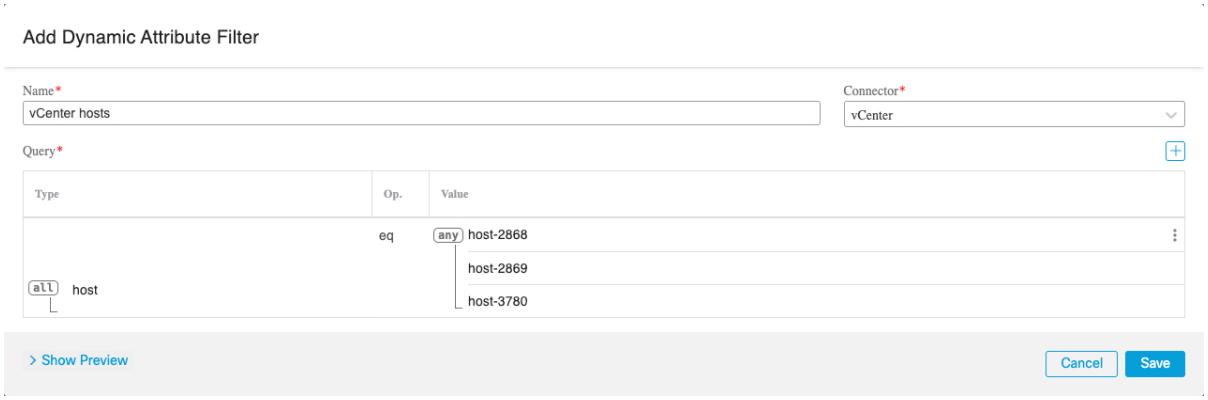
このトピックでは、動的属性フィルタの設定例をいくつか示します。

例：vCenter

次の例は、1 つの基準を示しています：VLAN。

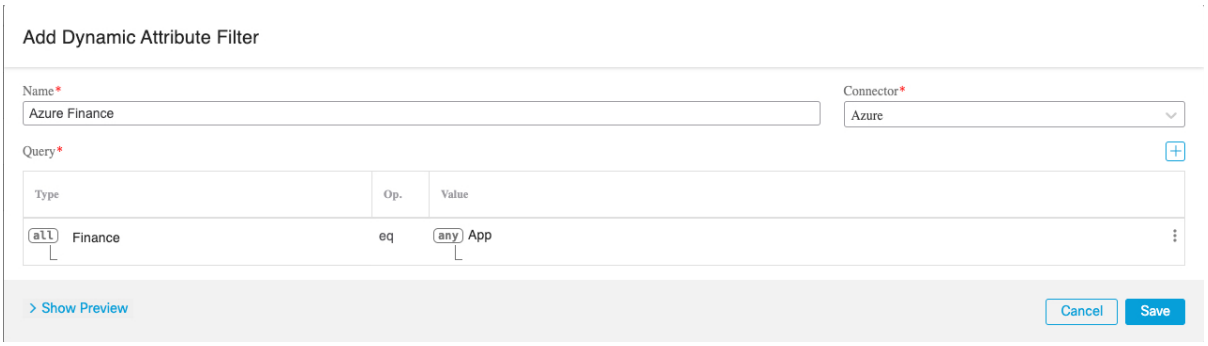


次の例は、OR で結合された 3 つの条件を示しています。クエリは 3 つのホストのいずれかに一致します。



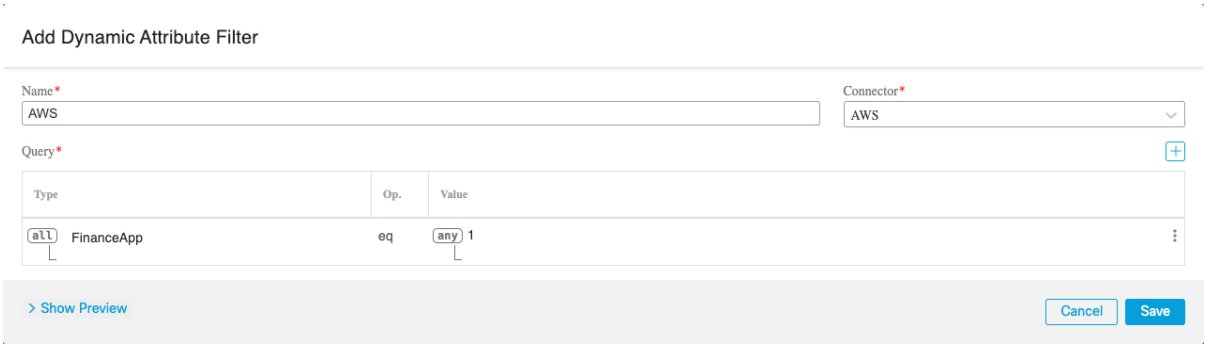
例：Azure

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。



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。