



Cisco Secure 動的属性コネクタ 1.1 構成ガイド

初版：2021年6月1日

最終更新：2022年6月27日

シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先：シスコ コンタクトセンター

0120-092-255（フリーコール、携帯・PHS含む）

電話受付時間：平日 10:00～12:00、13:00～17:00

<http://www.cisco.com/jp/go/contactcenter/>



目次

Full Cisco Trademarks with Software License ?

第 1 章

Cisco 動的属性コネクタについて 1

Cisco Secure 動的属性コネクタについて 1

第 2 章

Cisco 動的属性コネクタのインストール 5

サポートされているオペレーティングシステムとサードパーティソフトウェア 5

前提条件ソフトウェアのインストール 6

前提条件ソフトウェアのインストール : CentOS 7

前提条件ソフトウェアのインストール : RHEL 8

前提条件ソフトウェアのインストール : Ubuntu 9

Cisco Secure 動的属性コネクタ のインストール 11

Cisco Secure 動的属性コネクタのアップグレード 13

第 3 章

Cisco Secure Dynamic Attributes Connector の設定 15

コネクタの作成 15

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

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。 16

AWS コネクタの作成 18

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

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 19

	Azure コネクタの作成	21
	Azure サービスタグコネクタの作成	22
	Office 365 コネクタの作成	23
	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	24
	vCenter コネクタの認証局 (CA) チェーンの取得	25
	vCenter コネクタの作成	26
	アダプタの作成	28
	動的属性コネクタの Firepower Management Center ユーザーの作成	28
	認証局 (CA) チェーンの手動での取得	30
	FMC アダプタの認証局 (CA) チェーンの取得	33
	FMC アダプタを作成する方法	34
	動的属性フィルタの作成	36
	動的属性フィルタの例	38
<hr/>		
第 4 章	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	41
	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	41
	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	42
<hr/>		
第 5 章	動的属性コネクタのトラブルシューティング	45
	エラーメッセージのトラブルシューティング	45
	トラブルシューティング ツール	47
	認証局 (CA) チェーンの手動での取得	49
<hr/>		
付録 A :	セキュリティとインターネットアクセス	53
	セキュリティ要件	53
	インターネット アクセス要件	53

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2021–2022 Cisco Systems, Inc. All rights reserved.



第 1 章

Cisco 動的属性コネクタについて

Cisco Secure 動的属性コネクタでは、クラウドプロバイダーからデータ（ネットワークや IP アドレスなど）を収集し、それを FMC（FMC）に送信して、アクセス制御ルールで使用できるようにします。

次のトピックでは、動的属性コネクタに関する背景について説明します。

- [Cisco Secure 動的属性コネクタについて（1 ページ）](#)

Cisco Secure 動的属性コネクタについて

Cisco Secure 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 Firepower Management Center（FMC）アクセス制御で使用できます。

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 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

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。

- 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。

- 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。

- Office 365

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

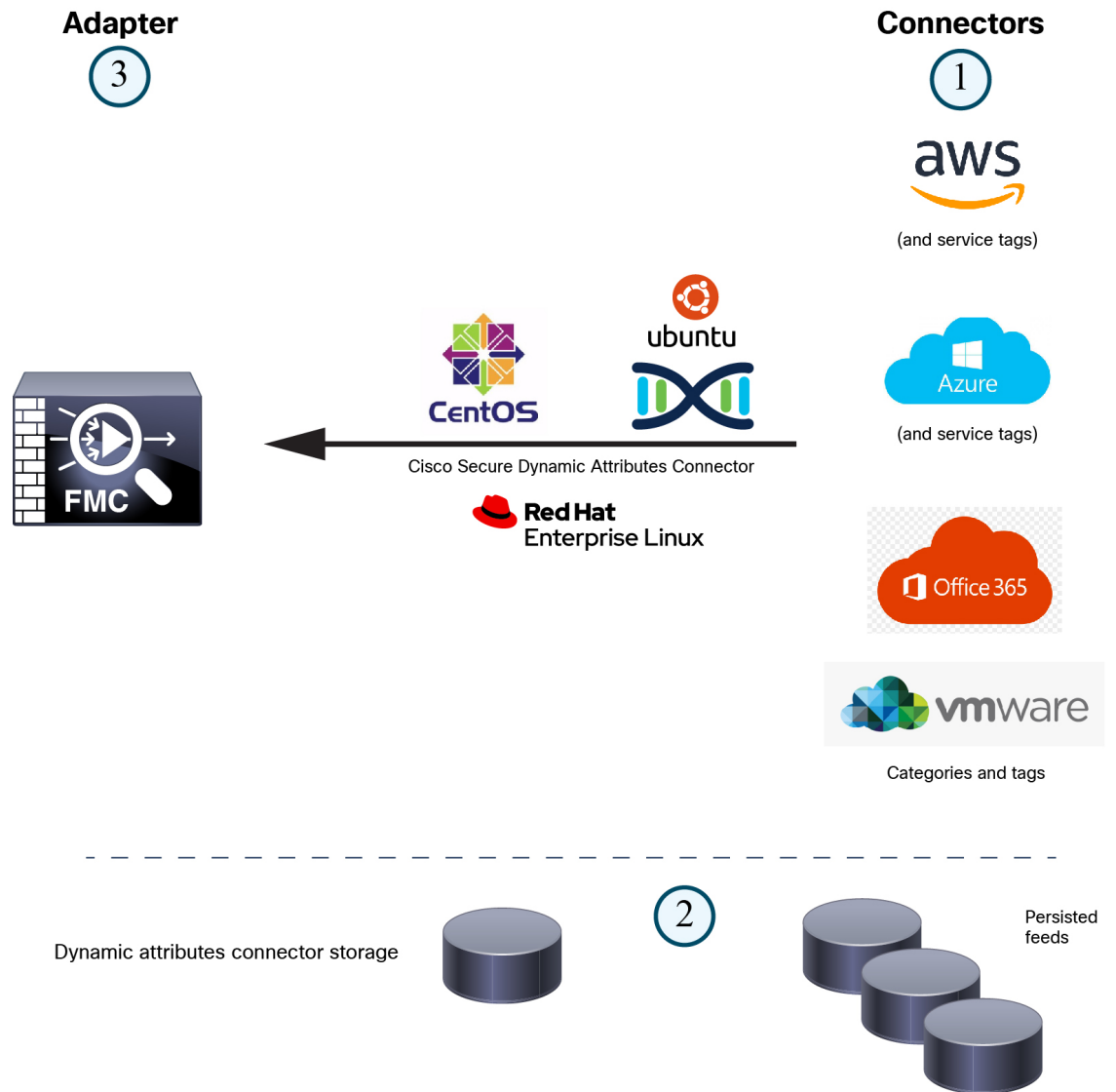
詳細については、[VMware ドキュメントサイトの「vSphere タグと属性」](#)などのリソースを参照してください。

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。

これらのタグと属性は、Ubuntu 仮想マシンで実行されている動的属性コネクタ Docker コンテナを使用して収集できます。Ansible コレクションを使用して、Ubuntu ホストに動的属性コネクタをインストールします。

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。



- コネクタには、クエリするタグとコンテナが含まれています。
たとえば、通常これらのタグは、動的に割り当てられたネットワークおよび IP アドレス（アクセス制御ルールは作成できません）を定義します。コネクタからの永続的なフィードは、高速にアクセスできるように動的属性コネクタに保存されます。
- タグ情報は、アクセス制御ルールで使用するために重要な情報を定義する動的属性フィルタを作成する動的属性コネクタに保持されます。
たとえば、AWS が経理部および財務部の仮想マシンのネットワークを定義している場合、財務ネットワークのみを指定する動的属性フィルタを作成できます。
- 動的属性コネクタによって定義されたアダプタは、これらの動的属性フィルタをダイナミックオブジェクトとして受け取り、アクセス制御ルールで使用できるようにします。



第 2 章

Cisco 動的属性コネクタのインストール

この章では、サポートされているすべてのオペレーティングシステムに Cisco 動的属性コネクタをインストールする方法について説明します。

- [サポートされているオペレーティングシステムとサードパーティソフトウェア \(5 ページ\)](#)
- [前提条件ソフトウェアのインストール \(6 ページ\)](#)
- [Cisco Secure 動的属性コネクタ のインストール \(11 ページ\)](#)
- [Cisco Secure 動的属性コネクタのアップグレード \(13 ページ\)](#)

サポートされているオペレーティングシステムとサードパーティソフトウェア

dynamic attributes connector の前提条件は次のとおりです。

- Ubuntu 18.04 または 20.04
- CentOS 7 Linux または 8
- Red Hat Enterprise Linux (RHEL) 7 または 8
- Python 3.6.x
- Ansible 2.9 以降

すべてのオペレーティングシステムの最小要件：

- 4 個の CPU
- 8 GB RAM
- 100 GB 使用可能なディスクスペース

vCenter 属性を使用する場合は、次も必要です。

- vCenter 6.7

- 仮想マシンに、VMware ツールがインストールされている必要があります。

前提条件ソフトウェアのインストール

始める前に

物理的または仮想的な設定があり、システムがFirepower Management Center と通信できることを確認してください。

ステップ 1 (オプション) テキストエディタを使用して `/etc/environment` を編集し、次の変数をエクスポートして、Ubuntu マシンがインターネットプロキシの背後にある場合にインターネットと通信できるようにします。

変数	値
<code>export http_proxy</code>	HTTP プロキシで使します。 <code>user:pass@host-or-ip:port</code>
<code>export https_proxy</code>	HTTPS プロキシでこれを使します。 <code>user:pass@host-or-ip:port</code>
<code>export no_proxy</code>	プロキシ構成を削除します。 <code>export no_proxy="localhost,127.0.0.1"</code>

例 :

認証なしの HTTP プロキシ :

```
vi /etc/environment
export http_proxy="myproxy.example.com:8181"
```

認証付き HTTPS プロキシ :

```
vi /etc/environment
export https_proxy="ben.smith:bens-password@myproxy.example.com:8181"
```

ステップ 2 別のコマンドウィンドウを使用して設定を確認します。

```
env grep | proxy
```

結果の例 :

```
http_proxy=myproxy.example.com:8181
```

ステップ 3 次のいずれかのセクションに進みます。

関連トピック

[前提条件ソフトウェアのインストール : Ubuntu](#) (9 ページ)

[前提条件ソフトウェアのインストール : CentOS](#) (7 ページ)

[前提条件ソフトウェアのインストール : RHEL](#) (8 ページ)

前提条件ソフトウェアのインストール : CentOS

始める前に

次のことをすべて行います。

- システムがサポートされているオペレーティングシステムとサードパーティソフトウェア (5 ページ) で説明した前提条件を満たしていることを確認します。
- (オプション) dynamic attributes connector へのプロキシアクセスが必要な場合は、[前提条件ソフトウェアのインストール \(6 ページ\)](#) を参照してください。

ステップ 1 Docker がインストールされていないことを確認し、インストールされている場合はアンインストールします。

```
docker --version
```

Docker がインストールされている場合は、[Ubuntu での Docker エンジンのアンインストール](#)の説明に従ってアンインストールします。

ステップ 2 リポジトリを更新およびアップグレードします。

CentOS 7 :

```
sudo yum -y update && sudo yum -y upgrade
```

ステップ 3 epel リポジトリをインストールします。

CentOS 7 :

```
sudo yum -y install epel-release
```

ステップ 4 (CentOS 7 のみ。) Python3 をインストールします。

```
sudo yum install -y python3 libseline-python3
```

ステップ 5 Ansible をインストールします。

CentOS 7 および CentOS 8 :

```
sudo yum install -y ansible
```

ステップ 6 Ansible のバージョンが 2.9 以降であることを確認します。

CentOS 7 :

```
ansible --version
ansible 2.9.24
config file = /etc/ansible/ansible.cfg
configured module search path = [u'/home/admin/.ansible/plugins/modules',
u'/usr/share/ansible/plugins/modules']
ansible python module location = /usr/lib/python2.7/site-packages/ansible
executable location = /usr/bin/ansible
python version = 2.7.5 (default, Apr 2 2020, 13:16:51) [GCC 4.8.5 20150623 (Red Hat 4.8.5-39)]
```

- (注) 前出の出力が示すように、Ansible が Python 2.x を参照するのは正常です。コネクタは引き続き Python 3 を使用します。

次のタスク

[Cisco Secure 動的属性コネクタ のインストール \(11 ページ\)](#) で説明されているように、コネクタをインストールします。

オプションで `dynamic attributes connector` でのプロキシの使用を停止するには、`/etc/environment` を編集してプロキシ構成を削除します。

前提条件ソフトウェアのインストール : RHEL

始める前に

次のことをすべて行います。

- システムがサポートされているオペレーティングシステムとサードパーティソフトウェア ([5 ページ](#)) で説明した前提条件を満たしていることを確認します。
- (オプション) `dynamic attributes connector` へのプロキシアクセスが必要な場合は、[前提条件ソフトウェアのインストール \(6 ページ\)](#) を参照してください。

ステップ 1 Docker がインストールされていないことを確認し、インストールされている場合はアンインストールします。

```
docker --version
```

Docker がインストールされている場合は、[Ubuntu](#) での [Docker エンジンのアンインストール](#) の説明に従ってアンインストールします。

ステップ 2 リポジトリを更新します。

RHEL 7 :

```
sudo yum -y update && sudo yum -y upgrade
```

RHEL 8 :

```
sudo dnf -y update && sudo dnf -y upgrade
```

ステップ 3 epel リポジトリをインストールします。

RHEL 7 :

```
sudo yum -y install https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm
```

RHEL 8 :

```
sudo dnf -y install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
```

ステップ 4 (RHEL 7 のみ。) Python3 をインストールします。

```
sudo yum install -y python3 libselinux-python3
```

ステップ 5 Ansible をインストールします。

RHEL 7 :

```
sudo yum -y install ansible
```

RHEL 8 :

```
sudo dnf install -y ansible
```

ステップ 6 Ansible のバージョンを確認します。

```
ansible --version
```

次に例を示します。

RHEL 7 :

```
ansible 2.9.24
  config file = /etc/ansible/ansible.cfg
  configured module search path = [u'/home/stevej/.ansible/plugins/modules',
u'/usr/share/ansible/plugins/modules']
  ansible python module location = /usr/lib/python2.7/site-packages/ansible
  executable location = /usr/bin/ansible
  python version = 2.7.5 (default, Mar 20 2020, 17:08:22) [GCC 4.8.5 20150623 (Red Hat 4.8.5-39)]
```

(注) 前出の出力が示すように、Ansible が Python 2.x を参照するのは正常です。コネクタは引き続き Python 3 を使用します。

RHEL 8 :

```
ansible 2.9.24
  config file = /etc/ansible/ansible.cfg
  configured module search path = ['/home/stevej/.ansible/plugins/modules',
'/usr/share/ansible/plugins/modules']
  ansible python module location = /usr/lib/python3.6/site-packages/ansible
  executable location = /usr/bin/ansible
  python version = 3.6.8 (default, Mar 18 2021, 08:58:41) [GCC 8.4.1 20200928 (Red Hat 8.4.1-1)]
```

次のタスク

[Cisco Secure 動的属性コネクタのインストール \(11 ページ\)](#) で説明されているように、コネクタをインストールします。

オプションで `dynamic attributes connector` でのプロキシの使用を停止するには、`/etc/environment` を編集してプロキシ構成を削除します。

前提条件ソフトウェアのインストール : Ubuntu

ステップ 1 Docker がインストールされていないことを確認し、インストールされている場合はアンインストールします。

```
docker --version
```

Docker がインストールされている場合は、[Ubuntu](#) での [Docker エンジン](#) のアンインストールの説明に従ってアンインストールします。

ステップ 2 リポジトリを更新します。

```
sudo apt -y update && sudo apt -y upgrade
```

ステップ 3 Python のバージョンを確認します。

```
/usr/bin/python3 --version
```

バージョンが 3.6 より前の場合は、バージョン 3.6.x をインストールする必要があります。

ステップ 4 Python 3.6 をインストールします。

```
sudo apt -y install python3.6
```

ステップ 5 共通ライブラリをインストールします。

```
sudo apt -y install software-properties-common
```

ステップ 6 Ansible をインストールします。

```
sudo apt-add-repository -y -u ppa:ansible/ansible && sudo apt -y install ansible
```

ステップ 7 Ansible のバージョンを確認します。

```
ansible --version
```

次に例を示します。

```
ansible --version
ansible 2.9.19
  config file = /etc/ansible/ansible.cfg
  configured module search path = [u'/home/admin/.ansible/plugins/modules',
u'/usr/share/ansible/plugins/modules']
  ansible python module location = /usr/lib/python2.7/dist-packages/ansible
  executable location = /usr/bin/ansible
  python version = 2.7.17 (default, Feb 27 2021, 15:10:58) [GCC 7.5.0]
```

(注) 前出の出力が示すように、Ansible が Python 2.x を参照するのは正常です。コネクタは引き続き Python 3.6 を使用します。

次のタスク

[Cisco Secure 動的属性コネクタ のインストール \(11 ページ\)](#) で説明されているように、コネクタをインストールします。

オプションで `dynamic attributes connector` でのプロキシの使用を停止するには、`/etc/environment` を編集してプロキシ構成を削除します。

Cisco Secure 動的属性コネクタ のインストール

インストールについて

このトピックでは、Cisco Secure 動的属性コネクタ のインストールについて説明します。sudo 権限を持つユーザーとしてコネクタをインストールする必要がありますが、非権限ユーザーとしてコネクタを実行できます。

はじめる前に

システムに次の前提条件ソフトウェアがインストールされていることを確認してください。

- Ubuntu 18.04 または 20.04
- CentOS 7 Linux または 8
- Red Hat Enterprise Linux (RHEL) 7 または 8
- Python 3.6.x
- Ansible 2.9 以降

すべてのオペレーティングシステムの最小要件：

- 4 個の CPU
- 8 GB RAM
- 100 GB 使用可能なディスクスペース

vCenter 属性を使用する場合は、次も必要です。

- vCenter 6.7
- 仮想マシンに、VMware ツールがインストールされている必要があります。

前提条件ソフトウェアをインストールするには、[前提条件ソフトウェアのインストール \(6 ページ\)](#) を参照してください。

Readme とリリース ノートの表示

最新のインストール情報については、以下を参照してください。

Readme : <https://galaxy.ansible.com/cisco/csdac>

リリースノート : [Cisco Secure 動的属性コネクタ リリースノート](#)

動的属性コネクタソフトウェアの取得

動的属性コネクタ ソフトウェアの最新バージョンを取得するには、次のコマンドを実行します。

```
ansible-galaxy collection install cisco.csdac
```

ムスター（収集）サービスのインストール

ムスター（収集）サービスは、動的属性コネクタの別名です。

~/ansible/collections/ansible_collections/cisco/csdac ディレクトリから次のコマンドを実行します。

```
ansible-playbook default_playbook.yml [--ask-become-pass] [--extra-vars " vars " ]
```

構文の説明

--ask-become-pass **sudo** パスワードを入力するように求められます。マシンで **sudo** が有効になっている場合は必須です。

--extra-vars 次のオプションの追加変数により、動的属性コネクタがプロキシを使用できるようになります。使用する値は、[前提条件ソフトウェアのインストール（6 ページ）](#)の説明に従って構成した `/etc/environment` の値と一致する必要があります。

- **csdac_proxy_enabled=true**
- **csdac_http_proxy_url=http://PROXY_URL**
csdac_https_proxy_url=PROXY_URL

次のオプションの追加変数は、動的属性コネクタに安全に接続するために使用できる自己署名証明書を作成します。これらのパラメータを省略すると、動的属性コネクタはデフォルトの証明書を使用します。

- **csdac_certificate_domain**
自動生成された証明書のドメイン名。デフォルト値は、ホストの自動検出されたホスト名です (ansible によって検出される)
- **csdac_certificate_country_name**
Two-letter country code. (デフォルト値は us)
- **csdac_certificate_organization_name**
組織名。 (デフォルト値は cisco)
- **csdac_certificate_organization_unit_name**
組織単位名 (デフォルト値は Cisco)

デフォルトの証明書を使用したインストール例

たとえば、デフォルトのオプションでソフトウェアをインストールするには：

```
ansible-galaxy collection install cisco.csdac
cd ~/.ansible/collections/ansible_collections/cisco/csdac
ansible-playbook default_playbook.yml --ask-become-pass
```

オプションの証明書を使用したインストール例

たとえば、オプションの証明書を使用してソフトウェアをインストールするには：

```
ansible-galaxy collection install cisco.csdac
cd ~/.ansible/collections/ansible_collections/cisco/csdac
ansible-playbook default_playbook.yml --ask-become-pass --extra-vars
"csdac_certificate_domain=domain.example.com csdac_certificate_country_name=US
csdac_certificate_organization_name=Cisco
csdac_certificate_organization_unit_name=Engineering"
```

証明書を作成したら、コネクタへのアクセスに使用する Web ブラウザに証明書をインポートします。証明書は ~/csdac/app/config/certs ディレクトリに作成されます。

インストールログの表示

インストールログは次の場所にあります。

```
~/.ansible/collections/ansible_collections/cisco/csdac/logs/csdac.log
```

証明書を使用した **dynamic attributes connector** への接続

証明書とキーがある場合は、それらを仮想マシンの ~/csdac/app/config/certs ディレクトリに配置します。

前のタスクを実行した後、次のコマンドを入力して、dynamic attributes connector の Docker コンテナを再起動します。

```
docker restart muster-ui
```

コネクタへのログイン

1. `https://ip-address` で 動的属性コネクタ にアクセスします。
2. ログインします。

初回ログインのユーザー名は `admin`、パスワードは `admin` です。初めてログインしたときに、パスワードを変更するよう求められます。

Cisco Secure 動的属性コネクタのアップグレード

このトピックでは、Cisco Secure 動的属性コネクタ バージョン 1.0 からバージョン 1.1 にアップグレードする方法について説明します。バージョン 1.0 は Ubuntu 18.04 でのみ利用可能だったため、これらの手順が適用されるオペレーティングシステムは Ubuntu 18.04 だけです。

このトピックでは、以前の Cisco Secure 動的属性コネクタ を現在のバージョンにアップグレードする方法について説明します。これらのタスクは、Cisco Secure 動的属性コネクタ のバージョンやオペレーティングシステムに関係なく実行できます。

ステップ 1 アップグレードするマシンにログインします。

ステップ 2 次のコマンドを入力します。

```
ansible-galaxy collection install cisco.csdac --force
ansible-playbook default_playbook.yml --ask-become-pass
ansible-playbook default_playbook.yml --ask-become-pass [--extra-vars vars]
```

構文の説明

--ask-become-pass **sudo** パスワードを入力するように求められます。マシンで **sudo** が有効になっている場合は必須です。

--extra-vars 次のオプションの追加変数により、動的属性コネクタがプロキシを使用できるようになります。使用する値は、[前提条件ソフトウェアのインストール \(6 ページ\)](#) の説明に従って構成した `/etc/environment` の値と一致する必要があります。

- **csdac_proxy_enabled=true**
- **csdac_http_proxy_url=http://PROXY_URL**
- **csdac_https_proxy_url=PROXY_URL**

次のオプションの追加変数は、動的属性コネクタに安全に接続するために使用できる自己署名証明書を作成します。これらのパラメータを省略すると、動的属性コネクタはデフォルトの証明書を使用します。

- **csdac_certificate_domain**
自動生成された証明書のドメイン名。デフォルト値は、ホストの自動検出されたホスト名です (ansible によって検出される)
- **csdac_certificate_country_name**
Two-letter country code. (デフォルト値は us)
- **csdac_certificate_organization_name**
組織名。 (デフォルト値は cisco)
- **csdac_certificate_organization_unit_name**
組織単位名 (デフォルト値は Cisco)

ステップ 3 アップグレードが完了するまで待ちます。

ステップ 4 アップグレードのログは次の場所にあります。

```
~/.ansible/collections/ansible_collections/cisco/csdac/logs/csdac.log
```

次のタスク

「[コネクタの作成 \(15 ページ\)](#)」を参照してください。



第 3 章

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 \(15 ページ\)](#)
- [アダプタの作成 \(28 ページ\)](#)
- [動的属性フィルタの作成 \(36 ページ\)](#)

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、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 2: 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（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。

-
- 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 **[ユーザーの追加 (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。

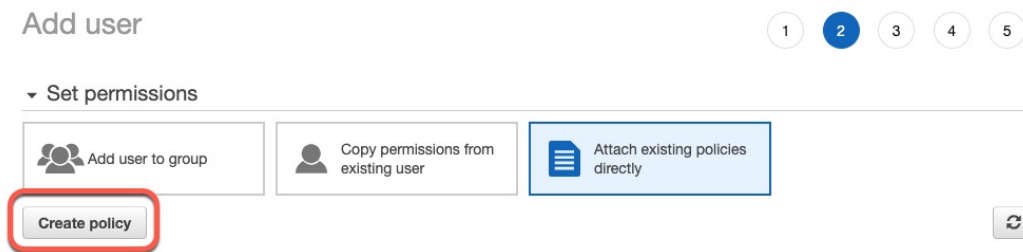
(注) これが、ユーザーのキーを取得する必要がある唯一の機会です。

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 \(18 ページ\)](#)。

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 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。 [\(16 ページ\)](#) 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 \(28 ページ\)](#)

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 \(19 ページ\)](#) を参照してください。

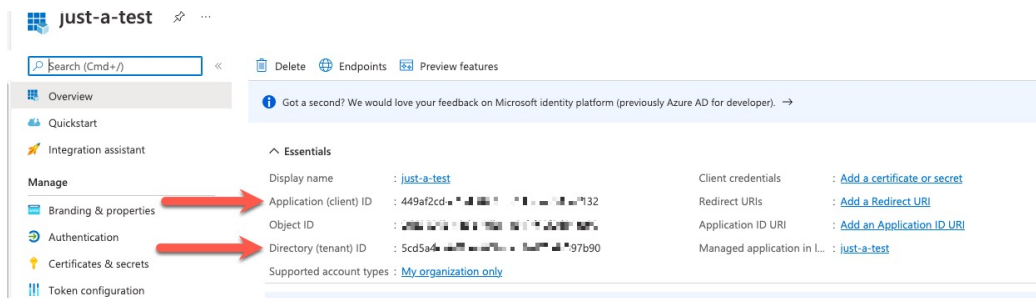
始める前に

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。

-
- 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。

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



- 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なため、クライアント値をクリップボードにコピーします。

Description	Expires	Value	Secret ID	Copy to clipboard
Sample only	10/15/2022	r_Wi...S9wMK...	...8fa75b1	

- 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。

The screenshot shows the 'Add role assignment' dialog in the Azure portal. The 'Members' tab is active, and a search for 'just' has been performed, resulting in 'No users, groups, or service principals found.' The 'Selected role' is 'Reader', and 'Assign access to' is set to 'User, group, or service principal'. The 'Members' list is currently empty. The 'Description' field contains the text 'Optional'. At the bottom, there are buttons for 'Review + assign', 'Previous', 'Next', 'Select', and '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 \(21 ページ\)](#)」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 \(19 ページ\)](#) 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 \(28 ページ\)](#)

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 \(28 ページ\)](#)

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 \(28 ページ\)](#)

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 \(30 ページ\)](#) 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。

- 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。
- 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。
- 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 \(30 ページ\)](#) 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。 <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 \(28 ページ\)](#)

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。

User Configuration

User Name

Real Name

Authentication Use External Authentication Method

Password

Confirm Password

Maximum Number of Failed Logins (0 = Unlimited)

Minimum Password Length

Days Until Password Expiration (0 = Unlimited)

Days Before Password Expiration Warning

Options

- Force Password Reset on Login
- Check Password Strength
- Exempt from Browser Session Timeout

User Role Configuration

Default User Roles

- Administrator
- External Database User (Read Only)
- Security Analyst
- Security Analyst (Read Only)
- Security Approver
- Intrusion Admin
- Access Admin
- Network Admin
- Maintenance User
- Discovery Admin
- 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 \(28 ページ\)](#)

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 \(26 ページ\)](#)
- [アダプタの作成 \(28 ページ\)](#)

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
```

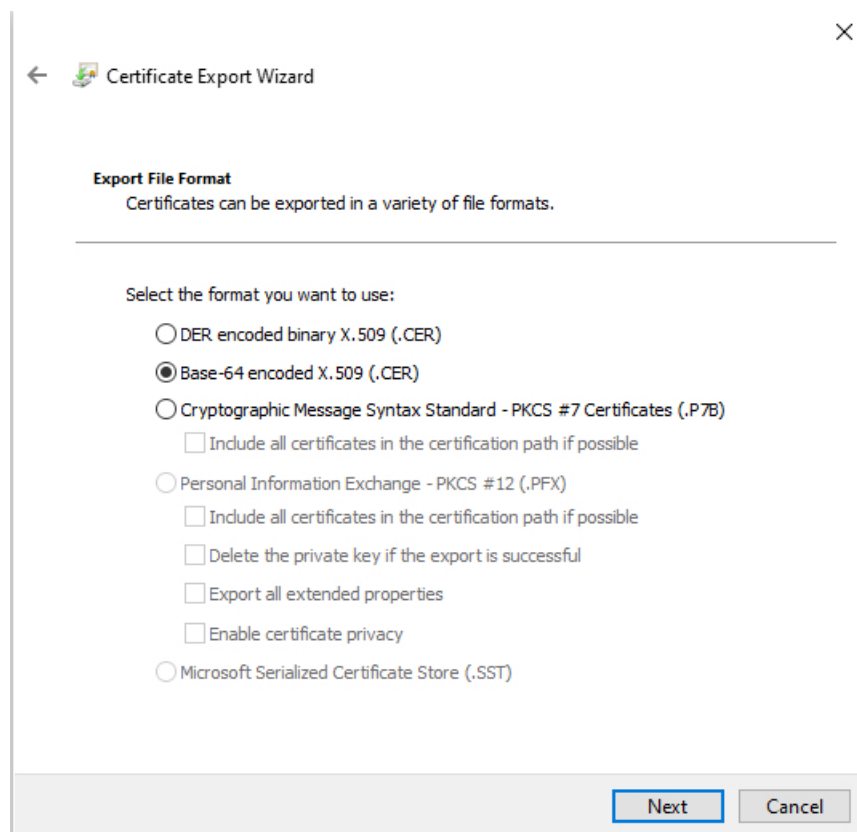
3. 証明書チェーン全体をプレーンテキストファイルに保存します。
 - すべての -----BEGIN CERTIFICATE----- および -----END CERTIFICATE----- 区切り文字を含めます。
 - 無関係なテキスト (たとえば、証明書の名前、山かっこ (<および>) に含まれるテキスト、および山かっこ自体を除外します。
4. vCenter と FMC の両方で、これらのタスクを繰り返します。

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。

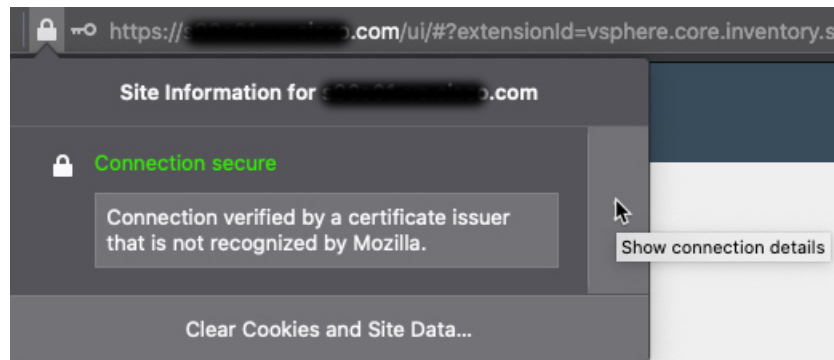


10. 指示に従ってエクスポートを完了します。
11. 証明書をテキストエディタで開きます。
12. チェーン内のすべての証明書に対してこのプロセスを繰り返します。
テキストエディタに各証明書を最初から最後まで順番に貼り付ける必要があります。
13. vCenter と FMC の両方でこれらのタスクを繰り返します。

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。

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 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 \(30 ページ\)](#) 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。

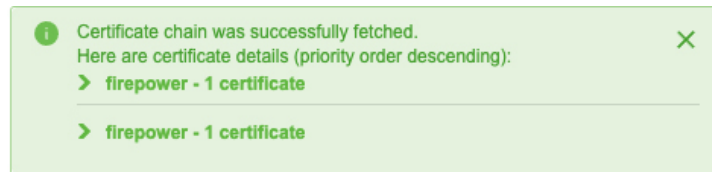
ステップ 5 [Fetch] をクリックします。

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 \(28 ページ\)](#) 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 (30 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 \(42 ページ\)](#) 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 \(6 ページ\)](#)
- [コネクタの作成 \(15 ページ\)](#)
- [アダプタの作成 \(28 ページ\)](#)

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	<ul style="list-style-type: none"> • 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。 <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)]。 • 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。

- 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。

Edit Dynamic Attribute Filter

Name* Connector*

Query*

Type	Op.	Value
<input type="button" value="all"/> network	eq	<input type="button" value="any"/> myVLAN

[> Show Preview](#)

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="button" value="all"/> host	eq	<input type="button" value="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="button" value="all"/> Finance	eq	<input type="button" value="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="button" value="all"/> FinanceApp	eq	<input type="button" value="any"/> 1

> Show Preview



第 4 章

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

dynamic attributes connector 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 FMC 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 \(41 ページ\)](#)
- [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 \(42 ページ\)](#)

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

動的属性フィルタを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 オンプレミス Firewall Management Center またはアダプタに自動的にプッシュされます。

これらのダイナミックオブジェクトは、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) 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。

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（これらのダイナミックオブジェクトは、前に作成した動的属性フィルタにちなんで命名されます）。

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) 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。

ステップ 1 FMC にログインします。

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

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

ステップ 4 [ルールの追加 (Add Rule)] をクリックします。

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

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

次の図は例を示しています。

The screenshot shows the 'Add Rule' configuration interface. At the top, there are fields for 'Name', 'Enabled' (checked), 'Insert' (set to 'into Mandatory'), 'Action' (set to 'Allow'), and 'Time Range' (set to 'None'). Below these are tabs for 'Zones', 'Networks', 'VLAN Tags', 'Users', 'Applications', 'Ports', 'URLs', 'Dynamic Attributes', 'Inspection', 'Logging', and 'Comments'. The 'Dynamic Attributes' tab is active. Under 'Available Attributes', there is a search bar and a list with 'Dynamic Objects' selected and 'FinanceNetwork' highlighted. 'Add to Source' and 'Add to Destination' buttons are visible. The 'Selected Source Attributes' and 'Selected Destination Attributes' sections are empty, both containing the text 'any'. At the bottom right, there are 'Cancel' and 'Add' buttons.

前の例は、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7 目的のオブジェクトを送信元または接続先属性に追加します。

ステップ8 必要に応じて、ルールに他の条件を追加します。

次のタスク

『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](#))



第 5 章

動的属性コネクタのトラブルシューティング

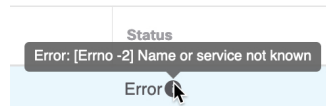
提供されているツールの使用など、dynamic attributes connector で問題をトラブルシューティングする方法。

- エラーメッセージのトラブルシューティング (45 ページ)
- トラブルシューティング ツール (47 ページ)
- 認証局 (CA) チェーンの手動での取得 (49 ページ)

エラーメッセージのトラブルシューティング

問題：名前またはサービスが不明なエラー

このエラーは、アダプタまたはコネクタのエラー状態にマウスを合わせると、ツールチップとして表示されます。次に例を示します。実際の表示とは異なる場合があります。



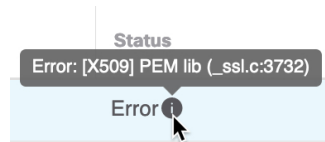
解決策：コネクタまたはアダプタを編集して、次を確認します。

- ホスト名の末尾のスラッシュ
- (FMC アダプタのみ。) ホスト名の先頭にあるスキーム (例 : `https://`)
- パスワードが正しいことを確認する
- FMC アダプタの場合、[FMCサーバー証明書 (FMC Server Certificate)] フィールドの内容を確認します。

詳細については、[認証局 \(CA\) チェーンの手動での取得 \(30 ページ\)](#) を参照してください。

問題 : [X509 PEM lib]

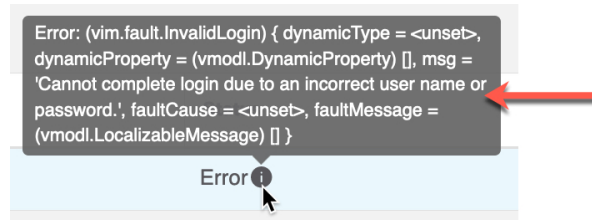
このエラーは、コネクタのエラー状態にマウスを合わせると、ツールチップとして表示されます。



解決策 : コネクタを編集し、CA チェーンを確認します。詳細については、[認証局\(CA\)チェーンの手動での取得 \(30 ページ\)](#) を参照してください。

問題 : 正しくないユーザー名またはパスワード

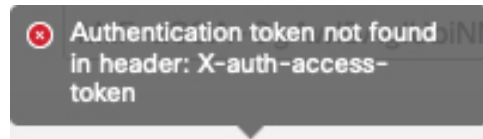
このエラーは、コネクタのエラー状態にマウスを合わせると、ツールチップとして表示されます。



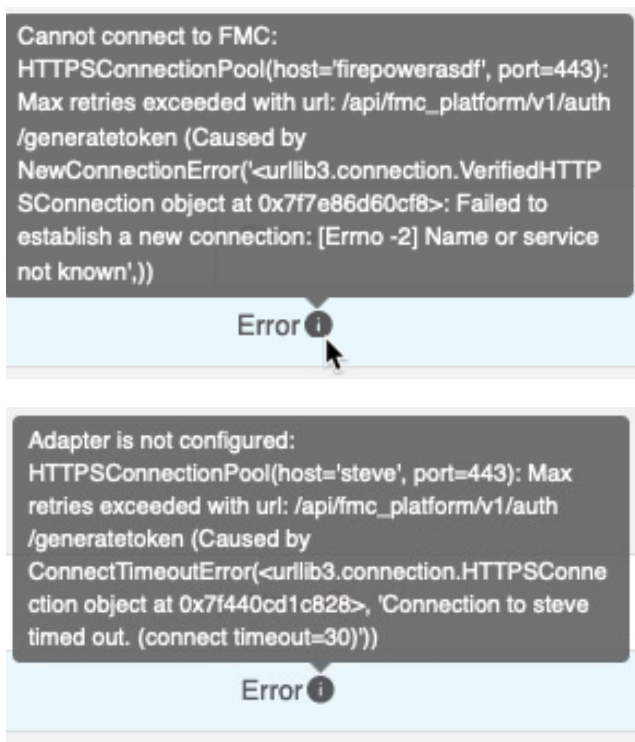
解決策 : コネクタを編集し、ユーザー名またはパスワードを変更します。

問題 : ヘッダーに認証トークンが見つかりません

このエラーは、FMC に対する十分な権限を持たないアダプタユーザーとの接続をテストしようとする则表示されます。

**問題 : アダプタのタイムアウトまたは最大再試行エラー**

このエラーは、アダプタのエラー状態にマウスを合わせると、ツールチップとして表示されます。



解決策：次のすべてを実行します。

- 管理センターが実行されていることを確認します。
- [FMCサーバー証明書 (FMC Server Certificate)] フィールドの内容を確認します。
- [IP] フィールドに入力した値が証明書の共通名と正確に一致していることを確認します。

詳細については、[認証局 \(CA\) チェーンの手動での取得 \(30 ページ\)](#) を参照してください。

トラブルシューティング ツール

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、**dynamic attributes connector** 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

dynamic attributes connector 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 ~/csdac/app
sudo ./muster-cli status
```

出力例を次に示します。

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

```

-----
muster-bee      ./docker-entrypoint.sh run ...  Up           50049/tcp, 50050/tcp
muster-etcd    etcd                               Up           2379/tcp, 2380/tcp
muster-ui      /docker-entrypoint.sh runs ...  Up (healthy) 0.0.0.0:443->8443/tcp, :::443->8443/tcp
muster-ui-backend ./docker-entrypoint.sh run ...  Up           50031/tcp
===== CONNECTORS AND ADAPTERS =====
-----
Name                                Command                                State        Ports
-----
muster-adapter-fmc.1                ./docker-entrypoint.sh run ...       Up           50070/tcp
muster-connector-vcenter.1          ./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

```

デバッグロ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
<code>/csdac/app/ts-bundle-timestamp/info</code>	etcd データベース格納ファイル
<code>/csdac/app/ts-bundle-timestamp/logs</code>	コンテナログファイル
<code>/csdac/app/ts-bundle-timestamp/status.log</code>	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

ダイナミックオブジェクトの確認

コネクタとアダプタがFMCでオブジェクトを作成していることを確認するには、FMC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/usmshredsvcs.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": []
}
```

例：失敗したオブジェクトの作成（この場合、アダプタユーザーに十分な権限がないため）：

```
26-Aug-2021 12:47:50.440, [INFO], (DefenseCenterServiceImpl.java:1442)
com.cisco.nm.vms.api.dc.DefenseCenterServiceImpl, ajp-nio-127.0.0.1-9009-exec-2
** REST Request [ CSM ]
** ID : 58566831-7532-4d61-a579-2bbc3c325b2f
** URL: POST /audit
{
  "version": "7.1.0",
  "requestId": "58566831-7532-4d61-a579-2bbc3c325b2f",
  "data": {
    "userName": "csdac-centos7",
    "subsystem": "API",
    "message": "GET
https://myfmc.example.com/api/fmc_config/v1/domain/e276abec-e0f2-11e3-8169-6d9ed49b625f/
object/dynamicobjects/vCenter_CentOS_7_4 Forbidden (403) - The server understood the
request, but is refusing to fulfill it",
    "sourceIP": "192.0.2.103",
    "domainUuid": "e276abec-e0f2-11e3-8169-6d9ed49b625f",
    "time": "1629982070404"
  },
  "deleteList": []
}
```

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 \(26 ページ\)](#)
- [アダプタの作成 \(28 ページ\)](#)

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。

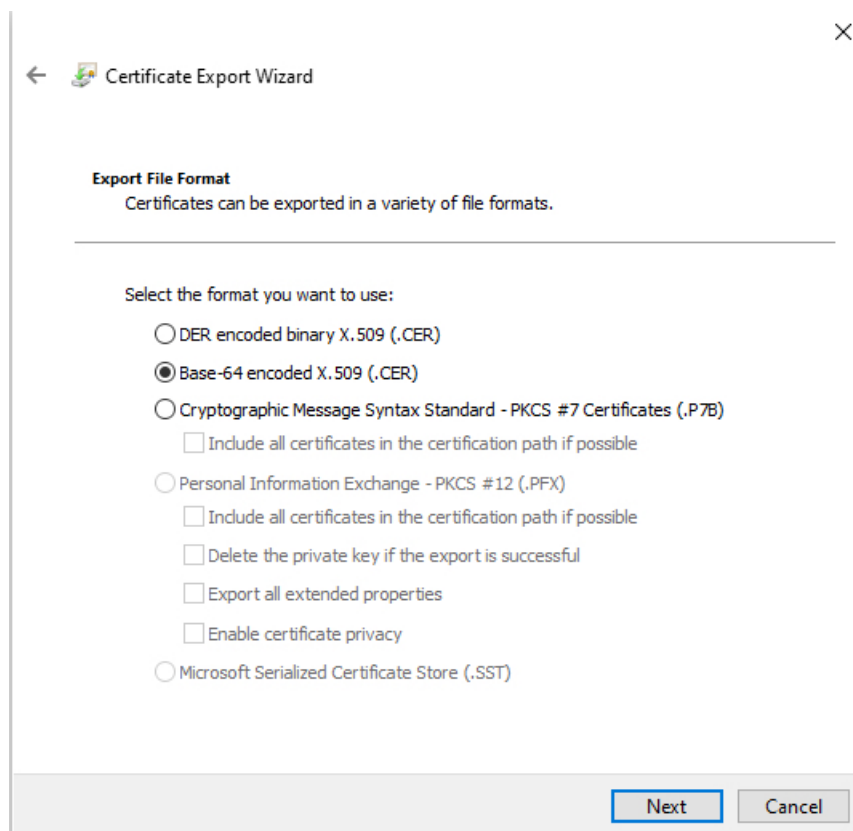
証明書チェーンの取得 : Windows Chrome

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。

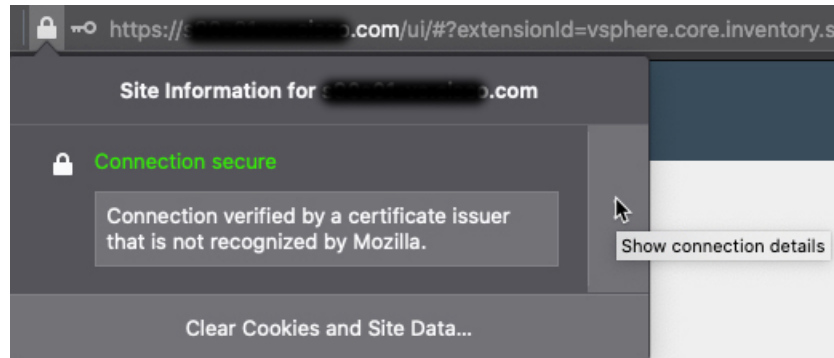


10. 指示に従ってエクスポートを完了します。
11. 証明書をテキストエディタで開きます。
12. チェーン内のすべての証明書に対してこのプロセスを繰り返します。
テキストエディタに各証明書を最初から最後まで順番に貼り付ける必要があります。
13. vCenter と FMC の両方でこれらのタスクを繰り返します。

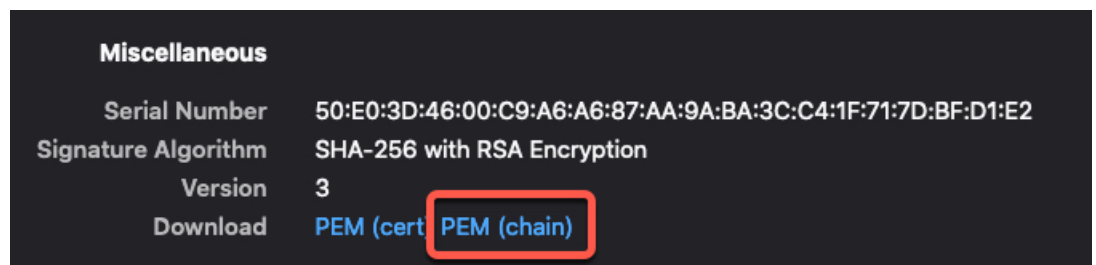
証明書チェーンの取得 : Windows Firefox

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。



付録 **A**

セキュリティとインターネットアクセス

動的属性コネクタがクラウドサービスプロバイダーおよびFMCと通信するときに使用するURLのリスト。

- [セキュリティ要件 \(53 ページ\)](#)
- [インターネットアクセス要件 \(53 ページ\)](#)

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FMCが同じネットワーク上に存在している場合は、FMC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、FMC 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 **FMC** 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
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

動的属性コネクタ **AWS** 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内部的に、動的属性コネクタに指定されたリージョンに基づいて、サービスエンドポイント URL をクエリします。それらは AWS Web サイト <https://docs.aws.amazon.com/general/latest/gr/ec2-service.html> に文書化されています。

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。

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。