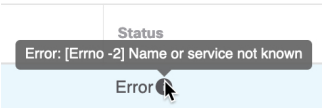
動的属性コネクタのトラブルシューティング

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

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。



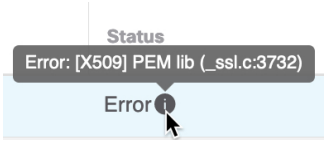
解決策：コネクタまたはアダプタを編集して、次を確認します。

- 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]

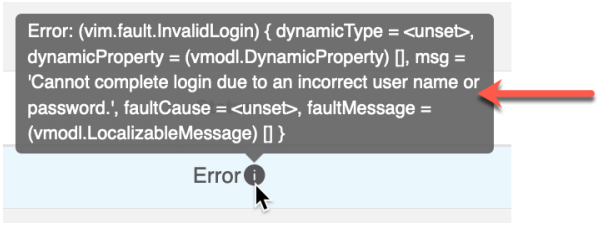
このエラーは、コネクタのエラー状態にマウスを合わせると、ツールチップとして表示されます。



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

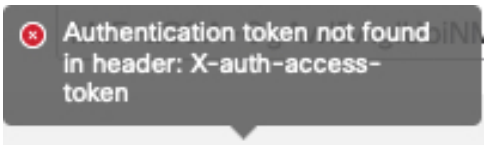
このエラーは、コネクタのエラー状態にマウスを合わせると、ツールチップとして表示されます。



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。

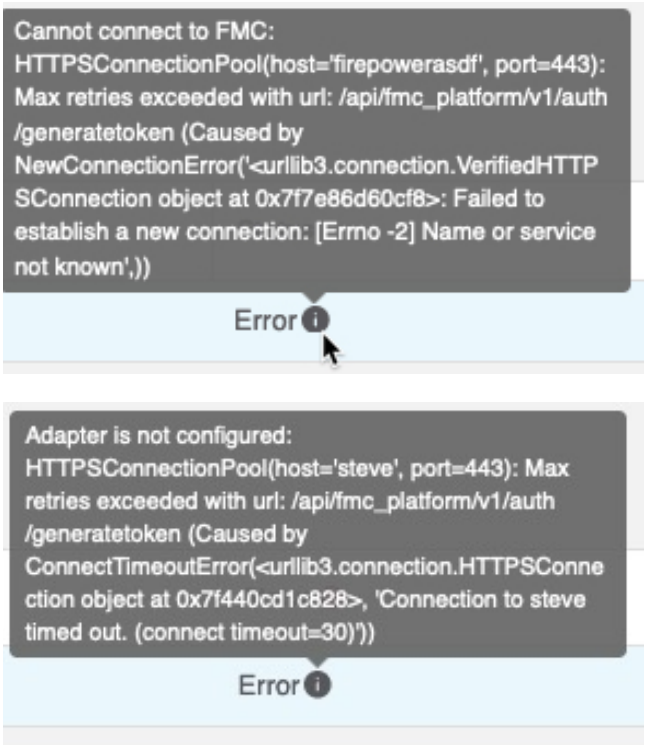
問題：ヘッダーに認証トークンが見つかりません

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と表示されます。



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
```

デバッグロギングの有効化とトラブルシューティング ファイルの生成

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

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

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

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

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

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/usmsharedsvcs.log
```

例：成功したオブジェクトの作成

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

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
- アダプタの作成

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。

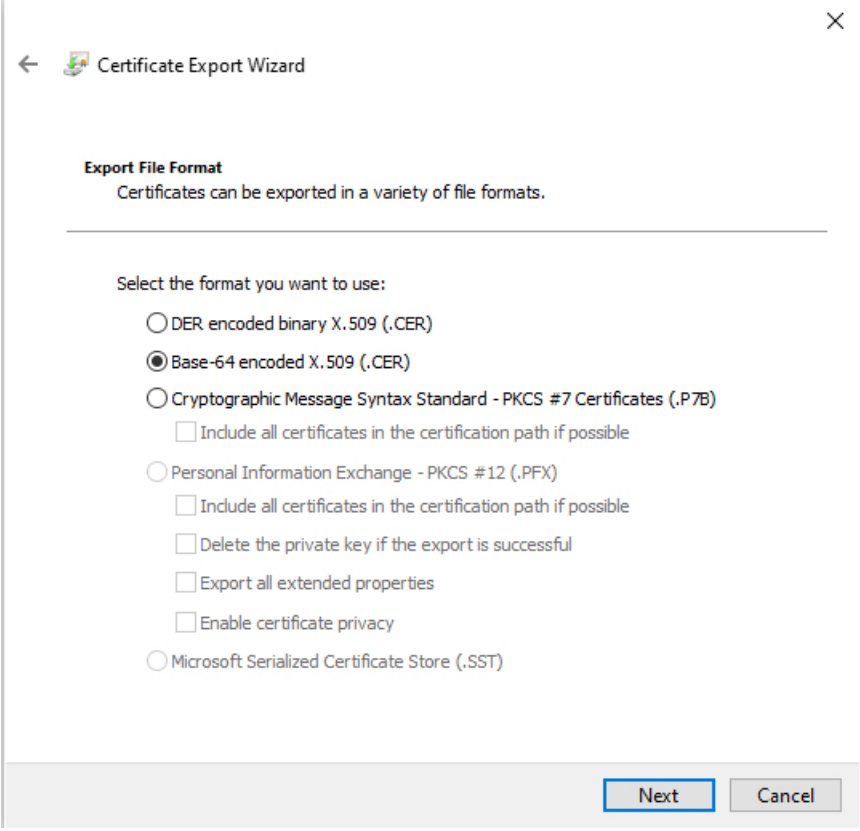
証明書チェーンの取得：Windows Chrome

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。



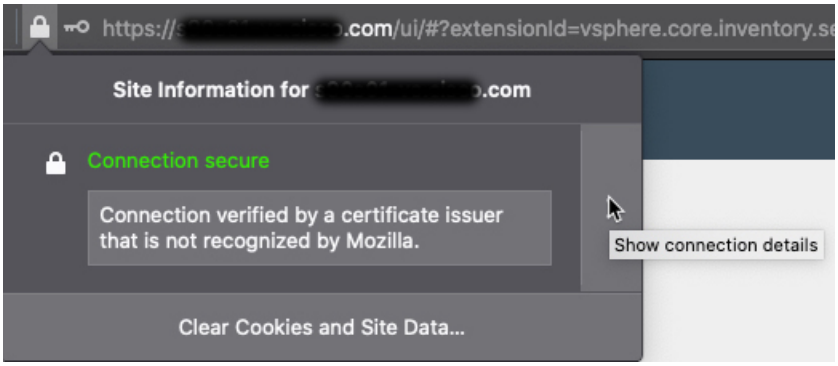
10. 指示に従ってエクスポートを完了します。
11. 証明書をテキストエディタで開きます。
12. チェーン内のすべての証明書に対してこのプロセスを繰り返します。

    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。

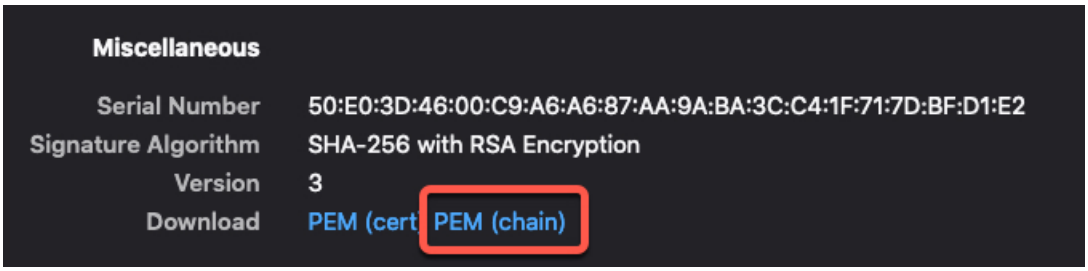
証明書チェーンの取得：Windows Firefox

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。

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。