REST APIによるASAからFDMへのDAPおよびHostScanの移行

内容

概要

このドキュメントでは、Cisco Adaptive Security Appliances(ASA)からFirepower Device Manager(FDM)によってローカルで管理されるCisco Firepower Threat Defense(FTD)へのダイナミックアクセスポリシー(DAP)およびHostScan設定の移行について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- FDMでのRA VPN設定に関する基礎知識。
- ASAでのDAPおよびHostscanの動作。
- REST APIおよびFDM Rest API エクスプローラの基礎知識。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- バージョン6.7.0が稼働するCisco FTD
- Cisco AnyConnect Secure Mobility Clientversion 4.9.00086
- Postmanまたはその他のAPI開発ツール

注：このドキュメントの情報は、特定のラボ環境のデバイスから作成されたものです。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。ネットワークが稼働中の場合は、設定変更による潜在的な影響について理解してお

いてください。

背景説明

FTDではリモートアクセスVPN(RAVPN)の設定がサポートされていますが、DAPのサポートはありません。リリース6.7.0以降、FTDでDAPのAPIサポートが追加されました。これは、ASAからFTDへの移行の非常に基本的な使用例をサポートすることを目的としています。ASAでDAPが設定されており、FTDに移行する途中のユーザには、RA VPN設定とともにDAP設定を移行するパスが用意されています。

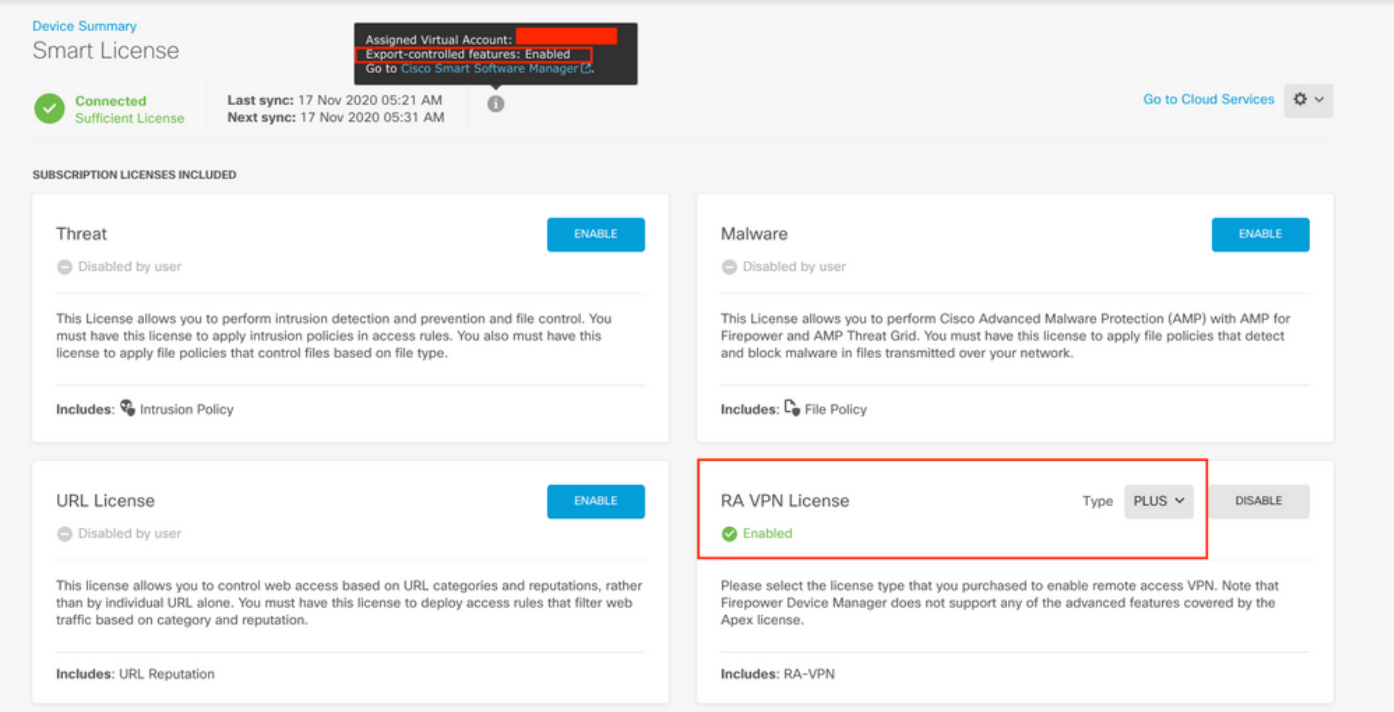
DAP設定をASAからFTDに正常に移行するには、次の条件を確認します。

- DAP/ホストスキャンが設定されたASA。
- ASAまたはASDMからASAへのTFTP/FTPサーバアクセス。
- バージョン6.7.0以降を実行するCisco FTDは、Firepower Device Manager(FDM)によって管理されます。
- FTDで設定され、動作しているRA VPN。

ライセンス

- [Export Controlled Features]を有効にしてスマートライセンスポータルに登録されたFTD（RA VPN設定タブを有効にするために）。
- 有効になっているAnyConnectライセンス（APEX、Plus、またはVPN-Only）。

ライセンスを確認するには：**[Devices] > [Smart Licenses]に移動します。**



機能制限

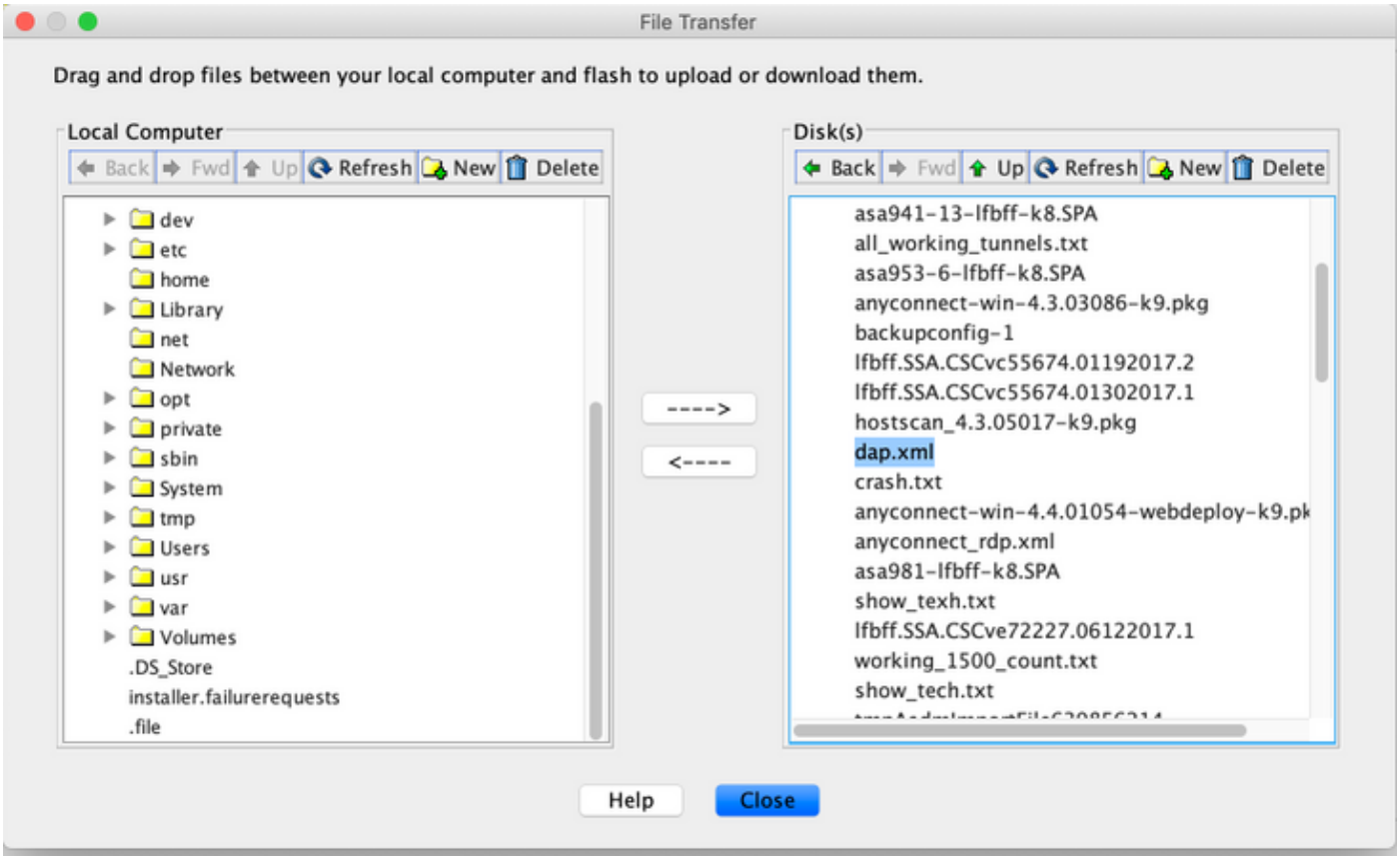
- これらの機能は、FDM/FTD REST APIインターフェイスでのみサポートされます。
- DAP名にREST APIの空白文字を含めることはできません。

コンフィギュレーション

ステップ 1： ASAからローカルPC/TFTPサーバにdap.xmlをコピーします。これを実現するには、次の2つの方法があります。

ASDM:

[Tools] > [File Management] > **[File Transfer] > [Local PC and Flash]に移動します。**



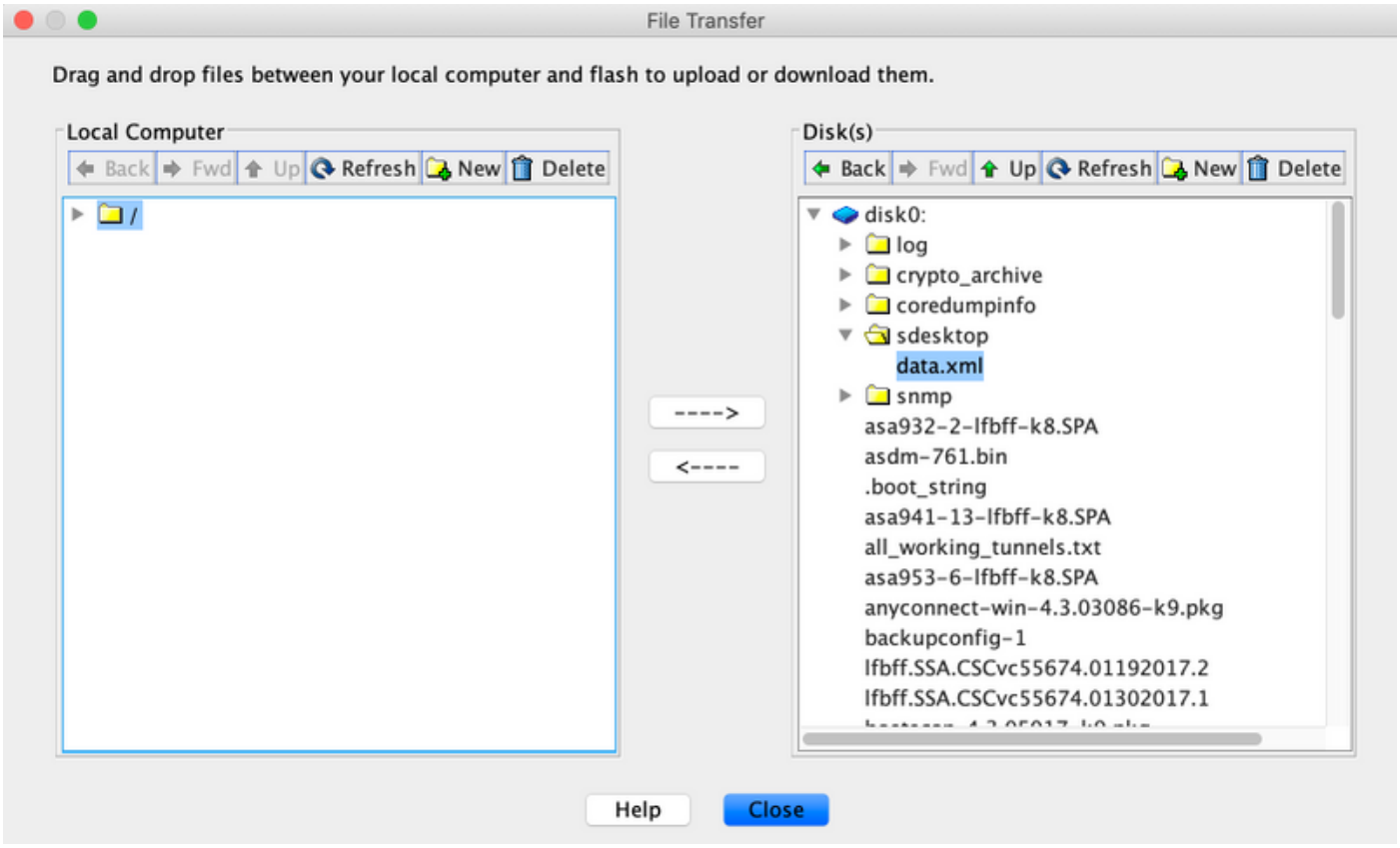
CLI：

```
ASA# copy flash: tftp:
Source filename []? dap.xml

Address or name of remote host []? 10.197.161.160

Destination filename [dap.xml]?

440 bytes copied in 0.40 secs
```

ステップ 2： ホストスキャン設定ファイル(data.xml)とホストスキャンイメージをASAからローカルデバイスにコピーします。

ASDM:

[Tools] > [File Management] > [File Transfer] > [Between Local PC and Flash] に移動します。



CLI：

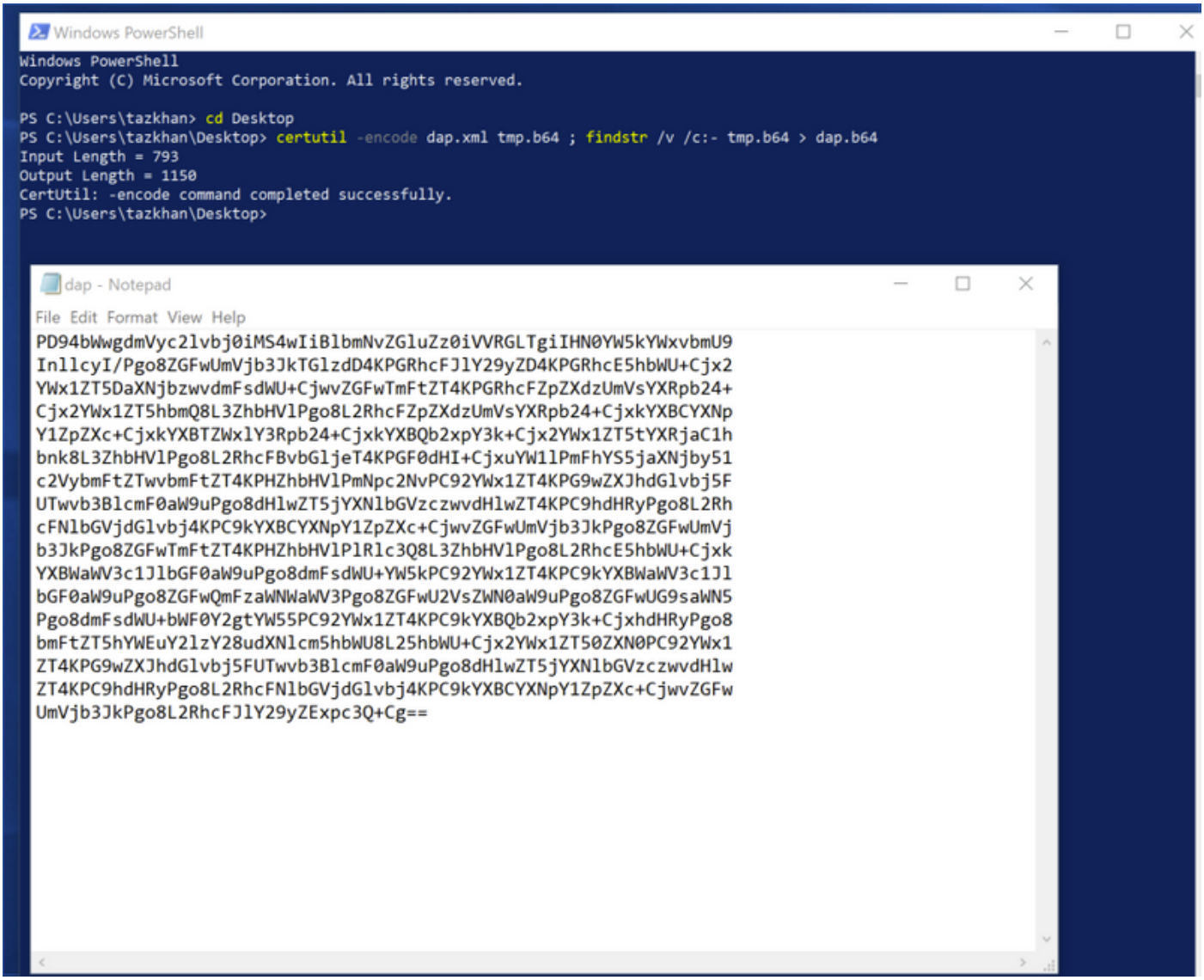
```
ASA# copy flash: tftp:
Source filename []? data.xml

Address or name of remote host []? 10.197.161.160

Destination filename [data.xml]?

500 bytes copied in 0.40 secs

ASA# copy flash: tftp:

Source filename []? hostscan_4.9.03047-k9.pkg

Address or name of remote host []? 10.197.161.160

Destination filename [hostscan_4.9.03047-k9.pkg]?
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
56202408 bytes copied in 34.830 secs (1653012 bytes/sec)
ASA#
```

ステップ 3： dap.xmlおよびdata.xmlのbase64エンコード値を取得します。

Mac:**base64 -i <file>**

```
tazkhan@TAZKHAN-M-32A3 Desktop % base64 -i dap.xml
PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiIHN0YW5kYWxvbmU9InllcyI/Pgo8ZGFwUmVjb3JkTGlzdD4KPGRhcFJlY29yZD4
KPGRhcE5hbWU+Cjx2YWx1ZT5XaW5kb3dzPC92YWx1ZT4KPC9kYXBOYW1lPgo8ZGFwVmlld3NSZWxhdGlvbj4KPHZhbHVlPmFuZDwvdmFsdWU+Cj
wvZGFwVmlld3NSZWxhdGlvbj4KPGRhcEJhc2ljVmlldz4KPGRhcFNlbGVjdGlvbj4KPGRhcFBvbGljeT4KPHZhbHVlPm1hdGNoLWFueTwvdmFsd
WU+CjwvZGFwUG9saWN5Pgo8YXR0cj4KPG5hbWU+YWFhLmNpc2NvLnVzZXJuYW1lPC9uYW1lPgo8dmFsdWU+Y2lzY288L3ZhbHVlPgo8cmVnZX
aW9uPkVRPC9vcGVyYXRpb24+Cjx0eXBlPmNhc2VsZXNzPC90eXBlPgo8dmFsdWU+bWF0Y2gtYW55PC92YWx1ZT4KPC9hdHI+CjwvZGFwUG9saWN5Pgo8dmFsdWU+bWF0Y2gtYW55PC92YWx1ZT4KPC9kYXBQb2xpY3k+Cjx2YWx1ZT5hbmQ8L3ZhbHVlPgo8L2RhcEZpZXdzUmVsYXRpb24+Cjx2YWx1ZT5hbmQ8L3ZhbHVlPgo8L2RhcEZpZXdzUmVsYXRpb24+CjwvZGFwUmVjb3JkPgo8L2RhcFJlY29yZExpc3
Q+Cg==
```

Windows Powershellの場合：**certutil -encode dap.xml tmp.b64 ;findstr /v /c:- tmp.b64 > dap.b64**



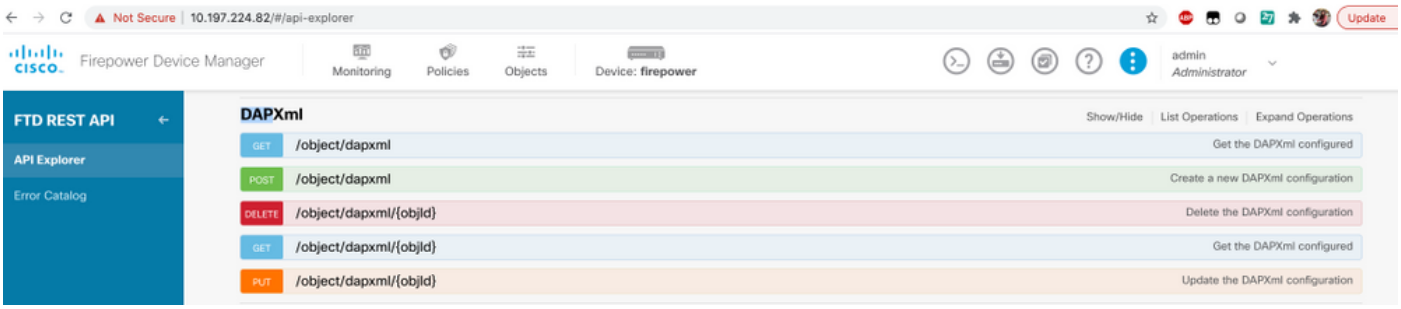
data.xmlについても同じ手順に従います。

ステップ4：ブラウザウィンドウでFTDのAPI Explorerを起動します。

https://<FTD Management IP>/api-explorerに移動します

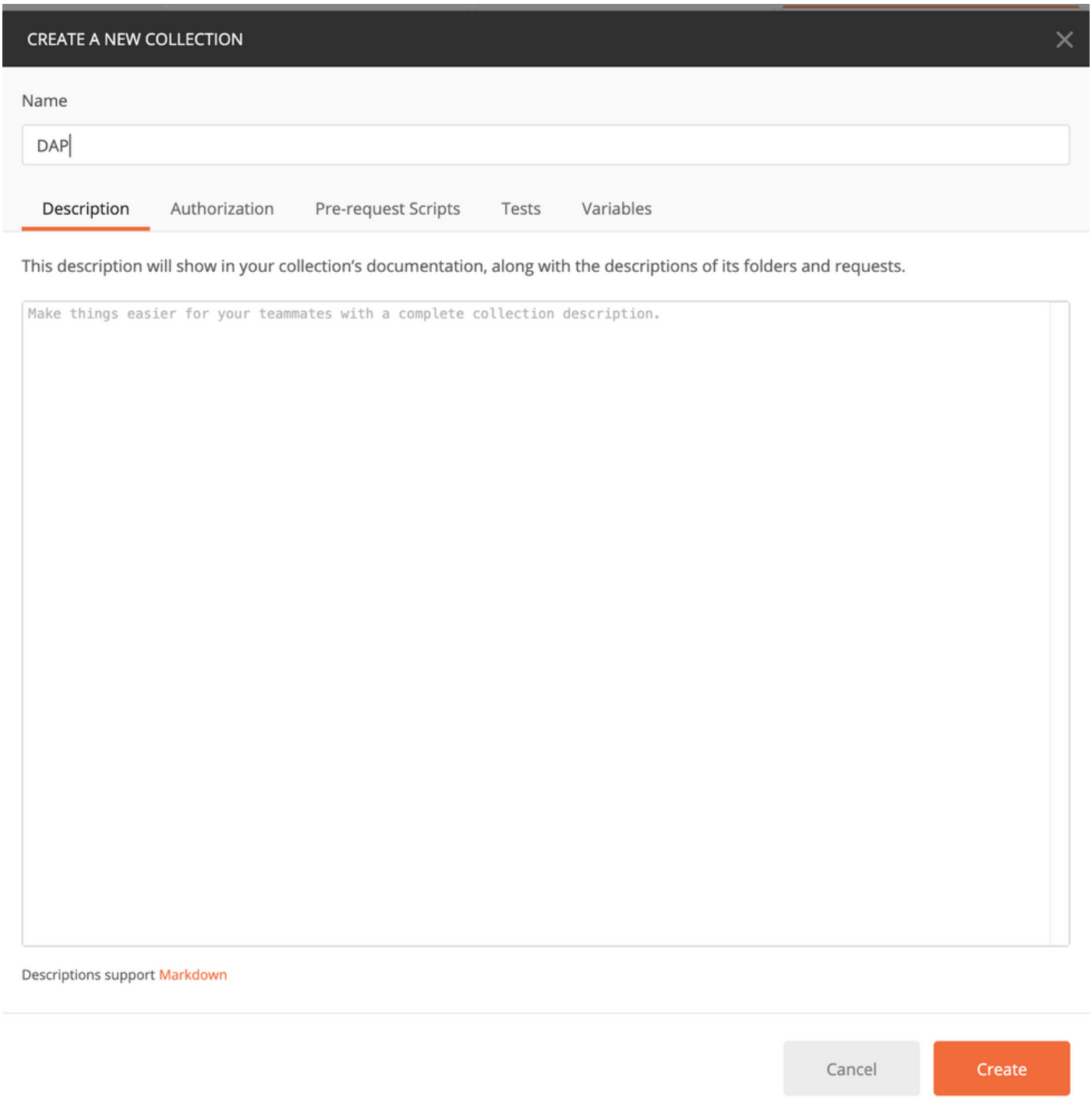
これには、FTDで使用可能なAPIのリスト全体が含まれます。これは、FDMでサポートされている複数のGET/POST/PUT/DELETE要求を含む主機能に基づいて分割されます。

DAPXmlとHostScanPackageFileが使用されるAPIです。



ステップ 5： DAPのPostmanコレクションを追加します。

コレクション**の名前**を指定します。次の図に示すように、[**Create**]をクリックします。



手順 6： 新しい要求の追加 **AUTH** トークンを取得してPOST/GET/PUT要求を認可するために、FTDへのログインPOST要求を作成します。[Save] をクリックします。