Migration DAP et HostScan d'ASA vers FDM via l'API REST

Contenu

Introduction

Ce document décrit la migration de la configuration DAP (Dynamic Access Policies) et HostScan des appliances de sécurité adaptatives Cisco (ASA) vers Cisco Firepower Threat Defense (FTD) gérée localement par Firepower Device Manager (FDM).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissance de base de la configuration VPN RA sur FDM.
- Fonctionnement de DAP et de Hostscan sur ASA.
- Connaissance de base de l'API REST et de l'Explorateur d'API FDM Rest.

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco FTD version 6.7.0
- Client Cisco AnyConnect Secure Mobility version 4.9.00086
- Postman ou tout autre outil de développement d'API

Remarque : les informations de ce document ont été créées à partir de périphériques dans un environnement de travaux pratiques spécifique. All of the devices used in this document

started with a cleared (default) configuration. Si votre réseau est actif, assurez-vous de bien comprendre l'impact potentiel de toute modification de configuration.

Informations générales

Même si FTD prend en charge la configuration RAVPN (Remote Access VPN), il ne prend pas en charge le DAP. Depuis la version 6.7.0, la prise en charge de l'API est ajoutée pour DAP sur le FTD. Il est destiné à prendre en charge le cas d'utilisation très basique de la migration d'ASA vers FTD. Les utilisateurs qui ont un DAP configuré sur leur ASA et qui sont en train de migrer vers les FTD ont maintenant un chemin pour migrer leur configuration DAP avec leur configuration VPN d'accès distant.

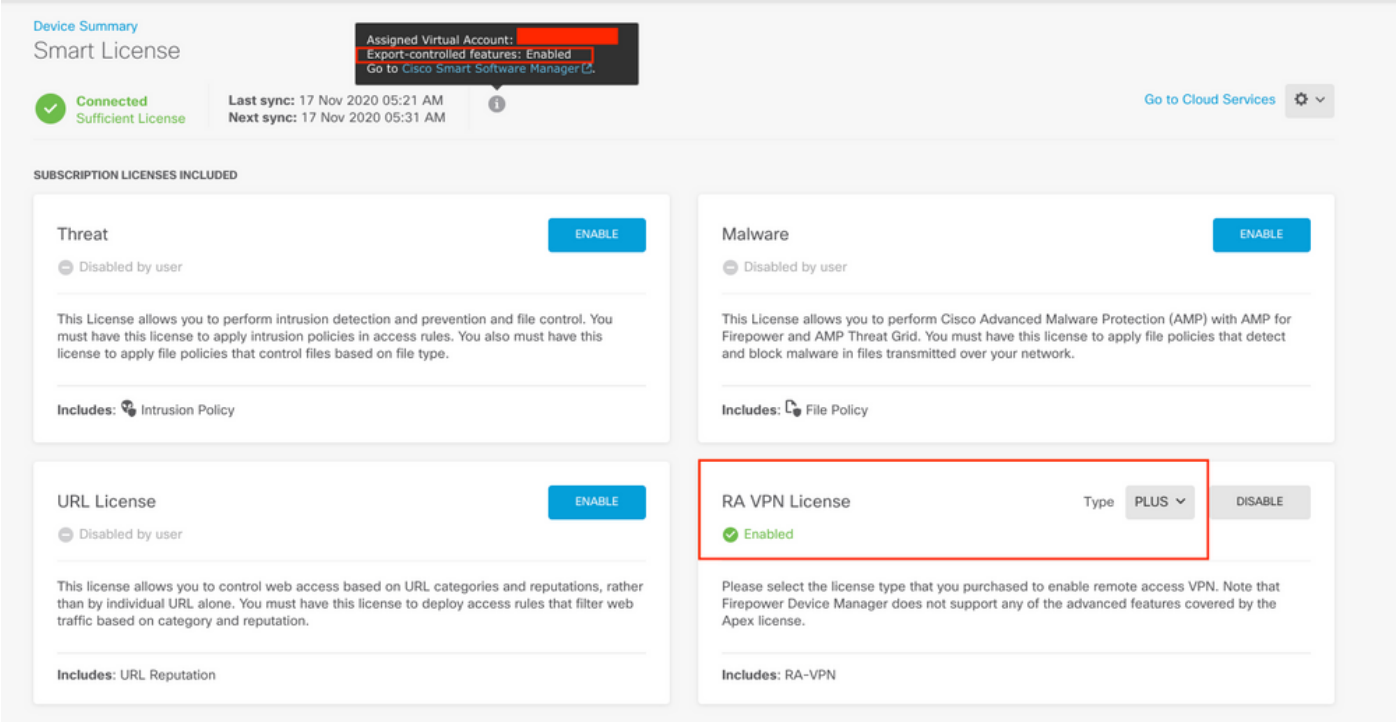
Afin de réussir la migration de la configuration DAP d'ASA vers FTD, assurez-vous que les conditions suivantes sont réunies :

- ASA avec DAP/Hostscan configuré.
- Accès au serveur TFTP/FTP depuis l'accès ASA ou ASDM à l'ASA.
- Cisco FTD version 6.7.0 et ultérieure gérée par Firepower Device Manager (FDM).
- VPN RA configuré et fonctionnant sur FTD.

Licence

- FTD enregistré sur le portail de licences Smart avec Export Controlled Features activé (afin d'autoriser l'activation de l'onglet de configuration VPN RA).
- Toutes les licences AnyConnect activées (APEX, Plus ou VPN uniquement).

Afin de vérifier la licence : Accédez à **Périphériques > Licences Smart**



Limitations des fonctionnalités

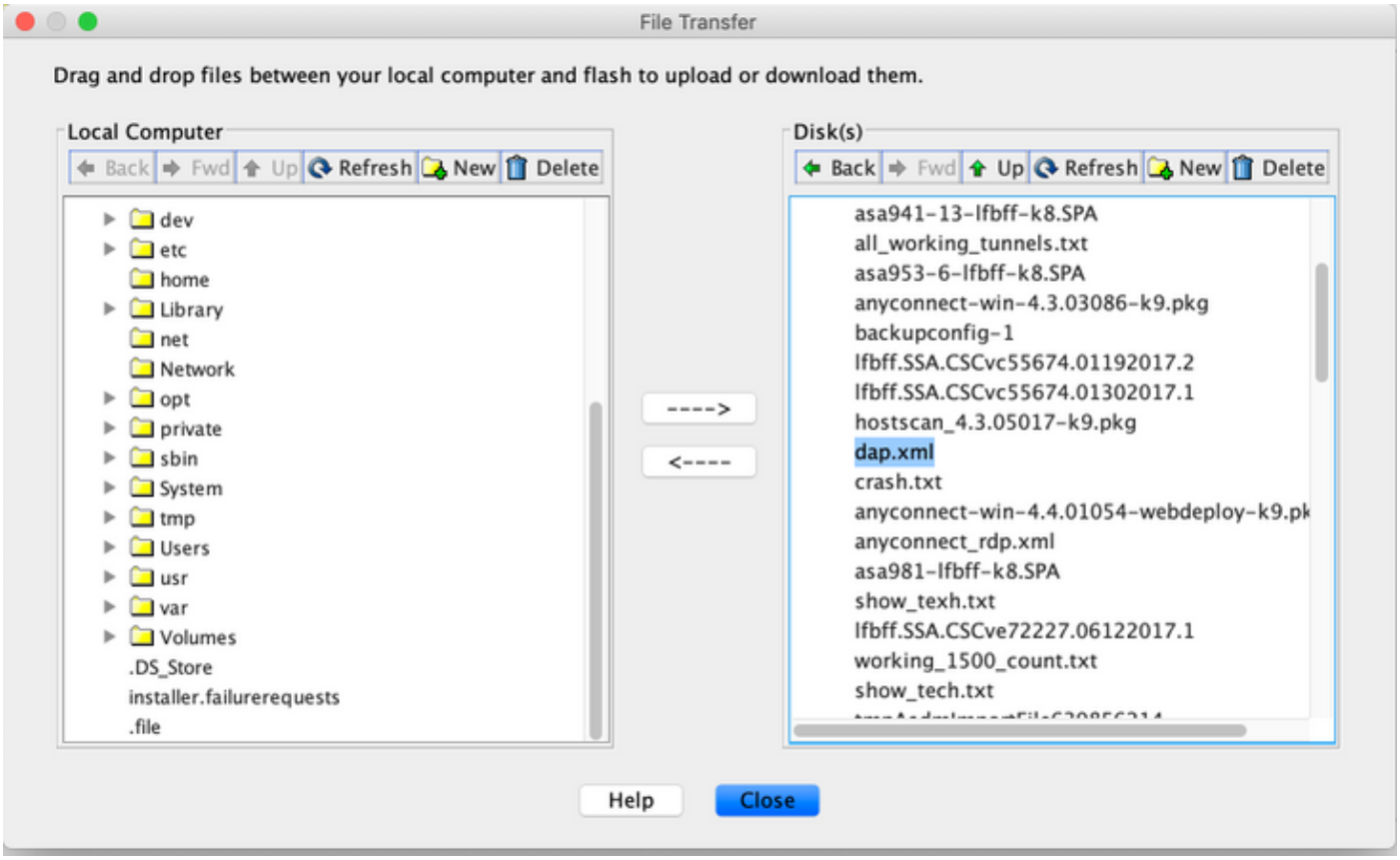
- Ces fonctionnalités sont uniquement prises en charge via l'interface API REST FDM/FTD.
- Le nom DAP ne peut pas contenir de caractères d'espace avec l'API REST.

Configuration

Étape 1. Copiez **dap.xml** d'ASA vers votre ordinateur local / serveur TFTP. Il existe deux façons d'y parvenir :

ASDM :

Accédez à **Outils > Gestion de fichiers >Transfert de fichiers >entre PC locaux et Flash**.



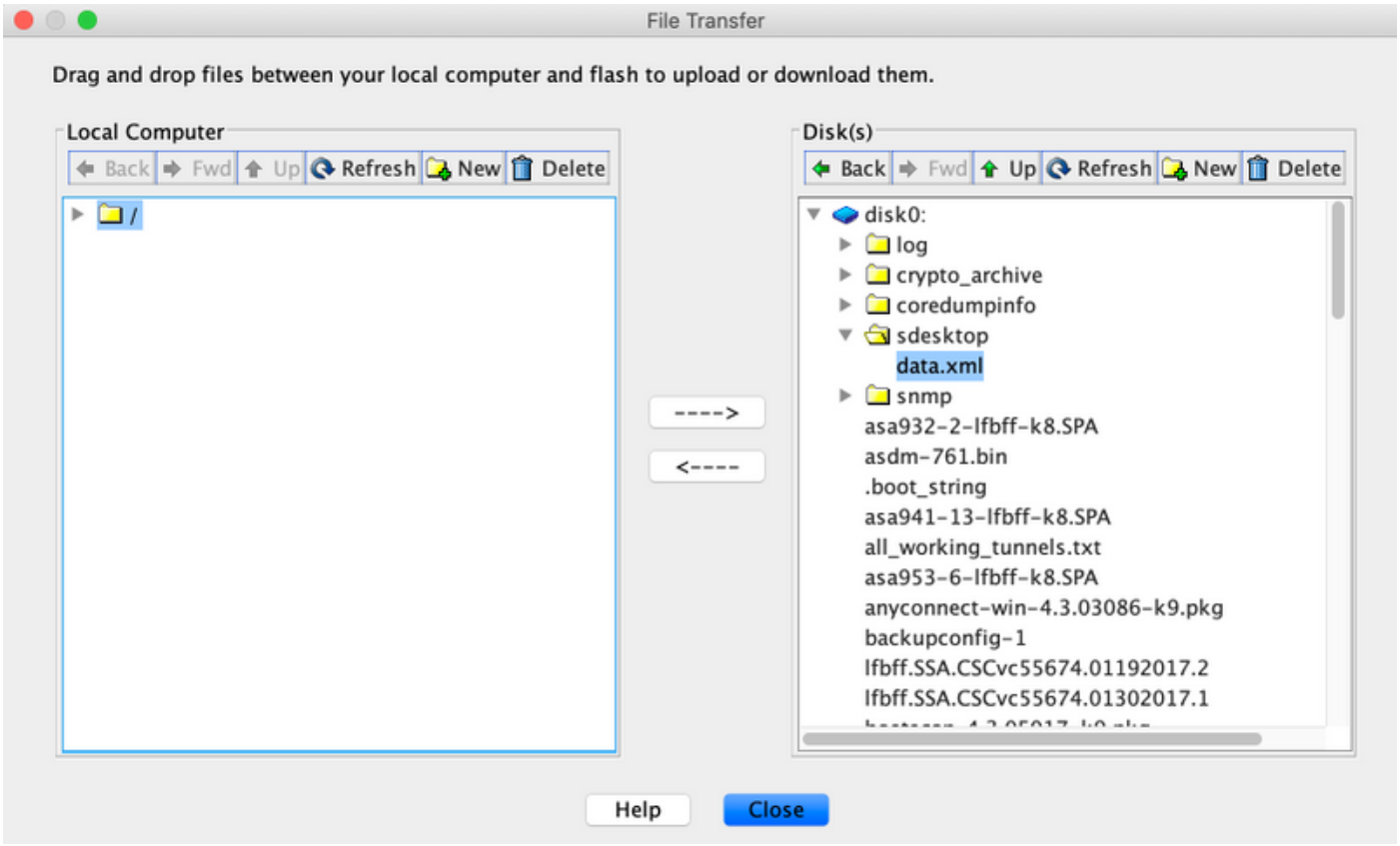
CLI :

```
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
```

Étape 2. Copiez le fichier de configuration hostscan (data.xml) et l'image hostscan d'ASA vers le périphérique local.

ASDM :

Accédez à **Outils > Gestion de fichiers >Transfert de fichiers >entre PC locaux et Flash**.



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#
```

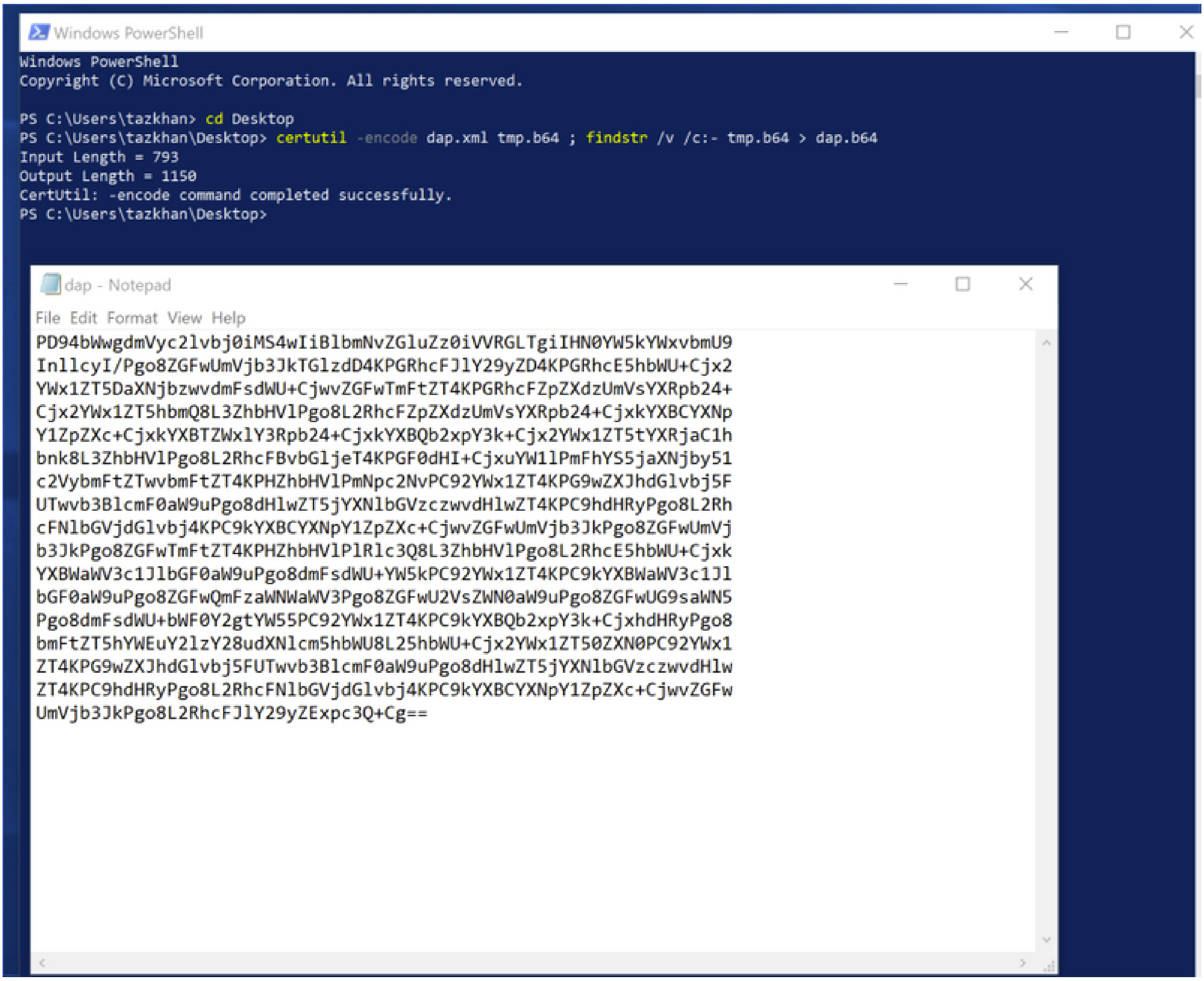
Étape 3. Obtient la valeur encodée base64 de **dap.xml** et **data.xml**.

Sur Mac : **base64 -i <fichier>**

```
tazkhan@TAZKHAN-M-32A3 Desktop % base64 -i dap.xml
```

PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiIHN0YW5kYWxvbmU9InllcyI/Pgo8ZGFwUmVjb3JkTGlzdD4KPGRhcFJlY29yZD4
KPGRhcE5hbWU+Cjx2YWx1ZT5XaW5kb3dzPC92YWx1ZT4KPC9kYXBOYW1lPgo8ZGFwVmlld3NSZWxhdGlvbj4KPHZhbHVlPmFuZDwvdmFsdWU+Cj
wvZGFwVmlld3NSZWxhdGlvbj4KPGRhcEJhc2ljVmlldz4KPGRhcFNlbGVjdGlvbj4KPGRhcFBvbGljeT4KPHZhbHVlPm1hdGNoLWFueTwvdmFsd
WU+CjwvZGFwUG9saWN5Pgo8YXR0cj4KPG5hbWU+YWFhLmNpc2NvLnVzZXJuYW1lPC9uYW1lPgo8dmFsdWU+Y2lzY288L3ZhbHVlPgo8b3BlcmF0
aW9uPkVRPC9vcGVyYXRpb24+Cjx0eXBlPmNhc2VsZXNzPC90eXBlPgo8L2F0dHI+CjwvZGFwU2VsZWN0aW9uPgo8ZGFwU2VsZWN0aW9uPgo8ZGF
wUG9saWN5Pgo8dmFsdWU+bWF0Y2gtYW55PC92YWx1ZT4KPC9kYXBQb2xpY3k+CjxkYXBTdWJTZWxlY3Rpb24+CjxkYXBQb2xpY3k+Cjx2YWx1ZT
5tYXRjaC1hbGw8L3ZhbHVlPgo8L2RhcFBvbGljeT4KPGF0dHI+CjxuYW1lPmVuZHBvaW50LmFueWNvbm5lY3QucGxhdGZvcm08L25hbWU+Cjx2Y
Wx1ZT53aW48L3ZhbHVlPgo8b3BlcmF0aW9uPkVRPC9vcGVyYXRpb24+CjwvYXR0cj4KPC9kYXBTdWJTZWxlY3Rpb24+CjwvZGFwU2VsZWN0aW9u
Pgo8L2RhcEJhc2ljVmlldz4KPC9kYXBSZWNvcmQ+CjxkYXBSZWNvcmQ+CjxkYXBOYW1lPgo8dmFsdWU+YTwvdmFsdWU+CjwvZGFwTmFtZT4KPGR
hcFZpZXdzUmVsYXRpb24+Cjx2YWx1ZT5hbmQ8L3ZhbHVlPgo8L2RhcFZpZXdzUmVsYXRpb24+CjwvZGFwUmVjb3JkPgo8L2RhcFJlY29yZExpc3
Q+Cg==

Sous Windows powershell : **certutil -encode dap.xml tmp.b64 ; findstr /v /c :- tmp.b64 > dap.b64**



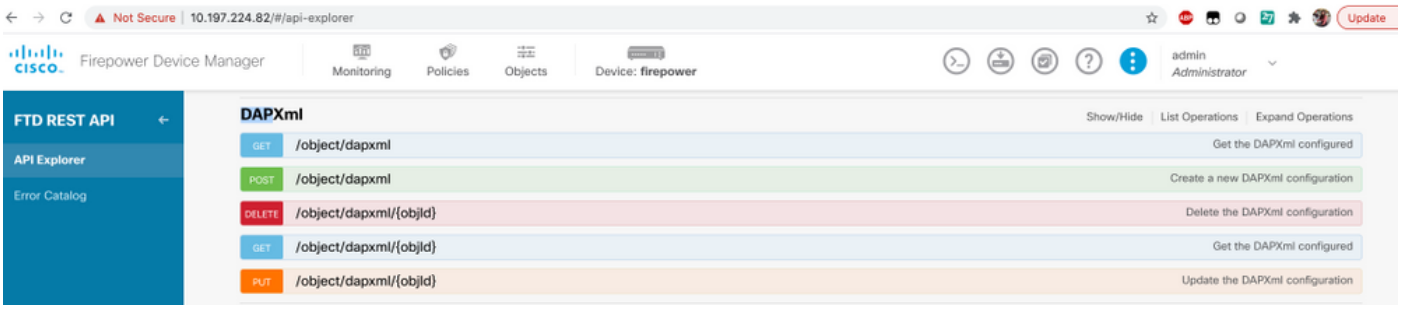
Suivez la même procédure pour data.xml.

Étape 4. Lancez l'Explorateur d'API du FTD dans une fenêtre de navigateur.

Accédez à **https://<FTD Management IP>/api-explorer**

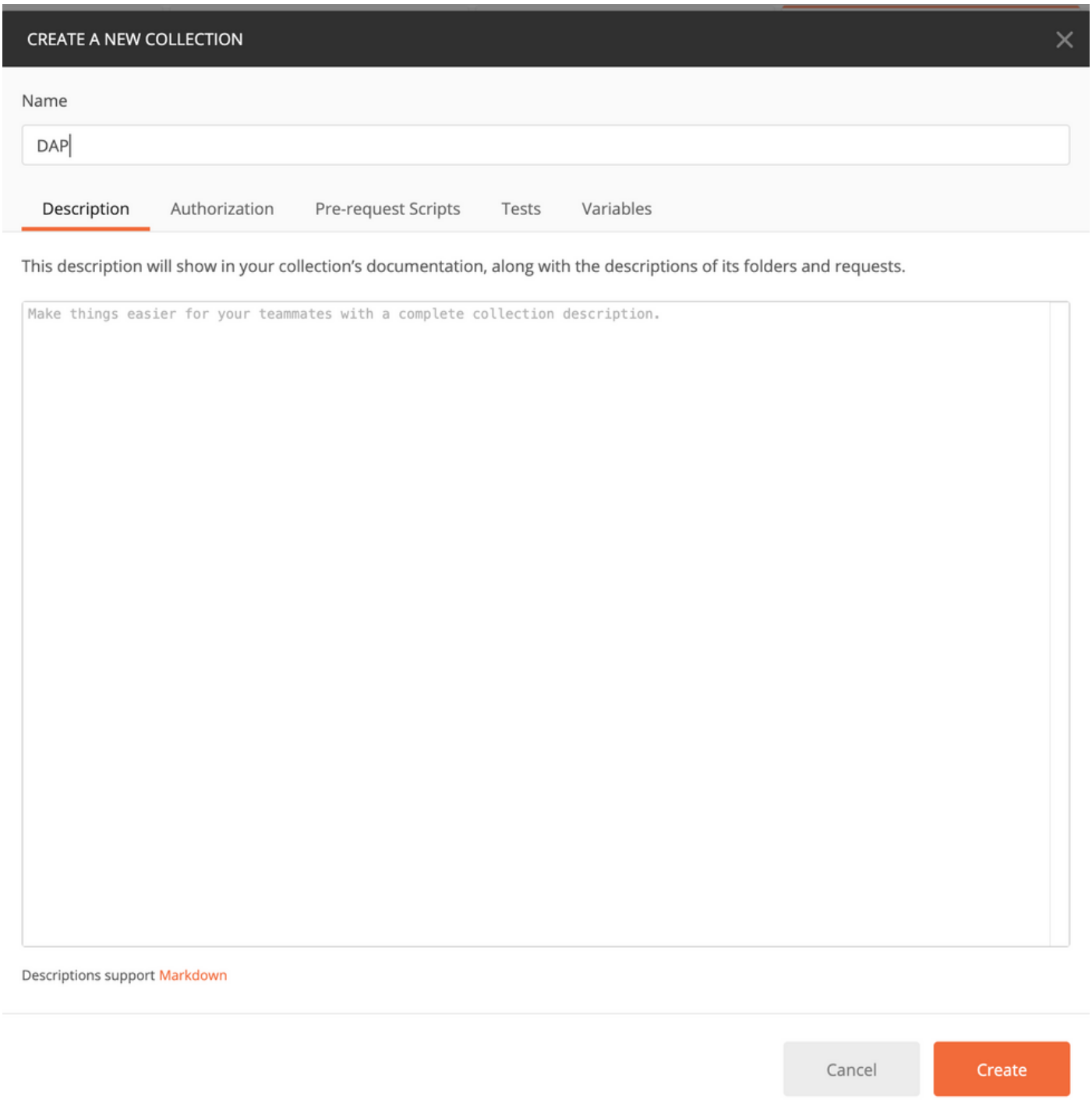
Il contient la liste complète des API disponibles sur le FTD. Il est divisé en fonction de la fonction principale avec plusieurs requêtes GET/POST/PUT/DELETE prises en charge par le module FDM.

DAPXml et **HostScanPackageFile** sont l'API utilisée.



Étape 5. Ajoutez une collection Postman pour DAP.

Indiquez un **nom** pour la collection. Cliquez sur **Créer**, comme illustré dans cette image.



Étape 6. Ajouter une nouvelle demande **authentification** pour créer une requête POST de connexion au FTD afin d'obtenir le jeton pour autoriser toute requête POST/GET/PUT. Cliquez sur

Enregistrer.