DAP- en Host Scan-migratie van ASA naar FDM via REST API

Inhoud

Inleiding

Dit document beschrijft de migratie van Dynamic Access Policy (DAP) en HostScan-configuratie van Cisco adaptieve security applicaties (ASA) naar Cisco Firepower Threat Defense (FTD), die lokaal wordt beheerd door Firepower Apparaatbeheer (FDM).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Basiskennis van RA VPN-configuratie op FDM.
- Werken van DAP en Hostscan op ASA.
- Basiskennis van REST API en FDM Rest API Explorer.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco FTD-versie 6.7.0
- Cisco AnyConnect Secure Mobility Clientversie 4.9.0086
- Postman of een ander API-ontwikkelingsmiddel

Opmerking: de informatie in dit document is gemaakt van apparatuur in een specifieke labomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg ervoor dat u de

potentiële impact van elke configuratie verandering begrijpt.

Achtergrondinformatie

Hoewel FTD ondersteuning heeft voor de configuratie van Remote Access VPN (RAVPN), biedt het geen ondersteuning voor DAP. Vanaf release 6.7.0 wordt API-ondersteuning voor DAP op de FTD toegevoegd. Het is bedoeld ter ondersteuning van het zeer fundamentele gebruiksgeval van migratie van ASA naar FTD. Gebruikers die DAP op hun ASA's hebben geconfigureerd en die momenteel naar FTD's migreren hebben nu een pad om hun DAP-configuratie samen met hun RA VPN-configuratie te migreren.

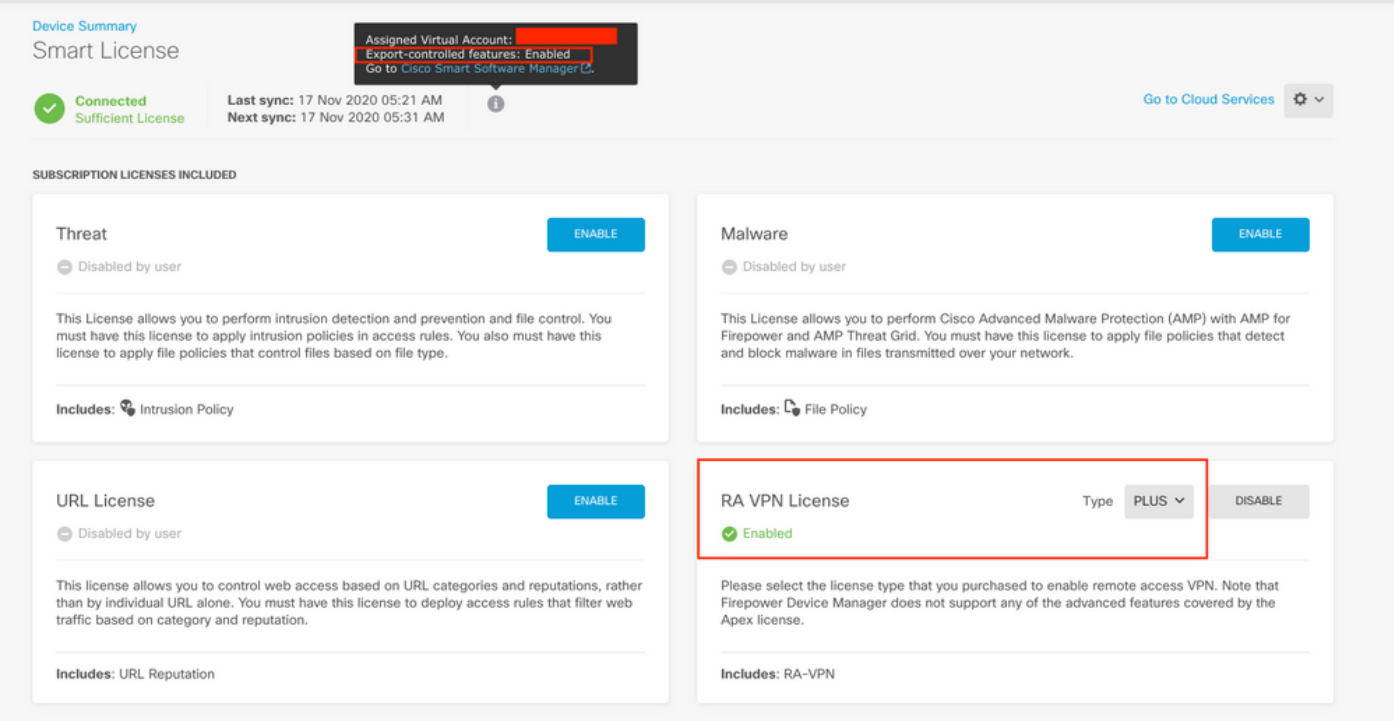
Om de DAP-configuratie van ASA naar FTD te kunnen migreren, moet u deze voorwaarden waarborgen:

- ASA met DAP/Hostscan ingesteld.
- TFTP/FTP-servertoegang van de ASA- of ASDM-toegang tot de ASA.
- Cisco FTD-versie 6.7.0 en hoger, beheerd door FirePOWER Apparaatbeheer (FDM).
- RA VPN geconfigureerd en werkt aan FTD.

Licentie

- FTD geregistreerd op het slimme licentiepatroon met Door export gecontroleerde functies ingeschakeld (om het tabblad RA VPN in te schakelen).
- AnyConnect-licenties zijn ingeschakeld (APEX, Plus of VPN-alleen).

Zo controleert u de vergunningen: Navigeren in naar **apparaten > Smart-licenties**



Functiebeperkingen

- Deze functies worden alleen ondersteund via FDM/FTD REST API-interface.

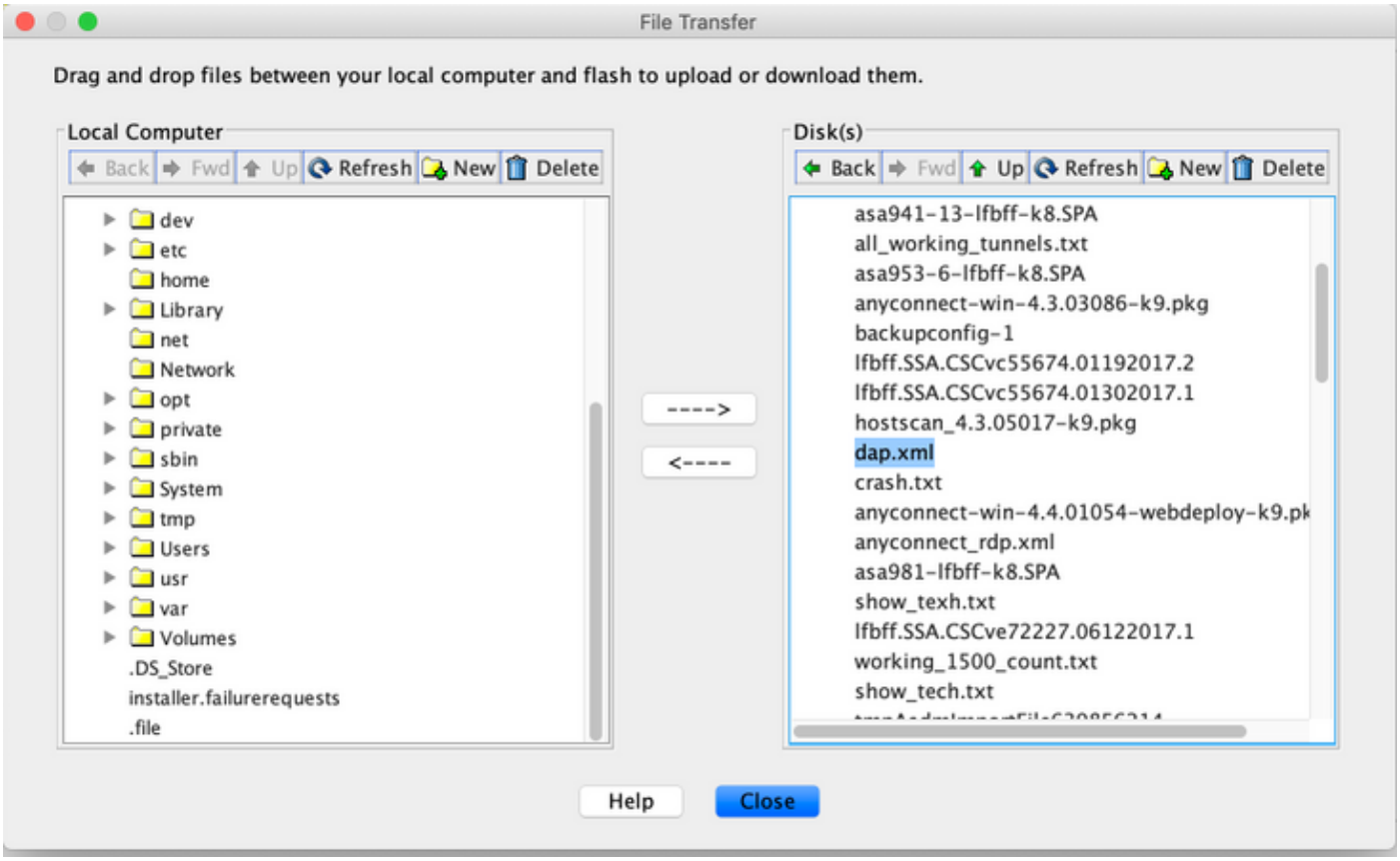
- De DAP-naam kan geen ruimtetekens met REST API bevatten.

Configuratie

Stap 1. Kopieer **dap.xml** van ASA naar uw lokale PC / TFTP Server. Er zijn twee manieren om hetzelfde te bereiken:

ASDM:

Navigeren in op **Gereedschappen>Bestandsbeheer > File Transfer >tussen lokale pc en Flash**.



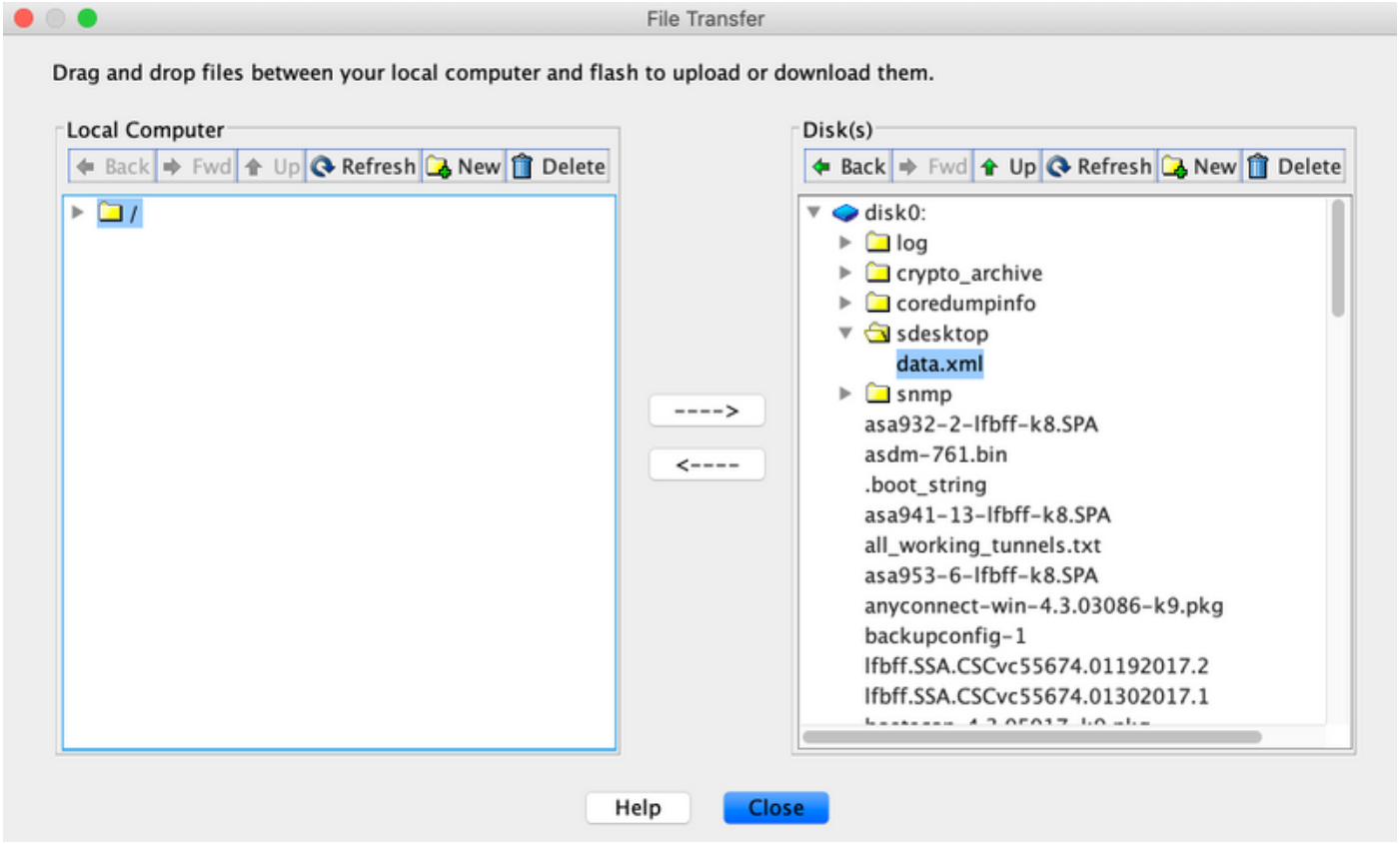
CLI:

```
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
```

Stap 2. Kopieert het bestand hostscan Setup (data.xml) en hostscan afbeelding van ASA naar het lokale apparaat.

ASDM:

Navigeer naar **tools > File Management > File Transfer >tussen lokale pc en Flash**.



CLI:

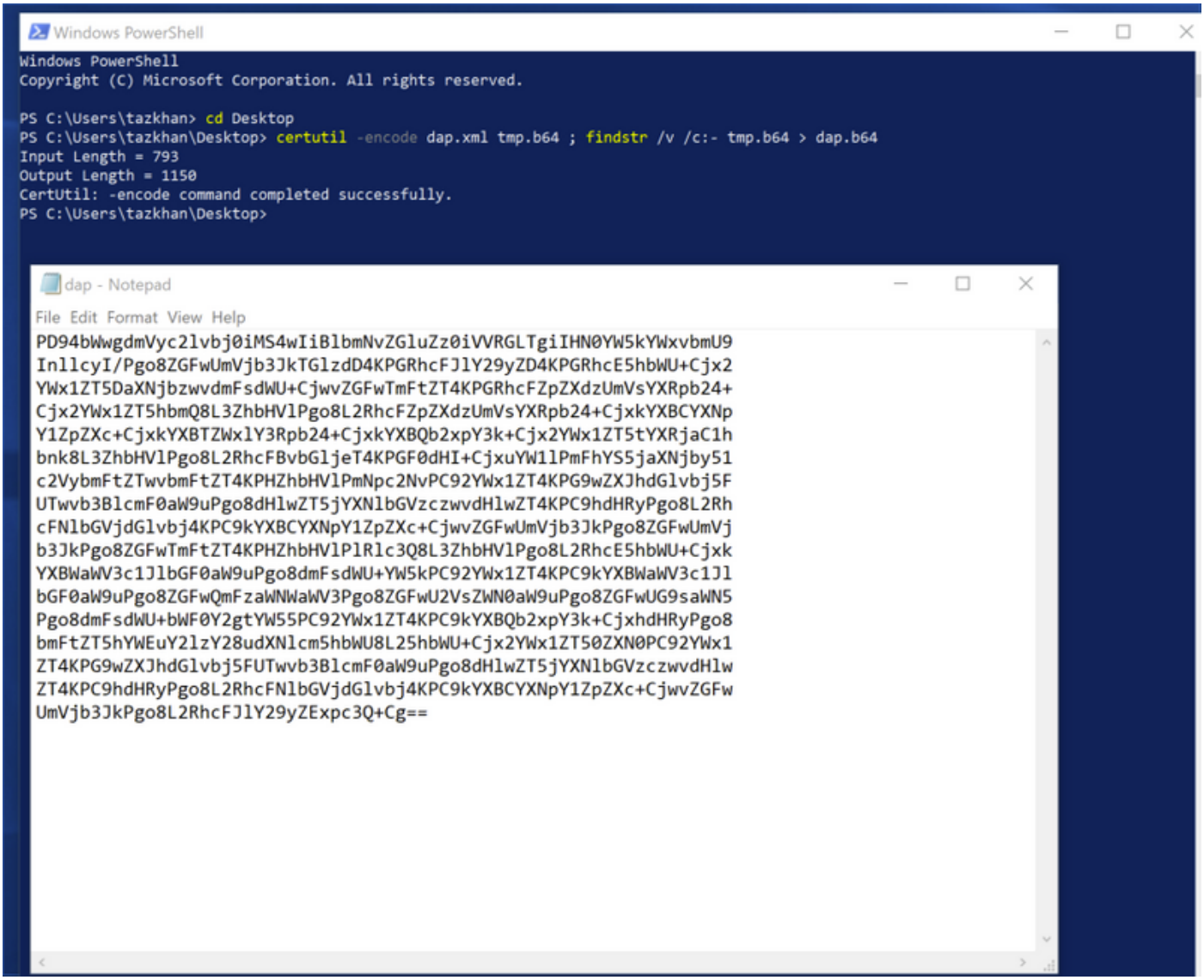
```
ASA# copy flash: tftp:
Source filename []? data.xml

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#
```

Stap 3. Ontvang de basis64-gecodeerde waarde van **dap.xml** en **data.xml**.

Op Mac: **base64-i <bestand>**

```
tazkhan@TAZKHAN-M-32A3 Desktop % base64 -i dap.xml
PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiIHN0YW5kYWxvbmU9InllcyI/Pgo8ZGFwUmVjb3JkTGlzdD4KPGRhcFJlY29yZD4
KPGRhcE5hbWU+Cjx2YWx1ZT5XaW5kb3dzPC92YWx1ZT4KPC9kYXBOYW1lPgo8ZGFwVmlld3NSZWxhdGlvbj4KPHZhbHVlPmFuZDwvdmFsdWU+Cj
wvZGFwVmlld3NSZWxhdGlvbj4KPGRhcEJhc2ljVmlldz4KPGRhcFNlbGVjdGlvbj4KPGRhcFBvbGljeT4KPHZhbHVlPm1hdGNoLWFueTwvdmFsd
WU+CjwvZGFwUG9saWN5Pgo8YXR0cj4KPG5hbWU+YWFhLmNpc2NvLnVzZXJuYW1lPC9uYW1lPgo8dmFsdWU+Y2lzY288L3ZhbHVlPgo8dmFsdW
aW9uPkVRPC9vcGVyYXRpb24+Cjx0eXBlPmNoc2VsZXNzPC90eXBlPgo8dW9sYWN5Pgo8dWF0Y2gtYW55PC92YWx1ZT4KPC9kYXRhPgo8ZGF0YT
5tYXRjaC1hbGw8L3ZhbHVlPgo8L2RhcFBvbGljeT4KPGxuYW1lPmVuZHBvaW50LmFueWNvbm5lY3QucGxhdGZvcm08L25hbWU+Cjx2Y
Wx1ZT53aW48L3ZhbHVlPgo8b3BlcmF0aW9uPkVRPC9vcGVyYXRpb24+CjwvZGFwU2VsZWN0aW9uPgo8ZGFwU2VsZWN0aW9u
Pgo8L2RhcEJhc2ljVmlldz4KPC9kYXBSZWNvcmQ+CjwvZGFwUmVjb3JkTGlzdD4KPC9kYXBQYXJhbXM+Cjx2YWx1ZT5hbmQ8L3ZhbHVlPgo8dmFsdWU+
Q+Cg==
```

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



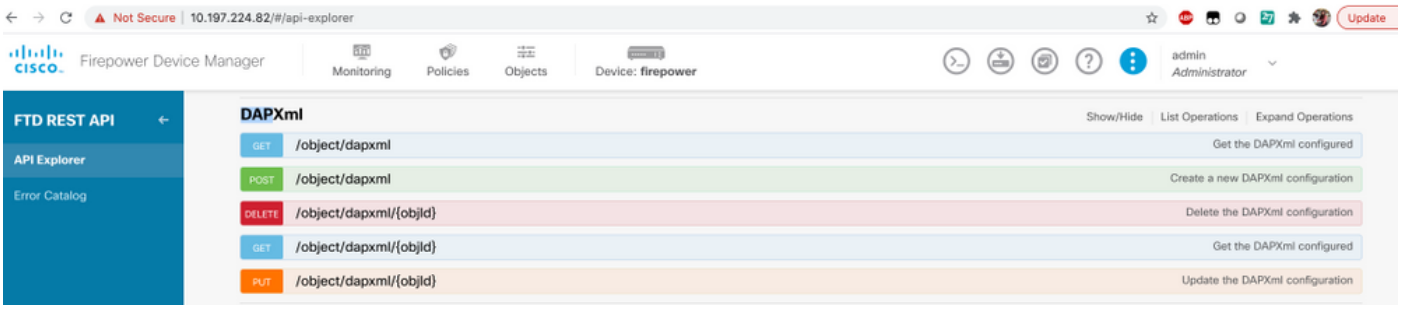
Volg dezelfde procedure voor data.xml.

Stap 4. Start de API-verkenner van de FTD op een browser.

Navigeren in naar **https://<FTD Management IP>/API-verkenner**

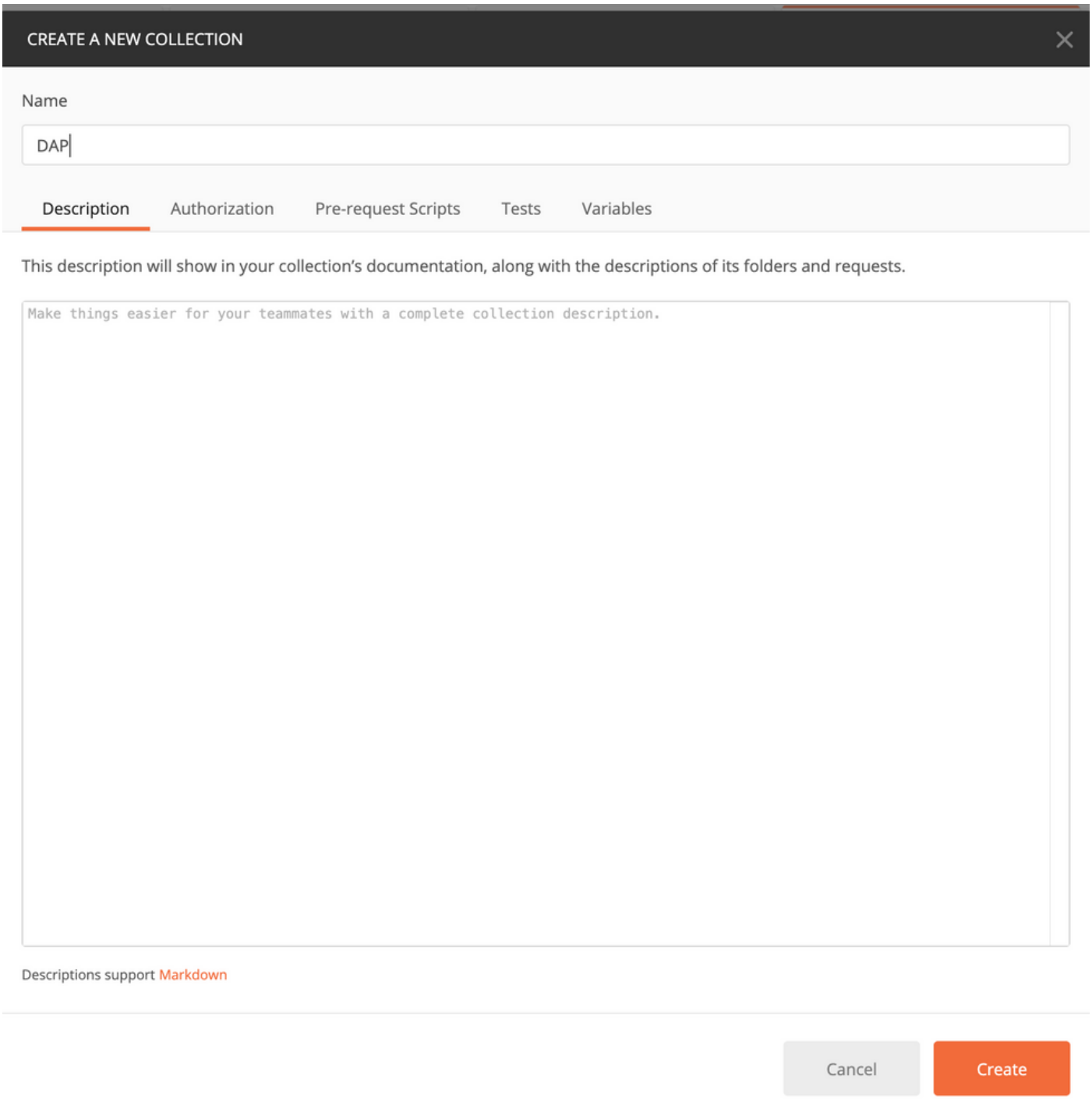
Dit bevat de volledige lijst van API's die op de FTD beschikbaar is. Het is verdeeld op basis van de hoofdfunctie met meerdere GET/POST/PUT/DELETE verzoeken die door de FDM worden ondersteund.

DAPXml en **HostScanPackageFile** worden gebruikt voor API.



Stap 5. Voeg een Postmanverzameling toe voor DAP.

Geef een **naam op** voor de verzameling. Klik op **Maken**, zoals in deze afbeelding wordt getoond.



Stap 6. Een nieuw verzoek toevoegen **Auth** om een loginlogPOST-aanvraag bij de FTD te maken om de token te hebben voor het autoriseren van POST/GET/PUT-aanvragen. Klik op **Opslaan**.