Migração de DAP e HostScan de ASA para FDM por meio da API REST

Contents

Introduction

Este documento descreve a migração das políticas de acesso dinâmico (DAP) e da configuração do HostScan dos Cisco Adaptive Security Appliances (ASA) para o Cisco Firepower Threat Defense (FTD) gerenciado localmente pelo Firepower Device Manager (FDM).

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento básico da configuração da VPN RA no FDM.
- Trabalho de DAP e Hostscan no ASA.
- Conhecimento básico da API REST e do API Explorer de Rest FDM.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco FTD executando a versão 6.7.0
- Cisco AnyConnect Secure Mobility Clientversion 4.9.00086
- Postman ou qualquer outra ferramenta de desenvolvimento de API

> **Observação:** as informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. All of the devices used in this document started with a cleared (default) configuration. Se a sua rede estiver ativa, certifique-se de que você

entende o impacto potencial de qualquer alteração de configuração.

Informações de Apoio

Embora o FTD tenha suporte à configuração de VPN de acesso remoto (RAVPN), ele não tem suporte para DAP. A partir da versão 6.7.0, o suporte à API é adicionado para DAP no FTD. Ela tem como objetivo apoiar o caso de uso muito básico da migração do ASA para o FTD. Os usuários que têm o DAP configurado em seus ASAs e estão no processo de migração para o FTD agora têm um caminho para migrar sua configuração de DAP junto com sua configuração de VPN RA.

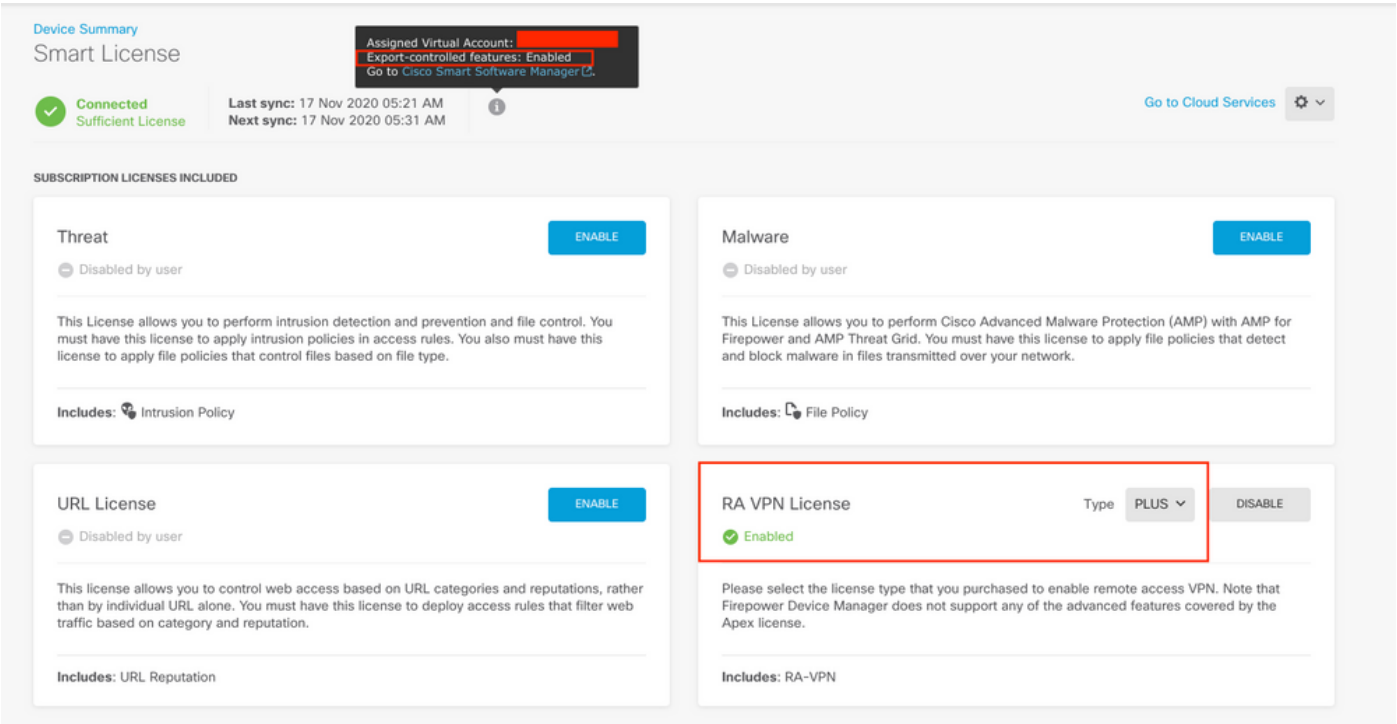
Para migrar com êxito a configuração do DAP do ASA para o FTD, assegure as seguintes condições:

- ASA com DAP/Hostscan configurado.
- Acesso do servidor TFTP/FTP do ASA ou ASDM ao ASA.
- Cisco FTD executando a versão 6.7.0 e superior gerenciado pelo Firepower Device Manager (FDM).
- VPN RA configurada e funcionando no FTD.

Licenciamento

- FTD registrado no portal de licenciamento inteligente com recurso controlado de exportação habilitado (para permitir que a guia de configuração da VPN RA seja ativada).
- Qualquer uma das licenças do AnyConnect habilitadas (APEX, Plus ou somente VPN).

Para verificar o licenciamento: Navegue até **Dispositivos > Licenças inteligentes**



Limitações da função

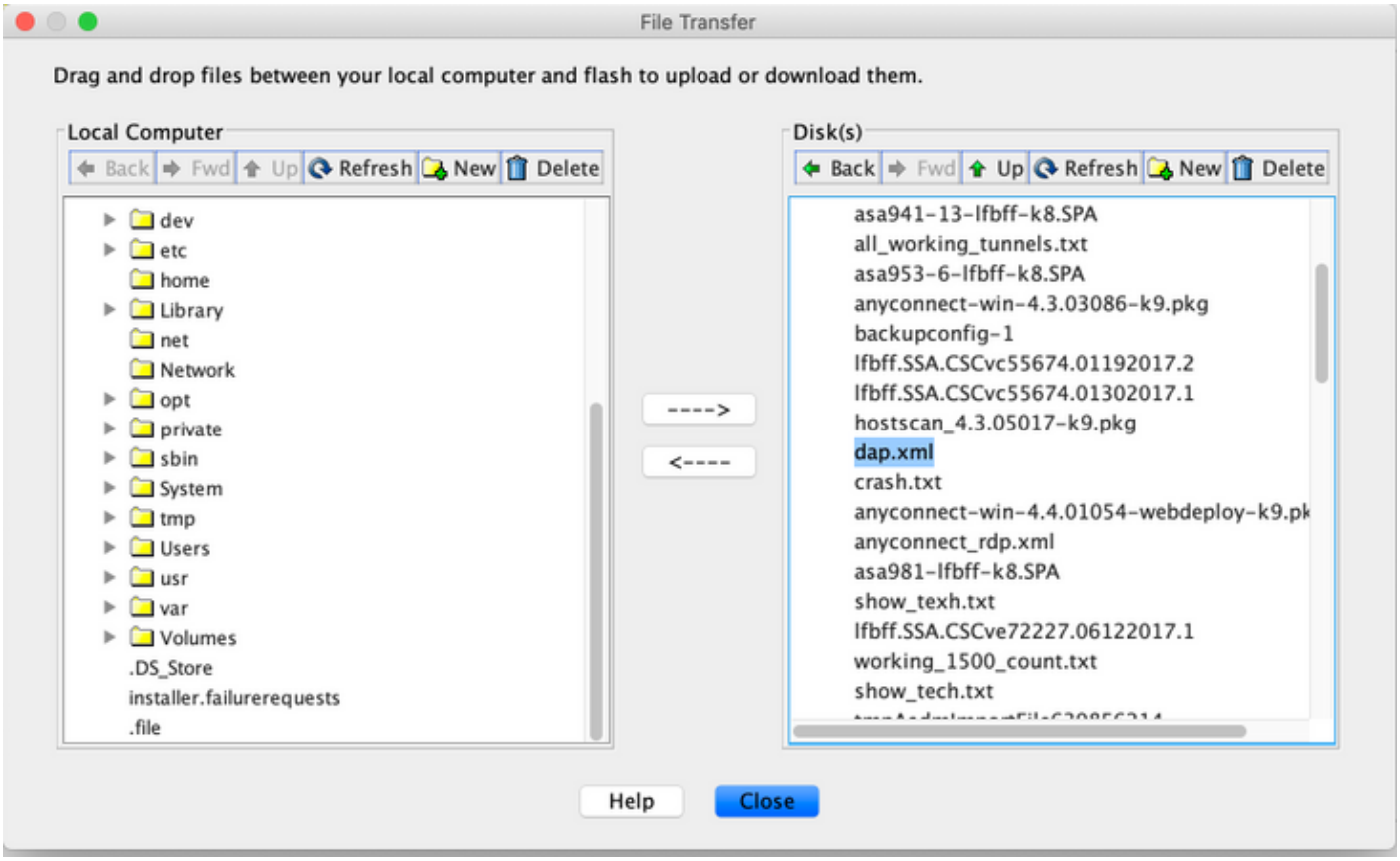
- Esses recursos são suportados apenas através da interface FDM/FTD REST API.
- O nome do DAP não pode conter caracteres de espaço com a API REST.

Configuração

Etapa 1. Copie **dap.xml** do ASA para o seu PC local / Servidor TFTP. Há duas maneiras de conseguir o mesmo:

ASDM:

Navegue até **Ferramentas > Gerenciamento de arquivos > Transferência de arquivos >entre PC local e Flash**.



CLI:

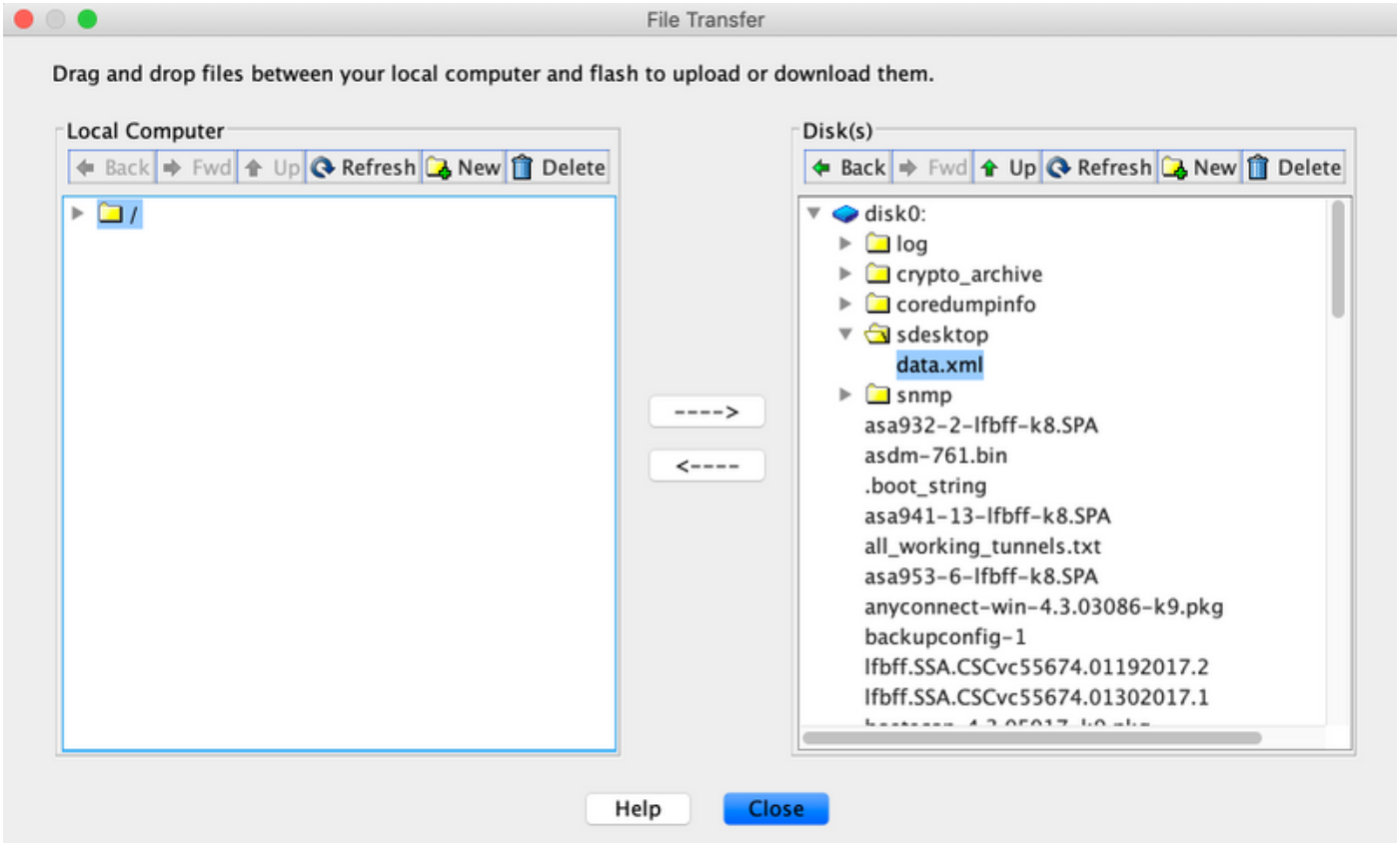
```
ASA# copy flash: tftp:
Source filename []? dap.xml

Address or name of remote host []? 10.197.161.160

Destination filename [dap.xml]?

440 bytes copied in 0.40 secs
```

Etapa 2. Copie o arquivo de configuração do hostscan (data.xml) e a imagem do hostscan do ASA para o dispositivo local.

ASDM:

Navegue até **Ferramentas > Gerenciamento de arquivos > Transferência de arquivos >entre PC**

local e Flash.



CLI:

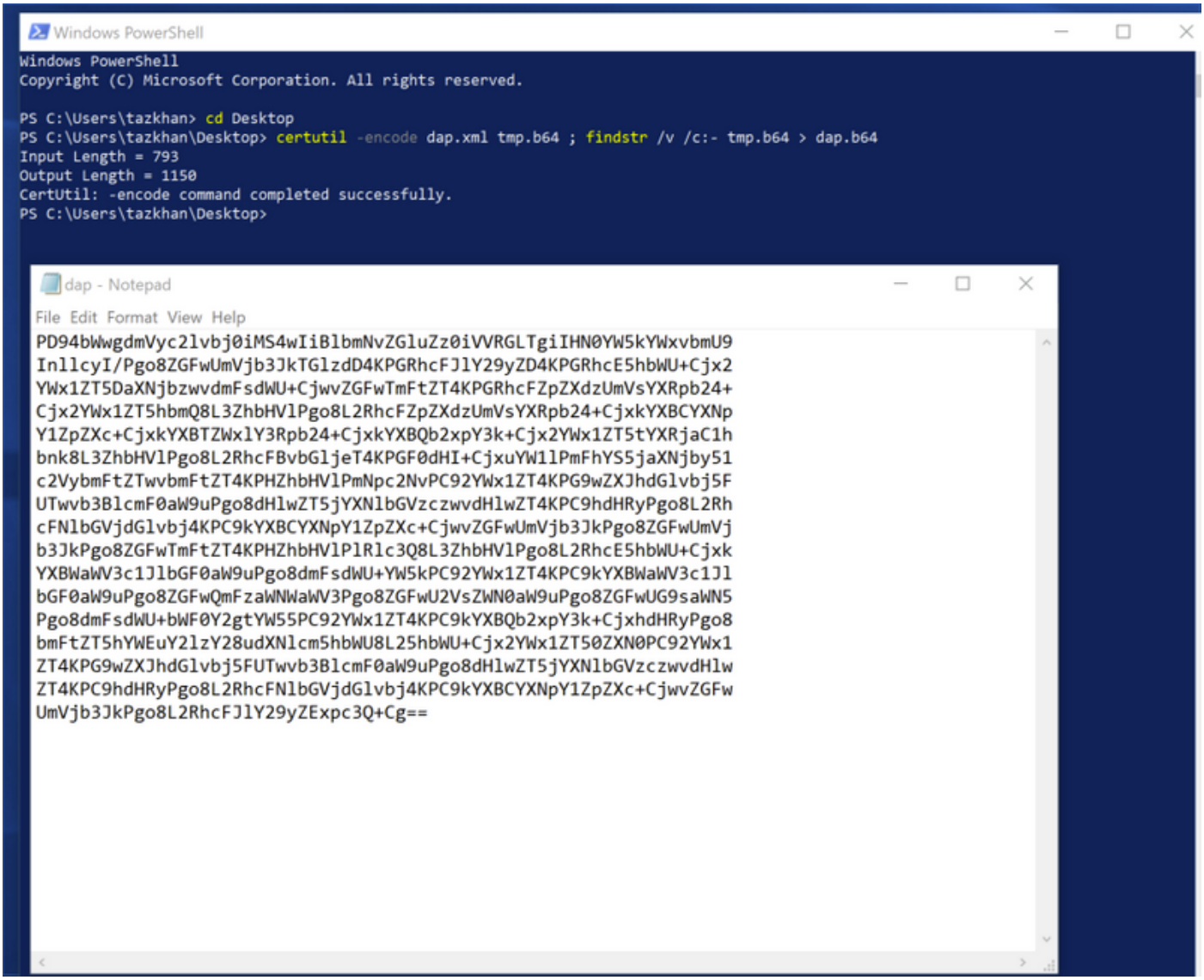
```
ASA# copy flash: tftp:
Source filename []? data.xml

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#
```

Etapa 3. Obtenha o valor codificado em base64 de **dap.xml** e **data.xml**.

No Mac: **base64 -i <arquivo>**

```
tazkhan@TAZKHAN-M-32A3 Desktop % base64 -i dap.xml
PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiIHN0YW5kYWxvbmU9InllcyI/Pgo8ZGFwUmVjb3JkTGlzdD4KPGRhcFJlY29yZD4
KPGRhcE5hbWU+Cjx2YWx1ZT5XaW5kb3dzPC92YWx1ZT4KPC9kYXBOYW1lPgo8ZGFwVmlld3NSZWxhdGlvbj4KPHZhbHVlPmFuZDwvdmFsdWU+Cj
wvZGFwVmlld3NSZWxhdGlvbj4KPGRhcEJhc2ljVmlldz4KPGRhcFNlbGVjdGlvbj4KPGRhcFBvbGljeT4KPHZhbHVlPm1hdGNoLWFueTwvdmFsd
WU+CjwvZGFwUG9saWN5Pgo8YXR0cj4KPG5hbWU+YWFhLmNpc2NvLnVzZXJuYW1lPC9uYW1lPgo8dmFsdWU+Y2lzY288L3ZhbHVlPgo8L2F0dHI
wUG9saWN5Pgo8dmFsdWU+bWF0Y2gtYW55PC92YWx1ZT4KPC9kYXBQb2xpY3k+CjxkYXBTdWJTZWxlY3RpbjI+CjxkYXBQb2xpY3k+Cjx2YWx1ZT
5tYXRjaC1hbGw8L3ZhbHVlPgo8L2RhcFBvbGljeT4KPGRhcGVudW1lcmF0aW50LmFueWNvbm5lY3QucGxhdGZvcm08L25hbWU+Cjx2Y
Wx1ZT53aW48L3ZhbHVlPgo8b3BlcmF0aW9uPkVRPC9vcGVyYXRpb24+CjwvYXR0cj4KPGRhcEJhc2ljVmlldz4KPC9kYXBSZWNvcmQ+CjxkYXBSZ
Pgo8L2RhcEJhc2ljVmlldz4KPGRhcFZpZXdzUmVsYXRpb24+CjwvZGFwVmlld3NSZWxhdGlvbj4KPC9kYXBSZWNvcmQ+CjwvZGFwTGlzdD4KPGR
hcFZpZXdzUmVsYXRpb24+Cjx2YWx1ZT5hbmQ8L3ZhbHVlPgo8L2RhcFZpZXdzUmVsYXRpb24+CjwvZGFwUmVjb3JkPgo8L2RhcFJlY29yZExpc3
Q+Cg==
```

No Windows powershell: **certutil -encode dap.xml tmp.b64 ; findstr /v /c:- tmp.b64 > dap.b64**



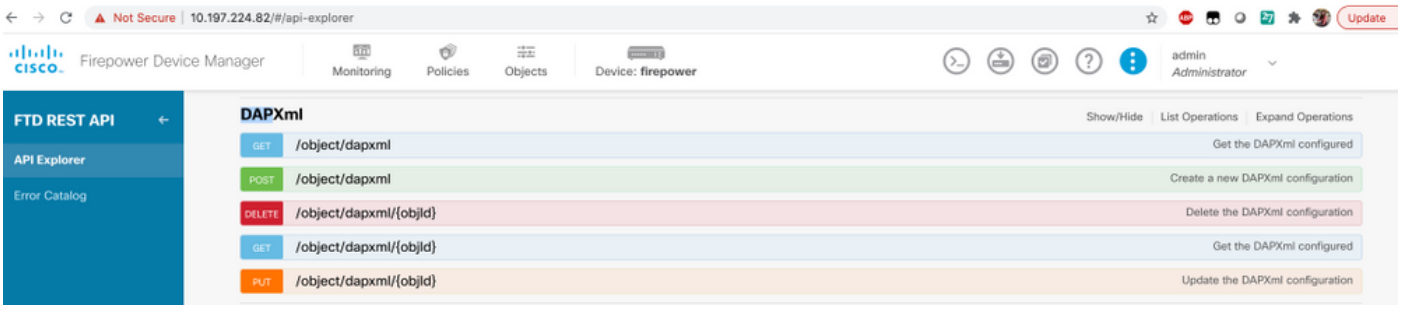
Siga o mesmo procedimento para data.xml.

Etapa 4. Inicie o API Explorer do FTD em uma janela do navegador.

Navegue até **https://<FTD Management IP>/api-explorer**

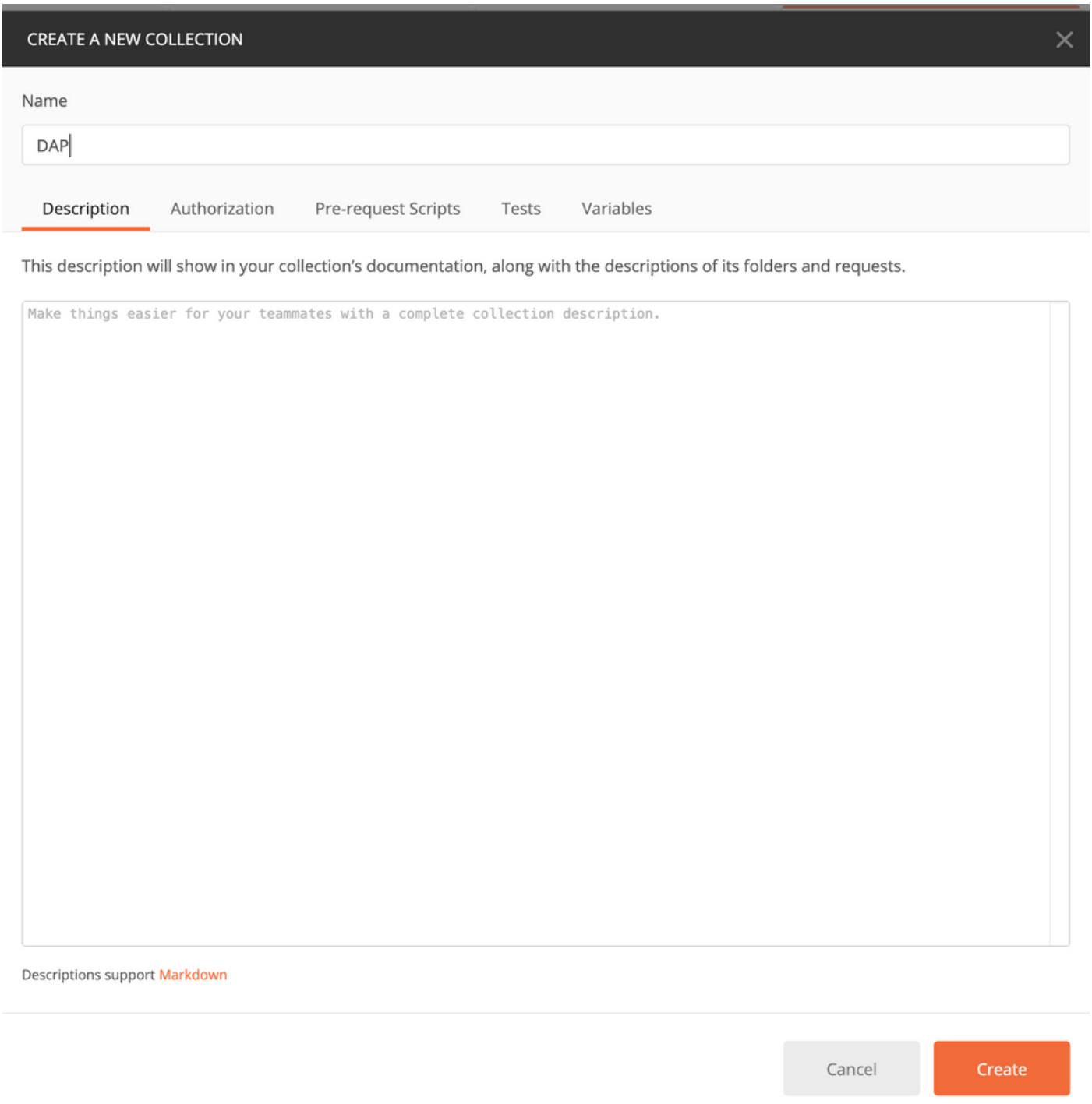
Contém a lista completa de APIs disponíveis no FTD. Ele é dividido com base no recurso principal com várias solicitações GET/POST/PUT/DELETE que são suportadas pelo FDM.

DAPXml e **HostScanPackageFile** são a API usada.



Etapa 5. Adicione uma coleção Postman para DAP.

Forneça um **Nome** para a coleção. Clique em **Criar**, conforme mostrado nesta imagem.



Etapa 6. Adicionar uma nova solicitação **Auth** para criar uma solicitação de POST de login para o FTD a fim obter o token para autorizar qualquer solicitação POST/GET/PUT. Clique em **Salvar**.