DAP和HostScan通过REST API从ASA迁移到FDM

目录

简介

本文档介绍动态访问策略(DAP)和HostScan配置从思科自适应安全设备(ASA)迁移到由Firepower设备管理器(FDM)本地管理的思科Firepower威胁防御(FTD)。

先决条件

要求

Cisco 建议您了解以下主题：

- FDM上RA VPN配置的基本知识。
- 在ASA上运行DAP和Hostscan。
- REST API和FDM Rest API资源管理器的基本知识。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行版本6.7.0的思科FTD
- 思科AnyConnect安全移动客户端版本4.9.00086
- 邮递员或任何其他API开发工具

注意：本文档中的信息是从特定实验环境中的设备创建的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解任何配置更改的潜在影响。

背景信息

即使FTD具有远程访问VPN(RAVPN)配置支持，它也缺乏对DAP的支持。自版本6.7.0起，FTD上为DAP添加了API支持。它旨在支持从ASA迁移到FTD的非常基本的使用案例。在其ASA上配置了DAP且正在迁移到FTD的用户现在有了迁移其DAP配置及其RA VPN配置的路径。

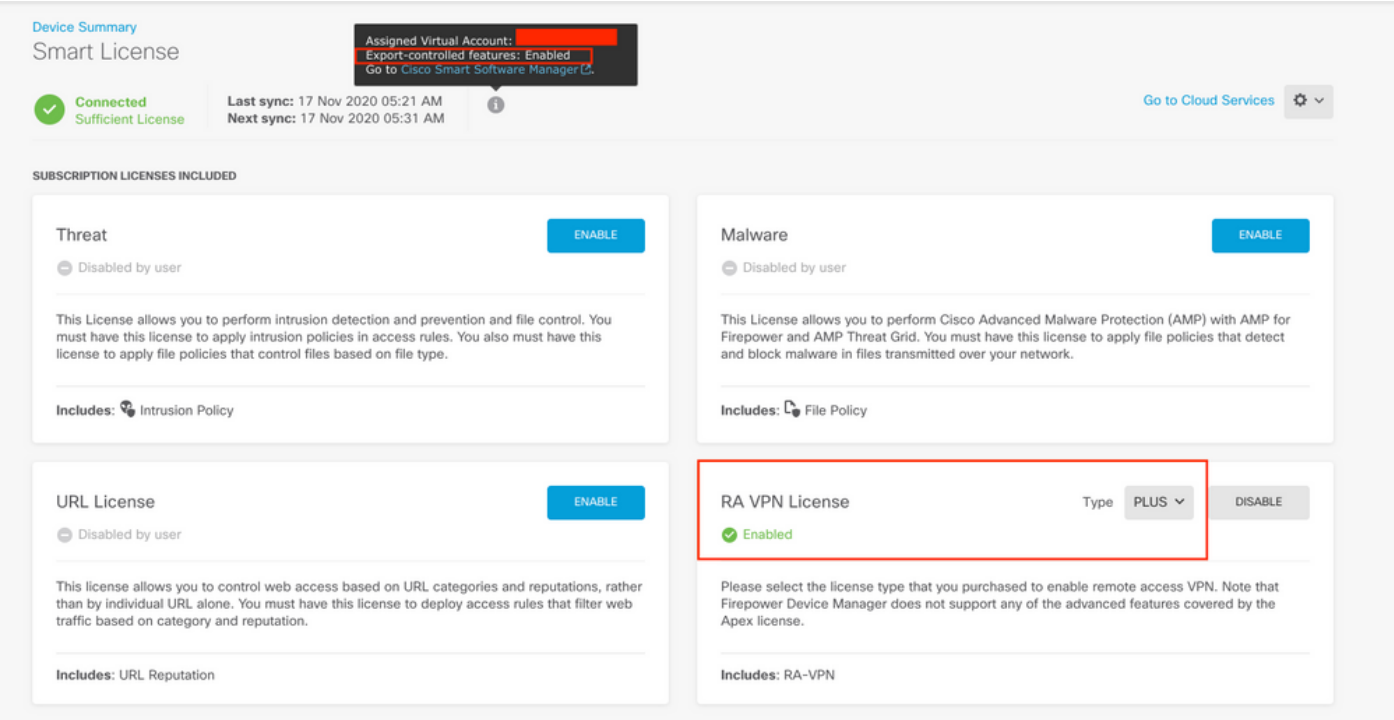
要成功将DAP配置从ASA迁移到FTD，请确保以下条件：

- 配置了DAP/Hostscan的ASA。
- 从ASA访问TFTP/FTP服务器或从ASDM访问ASA。
- 运行版本6.7.0及更高版本的Cisco FTD，由Firepower设备管理器(FDM)管理。
- 在FTD上配置和运行RA VPN。

许可

- FTD已注册到智能许可门户，并启用了导出受控功能（以允许启用RA VPN配置选项卡）。
- 任何一个AnyConnect许可证都已启用（APEX、Plus或仅VPN）。

要检查许可：导航至**设备>智能许可证**



功能限制

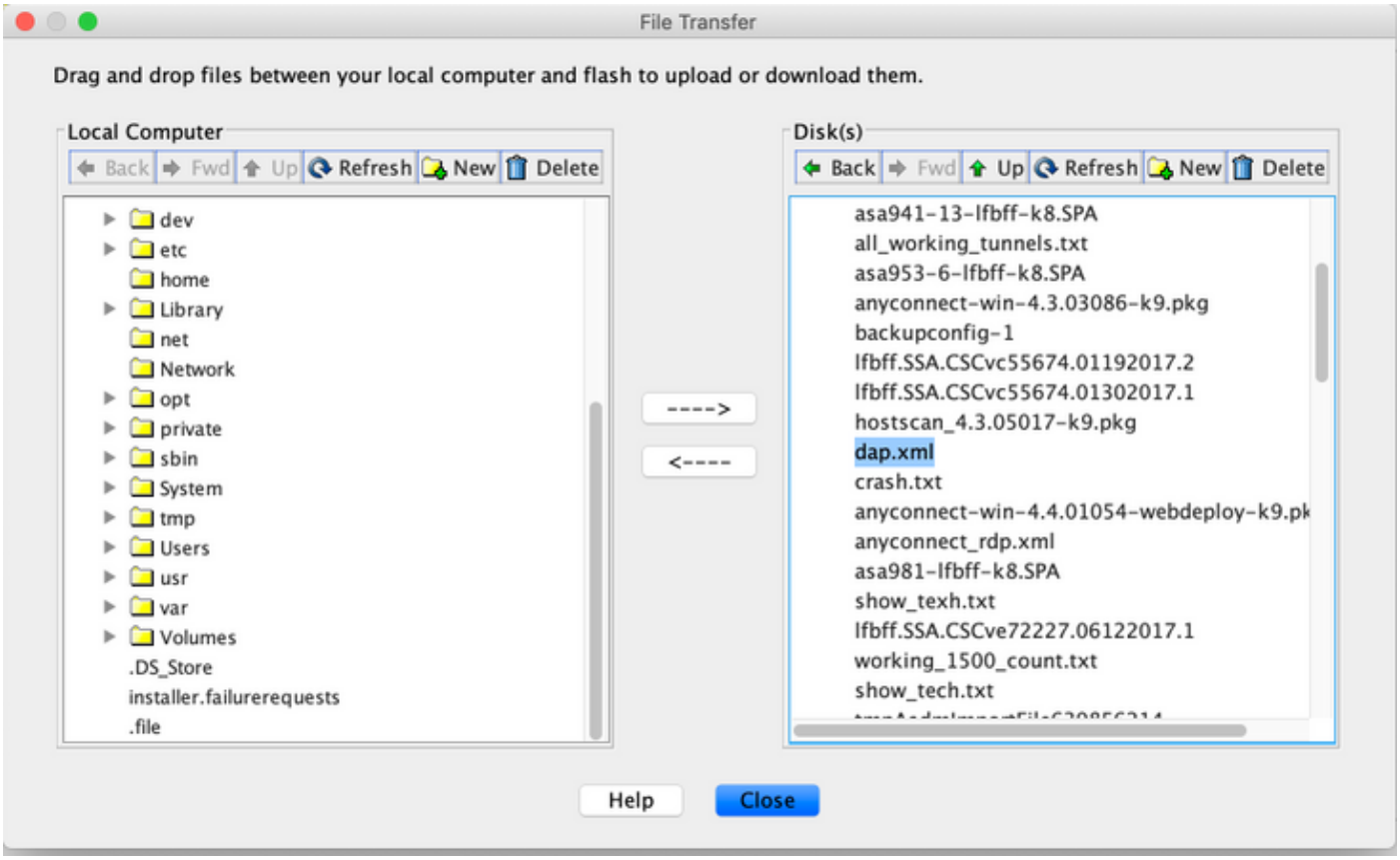
- 仅通过FDM/FTD REST API接口支持这些功能。
- DAP名称不能包含REST API的空格字符。

配置

步骤1：将dap.xml从ASA复制到本地PC/TFTP服务器。实现这一目标有两种方法：

ASDM:

导航至**工具>文件管理>文件传输>本地PC和闪存之间。**



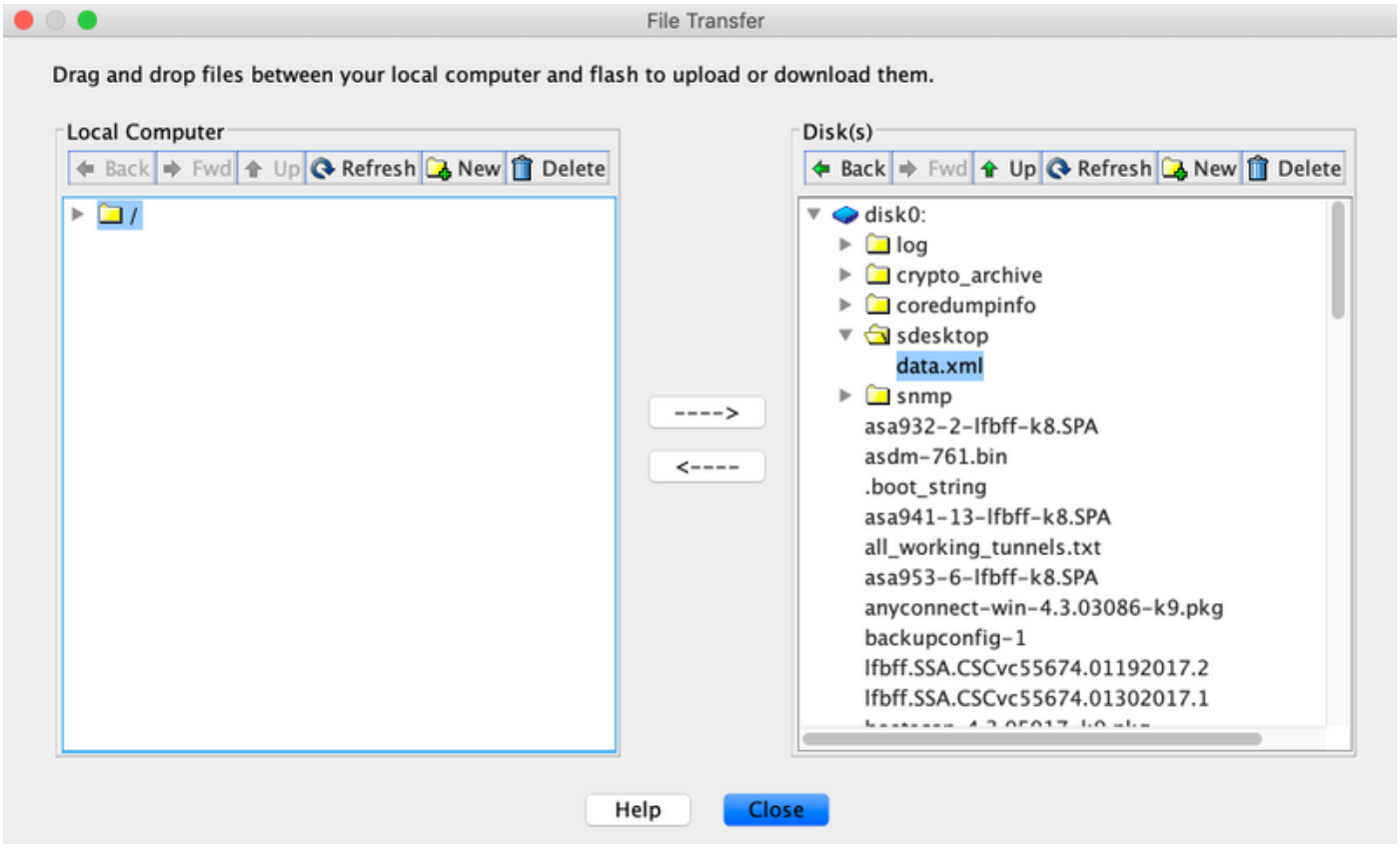
CLI：

```
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
```

第二步： 将主机扫描配置文件(data.xml)和主机扫描映像从ASA复制到本地设备。

ASDM:

导航至**工具 >文件管理>文件传输>本地PC和闪存之间。**



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#
```

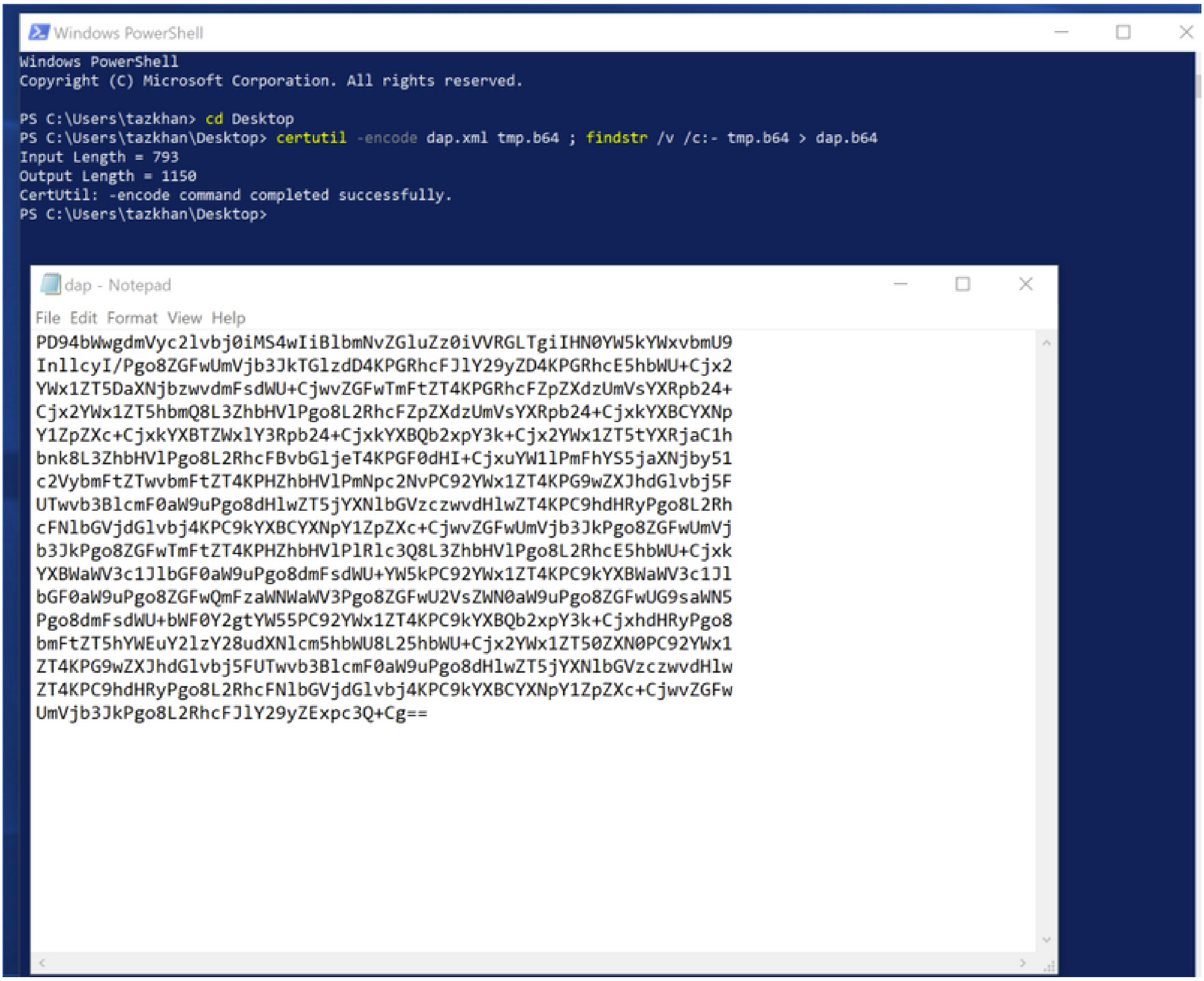
第三步： 获取dap.xml和data.xml的**base64编码值。**

在Mac上： **base64 -i <file>**

```
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==
```


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



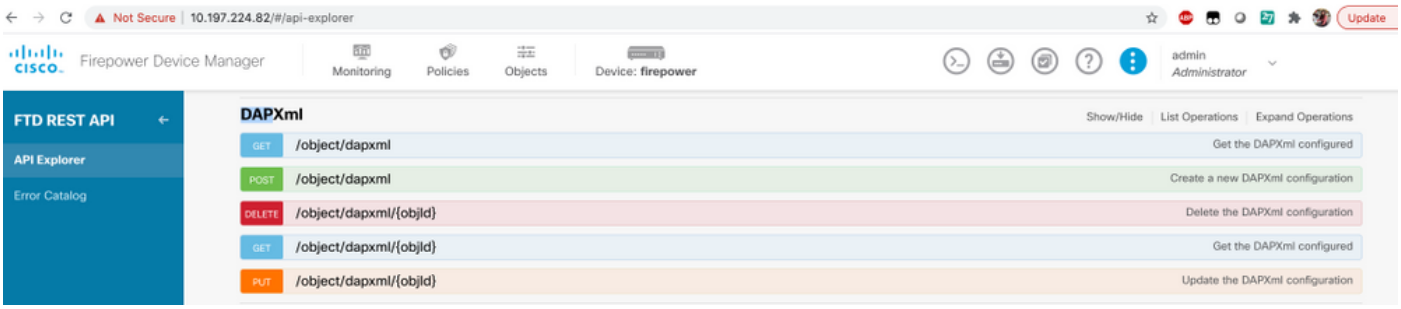
对data.xml执行相同的步骤。

步骤4.在浏览器窗口中启动FTD的API浏览器。

导航至**https://<FTD管理IP>/api-explorer**

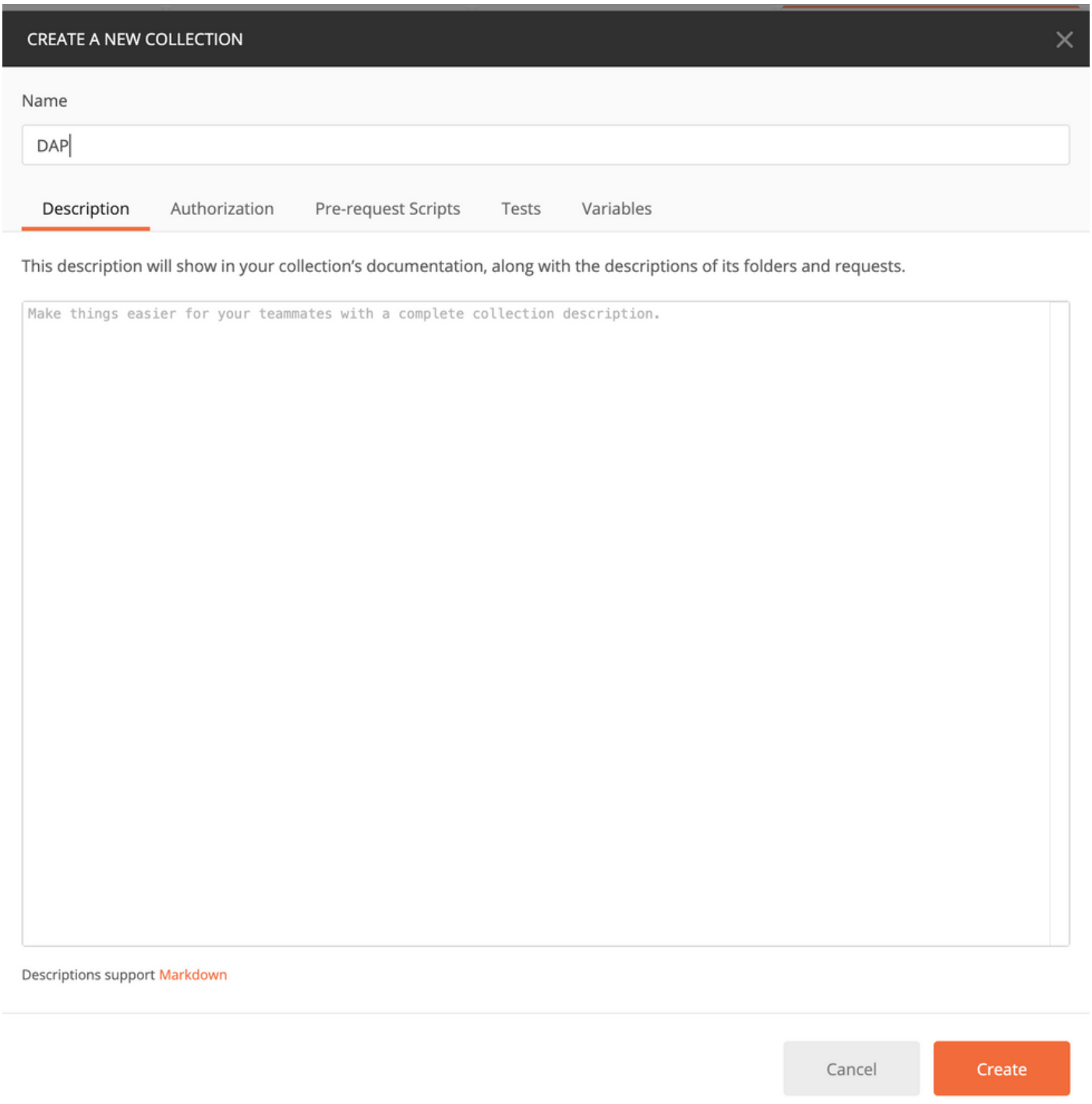
这包含FTD上可用的API的完整列表。它根据FDM支持的多个GET/POST/PUT/DELETE请求的主要功能进行划分。

DAPXml和**HostScanPackageFile**是使用的API。



第五步： 为DAP添加Postman集合。

为集合**提**供名称。单击“**创建**”，如下图所示。



第六步： 添加新请求 **auth** 创建到FTD的登录POST请求，以便获取令牌以授权任何POST/GET/PUT请求。单击“**Save(保存)**”。