Migración de DAP y HostScan de ASA a FDM a través de la API REST

Contenido

Introducción

Este documento describe la migración de las políticas de acceso dinámico (DAP) y la configuración de HostScan de Cisco Adaptive Security Appliances (ASA) a Cisco Firepower Threat Defense (FTD) gestionada localmente por Firepower Device Manager (FDM).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento básico de la configuración de VPN RA en FDM.
- Trabajo de DAP y HostScan en ASA.
- Conocimiento básico de la API REST y el Explorador de API Rest de FDM.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco FTD ejecutando la versión 6.7.0
- Cliente de Cisco AnyConnect Secure Mobility versión 4.9.00086
- Postman o cualquier otra herramienta de desarrollo API

Nota: La información de este documento se creó a partir de dispositivos en un entorno de laboratorio específico. All of the devices used in this document started with a cleared

(default) configuration. Si su red está activa, asegúrese de comprender el impacto potencial de cualquier cambio de configuración.

Antecedentes

Aunque FTD tiene compatibilidad con la configuración de VPN de acceso remoto (RAVPN), carece de compatibilidad con DAP. A partir de la versión 6.7.0, se agrega soporte de API para DAP en el FTD. Se ha diseñado para admitir el caso práctico más básico de la migración de ASA a FTD. Los usuarios que tienen DAP configurado en sus ASA y están en proceso de migrar a FTD ahora tienen una ruta para migrar su configuración DAP junto con su configuración de VPN RA.

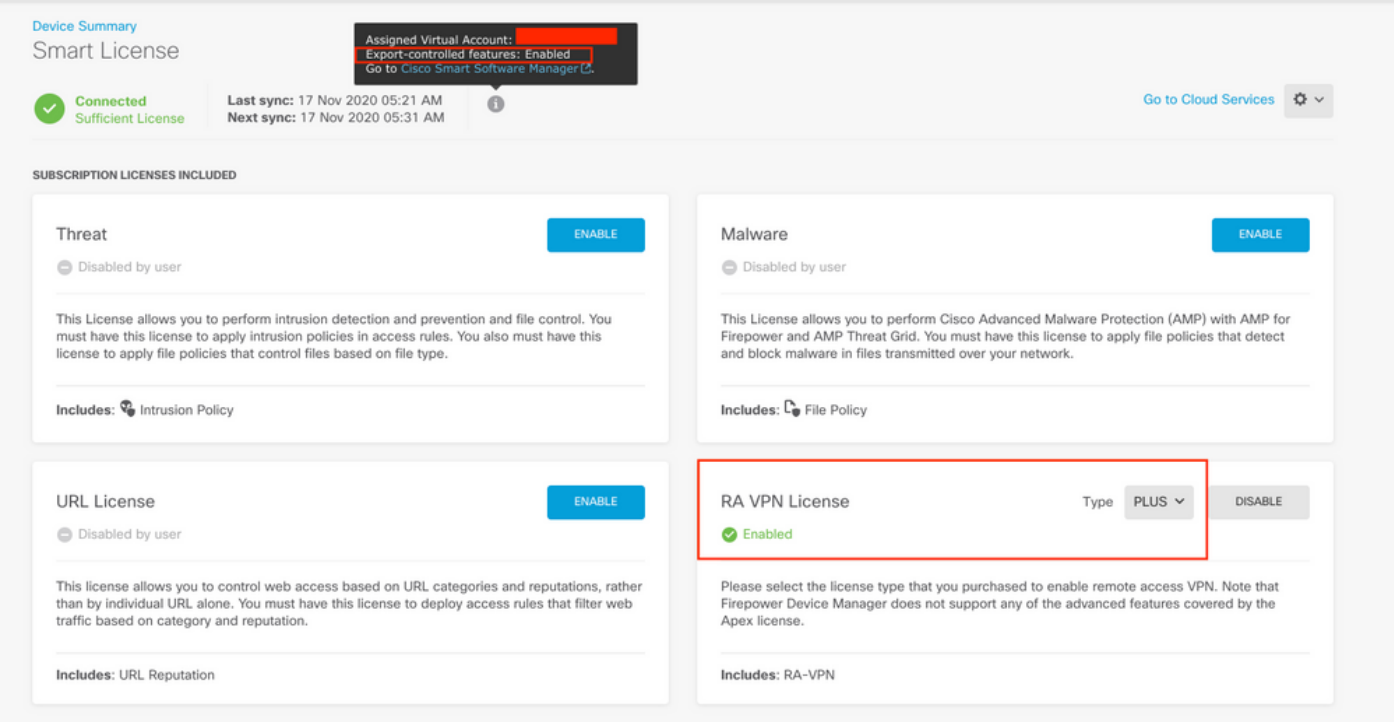
Para migrar correctamente la configuración DAP de ASA a FTD, asegúrese de estas condiciones:

- ASA con DAP/HostScan configurado.
- Acceso al servidor TFTP/FTP desde ASA o ASDM al ASA.
- Cisco FTD que ejecuta la versión 6.7.0 y las versiones posteriores gestionadas por Firepower Device Manager (FDM).
- VPN RA configurada y funcionando en FTD.

Licencias

- FTD se registró en el portal de licencias inteligente con las funciones controladas de exportación activadas (para permitir que se habilite la ficha de configuración de VPN de RA).
- Cualquiera de las licencias de AnyConnect habilitadas (APEX, Plus o VPN-Only).

Para verificar la licencia: Vaya a **Dispositivos > Licencias inteligentes**



Limitaciones de la función

- Estas funciones solo se admiten a través de la interfaz API FDM/FTD REST.

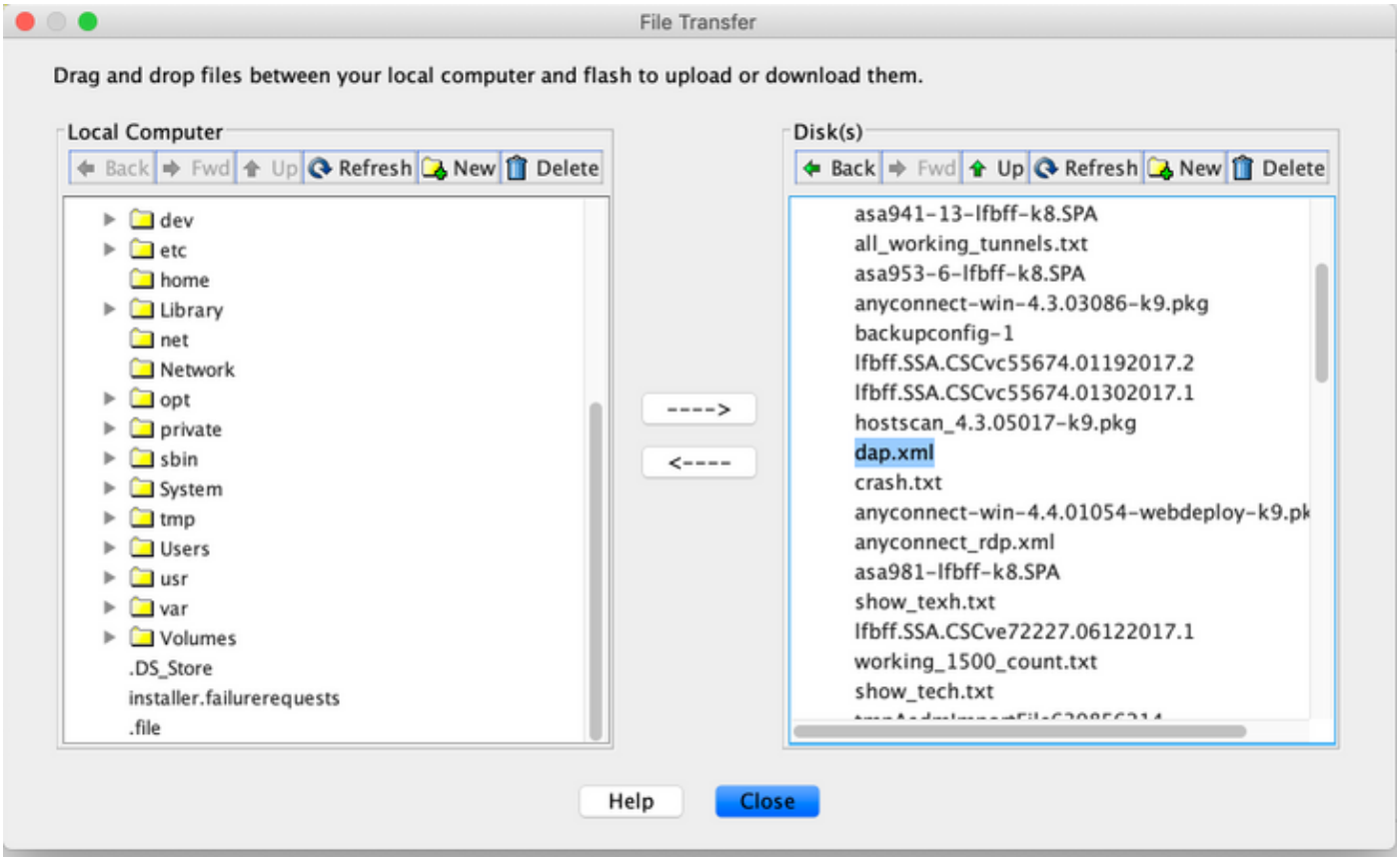
- El nombre DAP no puede contener caracteres de espacio con la API REST.

Configuración

Paso 1. Copie dap.xml de ASA en su PC local / servidor TFTP. Hay dos maneras de lograr lo mismo:

ASDM:

Vaya a **Herramientas > Administración de archivos > Transferencia > Entre PC local y Flash**.



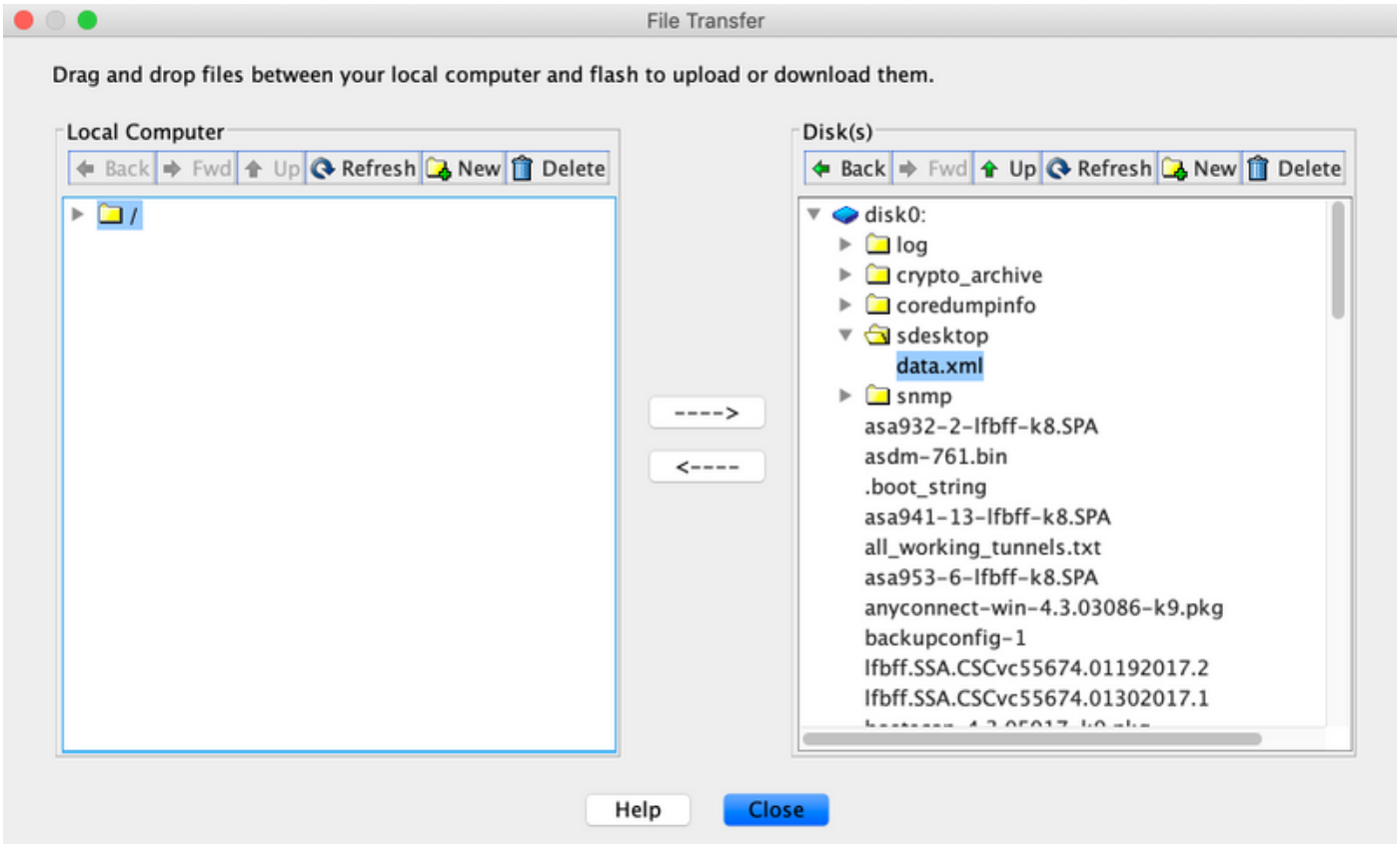
CLI:

```
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
```

Paso 2. Copie el archivo de configuración de HostScan (data.xml) y la imagen de HostScan desde ASA al dispositivo local.

ASDM:

Vaya a **Herramientas > Administración de archivos > Transferencia > Entre PC local y Flash**.



CLI:

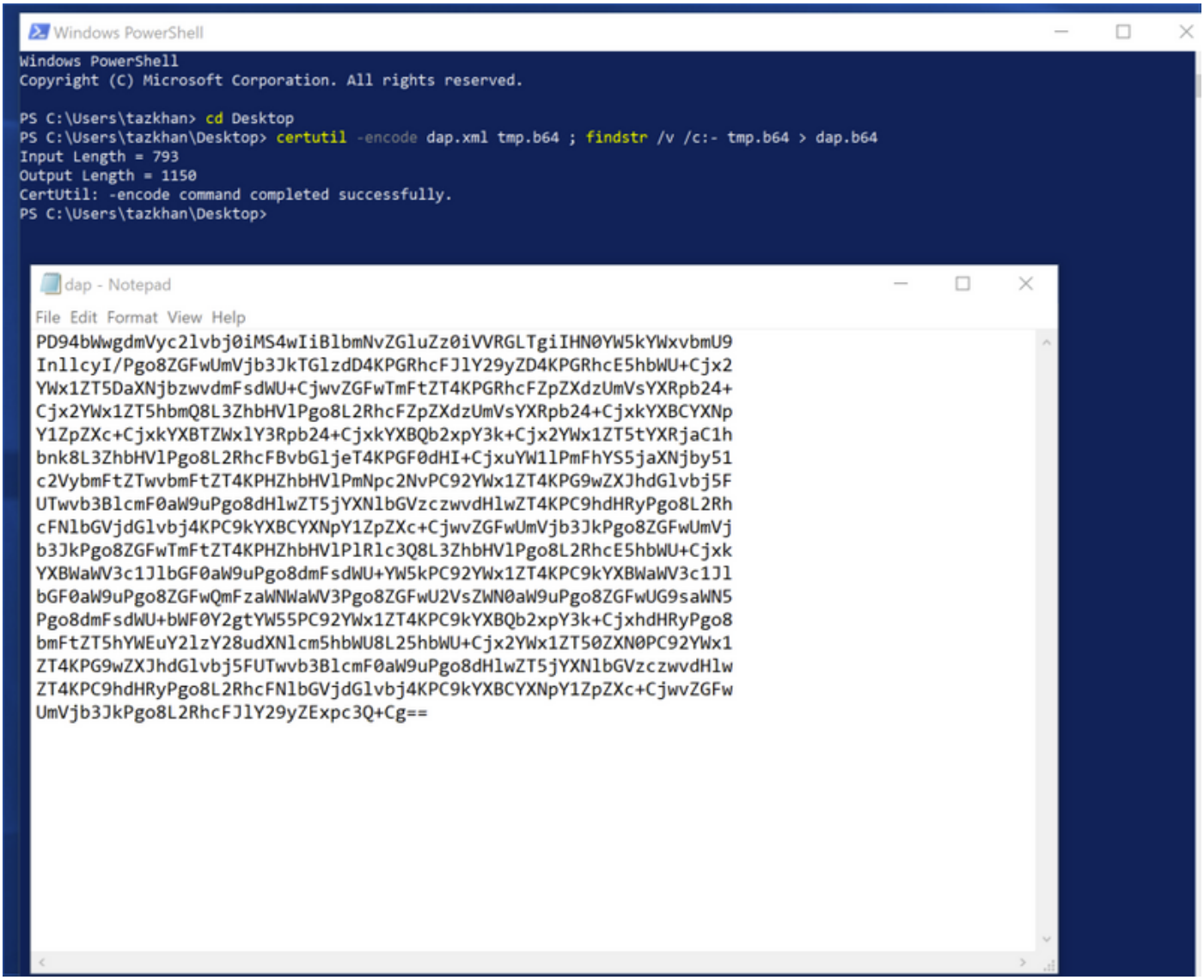
```
ASA# copy flash: tftp:
Source filename []? data.xml

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#
```

Paso 3. Obtenga el valor codificado base64 de **dap.xml** y **data.xml**.

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

```
tazkhan@TAZKHAN-M-32A3 Desktop % base64 -i dap.xml
PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiIHN0YW5kYWxvbmU9InllcyI/Pgo8ZGFwUmVjb3JkTGlzdD4KPGRhcFJlY29yZD4
KPGRhcE5hbWU+Cjx2YWx1ZT5XaW5kb3dzPC92YWx1ZT4KPC9kYXBOYW1lPgo8ZGFwVmlld3NSZWxhdGlvbj4KPHZhbHVlPmFuZDwvdmFsdWU+Cj
wvZGFwVmlld3NSZWxhdGlvbj4KPGRhcEJhc2ljVmlldz4KPGRhcFNlbGVjdGlvbj4KPGRhcFBvbGljeT4KPHZhbHVlPm1hdGNoLWFueTwvdmFsd
WU+CjwvZGFwUG9saWN5Pgo8YXR0cj4KPG5hbWU+YWFhLmNpc2NvLnVzZXJuYW1lPC9uYW1lPgo8dmFsdWU+Y2lzY288L3ZhbHVlPgo8b3BlcmF0
aW9uPkFkVRPC9vcGVyYXRpb24+Cjx0eXBlPmNhc2VsZXNzPC90eXBlPgo8L2F0dHI+CjxhdHRyPgo8bmFtZT5hbWQ8L25hbWU+CjwvYXR0cj4K
PC9kYXBSZWNvcmQ+CjxkYXBSZWNvcmQ+CjxkYXBOYW1lPgo8dmFsdWU+V2luZG93czwvdmFsdWU+CjwvZGFwTmFtZT4KPGRhcFZpZXdzUmVsYXRpb24+Cjx2YWx1ZT5hbmQ8L3ZhbHVlPgo8L2RhcFZpZXdzUmVsYXRpb24+CjwvZGFwUmVjb3JkTGlzdD4KPC9kYXBzZXNzaW9uRGF0YT4K
Q+Cg==
```

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



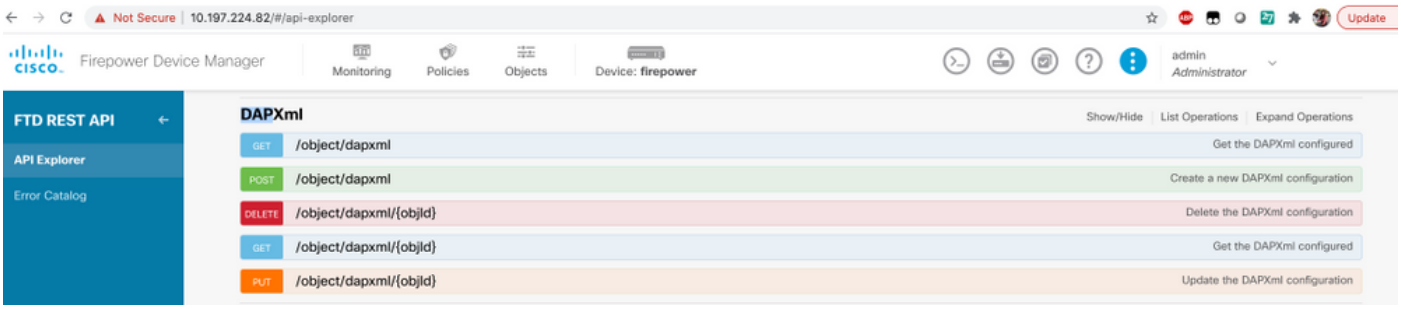
Siga el mismo procedimiento para data.xml.

Paso 4. Inicie el Explorador de API del FTD en una ventana del explorador.

Vaya a **https://<FTD Management IP>/api-explorer**

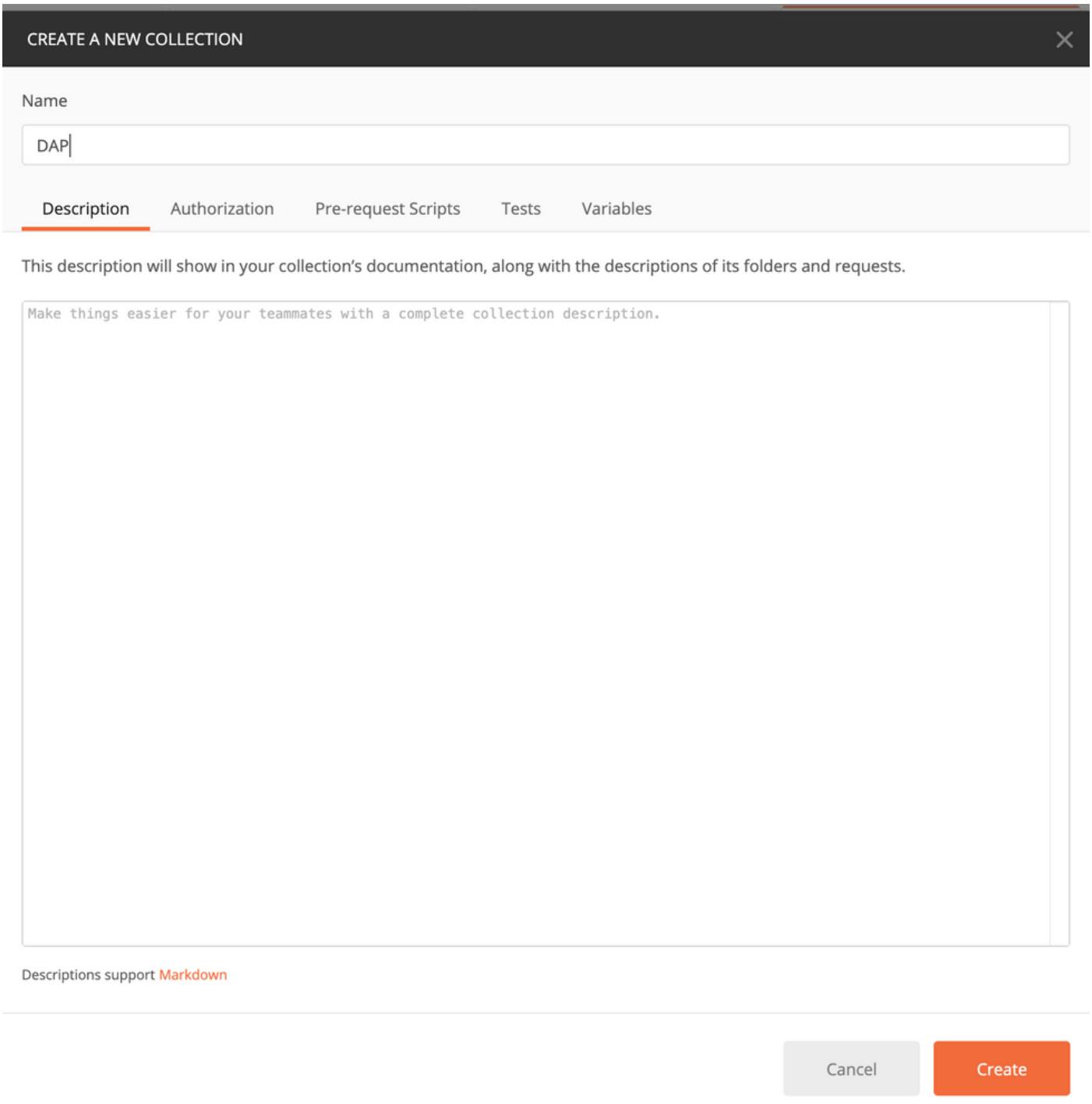
Esto contiene la lista completa de API disponibles en el FTD. Se divide en función de la función principal con varias solicitudes GET/POST/PUT/DELETE que admite el FDM.

DAPXml y **HostScanPackageFile** son la API utilizada.



Paso 5. Agregue una colección Postman para DAP.

Proporcione un **nombre** para la colección. Haga clic en **Crear**, como se muestra en esta imagen.



Paso 6. Agregar una nueva solicitud **Autenticación** para crear una solicitud POST de inicio de sesión en el FTD para obtener el token para autorizar cualquier solicitud POST/GET/PUT. Haga

clic en **Guardar**.