# 通過REST API從ASA遷移到FDM的DAP和 HostScan

## 目錄

<u>簡介</u> <u>必要條件</u> <u>需求</u> <u>採用元件</u> <u>背景資訊</u> <u>授權</u> <u>功能限制</u> <u>組態</u> <u>驗證</u> <u>從FTD GUI進行部署驗證</u> <u>從FTD CLI進行部署驗證</u> <u>疑難排解</u>

# 簡介

本檔案介紹將動態存取原則(DAP)和HostScan組態從思科調適型安全裝置(ASA)遷移到由 Firepower裝置管理員(FDM)本地管理的Cisco Firepower威脅防禦(FTD)的過程。

## 必要條件

### 需求

思科建議您瞭解以下主題:

- 有關FDM上的RA VPN配置的基本知識。
- •在ASA上使用DAP和Hostscan。
- REST API和FDM Rest API資源管理器基礎知識。

### 採用元件

本文中的資訊係根據以下軟體和硬體版本:

- 執行6.7.0版的Cisco FTD
- Cisco AnyConnect安全行動化使用者端版本4.9.00086
- Postman或任何其他API開發工具

**注意:**本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清 除(預設)的組態來啟動。如果您的網路正在作用,請確保您已瞭解任何組態變更的潛在影響 。

背景資訊

即使FTD具有遠端存取VPN(RAVPN)組態支援,它仍缺乏對DAP的支援。自6.7.0版起,FTD上新增 對DAP的API支援。它旨在支援從ASA遷移到FTD的基本使用案例。在ASA上配置了DAP並正在遷 移到FTD的使用者現在具有遷移其DAP配置及其RA VPN配置的路徑。

若要成功將DAP配置從ASA遷移到FTD,請確保以下條件:

- •配置了DAP/Hostscan的ASA。
- TFTP/FTP伺服器從ASA訪問,或ASDM訪問ASA。
- 運行版本6.7.0及更高版本的Cisco FTD,由Firepower裝置管理器(FDM)管理。
- •已配置RA VPN並正在處理FTD。

### 授權

- FTD已註冊到已啟用匯出控制功能的智慧許可門戶(以便啟用RA VPN配置頁籤)。
- •任何一個AnyConnect許可證已啟用(APEX、Plus或僅VPN)。

### 若要檢查授權:導覽至Devices > Smart Licenses

<sup>Device Summary</sup> Smart License	Assigned Virtual Account: Export-controlled features: Enabled Go to Cisco Smart Software Manager C.	
Connected Sufficient License	Last sync: 17 Nov 2020 05:21 AM Next sync: 17 Nov 2020 05:31 AM	Go to Cloud Services 🗘 🗸
SUBSCRIPTION LICENSES INCL	UDED	
Threat Disabled by user	ENABLE	Malware ENABLE
This License allows you must have this license to license to apply file polic	to perform intrusion detection and prevention and file control. You o apply intrusion policies in access rules. You also must have this cies that control files based on file type.	This License allows you to perform Cisco Advanced Malware Protection (AMP) with AMP for Firepower and AMP Threat Grid. You must have this license to apply file policies that detect and block malware in files transmitted over your network.
Includes: 🌯 Intrusion Pe	olicy	Includes: C File Policy
URL License Disabled by user	ENABLE	RA VPN License Type PLUS V DISABLE
This license allows you t than by individual URL al traffic based on category	to control web access based on URL categories and reputations, rather lone. You must have this license to deploy access rules that filter web y and reputation.	Please select the license type that you purchased to enable remote access VPN. Note that Firepower Device Manager does not support any of the advanced features covered by the Apex license.
Includes: URL Reputatio	n	Includes: RA-VPN

### 功能限制

- 僅通過FDM/FTD REST API介面支援這些功能。
- DAP名稱不能包含帶有REST API的空格字元。

### 組態

步驟1.將dap.xml從ASA複製到本地PC/TFTP伺服器。實現相同目標的方式有兩種:

ASDM:

### 導覽至Tools > File Management >File Transfer >Between Local PC and 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
步驟2. 將hostscan配置檔案(data.xml)和hostscan映像從ASA複製到本地裝置。
```

ASDM:

導航到Tools > File Management >File Transfer >Between Local PC and 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

步驟3. 獲取dap.xml和data.xml的base64編碼值。

在Mac上: base64 -i <file>

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

PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiIHN0YW5kYWxvbmU9InllcyI/Pgo8ZGFwUmVjb3JkTGlzdD4KPGRhcFJlY29yZD4 KPGRhcE5hbWU+Cjx2YWx1ZT5XaW5kb3dzPC92YWx1ZT4KPC9kYXB0YW1lPgo8ZGFwVmlld3NSZWxhdGlvbj4KPHZhbHV1PmFuZDwvdmFsdWU+Cj wvZGFwVmlld3NSZWxhdGlvbj4KPGRhcEJhc2ljVmlldz4KPGRhcFNlbGVjdGlvbj4KPGRhcFBvbGljeT4KPHZhbHV1Pm1hdGNoLWFueTwvdmFsd WU+CjwvZGFwUG9saWN5Pgo8YXR0cj4KP65hbWU+YWFhLmNpc2NvLnVzZXJuYW11PC9uYW11Pgo8dmFsdWU+Y2lzY288L3ZhbHV1Pgo8b3BlcmF0 aW9uPkVRPC9vcGVyYXRpb24+Cjx0eXB1PmNhc2VsZXNzPC90eXB1Pgo8L2F0dHI+CjwvZGFwU2VsZWN0aW9uPgo8ZGFWU2VsZWN0aW9uPgo8ZGF wUG9saWN5Pgo8dmFsdWU+bWF0Y2gtYW55PC92YWx1ZT4KPC9kYXBQb2xpY3k+CjxkYXBTdWJTZWx1Y3Rpb24+CjxkYXBQb2xpY3k+Cjx2YWx1ZT 5tYXRjaC1hbGw8L3ZhbHV1Pgo8L2RhcFBvbG1jeT4KPGF0dHI+CjxuYW11PmVuZHBvaW50LmFueWNvbm51Y3QucGxhdGZvcm08L25hbWU+cjx2Y Wx1ZT53aW48L3ZhbHV1Pgo8b3B1cmF0aW9uPkVRPC9vcGVyYXRpb24+CjwvYXR0cj4KPC9kYXBTdWJTZWx1Y3Rpb24+CjwvZGFwU2VsZWN0aW9u Pgo8L2RhcEJhc21jVmlldz4KPC9kYXBSZWNvcmQ+CjxkYXBSZWNvcmQ+CjxkYXBOYW1Pgo8dmFsdWU+YTwvdmFsdWU+CjwvZGFwTmFtZT4KPGR hcFzpZXdzUmVsYXRpb24+cjx2YWx1ZT5hbmQ8L3ZhbHV1Pgo8L2RhcFZpZXdzUmVsYXRpb24+CjwvZGFwUmVjb3JkPgo8L2RhcFJ1Y29yZExpc3 Q+Cg==

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

Windows PowerShell	-	]	×
<pre>Windows PowerShell Copyright (C) Microsoft Corporation. All rights reserved. PS C:\Users\tazkhan&gt; cd Desktop PS C:\Users\tazkhan\Desktop&gt; certutil -encode dap.xml tmp.b64 ; findstr /v /c:- tmp.b64 &gt; dap.b64 Input Length = 793 Output Length = 1150 CertUtil: -encode command completed successfully. PS C:\Users\tazkhan\Desktop&gt;</pre>			
	×		

對data.xml執行相同的過程。

步驟4.在瀏覽器視窗中啟動FTD的API瀏覽器。

#### 導覽至https://<FTD Management IP>/api-explorer

此清單包含FTD上可用的全部API清單。它基於FDM支援的多個GET/POST/PUT/DELETE請求的主要功能進行劃分。

使用的是DAPXml和HostScanPackageFile。

← → C ▲ Not Secure	10.197.224.82/#/	api-explorer										٦	à 💿 🖬 O	27	🛊 🐒 🗘 Update
CISCO. Firepower Devi	ice Manager	题 Monitoring	Ø Policies	iiz: Objects	Device: firepo	er		(ک	()	0	?	•	admin Administrator	Ň	
FTD REST API 🗧 🗧	DAPX	ml									Show	w/Hide	List Operations	Expand	I Operations
ADI Evolorer	GET	/object/dapxml											Get the	e DAPXn	l configured
AFTEXPIOLE	POST	/object/dapxml											Create a new [	APXml o	onfiguration
Error Catalog	DELETE	/object/dapxml/{ol	bjld}										Delete the D	APXml c	onfiguration
	GET	Get the DAPXml (objid) Get the DAPXml of							l configured						
	PUT	/object/dapxml/{ol	bjld}										Update the I	APXml o	onfiguration

### 步驟5. 為DAP新增Postman集合。

為集合提供**名稱**。按一下「Create」,如下圖所示。

CREATE A NEW (	COLLECTION				×
Name					
DAP					
Description	Authorization	Pre-request Scripts	Tests	Variables	

This description will show in your collection's documentation, along with the descriptions of its folders and requests.

Make things easier for your teammates with a complete collection description.

Descriptions support Markdown

Cancel

reate

# **步驟6.** 新增新請求 **身份驗證** 建立到FTD的登入POST要求,以取得權杖來授權任何 POST/GET/PUT要求。按一下Save。