從FMC GUI下載FTD裝置上的檔案

簡介

本檔案介紹將任何檔案從FTD和FMC裝置下載到FMC GUI的程式。

必要條件

需求

思科建議您瞭解以下產品:

- 安全防火牆管理中心(FMC)
- Firepower Threat Defense (FTD)

採用元件

本文中的資訊係根據以下軟體和硬體版本:

- 適用於VMware的Firepower威脅防禦7.0.4版
- 適用於VMware的安全防火牆管理中心版本7.2.2

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。如果您的網路運作中,請確保您瞭解任何指令可能造成的影響。

背景資訊

進行FTD或FMC疑難排解時,有時您必須從上述裝置下載檔案(例如透過外部工具進行分析的封包 擷取),或是將來自您裝置的檔案提供給Cisco TAC進行分析。待下載的檔案識別出來後,此操作 將變成兩個步驟:首先,將檔案移動到正確的位置;其次,從FMC GUI下載檔案。

程式

將檔案移到正確的資料夾

FMC

在此範例中,您可以從FMC GUI下載TAC要求的其他疑難排解和根本原因分析的Core檔案。

將檔案移動到/var/common資料夾

在這種情況下,Core檔案已經位於/var/common資料夾中,但是您可以分別使用cp或mv命令來移動 檔案,以便複製或移動,如下圖所示。

<#root>

expert

sudo su

{cp | mv} /

/

/var/common/

> expert admin@firepower:~\$ sudo su Last login: Tue Mar 28 17:18:27 UTC 2023 on pts/0 root@firepower:/Volume/home/admin# ls -ls /var/common | grep -i core 11572 -rw----- 1 root root 11847876 Mar 28 17:17 core_1680023838_firepower_SFD ataCorrelato_6.9451.gz root@firepower:/Volume/home/admin#

FTD

在本範例中,從FTD產生並下載show tech-support,然後從FMC GUI下載。

首先,運行show tech-support命令並重定向該命令,如下圖所示。

<#root>

show tech-support | redirect disk0:/show-tech.log

firepower# show tech-support redirect disk0:/show-tech.log firepower# dir disk0:									
Directory of disk0:/									
125	-rwx	1005	04:33:12	Jul	28	2021	lina phase1.log		
58	drwx	4096	20:25:40	Dec	06	2022	log		
64	drwx	4096	20:27:48	Jul	13	2022	coredumpinfo		
126	-rwx	0	16:53:28	Mar	01	2023	hitcnt_del_ruleid_list		
127	-rwx	4234	20:15:00	Dec	06	2022	backup-config.cfg		
128	-rwx	4127	20:15:00	Dec	06	2022	modified-config.cfg		
57	-rwx	3402	06:12:42	Mar	11	2023	asa-cmd-server.log		
60	-rwx	39	06:12:45	Mar	11	2023	<pre>snortpacketinfo.conf</pre>		
61	-rwx	1794	06:13:04	Mar	11	2023	dpdk.log		
129	drwx	4096	16:38:58	Feb	16	2023	cd-delta		
136	-rwx	282826	17:06:01	Mar	28	2023	show-tech.log		

將檔案移動到/ngfw/var/common資料夾

在這種情況下,當您將檔案儲存在disk0上時,您需要將其從/mnt/disk0移到/ngfw/var/common,如 下圖所示。

<#root>

expert

sudo su

從FMC GUI下載檔案

```
expert
sudadmin@firepower:~$ sudo su
Password:
root@firepower:/home/admin# cd /mnt/disk0
root@firepower:/mnt/disk0# ls -ls
total 328
  4 -rwxr-xr-x 1 root root
                             3402 Mar 11 06:12 asa-cmd-server.log
  8 -rwxr-xr-x 1 root root 4234 Dec 6 20:15 backup-config.cfg
  4 drwxr-xr-x 2 root root
                            4096 Feb 16 16:38 cd-delta
                                          2022 coredumpinfo
  4 drwxr-xr-x 2 root root 4096 Jul 13
                            4096 Jul 13 2022 csco config
  4 drwxr-xr-x 4 root root
  4 -rwxr-xr-x 1 root root
                             1794 Mar 11 06:13 dpdk.log
                                0 Mar 1 16:53 hitcnt del ruleid list
  0 -rwxr-xr-x 1 root root
                             1005 Jul 28
  4 -rwxr-xr-x 1 root root
                                          2021 lina phase1.log
  4 drwxr-xr-x 2 root root
                             4096 Dec 6 20:25 log
                                      6 20:15 modified-config.cfg
  8 -rwxr-xr-x 1 root root
                             4127 Dec
280 -rwxr-xr-x 1 root root 282826 Mar 28 17:06 show-tech.log
  4 -rwxr-xr-x 1 root root
                               39 Mar 11 06:12 snortpacketinfo.conf
root@firepower:/mnt/disk0#
root@firepower:/mnt/disk0# cp show-tech.log /ngfw/var/common
root@firepower:/mnt/disk0# ls -ls /ngfw/var/common/ | grep -i show
280 -rwxr-xr-x 1 root root 282826 Mar 28 17:20 show-tech.log
```

```
/ngfw/var/common/
```

```
cd /mnt/disk0
```

1

{cp | mv} /

在FMC GUI上,前往System > Health > Monitor,並選擇要從中下載檔案的裝置,如下圖所示。

System / Health / Monitor	nt Center Overview Analysis Policies De	Deploy Q 🔮 🔯 @ admin 🔻 🖓			
Monitoring	Health Status 2 critical 0 warnings 1 normal 0 disabled Firewall Management Center Devices	Configuration Users Domains Updates	Health Monitor Policy Events Exclude	Monitoring Audit Syslog Statistics	
testFTD102old	Device	Version	Licenses	Monitor Alerts	Tools
testftd118	> 0 FMC	7.2.2	Smart Licenses		Backup/Restore
	• testFTD102old • e testft118	7.0.4	Classic Licenses		Scheduling Import/Export Data Purge

選擇View System and Troubleshoot Details ...選項,該選項將展開Advanced Troubleshooting選項 ,如下圖所示。



選擇Advanced Troubleshooting選項,如下圖所示。

Monitoring E Health: testftd118 • Critical							Last 2023		
쉾 Home	System Details						Troubleshooting & Links		
Eirewall Management Center	Up Time:	17 days 9 hour	s		VDB:	Build 357 -	2022-07-19 19:54:00.0	Generate Troubleshooting Files	
	Version:	7.0.4			LSP:	lsp-rel-202	30322-1438	Advanced Troubleshooting	
V Devices (2)	Model:	Cisco Firepowe	er Threat Defe	nse for VMware	Snort:	3.1.0.400-1	12	Health Policy (Initial_Health_Policy 2022-06-16 13:34:26)	
testFTD102old	Mode:	ROUTED						Health Alerts	
e testftd118	Overview	W CPU	Memory	Interfaces	Connections	Snort	ASP drops		

您在「File Download」索引標籤上,輸入您要下載的檔案的名稱,然後選擇Download,如下圖所 示。



檔案下載從FMC GUI開始。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件,讓全世界的使用者能夠以自己的語言理解支援內容。請注 意,即使是最佳機器翻譯,也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準 確度概不負責,並建議一律查看原始英文文件(提供連結)。