从FMC GUI下载FTD设备上的文件

目录

箇介

先決条件

要求

使用的组件

背景信息

步骤

将文件移动到正确的文件夹

FMC

将文件移动到/var/common文件夹

FTD

将文件移动到/ngfw/var/common文件夹

从FMC GUI下载文件

简介

本文档介绍从FTD和FMC设备下载任何文件到FMC GUI的过程。

先决条件

要求

思科建议您了解以下产品:

- 安全防火墙管理中心(FMC)
- Firepower Threat Defense (FTD)

使用的组件

本文档中的信息基于以下软件和硬件版本:

- 适用于VMware的Firepower威胁防御7.0.4版
- 适用于VMware的安全防火墙管理中心版本7.2.2

本文档中的信息都是基于特定实验室环境中的设备编写的。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,请确保您了解所有命令的潜在影响。

背景信息

当FTD或FMC进行故障排除时,有时您必须从上述设备下载文件,例如数据包捕获以便在外部工具 上进行分析,或者从您的设备向思科TAC提供文件以供分析。确定要下载的文件后,此操作将分为 两个步骤:首先,将文件移动到正确的位置;其次,从FMC GUI下载文件。

步骤

将文件移动到正确的文件夹

FMC

在本例中,您将从FMC GUI下载一个TAC请求的核心文件,以进行其他故障排除和根本原因分析。

将文件移动到/var/common文件夹

在这种情况下,Core文件已经位于/var/common文件夹中,但您可以分别使用cp或mv命令来移动文件,以便复制或移动,如图所示。

<#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

在本示例中,从FTD生成并下载show tech-support,然后从FMC GUI下载该软件。

首先,运行show tech-support命令并将其重定向,如图所示。

<#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					

将文件移动到/ngfw/var/common文件夹

在这种情况下,当您将文件保存在disk0上时,您需要将其从/mnt/disk0移到/ngfw/var/common,如 映像所示。

<#root>

expert

sudo su

```
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
                            4096 Jul 13
  4 drwxr-xr-x 2 root root
                            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/
```

```
/
```

{cp | mv} /

cd /mnt/disk0

在FMC GUI上,转到System > Health > Monitor,并选择要从中下载文件的设备,如图所示。

Firewall Manageme System / Health / Monitor	nt Center Overview Analysis Policies D	evices Objects Integration	Deploy	९ 🔮 📮 🛛 adm	in • sisco SECURE
Monitoring බ Home * Firewall Management Center Devices (2)	Health Status 3 total 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	
e testFTD102old	Device	Version	Licenses	Monitor Alerts	Tools
testftd118	> 9 FMC	7.2.2	Smart Licenses		Backup/Restore
	> etestFTD102old	7.0.4	Classic Licenses		Scheduling
	> e testftd118	7.0.4			Import/Export Data Purge

选择View System和Troubleshoot Details ...选项,该选项将展开Advanced Troubleshooting选项 ,如图所示。



选择Advanced Troubleshooting选项,如图所示。

Monitoring	Health: testftd118 • Critical										
ि Home	etails					Troubleshooting & Links					
Firewall Management Center	Up Time: 17 days 9 hours			VDB:	Build 357 - 2022-07-19 19:54:00.0			Generate Troubleshooting Files			
Devices (0)	Version:	ersion: 7.0.4				lsp-rel-20230322-1438			Advanced Troubleshooting		
V Devices (2)	Model:	del: Cisco Firepower Threat Defense for VMware			Snort:	3.1.0.400-12			Health Policy (Initial_Health_Policy 2022-06-16 13:34:26)		
testFTD102old	Mode: ROUTED								Health Alerts		
e testftd118	Overviev	w CPU	Memory	Interfaces	Connections	Snort	ASP drops				

您在文件下载选项卡上,在此处输入要下载的文件的名称,然后选择下载,如图所示。

Firewall Management Center Devices / Troubleshoot / File Download	Overview	Analysis	Policies	Devices	Objects	Integration		Deploy	۹ (9 🗘	🕜 adm	in • 🔤	iste SEC	CURE
		_						Threat Defe	nse CLI	Pa	sket Captur	e Pa	cket Trac	cer
		Device testftd1	118		•									
		Enter th	Enter the name of the file to download from /ngfw/var/commo											
				Back	Downloa	d								

文件下载从FMC GUI开始。

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言,希望全球的用户都能通过各 自的语言得到支持性的内容。

请注意:即使是最好的机器翻译,其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任,并建议您总是参考英文原始文档(已提供 链接)。