

从 FMC 和 FTD 下载文件

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[复制文件](#)

[将文件从FTD复制到FMC](#)

[将文件从FMC复制到本地计算机](#)

[使用SCP进行复制](#)

[从GUI下载](#)

简介

本文档介绍如何将日志文件从思科Firepower管理中心(FMC)和Firepower威胁防御(FTD)下载到本地计算机。

先决条件

要求

Cisco 建议您了解以下主题：

- Cisco Firepower设备
- 虚拟设备型号

使用的组件

本文档不限于特定的软件和硬件版本。

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。

复制文件

将文件从FTD复制到FMC

FMC上有一个安全复制协议(SCP)服务器，因此，文件可以从FTD移动到FMC。

```
root@FMC:~$ scp admin@<FTD ip>:<path to file> <path to local directory where to store>
```

一个常见的示例是将核心文件从FTD移动到FMC。

在FTD上：

```
root@ciscoasa:/ngfw/var/common# ls -l
total 1557960
-rw-r--r-- 1 root root 23231 Sep 6 03:43 core_1482327396_Firepower-module1_snort_6
-rw----- 1 root root 560128000 Apr 26 01:47 core_1556242979_ciscoasa_snort_6.8777
-rw----- 1 root root 383381504 Aug 25 23:05 core_1566774281_ciscoasa_snort_11.31618
-rw----- 1 root root 69562368 Aug 25 23:05 core_1566774281_ciscoasa_snort_11.31620
-rw----- 1 root root 465424384 Aug 28 02:21 core_1566958444_ciscoasa_snort_6.18352
-rw----- 1 root root 116887552 Aug 28 02:18 core_1566958688_ciscoasa_snort_6.18340
-rw----- 1 root root 52338688 Aug 28 02:18 core_1566958689_ciscoasa_snort_6.18341
-rw----- 1 root root 465514496 Sep 2 02:20 core_1567390346_ciscoasa_snort_6.27631
-rw----- 1 root root 151572480 Sep 2 02:17 core_1567390618_ciscoasa_snort_6.27435
```

现在，将文件传输到FMC：

```
root@FMC:/Volume/home/admin# scp admin@10.10.10.10:/ngfw/var/common/core_1567390618_ciscoasa_snort_6.27
```

 注意：在scp命令上添加-v表示详细日志记录，以便进一步排除故障。

将文件从FMC复制到本地计算机

使用SCP进行复制

FMC上有一个安全复制协议(SCP)服务器，它使用可以从FMC移动到其他设备的文件。

```
root@FMC:~$ scp <path to local directory where to store> admin@<FMC ip>:<path to file>
```

一种常见的做法是将核心文件从FMC移动到本地桌面：

```
root@localMachine:/Volume/home/admin# scp admin@10.10.10.20:/var/common/core_1567390618_ciscoasa_snort_
```

[WinSCP](#)是一种常用的工具，经常用于Windows。此工具提供基于GUI的界面。

In FMC 6.4 and above, SCP to the FMC is not possible directly. For that, the following is needed(the be

```
root@FMC:/Volume/home/admin# usermod --shell /bin/bash admin
```

After this SCP to the FMC will work. Once done, please remember to rollback (prior to closing the session).

```
root@FMC:/Volume/home/admin# usermod --shell /usr/bin/clish admin
```

从GUI下载

可以从GUI下载存在/var/common的文件。

If there are any file(s) and/or tcpdump generated on the FMC, please move to /var/common, so that it can be accessed.

步骤1: 导航到系统>运行状况>监控，然后点击需要从中下载文件的传感器，如图所示：

The screenshot shows the 'Health Monitor' page in the FMC GUI. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', 'Intelligence', 'Deploy', 'System', 'Help', and 'admin'. The main content area is divided into two sections. On the left, there is a table titled 'Appliance Status Summary' with columns for 'Status' and 'Count'. On the right, there is a pie chart titled 'Appliance Status Summary' showing the distribution of appliance statuses. Below these, there is a table of appliances with columns for 'Appliance' and 'Description'. The 'firepower (Part Blacklisted)' appliance is highlighted with a red box.

Status	Count
Error	0
Critical	1
Warning	0
Recovered	0
Normal	1
Disabled	0

Appliance Status Summary

Normal (50.00%)
Critical (50.00%)

Appliance	Description
firepower (Part Blacklisted)	Critical Modules:1,Normal Modules:17,Disabled Modules:15 ModuleSmart License Monitor: Smart License usage is out of compliance

第二步：导航到系统 > 运行状况 > 监控，然后点击高级故障排除，如图所示：

The screenshot shows the 'Health Monitor' page in the FMC GUI, specifically the 'Advanced Troubleshooting' view for the 'firepower (Part Blacklisted)' appliance. The top navigation bar is the same as in the previous screenshot. The main content area is divided into two sections. On the left, there is a table titled 'Alert Detail (firepower)' with columns for 'Alert', 'Time', 'Description', and 'Display'. On the right, there is a pie chart titled 'Module Status Summary' showing the distribution of module statuses. Below these, there is a table of alerts with columns for 'Alert', 'Time', 'Description', and 'Display'. The 'Advanced Troubleshooting' button is highlighted with a red box.

Module Status Summary

Disabled (45.45%)
Normal (51.52%)
Critical (3.03%)

Alert	Time	Description	Display
Smart License Monitor	2019-09-02 21:47:23	Smart License usage is out of compliance	Run Events Graph
Appliance Heartbeat	2019-09-02 21:47:23	All appliances are sending heartbeats correctly	Run Events
Backlog Status	2019-09-02 21:47:23	No event backlog exists on any device	Run Events
Classic License Monitor	2019-09-02 21:47:23	Licenses are up to date	Run Events Graph
Disk Usage - Disk Test	2019-09-02 21:47:23	/ using 39%: 1.3G (2.2G Avail) of 3.7G	Run Events Graph
FMC HA Status	2019-09-02 21:47:23	Not in HA	Run Events
Hardware Alarms	2019-09-02 21:47:23	Hardware is functioning normally	Run Events

第三步：输入文件名并单击download，如图所示：

Advanced Troubleshooting

Firepower

File Download

File:

Opening core_1556148704_FMC_PerMessageHand_11.5976

You have chosen to open:

- core_1556148704_FMC_PerMessageHand_11.5976
which is: Text Document
from: https://fmc

What should Firefox do with this file?

Open with Notepad (default)

Save File

Do this automatically for files like this from now on.

```
vFMC
admin@FMC:/var/common$ ls -lh
total 67M
-rw-r--r-- 1 root root 70M Apr 24 23:31 core_1556148704_FMC_PerMessageHand_11.5976
admin@FMC:/var/common$
```

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）。