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复制
- 从GUI下载

简介

本文档介绍如何将日志文件从Cisco 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
- 虚拟设备模型

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以进行详细日志记录，以进一步排除故障。

将文件从FMC复制到本地计算机

使用SCP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 please create a new user with t
[Please make sure that this user does not exist on the device]

root@FMC:/Volume/home/admin# useradd -s /bin/bash temp_admin
root@FMC:/Volume/home/admin# passwd temp_admin

After this SCP to the FMC will work. Once done, please remeber to delete the user:

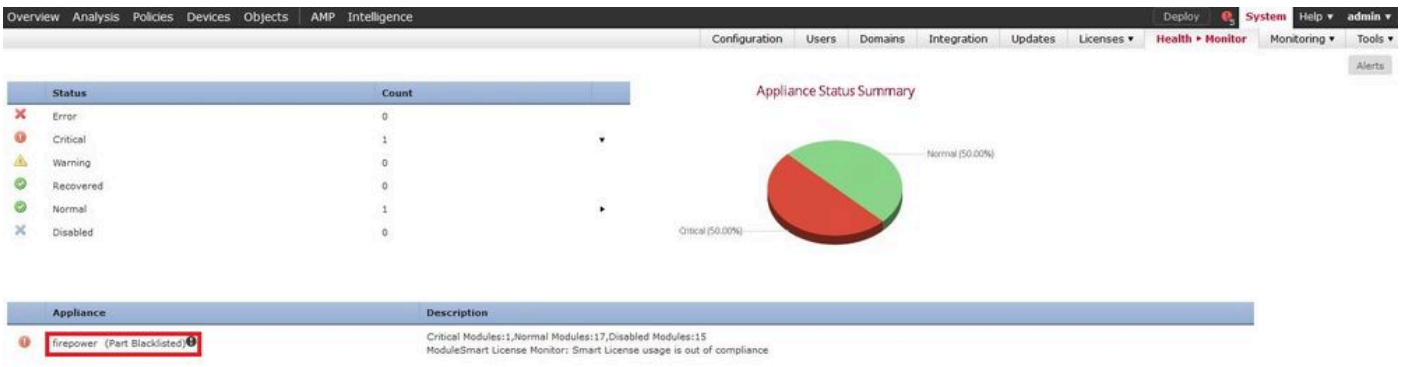
root@FMC:/Volume/home/admin# userdel temp_admin
```

从GUI下载

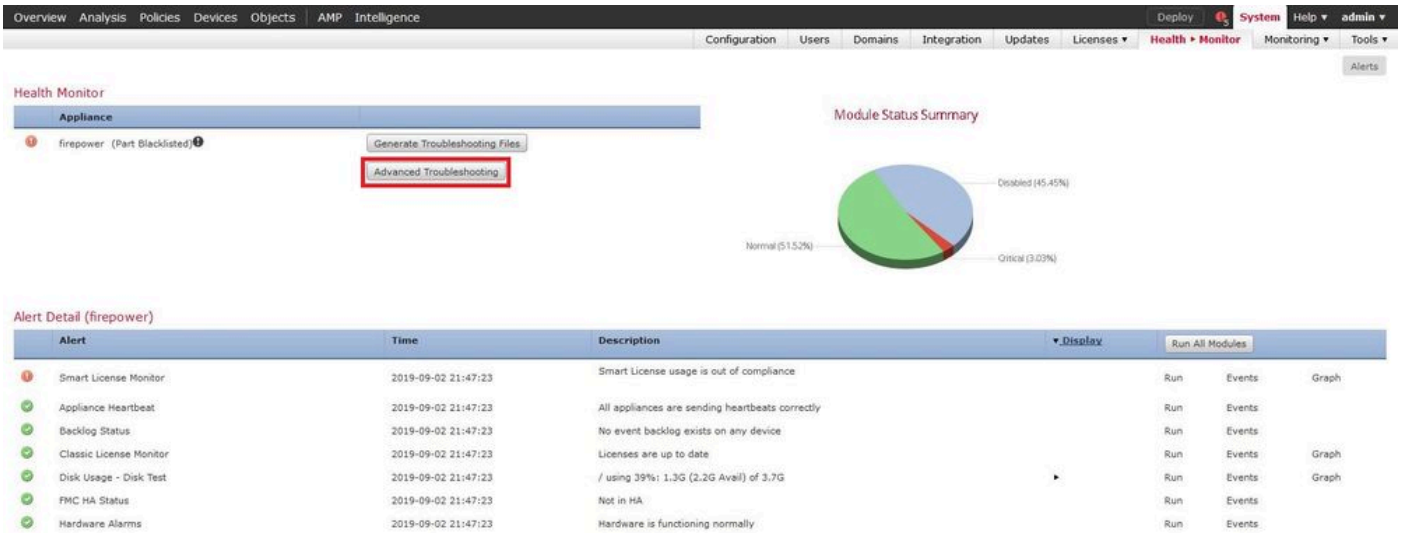
存在/var/common的文件可以从GUI下载。

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

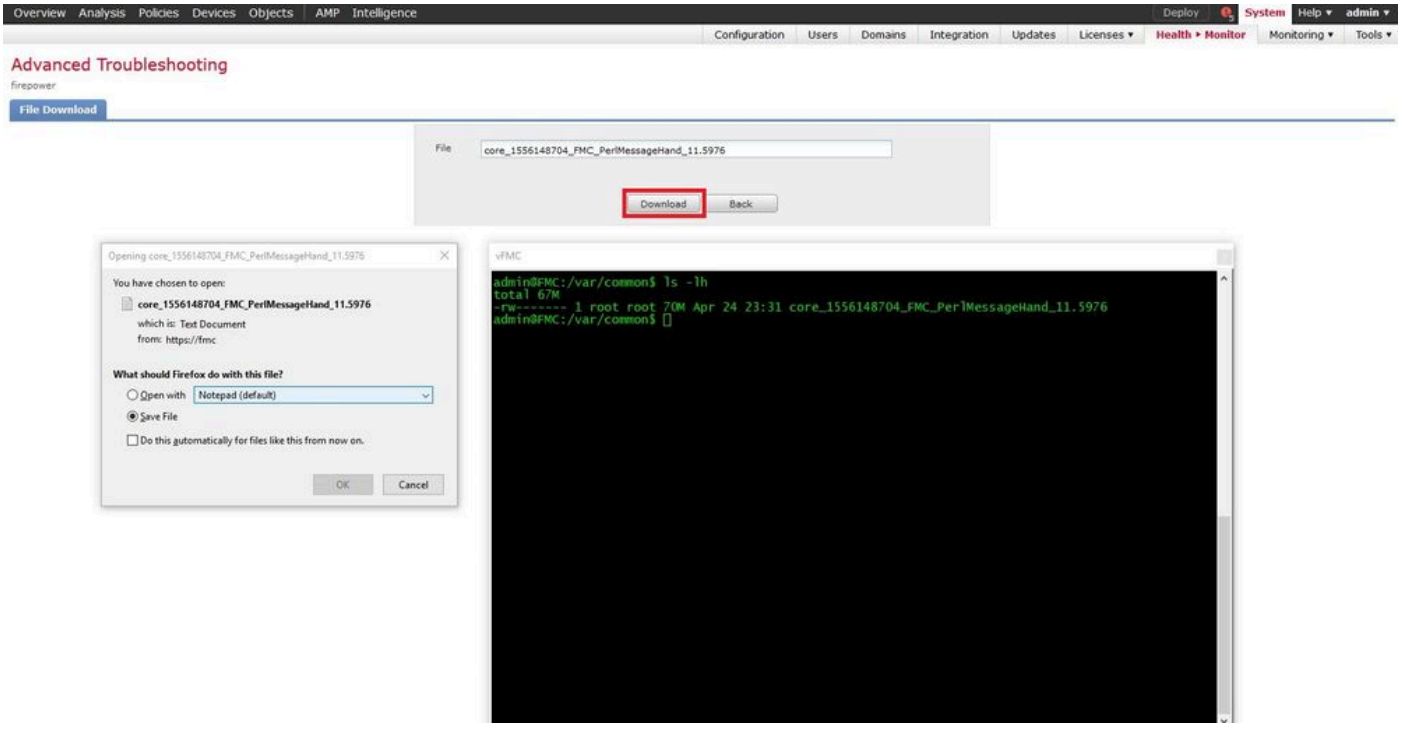
步骤1.导航到System > Health > Monitor，然后点击需要从中下载文件的传感器，如图所示：



步骤2.导航到System > Health > Monitor，然后单击Advanced Troubleshooting，如图所示：



步骤3.输入filename并单击download，如图所示：



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）。