Download Files from FMC and FTD

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Copy Files

- Copy File from FTD to FMC
- Copy Files from FMC to Local Machine
- Use SCP to Copy
- Download from GUI

Introduction

This document describes how to download log files from Cisco Firepower Management Center (FMC) and Firepower Threat Defense (FTD) to a local computer.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Firepower device
- Virtual device models

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Copy Files

Copy File from FTD to FMC

There is a Secure Copy Protocol (SCP) server on FMC, therefore, the files can be moved from FTD to FMC.

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

A common example is to move the core file(s) from FTD to the FMC.

On the FTD:

```
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
```

Now, transfer the file to the FMC:

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

Note: Add -v for verbose logging on the **scp** command to troubleshoot further.

Copy Files from FMC to Local Machine

Use SCP to Copy

There is a Secure Copy Protocol (SCP) server on FMC, and it uses the files that can be moved from FMC to another device.

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

A common practice is to move the core files from the FMC to local Desktop:

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

A popular tool, WInSCP is often used on Windows. This tool provides a GUI based interface.

```
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:

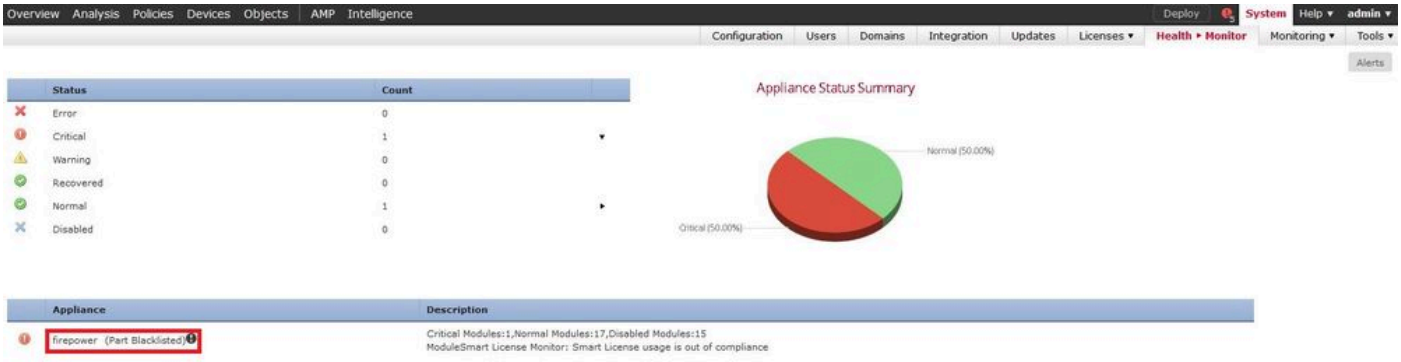
root@FMC:/Volume/home/admin# userdel temp_admin
```

Download from GUI

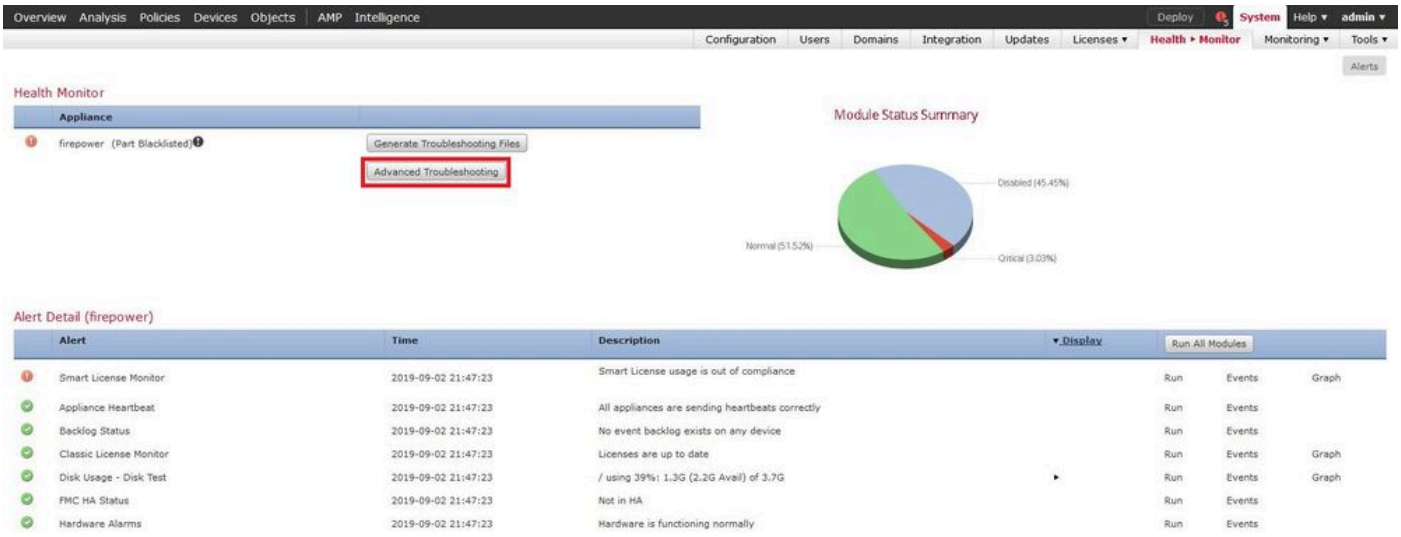
The files which are present /var/common can be downloaded from the GUI.

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

Step 1. Navigate to **System** > **Health** > **Monitor** and click the **sensor** from which the file needs to be downloaded, as shown in the image:



Step 2. Navigate to **System** > **Health** > **Monitor** and click **Advanced Troubleshooting**, as shown in the image:



Step 3. Enter the **filename** and click **download**, as shown in the image:

