

Download de arquivos do FMC e do FTD

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Copiar Arquivos](#)

[Copiar arquivo do FTD para o FMC](#)

[Copiar arquivos do FMC para o computador local](#)

[Usar SCP para copiar](#)

[Download da GUI](#)

Introduction

Este documento descreve como fazer o download de arquivos de log do Cisco Firepower Management Center (FMC) e do Firepower Threat Defense (FTD) para um computador local.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- dispositivo Cisco Firepower
- Modelos de dispositivo virtual

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Copiar Arquivos

Copiar arquivo do FTD para o FMC

Há um servidor Secure Copy Protocol (SCP) no FMC, portanto, os arquivos podem ser movidos do FTD para o FMC.

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

Um exemplo comum é mover o(s) arquivo(s) principal(is) do FTD para o FMC.

No 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
```

Agora, transfira o arquivo para o FMC:

```
root@FMC:/Volume/home/admin# scp admin@10.10.10.10:/ngfw/var/common/core_1567390618_ciscoasa_snort_6.27435
```

Observação: adicione -v para registro extenso no comando scp para fazer troubleshooting adicional.

Copiar arquivos do FMC para o computador local

Usar SCP para copiar

Há um servidor Secure Copy Protocol (SCP) no FMC e ele usa os arquivos que podem ser movidos do FMC para outro dispositivo.

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

Um procedimento comum é mover os arquivos principais do FMC para a área de trabalho local:

```
root@localMachine:/Volume/home/admin# scp admin@10.10.10.20:/var/common/core_1567390618_ciscoasa_snort_6
```

Uma ferramenta popular [WInSCP](#) é frequentemente usada no Windows. Essa ferramenta fornece uma interface baseada em GUI.

In FMC 6.4 and above, SCP to the FMC is not possible directly. For that, the following is needed(the bel
root@FMC:/Volume/home/admin# usermod --shell /bin/bash admin

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

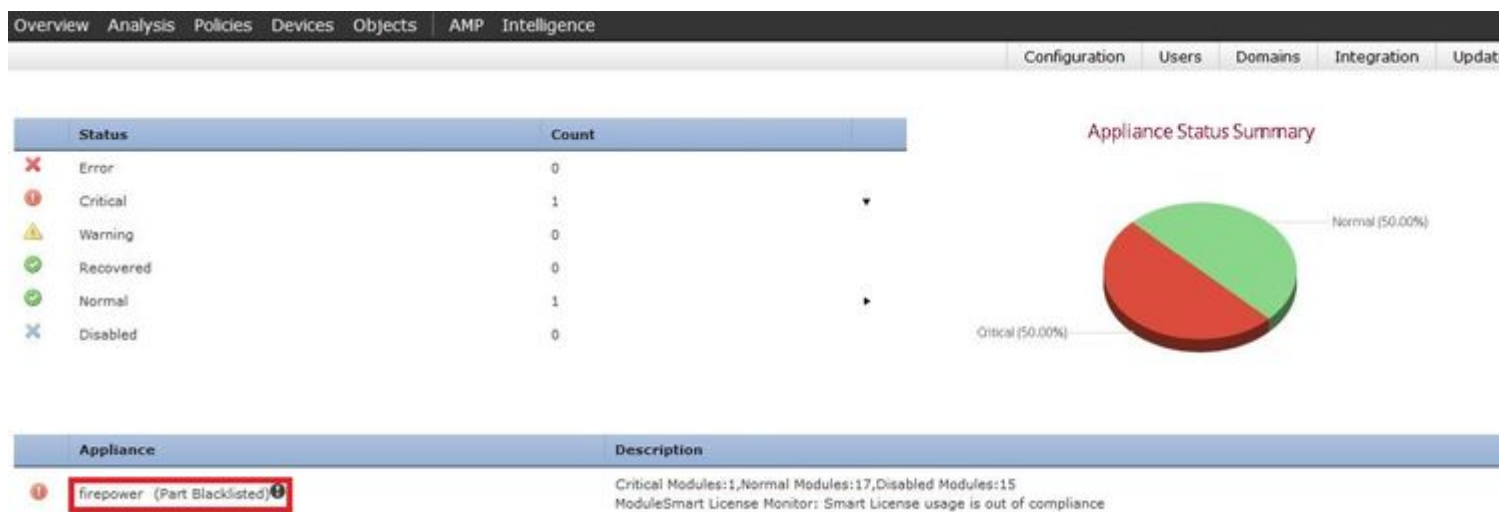
```
root@FMC:/Volume/home/admin# usermod --shell /usr/bin/clish admin
```

Download da GUI

Os arquivos que estão presentes **/var/common** podem ser baixados da GUI.

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

Etapa 1. Navegue até **System > Health > Monitor** e **clique** no sensor do qual o arquivo precisa ser baixado, como mostrado na imagem:



Etapa 2. Navegue até **System > Health > Monitor** e **clique** em Advanced Troubleshooting (Solução de problemas avançada), como mostrado na imagem:

Health Monitor

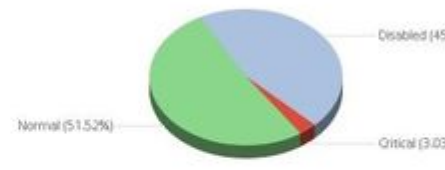
Appliance

firepower (Part Blacklisted)

Generate Troubleshooting Files

Advanced Troubleshooting

Module Status Summary



Alert Detail (firepower)

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

Etapa 3. Insira o nome do arquivo e **clique em download**, como mostrado na imagem:

Advanced Troubleshooting

firepower

File Download

File: core_1556148704_FMC_PerlMessageHand_11.5976

Download Back

Opening core_1556148704_FMC_PerlMessageHand_11.5976

You have chosen to open:

core_1556148704_FMC_PerlMessageHand_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.

OK Cancel

```
vFMC
admin@FMC:/var/common$ ls -lh
total 67M
-rw----- 1 root root 70M Apr 24 23:31 core_1556148704_FMC_PerlMessageHand
admin@FMC:/var/common$
```

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.