Bestanden downloaden van FMC en FTD

Inhoud

Inleiding

Dit document beschrijft hoe u logbestanden kunt downloaden van Cisco Firepower Management Center (FMC) en Firepower Threat Defence (FTD) naar een lokale computer.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco FirePOWER-apparaat
- Modellen voor virtuele apparaten

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Bestanden kopiëren

Bestand van FTD naar FMC kopiëren

Er is een Secure Copy Protocol (SCP)-server op het VCC, zodat de bestanden van het FTD naar het FMC kunnen worden verplaatst.

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

Een veel voorkomend voorbeeld is het verplaatsen van de kernbestanden van FTD naar FMC.

Wat het FTD betreft:

```
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
```

Overdracht het bestand nu naar het VCC:

```
root@FMC:/Volume/home/admin# scp admin@10.10.10.10:/ngfw/var/common/core_1567390618_ciscoasa_snort_6.274
```

Opmerking: Voeg -v toe voor breedsprakige logboekregistratie in de SCP-opdracht om verder problemen op te lossen.

Bestanden van VCC naar lokale machine kopiëren

SCP gebruiken om te kopiëren

Er is een Secure Copy Protocol (SCP)-server op het VCC en deze gebruikt de bestanden die van het VCC naar een ander apparaat kunnen worden verplaatst.

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

Een veel gebruikte optie is om de corefiles van het VCC naar het lokale bureaublad te verplaatsen:

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

Een populaire tool WInSCP wordt vaak gebruikt in Windows. Dit gereedschap biedt een op GUI gebaseerde interface.

```
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:
```

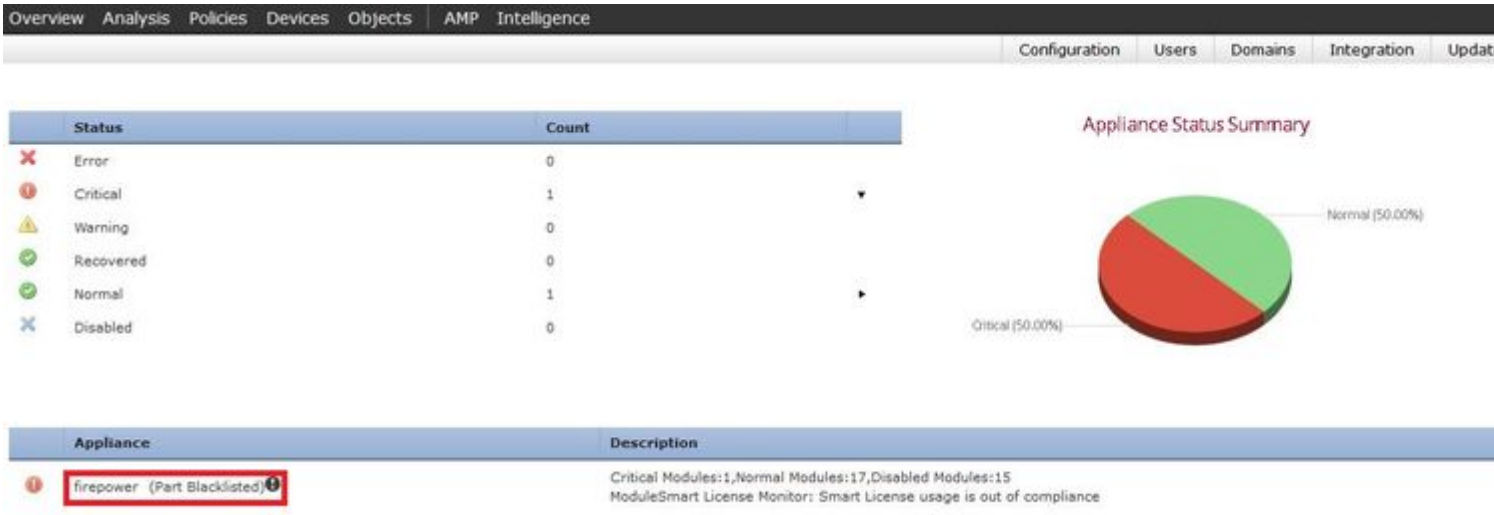
```
root@FMC:/Volume/home/admin# usermod --shell /usr/bin/clish admin
```

Downloaden vanuit GUI

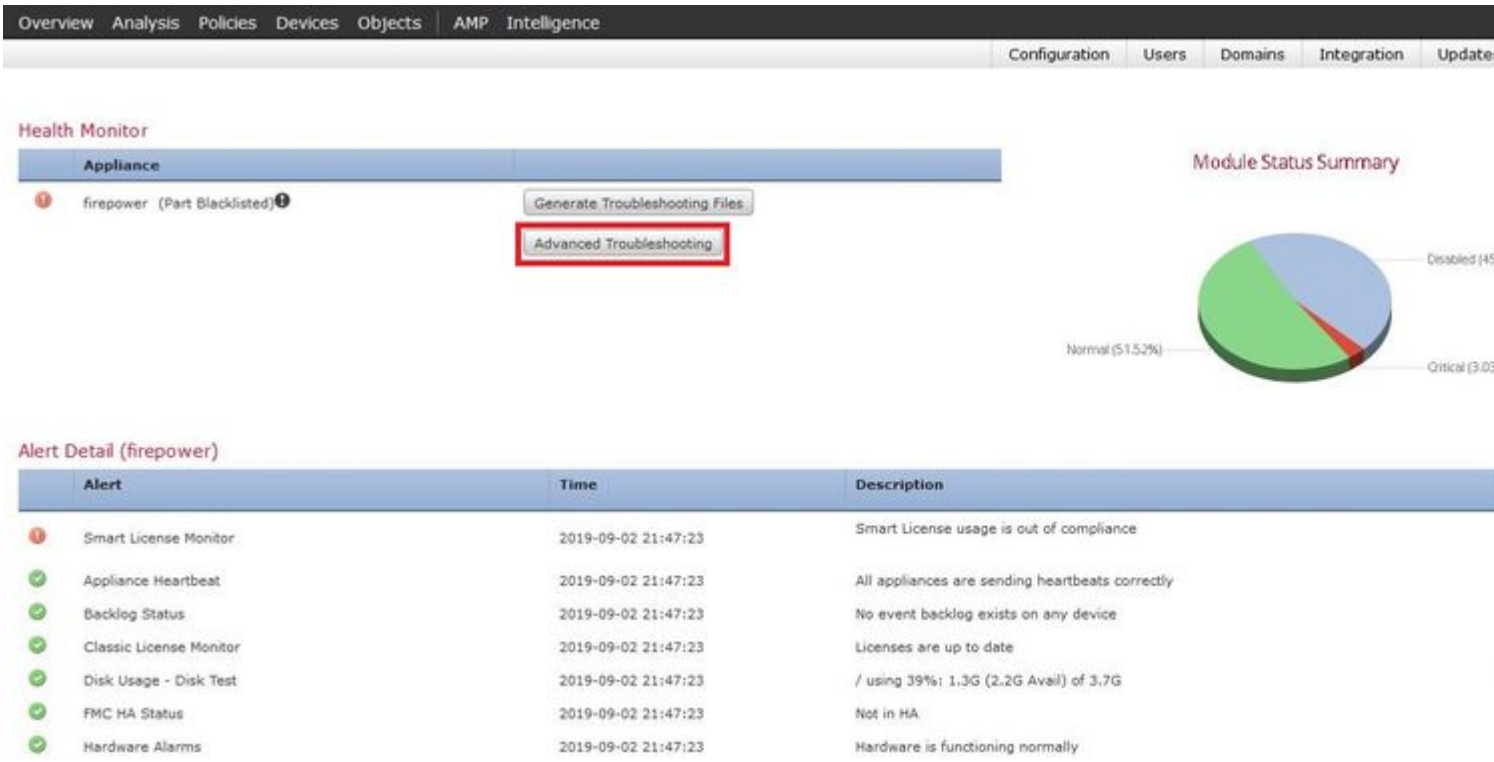
De bestanden die aanwezig zijn **/var/common** kunnen worden gedownload van de GUI.

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

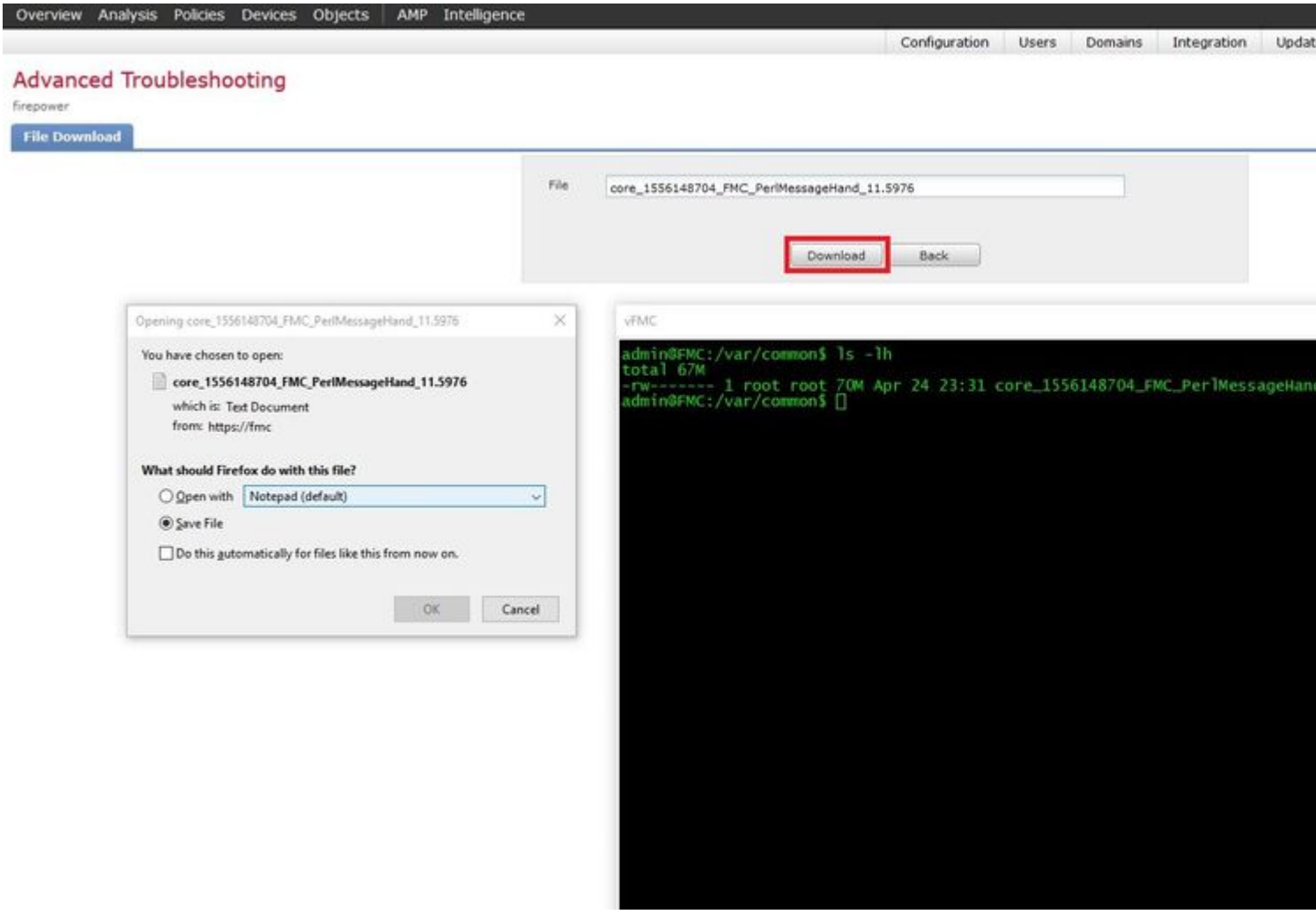
Stap 1. Navigeer naar **Systeem** > **Gezondheid** > **Monitor** en **klik** op de sensor van waaruit het bestand gedownload moet worden, zoals in de afbeelding:



Stap 2. Navigeer naar **Systeem > Gezondheid > Monitor** en **klik** op Geavanceerde probleemoplossing, zoals getoond in het beeld:



Stap 3. Voer de bestandsnaam in en **klik op** downloaden, zoals in de afbeelding:



Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.