

Foutberichten voor FMC- en FTD-upgrade oplossen

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrond](#)

[Foutberichten voor Firepower Management Center en Firepower Threat Defense upgrade](#)

[Communicatiefout](#)

[De FMC-HA-communicatie wordt gecompromitteerd](#)

[De communicatie tussen het VCC en het FTD wordt verstoord](#)

[Er is onvoldoende schijfruimte voor de upgrade van het apparaat](#)

[Opdrachten voor FTD-opdrachten voor probleemoplossing bij schijfgebruik](#)

[Databasecorruptie](#)

[Referenties](#)

Inleiding

In dit document worden de stappen beschreven voor het oplossen van problemen bij het upgraden van foutmeldingen op Firepower Management Center (FMC) en Firepower Threat Defence (FTD).

Voorwaarden

Vereisten

Cisco raadt aan kennis te hebben van de volgende onderwerpen

- Basiskennis van Linux shell.
- Firepower Management Center (FMC)
- Firepower Threat Defense (FTD)

Gebruikte componenten

- FMCv voor VMWare in versie 7.2.8.
- FTDv voor VMWare op versie 7.2.8.

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.

Achtergrond

Cisco genereert de corresponderende handleidingen om met de upgrade voor FirePOWER-apparaten te beginnen. Zelfs na het controleren van deze gids, kan de gebruiker om het even welk van deze scenario's onder ogen zien:

Foutberichten voor Firepower Management Center en Firepower Threat Defense upgrade

Communicatiefout

Dit bericht kan in de volgende scenario's worden weergegeven.

De FMC-HA-communicatie wordt gecompromitteerd

Dit gebeurt wanneer de communicatie tussen de FMC-HA mislukt. De klant kan deze opdrachten uitvoeren om de verbinding tussen de apparaten te controleren.

De volgende opdrachten moeten worden toegepast op het FMC-wortelniveau.

ping <peer-ip-adres>. Deze opdracht kan worden gebruikt om de bereikbaarheid tussen beide apparaten te controleren.

netstat -an | grep 8305. Deze opdracht geeft de apparaten weer die zijn aangesloten op poort 8305.



Opmerking: de poort 8305 is de standaardpoort die op de FirePOWER-apparaten is geconfigureerd om het communicatiekanaal met het VCC te creëren.

Om meer informatie te verkrijgen uit de FMC-HA gezondheidsstatus kan de gebruiker het script `troubleshoot_HADC.pl` uitvoeren

```
<#root>
```

```
> expert
```

```
admin@firepower:~$
```

```
sudo su
```

```
root@firepower:/Volume/home/admin#
```

```
ping xx.xx.18.102
```

```
PING xx.xx.18.102 (xx.xx.18.102) 56(84) bytes of data.  
64 bytes from xx.xx.18.102: icmp_seq=1 ttl=64 time=0.533 ms  
64 bytes from xx.xx.18.102: icmp_seq=2 ttl=64 time=0.563 ms  
64 bytes from xx.xx.18.102: icmp_seq=3 ttl=64 time=0.431 ms  
^C  
--- xx.xx.18.102 ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 59ms  
rtt min/avg/max/mdev = 0.431/0.509/0.563/0.056 ms
```

```
root@firepower:/Volume/home/admin#
```

```
netstat -an | grep 8305
```

```
tcp 0 0 xx.xx.18.101:8305 0.0.0.0:* LISTEN  
tcp 0 0 xx.xx.18.101:8305 xx.xx.18.253:48759 ESTABLISHED  
tcp 0 0 xx.xx.18.101:8305 xx.xx.18.254:53875 ESTABLISHED  
tcp 0 0 xx.xx.18.101:8305 xx.xx.18.254:49205 ESTABLISHED  
tcp 0 0 xx.xx.18.101:60871 xx.xx.18.253:8305 ESTABLISHE
```

```
root@firepower:/Volume/home/admin#
```

```
troubleshoot_HADC.pl
```

```
***** Troubleshooting Utility *****
```

- 1 Show HA Info Of FMC
- 2 Execute Sybase DBPing
- 3 Show Arbiter Status
- 4 Check Peer Connectivity
- 5 Print Messages of AQ Task
- 6 Show FMC HA Operations History (ASC order)
- 7 Dump To File: FMC HA Operations History (ASC order)
- 8 Last Successful Periodic Sync Time (When it completed)
- 9 Print HA Status Messages
- 10 Compare active and standby device list
- 11 Check manager status of standby missing devices
- 12 Check critical PM processes details
- 13 Get Remote Stale Sync AQ Info
- 14 Help
- 0 Exit

```
*****
```

```
Enter choice:
```

De communicatie tussen het VCC en het FTD wordt verstoord

Om de communicatie van de FTD naar het VCC te valideren, kan de klant deze opdrachten uitvoeren vanaf het niveau van de clish:

ping-systeem <fmc-IP> Om een ICMP-stroom te genereren uit de FTD-beheerinterface.

show managers Dit commando geeft de informatie van de managers waar het apparaat is geregistreerd.

sftunnel-status Deze opdracht valideert het communicatiekanaal dat tussen de apparaten is

ingesteld. Dit kanaal krijgt de naam sftunnel.

```
<#root>
```

```
>
```

```
ping system xx.xx.18.102
```

```
PING xx.xx.18.102 (xx.xx.18.102) 56(84) bytes of data.  
64 bytes from xx.xx.18.102: icmp_seq=1 ttl=64 time=0.595 ms  
64 bytes from xx.xx.18.102: icmp_seq=2 ttl=64 time=0.683 ms  
64 bytes from xx.xx.18.102: icmp_seq=3 ttl=64 time=0.642 ms  
64 bytes from xx.xx.18.102: icmp_seq=4 ttl=64 time=24.4 ms  
64 bytes from xx.xx.18.102: icmp_seq=5 ttl=64 time=11.4 ms  
^C  
--- xx.xx.18.102 ping statistics ---  
5 packets transmitted, 5 received, 0% packet loss, time 128ms  
rtt min/avg/max/mdev = 0.595/7.545/24.373/9.395 ms
```

```
> show managers
```

```
Type : Manager  
Host : xx.xx..18.101  
Display name : xx.xx..18.101  
Version : 7.2.8 (Build 25)  
Identifier : fc3e3572-xxxx-xxxx-xxxx-39e0098c166c  
Registration : Completed  
Management type : Configuration and analytics
```

```
Type : Manager  
Host : xx.xx..18.102  
Display name : xx.xx..18.102  
Version : 7.2.8 (Build 25)  
Identifier : bb333216-xxxx-xxxx-xxxx-c68c0c388b44  
Registration : Completed  
Management type : Configuration and analytics
```

```
> sftunnel-status
```

```
SFTUNNEL Start Time: Mon Oct 14 21:29:16 2024
```

```
Both IPv4 and IPv6 connectivity is supported  
Broadcast count = 5  
Reserved SSL connections: 0  
Management Interfaces: 2  
eth0 (control events) xx.xx..18.254,  
tap_nlp (control events) 169.254.1.2,fd00:0:0:1::2
```

```
*****
```

```
**RUN STATUS**xx.xx..18.102*****
```

```
Key File = /var/sf/peers/bb333216-xxxx-xxxx-xxxx-c68c0c388b44/sftunnel-key.pem  
Cert File = /var/sf/peers/bb333216-xxxx-xxxx-xxxx-c68c0c388b44/sftunnel-cert.pem  
CA Cert = /var/sf/peers/bb333216-xxxx-xxxx-xxxx-c68c0c388b44/cacert.pem  
Cipher used = TLS_AES_256_GCM_SHA384 (strength:256 bits)  
ChannelA Connected: Yes, Interface eth0
```

Cipher used = TLS_AES_256_GCM_SHA384 (strength:256 bits)
ChannelB Connected: Yes, Interface eth0
Registration: Completed.
IPv4 Connection to peer 'xx.xx..18.102' Start Time: Tue Oct 15 00:38:43 2024 UTC
IPv4 Last outbound connection to peer 'xx.xx..18.102' via Primary ip/host 'xx.xx..18.102'

PEER INFO:

sw_version 7.2.8
sw_build 25
Using light registration
Management Interfaces: 1
eth0 (control events) xx.xx..18.102,
Peer channel Channel-A is valid type (CONTROL), using 'eth0', connected to 'xx.xx..18.102' via 'xx.xx..18.102'
Peer channel Channel-B is valid type (EVENT), using 'eth0', connected to 'xx.xx..18.102' via 'xx.xx..18.102'

RUN STATUSxx.xx..18.101*****

Key File = /var/sf/peers/fc3e3572-xxxx-xxxx-xxxx-39e0098c166c/sftunnel-key.pem
Cert File = /var/sf/peers/fc3e3572-xxxx-xxxx-xxxx-39e0098c166c/sftunnel-cert.pem
CA Cert = /var/sf/peers/fc3e3572-xxxx-xxxx-xxxx-39e0098c166c/cacert.pem
Cipher used = TLS_AES_256_GCM_SHA384 (strength:256 bits)
ChannelA Connected: Yes, Interface eth0
Cipher used = TLS_AES_256_GCM_SHA384 (strength:256 bits)
ChannelB Connected: Yes, Interface eth0
Registration: Completed.
IPv4 Connection to peer 'xx.xx..18.101' Start Time: Mon Oct 14 21:29:15 2024 UTC
IPv4 Last outbound connection to peer 'xx.xx..18.101' via Primary ip/host 'xx.xx..18.101'

PEER INFO:

sw_version 7.2.8
sw_build 25
Using light registration
Management Interfaces: 1
eth0 (control events) xx.xx..18.101,
Peer channel Channel-A is valid type (CONTROL), using 'eth0', connected to 'xx.xx..18.101' via 'xx.xx..18.101'
Peer channel Channel-B is valid type (EVENT), using 'eth0', connected to 'xx.xx..18.101' via 'xx.xx..18.101'

RPC STATUSxx.xx..18.102*****

'uuid' => 'bb333216-xxxx-xxxx-xxxx-c68c0c388b44',
'uuid_gw' => '',
'last_changed' => 'Wed Oct 9 07:00:11 2024',
'active' => 1,
'name' => 'xx.xx..18.102',
'ip' => 'xx.xx..18.102',
'ipv6' => 'IPv6 is not configured for management'

RPC STATUSxx.xx..18.101*****

'uuid_gw' => '',
'uuid' => 'fc3e3572-xxxx-xxxx-xxxx-39e0098c166c',
'last_changed' => 'Mon Jun 10 18:59:54 2024',
'active' => 1,
'ip' => 'xx.xx..18.101',
'ipv6' => 'IPv6 is not configured for management',
'name' => 'xx.xx..18.101'

Check routes:

No peers to check

/ngfw/var:Performance Statistics	1.325 GB	217.177 MB	1.485 GB
/ngfw/var:Other Events	0 KB	434.354 MB	868.710 MB
/ngfw/var:IP Reputation & URL Filtering	0 KB	542.943 MB	1.060 GB
/ngfw/var:arch_debug_file	0 KB	2.121 GB	12.725 GB
/ngfw/var:Archives & Cores & File Logs	0 KB	868.710 MB	8.483 GB
/ngfw/var:RNA Events	0 KB	868.710 MB	1.485 GB
/ngfw/var:Unified Low Priority Events	2.185 GB	1.060 GB	5.302 GB
/ngfw/var:File Capture	0 KB	2.121 GB	4.242 GB
/ngfw/var:Unified High Priority Events	0 KB	3.181 GB	7.423 GB
/ngfw/var:IPS Events	292 KB	2.545 GB	6.363 GB

>

system support silo-drain

Available Silos

- 1 - Temporary Files
- 2 - Action Queue Results
- 3 - User Identity Events
- 4 - UI Caches
- 5 - Backups
- 6 - Updates
- 7 - Other Detection Engine
- 8 - Performance Statistics
- 9 - Other Events
- 10 - IP Reputation & URL Filtering
- 11 - arch_debug_file
- 12 - Archives & Cores & File Logs
- 13 - RNA Events
- 14 - Unified Low Priority Events
- 15 - File Capture
- 16 - Unified High Priority Events
- 17 - IPS Events
- 0 - Cancel and return

Select a Silo to drain:

Databasecorruptie

Dit bericht wordt meestal weergegeven nadat de gereedheidscontrole van het updatepakket is uitgevoerd. Het wordt het meest waargenomen in het VCC.

Wanneer deze fout in het VCC wordt weergegeven, vergeet dan niet om de bestanden voor probleemoplossing te genereren vanuit het VCC.

Dit stelt de TAC engineer in staat om te beginnen met het logboekonderzoek, te bepalen wat het probleem is en sneller een actieplan te leveren.

<#root>

FMC Database error

Fatal error: Database integrity check failed. Error running script 000_start/110_DB_integrity_check.sh.

Referenties

[Cisco Firepower Threat Defense Upgrade Guide voor Firepower Management Center.](#)

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.