

Problemen oplossen met Firepower 1010

Continu opnieuw opstarten (opstartlus) met meerdere AnyConnect-images na software-upgrade

Inhoud

uitgifte

Na de software-upgrade start Firepower 1010 continu opnieuw op (ook wel de opstartlus genoemd).

De terminalsessie toont de foutberichten "mmap64: Cannot allocate memory" en de afsluitberichten van Firepower eXtensible Operating System (FXOS):

```
mmap64: Cannot allocate memory
mmap64: Cannot allocate memory
mmap64: Cannot allocate memory
mmap64: Cannot allocate memory
Rebooting ... (status 0x9)
```

```
Jun 24 08:25:48 root: FXOS shutdown log started: pid = 39475 cmdline = /bin/sh/sbin/fxos log_shutdown #
Jun 24 08:25:49 root: FXOS shutdown log completed: pid = 39475
The system is going down for reboot NOW!
```

milieu

- Door FMC beheerde standalone Firepower 1010
- Voor het eerst gezien na de software-upgrade van versie 7.4.2 naar 7.6.4. Ook andere versies kunnen worden beïnvloed
- Op de firewall is het virtuele privénetwerk voor externe toegang (RAVPN) geconfigureerd

met meerdere AnyConnect/Secure Client-images

resolutie

Permanente resolutie vereist software-upgrade naar de versie met de oplossing van Cisco bug ID [CSCwc82675](#).

Als tijdelijke oplossing moet u het aantal AnyConnect/Secure Client-images verminderen om te voorkomen dat de firewall continu opnieuw wordt opgestart.

Deze stappen worden geverifieerd op een standalone firewall:

1. Controleer of het systeem in de faalveilige modus staat. De faalveilige modus voor de FTD/ASA-toepassing op Firepower 1000/2100 of Secure Firewall 3100 wordt geactiveerd vanwege de continue opstartlus, traceback, enzovoort. Als de firewall 7 keer opnieuw wordt opgestart binnen 7200 (verhoogd van 3600 seconden met de oplossing van Cisco-bug-ID [CSCwj91341](#)) seconden, wordt de firewall in de faalveilige modus gezet en stopt de reboot. Wanneer het systeem in de faalveilige modus staat:

- De systeemnaam wordt toegevoegd aan de mislukte tekenreeks:

```
<#root>
```

```
firepower-1010
```

```
-failed
```

```
/ssa #
```

- De uitvoer van de opdracht show failsafe-params in de FXOS local-mgmt command shell bevat een waarschuwingsbericht:

```
<#root>
```

```
firepower-1010-failed(local-mgmt)#
```

```
show failsafe-params
```

```
Max Restart: 1
```

Current Reboot Count: 1
Restart Time Interval(secs): 3600

WARNING: System in Failsafe mode. Applications are not running!

2. Als het systeem zich niet in de faalveilige modus bevindt, kunt u de activering van de faalveilige modus versnellen door Max Restart in te stellen op Current Reboot Count + 1:

<#root>

firepower-1010#

connect local-mgmt

firepower(local-mgmt)#

show failsafe-params

Max Restart: 7

Current Reboot Count: 2

Restart Time Interval(secs): 3600

firepower-1010(local-mgmt)#

config failsafe-max-restart

0 shall Disable Failsafe Mode!!!
Set a max_restart (0-8) value Or [x] to exit:

3

System may come up in Normal state post Reboot.

Configuration Successful

```
firepower-1010(local-mgmt)#
```

```
show failsafe-params
```

Max Restart:

3

Current Reboot Count:

2

Restart Time Interval(secs): 3600

3. Bij de volgende herstart komt de firewall in de faalveilige modus. Raadpleeg stap 1 voor verificatie.

4. Wanneer de firewall wordt opgestart, komt deze in de faalveilige modus. Meld u aan bij de firewall, maak verbinding met de firewall via de opdracht ftd verbinden en de switch met de expertmodus zodra de aanmeldingsprompt verschijnt:

```
<#root>
```

```
firepower-1010#
```

```
connect ftd
```

```
> expert
```

```
firepower-1010:/$
```

5. Controleer in de modus Expert de AnyConnect/Secure Client-images in de opstartconfiguratie:

```
<#root>
```

```
firepower-1010:/$
```

```
grep "anyconnect image" /mnt/disk0/.private/startup-config
anyconnect image disk0:/csm/cisco-secure-client-linux64-5.1.8.122-webdeploy-k9.pkg 1 regex "Linux"
anyconnect image disk0:/csm/cisco-secure-client-macos-5.1.8.122-webdeploy-k9.pkg 2 regex "Mac OS"
anyconnect image disk0:/csm/cisco-secure-client-win-5.1.8.122-webdeploy-k9.pkg 3 regex "Windows"
```

6. Kopieer het bestand /mnt/disk0/.private/startup-config naar de map /ngfw/var/common. Deze stap is belangrijk:

```
<#root>
```

```
firepower-1010:~$
```

```
cp /mnt/disk0/.private/startup-config /ngfw/var/common/
```

```
firepower-1010:~$
```

```
ls -l /ngfw/var/common/
```

```
total 12
```

```
...
```

```
-rwxr-xr-x 1 admin admin 11305 Jun 25 09:20
```

```
startup-config
```

7. Bepaal welke afbeeldingen kunnen worden verwijderd.

8. Verwijder de regels met afbeeldingen uit stap 5 totdat er maximaal 2 afbeeldingen zijn. Gebruik vim of verwijder regels met de sed-opdracht als volgt:

```
<#root>
```

```
firepower-1010:/$
```

```
grep "anyconnect image" /mnt/disk0/.private/startup-config
```

```
anyconnect image disk0:/csm/cisco-secure-client-linux64-5.1.8.122-webdeploy-k9.pkg 1 regex "Linux"
```

```
anyconnect image disk0:/csm/cisco-secure-client-macos-5.1.8.122-webdeploy-k9.pkg 2 regex "Mac OS"
```

```
anyconnect image disk0:/csm/cisco-secure-client-win-5.1.8.122-webdeploy-k9.pkg 3 regex "Windows"
```

```
firepower-1010:/$#
```

```
sudo sed -i '\#anyconnect image disk0:/csm/cisco-secure-client-macos-5.1.8.122-webdeploy-k9.pkg 2 regex
```

9. Bevestig dat de regel wordt verwijderd:

```
<#root>
```

```
firepower-1010:/$
```

```
grep "anyconnect image" /mnt/disk0/.private/startup-config
```

```
anyconnect image disk0:/csm/cisco-secure-client-linux64-5.1.8.122-webdeploy-k9.pkg 1 regex "Linux"  
anyconnect image disk0:/csm/cisco-secure-client-win-5.1.8.122-webdeploy-k9.pkg 3 regex "Windows"
```

10. Keer terug naar de FXOS local-mgmt shell en keer de fail-safe parameters terug naar de oorspronkelijke waarden van stap 1, indien gewijzigd. Sluit vervolgens de faalveilige modus af en start de firewall opnieuw op:

```
<#root>
```

```
firepower-1010:/$
```

```
exit
```

```
>
```

```
exit
```

```
firepower-1010#
```

```
connect local-mgmt
```

```
firepower-1010(local-mgmt)#
```

```
config failsafe-max-restart
```

```
0 shall Disable Failsafe Mode!!!  
Set a max_restart (0-8) value Or [x] to exit:
```

System may come up in Normal state post Reboot.
Configuration Successful

firepower-1010-failed(local-mgmt)#

show failsafe-params

Max Restart: 7

Current Reboot Count: 1

Restart Time Interval(secs): 3600

firepower-1010-failed(local-mgmt)#

failsafe-exit

System may reboot? (y/n)

y

Reset Successful

firepower-1010-failed(local-mgmt)#

exit

firepower-1010-failed#

scope chassis

KSEC-FPR1010-2 /chassis* #

reboot no-prompt

Broadcast message from root@KSEC-FPR1010-2 (Thu Jun 24 15:59:22 2026):
All shells being terminated due to system /sbin/reboot

11. Controleer de sessielogboeken. Het verwachte gedrag is dat de firewall na het opnieuw opstarten niet meer continu opnieuw opstart.

12. Als de firewall niet meer continu opnieuw wordt opgestart, wacht u tot de firewall online is. Verwijder vervolgens dezelfde AnyConnect/Secure Client-images uit stap 8 van de FMC/FDM UI en implementeer het beleid. Anders worden de images opnieuw toegepast bij de volgende beleidsimplementatie.

13. Zorg ervoor dat u de software naar de versie bijwerkt met de oplossing van Cisco bug ID [CSCwc82675](#).

14. Nadat de software is geüpgraded naar de versie met de oplossing van Cisco-bug-ID [CSCwc82675](#), voegt u de AnyConnect/Secure Client-images toe die bij stap 12 zijn verwijderd en implementeert u het beleid.

Oorzaak

Meerdere AnyConnect/Secure Client-images leiden tot een verhoogd geheugengebruik op Firepower 1010 vanwege de beperkte hoeveelheid geheugen die beschikbaar is voor het gegevensvlak (Lina-engine). Vanwege de beperkte hoeveelheid geheugen kan het systeem het Lina-motorgeheugen uitputten, wat meestal resulteert in het opnieuw opstarten van Lina en het invoeren van een continue heropstartlus. In sommige gevallen kunnen verschillende Lina-processen ook een traceback activeren en kernbestanden genereren.

Dit probleem wordt bijgehouden in Cisco bug ID [CSCwc82675](#). Bovendien vermeldt het hoofdstuk Remote Access VPN in de apparaatconfiguratiegids van het Firewall Management Center: "Het gebruik van meerdere Secure Client-pakketten op apparaten voor dreigingsverdediging kan het geheugengebruik verhogen en de prestaties van het apparaat beïnvloeden. We raden u aan niet meerdere Secure Client-pakketten te gebruiken op low-end dreigingsverdedigingsapparaten om continue herstart te voorkomen vanwege geheugenuitputting."

Raadpleeg voor meer informatie Cisco bug ID [CSCwj59682](#) en Cisco bug ID [CSCwm72469](#).

Gerelateerde inhoud

- Cisco bug ID [CSCwm47108](#)
- Cisco bug ID [CSCwc82675](#)
- Cisco bug ID [CSCwm72469](#)
- Cisco bug ID [CSCwj59682](#)
- Cisco bug ID [CSCwj91341](#)
- [Cisco FXOS-handleiding voor probleemoplossing voor de firewallbeveiliging](#)

- [Hoofdstuk: Remote Access VPN](#)

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.