

Risoluzione dei problemi di Firepower 1010 Riavvio continuo (loop di avvio) con più immagini AnyConnect dopo l'aggiornamento del software

Sommario

Problema

Dopo l'aggiornamento del software, Firepower 1010 si riavvia continuamente (noto anche come loop di avvio).

La sessione terminale mostra il messaggio "mmap64: Cannot allocate memory" (Impossibile allocare memoria) e i messaggi di errore Firepower eXtensible Operating System (FXOS) e di arresto:

```
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!
```

Ambiente

- Firepower 1010 standalone gestito da FMC
- Visualizzato per la prima volta dopo l'aggiornamento del software dalla versione 7.4.2 alla 7.6.4. Il problema può riguardare anche altre versioni

- Sul firewall, la VPN (Virtual Private Network) ad accesso remoto è configurata con più immagini AnyConnect/Secure Client

Risoluzione

La risoluzione permanente richiede l'aggiornamento del software alla versione con la correzione dell'ID bug Cisco [CSCwc82675](#).

Per ovviare al problema, ridurre il numero di immagini AnyConnect/Secure Client per impedire il riavvio continuo del firewall.

Questi passaggi vengono verificati su un firewall autonomo:

1. Verificare se il sistema è in modalità di sicurezza in caso di errore. La modalità fail-safe per l'applicazione FTD/ASA su Firepower 1000/2100 o Secure Firewall 3100 è attivata a causa di loop di avvio continuo, traceback e così via. Se il firewall si riavvia 7 volte entro 7200 (con un aumento da 3600 secondi con la correzione dell'ID bug Cisco [CSCwj91341](#)) secondi, il firewall entra in modalità di sicurezza e il riavvio si arresta. Quando il sistema è in modalità fail-safe:

- Al nome del sistema viene aggiunta la stringa non riuscito:

```
<#root>
```

```
firepower-1010
```

```
-failed
```

```
/ssa #
```

- L'output del comando show failsafe-params nella shell del comando FXOS local-mgmt contiene un messaggio di avviso:

```
<#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. Se il sistema non è in modalità provvisoria, è possibile accelerare l'attivazione della modalità provvisoria impostando Max Restart su 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. Al successivo riavvio, il firewall entra in modalità di protezione da errori. Fare riferimento al punto 1 per la verifica.

4. All'avvio, il firewall entra in modalità di sicurezza. Non appena viene visualizzato il prompt di accesso, accedere al firewall, connettersi al firewall utilizzando il comando `connect ftd` e passare alla modalità Expert:

```
<#root>
```

```
firepower-1010#
```

```
connect ftd
```

```
> expert
```

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

5. In modalità Expert, controllare le immagini AnyConnect/Secure Client nella configurazione di avvio:

```
<#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. Copiare il file /mnt/disk0/.private/startup-config nella directory /ngfw/var/common. Questa operazione è importante:

```
<#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. Decidere quali immagini possono essere eliminate.

8. Eliminare le linee con immagini dal punto 5 fino a un massimo di 2 immagini. Utilizzare vim o, in alternativa, eliminare le righe utilizzando il comando sed come indicato di seguito:

```
<#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. Confermare l'eliminazione della riga:

```
<#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. Tornare alla shell FXOS local-mgmt e ripristinare i parametri fail-safe ai valori originali del passaggio 1, se modificati. Uscire quindi dalla modalità provvisoria e riavviare il firewall:

```
<#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. Monitorare i registri della sessione. Il comportamento previsto è che dopo il riavvio, il firewall non si riavvia più continuamente.

12. Se il firewall non si riavvia più continuamente, attendere che sia online, quindi accertarsi di eliminare le stesse immagini AnyConnect/Secure Client dal passaggio 8 dall'interfaccia utente di FMC/FDM e distribuire i criteri. In caso contrario, le immagini verranno riapplicate durante la successiva distribuzione dei criteri.

13. Aggiornare il software alla versione corretta con l'ID bug Cisco [CSCwc82675](#).

14. Dopo aver aggiornato il software alla versione con la correzione dell'ID bug Cisco [CSCwc82675](#), aggiungere le immagini AnyConnect/Secure Client eliminate al passaggio 12 e distribuire i criteri.

Causa

Più immagini AnyConnect/Secure Client determinano un elevato utilizzo della memoria su Firepower 1010 a causa della quantità limitata di memoria disponibile per il piano dati (motore Lina). A causa della quantità limitata di memoria, il sistema può esaurire la memoria del motore Lina, il che di solito comporta il riavvio e l'avvio di un loop di riavvio continuo. In alcuni casi, diversi processi Lina possono anche attivare un traceback e generare file di base.

Questo problema viene rilevato nell'ID bug Cisco [CSCwc82675](#). Inoltre, il capitolo sulla VPN ad accesso remoto nella Guida alla configurazione dei dispositivi di Centro gestione firewall indica che l'utilizzo di più pacchetti Secure Client sui dispositivi di difesa dalle minacce può aumentare l'utilizzo della memoria e influire sulle prestazioni del dispositivo. È consigliabile non utilizzare più pacchetti Secure Client su dispositivi di difesa dalle minacce di basso livello per evitare il riavvio continuo a causa dell'esaurimento della memoria. "

Per ulteriori informazioni, fare riferimento all'ID bug Cisco [CSCwj59682](#) e all'ID bug Cisco [CSCwm72469](#).

Contenuto correlato

- ID bug Cisco [CSCwm47108](#)
- ID bug Cisco [CSCwc82675](#)
- ID bug Cisco [CSCwm72469](#)
- ID bug Cisco [CSCwj59682](#)
- ID bug Cisco [CSCwj91341](#)
- [Guida alla risoluzione dei problemi di Cisco FXOS per la difesa dalle minacce del firewall](#)
- [Capitolo: VPN ad accesso remoto](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).