

Dépannage de Firepower 1010 ; Continuous Reboot (Boot Loop) avec plusieurs images AnyConnect après la mise à niveau logicielle

Table des matières

Problème

Après la mise à niveau logicielle, Firepower 1010 redémarre en permanence (également appelé boucle de démarrage).

La session de terminal affiche le « mmap64: Les messages d'erreur « Cannot allocate memory » et les messages d'arrêt de 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!
```

Environnement

- Firepower 1010 autonome géré par FMC
- Vue pour la première fois après la mise à niveau du logiciel de la version 7.4.2 à la version 7.6.4. D'autres versions peuvent également être affectées
- Sur le pare-feu, le réseau privé virtuel à accès distant (RAVPN) est configuré avec plusieurs images AnyConnect/Secure Client

Résolution

La résolution permanente nécessite une mise à niveau logicielle vers la version avec le correctif de l'ID de bogue Cisco [CSCwc82675](#).

Pour contourner ce problème, réduisez le nombre d'images AnyConnect/Secure Client pour empêcher le pare-feu de redémarrer en continu.

Les étapes suivantes sont vérifiées sur un pare-feu autonome :

1. Vérifiez si le système est en mode de sécurité intégrée. Le mode de sécurité intégrée pour l'application FTD/ASA sur Firepower 1000/2100 ou Secure Firewall 3100 est activé en raison d'une boucle de démarrage continue, du retraçage, etc. Si le pare-feu redémarre 7 fois dans les 7200 (augmenté de 3600 secondes avec le correctif de l'ID de bogue Cisco [CSCwj91341](#)) secondes, le pare-feu passe en mode de sécurité intégrée et le redémarrage s'arrête. Lorsque le système est en mode de sécurité intégrée :

- Le nom du système est ajouté à la chaîne -failed :

```
<#root>
```

```
firepower-1010
```

```
-failed
```

```
/ssa #
```

- Le résultat de la commande show failsafe-params dans l'interpréteur de commandes FXOS local-mgmt contient un message d'avertissement :

```
<#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. Si le système n'est pas en mode de sécurité intégrée, vous pouvez accélérer l'activation du mode de sécurité intégrée en définissant Max Restart sur 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. Au prochain redémarrage, le pare-feu passe en mode de sécurité intégrée. Reportez-vous à l'étape 1 pour la vérification.

4. Lorsque le pare-feu démarre, il passe en mode de sécurité intégrée. Dès que l'invite de connexion apparaît, connectez-vous au pare-feu, connectez-vous au pare-feu à l'aide de la commande `connect ftd` et passez en mode expert :

<#root>

firepower-1010#

connect ftd

> expert

firepower-1010:/\$

5. En mode expert, vérifiez les images AnyConnect/Secure Client dans la configuration initiale :

<#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. Copiez le fichier /mnt/disk0/.private/startup-config dans le répertoire /ngfw/var/common. Cette étape est 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. Déterminez quelles images peuvent être supprimées.

8. Supprimez les lignes contenant des images de l'étape 5 jusqu'à ce qu'il y ait un maximum de 2 images. Utilisez vim ou supprimez des lignes à l'aide de la commande sed comme suit :

```
<#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. Confirmez que la ligne est supprimée :

```
<#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. Revenez à l'interpréteur de commandes FXOS local-mgmt et restaurez les paramètres de sécurité intégrée aux valeurs d'origine de l'étape 1, si elles ont été modifiées. Quittez ensuite le mode à sécurité intégrée et redémarrez le pare-feu :

```
<#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:
```

```
7
```

```
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. Surveillez les journaux de session. Le comportement attendu est qu'après le redémarrage, le pare-feu ne redémarre plus continuellement.

12. Si le pare-feu ne redémarre plus en continu, attendez qu'il soit en ligne, puis assurez-vous de supprimer les mêmes images AnyConnect/Secure Client de l'étape 8 de l'interface utilisateur FMC/FDM et déployez des stratégies. Sinon, les images sont réappliquées lors du prochain déploiement de stratégie.

13. Assurez-vous de mettre à niveau le logiciel vers la version avec le correctif de l'ID de bogue Cisco [CSCwc82675](#).

14. Après la mise à niveau logicielle vers la version avec le correctif de l'ID de bogue Cisco [CSCwc82675](#), ajoutez les images AnyConnect/Secure Client supprimées à l'étape 12 et déployez

les stratégies.

Motif

Plusieurs images AnyConnect/Secure Client entraînent une utilisation élevée de la mémoire sur Firepower 1010 en raison de la quantité limitée de mémoire disponible pour le plan de données (moteur Lina). En raison de la quantité limitée de mémoire, le système peut épuiser la mémoire du moteur Lina, ce qui entraîne généralement le redémarrage de Lina et l'entrée d'une boucle de redémarrage continue. Dans certains cas, différents processus Lina peuvent également déclencher un traceback et générer des fichiers de base.

Ce problème est suivi dans l'ID de bogue Cisco [CSCwc82675](#). En outre, le chapitre VPN d'accès à distance dans le Guide de configuration du périphérique du Centre de gestion des pare-feu mentionne « L'utilisation de plusieurs packages de client sécurisé sur des périphériques de défense contre les menaces peut augmenter l'utilisation de la mémoire et affecter les performances du périphérique. Nous vous recommandons de ne pas utiliser plusieurs packages Secure Client sur des périphériques de défense contre les menaces de bas de gamme pour éviter des redémarrages continus en raison d'un manque de mémoire. »

Pour plus d'informations, référez-vous à l'ID de bogue Cisco [CSCwj59682](#) et à l'ID de bogue Cisco [CSCwm72469](#).

Autres informations utiles

- ID de bogue Cisco [CSCwm47108](#)
- ID de bogue Cisco [CSCwc82675](#)
- ID de bogue Cisco [CSCwm72469](#)
- ID de bogue Cisco [CSCwj59682](#)
- ID de bogue Cisco [CSCwj91341](#)
- [Guide de dépannage de Cisco FXOS pour la défense pare-feu](#)
- [Chapitre : VPN d'accès à distance](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.