

# Solución de problemas de Firepower 1010 Reinicio continuo (bucle de inicio) con varias imágenes de AnyConnect después de la actualización del software

## Contenido

---

## Problema

Después de la actualización del software, Firepower 1010 se reinicia continuamente (también conocido como bucle de inicio).

La sesión de terminal muestra el "mmap64: Mensajes de error "No se puede asignar memoria" y mensajes de apagado del sistema operativo extensible (FXOS) de Firepower:

```
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!
```

## Entorno

- Firepower 1010 independiente gestionado por FMC
- Visto por primera vez después de la actualización de software de la versión 7.4.2 a la 7.6.4. Otras versiones también pueden verse afectadas
- En el firewall, la red privada virtual de acceso remoto (RAVPN) se configura con varias

## Resolución

La resolución permanente requiere la actualización de software a la versión con la corrección del Id. de error de Cisco [CSCwc82675](#).

Como solución alternativa, reduzca el número de imágenes de AnyConnect/Secure Client para evitar que el firewall se reinicie continuamente.

Estos pasos se verifican en un firewall independiente:

1. Compruebe si el sistema está en modo de seguridad contra fallos. El modo de seguridad contra fallos para la aplicación FTD/ASA en Firepower 1000/2100 o Secure Firewall 3100 se activa debido a un bucle de arranque continuo, seguimiento posterior, etc. Si el firewall se reinicia 7 veces dentro de 7200 (aumentado de 3600 segundos con la corrección del error de Cisco ID [CSCwj91341](#))seconds, el firewall ingresa en el modo de seguridad contra fallos y se detiene el reinicio. Cuando el sistema está en modo de seguridad contra fallos:

- El nombre del sistema se anexa con la cadena -failed:

```
<#root>
```

```
firepower-1010
```

```
-failed
```

```
/ssa #
```

- El resultado del comando show failsafe-params en el shell de comandos local-mgmt de FXOS contiene un mensaje de advertencia:

```
<#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 el sistema no está en el modo de seguridad contra fallos, puede acelerar la activación del modo de seguridad contra fallos estableciendo Max Restart en 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. En el siguiente reinicio, el firewall entra en el modo de seguridad contra fallos. Consulte el paso 1 para realizar la verificación.

4. Cuando el firewall se inicia, entra en el modo de seguridad contra fallos. Tan pronto como aparezca el mensaje de inicio de sesión, inicie sesión en el firewall, conéctese al firewall usando el comando `connect ftd` y cambie al modo experto:

```
<#root>
```

```
firepower-1010#
```

```
connect ftd
```

```
> expert
```

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

5. En el modo experto, verifique las imágenes de AnyConnect/Secure Client en la configuración de inicio:

```
<#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. Copie el archivo /mnt/disk0/.private/startup-config en el directorio /ngfw/var/common. Este paso es 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. Decida qué imágenes se pueden eliminar.

8. Elimine las líneas con imágenes del paso 5 hasta que haya un máximo de 2 imágenes. Utilice vim o, alternativamente, elimine líneas usando el comando sed de la siguiente manera:

```
<#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. Confirme que se suprime la línea:

```
<#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. Vuelva al shell de administración local de FXOS y revierta los parámetros de seguridad contra fallos a los valores originales del paso 1, si se modifican. A continuación, salga del modo de seguridad contra fallos y reinicie el 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. Supervise los registros de sesión. El comportamiento esperado es que después del reinicio, el firewall ya no se reinicia continuamente.

12. Si el firewall ya no se reinicia de forma continua, espere hasta que esté online y asegúrese de eliminar las mismas imágenes de AnyConnect/Secure Client del paso 8 de la interfaz de usuario de FMC/FDM e implementar políticas. De lo contrario, las imágenes se vuelven a aplicar durante la siguiente implementación de políticas.

13. Asegúrese de actualizar el software a la versión con la corrección del Id. de error de Cisco [CSCwc82675](#).

14. Después de actualizar el software a la versión con la corrección del Id. de error de Cisco [CSCwc82675](#), agregue las imágenes de AnyConnect/Secure Client eliminadas en el paso 12 e implemente políticas.

## Causa

El uso de varias imágenes de AnyConnect/Secure Client aumenta el uso de memoria en Firepower 1010 debido a la cantidad limitada de memoria disponible para el plano de datos (motor de línea). Debido a la cantidad limitada de memoria, el sistema puede agotar la memoria del motor Lina, lo que suele dar lugar a que Lina se reinicie y entre en un bucle de reinicio continuo. En algunos casos, diferentes procesos de Lina también pueden activar un seguimiento y generar archivos de núcleo.

Este problema se rastrea en el Id. de error de Cisco [CSCwc82675](#). Además, el capítulo VPN de acceso remoto de la Guía de configuración de dispositivos de Firewall Management Center menciona "El uso de varios paquetes Secure Client en dispositivos de defensa contra amenazas puede aumentar el uso de memoria y afectar el rendimiento del dispositivo. Se recomienda no utilizar varios paquetes de Secure Client en dispositivos de defensa contra amenazas de gama baja para evitar los reinicios continuos debido al agotamiento de la memoria. "

Para obtener más información, refiérase al ID de bug de Cisco [CSCwj59682](#) y al ID de bug de Cisco [CSCwm72469](#).

## Contenido relacionado

- ID de bug de Cisco [CSCwm47108](#)
- ID de bug de Cisco [CSCwc82675](#)
- ID de bug de Cisco [CSCwm72469](#)
- ID de bug de Cisco [CSCwj59682](#)
- ID de bug de Cisco [CSCwj91341](#)

- [Guía de solución de problemas de Cisco FXOS para Firewall Threat Defence](#)
- [Capítulo: VPN de acceso remoto](#)

#### Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).