

Fehlerbehebung bei Firepower 1010 Continuous Reboot (Boot-Schleife) mit mehreren AnyConnect-Images nach dem Software-Upgrade

Inhalt

Problem

Nach dem Software-Upgrade startet die Firepower 1010 kontinuierlich neu (auch als Boot-Loop bekannt).

Die Terminalsitzung zeigt die "mmap64: Fehlermeldungen "Memory" und die FirePOWER eXtensible Operating System (FXOS)-Abschaltmeldungen können nicht zugewiesen werden:

```
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!
```

Umwelt

- FMC-verwaltete Standalone-FirePOWER 1010
- Erstmals nach dem Software-Upgrade von Version 7.4.2 auf 7.6.4 sichtbar. Andere Versionen können ebenfalls betroffen sein.
- Auf der Firewall wird das RAVPN (Virtual Private Network) für den Remote-Zugriff mit

mehreren AnyConnect/Secure Client-Images konfiguriert.

Auflösung

Für eine dauerhafte Behebung ist ein Software-Upgrade auf die Version mit der Cisco Bug-ID [CSCwc82675](#) erforderlich.

Als Problemumgehung sollten Sie die Anzahl der AnyConnect/Secure Client-Images reduzieren, um einen kontinuierlichen Neustart der Firewall zu verhindern.

Diese Schritte werden mit einer Standalone-Firewall verifiziert:

1. Überprüfen Sie, ob sich das System im ausfallsicheren Modus befindet. Der Fail-Safe-Modus für die FTD/ASA-Anwendung auf Firepower 1000/2100 oder Secure Firewall 3100 wird durch einen kontinuierlichen Boot-Loop, Traceback usw. aktiviert. Wenn die Firewall innerhalb von 7.200 Sekunden 7 Mal neu startet (mit der Fehlerbehebung Cisco Bug-ID [CSCwj91341](#) von 3.600 Sekunden erhöht), wechselt die Firewall in den ausfallsicheren Modus und der Neustart wird gestoppt. Wenn sich das System im ausfallsicheren Modus befindet:

- Der Systemname wird mit der Zeichenfolge -failed angehängt:

```
<#root>
```

```
firepower-1010
```

```
-failed
```

```
/ssa #
```

- Die Ausgabe des Befehls show failure-safe-params in der FXOS-Befehlszeile local-mgmt enthält eine Warnmeldung:

```
<#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. Wenn sich das System nicht im ausfallsicheren Modus befindet, können Sie die Aktivierung des ausfallsicheren Modus beschleunigen, indem Sie "Max Restart" auf "Current Reboot Count + 1" (Aktuelle Neustartzahl + 1) einstellen:

<#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. Beim nächsten Neustart wechselt die Firewall in den ausfallsicheren Modus. Überprüfen Sie dies anhand von Schritt 1.

4. Wenn die Firewall bootet, wechselt sie in den ausfallsicheren Modus. Sobald die Anmeldeaufforderung angezeigt wird, melden Sie sich bei der Firewall an, stellen mit dem Befehl `connect ftd` eine Verbindung zur Firewall her und wechseln in den Expertenmodus:

```
<#root>
```

```
firepower-1010#
```

```
connect ftd
```

```
> expert
```

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

5. Aktivieren Sie im Expertenmodus AnyConnect/Secure Client-Images in der Startkonfiguration:

```
<#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. Kopieren Sie die Datei /mnt/disk0/.private/startup-config in das Verzeichnis /ngfw/var/common.
Dieser Schritt ist wichtig:

```
<#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. Entscheiden Sie, welche Bilder gelöscht werden können.

8. Löschen Sie die Zeilen mit Bildern aus Schritt 5, bis maximal 2 Bilder vorhanden sind.
Verwenden Sie vim, oder löschen Sie Zeilen mit dem Befehl sed wie folgt:

```
<#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. Bestätigen Sie, dass die Zeile gelöscht wird:

```
<#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. Kehren Sie zur FXOS-Shell für lokale Verwaltung zurück, und setzen Sie die ausfallsicheren Parameter, falls geändert, auf die ursprünglichen Werte aus Schritt 1 zurück. Beenden Sie dann den ausfallsicheren Modus, und starten Sie die Firewall neu:

```
<#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. Überwachung der Sitzungsprotokolle Es wird erwartet, dass die Firewall nach dem Neustart nicht mehr kontinuierlich neu startet.

12. Wenn die Firewall nicht mehr kontinuierlich neu startet, warten Sie, bis die Firewall online ist, und löschen Sie die gleichen AnyConnect/Secure Client-Images aus Schritt 8 aus der FMC/FDM-Benutzeroberfläche, und stellen Sie Richtlinien bereit. Andernfalls werden die Images bei der nächsten Richtlinienbereitstellung erneut angewendet.

13. Stellen Sie sicher, dass Sie die Software auf die Version mit der Cisco Bug-ID [CSCwc82675](#) aktualisieren.

14. Fügen Sie nach dem Software-Upgrade auf die Version mit der Behebung des Cisco Bugs [CSCwc82675](#) die in Schritt 12 gelöschten AnyConnect/Secure Client-Images hinzu, und stellen Sie Richtlinien bereit.

Ursache

Mehrere AnyConnect/Secure Client-Images führen zu einer erhöhten Speichernutzung bei Firepower 1010, da nur wenig Speicher für die Datenebene (Lina-Engine) zur Verfügung steht. Aufgrund der begrenzten Speicherkapazität kann das System den Speicher des Lina-Motors aufbrauchen, was in der Regel dazu führt, dass Lina neu startet und in eine fortlaufende Neustart-Schleife eintritt. In einigen Fällen können verschiedene Lina-Prozesse auch ein Traceback auslösen und Core-Dateien generieren.

Dieses Problem wird in der Cisco Bug-ID [CSCwc82675](#) verfolgt. Außerdem wird im Kapitel Remote Access VPN im Firewall Management Center Device Configuration Guide erwähnt: "Die Verwendung mehrerer Secure Client-Pakete auf Threat Defense-Geräten kann die Speichernutzung erhöhen und die Leistung des Geräts beeinträchtigen. Wir empfehlen, dass Sie nicht mehrere Secure Client-Pakete auf einfachen Abwehrgeräten verwenden, um einen kontinuierlichen Neustart aufgrund von Speichererschöpfung zu vermeiden. "

Weitere Informationen finden Sie unter Cisco Bug-ID [CSCwj59682](#) und Cisco Bug-ID [CSCwm72469](#).

Verwandte Inhalte

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

- [Cisco FXOS - Leitfaden zur Fehlerbehebung für die Firewall-Bedrohungsabwehr](#)
- [Kapitel: Remote Access-VPN](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.