

ソフトウェアアップグレード後に複数のAnyConnectイメージを使用してFirepower 1010の連続リブート（ブートループ）を行う

内容

問題

ソフトウェアのアップグレード後、Firepower 1010は連続的にリブートします（ブートループとも呼ばれます）。

ターミナルセッションで「mmap64: Cannot allocate memory」エラーメッセージとFirepower eXtensible Operating System(FXOS)のシャットダウンメッセージが表示されます。

```
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!
```

環境

- FMCマネージド型スタンドアロンFirepower 1010
- 最初に見られるのは、バージョン7.4.2から7.6.4へのソフトウェアアップグレード後です。他のバージョンも影響を受ける可能性があります
- ファイアウォールでは、リモートアクセス仮想プライベートネットワーク(RAVPN)が複数

のAnyConnect/Secure Clientイメージで設定されます

解決方法

永続的な解決には、Cisco Bug ID [CSCwc82675](#)の修正によるバージョンへのソフトウェアアップグレードが必要です。

回避策として、AnyConnect/Secure Clientイメージの数を減らして、ファイアウォールがリブートし続けないようにします。

次の手順は、スタンドアロンファイアウォールで確認されます。

1. システムがフェールセーフモードかどうかを確認します。Firepower 1000/2100またはセキュアファイアウォール3100上のFTD/ASAアプリケーションのフェールセーフモードは、連続ブートループ、トレースバックなどが原因でアクティブになります。7200秒以内に (Cisco Bug ID CSCwj91341の修正により3600秒から増加して) ファイアウォールが7回リブートした場合、ファイアウォールはフェールセーフモードになり、リブートが停止します。システムがフェールセーフモードの場合：

- システム名には、-failedという文字列が追加されます。

```
<#root>
```

```
firepower-1010
```

```
-failed
```

```
/ssa #
```

- FXOS local-mgmtコマンドシエルのshow failsafe-paramsコマンドの出力には、警告メッセージが含まれています。

```
<#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. システムがフェールセーフモードでない場合は、Max RestartをCurrent Reboot Count + 1に設定して、フェールセーフモードのアクティブ化を加速できます。

<#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. 次のリブート時に、ファイアウォールはフェールセーフモードに入ります。検証については、ステップ1を参照してください。

4. ファイアウォールが起動すると、フェールセーフモードに入ります。ログインプロンプトが表示されたら、すぐにファイアウォールにログインし、connect ftdコマンドを使用してファイアウォールに接続し、expertモードに切り替えます。

```
<#root>
```

```
firepower-1010#
```

```
connect ftd
```

```
> expert
```

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

5. エキスパートモードで、スタートアップコンフィギュレーションのAnyConnect/セキュアクライアントイメージを確認します。

```
<#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. ファイル/mnt/disk0/.private/startup-configをディレクトリ/ngfw/var/commonにコピーします。
この手順は重要です。

<#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. 削除できるイメージを決定します。

8. イメージがある行をステップ5から削除し、イメージの最大数を2にします。vimを使用するか、またはsedコマンドを使用して次のように行を削除します。

<#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. 品目が削除されたことを確認します。

```
<#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. FXOS local-mgmtシェルに戻り、フェールセーフパラメータを変更した場合はステップ1の値に戻します。次にフェールセーフモードを終了し、ファイアウォールをリブートします。

```
<#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. セッション・ログを監視します。正常な動作は、リブート後にファイアウォールが連続してリブートしないことです。

12. ファイアウォールが継続的にリブートしなくなった場合は、ファイアウォールがオンラインになるまで待ち、ステップ8で同じAnyConnect/Secure ClientイメージをFMC/FDM UIから削除し、ポリシーを展開します。それ以外の場合、イメージは次のポリシー導入時に再適用されます。

13. Cisco Bug ID [CSCwc82675](#)の修正を使用して、ソフトウェアをバージョンにアップグレードしてください。

14. Cisco Bug ID [CSCwc82675](#)の修正でバージョンをソフトウェアアップグレードした後、ステップ12で削除したAnyConnect/Secure Clientイメージを追加して、ポリシーを展開します。

原因

複数のAnyConnect/Secure Clientイメージを使用すると、データプレーン (Linaエンジン) で使用できるメモリ量が制限されるため、Firepower 1010のメモリ使用量が増加します。 メモリの量が限られているため、システムはLinaエンジンメモリを使い果たすことがあり、通常はLinaが再起動して連続リブートループに入ります。場合によっては、異なるLinaプロセスがトレースバックをトリガーし、コアファイルを生成することもあります。

この問題は、Cisco Bug ID [CSCwc82675](#)で追跡されています。さらに、『Firewall Management Center Device Configuration Guide』の「Remote Access VPN」の章にある「Using multiple Secure Client package on threat defense devices can increase memory usage and affect the performance of the device.」ローエンドの脅威対策デバイスで複数のSecure Clientパッケージを使用して、メモリ不足による連続的なリブートを回避することをお勧めします。

詳細については、Cisco Bug ID [CSCwj59682](#)およびCisco Bug ID [CSCwm72469](#)を参照してください。

関連コンテンツ

- Cisco Bug ID CSCwm47108
- Cisco Bug ID CSCwc82675
- Cisco Bug ID CSCwm72469
- Cisco Bug ID CSCwj59682
- Cisco Bug ID CSCwj91341
- [ファイアウォールの脅威対策に関するCisco FXOSトラブルシューティングガイド](#)
- [第1章：リモートアクセスVPN](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。