

소프트웨어 업그레이드 후 여러 AnyConnect 이미지를 사용하여 Firepower 1010 문제 해결 (&N);연속 재부팅(부팅 루프)

목차

문제

소프트웨어 업그레이드 후, Firepower(1010)는 지속적으로 재부팅됩니다(부트 루프라고도 함).

터미널 세션에는 "mmap64: 메모리를 할당할 수 없습니다." 오류 메시지 및 Firepower FXOS(eXtensible Operating System) 종료 메시지:

```
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!
```

환경

- FMC 관리 독립형 Firepower 1010
- 버전 7.4.2에서 7.6.4로 소프트웨어를 업그레이드한 후 처음 확인됨. 다른 버전도 영향을 받을 수 있음
- 방화벽에서 RAVPN(Remote Access Virtual Private Network)이 여러 AnyConnect/Secure Client 이미지로 구성됩니다

해결

영구 확인을 위해서는 Cisco 버그 ID CSCwc82675가 수정된 버전으로 소프트웨어를 [업그레이드해야 합니다](#).

이를 해결하려면 AnyConnect/Secure Client 이미지 수를 줄여 방화벽이 지속적으로 재부팅되지 않도록 합니다.

이 단계는 독립형 방화벽에서 검증됩니다.

1. 시스템이 안전(fail-safe) 모드인지 확인합니다. firepower 1000/2100 또는 Secure Firewall 3100의 FTD/ASA 애플리케이션에 대한 Fail-Safe 모드는 지속적인 부팅 루프, 역추적 등으로 인해 활성화됩니다. Cisco 버그 ID CSCwj91341을 수정하여 7200초 이내에 방화벽이 7번 재부팅되면 (3600초에서 증가)방화벽은 유사 시 안전 모드로 전환되고 재부팅이 중지됩니다. 시스템이 안전 (fail-safe) 모드에 있는 경우:

- 시스템 이름에 실패한 문자열이 추가됩니다.

```
<#root>
```

```
firepower-1010
```

```
-failed
```

```
/ssa #
```

- FXOS local-mgmt 명령 셸에서 show failsafe-params 명령의 출력에는 다음과 같은 경고 메시지가 포함됩니다.

```
<#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. 시스템이 안전 실패 모드가 아닐 경우 최대 재시작을 현재 재부팅 수 + 1로 설정하여 안전 실패 모드를 신속하게 활성화할 수 있습니다.

```
<#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. 다음 재부팅 시 방화벽이 유사 시 안전 모드로 들어갑니다. 확인은 1단계를 참조하십시오.

4. 방화벽이 부팅될 때 오류 방지 모드로 들어갑니다. 로그인 프롬프트가 나타나면 방화벽에 로그인하고 `connect ftd` 명령을 사용하여 방화벽에 연결한 다음 expert 모드로 전환합니다.

<#root>

firepower-1010#

connect ftd

> expert

firepower-1010:/\$

5. expert 모드의 시작 컨피그레이션에서 AnyConnect/Secure Client 이미지를 확인합니다.

<#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. /mnt/disk0/.private/startup-config 파일을 /ngfw/var/common 디렉토리에 복사합니다. 이 단계는 중요합니다.

```
<#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. 삭제할 이미지를 결정합니다.

8. 5단계에서 최대 2개의 이미지가 나타날 때까지 이미지가 있는 줄을 삭제합니다. vim을 사용하거나, 다음과 같이 sed 명령을 사용하여 줄을 삭제합니다.

```
<#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. 라인이 삭제되었는지 확인합니다.

<#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 셸로 돌아가 1단계의 원래 값으로 유사 시 대기 매개변수를 되돌립니다(변경된 경우). 그런 다음 Fail-Safe 모드를 종료하고 방화벽을 재부팅합니다.

<#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. 세션 로그를 모니터링합니다. 예상된 동작은 재부팅 후 방화벽이 더 이상 계속 재부팅되지 않는 것입니다.

12. 방화벽이 더 이상 계속 재부팅되지 않는 경우 방화벽이 온라인 상태가 될 때까지 기다린 다음 FMC/FDM UI에서 8단계에서 동일한 AnyConnect/Secure Client 이미지를 삭제하고 정책을 배포합니다. 그렇지 않으면 다음 정책 구축 중에 이미지가 다시 적용됩니다.

13. Cisco 버그 ID CSCwc82675를 수정하여 소프트웨어를 해당 버전으로 [업그레이드해야 합니다](#).

14. Cisco 버그 ID CSCwc82675를 수정하여 소프트웨어 버전으로 업그레이드한 후 12단계에서 삭제된 AnyConnect/Secure Client 이미지를 추가하고 정책을 구축합니다.

원인

데이터 플레인(Lina 엔진)에 사용할 수 있는 메모리 양이 제한되어 있기 때문에 여러 AnyConnect/Secure Client 이미지가 Firepower 1010의 메모리 사용량을 높입니다. 제한된 메모리 양으로 인해 시스템은 Lina 엔진 메모리를 소진할 수 있으며, 이로 인해 대개 Lina가 다시 시작되고 연속 리부팅 루프가 시작됩니다. 경우에 따라 서로 다른 Lina 프로세스가 역추적을 트리거하여 코어 파일을 생성할 수도 있습니다.

이 문제는 Cisco 버그 ID CSCwc82675에서 추적됩니다. 또한 Firewall Management Center Device Configuration Guide의 Remote Access VPN 장에서 "Using multiple Secure Client packages on threat defense devices can make memory usage and impact the performance of the device"에 대해 설명합니다. 메모리 소진으로 인한 지속적인 재부팅을 방지하기 위해 로우엔드 위협 방어 디바이스에서 여러 Secure Client 패키지를 사용하지 않는 것이 좋습니다. "

자세한 내용은 Cisco 버그 ID CSCwj59682 및 Cisco 버그 ID CSCwm72469 [를 참조하십시오](#).

관련 콘텐츠

- Cisco 버그 ID [CSCwm47108](#)
- Cisco 버그 ID [CSCwc82675](#)
- Cisco 버그 ID [CSCwm72469](#)
- Cisco 버그 ID [CSCwj59682](#)
- Cisco 버그 ID [CSCwj91341](#)
- [방화벽 위협 방어를 위한 Cisco FXOS 트러블슈팅 가이드](#)
- [장: 원격 액세스 VPN](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.