

Solucionar problemas de reinicialização contínua do Firepower 1010 (loop de inicialização) com várias imagens do AnyConnect após a atualização do software

Contents

Problema

Após a atualização do software, o Firepower 1010 é reiniciado continuamente (também conhecido como loop de inicialização).

A sessão de terminal mostra o "mmap64: Mensagens de erro "Não é possível alocar memória" e mensagens de desligamento do 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!
```

Ambiente

- Firepower 1010 autônomo gerenciado pelo FMC
- Visto pela primeira vez após a atualização do software da versão 7.4.2 para 7.6.4. Outras versões também podem ser afetadas
- No firewall, a rede virtual privada (RAVPN) de acesso remoto é configurada com várias

Resolução

A resolução permanente requer atualização de software para a versão com a correção do bug da Cisco ID [CSCwc82675](#).

Como solução alternativa, reduza o número de imagens do AnyConnect/Secure Client para impedir a reinicialização contínua do firewall.

Estas etapas são verificadas em um firewall autônomo:

1. Verifique se o sistema está no modo de segurança contra falhas. O modo à prova de falhas para o aplicativo FTD/ASA no Firepower 1000/2100 ou no Secure Firewall 3100 é ativado devido ao loop de inicialização contínuo, ao retorno de rastreamento e assim por diante. Se o firewall for reinicializado 7 vezes dentro de 7200 (aumentado de 3600 segundos com a correção do bug da Cisco ID [CSCwj91341](#)) segundos, ele entrará no modo de segurança contra falhas e a reinicialização será interrompida. Quando o sistema estiver no modo de segurança contra falhas:

- O nome do sistema é anexado à sequência de caracteres -failed:

```
<#root>
```

```
firepower-1010
```

```
-failed
```

```
/ssa #
```

- A saída do comando show failsafe-params no shell de comando FXOS local-mgmt contém uma mensagem de aviso:

```
<#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. Se o sistema não estiver no modo de segurança contra falhas, você poderá acelerar a ativação do modo de segurança contra falhas definindo Reinicialização Máxima como Contagem de Reinicialização Atual + 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. Na próxima reinicialização, o firewall entra no modo de segurança contra falhas. Consulte a etapa 1 para obter a verificação.

4. Quando o firewall inicializa, ele entra no modo de segurança contra falhas. Assim que o prompt de login for exibido, efetue login no firewall, conecte-se ao firewall usando o comando `connect ftd` e alterne para o modo especialista:

```
<#root>
```

```
firepower-1010#
```

```
connect ftd
```

```
> expert
```

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

5. No modo especialista, verifique as imagens do AnyConnect/Secure Client na configuração de inicialização:

```
<#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 o arquivo /mnt/disk0/.private/startup-config para o diretório /ngfw/var/common. Esta etapa é 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 quais imagens podem ser excluídas.

8. Exclua as linhas com imagens da etapa 5 até que haja um máximo de 2 imagens. Use vim ou, como alternativa, exclua linhas usando o comando sed da seguinte maneira:

```
<#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 se a linha foi deletada:

```
<#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. Retorne ao shell FXOS local-mgmt e reverta os parâmetros à prova de falhas para os valores originais a partir da etapa 1, se alterado. Em seguida, saia do modo de segurança contra falhas e reinicialize o 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. Monitore os logs de sessão. O comportamento esperado é que após a reinicialização, o firewall não reinicialize mais continuamente.

12. Se o firewall não for mais reinicializado continuamente, aguarde até que ele esteja on-line, assegure-se de excluir as mesmas imagens do AnyConnect/Secure Client da etapa 8 da interface do usuário do FMC/FDM e implante as políticas. Caso contrário, as imagens serão reaplicadas durante a próxima implantação da política.

13. Certifique-se de atualizar o software para a versão com a correção do bug da Cisco ID [CSCwc82675](#).

14. Após a atualização do software para a versão com a correção do bug da Cisco ID [CSCwc82675](#), adicione as imagens do AnyConnect/Secure Client excluídas na etapa 12 e implante as políticas.

Causa

Várias imagens do AnyConnect/Secure Client resultam em uso elevado de memória no Firepower 1010 devido à quantidade limitada de memória disponível para o plano de dados (mecanismo Lina). Devido à quantidade limitada de memória, o sistema pode esgotar a memória do mecanismo Lina, o que geralmente resulta na reinicialização de Lina e em um loop de reinicialização contínuo. Em alguns casos, diferentes processos do Lina também podem acionar um traceback e gerar arquivos de núcleo.

Esse problema é rastreado na ID de bug da Cisco [CSCwc82675](#). Além disso, o capítulo sobre VPN de acesso remoto no Guia de Configuração de Dispositivos do Centro de Gerenciamento de Firewall menciona "Usar vários pacotes de Cliente Seguro em dispositivos de defesa contra ameaças pode aumentar o uso de memória e afetar o desempenho do dispositivo. Recomendamos que você não use vários pacotes do Secure Client em dispositivos de defesa contra ameaças low-end para evitar reinicializações contínuas devido ao esgotamento de memória. "

Para obter mais informações, consulte o bug da Cisco ID [CSCwj59682](#) e o bug da Cisco ID [CSCwm72469](#).

Conteúdo relacionado

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

- [Guia de solução de problemas do Cisco FXOS para Firewall Threat Defense](#)
- [Capítulo: VPN de acesso remoto](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.