Falha na interface de gerenciamento FTD após atualização de 7.4.3 para 7.6.4

Contents

Problema

Após atualizar um par de HA (High Availability, alta disponibilidade) do Cisco Secure Firewall 3130 de 7.4.3 para 7.6.4, a unidade primária parecia falhar com 99% de conclusão no FMC (Firewall Management Center) e não respondeu. A unidade secundária foi atualizada com êxito e se tornou ativa no par HA. A unidade primária não estava respondendo às conexões SSH e o FMC não pôde se comunicar com ela.

Após a investigação, esta falha crítica foi observada no FXOS:

```
Critical  F1000398 2026-08-14T20:52:06.297     58437 [FSM:FAILED]: out-of-band interface configuration(
```

Os registros de atualização do FTD mostraram que a atualização foi realmente concluída com êxito (100% concluída), mas o serviço SFTunnel não estava sendo iniciado corretamente, impedindo a comunicação entre o FTD e o FMC. O dispositivo pode fazer ping em si mesmo, em seu gateway e na unidade FTD correspondente, mas não pode acessar os FMCs que residem em sub-redes diferentes.

Ambiente

- Par Cisco Secure Firewall 3130 Threat Defense HA
- Versão original do software: FTD 7.4.3
- Versão do software de destino: FTD 7.6.4 (Build 69)
- Sistema operacional extensível Cisco Firepower (FX-OS) v2.16.1 (build 147)

- Interface de gerenciamento configurada com endereçamento IP estático
- Servidores FMC localizados em sub-redes diferentes da rede de gerenciamento do FTD

Resolução

O problema foi resolvido com a reconfiguração completa da interface de gerenciamento na unidade de FTD afetada. Estas etapas foram executadas:

Passo 1: Conecte-se ao FTD através do acesso de console, já que o SSH não estava funcionando.

Passo 2: Verifique o status de conclusão da atualização verificando os logs de atualização:

```
root@device:/ngfw/var/log/sf/Cisco_FTD_SSP_FP3K_Upgrade-7.6.4# cat status.log
```

Passo 3: Confirme a falha da interface de gerenciamento em FXOS:

```
device# show fault
```

Passo 4: Tente solucionar o problema básico reconfigurando o endereço IP de gerenciamento (isso não resolveu o problema).

Passo 5: Execute uma reinicialização a frio (isso não resolveu o problema).

Passo 6: Desative completamente a interface management0 da CLI do FTD:

```
configure network management-interface disable management0
```

Passo 7: Reative a interface management0:

```
configure network management-interface enable management0
```

Passo 8: Redefina as configurações de rede para a interface de gerenciamento:

```
configure network ipv4 manual <ip_address> <netmask> <gateway>
```

Etapa 9: Verifique se os alertas FXOS foram eliminados e se o FTD agora pode efetuar ping no FMC:

```
root@device:/# ping <FMC_IP_address>
```

Etapa 10: Reinicie o serviço SFTunnel usando o script manage_procs.pl:

```
manage_procs.pl restart sftunnel
```

Etapa 11: Verifique a conectividade do túnel SFT:

```
root@device:/# sftunnel_status.pl
```

Etapa 12: Testar a funcionalidade de failover para garantir que as operações de HA estejam funcionando corretamente.

Após concluir essas etapas, o FTD conseguiu se comunicar corretamente com o FMC, e todos os testes de conectividade e failover foram bem-sucedidos. A atualização do hotfix pode ser aplicada sem problemas.

Causa

A causa raiz foi uma falha da interface de gerenciamento ao inicializar corretamente após a atualização do FTD de 7.4.3 para 7.6.4, apesar da conclusão bem-sucedida do processo de atualização. A FSM (máquina de estado finito) de configuração da interface de gerenciamento fora de banda falhou durante o processo de atualização, impedindo que a interface de gerenciamento estabeleça conectividade apropriada. Esse comportamento foi documentado no bug da Cisco ID CSCww08417.

Esse problema é semelhante aos defeitos reportados anteriormente no bug da Cisco ID CSCwj04154 e no bug da Cisco ID CSCwa69303, mas ocorre sob condições diferentes. A falha da interface de gerenciamento criou uma falsa impressão de falha de atualização com 99% de conclusão, quando, na realidade, a atualização foi concluída com êxito, mas a conectividade de gerenciamento foi interrompida.

Conteúdo relacionado

- ID de bug Cisco CSCww08417 - A interface de gerenciamento FTD pode falhar ao iniciar após a atualização
- Guia de compatibilidade da Threat Defense do Cisco Secure Firewall
- Suporte técnico e downloads da Cisco

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.