Entender as Etapas e o Impacto do Procedimento de Upgrade de Alta Disponibilidade do FTD

Contents

Problema

Um administrador de firewall precisa entender o procedimento de atualização recomendado para dispositivos FTD (Firewall Threat Defense) configurados em um par HA (High Availability, alta disponibilidade) e gerenciados pelo Cisco Firewall Management Center (FMC). As perguntas específicas incluem qual é o processo recomendado para atualizações de software nessas unidades, se as atualizações podem ser executadas "sem interrupções" e qual impacto esperar durante o processo de atualização.

Ambiente

- FTD executando a versão 7.4. Outras versões de software também podem ser afetadas.
- FTD configurado no modo de par de Alta Disponibilidade (HA).
- FMC 7.4 — Gestão do FTD HA. Outras versões de software também podem ser afetadas.

Resolução

O procedimento de atualização do FTD na configuração HA usa uma sequência específica para minimizar o tempo de inatividade e manter a integridade do sistema.

Pedido de atualização recomendado

Etapa 1. Atualizar o FMC primeiro

A orientação da Cisco exige que o FMC execute a mesma versão ou uma versão mais recente do que os dispositivos que ele gerencia. Você não pode atualizar um dispositivo FTD após o FMC para uma versão principal ou de manutenção mais recente.

Etapa 2. Atualizar o par FTD HA do FMC

Ao atualizar um par FTD HA gerido pelo FMC, o FMC atualiza um ponto por vez (em espera primeiro, depois ativo) e ocorre uma falha como parte do processo.

Expectativas de tempo de inatividade e impacto do tráfego

- Você deve planejar uma janela de manutenção. A Cisco observa que as atualizações podem incluir interrupções no fluxo e na inspeção do tráfego, e os dispositivos podem parar de transmitir tráfego durante a atualização ou se uma atualização falhar.
- Com um par HA, o objetivo é minimizar o impacto, mas você precisa esperar pelo menos um evento de failover e uma possível breve interrupção (por exemplo, adjacência de roteamento ou renegociação de VPN, dependendo do seu ambiente).
- Evite alterações de política e configuração durante a atualização (nenhuma implantação ou alteração até que ambos os membros do HA sejam totalmente atualizados e estáveis).

Verificações de Integridade de Pré-Atualização para FTD HA

Antes de iniciar a atualização, confirme se o HA do FTD está estável e se ambas as unidades concordam nos estados Ativo e Pronto para espera:

<#root>

```
device#

show failover state


               State          Last Failure Reason      Date/Time
This host  -   Primary
```

```
Active

None
Other host -   Secondary


Standby Ready

  Comm Failure             16:10:34 UTC Apr 13 2026

====Configuration State===
        Sync Skipped
====Communication State===
        Mac set
```

Causa

Trata-se de um inquérito processual relativo às melhores práticas para a atualização dos sistemas FMC e FTD na configuração HA. A pergunta aborda a necessidade de entender a sequência de atualização apropriada, as expectativas de tempo de inatividade e as estratégias de mitigação de impacto para infraestruturas críticas de firewall.

Conteúdo relacionado

- Planejamento de atualização do Secure Firewall Management Center
- Atualização do FTD HA Gerenciado pelo FMC
- Guia de compatibilidade do Management Center
- Guia de compatibilidade da Threat Defense
- 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.