Atualizar o fluxo de trabalho HA FTD gerenciado pelo FMC executando a versão 7.4.2

Problema

O principal problema abordado é o fluxo de trabalho e os requisitos técnicos para executar uma atualização de alta disponibilidade (HA) em dispositivos Cisco Firepower Threat Defense (FTD) (especificamente FPR1120) gerenciados por um Firepower Management Center (FMC) 4700 executando a versão 7.4.2. Este artigo detalha as etapas preparatórias, as melhores práticas e as considerações para garantir uma operação de atualização de HA FTD bem-sucedida.

Ambiente

- Tecnologia: Cisco Secure Firewall Firepower - 7.4
- Subtecnologia: Firepower Threat Defense (FTD) - Atualização de software / Atualização de segurança / Recriação / Migração / Backup e restauração
- Linha de produtos: FPRLOW (inclui FPR1120)
- Firepower Threat Defense (FTD) em par de alta disponibilidade (HA)
- Gerenciado pelo Firepower Management Center (FMC) 4700
- Versão do software FMC: 7.4.2
- Atividade de atualização planejada programada dentro de uma janela de manutenção definida

Resolução

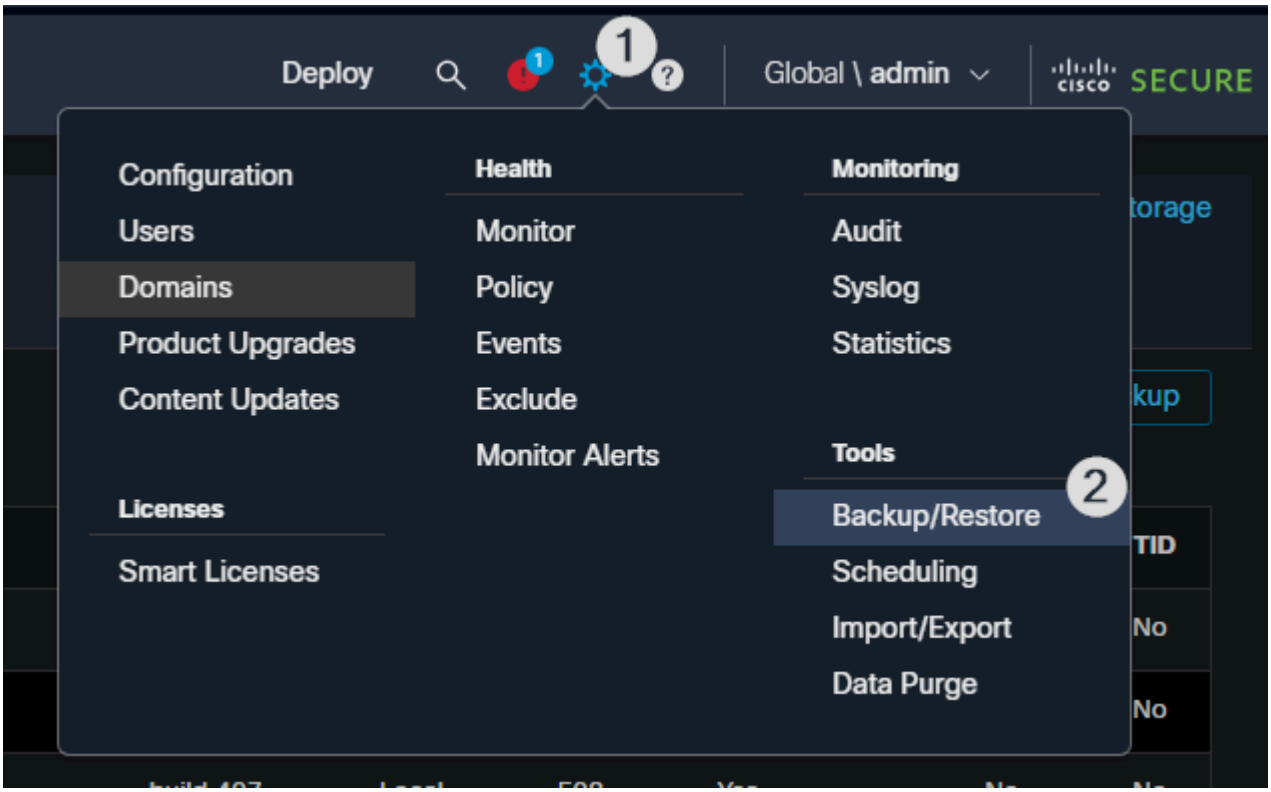
Aderir a este fluxo de trabalho detalhado para garantir uma atualização bem-sucedida dos pares HA do FTD gerenciados pelo FMC:

Etapa 1: Preparar-se para a atualização

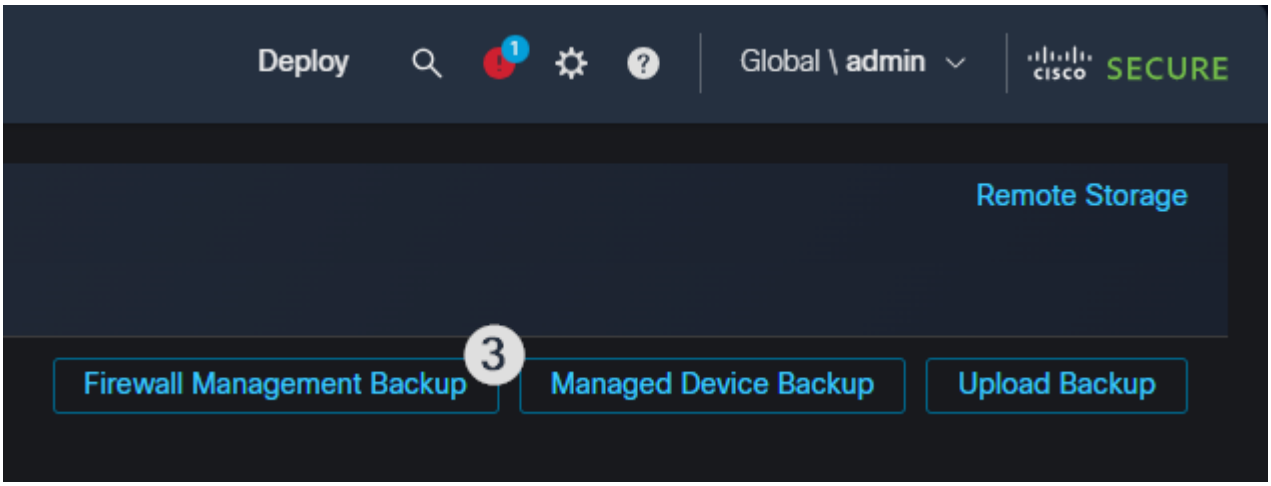
Antes de iniciar o processo de atualização, é essencial gerar e armazenar backups de

configuração dos dispositivos HA do FTD e do FMC. Isso garante que as configurações possam ser restauradas em caso de falha de atualização ou problema inesperado.

Para fazer backup da configuração do FMC: navegue até System > Tools: Backup/Restore na interface do usuário do FMC e clique no botão Firewall Management Backup:



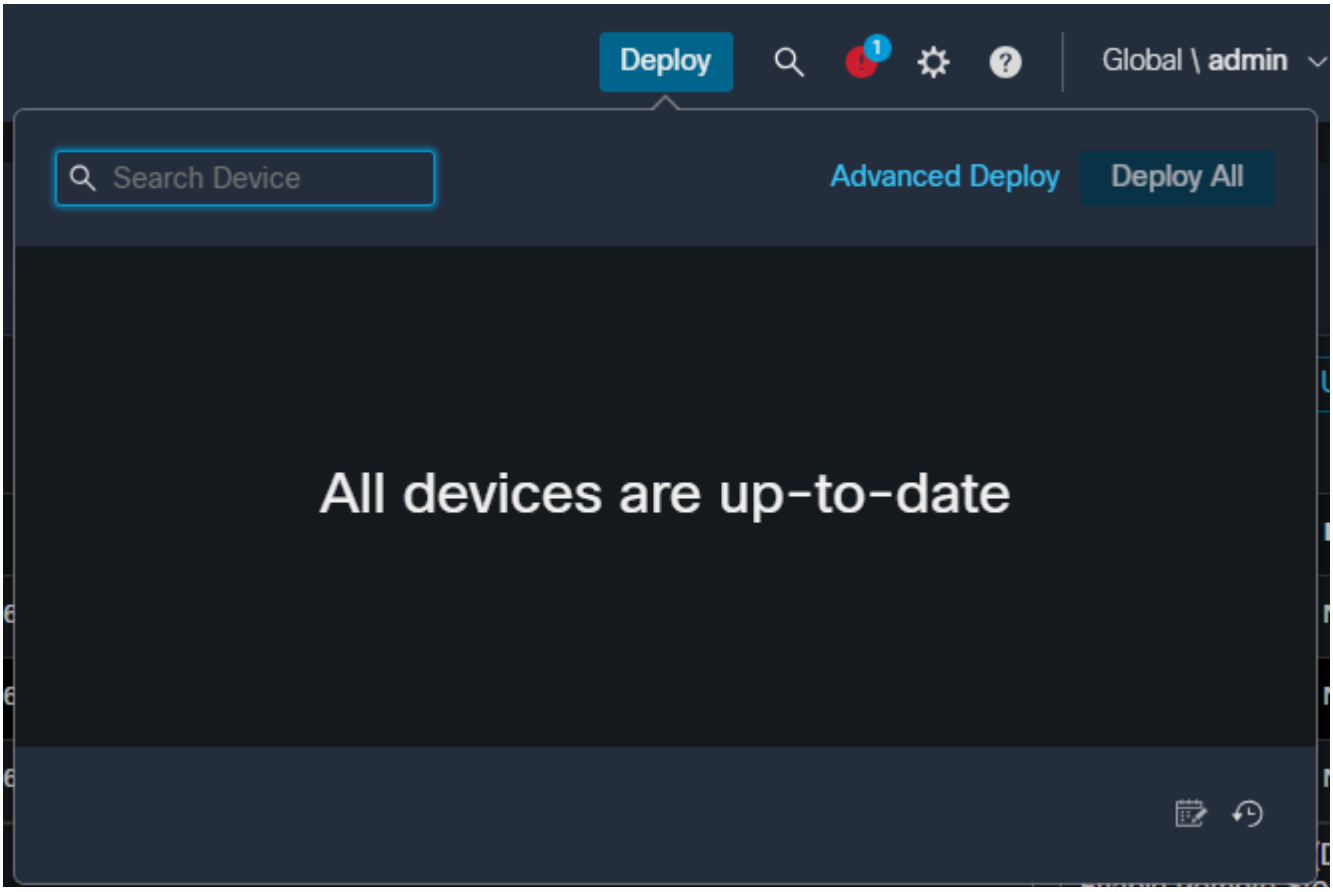
inline_image_0.png



inline_image_1.png

Clique no botão Managed Device Backup para fazer backup do par FTD HA.

Para garantir que o estado da configuração do dispositivo FTD seja preservado, confirme se a implantação da configuração mais recente foi concluída do FMC para os dois pares HA:



inline_image_2.png

Etapa 2: Verifique o status atual do par FTD HA

Antes de continuar com a atualização, verifique o status do HA para confirmar se os dois pares estão íntegros e sincronizados. Na CLI do FTD, use este comando para verificar o status do dispositivo:

```
> show failover state
```

Saída de exemplo:

```
Data/Hora do Motivo da Última Falha do Estado

Este host - Principal

 Nenhum Ativo

Outro host - Secundário

 Pronto para Espera Nenhum
```

```
====Estado da configuração===

 Sincronização ignorada

====Estado da Comunicação===
```

Mac setStep 3: Agendar e comunicar a janela de manutenção

Certifique-se de que a janela de manutenção esteja claramente definida e que todos os participantes sejam informados. Para este workflow, a manutenção foi programada de acordo:

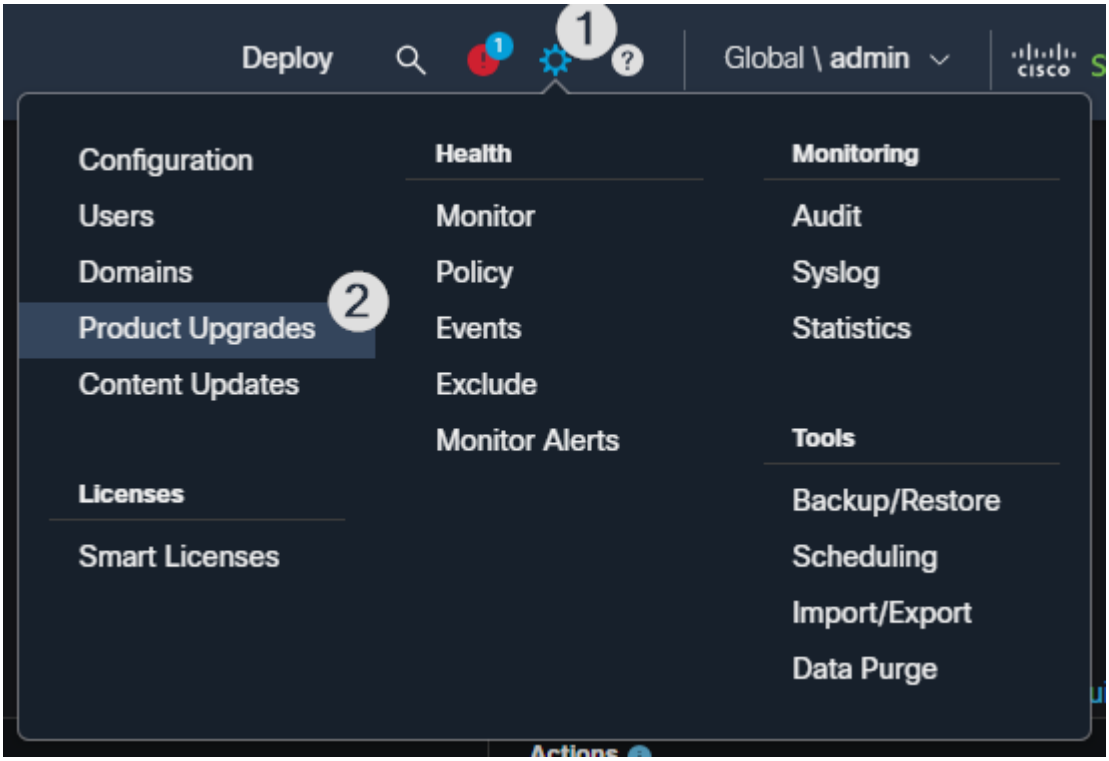
- Hora de início: 18/11/2025 12:00:00 (UTC -3 Argentina/Buenos_Aires)
- Hora de término: 18/11/2025 14:00:00 (UTC -3 Argentina/Buenos_Aires)

Etapa 4: Iniciar a atualização do FTD HA

Inicie a atualização no FMC, garantindo que você siga o procedimento recomendado pela Cisco para atualizar os pares HA do FTD. Durante o processo de atualização, a atualização é normalmente executada de forma contínua automaticamente:

1. Atualize o FTD de standby.
2. Execute o failover para o FTD recém-atualizado e torne-o ativo.
3. Atualize o outro FTD agora em espera.

Na GUI do FMC, navegue para System > Product Upgrades e selecione a versão de destino para atualização.



inline_image_3.png

Etapa 5: Monitorar o Processo de Atualização

Monitore de perto o progresso da atualização para ambas as unidades. Use a seção de monitoramento de trabalhos da GUI do FMC ou a CLI para atualizações de status. Para verificar o progresso da atualização na CLI:

```
> show upgrade status
```

Saída de exemplo:

```
Atualização em andamento na unidade em espera...

Atualização concluída na unidade em espera.

Iniciando failover...

Atualização em andamento na unidade ativa...

Atualização concluída em ambas as unidades.
```

O par HA está sincronizado.Etapa 6: Verificação pós-atualização

Após a conclusão do upgrade, verifique se:

- Ambos os dispositivos FTD estão executando a versão de software pretendida.
- O status de HA relata ambas as unidades como íntegras e sincronizadas.
- Todos os serviços e fluxos de rede pretendidos estão funcionando conforme esperado.

```
> show version
```

Saída de exemplo:

```
---------------[ firepower ]---------------

Modelo: Cisco Firepower Threat Defense for VMware (75) versão 7.4.2.4 (Build 9)

UUID: bc9d31e8-0517-11f0-9c89-c358b8259f96

Versão LSP : lsp-rel-20260128-1954

Versão do VDB: 404

-----------------------------------------------------

> show failover
```

Saída de exemplo:

```
> show failover

Failover Ativado

Unidade de failover primária

Interface de LAN de failover: GigabitEthernet0/7 de estado de failover (ativa)

Tempo limite de reconexão 0:00:00
```

Frequência de Sondagem de Unidade 1 segundo, tempo de espera 15 segundos

Frequência de pesquisa de interface de 5 segundos, tempo de espera de 25 segundos

Política de interface 1

Interfaces Monitoradas 4 de um máximo de 361

Intervalo de Notificação de Movimentação de Endereço MAC não definido

failover replication http

Versão: Nossa 9.20(2)121, Companheiro 9.20(2)121

Número de série: nosso SERIAL, Mate SERIAL

Último failover em: 14:29:08 UTC 31 de dezembro de 2025

 Este host: Principal - Ativo

 Tempo ativo: 3418340 (s)

 slot 0: status do ASAv hw/sw rev (/9.20(2)121) (sistema ativo)

 Interface OUTSIDE (IPADDRESS): normal (monitorada)

 Interface INSIDE (IPADDRESS): normal (monitorada)

 Interface DMZ (IPADDRESS): normal (monitorada)

 Gerenciamento de interface (IPADDRESS): normal (monitorado)

 slot 1: snort rev (1.0) status (up)

 slot 2: status do diskstatus rev (1.0) (up)

 Outro host: Secundário - Pronto para Espera

```
Tempo ativo: 0 (seg)

Interface OUTSIDE (IPADDRESS): normal (monitorada)

Interface INSIDE (IPADDRESS): normal (monitorada)

Interface DMZ (IPADDRESS): normal (monitorada)

Gerenciamento de interface (IPADDRESS): normal (monitorado)

slot 1: snort rev (1.0) status (up)
```

slot 2: status do diskstatus rev (1.0) (up)

Etapa 7: Verifique se os backups estão atualizados

Como etapa final, gere novos backups do FMC e do FTD após a atualização para capturar o estado atual da configuração atualizada.

Repita o processo de backup conforme descrito na Etapa 1.

Causa

Nenhum. Este é um fluxo de trabalho de atualização padrão para HA do Cisco FTD gerenciado pelo FMC.

Conteúdo relacionado

- Suporte técnico e downloads da Cisco
- Atualização do FTD HA Gerenciado pelo FMC
- Solucionar problemas de procedimentos de geração de arquivos do Firepower
- Notas de versão

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.