

Migre o FMC local para a nuvem (cdFMC) com o Security Cloud Control

Contents

[Problema](#)

[Ambiente](#)

[Resolução](#)

[Causa](#)

[Conteúdo relacionado](#)

- [Problema](#)
 - [Ambiente](#)
 - [Resolução](#)
 - [Causa](#)
 - [Conteúdo relacionado](#)
-

Problema

Um usuário precisa de assistência para migrar seu dispositivo virtual do Firewall Management Center (FMCv300) de produção para o FMC fornecido em nuvem (cdFMC) no locatário do Security Cloud Control (SCC). As preocupações específicas incluem:

- Entenda quais partes do processo de migração podem causar inatividade e como minimizar o impacto na produção.
- Obtenha orientação passo a passo para o fluxo de trabalho de migração.
- Determine o que fazer com o FMCv300 após a conclusão da migração.
- Planeje uma abordagem de migração em fases para vários dispositivos FTD (Firewall Threat Defense) em configurações de HA (High Availability, alta disponibilidade).
- Esclareça se a configuração FMC local deve ser importada manualmente para o cdFMC antes de acionar o assistente de migração.

Ambiente

- FMC de origem: Dispositivo virtual FMCv300, versão 7.6.5. Outras plataformas de hardware (HW) e software (SW) também podem ser implantadas.
- Destino: cdFMC provisionado pelo locatário.
- Os dispositivos gerenciados são FTDs de diferentes versões de HW e SW, por exemplo:
 - 2x Secure Firewall 3130, FTD 7.6.4, configurado no par HA.
 - 2x Firepower 2130, FTD 7.4.4, configurado no par HA.
 - 1x FTDv no Azure, 7.6.4, configuração independente.

Resolução

Pré-requisitos de Migração e Validação de Versão

As versões de ambiente atendem aos pré-requisitos para migração para o cdFMC:

- O FMC 7.6.5 atende aos requisitos mínimos documentados para o fluxo de trabalho de migração.
- As versões 7.6.4 e 7.4.4 do FTD atendem ao mínimo documentado para migração.
- O cdFMC suporta as trilhas de liberação de FTD no ambiente.

Etapas de Validação Pré-Migração

Antes de iniciar a migração, valide estes pré-requisitos:

- Nenhuma implantação pendente no FMCv300.
- Ambos os pares de HA são saudáveis e sincronizados.
- Backup do FMCv300 concluído.
- Espaço em disco adequado do CVP disponível (pelo menos 10 % livre).
- Resolução DNS funcionando a partir do caminho de gerenciamento do FTD.
- Conectividade de saída permitida das interfaces de gerenciamento FTD para cdFMC através das portas de gerenciamento de nuvem necessárias (TCP 443 e TCP 8305).

- O FMCv300 tem acesso HTTPS de saída ao SCC.

Processo de Importação de Configuração

A configuração FMCv300 local não precisa ser importada manualmente para o cdFMC antes da execução do assistente de migração. O fluxo de trabalho "Migrar FTD para cdFMC" trata a importação de configuração como parte do trabalho de migração:

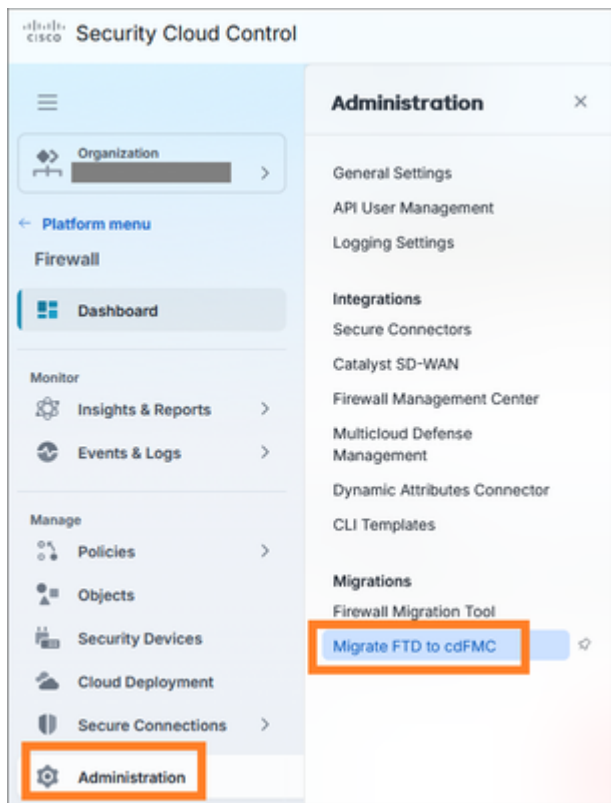
1. O SCC se conecta ao FMCv300 local.
2. Exporta a configuração pertinente do CVP local.
3. Importa políticas/objetos compartilhados para o cdFMC.
4. Importa configurações específicas do dispositivo, como interfaces e roteamento.
5. Registra os dispositivos FTD selecionados no cdFMC.
6. O período de avaliação de 14 dias começa após a conclusão da migração.

Se você criar manualmente políticas ou objetos no cdFMC antes da migração com os mesmos nomes dos itens no FMCv300, o fluxo de trabalho de migração poderá usar o item de cdFMC existente em vez de importar a versão local, o que pode causar resultados inesperados.

Sequência de migração recomendada

Fase 1: Configuração pré-migração

1. Implante o cdFMC em seu locatário SCC.
2. Integre o FMCv300 atual ao SCC.
3. Confirme o Smart Licensing para o cdFMC.
4. Inicie o fluxo de trabalho de migração em Firewall > Administration > Migrations > Migrate FTD to cdFMC:



5. Use a opção para pausar após a importação da política compartilhada para revisão:

 **Security Cloud Control**

Migrate FTD to cdFMC

Migrate FTD from On-Prem FMC to cloud

- 1 Before you begin
- 2 Select On-Prem FMC **On-Prem FMC: FMC**
- 3 Select Devices

Select FTD device(s) to migrate from On-Prem FMC to cloud, and specify an action in bulk or per device.
Last Synced time : 7 minutes ago [Sync from On-Prem FMC now](#)

Search:

☐	Name	Domain
☐	FTD3140-HA	Global

0 device(s) selected

☒ Pause migration to review imported shared policy ⓘ

☐ Auto deploy to FTDs after successful migration ⓘ

[Migrate FTD to cdFMC](#)

Fase 2: Execução da Migração

Durante a janela de manutenção, migre dispositivos usando uma abordagem em fases:

1. Comece com o FTD independente (impacto mais baixo).
2. Migre o primeiro par HA.
3. Valide a integridade e a funcionalidade do dispositivo.
4. Migre o segundo par HA.

Fase 3: Validação pós-migração

Após a migração de cada dispositivo ou par de alta disponibilidade:

1. Confirme a integridade do dispositivo no cdFMC.
2. Confirme o estado de HA quando aplicável.
3. Revise a visualização/avisos da implantação.
4. Implantar do cdFMC.
5. Valide a visibilidade de tráfego e eventos.

Plano de migração trifásico com congelamento de configuração

A abordagem recomendada envolve a execução de migrações de FTD em três fases, cada uma ocorrendo em datas separadas, com um mínimo de três dias de monitoramento pós-transição por fase. Essa abordagem reduz os riscos e oferece tempo para validar:

- Implantação de política do cdFMC.
- Status de integridade do dispositivo.
- Status de HA para ambos os pares de HA.
- Visibilidade de eventos/análises na nuvem.
- Quaisquer problemas operacionais antes de passar para a próxima fase.

Implementação de congelamento de configuração

Implemente um congelamento de configuração durante o período de migração/avaliação com esta abordagem:

- Melhor opção: Congelar todas as alterações de configuração relacionadas ao FTD no FMCv300 e no cdFMC até que cada fase seja validada e confirmada.
- Opção mínima: Congele os dispositivos que estão sendo migrados e quaisquer políticas/objetos compartilhados usados por dispositivos migrados e não migrados.
- Evite editar as mesmas políticas/objetos compartilhados no FMCv300 e no cdFMC durante a migração em fases.
- Evite alterações importantes durante o período de avaliação.

Processo de alteração de emergência

Para alterações de emergência durante a migração:

- Aplique a alteração somente no gerenciador autoritativo atual para esse dispositivo:
 - Dispositivos ainda não migrados: FMCv300
 - Dispositivos já migrados: cdFMC.
- Documente a alteração, a política/objeto afetado, o carimbo de data/hora e o escopo do dispositivo.
- Reconcilie a alteração após a conclusão da fase, especialmente se ela afetar objetos compartilhados ou políticas compartilhadas.

Gerenciamento do Período de Avaliação

Considerações importantes para o período de avaliação de 14 dias:

- Controle a janela de avaliação de 14 dias para cada fase/trabalho de migração.
- Não permita que nenhuma fase atinja a confirmação automática sem intenção.
- Se o monitoramento de três dias for bem-sucedido, confirme essa fase manualmente, em vez de aguardar os 14 dias completos.

Processo de desativação do FMCv300

Não desligue ou remova o FMCv300 imediatamente após a migração do dispositivo. Mantenha o FMCv300 disponível até:

- Todos os dispositivos de FTD são migrados com êxito.
- as implantações de cdFMC foram bem-sucedidas.
- Os eventos/análises de nuvem são confirmados.
- A migração foi confirmada.
- Todos os requisitos de retenção de log/evento são atendidos.

- Um backup FMCv300 final é retido de acordo com a política organizacional.

Depois que essas condições são atendidas, o FMCv300 pode ser removido do uso ativo e descomissionado de acordo com os processos padrão de retirada de máquinas virtuais.

Causa

Esta é uma migração planejada do FMC local para o cdFMC. A migração é motivada pela necessidade de aproveitar os recursos de gerenciamento baseados em nuvem e desativar o dispositivo virtual FMCv300 existente.

Conteúdo relacionado

- [Migrar FTD para cdFMC - Documentação da Cisco](#)
- [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.