# Atualizar o FMCv e migrar do VMware ESXi 7.0 para o ESXi 8.0: Abordagem em etapas e práticas recomendadas

## Contents

## Problema

Um administrador que executa o Firewall Management Center Virtual (FMCv) versão 7.3.1 no VMware ESXi 7.0 está planejando atualizar o FMC para uma versão com suporte superior e, posteriormente, migrar a máquina virtual do FMCv para um novo cluster do VMware ESXi 8.0. Essas preocupações foram levantadas durante este esforço de planejamento:

- Se é seguro atualizar primeiro o FMCv de 7.3.1 para 7.4.2 e depois migrar a VM para o cluster ESXi 8.0, antes de executar quaisquer atualizações adicionais.
- Se há problemas ou restrições de compatibilidade conhecidos durante a migração de um FMCv executando a versão 7.3.1 ou 7.4.2 para um ambiente VMware ESXi 8.0.
- Se o VMware vMotion pode ser usado para executar uma migração perfeita do mesmo IP da máquina virtual FMCv para o novo cluster sem criar uma nova instância de VM.
- Se os snapshots do VMware podem ser usados como um mecanismo de backup e reversão em caso de falha na atualização ou migração.
- Qual é a versão mais compatível do FMC para o cenário de dispositivos gerenciados existente, que inclui dispositivos de Firewall Threat Defense (FTD) que variam da versão 7.2.8 à 7.4.2.
- Como evitar conflitos de endereço IP ao transferir para a nova instância do FMCv no novo cluster, mantendo o mesmo endereço IP e nome de host de gerenciamento.
- Qual é a ordem correta das operações para um plano de atualização e migração em fases que minimiza o risco e o tempo de inatividade.

## Ambiente

- Produto: FMCv
- Versão atual do software FMC: 7.3.1
- Plataforma de hipervisor atual: VMware ESXi 7.0
- Plataforma de hipervisor de destino: VMware ESXi 8.0.3 (novo cluster)
- Tipo de implantação do FMC: Autônomo (não faz parte de um par de alta disponibilidade)
- Dispositivos gerenciados: Vários dispositivos FTD variando da versão 7.2.8 a 7.4.2

# Resolução

A abordagem recomendada para esse ambiente é um plano de atualização e migração em etapas e em fases. Esse plano separa a atualização do software FMC, a migração da plataforma do hipervisor e qualquer atualização subsequente da versão do FMC em eventos de manutenção distintos. Essa abordagem reduz o risco em cada fase e fornece pontos de reversão claros. O uso do VMware vMotion, instantâneos, clonagem ou migração direta no nível da VM não é explicitamente o método suportado para migrar o FMCv entre clusters ou versões.

## Importante: Snapshots, vMotion e clonagem do VMware não são compatíveis com a migração do FMCv

Antes de prosseguir com qualquer fase deste plano, é essencial entender as seguintes restrições em relação aos métodos de migração nativos do VMware:

- Os snapshots do VMware não são um método compatível de backup, restauração ou reversão para upgrades ou migrações do FMCv. Reverter um FMCv para um instantâneo do VMware pode causar corrupção do banco de dados, incompatibilidades de atualização de versão e conteúdo ou um estado de sistema sem suporte.
- O VMware vMotion, a clonagem e a migração direta de máquina virtual entre clusters não são o método suportado para migrar o FMCv para uma nova plataforma de hipervisor. Estes métodos ignoram os mecanismos internos de integridade dos dados do CVP.
- O único método compatível para migrar o FMCv para um novo cluster ou host é o fluxo de trabalho de backup e restauração nativo do FMC, combinado com a implantação de uma nova instância do FMCv na plataforma de destino.

A estratégia de reversão correta, se a validação falhar após a transferência, é desligar a nova instância do FMCv e colocar o FMCv original em serviço. Não dependa de reversões de instantâneo para essa finalidade.

## Fase 1: Verificação de Compatibilidade Pré-Atualização

Antes de iniciar qualquer atualização do software FMC, confirme as versões exatas do software de todos os dispositivos FTD gerenciados no ambiente.

- O FMC 7.4.2 suporta o gerenciamento de dispositivos FTD executando a versão 7.0 e posterior.
- O FMC 7.6.6 suporta o gerenciamento de dispositivos FTD executando a versão 7.1 e posterior.
- Se qualquer dispositivo de DTF instalado no ambiente estiver a funcionar com uma versão < 7.0, esse dispositivo deve ser atualizado para, pelo menos, a versão 7.0 enquanto o CVP permanecer na versão 7.3.1, antes de o próprio CVP ser atualizado.
- Para o ambiente documentado (intervalo de FTD: 7.2.8 a 7.4.2), todos os dispositivos geridos estão dentro da gama de compatibilidade tanto para o FMC 7.4.2 como para o FMC 7.6.6. Neste caso, não é necessária nenhuma pré-atualização do FTD.

Confirme também estes antes de continuar:

- O CVP é autônomo e não faz parte de um par de alta disponibilidade (HA).
- O VMware ESXi 8.0 exato baseia-se no novo cluster (confirmado como ESXi 8.0.3 neste ambiente).
- O perfil de recursos do FMCv (vCPUs, memória, disco) atende aos requisitos da versão do FMC de destino. A especificação atual de 4 vCPUs, 32 GB de RAM e 250 GB de disco deve ser analisada em relação às diretrizes de implantação atuais, especialmente antes da atualização para o FMC 7.6.6.
- Se o endereço IP e o nome do host de gerenciamento do FMC permanecem os mesmos após a migração (altamente recomendável para evitar a necessidade de atualizações do endereço do gerente em todos os dispositivos de FTD gerenciados).

## Fase 2: Atualizar o FMCv existente da versão 7.3.1 para a 7.4.2 no cluster ESXi 7.0

atual

Essa fase atualiza o software FMCv para a versão 7.4.2 enquanto ele permanece na infraestrutura existente do ESXi 7.0. O FMCv 7.4.2 adiciona suporte explícito ao VMware ESXi 8.0, que é necessário antes da migração da plataforma na Fase 3.

Passo 1: Antes de iniciar a atualização, confirme se não há implantações de política pendentes, trabalhos de backup ativos ou tarefas em segundo plano em execução no FMC.

Passo 2: Execute um backup FMC nativo completo usando o utilitário de backup integrado do FMC. Armazene o backup em um local remoto seguro fora da máquina virtual FMCv. Verifique se o backup foi concluído com êxito antes de continuar.

Passo 3: Concluir todas as verificações de preparação para atualização, conforme documentado no guia de planejamento de atualização do FMC 7.4. Resolva todos os problemas sinalizados antes de iniciar a atualização.

Passo 4: Atualizar o FMCv existente da versão 7.3.1 para a versão 7.4.2. Utiliza o caminho de transição de atualização suportado: 7.3 → 7.4.

Passo 5: Após a conclusão da atualização, execute a validação pós-atualização:

- Verifique se todos os dispositivos FTD gerenciados foram reconectados ao FMC.
- Confirme se a ingestão de eventos está ativa e se os eventos estão aparecendo no FMC.
- Confirme se o status do licenciamento está correto.
- Execute uma implantação de política de teste para um dispositivo gerenciado e confirme se ela foi bem-sucedida.

Não prossiga para a Fase 3 até que todas as etapas de validação pós-atualização tenham sido aprovadas com êxito no FMCv 7.4.2 atualizado.

## Fase 3: Migrar o FMCv para o cluster do VMware ESXi 8.0.3 usando backup e restauração nativos

Essa fase migra o FMCv do cluster ESXi 7.0 existente para o novo cluster ESXi 8.0.3. Isso é realizado com a implantação de uma nova instância do FMCv no cluster de destino e a restauração de um backup do FMC nativo nele. O mesmo endereço IP de gerenciamento e o mesmo nome de host são mantidos para evitar a necessidade de alterações de endereço de gerente em todos os dispositivos FTD gerenciados.

Passo 1: Uma vez confirmado que o FMCv está estável na versão 7.4.2, gere um novo backup do FMC nativo. Armazene-o em um local seguro e remoto. Verifique se o backup foi concluído e se é válido antes de continuar.

Passo 2: Implante uma nova instância do FMCv no cluster ESXi 8.0.3. A versão do software e a compilação desta nova instância devem corresponder exatamente à versão do FMCv (incluindo patches e hotfixes) do qual o backup foi feito (FMCv 7.4.2). Verifique se a nova instância está configurada com recursos equivalentes ou maiores (vCPUs, memória, disco) e se a configuração de rede está preparada, mas o endereço IP de gerenciamento de produção ainda não foi atribuído à nova instância neste ponto.

Passo 3: Restaure o backup do FMC nativo na nova instância do FMCv no ESXi 8.0.3.

Passo 4: Antes de colocar o novo FMCv on-line com o endereço IP e o nome do host de gerenciamento de produção, desligue completamente ou desconecte o FMCv original da rede. Esta é uma etapa obrigatória para evitar a duplicação de uma condição IP e para evitar que duas instâncias do FMC tentem comunicar-se simultaneamente com os mesmos dispositivos de FTD gerenciado.

Durante o período em que o FMCv original é desligado e antes de o novo FMCv estar em linha, espera-se este comportamento para os dispositivos de FTD geridos:

- Encaminhamento de tráfego: Os dispositivos de FTD operam planos de dados independentemente do FMC e continuam a encaminhar o tráfego sem interrupções e a aplicar a última política de controle de acesso implantada com êxito, exceto nos casos mencionados aqui.
- Mudanças de gerenciamento e visibilidade: As implantações de políticas, os ajustes de configuração, os alertas de integridade do FMC e a visibilidade do gerenciamento de dispositivos estão completamente indisponíveis.
- Buffer de eventos e perda potencial: A visibilidade de eventos em tempo real no FMC é pausada. Enquanto o FTD tenta registrar eventos de segurança e conexão localmente em seus arquivos unificados temporários, esses arquivos têm limites de armazenamento rigorosos e operam em uma base de substituição circular. Os registros de conexão de alto volume podem ser substituídos ou perdidos durante uma janela de migração estendida. Os

eventos que permanecem no buffer local são transmitidos para o novo FMC quando este estiver online.

- Regras de malware (AMP): As solicitações de pesquisa em nuvem em tempo real para arquivos sem cache estão temporariamente indisponíveis porque o FMC envia essas consultas de reputação para a nuvem da AMP. O FTD continua a aplicar regras de bloqueio ou permissão apenas para arquivos já armazenados em seu cache de disposição local. Os arquivos sem cache ignoram a análise em nuvem e usam as configurações à prova de falhas da sua política (geralmente falhando ao abrir para evitar a interrupção do tráfego). Os envios de sandboxing para o Threat Grid e os alertas retrospectivos são pausados até que o novo FMC esteja operacional.

- Regras baseadas em identidade: Os usuários que já estão conectados e mapeados para um endereço IP não sofrem interrupção, pois o FTD retém os mapeamentos ativos na memória local. No entanto, como o FMC atua como o agente para origens de identidade (por exemplo, Cisco ISE ou Ative Diretory Agents), novos logins de usuário ou alterações de IP durante essa janela não podem ser aprendidos pelo FTD. Essas sessões desconhecidas retornam às regras padrão ou de convidado da sua política.

- Filtragem de URL: Pesquisas de nuvem ao vivo para sites completamente desconhecidos estão temporariamente indisponíveis porque o FMC direciona solicitações de URL desconhecidas para a nuvem do Cisco Talos. O FTD continua a filtrar e aplicar totalmente a política apenas para sites já encontrados dentro de seu conjunto de dados local enviado ou seu cache de memória local ativo. O tráfego da Web que atinge uma URL desconhecida e sem cache ignora a classificação de nuvem e corresponde às configurações de fallback da sua política para tráfego sem categoria (normalmente permitido). As atualizações do pacote de banco de dados de URL são pausadas até que o novo FMC esteja online.

Passo 5: Atribua o endereço IP e o nome do host de gerenciamento de produção ao FMCv restaurado no ESXi 8.0.3 e coloque-o on-line. Como o mesmo endereço IP e nome de host são usados, os dispositivos FTD gerenciados podem se reconectar ao FMC automaticamente sem exigir alterações de endereço de gerente em dispositivos FTD individuais.

Passo 6: Executar validação pós-migração:

- Verifique se todos os dispositivos FTD gerenciados foram reconectados à nova instância do FMCv.

- Verifique o status do licenciamento e confirme se todas as licenças foram aplicadas corretamente.

- Confirme se o fluxo de eventos e todas as integrações externas estão funcionando corretamente.

- Execute uma implantação de política controlada em um dispositivo gerenciado e confirme se ela é bem-sucedida.

Se a validação falhar em qualquer ponto durante essa fase, desligue a nova instância do FMCv, restaure o FMCv original no ESXi 7.0 para funcionamento e solucione os problemas antes de tentar a migração novamente. Não use uma reversão de instantâneo do VMware como mecanismo de reversão.

## Fase 4: Atualização do FMCv de 7.4.2 para 7.6.6 (após a confirmação da estabilidade da migração)

Depois que a migração do FMCv para o ESXi 8.0.3 for totalmente validada e confirmada como estável, uma atualização adicional para o FMC 7.6.6 poderá ser considerada. É altamente recomendável não combinar a migração da plataforma do hipervisor (Fase 3) e essa atualização adicional da versão do FMC em um único evento de manutenção. Concluir a migração primeiro fornece um ponto de verificação limpo e de baixo risco antes de continuar.

Antes de iniciar o upgrade para a versão 7.6.6, confirme estes pré-requisitos:

- Cada dispositivo FTD gerenciado no ambiente está executando a versão 7.1 ou posterior. O FMC 7.6.6 não suporta o gerenciamento de dispositivos de FTD < versão 7.1. No ambiente documentado (intervalo de FTD: 7.2.8 a 7.4.2), todos os dispositivos atendem a esse requisito.
- O perfil de recursos do FMCv (4 vCPUs, 32 GB de RAM, disco de 250 GB) foi validado em relação às diretrizes de implantação do FMC 7.6.6 para a contagem total de dispositivos gerenciados e os requisitos de retenção de eventos nesse ambiente.
- O caminho de transição de atualização com suporte foi confirmado: 7.4 → 7.6.
- O CVP é confirmado como autônomo (não faz parte de um par de alta disponibilidade).

Passo 1: Crie e verifique um novo backup FMC nativo da instância estável do FMCv 7.4.2 no ESXi 8.0.3. Armazene-o em um local remoto seguro.

Passo 2: Atualizar o FMCv da versão 7.4.2 para a versão 7.6.6.

Passo 3: Executar validação final pós-atualização:

- Verifique se todos os dispositivos FTD gerenciados foram reconectados ao FMC.
- Confirme se a manipulação e a inclusão de eventos estão funcionando corretamente.

- Confirme se o status do licenciamento está correto.
- Execute uma implantação de política controlada para confirmar se a aplicação de política foi bem-sucedida.

## Resumo do caminho de atualização e da sequência de transição

A tabela resume o plano em etapas completo, as transições de atualização suportadas e a ação principal em cada fase:

| Fase | Ação | Versão do FMC | Hipervisor | Transição suportada |
|---|---|---|---|---|
| Fase 1 | Verificação de compatibilidade pré-upgrade; confirmar versões de FTD, status de HA do FMC e perfil de recursos | 7.3.1 (atual) | ESXi 7.0 | N/A — apenas preparação |
| Fase 2 | Atualizar o software FMCv; executar backup nativo; validar dispositivos gerenciados e implantação de políticas | 7.3.1 → 7.4.2 | ESXi 7.0 | 7.3 → 7.4 (suportado) |
| Fase 3 | Implantar novo FMCv no ESXi 8.0.3; restaurar backup nativo; cortar usando o mesmo IP/nome de host; validar | 7.4.2 (sem alteração de versão) | ESXi 7.0 → ESXi 8.0.3 | Backup/restauração nativo — método compatível |
| Fase 4 | Depois que a migração estiver estável: Melhorar o FMCv; validar a conectividade, o licenciamento, os eventos e a política do dispositivo | 7.4.2 → 7.6.6 | ESXi 8.0.3 | 7.4 → 7.6 (suportado) |

## Considerações principais

- Conformidade de caminho de atualização: A sequência de atualização completa (7.3.1 → 7.4.2 → 7.6.6) utiliza os caminhos de transição de atualização do FMC suportados (7.3 → 7.4 e 7.4 → 7.6). Ignorar versões intermediárias ou combinar fases em um único evento não é

recomendado.

- Compatibilidade FMC-FTD: O FMC 7.6.6 mantém total compatibilidade de gerenciamento com dispositivos FTD executando as versões 7.2.8 a 7.4.2. O FMC 7.6 exige que todos os dispositivos FTD gerenciados sejam da versão 7.1 ou posterior.
- Transição do mesmo endereço IP: O FMCv original deve ser totalmente desligado ou desligado da rede antes de o FMCv de substituição ser colocado em linha com o endereço IP de gestão da produção. Isso evita uma condição de IP duplicado e evita que dois centros de gerenciamento tentem se comunicar simultaneamente com os mesmos dispositivos de FTD. Quando o FMCv restaurado retorna com o mesmo endereço IP e nome de host, os dispositivos FTD gerenciados podem se reconectar sem exigir alterações no endereço do gerente.
- Validação de recursos antes do 7.6.6: O perfil de recursos do FMCv (4 vCPUs, 32 GB de RAM, disco de 250 GB) deve ser analisado em relação às diretrizes de implantação atuais antes da atualização para o FMC 7.6.6, levando em conta a contagem total de dispositivos gerenciados e os requisitos de retenção de eventos para o ambiente.
- Verificação de backup nativo: Em cada fase em que é feito um backup FMC nativo, o backup deve ser verificado como completo e válido antes de prosseguir. Os backups devem ser armazenados em um local remoto seguro fora da máquina virtual FMCv.
- Não combinar migração e atualização: A migração da plataforma (fase 3) e a subsequente atualização da versão do FMC para a versão 7.6.6 (fase 4) devem ser realizadas como eventos de manutenção separados. Isso garante a existência de um ponto de verificação limpo no FMCv 7.4.2 no ESXi 8.0.3 antes de qualquer outra alteração ser feita.

# Causa

Esse não é um problema de quebra/conserto resultante de um defeito ou configuração incorreta do software. A causa subjacente que requer esta orientação é uma combinação de requisitos de compatibilidade de versão e restrições de migração de plataforma específicas para o Cisco FMCv no VMware:

- Compatibilidade da versão do FMC com o FTD 7.4.2: A presença de um dispositivo FTD gerido que execute a versão 7.4.2 no ambiente exige que o FMC seja atualizado para uma versão mínima de 7.4.2, uma vez que as versões anteriores do FMC não podem gerir dispositivos FTD numa versão superior à do próprio FMC.
- Suporte FMCv para VMware ESXi 8.0: O FMCv 7.3.1 não oferece suporte ao VMware ESXi 8.0 como uma plataforma de hipervisor. O FMCv deve ser atualizado para a versão 7.4.2 (ou posterior) antes de ser implantado ou operado no ESXi 8.0.x. A tentativa de migrar a VM

do FMCv 7.3.1 diretamente para o ESXi 8.0 sem primeiro atualizar o software do FMC apresenta risco de compatibilidade.

- Métodos de migração de VM sem suporte: VMware vMotion, instantâneos, clonagem e migração direta de VMs não são métodos compatíveis para migração de FMCv entre clusters ou versões de hipervisor. Esses métodos podem resultar em corrupção do banco de dados, incompatibilidade de versão ou um estado do sistema sem suporte. O único caminho de migração compatível é o fluxo de trabalho de backup e restauração nativo do FMC combinado com uma nova implantação do FMCv na plataforma de destino.

## Conteúdo relacionado

- Guia de atualização do Cisco Secure Firewall Management Center, Versão 7.4 — Planejamento de atualização e caminhos suportados
- Guia de atualização do Cisco Secure Firewall Management Center, Versão 7.6 — Planejamento de atualização e caminhos suportados
- Guia de compatibilidade do Cisco Secure Firewall Management Center (Matriz de compatibilidade FMC e FTD)
- Cisco Secure Firewall Management Center Novos Recursos por Versão — Versão 7.4.2
- Guia de atualização do Cisco Firepower Management Center — Planejamento de atualização
- 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.