Actualización de FMCv y migración de VMware ESXi 7.0 a ESXi 8.0: Enfoque por fases y prácticas recomendadas

Contenido

Problema

Un administrador que ejecuta la versión 7.3.1 de Firewall Management Center virtual (FMCv) en VMware ESXi 7.0 tiene previsto actualizar el FMC a una versión más alta compatible y, posteriormente, migrar la máquina virtual FMCv a un nuevo clúster de VMware ESXi 8.0. Estas preocupaciones se plantearon durante este esfuerzo de planificación:

- Si es seguro actualizar primero FMCv de 7.3.1 a 7.4.2 y, a continuación, migrar la VM al clúster de ESXi 8.0 antes de realizar actualizaciones posteriores.
- Si se conocen problemas de compatibilidad o restricciones al migrar un FMCv que ejecuta la versión 7.3.1 o 7.4.2 a un entorno VMware ESXi 8.0.
- Si se puede utilizar VMware vMotion para realizar una migración perfecta de la misma IP de la máquina virtual FMCv al nuevo clúster sin necesidad de crear una nueva instancia de VM.
- Si las instantáneas de VMware se pueden utilizar como mecanismo de copia de seguridad y reversión en caso de que la actualización o migración falle.
- ¿Cuál es la versión de FMC compatible más alta para el panorama de dispositivos gestionados existente, que incluye los dispositivos de defensa frente a amenazas de firewall (FTD) que van desde la versión 7.2.8 a la 7.4.2.
- Cómo evitar conflictos de direcciones IP al pasar a la nueva instancia de FMCv en el nuevo clúster manteniendo la misma dirección IP de administración y el mismo nombre de host.
- Cuál es el orden correcto de las operaciones para un plan de migración y actualización por fases que minimice el riesgo y el tiempo de inactividad.

Entorno

- Producto: FMCv
- Versión actual del software FMC: 7.3.1
- Plataforma de hipervisor actual: VMware ESXi 7.0
- Plataforma de hipervisor objetivo: VMware ESXi 8.0.3 (nuevo clúster)
- Tipo de implementación de FMC: Independiente (no forma parte de un par de alta disponibilidad)
- Dispositivos gestionados: Varios dispositivos FTD que van desde la versión 7.2.8 a la 7.4.2

Resolución

El enfoque recomendado para este entorno es un plan de migración y actualización por fases. Este plan separa la actualización del software de FMC, la migración de la plataforma del hipervisor y cualquier actualización posterior de la versión de FMC en distintos eventos de mantenimiento. Este enfoque reduce el riesgo en cada fase y proporciona puntos de reversión claros. El uso de VMware vMotion, las instantáneas, la clonación o la migración directa a nivel de VM no es explícitamente el método admitido para migrar FMCv entre clústeres o versiones.

Importante: Las instantáneas, vMotion y la clonación de VMware no son compatibles con la migración a FMCv

Antes de continuar con cualquier fase de este plan, es fundamental comprender estas limitaciones con respecto a los métodos de migración nativos de VMware:

- Las instantáneas de VMware no son un método de copia de seguridad, restauración o reversión compatible para las actualizaciones o migraciones de FMCv. Revertir un FMCv a una instantánea de VMware puede provocar daños en la base de datos, discrepancias en la actualización de la versión y el contenido o un estado del sistema no compatible.
- VMware vMotion, la clonación y la migración directa de máquinas virtuales entre clústeres no son el método admitido para migrar FMCv a una nueva plataforma de hipervisor. Estos métodos eluden los mecanismos internos de integridad de los datos del CSP.
- El único método compatible para migrar FMCv a un nuevo clúster o host es el flujo de trabajo de restauración y copia de seguridad nativa de FMC, combinado con la implementación de una nueva instancia de FMCv en la plataforma de destino.

La estrategia de reversión correcta, si la validación falla después de la transición, es apagar la nueva instancia de FMCv y devolver el FMCv original al servicio. No confíe en los retornos de instantáneas para este fin.

Fase 1: Comprobación de compatibilidad previa a la actualización

Antes de iniciar cualquier actualización de software de FMC, confirme las versiones exactas de software de todos los dispositivos FTD gestionados del entorno.

- FMC 7.4.2 admite la gestión de dispositivos FTD que ejecuten la versión 7.0 y posteriores.
- FMC 7.6.6 admite la gestión de dispositivos FTD que ejecuten la versión 7.1 y posteriores.
- Si algún dispositivo FTD del entorno ejecuta una versión < 7.0, dicho dispositivo debe actualizarse al menos a la versión 7.0 mientras el FMC permanece en la versión 7.3.1, antes de que se actualice el FMC.
- Para el entorno documentado (intervalo FTD: 7.2.8 a 7.4.2), todos los dispositivos gestionados se encuentran dentro del intervalo de compatibilidad tanto para FMC 7.4.2 como para FMC 7.6.6. En este caso no se requiere una preactualización de FTD.

Confirme también lo siguiente antes de continuar:

- El FMC es independiente y no forma parte de un par de alta disponibilidad (HA).
- La versión exacta de VMware ESXi 8.0 se basa en el nuevo clúster (confirmado como ESXi 8.0.3 en este entorno).
- El perfil de recursos de FMCv (vCPU, memoria, disco) cumple los requisitos de la versión de FMC objetivo. La especificación actual de 4 vCPU, 32 GB de RAM y 250 GB de disco debe revisarse con las directrices de implementación actuales, especialmente antes de actualizar a FMC 7.6.6.
- Si la dirección IP y el nombre de host de administración de FMC son los mismos después de la migración (se recomienda encarecidamente evitar la necesidad de actualizaciones de la dirección del administrador en todos los dispositivos FTD administrados).

Fase 2: Actualización de FMCv existente de 7.3.1 a 7.4.2 en el clúster actual de ESXi 7.0

Esta fase actualiza el software FMCv a la versión 7.4.2 mientras permanece en la infraestructura ESXi 7.0 existente. FMCv 7.4.2 añade compatibilidad explícita para VMware ESXi 8.0, que es necesario antes de la migración de la plataforma en la fase 3.

Paso 1: Antes de comenzar la actualización, confirme que no hay implementaciones de políticas pendientes, trabajos de copia de seguridad activos o tareas en segundo plano en ejecución en el FMC.

Paso 2: Realice una copia de seguridad completa de FMC nativa mediante la utilidad de copia de seguridad integrada de FMC. Almacene la copia de seguridad en una ubicación remota y segura fuera de la máquina virtual FMCv. Compruebe que la copia de seguridad se ha realizado correctamente antes de continuar.

Paso 3: Complete todas las comprobaciones de preparación para la actualización como se describe en la guía de planificación de actualización de FMC 7.4. Resuelva los problemas marcados antes de iniciar la actualización.

Paso 4: Actualice el FMCv existente de la versión 7.3.1 a la versión 7.4.2. Utiliza la ruta de transición de actualización admitida: 7,3 → 7,4.

Paso 5: Una vez completada la actualización, realice la validación posterior a la actualización:

- Verifique que todos los dispositivos FTD gestionados se hayan vuelto a conectar al FMC.
- Confirme que la ingestión de eventos está activa y que los eventos aparecen en el FMC.
- Confirme que el estado de la licencia es correcto.
- Ejecute una implementación de directiva de prueba en un dispositivo administrado y confirme que se realiza correctamente.

No continúe con la Fase 3 hasta que todos los pasos de validación posteriores a la actualización se realicen correctamente en el FMCv 7.4.2 actualizado.

Fase 3: Migración de FMCv al clúster VMware ESXi 8.0.3 mediante backup y restauración nativos

Esta fase migra el FMCv del clúster ESXi 7.0 existente al nuevo clúster ESXi 8.0.3. Esto se

consigue mediante la implementación de una nueva instancia de FMCv en el clúster de destino y la restauración de una copia de seguridad de FMC nativa en él. Se conservan la misma dirección IP de administración y el mismo nombre de host para evitar que se requieran cambios en la dirección del administrador en todos los dispositivos FTD administrados.

Paso 1: Una vez que se confirme que FMCv es estable en la versión 7.4.2, genere una nueva copia de seguridad de FMC nativa. Almacénelo en una ubicación remota y segura. Compruebe que la copia de seguridad está completa y es válida antes de continuar.

Paso 2: Implemente una nueva instancia de FMCv en el clúster de ESXi 8.0.3. La versión de software y la compilación de esta nueva instancia deben coincidir exactamente con la versión de FMCv (incluidos los parches y las revisiones) de la que se tomó la copia de seguridad (FMCv 7.4.2). Asegúrese de que la nueva instancia esté configurada con recursos equivalentes o superiores (vCPU, memoria, disco) y que la configuración de red esté en fases, pero que la dirección IP de administración de producción aún no esté asignada a la nueva instancia en este momento.

Paso 3: Restaure la copia de seguridad nativa de FMC en la nueva instancia de FMCv en ESXi 8.0.3.

Paso 4: Antes de poner el nuevo FMCv en línea con la dirección IP y el nombre de host de gestión de producción, apague por completo o desconecte el FMCv original de la red. Este es un paso obligatorio para evitar una condición de IP duplicada y para evitar que dos instancias de FMC intenten comunicarse con los mismos dispositivos FTD administrados simultáneamente.

Durante el período en el que el FMCv original está apagado y antes de que el nuevo FMCv esté en línea, se espera este comportamiento para los dispositivos FTD gestionados:

- Reenvío de tráfico: Los dispositivos FTD operan planos de datos independientemente del FMC y continúan reenviando tráfico sin problemas y aplicando la última política de control de acceso implementada correctamente, excepto en los casos aquí mencionados.
- Cambios en la gestión y visibilidad: Las implementaciones de políticas, los ajustes de configuración, las alertas de estado de FMC y la visibilidad de la gestión de dispositivos no están disponibles en absoluto.
- Almacenamiento en búfer de eventos y posibles pérdidas: Se pausa la visibilidad de eventos en tiempo real en el FMC. Mientras que el FTD intenta registrar los eventos de seguridad y conexión localmente en sus archivos unificados temporales, estos archivos tienen límites de almacenamiento estrictos y funcionan sobre una base de sobrescritura circular. Los registros de conexión de gran volumen se pueden sobrescribir o perder durante una ventana de migración ampliada. Los eventos que permanecen en el búfer local se transmiten al nuevo FMC una vez que está en línea.

- Reglas de malware (AMP): Las solicitudes de búsqueda en la nube en tiempo real de archivos no almacenados en caché no están disponibles temporalmente porque FMC envía estas consultas de reputación a la nube de AMP. El FTD sigue aplicando reglas de bloqueo o permiso sólo para los archivos ya almacenados en su caché de disposición integrada local. Los archivos no almacenados en caché omiten el análisis de la nube y utilizan la configuración de seguridad contra fallos de la política (normalmente no se abre para evitar la interrupción del tráfico). Los envíos de sandboxing a Threat Grid y las alertas retrospectivas se pausan hasta que el nuevo FMC esté operativo.
- Reglas basadas en identidad: Los usuarios que ya han iniciado sesión y están asignados a una dirección IP no experimentan ninguna interrupción, ya que el FTD conserva las asignaciones activas en su memoria local. Sin embargo, dado que FMC actúa como agente para las fuentes de identidad (por ejemplo, Cisco ISE o agentes de Active Directory), el FTD no puede aprender los nuevos inicios de sesión de los usuarios ni los cambios de IP que se produzcan durante esta ventana. Estas sesiones desconocidas vuelven a las reglas predeterminadas o de invitado de su política.
- URL Filtering : Las búsquedas en la nube en directo de sitios web completamente desconocidos no están disponibles temporalmente porque FMC envía proxy de solicitudes de URL desconocidas a la nube de Cisco Talos. El FTD continúa filtrando y aplicando completamente la política solamente para los sitios web que ya se encuentran dentro de su conjunto de datos local transferido o su caché de memoria local activa. El tráfico web que llega a una URL desconocida y sin almacenar en caché omite la clasificación de la nube y coincide con la configuración de reserva de la política para el tráfico sin categorizar (normalmente permitido). Las actualizaciones del paquete de la base de datos de URL se pausan hasta que el nuevo FMC esté en línea.

Paso 5: Asigne la dirección IP y el nombre de host de gestión de producción al FMCv restaurado en ESXi 8.0.3 y conéctelo. Dado que se utilizan la misma dirección IP y el mismo nombre de host, los dispositivos FTD gestionados pueden volver a conectarse al FMC automáticamente sin necesidad de realizar cambios en la dirección del jefe de cada dispositivo FTD.

Paso 6: Realice la validación posterior a la migración:

- Verifique que todos los dispositivos FTD gestionados se hayan vuelto a conectar a la nueva instancia de FMCv.
- Compruebe el estado de las licencias y confirme que todas se han aplicado correctamente.
- Confirme que el flujo de eventos y las integraciones externas funcionan correctamente.
- Ejecute una implementación de políticas controlada en un dispositivo administrado y confirme que se realiza correctamente.

Si la validación falla en algún momento durante esta fase, apague la nueva instancia de FMCv,

restaure el FMCv original en ESXi 7.0 al servicio y solucione los problemas antes de volver a intentar la migración. No utilice una reversión de instantánea de VMware como mecanismo de reversión.

Fase 4: Actualización de FMCv de 7.4.2 a 7.6.6 (después de que la migración se confirme estable)

Una vez que la migración de FMCv a ESXi 8.0.3 se haya validado completamente y se haya confirmado que es estable, se puede considerar realizar una nueva actualización a FMC 7.6.6. Se recomienda encarecidamente no combinar la migración de la plataforma del hipervisor (fase 3) y esta actualización adicional de la versión de FMC en un único evento de mantenimiento. Completar primero la migración proporciona un punto de control limpio y de bajo riesgo antes de continuar.

Antes de iniciar la actualización a 7.6.6, confirme estos requisitos previos:

- Todos los dispositivos FTD gestionados del entorno ejecutan la versión 7.1 o posterior. El FMC 7.6.6 no admite la gestión de dispositivos FTD < versión 7.1. En el entorno documentado (intervalo FTD: 7.2.8 a 7.4.2), todos los dispositivos cumplen este requisito.
- El perfil de recursos de FMCv (4 vCPU, 32 GB de RAM, 250 GB de disco) se ha validado con las directrices de implementación de FMC 7.6.6 para el recuento total de dispositivos gestionados y los requisitos de retención de eventos en este entorno.
- Se confirma la ruta de transición de actualización admitida: 7,4 → 7,6.
- El FMC se confirma como independiente (no forma parte de un par de alta disponibilidad).

Paso 1: Cree y verifique una copia de seguridad de FMC nativa nueva a partir de la instancia estable de FMCv 7.4.2 en ESXi 8.0.3. Guárdela en una ubicación remota y segura.

Paso 2: Actualice el FMCv de la versión 7.4.2 a la versión 7.6.6.

Paso 3: Realice la validación final posterior a la actualización:

- Verifique que todos los dispositivos FTD gestionados se hayan vuelto a conectar al FMC.
- Confirme que la gestión y la ingestión de eventos funcionan correctamente.
- El estado de confirmación de licencia es correcto.

- Ejecute una implementación de políticas controlada para confirmar que la aplicación de políticas se ha realizado correctamente.

Resumen de la ruta de actualización y la secuencia de transición

En la tabla se resume el plan por fases completo, las transiciones de actualización admitidas y la acción clave en cada fase:

Fase	Acción	Versión de FMC	Hipervisor	Transición admitida
Fase 1	Comprobación de compatibilidad previa a la actualización; confirmar versiones de FTD, estado de FMC HA y perfil de recursos	7.3.1 (actual)	ESXi 7.0	N/D: solo preparación
Fase 2	Actualizar el software FMCv; realizar copias de seguridad nativas; validar dispositivos administrados e implementación de políticas	7.3.1 → 7.4.2	ESXi 7.0	7.3 → 7.4 (compatible)
Fase 3	Implementar el nuevo FMCv en ESXi 8.0.3; restaurar copia de seguridad nativa; cortar utilizando el mismo nombre de host/IP; validar	7.4.2 (sin cambio de versión)	ESXi 7.0 → ESXi 8.0.3	Copia de seguridad/restauración nativa: método admitido
Fase 4	Después de que la migración sea estable: actualizar FMCv; validar la conectividad, las licencias, los eventos y las políticas de los dispositivos	7.4.2 → 7.6.6	ESXi 8.0.3	7.4 → 7.6 (compatible)

Consideraciones clave

- Cumplimiento de trayecto de actualización: La secuencia de actualización completa (7.3.1 → 7.4.2 → 7.6.6) utiliza las rutas de transición de actualización FMC compatibles (7.3 → 7.4 y

7.4 → 7.6). No se recomienda omitir versiones intermedias o combinar fases en un único evento.

- Compatibilidad FMC-FTD: FMC 7.6.6 mantiene una compatibilidad de gestión completa con los dispositivos FTD que ejecutan las versiones 7.2.8 a 7.4.2. FMC 7.6 requiere que todos los dispositivos FTD gestionados estén en la versión 7.1 o posterior.
- Transición a la misma dirección IP: El FMCv original debe estar completamente apagado o desconectado de la red antes de que el FMCv de sustitución se conecte con la dirección IP de gestión de producción. Esto evita una condición de IP duplicada y evita que dos centros de administración intenten comunicarse simultáneamente con los mismos dispositivos FTD. Cuando el FMCv restaurado vuelve con la misma dirección IP y el mismo nombre de host, los dispositivos FTD gestionados pueden volver a conectarse sin necesidad de realizar cambios en la dirección del jefe.
- Validación de recursos antes de 7.6.6: El perfil de recursos de FMCv (4 vCPU, 32 GB de RAM, 250 GB de disco) debe revisarse con respecto a las directrices de implementación actuales antes de actualizar a FMC 7.6.6, teniendo en cuenta el recuento total de dispositivos gestionados y los requisitos de retención de eventos para el entorno.
- Verificación de respaldo nativo: En cada fase en la que se lleve a cabo una copia de seguridad de FMC nativa, la copia de seguridad debe verificarse como completa y válida antes de continuar. Las copias de seguridad deben almacenarse en una ubicación remota segura fuera de la máquina virtual FMCv.
- No combine la migración y la actualización: La migración de la plataforma (fase 3) y la posterior actualización de la versión de FMC a la 7.6.6 (fase 4) deben realizarse como eventos de mantenimiento independientes. Esto garantiza la existencia de un punto de control limpio en FMCv 7.4.2 en ESXi 8.0.3 antes de realizar cualquier otro cambio.

Causa

No se trata de un problema de corrección de averías debido a un defecto de software o a un error de configuración. La causa subyacente que requiere esta guía es una combinación de requisitos de compatibilidad de versiones y restricciones de migración de plataformas específicas de Cisco FMCv en VMware:

- Compatibilidad de la versión FMC con FTD 7.4.2: La presencia en el entorno de un dispositivo FTD gestionado que ejecute la versión 7.4.2 requiere que el FMC se actualice a un mínimo de la versión 7.4.2, ya que las versiones anteriores del FMC no pueden gestionar dispositivos FTD en una versión superior a la del FMC en sí.
- Compatibilidad con FMCv para VMware ESXi 8.0: FMCv 7.3.1 no admite VMware ESXi 8.0

como plataforma de hipervisor. El FMCv debe actualizarse a la versión 7.4.2 (o posterior) antes de que pueda implementarse o utilizarse en ESXi 8.0.x. Intentar migrar la VM de FMCv 7.3.1 directamente a ESXi 8.0 sin actualizar primero el software de FMC supone un riesgo de compatibilidad.

- Métodos de migración de VM no compatibles: VMware vMotion, las instantáneas, la clonación y la migración directa de VM no son métodos compatibles para migrar FMCv entre clústeres o versiones de hipervisor. Estos métodos pueden provocar daños en la base de datos, discrepancias de versiones o un estado del sistema no compatible. La única ruta de migración admitida es el flujo de trabajo de restauración y copia de seguridad nativo de FMC combinado con una implementación de FMCv nueva en la plataforma de destino.

Contenido relacionado

- Guía de actualización de Cisco Secure Firewall Management Center, versión 7.4: planificación de actualizaciones y rutas admitidas
- Guía de actualización de Cisco Secure Firewall Management Center, versión 7.6: planificación de actualizaciones y rutas admitidas
- Guía de compatibilidad de Cisco Secure Firewall Management Center (Matriz de compatibilidad de FMC y FTD)
- Cisco Secure Firewall Management Center Nuevas funciones por versión, versión 7.4.2
- Guía De Actualización De Cisco Firepower Management Center: Planificación De Actualizaciones
- Soporte técnico y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).