Aggiornamento di FMCv e migrazione da VMware ESXi 7.0 a ESXi 8.0: Approccio a fasi e best practice

Sommario

Problema

Un amministratore che esegue Firewall Management Center virtual (FMCv) versione 7.3.1 su VMware ESXi 7.0 sta pianificando l'aggiornamento del FMC a una versione più recente supportata e successivamente la migrazione del computer virtuale FMCv a un nuovo cluster VMware ESXi 8.0. Queste preoccupazioni sono state sollevate nel corso di questo sforzo di pianificazione:

- Se è sicuro aggiornare FMCv dalla versione 7.3.1 alla 7.4.2, quindi migrare la VM al cluster ESXi 8.0 prima di eseguire ulteriori aggiornamenti.
- Se esistono problemi o vincoli noti di compatibilità durante la migrazione di un FMCv con versione 7.3.1 o 7.4.2 in un ambiente VMware ESXi 8.0.
- Se VMware vMotion può essere utilizzato per eseguire una migrazione omogenea e basata su IP della macchina virtuale FMCv al nuovo cluster senza creare una nuova istanza della VM.
- Possibilità di utilizzare le snapshot VMware come meccanismo di backup e rollback in caso di errore durante l'aggiornamento o la migrazione.
- Qual è la versione FMC più avanzata per lo scenario esistente dei dispositivi gestiti, che include i dispositivi Firewall Threat Defense (FTD) dalla versione 7.2.8 alla 7.4.2?
- Come evitare conflitti di indirizzi IP durante il trasferimento alla nuova istanza di FMCv sul nuovo cluster mantenendo gli stessi indirizzo IP di gestione e nome host.
- Qual è l'ordine corretto delle operazioni per un piano di aggiornamento e migrazione a fasi che riduca al minimo i rischi e i tempi di inattività?

Ambiente

- Prodotto: FMCv
- Versione corrente del software FMC: 7.3.1
- Piattaforma hypervisor corrente: VMware ESXi 7.0
- Piattaforma hypervisor di destinazione: VMware ESXi 8.0.3 (nuovo cluster)
- Tipo di distribuzione FMC: Standalone (non fa parte di una coppia di disponibilità elevata)
- Dispositivi gestiti: Più dispositivi FTD dalla versione 7.2.8 alla 7.4.2

Risoluzione

L'approccio consigliato per questo ambiente è un piano di aggiornamento e migrazione a fasi. Questo piano separa l'aggiornamento del software FMC, la migrazione della piattaforma dell'hypervisor e gli eventuali aggiornamenti successivi della versione FMC in eventi di manutenzione distinti. Questo approccio riduce i rischi in ogni fase e fornisce chiari punti di rollback. L'utilizzo di VMware vMotion, snapshot, duplicazione o migrazione diretta a livello di VM non è esplicitamente il metodo supportato per la migrazione di FMCv tra cluster o versioni.

Importante: Snapshot VMware, vMotion e duplicazione non supportati per la migrazione FMCv

Prima di procedere con qualsiasi fase di questo piano, è fondamentale comprendere i seguenti vincoli relativi ai metodi di migrazione nativi di VMware:

- Le snapshot VMware non sono un metodo di backup, ripristino o rollback supportato per gli aggiornamenti o le migrazioni FMCv. Il ripristino di una copia istantanea di FMCv su VMware può causare il danneggiamento del database, la mancata corrispondenza degli aggiornamenti della versione e del contenuto o uno stato del sistema non supportato.
- VMware vMotion, la duplicazione e la migrazione diretta delle macchine virtuali tra cluster non sono il metodo supportato per la migrazione di FMCv a una nuova piattaforma hypervisor. Tali metodi ignorano i meccanismi interni di integrità dei dati del CCP.
- L'unico metodo supportato per la migrazione di FMCv a un nuovo cluster o host è il flusso di lavoro di backup e ripristino nativo di FMC, combinato con l'installazione di una nuova istanza di FMCv sulla piattaforma di destinazione.

Se la convalida non riesce dopo il cutover, la strategia di rollback corretta consiste nello spegnere la nuova istanza di FMCv e rimettere in servizio l'istanza originale. Non fare affidamento sui ripristini delle istantanee per questo scopo.

Fase 1: Verifica compatibilità pre-aggiornamento

Prima di avviare un aggiornamento del software FMC, verificare le versioni esatte di tutti i dispositivi FTD gestiti nell'ambiente.

- FMC 7.4.2 supporta la gestione di dispositivi FTD con versione 7.0 e successive.
- FMC 7.6.6 supporta la gestione dei dispositivi FTD con versione 7.1 e successive.
- Se un dispositivo FTD nell'ambiente esegue una versione < 7.0, deve essere aggiornato almeno alla versione 7.0 mentre il FMC rimane sulla versione 7.3.1, prima che il FMC stesso venga aggiornato.
- Per l'ambiente documentato (intervallo FTD: da 7.2.8 a 7.4.2), tutti i dispositivi gestiti rientrano nella gamma di compatibilità sia per FMC 7.4.2 che per FMC 7.6.6. In questo caso non è necessario alcun pre-aggiornamento FTD.

Prima di procedere, confermare anche quanto segue:

- Il CCP è autonomo e non fa parte di una coppia ad alta disponibilità (HA).
- L'esatto VMware ESXi 8.0 si basa sul nuovo cluster (confermato come ESXi 8.0.3 in questo ambiente).
- Il profilo di risorsa FMCv (vCPU, memoria, disco) soddisfa i requisiti per la versione del FMC di destinazione. La specifica corrente di 4 vCPU, 32 GB di RAM e 250 GB di disco deve essere verificata in base alle attuali linee guida per l'installazione, in particolare prima dell'aggiornamento a FMC 7.6.6.
- Se l'indirizzo IP e il nome host di gestione del CCP rimangono gli stessi dopo la migrazione (si consiglia di evitare di richiedere aggiornamenti dell'indirizzo del gestore su tutti i dispositivi FTD gestiti).

Fase 2: Aggiornamento di FMCv esistente dalla versione 7.3.1 alla 7.4.2 sul cluster ESXi 7.0 corrente

Questa fase consente di aggiornare il software FMCv alla versione 7.4.2 mentre rimane sull'infrastruttura ESXi 7.0 esistente. FMCv 7.4.2 aggiunge il supporto esplicito per VMware ESXi 8.0, necessario prima della migrazione della piattaforma nella fase 3.

Passaggio 1: Prima di iniziare l'aggiornamento, verificare che nel FMC non siano in esecuzione distribuzioni di criteri in sospeso, processi di backup attivi o attività in background.

Passaggio 2: Eseguire un backup FMC nativo completo utilizzando l'utilità di backup incorporata di FMC. Archiviare il backup in una posizione remota protetta all'esterno della macchina virtuale FMCv. Verificare che il backup sia stato completato correttamente prima di procedere.

Passaggio 3: Completare tutti i controlli di preparazione all'aggiornamento come documentato nella guida alla pianificazione dell'aggiornamento di FMC 7.4. Risolvere eventuali problemi contrassegnati prima di avviare l'aggiornamento.

Passaggio 4: Aggiornare FMCv esistente dalla versione 7.3.1 alla versione 7.4.2. Verrà utilizzato il percorso di transizione dell'aggiornamento supportato: 7.3 → 7.4.

Passaggio 5: Al termine dell'aggiornamento, eseguire la convalida successiva all'aggiornamento:

- Verificare che tutti i dispositivi FTD gestiti siano stati ricollegati al CCP.
- Confermare che l'acquisizione degli eventi sia attiva e che gli eventi vengano visualizzati nel FMC.
- Confermare che lo stato della licenza sia corretto.
- Eseguire una distribuzione di criteri di test in un dispositivo gestito e confermarne l'esito.

Non passare alla fase 3 finché tutte le fasi di convalida successive all'aggiornamento non sono state completate correttamente in FMCv 7.4.2 aggiornato.

Fase 3: Migrazione di FMCv al cluster VMware ESXi 8.0.3 tramite backup e ripristino nativo

In questa fase viene eseguita la migrazione di FMCv dal cluster ESXi 7.0 esistente al nuovo cluster ESXi 8.0.3. A tale scopo, è necessario distribuire una nuova istanza di FMCv nel cluster di destinazione e ripristinarvi un backup FMC nativo. Vengono mantenuti lo stesso indirizzo IP di

gestione e nome host per evitare di richiedere modifiche all'indirizzo del manager su tutti i dispositivi FTD gestiti.

Passaggio 1: Una volta confermata la stabilità di FMCv nella versione 7.4.2, generare un nuovo backup nativo di FMC. Archiviarlo in un luogo sicuro e remoto. Verificare che il backup sia completo e valido prima di procedere.

Passaggio 2: Distribuire una nuova istanza di FMCv sul cluster ESXi 8.0.3. La versione software e la build di questa nuova istanza devono corrispondere esattamente alla versione di FMCv (incluse patch e aggiornamenti rapidi) da cui è stato eseguito il backup (FMCv 7.4.2). Verificare che la nuova istanza sia configurata con risorse equivalenti o superiori (vCPU, memoria, disco) e che la configurazione di rete sia gestita, ma a questo punto l'indirizzo IP di gestione produzione non è ancora assegnato alla nuova istanza.

Passaggio 3: Ripristinare il backup FMC nativo nella nuova istanza FMCv su ESXi 8.0.3.

Passaggio 4: Prima di mettere in linea il nuovo FMCv con l'indirizzo IP di gestione della produzione e il nome host, spegnere o scollegare completamente il FMCv originale dalla rete. Si tratta di un passaggio obbligatorio per evitare la duplicazione di una condizione IP ed evitare che due istanze del CCP tentino di comunicare contemporaneamente con gli stessi dispositivi FTD gestiti.

Durante il periodo in cui il CCPv originale è spento e prima che il nuovo CCPv sia in linea, è previsto questo comportamento per i dispositivi FTD gestiti:

- Inoltro traffico: I dispositivi FTD gestiscono i piani dati indipendentemente dal FMC e continuano a inoltrare il traffico in modo trasparente e a applicare l'ultima policy di controllo dell'accesso implementata correttamente, ad eccezione dei casi menzionati in questo documento.
- Modifiche alla gestione e alla visibilità: Le distribuzioni di policy, le modifiche alla configurazione, gli avvisi di integrità del FMC e la visibilità della gestione dei dispositivi non sono completamente disponibili.
- Buffering degli eventi e potenziali perdite: La visibilità degli eventi in tempo reale nel CCP è sospesa. Mentre l'FTD tenta di registrare gli eventi di sicurezza e connessione localmente nei propri file unificati temporanei, questi file hanno limiti di archiviazione rigorosi e funzionano su una base di sovrascrittura circolare. I log delle connessioni con volumi elevati possono essere sovrascritti o persi durante una finestra di migrazione estesa. Gli eventi rimanenti nel buffer locale vengono trasmessi al nuovo FMC quando è in linea.
- Regole malware (AMP): Le richieste di ricerca cloud in tempo reale per i file non memorizzati nella cache sono temporaneamente non disponibili perché la console Gestione configurazione server inoltra queste query di reputazione al cloud AMP. L'FTD continua ad

applicare le regole di blocco o di autorizzazione solo per i file già archiviati nella cache locale di disposizione integrata. I file non memorizzati nella cache ignorano l'analisi cloud e utilizzano le impostazioni di sicurezza dagli errori del criterio (in genere l'apertura non riesce per evitare l'interruzione del traffico). Gli invii di sandbox a Threat Grid e gli avvisi retrospettivi vengono sospesi fino a quando il nuovo FMC non è operativo.

- Regole basate sull'identità: Gli utenti che hanno già eseguito il login e che sono mappati a un indirizzo IP non subiscono interruzioni, in quanto l'FTD mantiene i mapping attivi nella sua memoria locale. Tuttavia, poiché il FMC funge da broker per le origini di identità (ad esempio, Cisco ISE o agenti Active Directory), durante questa finestra non è possibile apprendere i nuovi accessi utente o le modifiche IP. Queste sessioni sconosciute ritornano alle regole predefinite o guest del criterio.
- Filtro URL: Le ricerche di siti Web completamente sconosciuti nel cloud live non sono al momento disponibili perché il FMC invia richieste di URL sconosciuti al cloud Cisco Talos. L'FTD continua a filtrare e applicare completamente i criteri solo per i siti Web già trovati nel relativo set di dati locale sottoposto a push o nella relativa cache di memoria locale attiva. Il traffico Web che raggiunge un URL non memorizzato nella cache ignora la classificazione del cloud e corrisponde alle impostazioni di fallback del criterio per il traffico non classificato (in genere consentito). Gli aggiornamenti dei pacchetti del database URL vengono sospesi finché il nuovo FMC non è online.

Passaggio 5: Assegnare l'indirizzo IP e il nome host di gestione della produzione al FMCv ripristinato su ESXi 8.0.3 e metterlo in linea. Poiché vengono utilizzati lo stesso indirizzo IP e lo stesso nome host, i dispositivi FTD gestiti possono riconnettersi automaticamente al CCP senza richiedere modifiche all'indirizzo del gestore sui singoli dispositivi FTD.

Passaggio 6: Convalida post-migrazione:

- Verificare che tutti i dispositivi FTD gestiti siano stati riconnessi alla nuova istanza di FMCv.
- Controllare lo stato delle licenze e verificare che tutte le licenze siano state applicate correttamente.
- Verificare che il flusso di eventi e le eventuali integrazioni esterne funzionino correttamente.
- Eseguire una distribuzione di criteri controllati in un dispositivo gestito e confermarne l'esito.

Se la convalida non riesce in alcun momento durante questa fase, spegnere la nuova istanza di FMCv, ripristinare il FMCv originale su ESXi 7.0 in funzione e risolvere i problemi prima di ritentare la migrazione. Non utilizzare il ripristino delle snapshot VMware come meccanismo di rollback.

Fase 4: Aggiornamento di FMCv dalla versione 7.4.2 alla 7.6.6 (dopo la conferma della stabilità della migrazione)

Una volta che la migrazione da FMCv a ESXi 8.0.3 è stata completamente convalidata e confermata come stabile, è possibile prendere in considerazione un ulteriore aggiornamento a FMC 7.6.6. Si consiglia vivamente di non combinare la migrazione della piattaforma dell'hypervisor (fase 3) con l'aggiornamento della versione FMC aggiuntiva in un unico evento di manutenzione. Il completamento della migrazione fornisce un checkpoint pulito e a basso rischio prima di procedere.

Prima di avviare l'aggiornamento alla versione 7.6.6, verificare i seguenti prerequisiti:

- Ogni dispositivo FTD gestito nell'ambiente esegue la versione 7.1 o successiva. FMC 7.6.6 non supporta la gestione di dispositivi FTD < versione 7.1. Nell'ambiente documentato (intervallo FTD: da 7.2.8 a 7.4.2), tutti i dispositivi soddisfano questo requisito.
- Il profilo delle risorse FMCv (4 vCPU, 32 GB di RAM, 250 GB di disco) è stato convalidato in base alle linee guida di distribuzione di FMC 7.6.6 per il numero totale di dispositivi gestiti e i requisiti di conservazione degli eventi in questo ambiente.
- Il percorso di transizione di aggiornamento supportato è confermato: 7.4 → 7.6.
- Il CCP è confermato come indipendente (non fa parte di una coppia di dispositivi ad alta disponibilità).

Passaggio 1: Creare e verificare un nuovo backup FMC nativo dall'istanza stabile di FMCv 7.4.2 su ESXi 8.0.3. Archiviarlo in una posizione remota e sicura.

Passaggio 2: Aggiornare FMCv dalla versione 7.4.2 alla versione 7.6.6.

Passaggio 3: Convalida finale post-aggiornamento:

- Verificare che tutti i dispositivi FTD gestiti siano stati ricollegati al CCP.
- Verificare che la gestione degli eventi e l'acquisizione degli eventi funzionino correttamente.
- Confermare che lo stato della licenza sia corretto.
- Eseguire una distribuzione di criteri controllata per confermare la corretta esecuzione dell'applicazione dei criteri.

Riepilogo del percorso di aggiornamento e della sequenza di transizione

Nella tabella sono riepilogati il piano di gestione temporanea completo, le transizioni di aggiornamento supportate e l'azione chiave in ogni fase:

Fase	Azione	Versione FMC	Hypervisor	Transizione supportata
Fase 1	Verifica di compatibilità pre-aggiornamento; conferma versioni FTD, stato HA FMC e profilo risorsa	7.3.1 (corrente)	ESXi 7.0	N/D — solo preparazione
Fase 2	Aggiornare il software FMCv; eseguire il backup nativo convalida distribuzione di dispositivi gestiti e criteri	7.3.1 → 7.4.2	ESXi 7.0	7.3 → 7.4 (supportato)
Fase 3	Installazione di un nuovo FMCv su ESXi 8.0.3; ripristino del backup nativo; tagliare usando lo stesso IP/nome host; convalidare	7.4.2 (nessuna modifica della versione)	ESXi 7.0 → ESXi 8.0.3	Backup/ripristino nativo: metodo supportato
Fase 4	Dopo la migrazione è stabile: aggiornare FMCv; convalida connettività dispositivo, licenze, eventi, criteri	7.4.2 → 7.6.6	ESXi 8.0.3	7.4 → 7.6 (supportato)

Considerazioni principali

- Conformità percorso di aggiornamento: La sequenza di aggiornamento completa (7.3.1 → 7.4.2 → 7.6.6) utilizza i percorsi di transizione di aggiornamento FMC supportati (7.3 → 7.4 e 7.4 → 7.6). Non è consigliabile ignorare le versioni intermedie o combinare le fasi in un singolo evento.
- Compatibilità FMC-FTD: FMC 7.6.6 mantiene la piena compatibilità di gestione con i dispositivi FTD che eseguono le versioni da 7.2.8 a 7.4.2. FMC 7.6 richiede che tutti i dispositivi FTD gestiti siano nella versione 7.1 o successive.
- Stesso contatore indirizzi IP: L'FMCv originale deve essere completamente spento o

disconnesso dalla rete prima che l'FMCv sostitutivo venga portato in linea con l'indirizzo IP di gestione della produzione. In questo modo si evita che si verifichino condizioni IP duplicate e che due centri di gestione tentino contemporaneamente di comunicare con gli stessi dispositivi FTD. Quando l'FMCv ripristinato viene restituito con lo stesso indirizzo IP e nome host, i dispositivi FTD gestiti possono riconnettersi senza richiedere modifiche all'indirizzo del manager.

- Convalida delle risorse prima della versione 7.6.6: Il profilo delle risorse FMCv (4 vCPU, 32 GB di RAM, 250 GB di disco) deve essere esaminato in base alle attuali linee guida per l'installazione prima di eseguire l'aggiornamento a FMC 7.6.6, tenendo conto del numero totale di dispositivi gestiti e dei requisiti di conservazione degli eventi per l'ambiente.
- Verifica backup nativo: In ogni fase in cui viene eseguito un backup FMC nativo, il backup deve essere verificato come completo e valido prima di procedere. I backup devono essere archiviati in una posizione remota protetta all'esterno della macchina virtuale FMCv.
- Non combinare migrazione e aggiornamento: La migrazione della piattaforma (fase 3) e il successivo aggiornamento della versione FMC alla versione 7.6.6 (fase 4) devono essere eseguiti come eventi di manutenzione separati. Ciò garantisce l'esistenza di un punto di controllo pulito a FMCv 7.4.2 su ESXi 8.0.3 prima di apportare ulteriori modifiche.

Causa

Non si tratta di un problema di correzione dell'errore causato da un difetto del software o da una configurazione errata. La causa alla base di questa guida è una combinazione di requisiti di compatibilità delle versioni e vincoli di migrazione della piattaforma specifici per Cisco FMCv su VMware:

- Compatibilità della versione FMC con FTD 7.4.2: La presenza nell'ambiente di un dispositivo FTD gestito che esegue la versione 7.4.2 richiede l'aggiornamento del CCP almeno alla versione 7.4.2, poiché le versioni precedenti del CCP non possono gestire i dispositivi FTD con una versione superiore rispetto al CCP stesso.
- Supporto FMCv per VMware ESXi 8.0: FMCv 7.3.1 non supporta VMware ESXi 8.0 come piattaforma hypervisor. Prima di poter essere installato o utilizzato su ESXi 8.0.x, è necessario aggiornare FMCv alla versione 7.4.2 o successive. Il tentativo di eseguire la migrazione della VM di FMCv 7.3.1 direttamente a ESXi 8.0 senza prima aggiornare il software FMC comporta un rischio di compatibilità.
- Metodi di migrazione delle macchine virtuali non supportati: VMware vMotion, le istantanee, la duplicazione e la migrazione diretta delle VM non sono metodi supportati per la migrazione di FMCv tra cluster o versioni di hypervisor. Questi metodi possono causare il danneggiamento del database, la mancata corrispondenza delle versioni o uno stato del

sistema non supportato. L'unico percorso di migrazione supportato è il flusso di lavoro di backup e ripristino nativo di FMC combinato con una nuova distribuzione di FMCv sulla piattaforma di destinazione.

Contenuto correlato

- Guida all'aggiornamento di Cisco Secure Firewall Management Center, versione 7.4 — Pianificazione degli aggiornamenti e percorsi supportati
- Guida all'aggiornamento di Cisco Secure Firewall Management Center, versione 7.6 — Pianificazione degli aggiornamenti e percorsi supportati
- Guida alla compatibilità di Cisco Secure Firewall Management Center (FMC e matrice di compatibilità FTD)
- Cisco Secure Firewall Management Center - Nuove funzionalità per versione - versione 7.4.2
- Guida all'aggiornamento di Cisco Firepower Management Center - Pianificazione degli aggiornamenti
- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).