升級FMCv並從VMware ESXi 7.0遷移到ESXi 8.0:分階段方法和最佳實踐

目錄

問題

在VMware ESXi 7.0上運行防火牆管理中心虛擬(FMCv)版本7.3.1的管理員計畫將FMC升級到受支援的更高版本，然後將FMCv虛擬機器遷移到新的VMware ESXi 8.0群集。在規劃工作期間提出了以下問題：

- 先將FMCv從7.3.1升級到7.4.2，然後將VM遷移到ESXi 8.0群集是否安全，然後再執行任何進一步的升級。
- 將運行版本7.3.1或7.4.2的FMCv遷移到VMware ESXi 8.0環境時，是否存在已知的相容性問題或限制。
- 是否可以使用VMware vMotion來執行FMCv虛擬機器到新群集的無縫、相同IP遷移，而不建立新的VM例項。
- 在升級或遷移失敗時，是否可以將VMware快照用作備份和回滾機制。
- 最高支援的FMC版本適用於現有受管裝置環境，包括防火牆威脅防禦(FTD)裝置（從7.2.8版到7.4.2版）。
- 如何在切換到新群集上的新FMCv例項時避免IP地址衝突，同時保持相同的管理IP地址和主機名。
- 正確的操作順序是分階段升級和遷移計畫，以最大程度降低風險和停機時間。

環境

- 產品:FMCv
- 當前FMC軟體版本：7.3.1
- 當前虛擬機器監控程式平台：VMware ESXi 7.0

- 目標虛擬機器監控程式平台：VMware ESXi 8.0.3（新群集）
- FMC部署型別：獨立（不是高可用性對的一部分）
- 受管裝置：多個FTD裝置，範圍從7.2.8版到7.4.2版

解析

針對此環境的推薦方法是分階段、分階段的升級和遷移計畫。此計畫將FMC軟體升級、虛擬機器監控程式平台遷移以及任何後續的FMC版本升級分為不同的維護事件。此方法可降低每個階段的風險，並提供明確的回滾點。使用VMware vMotion、快照、克隆或直接的VM級遷移顯然不是在群集或版本之間遷移FMCv的支持方法。

重要：FMCv遷移不支援VMware快照、vMotion和克隆

在繼續本計畫的任何階段之前，必須瞭解有關VMware本機遷移方法的這些限制：

- 對於FMCv升級或遷移，VMware快照不是受支援的備份、還原或回滾方法。將FMCv還原為VMware快照可能會導致資料庫損壞、版本和內容更新不匹配，或系統狀態不受支援。
- VMware vMotion、克隆和群集之間的直接虛擬機器遷移不支援將FMCv遷移到新的虛擬機器監控程式平台。這些方法繞過FMC的內部資料完整性機制。
- 將FMCv遷移到新群集或主機的唯一受支援的方法是FMC本機備份和還原工作流，以及在目標平台上部署新的FMCv例項。

如果轉換後驗證失敗，正確的回滾策略是關閉新的FMCv例項並將原始FMCv恢復為服務。不要依賴快照還原來實現此目的。

第1階段：升級前相容性檢查

在啟動任何FMC軟體升級之前，請確認環境中所有受管FTD裝置的確切軟體版本。

- FMC 7.4.2支援對運行7.0及更高版本的FTD裝置進行管理。

- FMC 7.6.6支援對運行7.1及更高版本的FTD裝置進行管理。
- 如果環境中的任何FTD裝置執行的版本低於7.0，則該裝置必須至少升級到7.0版，同時FMC仍保留在7.3.1版上，然後升級FMC本身。
- 對於已記錄環境(FTD範圍：7.2.8到7.4.2)，所有受管裝置都在FMC 7.4.2和FMC 7.6.6的相容性範圍內。在這種情況下，不需要FTD預升級。

在繼續操作之前，請確認以下內容：

- FMC是獨立的，不屬於高可用性(HA)對。
- 在新群集上構建的精確VMware ESXi 8.0（在此環境中已確認為ESXi 8.0.3）。
- FMCv資源配置檔案（vCPU、記憶體、磁碟）滿足目標FMC版本的要求。必須根據當前的部署指南檢查當前的4個vCPU、32 GB RAM和250 GB磁碟規格，尤其是在升級到FMC 7.6.6之前。
- 遷移後FMC管理IP地址和主機名是否保持不變（強烈建議避免在所有受管FTD裝置上要求管理員地址更新）。

第2階段：將當前ESXi 7.0群集上的現有FMCv從7.3.1升級到7.4.2

此階段將FMCv軟體升級到版本7.4.2，同時它仍保留在現有的ESXi 7.0基礎架構上。FMCv 7.4.2新增了對VMware ESXi 8.0的明確支援，這是在第3階段的平台遷移之前需要的。

步驟 1:在開始升級之前，請確認當前在FMC上未運行任何掛起的策略部署、活動備份作業或後台任務。

步驟 2:使用FMC內建備份實用程式執行完全本機FMC備份。將備份儲存在FMCv虛擬機器之外的安全遠端位置。在繼續操作之前，驗證備份是否成功完成。

步驟 3:完成FMC 7.4升級計畫指南中記錄的所有升級準備情況檢查。在啟動升級之前解決任何已標籤的問題。

步驟 4:將現有FMCv從版本7.3.1升級到版本7.4.2。這將使用支援的升級轉換路徑：7.3 → 7.4。

步驟 5:升級完成後，執行升級後驗證：

- 驗證所有受管FTD裝置是否已重新連線到FMC。

- 確認事件接收處於活動狀態且事件顯示在FMC中。
- 確認許可狀態正確。
- 對受管裝置執行測試策略部署並確認成功。

在升級的FMCv 7.4.2上成功通過所有升級後驗證步驟之前，不要進入第3階段。

第3階段：使用本機備份和還原將FMCv遷移到VMware ESXi 8.0.3群集

此階段將FMCv從現有的ESXi 7.0群集遷移到新的ESXi 8.0.3群集。通過在目標群集上部署新的FMCv例項並將本機FMC備份還原到該例項上，即可完成此操作。系統會保留相同的管理IP地址和主機名，以避免要求所有託管FTD裝置上的管理器地址發生更改。

步驟 1:在7.4.2版上確認FMCv穩定後，生成新的本機FMC備份。將其儲存在安全的遠端位置。在繼續之前，驗證備份是否完整有效。

步驟 2:在ESXi 8.0.3群集上部署新的FMCv例項。此新例項的軟體版本和內部版本必須與從中進行備份的FMCv(FMCv 7.4.2)的版本完全匹配（包括修補程式和修補程式）。 確保新例項配置了等效資源或更高資源（vCPU、記憶體、磁碟），並且網路配置是暫存的，但此時尚未將生產管理IP地址分配給新實例。

步驟 3:將本機FMC備份還原到ESXi 8.0.3上的新FMCv例項上。

步驟 4:在將新FMCv與生產管理IP地址和主機名聯機之前，請完全關閉原始FMCv或將其斷開網路。這是防止重複IP條件和避免兩個FMC例項嘗試同時與相同的受管FTD裝置通訊的強制步驟。

在原始FMCv關閉電源且新的FMCv聯機之前，受管FTD裝置的預期行為如下：

- 流量轉發：FTD裝置獨立於FMC運作資料平面，並繼續無縫轉送流量和執行上一次成功部署的存取控制原則（此處提到的案例除外）。
- 管理和可視性變更：策略部署、配置調整、FMC運行狀況警報和裝置管理可視性完全不可用。
- 事件緩衝和潛在損失：FMC的即時事件可視性暫停。當FTD嘗試在其臨時整合檔案中本地記錄安全和連線事件時，這些檔案具有嚴格的儲存限制，並以循環覆寫方式運作。在擴展遷移期間，高容量連線日誌可能會被覆蓋或丟失。在新的FMC聯機後，本地緩衝區中剩餘的事件將

流式傳輸到新的FMC。

- 惡意軟體(AMP)規則：未快取檔案的即時雲查詢請求暫時不可用，因為FMC將這些信譽查詢代理到AMP雲。FTD會繼續只對已儲存在其本機機上部署快取中的檔案執行封鎖或允許規則。未快取的檔案繞過雲分析並使用策略的故障安全設定（通常無法開啟以防止流量中斷）。 在新的FMC運行之前，暫停向Threat Grid提交沙盒和追溯警報。
- 基於身份的規則：已登入並對映到IP地址的使用者不會遇到中斷，因為FTD在其本地記憶體中保留活動對映。但是，由於FMC充當身份源（例如，思科ISE或Active Directory代理）的代理，因此FTD無法獲知此視窗期間的新使用者登入或IP更改。這些未知會話將回退到策略的預設或訪客規則。
- URL篩選：完全未知網站的即時雲查詢暫時不可用，因為FMC將未知URL請求代理到Cisco Talos雲。FTD將繼續完全篩選和強制執行策略，只對已在其推送的本地資料集或其活動的本地記憶體快取中找到的網站執行策略。命中未快取的未知URL的Web流量會繞過雲分類，並匹配未分類流量的策略回退設定（通常允許）。URL資料庫包更新暫停，直到新的FMC聯機。

步驟 5:將生產管理IP地址和主機名分配給ESXi 8.0.3上已恢復的FMCv並使其聯機。由於使用相同的IP位址和主機名稱，因此受管FTD裝置可以自動重新連線到FMC，而無需在單個FTD裝置上進行管理員位址變更。

步驟 6:執行遷移後驗證：

- 驗證所有受管FTD裝置是否已重新連線到新的FMCv例項。
- 檢查許可狀態並確認所有許可證已正確應用。
- 確認事件流和任何外部整合均正常運行。
- 對受管裝置執行受控策略部署並確認成功。

如果驗證在此階段的任何時候失敗，請關閉新的FMCv例項，將ESXi 7.0上的原始FMCv還原為服務，並在重新嘗試遷移之前進行故障排除。請勿將VMware快照還原用作回滾機制。

第4階段：將FMCv從7.4.2升級到7.6.6（遷移確認穩定後）

FMCv到ESXi 8.0.3的遷移經過完全驗證且確認穩定後，可以考慮進一步升級到FMC 7.6.6。強烈建議不要將管理程式平台遷移（第3階段）和此附加FMC版本升級結合到單個維護事件中。完成遷移首先提供一個乾淨、低風險的檢查點，然後繼續操作。

開始升級到7.6.6之前，請確認以下前提條件：

- 環境中的每個託管FTD裝置都運行版本7.1或更高版本。FMC 7.6.6不支援管理<版本7.1的FTD裝置。在文檔環境(FTD範圍：7.2.8至7.4.2)，所有裝置均符合此要求。
- FMCv資源配置檔案（4個vCPU、32 GB RAM和250 GB磁碟）已根據FMC 7.6.6部署指南進行驗證，以瞭解此環境中的受管裝置總數和事件保留要求。
- 支援的升級轉換路徑已確認：7.4 → 7.6。
- FMC被確認為獨立（不是高可用性對的一部分）。

步驟 1:從ESXi 8.0.3上穩定的FMCv 7.4.2例項建立並驗證新的本機FMC備份。將其儲存在安全的遠端位置。

步驟 2:將FMCv從版本7.4.2升級到版本7.6.6。

步驟 3:執行最終升級後驗證：

- 驗證所有受管FTD裝置是否已重新連線到FMC。
- 確認事件處理和事件接收是否正常工作。
- 確認許可狀態正確。
- 執行受控策略部署以確認策略應用成功。

升級路徑和過渡順序摘要

該表彙總了完整的階段計畫、支援的升級過渡以及每個階段的關鍵操作：

Phase	動作	FMC版本	虛擬機器監控程式	支援的過渡
第1階段	升級前相容性檢查；確認FTD版本、FMC HA狀態和資源設定檔	7.3.1（當前）	ESXi 7.0	不適用 — 僅準備
第2階段	升級FMCv軟體；執行本機備份；驗證受管裝置和策略部署	7.3.1 → 7.4.2	ESXi 7.0	7.3 → 7.4（支援）
第3階段	在ESXi 8.0.3上部署新的FMCv;恢復本機備份；使用相同的IP/主機名進行切換；驗證	7.4.2（無版本更改）	ESXi 7.0→ESXi	本機備份/恢復 — 支援的方法

			8.0.3	
第4階段	遷移穩定後：升級FMCv;驗證裝置連線、許可、事件、策略	7.4.2 → 7.6.6	ESXi 8.0.3	7.4 → 7.6（支援）

主要考慮因素

- 升級路徑合規性：完整的升級序列(7.3.1 → 7.4.2 → 7.6.6)使用支援的FMC升級過渡路徑(7.3 → 7.4和7.4 → 7.6)。 不建議跳過中間版本或將階段組合到單個事件中。
- FMC-FTD相容性：FMC 7.6.6與運行7.2.8至7.4.2版的FTD裝置保持完全管理相容性。FMC 7.6要求所有託管FTD裝置都為7.1版或更高版本。
- 相同的IP地址轉換：在使用生產管理IP地址將替代FMCv聯機之前，必須完全關閉原始FMCv的電源或者將其從網路斷開。這可防止重複IP情況，並可避免兩個管理中心同時嘗試與同一FTD裝置通訊。當還原的FMCv返回相同的IP地址和主機名時，託管的FTD裝置可以重新連線，而無需更改管理器地址。
- 7.6.6之前的資源驗證：在升級到FMC 7.6.6之前，必須根據當前的部署指南審查FMCv資源配置檔案（4個vCPU、32 GB RAM、250 GB磁碟），同時考慮環境的受管裝置總數和事件保留要求。
- 本機備份驗證：在執行本機FMC備份的每個階段，必須先驗證備份是否完整有效，然後才能繼續。備份必須儲存在FMCv虛擬機器之外的安全的遠端位置。
- 不要將遷移和升級結合起來：平台遷移（第3階段）和後續FMC版本升級到7.6.6（第4階段）必須作為單獨的維護事件執行。這可確保ESXi 8.0.3上的FMCv 7.4.2存在乾淨的檢查點，然後進行任何進一步的更改。

原因

這不是由軟體缺陷或配置錯誤導致的中斷修復問題。需要本指南的根本原因是版本相容性要求與VMware上思科FMCv特有的平台遷移限制相結合：

- FMC版本與FTD 7.4.2的相容性：環境中存在運行版本7.4.2的受管FTD裝置需要將FMC升級到版本7.4.2的最低版本，因為早期的FMC版本無法管理版本高於FMC本身的FTD裝置。
- 適用於VMware ESXi 8.0的FMCv支援：FMCv 7.3.1不支援將VMware ESXi 8.0用作虛擬機器監控程式平台。FMCv必須先升級到7.4.2版（或更高版本），然後才能在ESXi 8.0.x上部署或

操作。嘗試將FMCv 7.3.1 VM直接遷移到ESXi 8.0而不首先升級FMC軟體會導致相容性風險。

- 不受支援的VM遷移方法：不支援在群集或虛擬機器監控程式版本之間遷移FMCv的VMware vMotion、快照、克隆和直接虛擬機器遷移方法。這些方法可能會導致資料庫損壞、版本不匹配或系統狀態不受支援。唯一支援的遷移路徑是FMC本機備份和還原工作流程，以及目標平台上的新FMCv部署。

相關內容

- Cisco Secure Firewall Management Center升級指南7.4版 — 升級規劃和支援的路徑
- Cisco Secure Firewall Management Center升級指南7.6版 — 升級規劃和支援的路徑
- 思科安全防火牆管理中心相容性指南（FMC和FTD相容性矩陣）
- Cisco Secure Firewall Management Center 7.4.2版新功能
- 思科Firepower管理中心升級指南 — 升級規劃
- 思科技術支援與下載

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。