

使用安全雲控制將本地FMC遷移到雲(cdFMC)

目錄

[問題](#)

[環境](#)

[解析](#)

[原因](#)

[相關內容](#)

- [問題](#)
 - [環境](#)
 - [解析](#)
 - [原因](#)
 - [相關內容](#)
-

問題

使用者需要幫助，才能將其生產防火牆管理中心(FMCv300)虛擬裝置遷移到安全雲控制(SCC)租戶中的雲交付的FMC(cdFMC)。具體關注事項包括：

- 瞭解遷移過程的哪些部分可能會導致停機，以及如何將生產影響降至最低。
- 獲取遷移工作流的逐步指導。
- 確定遷移完成後如何處理FMCv300。
- 為高可用性(HA)配置中的多個防火牆威脅防禦(FTD)裝置規劃分階段遷移方法。
- 明確在觸發遷移嚮導之前，是否必須手動將本地FMC配置匯入到cdFMC。

環境

- 來源FMC:FMCv300虛擬裝置，版本7.6.5。還可以部署其他硬體(HW)和軟體(SW)平台。
- 目標：cdFMC租戶已調配。

- 受管裝置是來自不同硬體和軟體版本的FTD，例如：
 - 2個安全防火牆3130,FTD 7.6.4，配置在HA對中。
 - 2個Firepower 2130,FTD 7.4.4，配置在HA對中。
 - 1個FTDv in Azure 7.6.4，獨立配置。

解析

遷移先決條件和版本驗證

環境版本滿足遷移到cdFMC的先決條件：

- FMC 7.6.5符合遷移工作流的書面最低要求。
- FTD版本7.6.4和7.4.4滿足已記錄的最低遷移要求。
- cdFMC支援環境中的FTD發佈系列。

遷移前驗證步驟

開始遷移之前，請確認以下前提條件：

- FMCv300上沒有掛起的部署。
- 兩個HA對都正常且已同步。
- FMCv300備份已完成。
- 足夠FMC磁碟空間（至少10%的可用空間）。
- 從FTD管理路徑執行的DNS解析。
- 允許通過所需的雲管理埠（TCP 443和TCP 8305）從FTD管理介面到cdFMC的出站連線。
- FMCv300具有對SCC的出站HTTPS訪問許可權。

配置匯入流程

運行遷移嚮導之前，無需手動將本地FMCv300配置匯入到cdFMC中。「將FTD遷移到cdFMC」工作流程將配置匯入作為遷移作業的一部分：

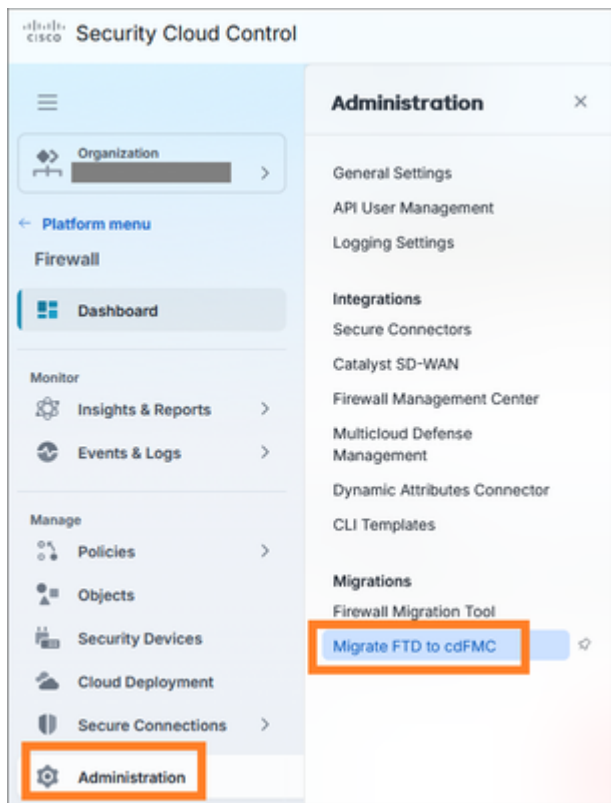
1. SCC連線到內部的FMCv300。
2. 它從本地FMC匯出相關配置。
3. 它將共用策略/對象匯入到cdFMC中。
4. 匯入裝置特定的配置，例如介面和路由。
5. 它將選定的FTD裝置註冊到cdFMC。
6. 14天的評估期在遷移完成後開始。

如果在遷移前在cdFMC中手動建立策略或對象，且其名稱與FMCv300上的專案相同，則遷移工作流程可以使用現有的cdFMC專案，而不是匯入本地版本，這會導致意外的結果。

推薦的遷移順序

第1階段：預遷移設定

1. 在您的SCC租戶中部署cdFMC。
2. 將當前FMCv300安裝到SCC。
3. 確認cdFMC的智慧許可。
4. 從Firewall > Administration > Migrations > Migrate FTD to cdFMC啟動遷移工作流：



5. 使用選項在共用策略匯入後暫停以供審閱：

 **Security Cloud Control**

Migrate FTD to cdFMC

Migrate FTD from On-Prem FMC to cloud

Organization

Platform menu

Firewall

Dashboard

Monitor

Insights & Reports

Events & Logs

Manage

Policies

Objects

Security Devices

Cloud Deployment

Secure Connections

Administration

Platform services

Favorites

Security Devices

Platform Management

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

☐	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

第2階段：遷移執行

在維護時段內，使用分階段的方法遷移裝置：

1. 從獨立FTD開始（影響最小）。
2. 遷移第一個HA配對。
3. 驗證裝置運行狀況和功能。
4. 遷移第二個HA對。

第3階段：遷移後驗證

遷移每個裝置或HA對之後：

1. 在cdFMC中確認裝置運行狀況。
2. 確認適用的HA狀態。
3. 檢視部署預覽/警告。
4. 從cdFMC部署。
5. 驗證流量和事件可視性。

包含配置凍結的三階段遷移計畫

推薦的方法包括分三個階段執行FTD遷移，每個階段分別在不同的日期執行，每個階段最少進行三天的轉換後監控。此方法降低了風險並提供了驗證時間：

- 來自cdFMC的策略部署。
- 裝置運行狀況狀態。
- 兩個HA對的HA狀態。
- 雲中的事件/分析可視性。
- 進入下一階段之前出現的任何操作問題。

配置凍結實施

使用以下方法在遷移/評估期間實施配置凍結：

- 最佳選擇：凍結跨FMCv300和cdFMC的所有FTD相關配置更改，直到驗證和提交每個階段為止。
- 最小值選項：凍結要遷移的裝置以及已遷移和非遷移裝置所使用的任何共用策略/對象。
- 避免在分階段遷移期間在FMCv300和cdFMC中編輯相同的共用策略/對象。
- 避免在評估期間發生重大變化。

緊急變更流程

對於遷移期間的緊急更改：

- 僅將更改應用於該裝置的當前授權管理器：
 - 尚未遷移的裝置：FMCv300。
 - 已遷移的裝置：cdFMC。
- 記錄更改、受影響的策略/對象、時間戳和裝置範圍。
- 在階段完成之後協調更改，尤其是當更改影響共用對象或共用策略時。

評估期管理

14天評估視窗的重要注意事項：

- 跟蹤每個遷移階段/作業的14天評估視窗。
- 請勿讓任何階段無意中達到自動提交。
- 如果三天監視成功，請手動提交該階段，而不是等待完整的14天。

FMCv300停用程式

遷移裝置後，請勿立即關閉或移除FMCv300。保持FMCv300可用，直到：

- 所有FTD裝置均成功遷移。
- cdFMC部署成功。
- 雲分析/事件已確認。
- 遷移已提交。
- 滿足任何日誌/事件保留要求。
- 根據組織策略保留最終FMCv300備份。

在滿足這些條件後，FMCv300可以按照標準虛擬機器淘汰流程從活動使用中移除和停用。

原因

這是從本地FMC到cdFMC的計畫遷移。遷移的驅動因素是需要利用基於雲的管理功能並停用現有的FMCv300虛擬裝置。

相關內容

- [將FTD移轉到cdFMC - Cisco檔案](#)
- [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）。