

# 在FMC上配置高可用性

## 目錄

---

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[開始之前](#)

[設定](#)

[配置輔助FMC](#)

[配置主FMC](#)

[驗證](#)

---

## 簡介

本檔案介紹防火牆管理中心(FMC)上的高可用性(HA)組態範例。

## 必要條件

### 需求

本文件沒有特定需求。

### 採用元件

本文檔中的資訊基於Secure FMC for VMware v7.2.5。

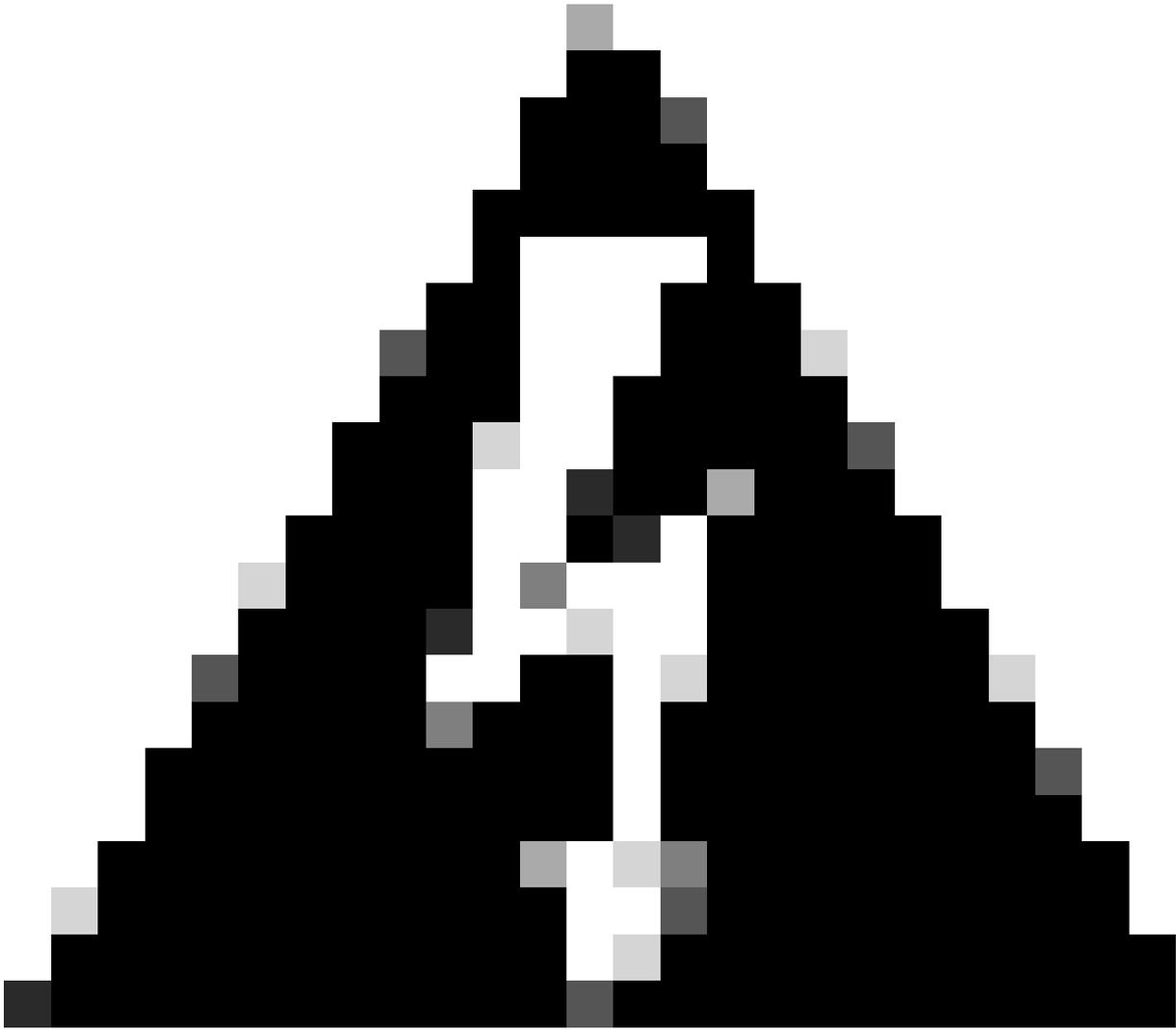
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除 ( 預設 ) 的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

## 背景資訊

本文檔的具體要求包括：

- 兩個FMC對等體必須位於相同的軟體版本、入侵規則更新、漏洞資料庫和輕量級安全包中
- 兩個FMC對等體必須具有相同的容量或硬體版本
- 兩個FMC都需要單獨的許可證

有關全套要求，請訪問[管理指南](#)。



警告：如果列出的要求不匹配，則無法配置HA。

---

所有硬體裝置都支援此過程。

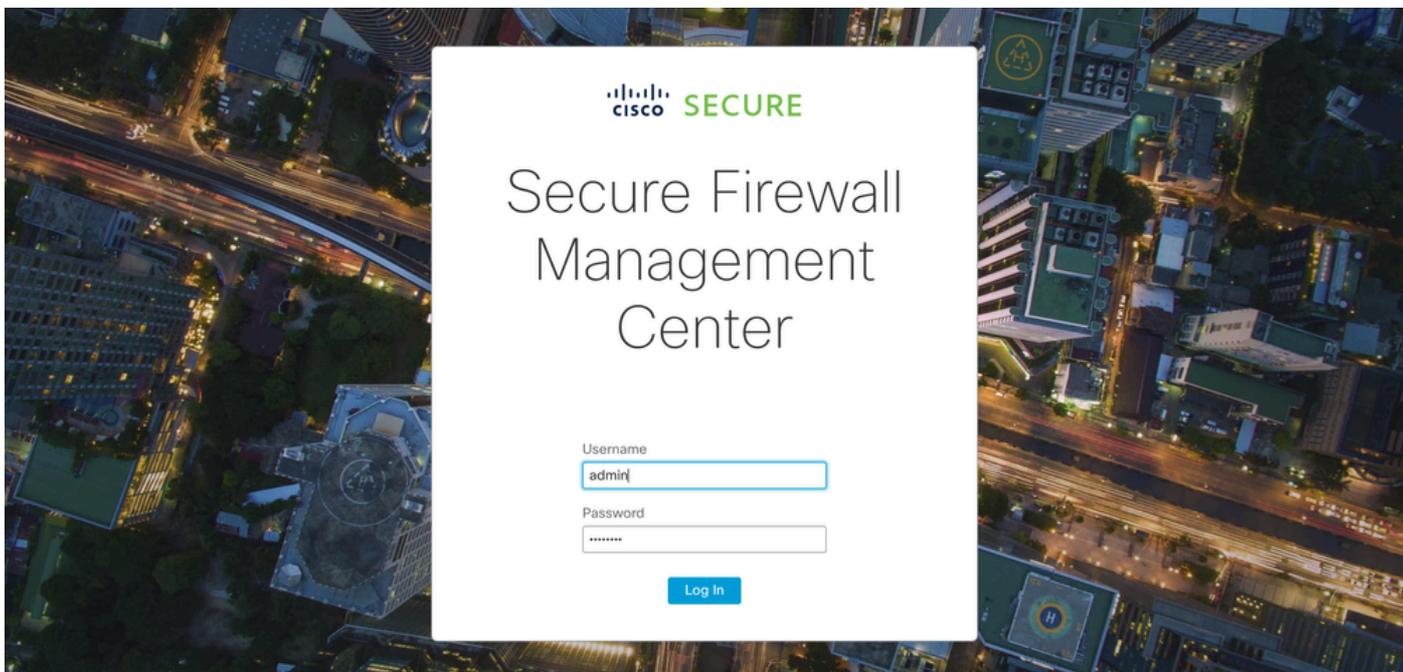
## 開始之前

- 確保對兩個FMC的管理員訪問許可權
- 確保管理介面之間的連線
- 請花點時間檢查軟體版本，並確保完成所有必要的升級

## 設定

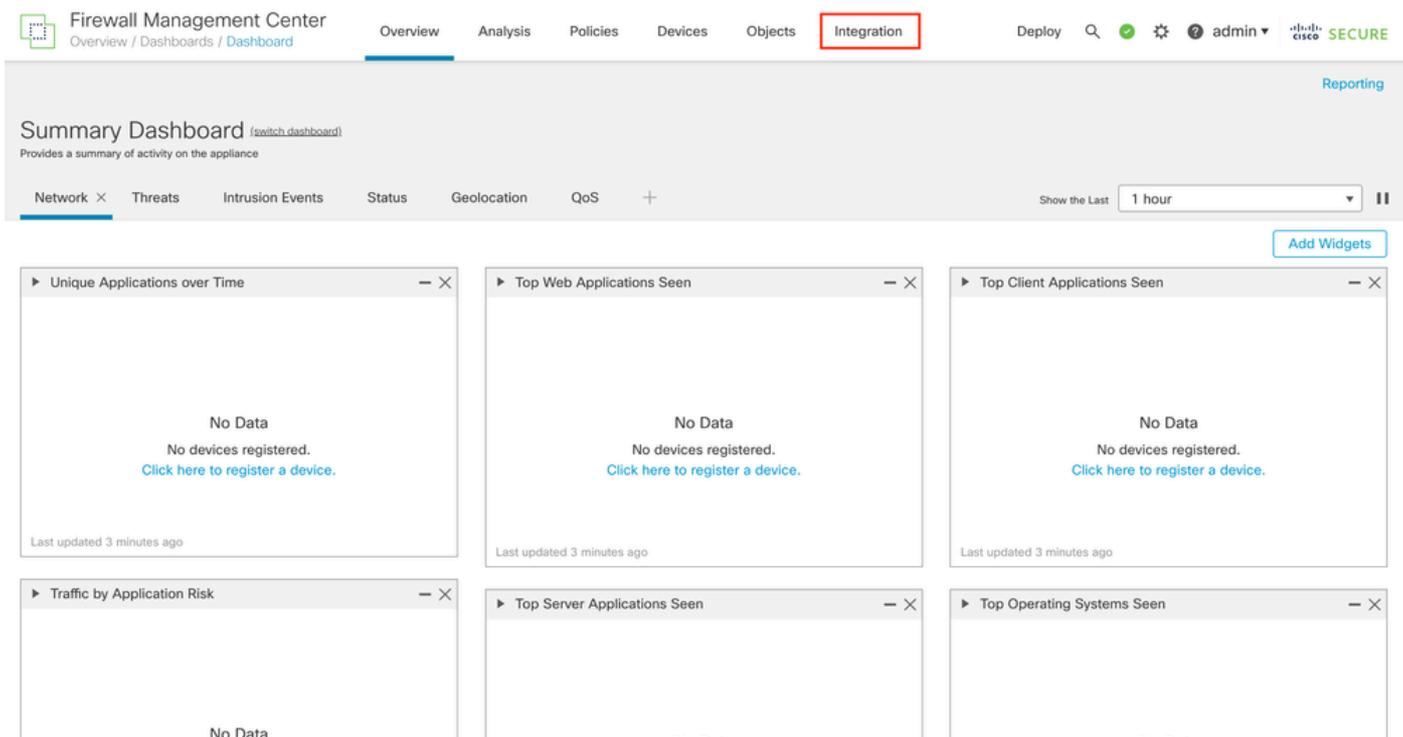
### 配置輔助FMC

步驟1.登入到將扮演輔助/備用角色的FMC裝置的圖形使用者介面(GUI)。



登入到FMC

步驟2.定位至「集成」標籤。



導航到整合

步驟3.按一下Other Integrations。

## SecureX

Security Analytics &amp; Logging

Other Integrations

## AMP

AMP Management

Dynamic Analysis Connections

## Intelligence

Incidents

Sources

Elements

Settings

導航到其他整合

步驟4. 定位至高可用性標籤。



## Firewall Management Center

Integration / Other Integrations / Cloud Services

Overview

Analysis

Policies

Devices

Objects

Integration

Cloud Services

Realms

Identity Sources

High Availability

eStreamer

Host Input Client

Smart Software Manager On-Prem

導航至高可用性

步驟5. 按一下Secondary。



## Firewall Management Center

Integration / Other Integrations / High Availability

Overview

Analysis

Policies

Devices

Objects

Integration

Deploy

🔍

✔

⚙️

❓

admin ▾

cisco SECURE

Cloud Services

Realms

Identity Sources

High Availability

eStreamer

Host Input Client

Smart Software Manager On-Prem

Peer Manager

Select a role for this Management Center and specify peer details to setup high availability.

Role For This Firewall Management Center:

Standalone (No High Availability)

Primary

Secondary

輸入資訊並為當前FMC選擇所需角色

步驟6. 輸入主/主對等體的資訊，然後單Register擊。

Select a role for this Management Center and specify peer details to setup high availability.

Role For This Firewall Management Center:

- Standalone (No High Availability)
- Primary
- Secondary

Peer Details:

After Firewall Management Center high availability is configured in virtual or cloud environment, each registered Firewall Threat Defense consumes an additional Firepower MCv Device license.

Primary Firewall Management Center Host:

Registration Key\*:

Unique NAT ID:

**Register**

† Either host or NAT ID is required.

附註：請注意註冊金鑰，因為它將用於活動的FMC。

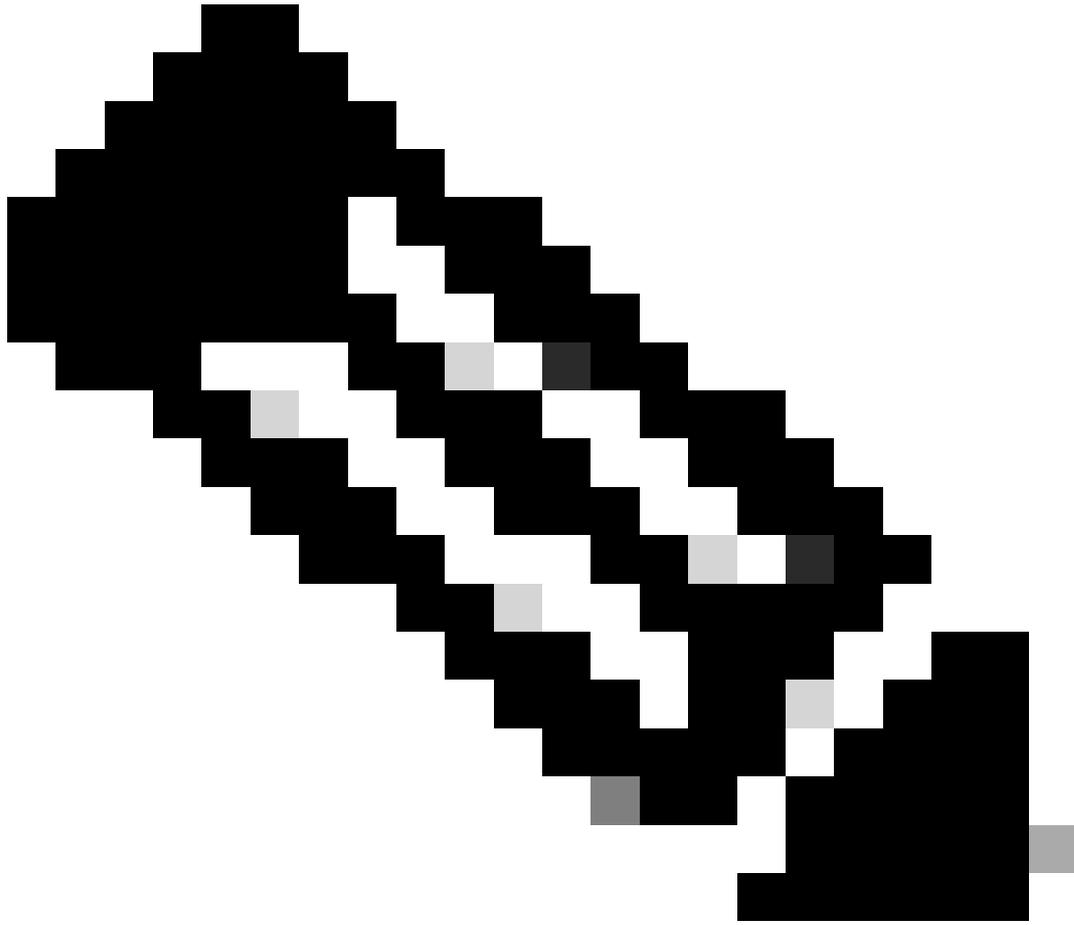
步驟7.此警告要求您確認，按一下 Yes.

## Warning

This operation may affect critical processes running in the background. Do you want to continue?

No

Yes



附註：在建立HA時，GUI將重新啟動，確保沒有其它任務正在運行。

---

步驟8.確認您要註冊主要對等體。

## Warning

---

Do you want to register primary peer:  
10.18.19.31?

No

Yes



警告：一旦建立HA，裝置/策略/配置的所有資訊將從輔助FMC中刪除。

步驟9. 檢驗輔助FMC狀態是否為「掛起」。

Firewall Management Center  
Integration / Other Integrations / Peer Manager

Overview Analysis Policies Devices Objects Integration Deploy 🔍 🟢 ⚙️ ⓘ admin ▾ cisco SECURE

Cloud Services Realms Identity Sources High Availability eStreamer Host Input Client Smart Software Manager On-Prem

Host	Last Modified	Status	State	
10.18.19.31	2023-09-28 13:53:56	Pending Registration	<input type="checkbox"/>	 

## 配置主FMC

在主用/主用FMC上重複步驟1 - 4。

步驟5. 按一下Primary。

Select a role for this Management Center and specify peer details to setup high availability.

Role For This Firewall Management Center:

- Standalone (No High Availability)
- Primary
- Secondary

Peer Details:

Configure the secondary Management Center with details of the primary before registration.

After Firewall Management Center high availability is configured in virtual or cloud environment, each registered Firewall Threat Defense consumes an additional Firepower MCv Device license.

Secondary Firewall Management Center Host:

Registration Key\*:

Unique NAT ID:

Register

† Either host or NAT ID is required.

步驟6.輸入有關輔助FMC的資訊，然後按一下Register。

Select a role for this Management Center and specify peer details to setup high availability.

Role For This Firewall Management Center:

- Standalone (No High Availability)
- Primary
- Secondary

Peer Details:

Configure the secondary Management Center with details of the primary before registration.

After Firewall Management Center high availability is configured in virtual or cloud environment, each registered Firewall Threat Defense consumes an additional Firepower MCv Device license.

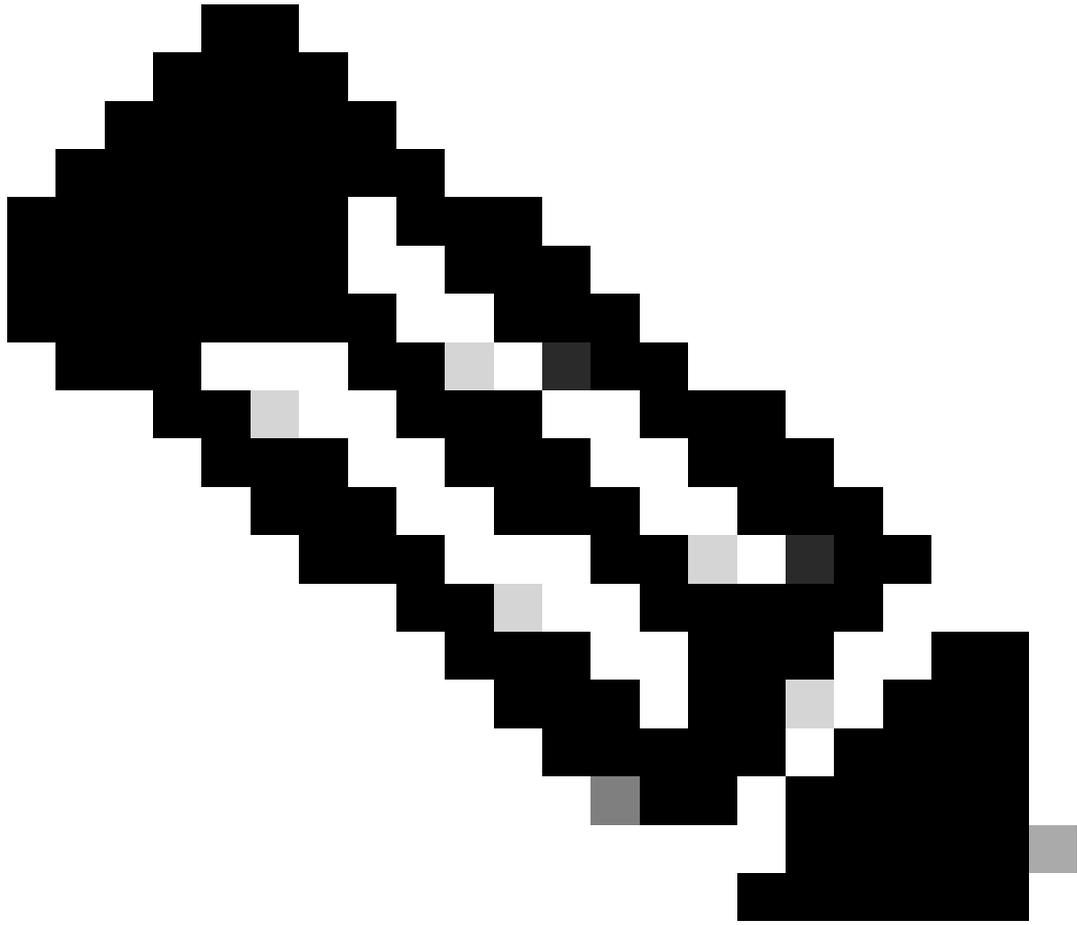
Secondary Firewall Management Center Host:

Registration Key\*:

Unique NAT ID:

Register

† Either host or NAT ID is required.



附註：使用與輔助FMC相同的註冊金鑰。

---

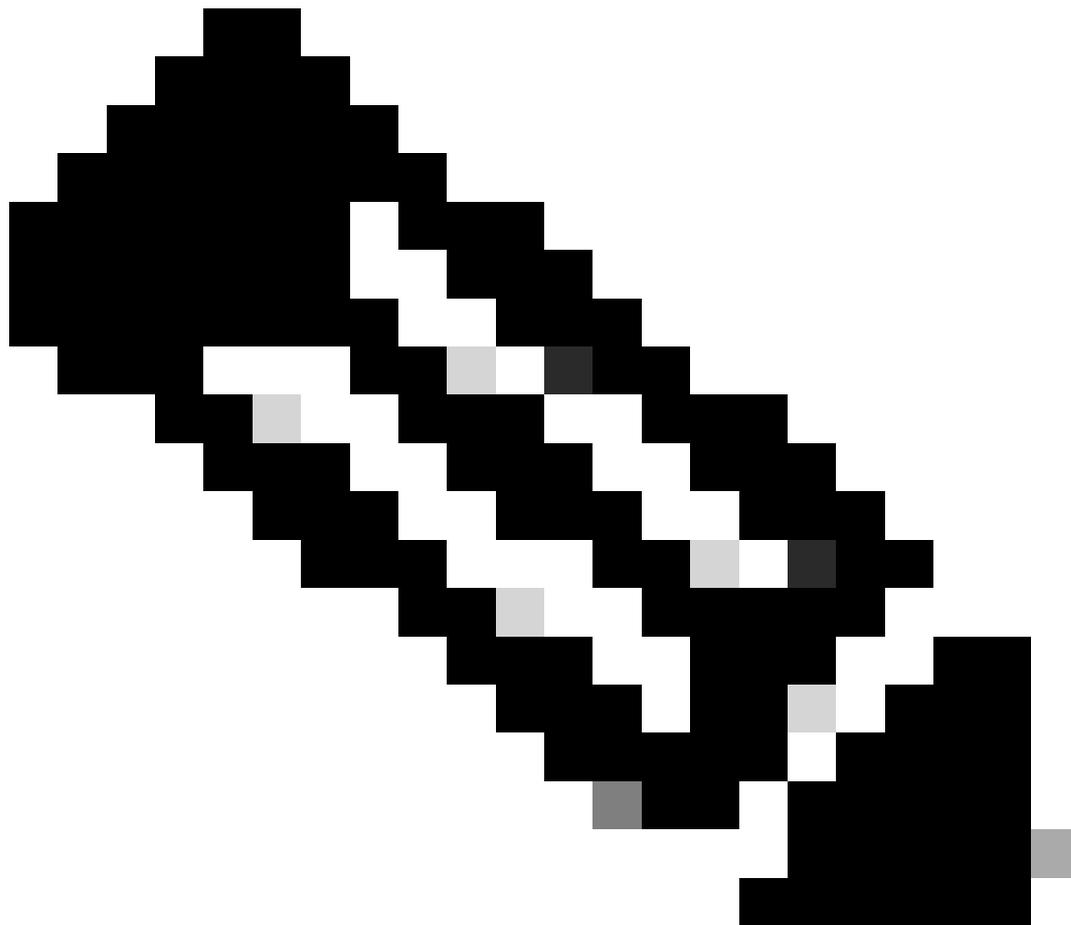
步驟7.此警告要求您確認，按一下 Yes.

## Warning

This operation may affect critical processes running in the background. Do you want to continue?

No

Yes



---

附註：確保沒有其他任務正在運行。

---

步驟8.確認要註冊輔助FMC。

## Warning

Secondary peer configuration and policies will be removed. After Firewall Management Center high availability is configured in virtual or cloud environment, each registered Firewall Threat Defense consumes an additional Firepower MCV Device license. Do you want to register secondary peer:  
10.18.19.32?

No

Yes

附註：確保輔助FMC上沒有重要資訊，因為接受此提示會從FMC中刪除所有配置。

主節點和輔助節點之間的同步啟動；持續時間取決於配置和裝置。可以從兩個單元監視此過程。

Firewall Management Center  
Integration / Other Integrations / High Availability

Overview Analysis Policies Devices Objects Integration Deploy 🔍 ⚙️ 👤 admin | cisco SECURE

Peer Manager

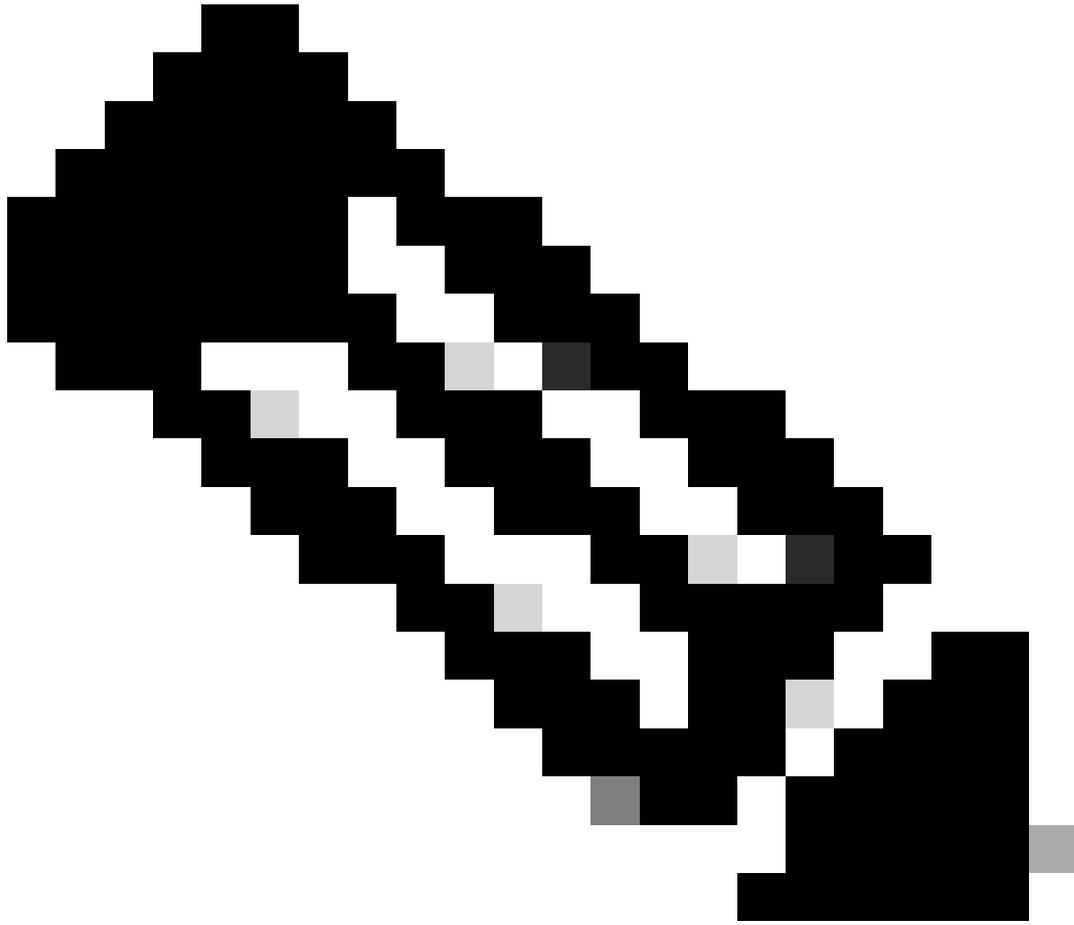
Cloud Services Realms Identity Sources High Availability eStreamer Host Input Client Smart Software Manager On-Prem

Switch Peer Roles Break HA Pause Synchronization

High availability operations are in progress. The status messages and alerts on this page are temporary. Please check after high availability operations are complete. These operations include file copy which may take time to complete. Database files synchronization: 100% of 379MB transferred

Summary	
Status	▲ Temporarily degraded- high availability operations are in progress.
Synchronization	▲ Failed
Active System	10.18.19.31
Standby System	10.18.19.32

System Status		
	Local Active - Primary (10.18.19.31)	Remote Standby - Secondary (10.18.19.32)
Operating System	7.2.5	7.2.5
Software Version	7.2.5-208	7.2.5-208
Model	Secure Firewall Management Center for VMware	Secure Firewall Management Center for VMware



附註：進行同步時，狀態應為Failed和Temporary degraded。此狀態顯示直到進程完成。

---

## 驗證

同步完成後，預期輸出為Status Healthy和Synchronization OK。

Firewall Management Center  
Integration / Other Integrations / High Availability

Overview Analysis Policies Devices Objects Integration Deploy 🔍 ⚙️ 👤 admin | Cisco SECURE

Peer Manager

Cloud Services Realms Identity Sources **High Availability** eStreamer Host Input Client Smart Software Manager On-Prem

Switch Peer Roles Break HA Pause Synchronization

Summary	
Status	🟢 Healthy
Synchronization	🟢 OK
Active System	10.18.19.31
Standby System	10.18.19.32

System Status		
	Local	Remote
	<b>Active - Primary</b> (10.18.19.31)	<b>Standby - Secondary</b> (10.18.19.32)
Operating System	7.2.5	7.2.5
Software Version	7.2.5-208	7.2.5-208
Model	Secure Firewall Management Center for VMware	Secure Firewall Management Center for VMware

主節點和輔助節點保持同步；這很正常。

Firewall Management Center  
Integration / Other Integrations / High Availability

Devices Integration 🔍 ⚙️ 👤 admin | Cisco SECURE

Peer Manager

Cloud Services **High Availability** eStreamer Host Input Client

Switch Peer Roles Break HA Pause Synchronization

Summary	
Status	🟢 Synchronization task is in progress
Synchronization	🟢 OK
Active System	10.18.19.31
Standby System	10.18.19.32

System Status		
	Local	Remote
	<b>Standby - Secondary</b> (10.18.19.32)	<b>Active - Primary</b> (10.18.19.31)
Operating System	7.2.5	7.2.5
Software Version	7.2.5-208	7.2.5-208
Model	Secure Firewall Management Center for VMware	Secure Firewall Management Center for VMware

請花點時間檢查您的裝置在主和輔助上是否都正確顯示。

## 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）。