在Firepower 4100上配置FTD多例項高可用性

目錄

簡介

本檔案介紹如何在FTD容器執行處理（多重執行處理）中設定容錯移轉。

必要條件

需求

思科建議您瞭解Firepower管理中心和防火牆威脅防禦。

採用元件

Cisco Firepower管理中心虛擬7.2.5
思科Firepower 4145 NGFW裝置(FTD) 7.2.5
Firepower可擴展作業系統(FXOS) 2.12 (0.498)
Windows 10

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。

在部署FTD多重執行處理之前，請務必瞭解它如何影響您的系統效能，並據此進行規劃。請務必參閱Cisco官方文檔或諮詢Cisco技術代表，以確保實現最佳部署和配置。

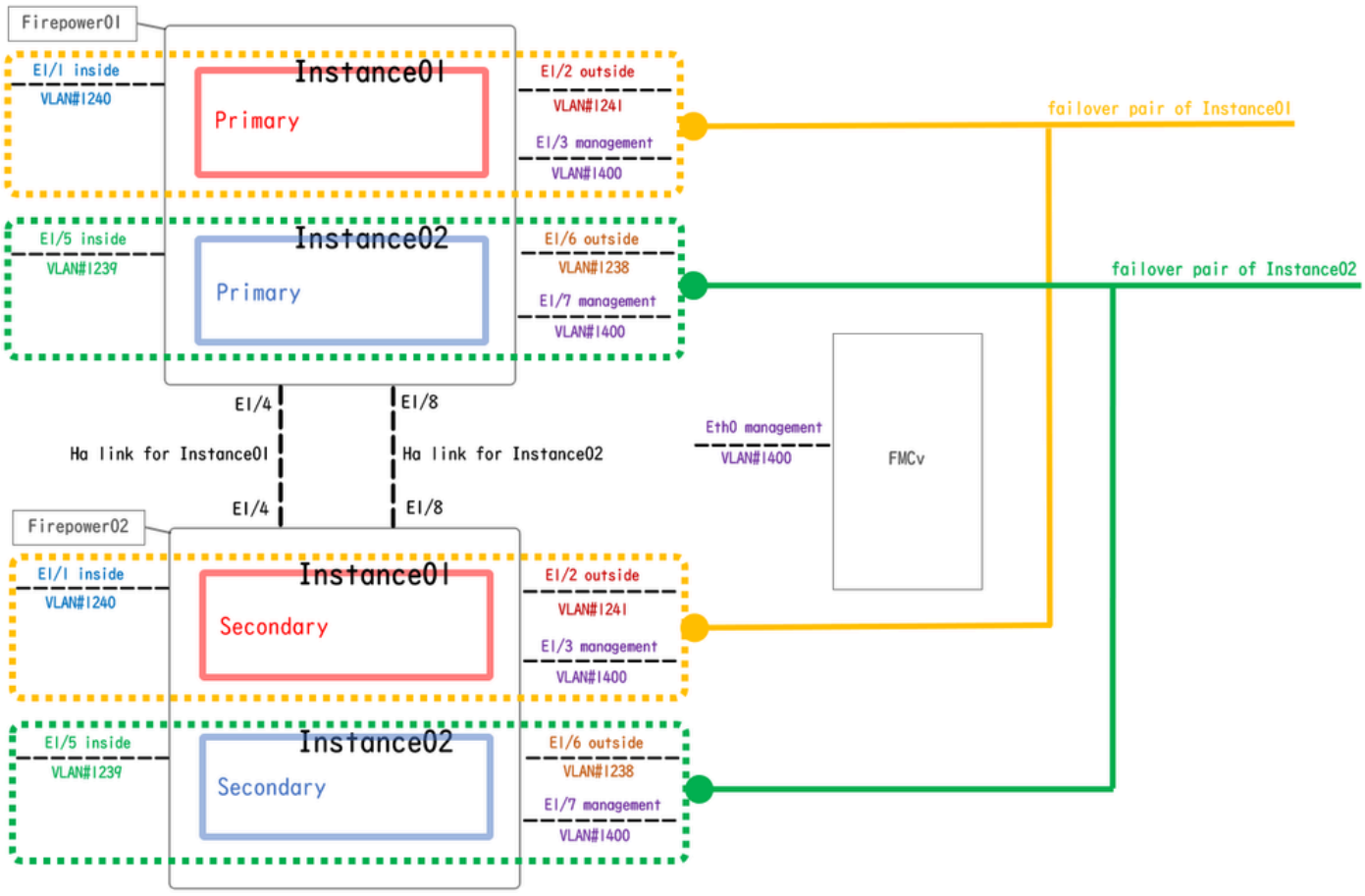
背景資訊

多例項是Firepower威脅防禦(FTD)的一項功能，它類似於ASA多情景模式。此功能可讓您在單一硬體上執行多個不同的FTD容器執行個體。每個容器例項允許硬資源分離、單獨的組態管理、單獨的重新載入、單獨的軟體更新和全面的威脅防禦功能支援。這對於需要不同部門或專案採用不同安全策略，但又不想投資於多個獨立硬體裝置的組織特別有用。多例項功能當前在運行FTD 6.4及更高版本的Firepower 4100和9300系列安全裝置上受支援。

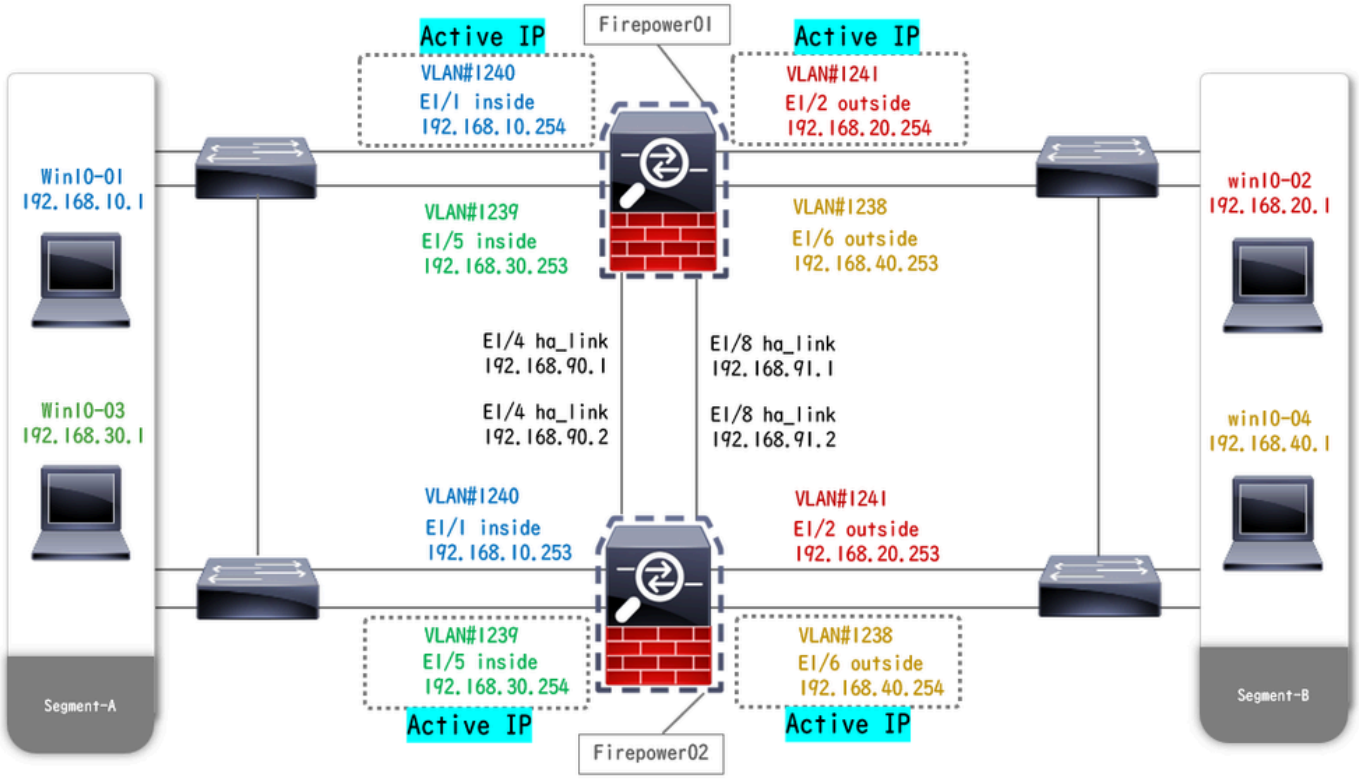
本文檔使用支援最多14個容器例項的Firepower4145。有關Firepower裝置支援的最大例項數，請參閱每個型號的最大容器例項和資源數。

網路圖表

本檔案介紹此圖表上多執行處理中HA的組態和驗證。



邏輯配置圖

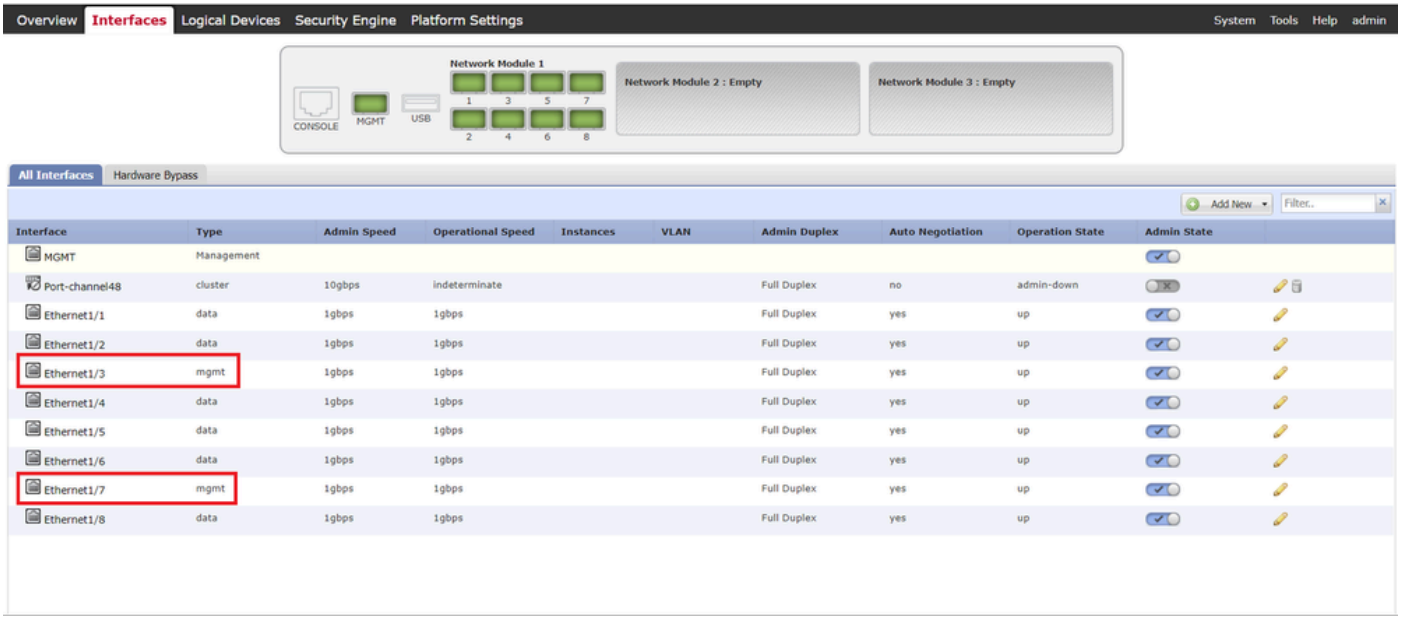


物理配置圖

組態

步驟 1.預配置介面

a.導航到FCM上的介面。設定2個管理介面。在本例中， Ethernet1/3和Ethernet1/7。

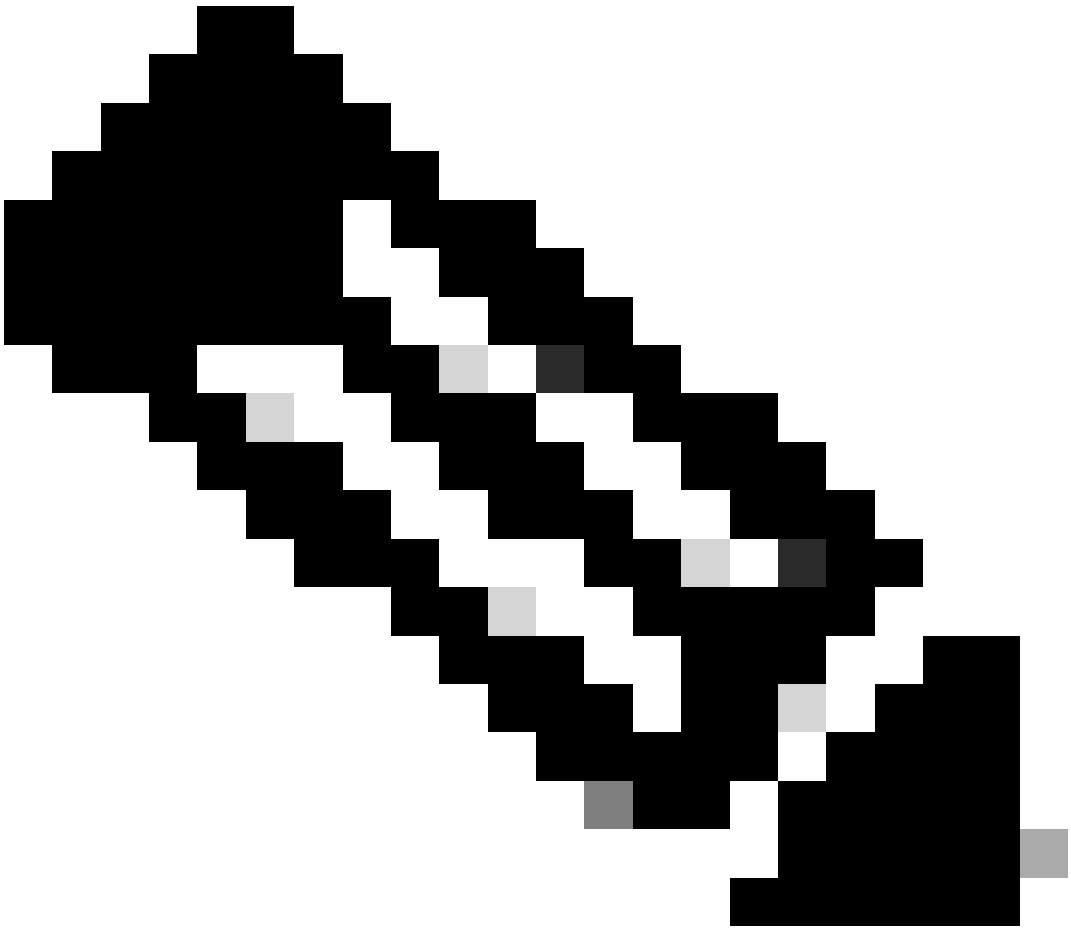


預配置介面

步驟 2.為容器例項增加2個資源配置檔案。

a.導航到平台設定 > 資源配置檔案 > 增加。設定第一個資源設定檔。

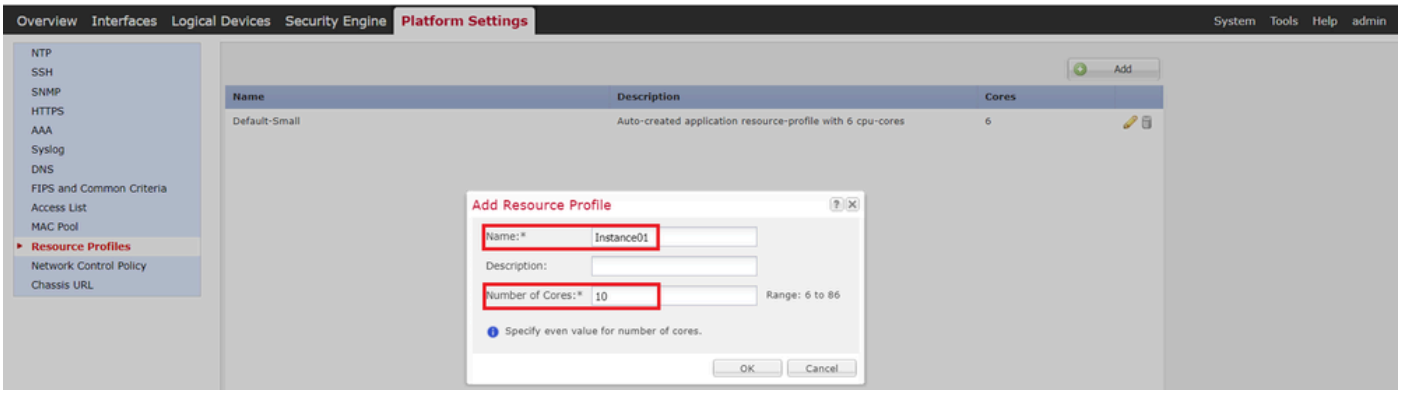
在本示例中：
·名稱：Instance01
·核心數：10個



註：對於容器例項對的HA，它們必須使用相同的資源配置檔案屬性。

將設定檔的名稱設定在1到64個字元之間。請注意，新增此設定檔後，您就無法變更其名稱。

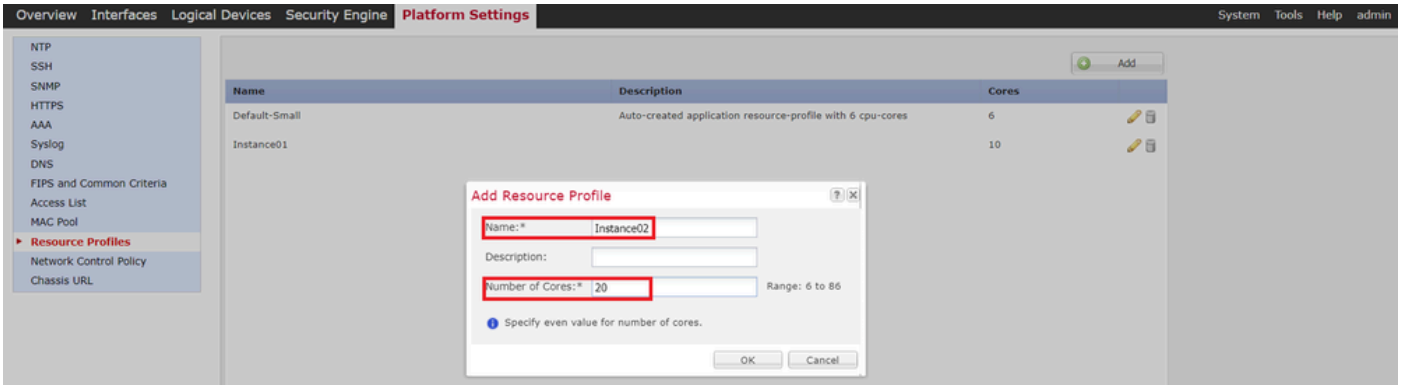
設定設定檔的核心數量，介於6和最大值之間。



新增第一個資源設定檔

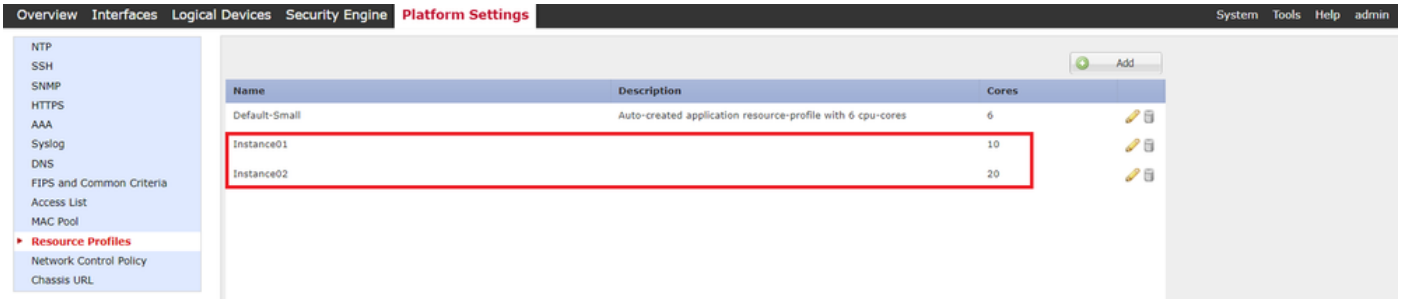
b.在步驟2中重複a.來配置第二個資源配置檔案。

在本示例中：
·名稱：Instance02
·核心數：20



新增第二個資源設定檔

c.檢查2個資源配置檔案已成功增加。



確認資源配置檔案

步驟3.（可選）為容器例項介面增加虛擬MAC地址的MAC池字首。

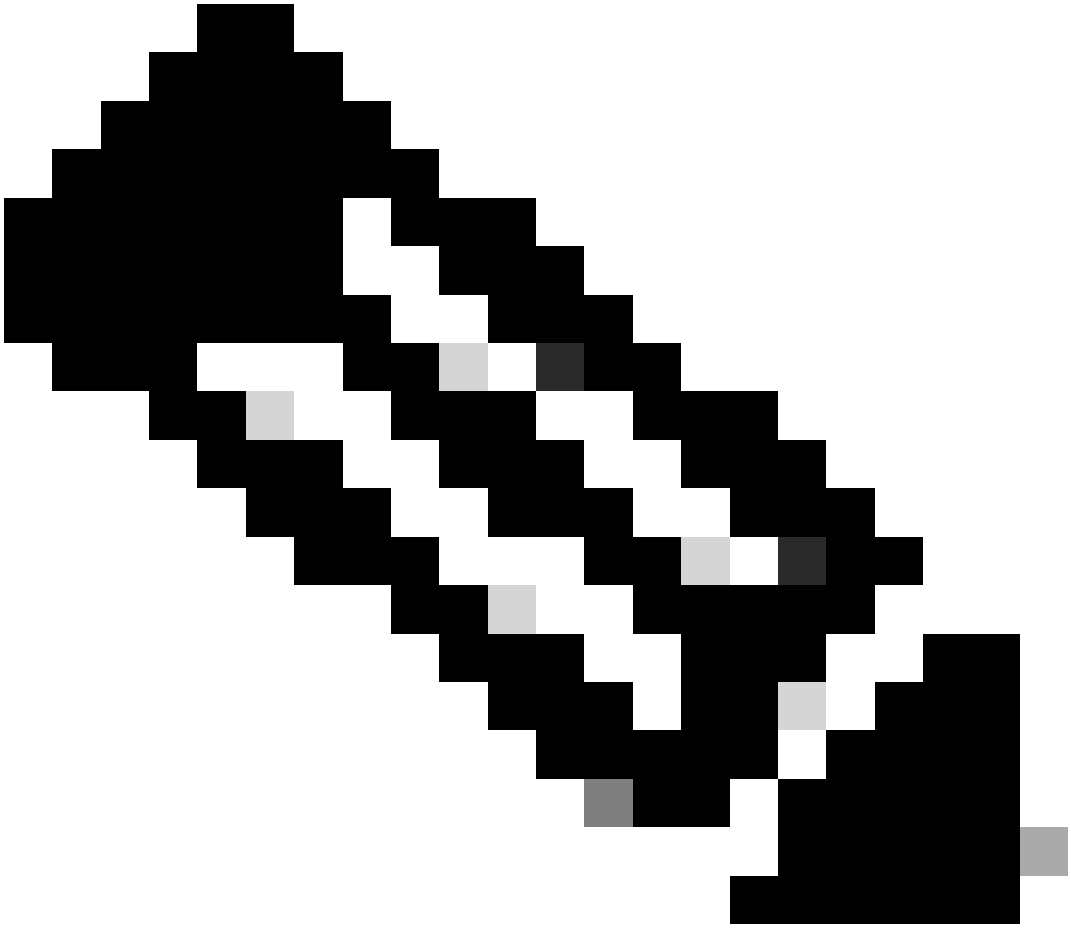
您可以手動設定主用/備用介面的虛擬MAC地址。如果未設定虛擬MAC地址，對於多例項功能，機箱會自動為例項介面生成MAC地址，並確保每個例項中的共用介面使用唯一的MAC地址。

有關MAC地址的詳細資訊，請檢查為容器例項介面增加MAC池字首和檢視MAC地址。

步驟 4.新增獨立執行處理。

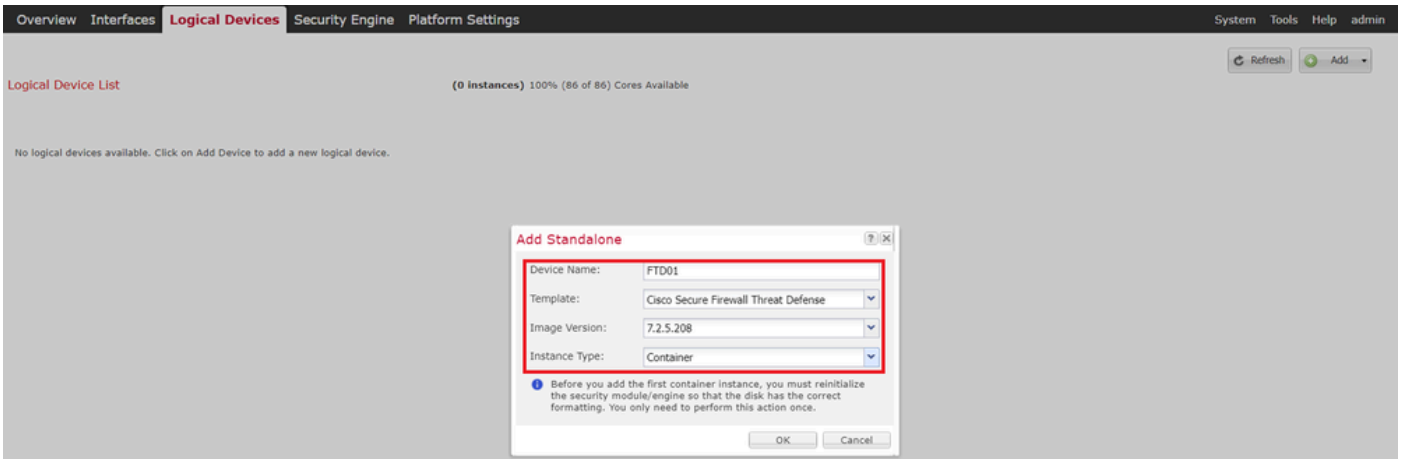
a.導航到邏輯裝置 > 增加獨立。設定第一個例項。

在本示例中：
·裝置名稱：FTD01
·例項型別：容器



注意：部署容器應用程式的唯一方法是預部署例項型別設定為容器的應用例項。 確保選擇 Container。

增加邏輯裝置後，無法更改此名稱。

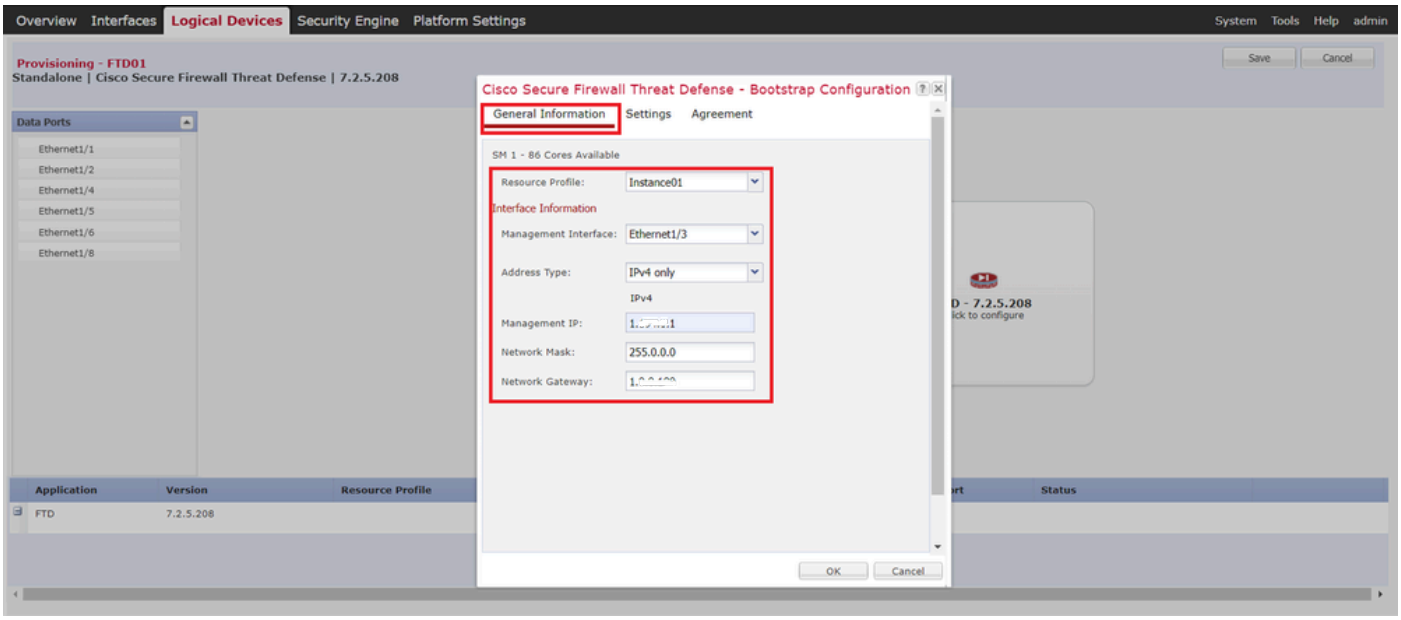


增加例項

步驟 5.配置介面

a.為Instance01設定Resource Profile、Management Interface和Management IP。

在本示例中：
·資源配置檔案：Instance01
·管理介面：Ethernet1/3
·管理IP：x.x.1.1



配置配置檔案/管理介面/管理IP

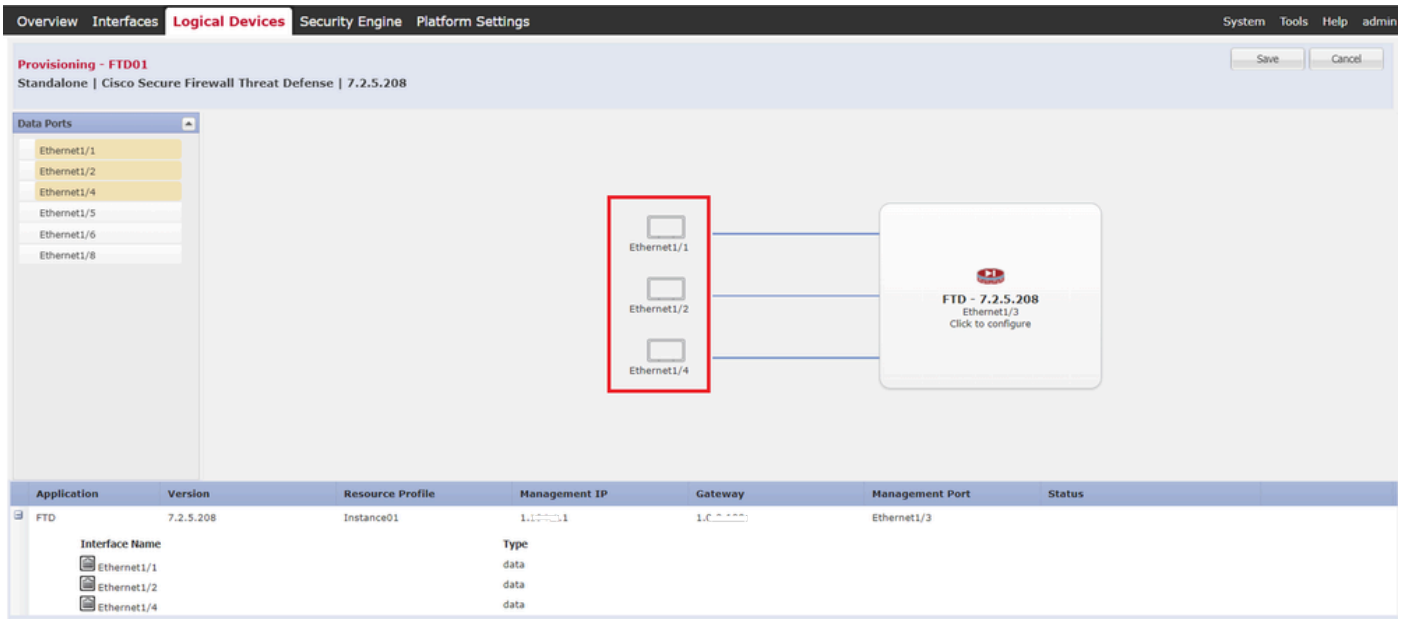
b.設定資料介面。

在本示例中：

·Ethernet1/1（用於內部）

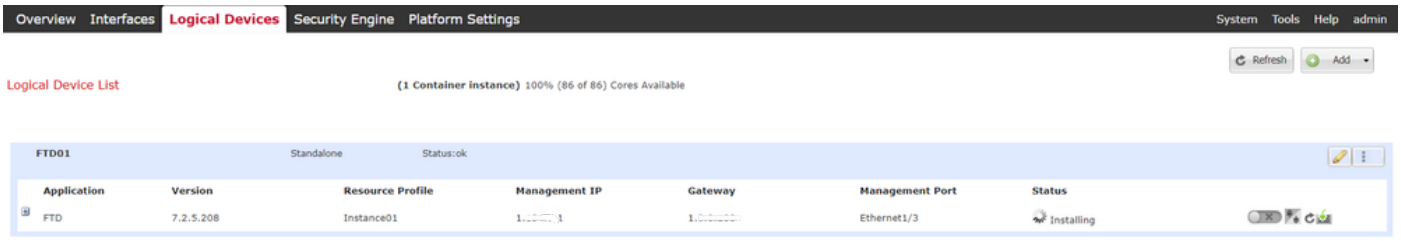
·Ethernet1/2（用於外部）

·Ethernet1/4（用於HA鏈路）



設定資料介面

c.導航至邏輯裝置。正在等待執行個體啟動。



確認Instance01的狀態

d.在步驟4.a和步驟5.a到c中重複a.以增加第二個例項並為其設定詳細資訊。

在本示例中：

· 裝置名稱：FTD11
· 例項型別：容器

· 資源配置檔案：Instance02
· 管理介面：Ethernet1/7
· 管理IP ： x.x.10.1

· 乙太網1/5 =內部

· 乙太網1/6 =外部

·Ethernet1/8 = HA鏈路

e.確認FCM上的2個執行處理為「線上」狀態。

確認主裝置中的例項狀態

f. （可選）在Firepower CLI中運行 scope ssa、 **scope slot 1** 和 **show app-Instance** 命令，確認2個例項處於聯機狀態。

<#root>

FPR4145-ASA-K9#

scope ssa

FPR4145-ASA-K9 /ssa #

scope slot 1

FPR4145-ASA-K9 /ssa/slot #

show app-Instance

Application Instance: App Name Identifier Admin State Oper State Running Version Startup Version Deplo

Online

7.2.5 208 7.2.5 208 Container No Instance01 Not Applicable None --> FTD01 Instance is Online ftd FTD11

Online

7.2.5 208 7.2.5 208 Container No Instance02 Not Applicable None --> FTD11 Instance is Online

g.在輔助裝置上執行相同的操作。 確認2個執行處理為線上狀態。

確認輔助裝置中的例項狀態

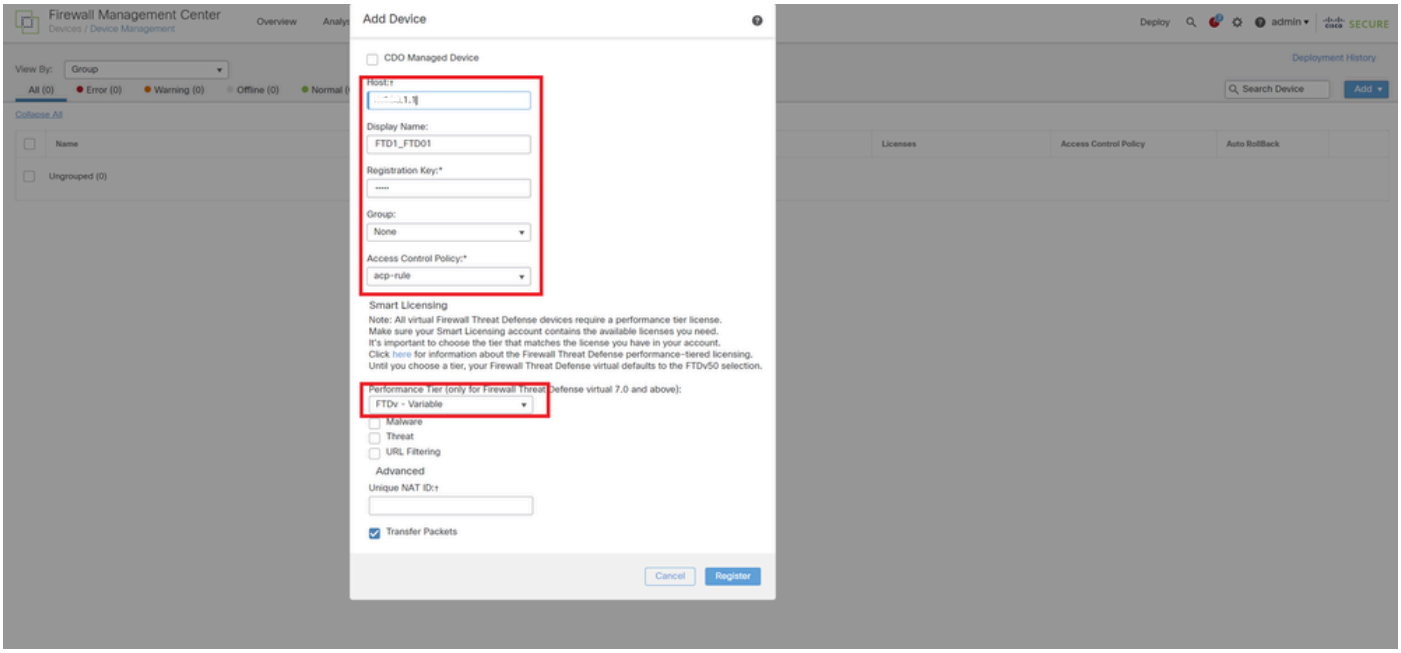
步驟 6.為每個例項增加高可用性對。

a.導航到**裝置** > **增加裝置**（在FMC上）。將所有例項增加到FMC。

在本示例中：

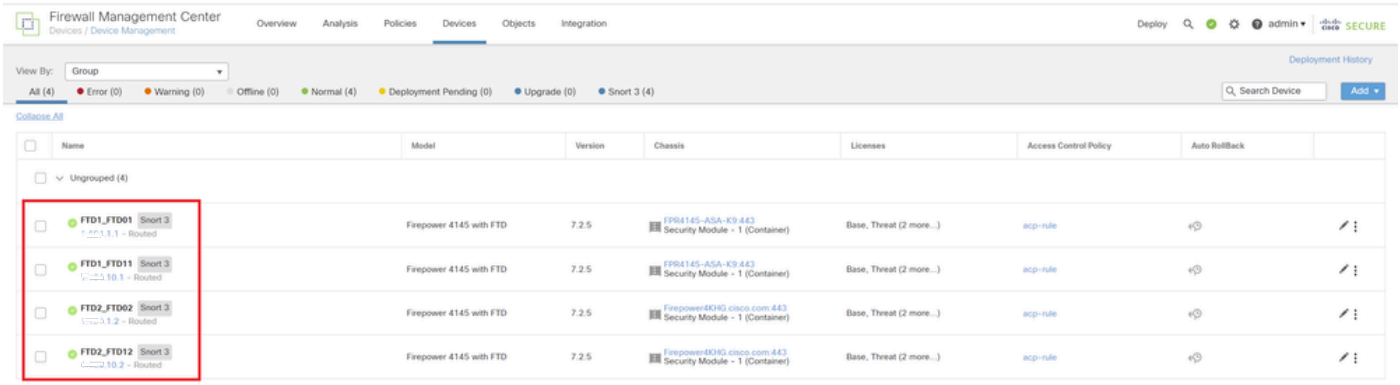
·FTD1之Instance01的顯示名稱：FTD1_FTD01
·FTD1之Instance02的顯示名稱：FTD1_FTD11
·FTD2的Instance01的顯示名稱：FTD2_FTD02
·FTD2的Instance02的顯示名稱：FTD2_FTD12

下圖顯示了**FTD1_FTD01**的設定。



將*FTD*執行處理新增至*FMC*

b.確認所有例項均為正常。



確認*FMC*中的例項狀態

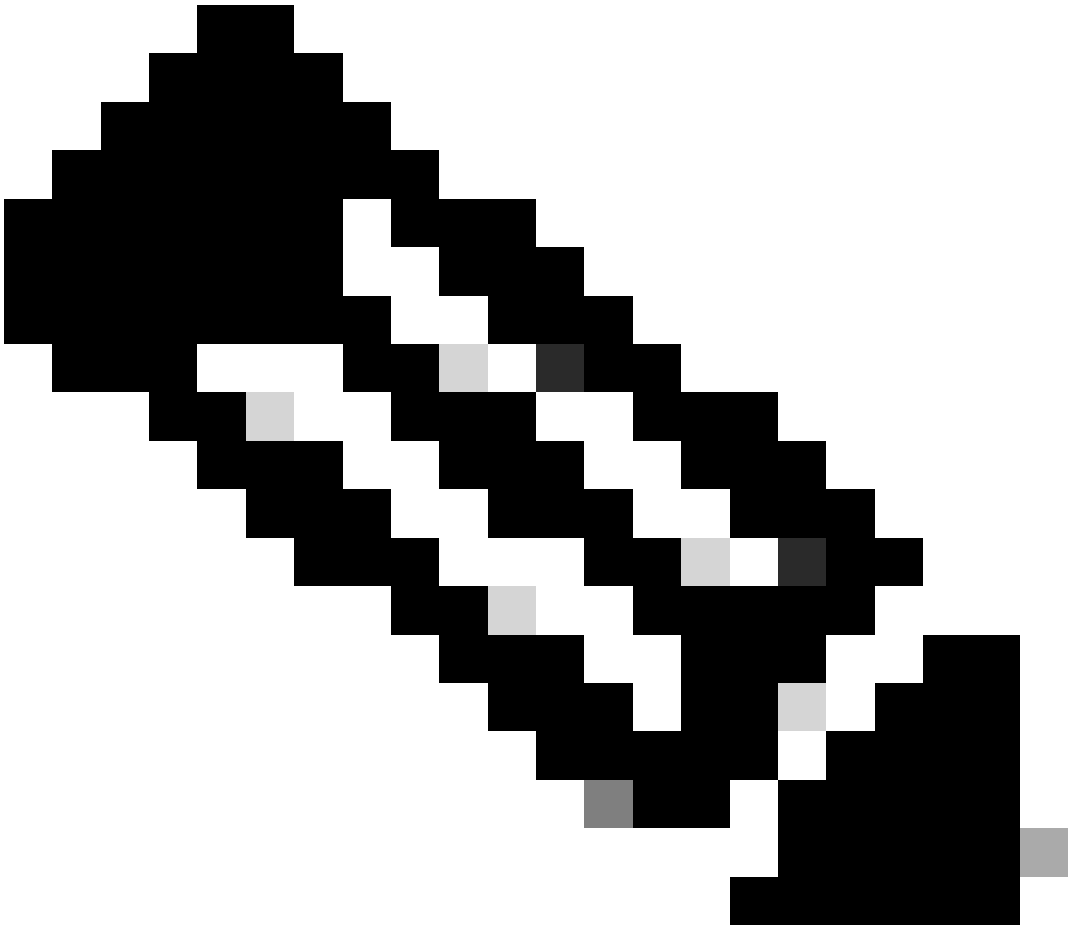
c.導航到**裝置** > **增加高可用性**。設定第一個故障轉移對。

在本示例中：

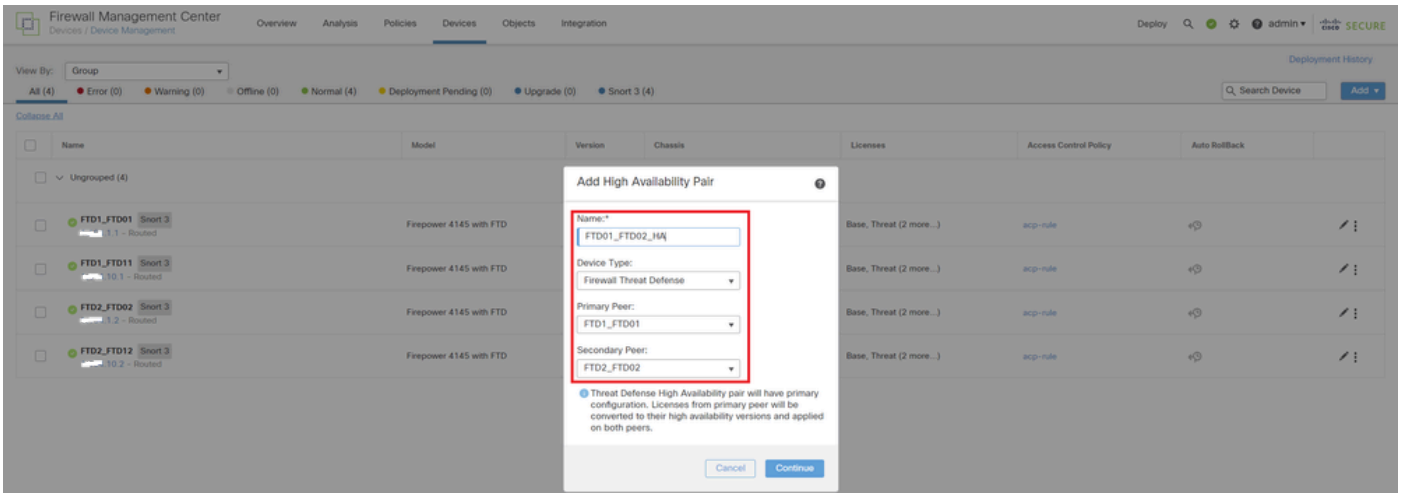
·**名稱：FTD01_FTD02_HA**

·**主要對等體：FTD1_FTD01**

·**輔助對等體：FTD2_FTD02**



註：確保選擇正確的裝置作為主要裝置。



增加第一個故障轉移對

d.為第1個故障轉移對中的故障轉移鏈路設定IP。

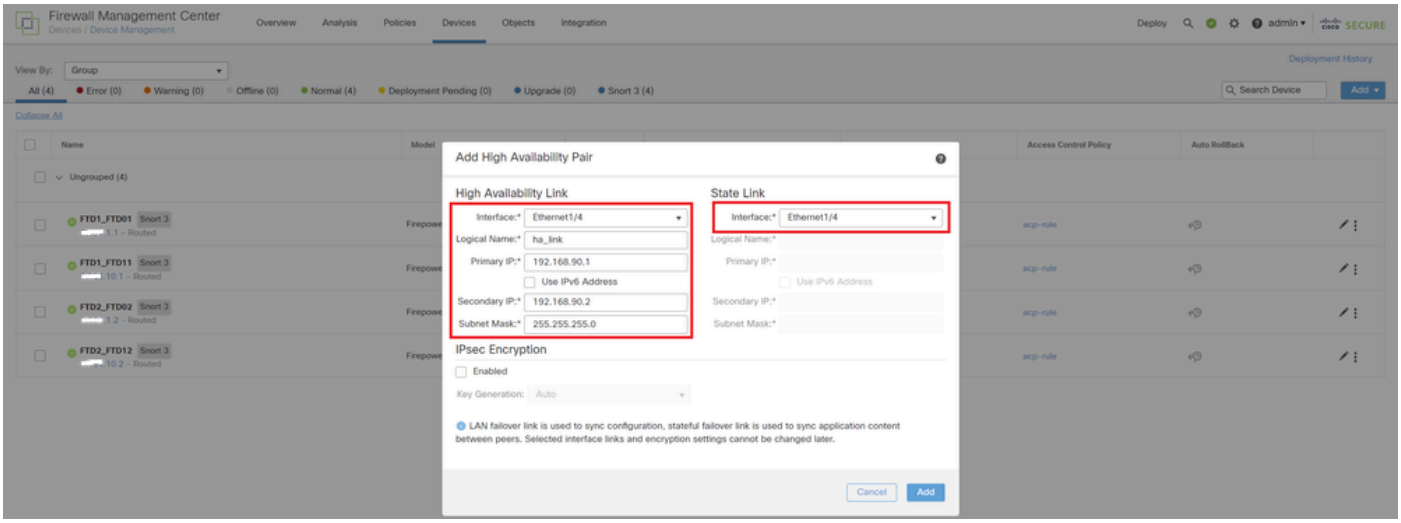
在本示例中：

·**高可用性鏈路：Ethernet1/4**

·**狀態鏈路：Ethernet1/4**

·**主IP：192.168.90.1/24**

·**輔助IP：192.168.90.2/24**

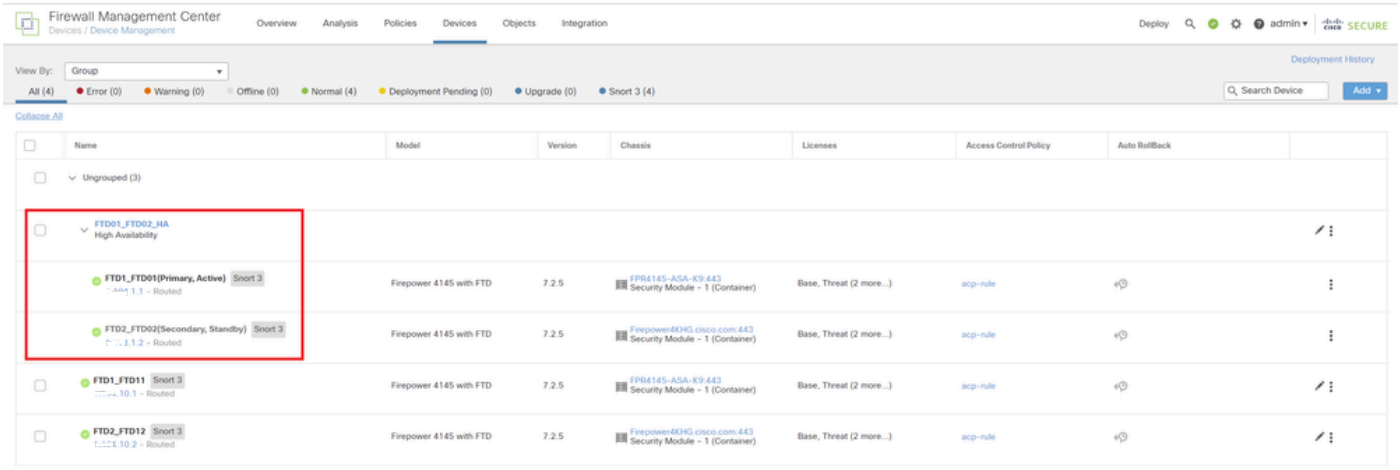


為第一個故障轉移對設定*HA*介面和*IP*

e.確認故障切換狀態

·**FTD1_FTD01：主用，活動**

·**FTD2_FTD02：輔助、備用**



確認第一個故障轉移對的狀態

f.**導航到裝置>點選FTD01_FTD02_HA**（在本示例中）**> 介面。** 為資料介面設定活動IP。

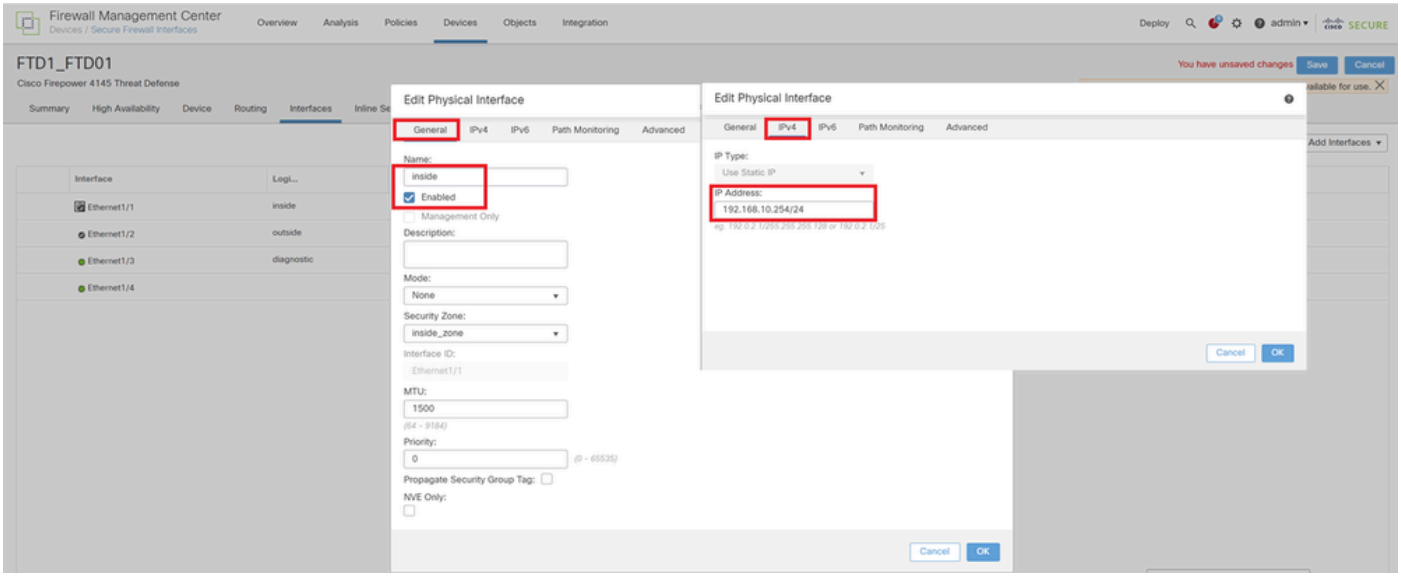
在本示例中：

· 乙太網1/1（內部）：192.168.10.254/24

· 乙太網1/2（外部）：192.168.20.254/24

· 乙太網1/3（診斷）：192.168.80.1/24

下圖顯示了**Ethernet1/1**的活動IP設定。



為資料介面設定活動*IP*

g.**導航到裝置** > **點選FTD01_FTD02_HA**（在本示例中）**> 高可用性。** 為資料介面設定備用IP。

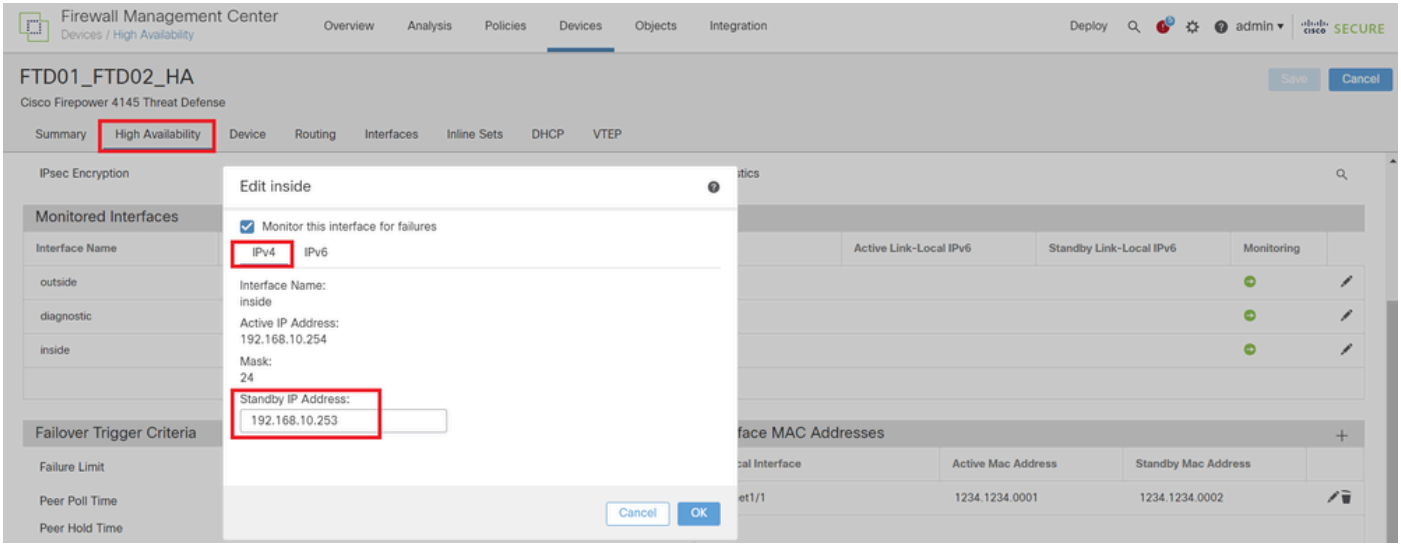
在本示例中：

· 乙太網1/1（內部）：192.168.10.253/24

· 乙太網1/2（外部）：192.168.20.253/24

· 乙太網1/3（診斷）：192.168.80.2/24

此圖顯示**Ethernet1/1**的備用IP設定。



設定資料介面的待命*IP*

h.重複步驟6.c到g，增加第2個故障轉移對。

在本示例中：

· 名稱：FTD11_FTD12_HA
· 主要對等點：FTD1_FTD11
· 次要同儕節點：FTD2_FTD12

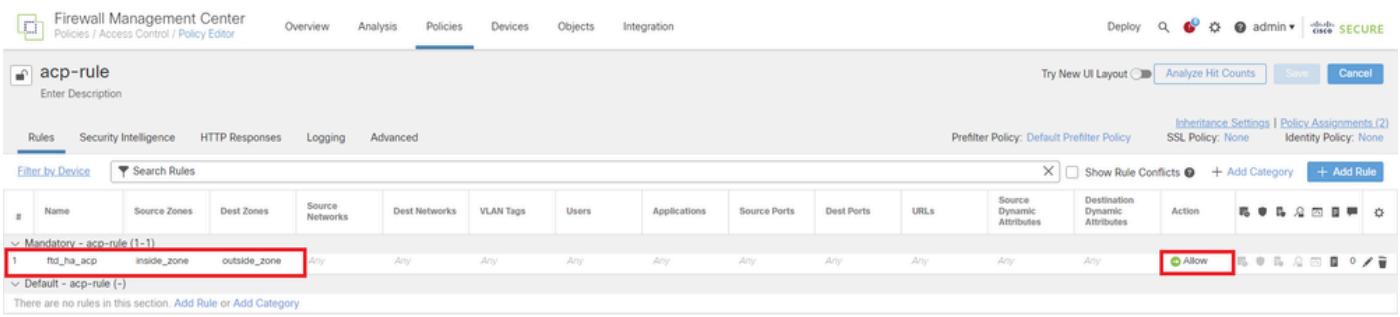
· 高可用性鏈路：Ethernet1/8
· 狀態鏈路：Ethernet1/8
· 乙太網1/8（ha_link活動）：192.168.91.1/24

· 乙太網1/5（內部活動）：192.168.30.254/24
· 乙太網1/6（外部活動）：192.168.40.254/24
· 乙太網路1/7（診斷作用中）：192.168.81.1/24

· 乙太網1/8（ha_link待機）：192.168.91.2/24

· 乙太網1/5（內部待機）：192.168.30.253/24
· 乙太網1/6（外部待機）：192.168.40.253/24
· 乙太網1/7（診斷待機）：192.168.81.2/24

i.導航到**邏輯裝置** > **增加獨立**。設定ACP規則以允許從內部到外部的流量。



j.將設定部署至FTD。

k.在CLI中確認高可用性狀態

每個例項的HA狀態也在Firepower CLI中確認，CLI與ASA相同。

運行 **show running-config failover** 和 **show failover** 命令以確認FTD1_FTD01（主例項01）的HA狀態。

```
<#root>

// confrim HA status of FTD1_FTD01 (Instance01 of Primary Device) >

show running-config failover

 failover failover lan unit primary failover lan interface ha_link Ethernet1/4 failover replication http

show failover

 Failover On Failover unit Primary Failover LAN Interface: ha_link Ethernet1/4 (up) ...... This host: P
...... Other host: Secondary - Standby Ready <---- Instance01 of FPR02 is Standby Interface diagnostic
```

運行 **show running-config failover** 和 **show failover** 命令以確認FTD1_FTD11(Primay Instance02)的HA狀態。

```
<#root>

// confrim HA status of FTD1_FTD11 (Instance02 of Primary Device) >

show running-config failover

 failover failover lan unit primary failover lan interface ha_link Ethernet1/8 failover replication http

show failover

 Failover On Failover unit Primary Failover LAN Interface: ha_link Ethernet1/8 (up) ...... This host: P
Other host: Secondary - Standby Ready <---- Instance02 of FPR02 is Standby Interface diagnostic (192.16
```

運行 **show running-config failover** 和 **show failover** 命令以確認FTD2_FTD02（輔助例項01）的HA狀態。

```
<#root>

// confrim HA status of FTD2_FTD02 (Instance01 of Secondary Device) >

show running-config failover

 failover failover lan unit secondary failover lan interface ha_link Ethernet1/4 failover replication h

show failover

 Failover On Failover unit Secondary Failover LAN Interface: ha_link Ethernet1/4 (up) ...... This host:
Other host: Primary - Active <---- Instance01 of FPR01 is Active Active time: 31651 (sec) slot 0: UCSB-
```

運行 **show running-config failover** 和 **show failover** 命令以確認FTD2_FTD12 (Seconday Instance02)的HA狀態。

<#root>

// confrim HA status of FTD2_FTD12 (Instance02 of Secondary Device) >

show running-config failover

```
 failover failover lan unit secondary failover lan interface ha_link Ethernet1/8 failover replication h
Other host: Primary - Active <---- Instance02 of FPR01 is Active Active time: 31275 (sec) slot 0: UCSB-
```

l.確認許可證使用

所有許可證按安全引擎/機箱使用，而不是按容器例項使用。

·自動分配基准許可證：每個安全引擎/機箱一個。

·功能許可證手動分配給每個例項，但每個功能每個安全引擎/機箱僅使用一個許可證。對於特定功能許可證，無論使用的例項數量如何，您總共只需要1個許可證。

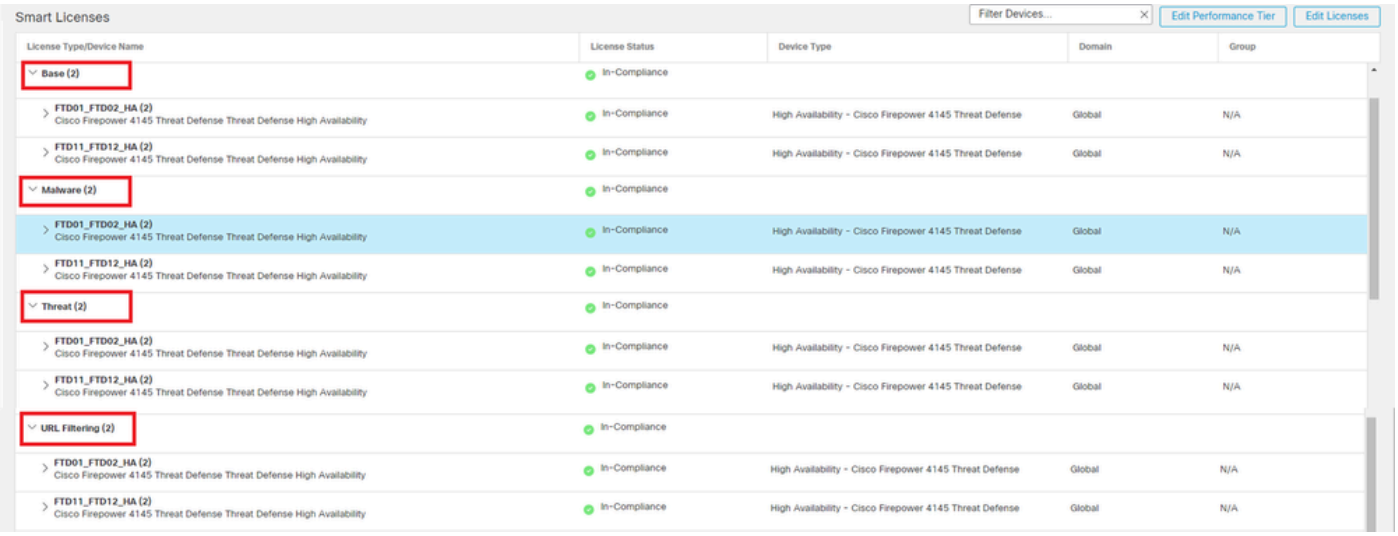
此表顯示了本文檔中許可證的使用方式。

FPR01	例項01	基礎、URL過濾、惡意軟體、威脅
	例項02	基礎、URL過濾、惡意軟體、威脅
FPR02	例項01	基礎、URL過濾、惡意軟體、威脅
	例項02	基礎、URL過濾、惡意軟體、威脅

授權總數

基礎	URL篩選	惡意軟體	威脅
2	2	2	2

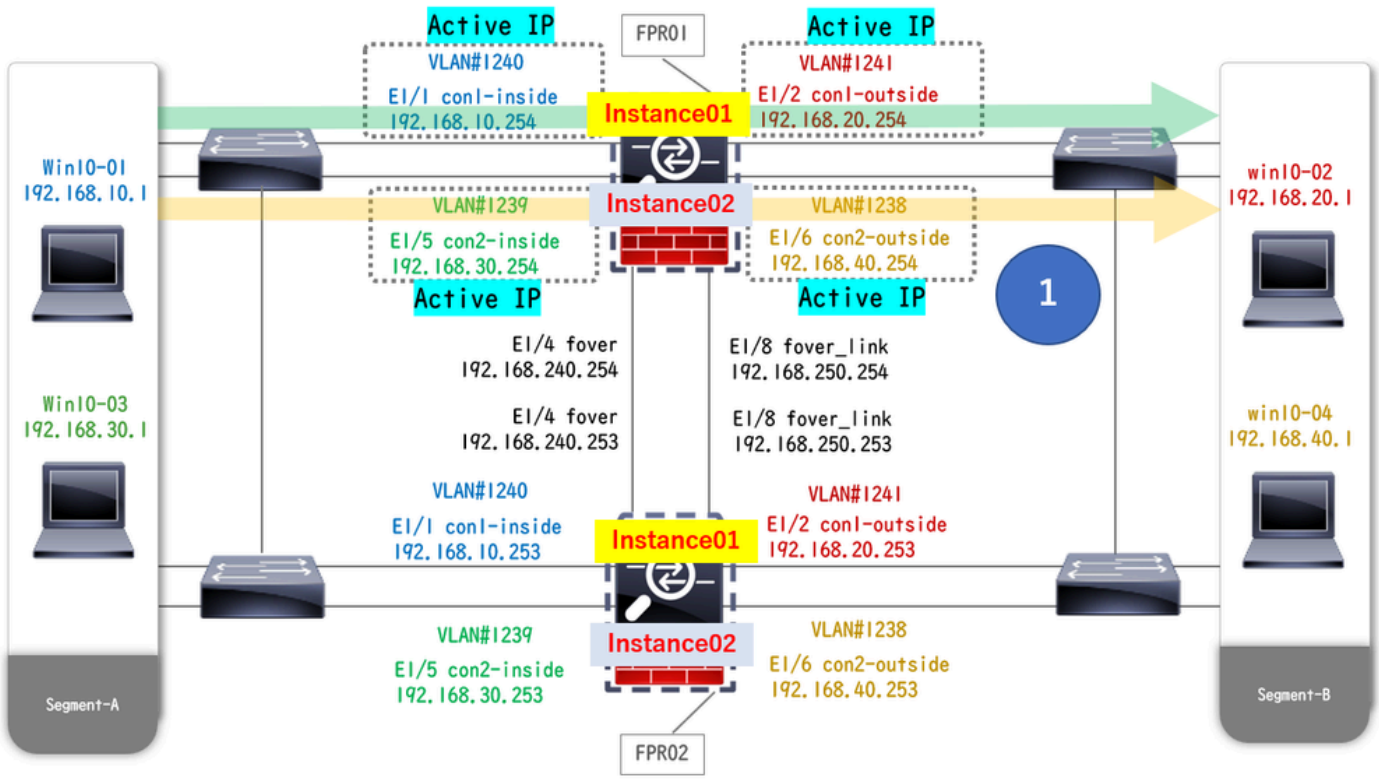
在FMC GUI中確認已使用的許可證數量。



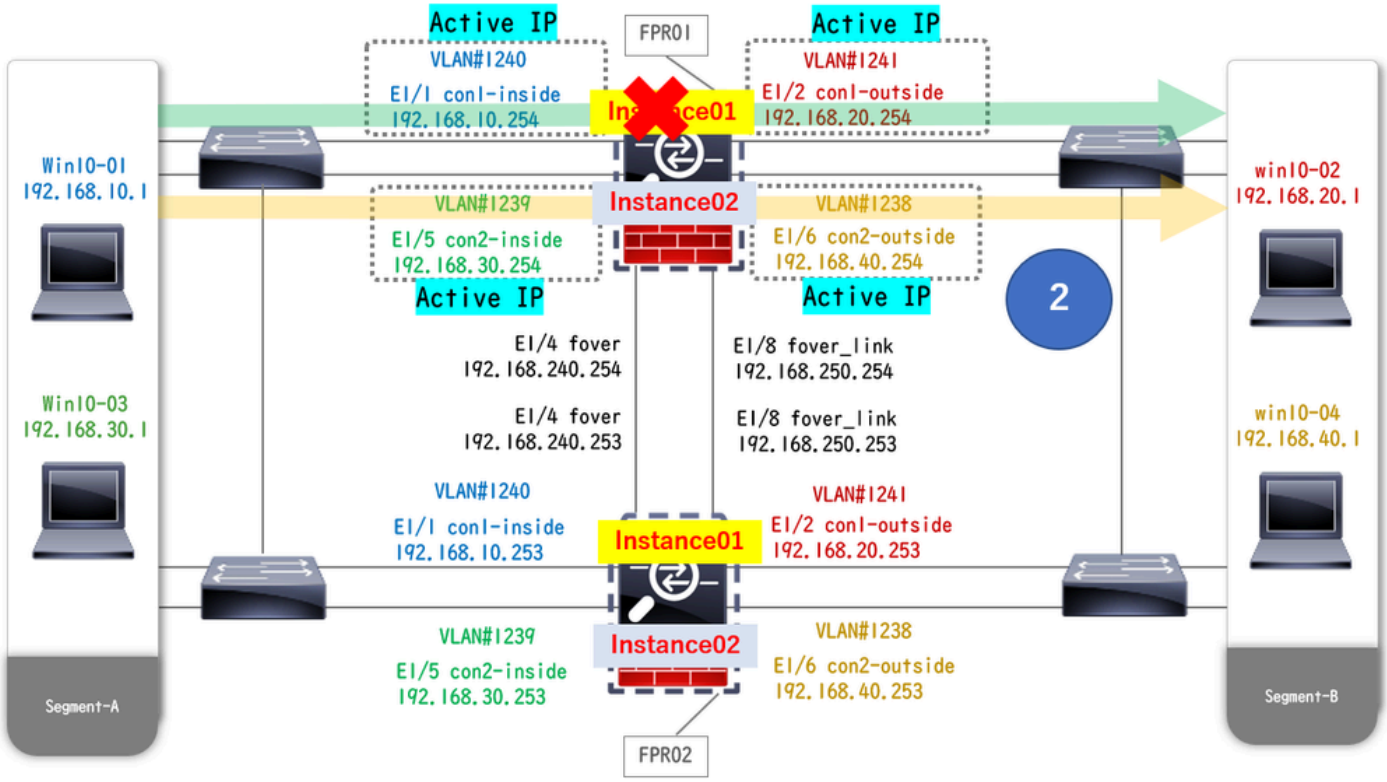
確認已使用的許可證

驗證

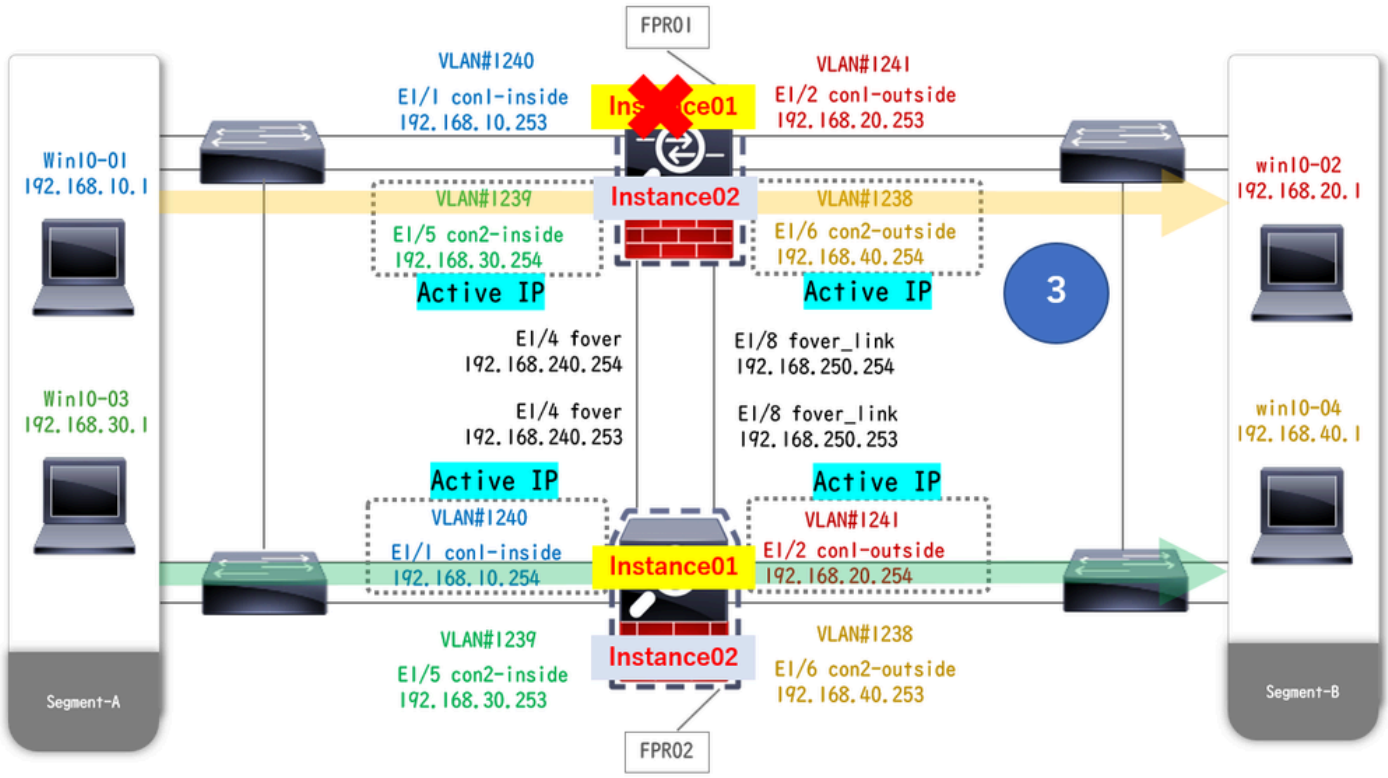
當FTD1_FTD01（主要執行處理01）發生當機時，會觸發Instance01的容錯移轉，且待命端上的資料介面會接管原始作用中介面的IP/MAC位址，以確保Firepower能夠持續傳遞流量（本檔案中的FTP連線）。



崩潰前



崩潰期間



故障轉移已觸發

步驟 1.從Win10-01到Win10-02發起FTP連線。

步驟 2.運行 show conn 命令以確認在Instance01兩個例項中都建立了FTP連線。

<#root>

// Confirm the connection in Instance01 of FPR01 >

```
show conn
 TCP outside 192.168.20.1:21 inside 192.168.10.1:49723, idle 0:00:11, bytes 529, flags UIO N1 // Confirm
show conn
 TCP outside 192.168.20.1:21 inside 192.168.10.1:49723, idle 0:00:42, bytes 530, flags UIO N1
```

步驟 3.從Win10-03到Win10-04發起FTP連線。

步驟 4.運行 **show conn** 命令以確認在Instance02兩個例項中都建立了FTP連線。

<#root>

// Confirm the connection in Instance02 of FPR01 >

```
show conn
 TCP outside 192.168.40.1:21 inside 192.168.30.1:52144, idle 0:00:02, bytes 530, flags UIO N1 // Confirm
show conn
 TCP outside 192.168.40.1:21 inside 192.168.30.1:52144, idle 0:00:13, bytes 530, flags UIO N1
```

步驟 5.運行 connect ftd FTD01和 system support diagnostic-cli命令以進入ASA CLI。 運行 enable和 **crashinfo force watchdog** 命令以強制使主/主用裝置中的Instance01崩潰。

<#root>

Firepower-module1>

```
connect ftd FTD01
 >
system support diagnostic-cli
 FTD01>
enable
 Password: FTD01# FTD01#
crashinfo force watchdog
 reboot. Do you wish to proceed? [confirm]:
```

步驟 6.故障切換發生在Instance01中，FTP連線未中斷。 運行 show failover和 show conn命令以確認Instance01在FPR02中的狀態。

<#root>

>

show failover

**Failover On Failover unit Secondary Failover LAN Interface: ha_link Ethernet1/4 (up) ..... This host:
Other host: Primary - Failed Interface diagnostic (192.168.80.2): Unknown (Monitored) Interface inside (**

show conn

TCP outside 192.168.20.1:21 inside 192.168.10.1:49723, idle 0:02:25, bytes 533, flags U N1

步驟 7.在Instance01中發生的崩潰對Instance02沒有影響。 運行 show failover和 show conn命令以確認Instance02的狀態。

<#root>

>

show failover

**Failover On Failover unit Secondary Failover LAN Interface: ha_link Ethernet1/8 (up) ..... This host:
Other host: Primary - Active Interface diagnostic (192.168.81.1): Normal (Monitored) Interface inside (1**

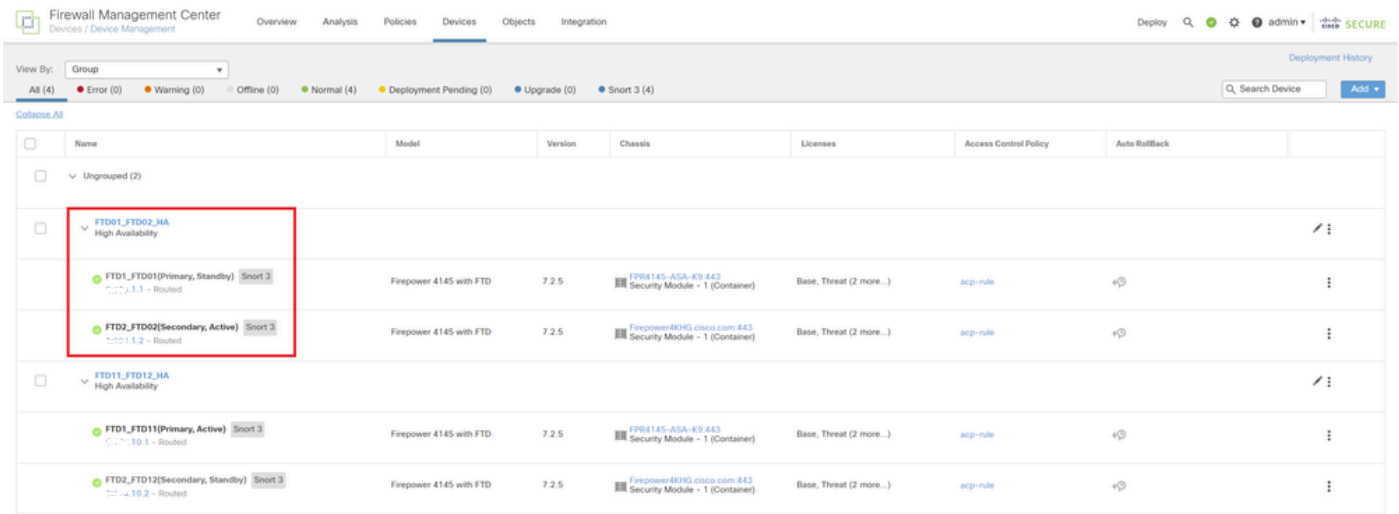
show conn

TCP outside 192.168.40.1:21 inside 192.168.30.1:52144, idle 0:01:18, bytes 533, flags UIO N1

步驟 8.在FMC上導航到**裝置** > **全部**。確認HA狀態。

·**FTD1_FTD01：主備模式**

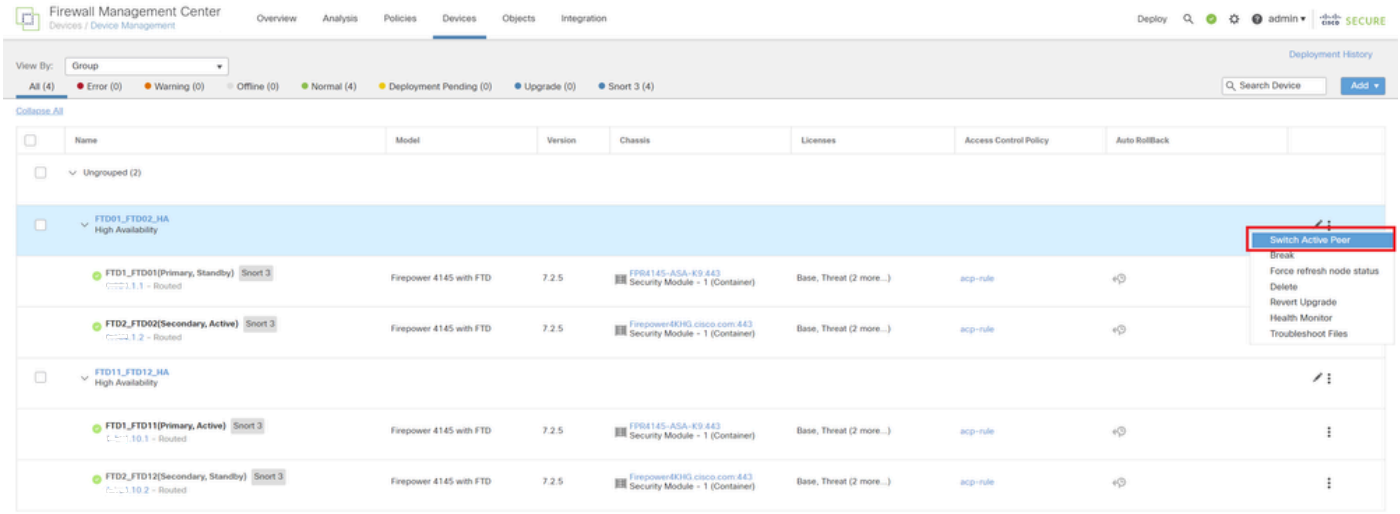
·**FTD2_FTD02：次要、活動**



確認*HA*狀態

步驟9.（可選）在FPR01的Instance01恢復正常後，您可以手動切換HA的狀態。這可以透過FMC GUI或FRP CLI來實現。

在FMC上，導航到**裝置** > **全部**。按一下**Switch Active Peer**以切換**FTD01_FTD02_HA**的HA狀態。



交換機*HA*狀態

在Firepower CLI上，運行 connect ftd FTD01和 system support diagnostic-cli命令以進入ASA CLI。 運行 enable和 **failover active** 命令以切換FTD01_FTD02_HA的HA。

<#root>

Firepower-module1>

connect ftd FTD01

>

system support diagnostic-cli

Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach. Type help or '?' for a list of availab

enable

firepower#

failover active

疑難排解

要驗證故障切換狀態，請運行 **show failover** 和 **show failover history** 命令。

<#root>

>

show failover

Failover On Failover unit Secondary Failover LAN Interface: ha_link Ethernet1/8 (up) ..... This host:
Other host: Primary - Active Interface diagnostic (192.168.81.1): Normal (Monitored) Interface inside (1

>

show failover history

```
================================================================================ From State To State Reason =
```

運行 debug fover <option>命令以啟用故障切換的調試日誌。

<#root>

>

```
debug fover
```

```
 auth Failover Cloud authentication cable Failover LAN status cmd-exec Failover EXEC command execution c
```

參考

https://www.cisco.com/c/en/us/support/docs/security/firepower-management-center/212699-configure-ftd-high-availability-on-firep.html

https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/multi-Instance/multi-Instance_solution.html

https://www.cisco.com/c/en/us/support/docs/availability/high-availability/217763-troubleshoot-firepower-threat-defense-hi.html#toc-hId-46641497

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）。