

升級由FDM管理的FTD HA

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[概觀](#)

[背景資訊](#)

[設定](#)

[步驟1.上傳升級包](#)

[步驟2.檢查準備情況](#)

[步驟3.在HA中升級FTD](#)

[步驟4.交換活動對等體 \(可選\)](#)

[步驟5.最終部署](#)

[驗證](#)

簡介

本文檔介紹由Firepower裝置管理器管理的Cisco Secure Firewall Threat Defense高可用性中的升級過程。

必要條件

需求

思科建議您瞭解以下主題：

- 高可用性(HA)概念和配置
- 思科安全Firepower裝置管理器(FDM)配置
- 思科安全防火牆威脅防禦(FTD)組態

採用元件

本檔案中的資訊是根據虛擬思科FTD版本7.2.8。

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。

概觀

FDM的工作方式是一次升級一個對等體。首先選擇Standby (備用)，然後選擇Active (活動)，在

活動升級開始之前執行故障切換。

背景資訊

升級軟體包必須先從software.cisco.com下載，然後才能升級。

在CLI關閉時，在作用中FTD中執行show high-availability configcommand以檢查HA的狀態。

```
> show high-availability config
```

```
Failover On
```

```
Failover unit Primary
```

```
Failover LAN Interface: failover-link GigabitEthernet0/2 (up)
```

```
Reconnect timeout 0:00:00
```

```
Unit Poll frequency 1 seconds, holdtime 15 seconds
```

```
Interface Poll frequency 5 seconds, holdtime 25 seconds
```

```
Interface Policy 1
```

```
Monitored Interfaces 3 of 311 maximum
```

```
MAC Address Move Notification Interval not set
```

```
failover replication http
```

```
Version: Ours 9.18(3)53, Mate 9.18(3)53
```

```
Serial Number: Ours 9A1QUNFWPK1, Mate 9A45VNEHB5C
```

```
Last Failover at: 11:57:26 UTC Oct 8 2024
```

```
    This host: Primary - Active
```

```
        Active time: 507441 (sec)
```

```
        slot 0: ASAv hw/sw rev (/9.18(3)53) status (Up Sys)
```

```
            Interface diagnostic (0.0.0.0): Normal (Waiting)
```

```
            Interface inside (192.168.45.1): Normal (Waiting)
```

```
            Interface outside (192.168.1.10): Normal (Waiting)
```

```
        slot 1: snort rev (1.0) status (up)
```

```
        slot 2: diskstatus rev (1.0) status (up)
```

```
    Other host: Secondary - Standby Ready
```

```
        Active time: 8 (sec)
```

```
            Interface diagnostic (0.0.0.0): Normal (Waiting)
```

```
Interface inside (0.0.0.0): Normal (Waiting)
Interface outside (0.0.0.0): Normal (Waiting)
slot 1: snort rev (1.0) status (up)
slot 2: diskstatus rev (1.0) status (up)
```

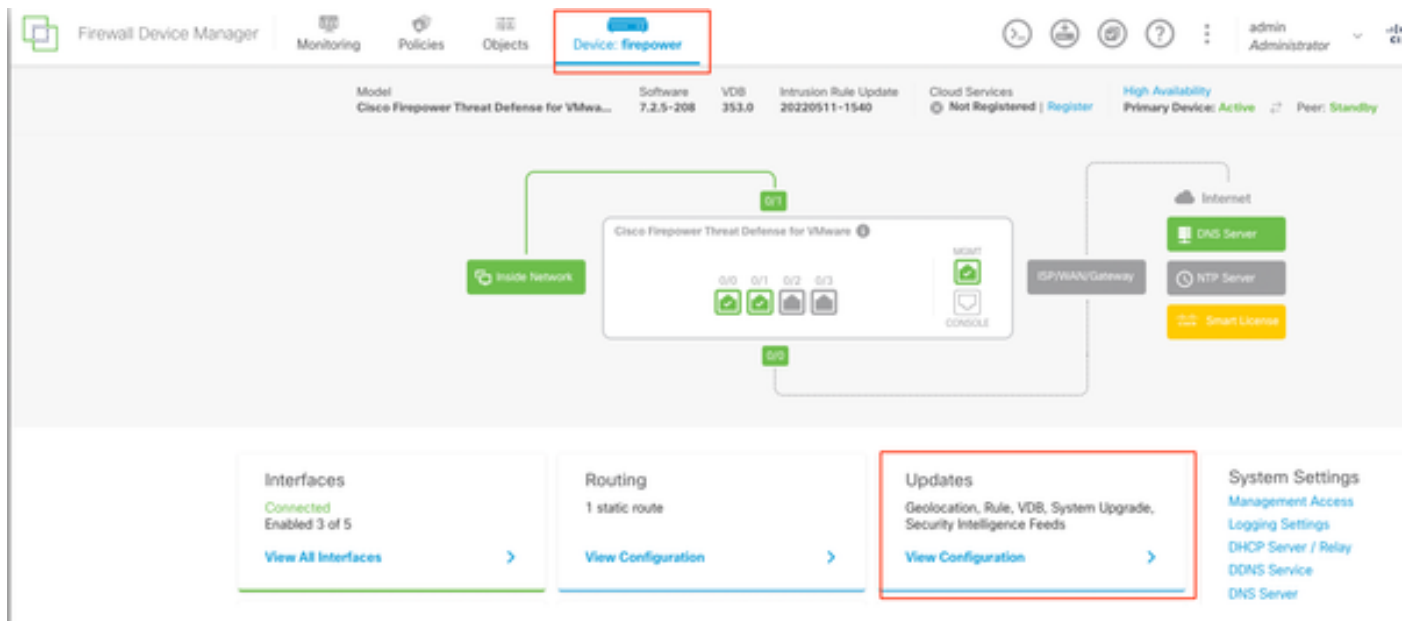
如果未顯示錯誤，則繼續升級。

設定

步驟1.上傳升級包

- 使用GUI將FTD升級包上傳到FDM。

先前必須根據FTD型號和所需的版本從思科軟體網站下載該封包。導覽至Device > Updates > System Upgrade。



更新

- 瀏覽找到先前下載的映像，然後選擇Upload。



附註：將映像上傳到主用和備用節點。

System Upgrade

Current version 7.2.5-208

Important

This device is a peer in a high availability configuration. You must install upgrades in a precise order. For details, see [link](#)

There are no software upgrades available on the system.

Upload an upgrade file to install.

BROWSE

運行就緒檢查

步驟2. 檢查準備情況

就緒性檢查確認裝置是否已準備好繼續升級。


- 選擇Run Upgrade Readiness Check。

System Upgrade

Current version 7.2.5-208

Important

This device is a peer in a high availability configuration. You must install upgrades in a precise order. For details, see [link](#)

File **Cisco_FTD_Upgrade-7.2.8-25.sh.REL....**  [Replace file](#)
14 Oct 2024 05:06 PM

Upgrade to **7.2.8-25**

Readiness Check **Not Performed Yet** | [Run Upgrade Readiness Check](#)

UPGRADE NOW

 Reboot required


運行就緒檢查

System Upgrade

Current version 7.2.5-208

i Important

This device is a peer in a high availability configuration. You must install upgrades in a precise order. For details, see [link](#)

File	Cisco_FTD_Upgrade-7.2.8-25.sh.REL....  Replace file
	14 Oct 2024 05:06 PM
Upgrade to	7.2.8-25


Readiness Check	Not Performed Yet	Run Upgrade Readiness Check
-----------------	-------------------	---------------------------------------------


UPGRADE NOW **i Reboot required**

運行就緒檢查

i Important

This device is a peer in a high availability configuration. You must install upgrades in a precise order. For details, see [link](#)

File	Cisco_FTD_Upgrade-7.2.8-25.sh.REL....  Replace file
	14 Oct 2024 05:06 PM
Upgrade to	7.2.8-25

Readiness Check	 Please Wait...
-----------------	-----------------------------------------------------------------------------------------------------------

UPGRADE NOW **i Reboot required**

運行就緒檢查


導航到System > Upgrade可以檢查進度。

System Upgrade

Current version 7.2.5-208

i Important

This device is a peer in a high availability configuration. You must install upgrades in a precise order. For details, see [link](#)

File **Cisco_FTD_Upgrade-7.2.8-25.sh.REL....**  | [Replace file](#)
14 Oct 2024 05:06 PM

Upgrade to **7.2.8-25**

Readiness Check **✓ Precheck Success** | [Run Upgrade Readiness Check](#)
14 Oct 2024 05:51 PM

UPGRADE NOW

i Reboot required

運行就緒檢查

當在FTD中完成就緒檢查且結果為「成功」時，即可完成升級。

步驟3.在HA中升級FTD

- 選擇Standby FDM，然後按一下Upgrade Now。

System Upgrade

Current version 7.2.5-208

i Important

This device is a peer in a high availability configuration. You must install upgrades in a precise order. For details, see [link](#)

File **Cisco_FTD_Upgrade-7.2.8-25.sh.REL....**  | [Replace file](#)
14 Oct 2024 05:06 PM

Upgrade to **7.2.8-25**

Readiness Check **✔ Precheck Success** | [Run Upgrade Readiness Check](#)
14 Oct 2024 05:51 PM

UPGRADE NOW

i Reboot required

立即升級

開始升級之前：

1. 請勿在系統升級的同時啟動系統還原。
2. 升級過程中請勿重新啟動系統。如果需要重新引導，系統會在升級期間的適當時間自動重新引導。
3. 升級過程中請勿關閉裝置的電源。中斷升級可能會使系統不可用。

升級開始時，您將退出系統。
安裝完成後，裝置將重新啟動。

Confirm System Upgrade



Before starting the upgrade:

1. Do not start a system restore at the same time as a system upgrade.
2. Do not reboot the system during the upgrade. The system automatically reboots at the appropriate time during upgrade if a reboot is necessary.
3. **Do not power off the device** during the upgrade. Interrupting the upgrade can leave the system in an unusable state.

You will be logged out of the system when the upgrade begins.
After the installation completes, the device will be rebooted.

UPGRADE OPTIONS

- Automatically cancel on upgrade failure and roll back to the previous version

CANCEL

CONTINUE

附註：每個FTD升級約需要20分鐘。

在CLI上，可以在升級資料夾/ngfw/var/log/sf中檢查進度；移至expert mode和enterroot access。

```
> expert
```

```
admin@firepower:~$ sudo su
```

```
Password:
```

```
root@firepower:/home/admin# cd /ngfw/var/log/sf
```

```
root@firepower:/ngfw/var/log/sf# ls
```

```
Cisco_FTD_Upgrade-7.2.8.
```

```
root@firepower:/ngfw/var/log/sf/Cisco_FTD_Upgrade-7.2.8# ls -lrt
```

```
root@firepower:/ngfw/var/log/sf/Cisco_FTD_Upgrade-7.2.8# tail -f status.log
```

```
ui: Upgrade in progress: ( 8% done.22 mins to reboot). Preparing to upgrade... (200_pre/011_check_self.
```

```
ui: Upgrade in progress: ( 8% done.22 mins to reboot). Preparing to upgrade... (200_pre/015_verify_rpm.
```

```
ui: Upgrade in progress: ( 8% done.22 mins to reboot). Preparing to upgrade... (200_pre/100_check_dashb
```

```
ui: Upgrade in progress: ( 8% done.22 mins to reboot). Preparing to upgrade... (200_pre/100_get_snort_f
```

```
ui: Upgrade in progress: (12% done.21 mins to reboot). Preparing to upgrade... (200_pre/110_setup_upgra
```

```
ui: Upgrade in progress: (12% done.21 mins to reboot). Preparing to upgrade... (200_pre/120_generate_au
```

```
ui: Upgrade in progress: (12% done.21 mins to reboot). Preparing to upgrade... (200_pre/152_save_etc_sf
```

```
ui: Upgrade in progress: (79% done. 5 mins to reboot). Finishing the upgrade... (999_finish/999_zz_inst
```

```
ui: Upgrade in progress: (83% done. 4 mins to reboot). Finishing the upgrade... (999_finish/999_zzz_com
```

```
ui: Upgrade complete
```

```
ui: The system will now reboot.
```

```
ui: System will now reboot.
```

```
Broadcast message from root@firepower (Mon Oct 14 12:01:26 2024):
```

```
System will reboot in 5 seconds due to system upgrade.
```

```
Broadcast message from root@firepower (Mon Oct 14 12:01:31 2024):
```

```
System will reboot now due to system upgrade.
```

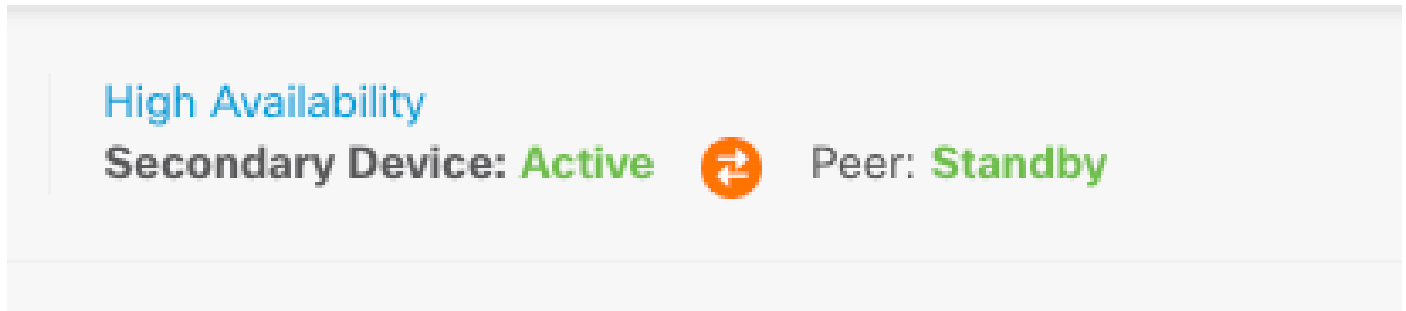
```
Broadcast message from root@firepower (Mon Oct 14 12:01:39 2024):
```

```
The system is going down for reboot NOW!
```

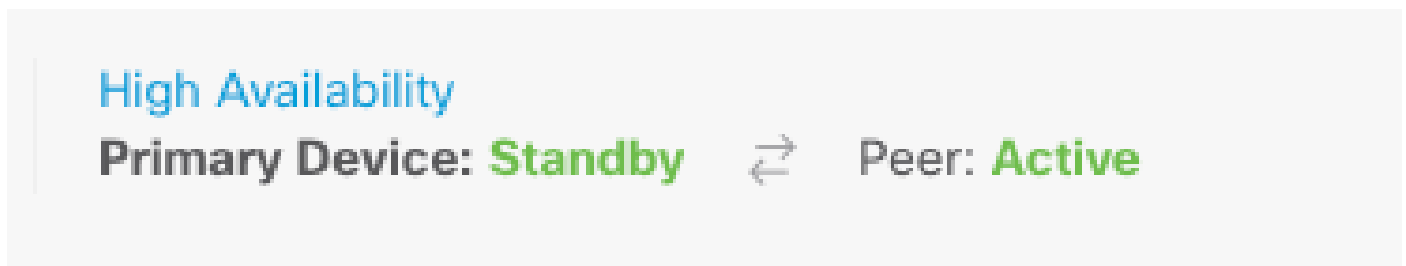
升級第二個裝置。

切換角色以使此裝置處於活動狀態：選擇Device> High Availability，然後從裝置選單中選擇Switch Mode。等待裝置的狀態，以便更改為活動狀態並確認流量正常流動。然後，註銷。

升級:重複上述步驟以登入新的備用裝置、上傳包、升級裝置、監控進度並驗證成功。



高可用性



高可用性

在CLI上，移至LINA（系統支援diagnostic-cli），並使用show failover state 指令檢查待命FTD上的容錯移轉狀態。

```
> system support diagnostic-cli
```

```
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
```

```
Type help or '?' for a list of available commands.
```

```
primary_ha> enable
```

```
Password:
```

```
primary_ha# show failover state
```

	State	Last Failure Reason	Date/Time
This host -	Primary		
	Standby Ready	None	
Other host -	Secondary		

Active None

====Configuration State====

 Sync Skipped - STANDBY

====Communication State====

 Mac set

primary_ha#

步驟4.交換活動對等體 (可選)



附註：如果輔助裝置處於活動狀態，它不會對操作有任何影響。

將主裝置設定為主用裝置，將輔助裝置設定為備用裝置，這是幫助跟蹤可能發生的任何故障轉移的最佳實踐。

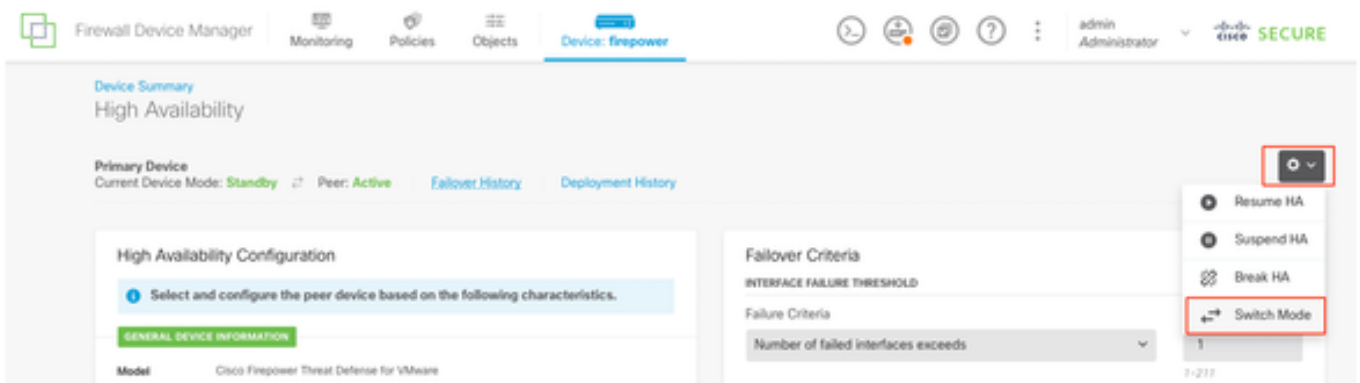
在此案例中，FTD Active現為Standby，可以使用手動故障切換將其設回Active。

- 導覽至Devices > High Availability。



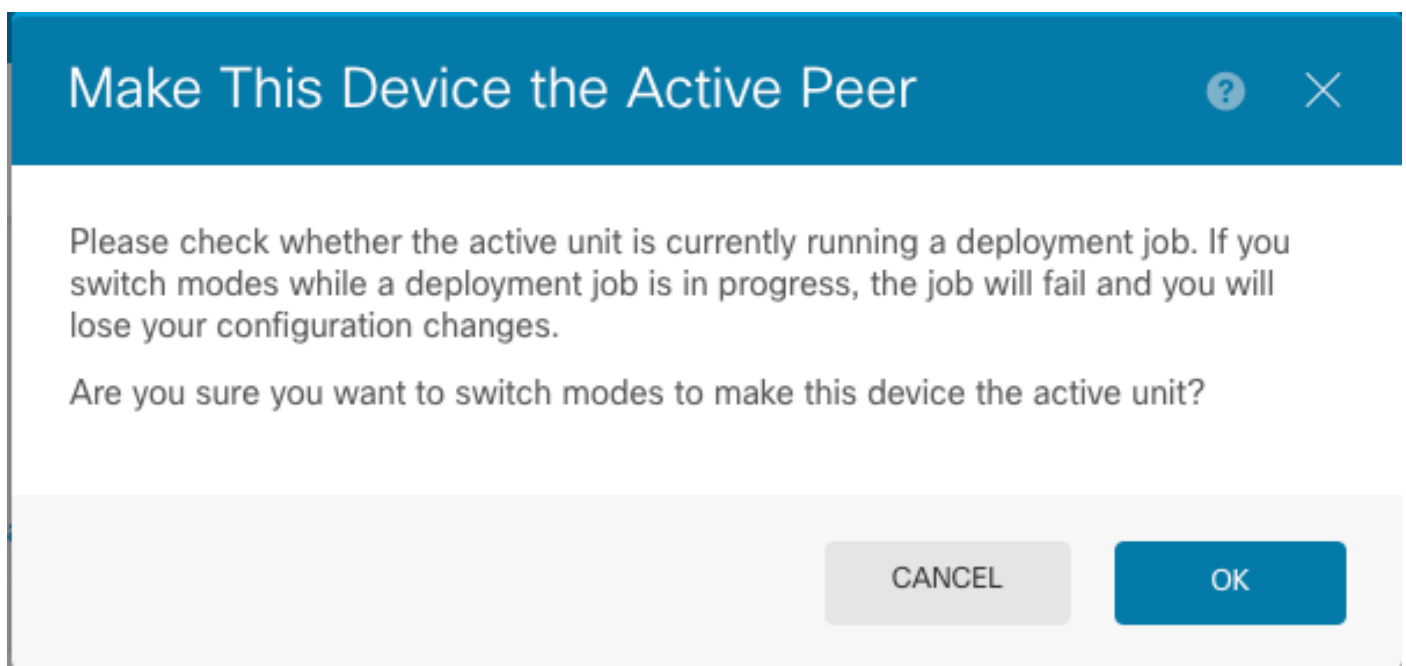
高可用性

- 選擇Switch Mode。



交換模式

- 選擇OK以確認故障轉移。



活動對等體

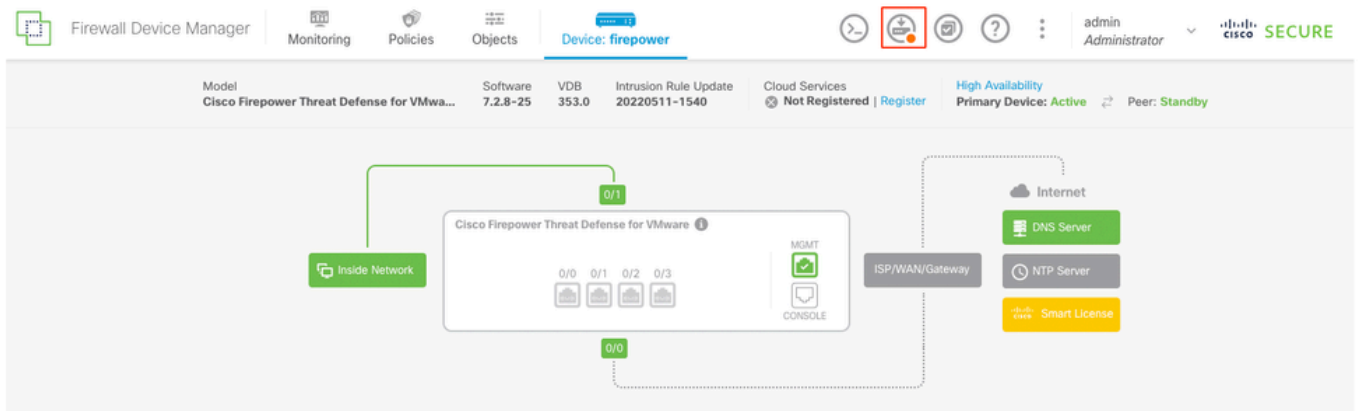
在升級結束時驗證HA狀態並完成故障轉移。



裝置

步驟5.最終部署

- 通過按一下Deploy (部署) 頁籤下的DEPLOY NOW (立即部署) 將策略部署到裝置。



Pending Changes



✓ **Last Deployment Completed Successfully**
14 Oct 2024 06:26 PM. [See Deployment History](#)

Deployed Version (14 Oct 2024 06:26 PM)	Pending Version	LEGEND
Rule Update Version Edited: 20220511-1540		
lastSuccessSRUDate: 2024-10-08 06:15:04Z	2024-10-14 12:53:26Z	
-	lspVersions[1]: 20220511-1540	
VDB Version Edited: 353		
+ Snort Version Added: 3.1.21.800-2		
-	snortVersion: 3.1.21.800-2	
-	snortPackage: /ngfw/var/sf/snort-3.1.21.800-2/snor...	
-	name: 3.1.21.800-2	
Data SSL Cipher Setting Edited: DefaultDataSSLCipherSetting		
SSL Cipher Edited: DefaultSSLCipher		
-	protocolVersions[0]: TLSV1	
-	protocolVersions[1]: DTLSV1	
-	protocolVersions[2]: TLSV1_1	
Intrusion Policy Edited: Security Over Connectivity - Cisco Talos		
Intrusion Policy Edited: Maximum Detection - Cisco Talos		
MORE ACTIONS ▾	CANCEL	DEPLOY NOW ▾

策略部署

驗證

若要確認HA狀態和升級是否完成，您必須確認狀態：

主要：Active（作用中）

輔助：備用就緒

兩者都使用最近變更的版本（本例中為7.2.8）。



容錯移轉

- 在CLI上，使用show failover states命令和show failoverflow命令檢查故障切換狀態，以瞭解更多詳細資訊。

Cisco Firepower可擴展作業系統(FX-OS)v2.12.1 (內部版本73)
適用於VMware v7.2.8的Cisco Firepower威脅防禦 (內部版本25)

```
> show failover state
```

	State	Last Failure Reason	Date/Time
This host -	Primary		
	Active	None	
Other host -	Secondary		
	Standby Ready	None	

```
====Configuration State====
```

```
    Sync Skipped
```

```
====Communication State====
```

```
    Mac set
```

```
> show failover
```

```
Failover On
```

```
Failover unit Primary
```

```
Failover LAN Interface: failover-link GigabitEthernet0/2 (up)
```

Reconnect timeout 0:00:00

Unit Poll frequency 1 seconds, holdtime 15 seconds

Interface Poll frequency 5 seconds, holdtime 25 seconds

Interface Policy 1

Monitored Interfaces 3 of 311 maximum

MAC Address Move Notification Interval not set

failover replication http

Version: Ours 9.18(4)210, Mate 9.18(4)210

Serial Number: Ours 9A1QUNFWPK1, Mate 9A45VNEHB5C

Last Failover at: 14:13:56 UTC Oct 15 2024

This host: Primary - Active

Active time: 580 (sec)

slot 0: ASAv hw/sw rev (/9.18(4)210) status (Up Sys)

Interface diagnostic (0.0.0.0): Normal (Waiting)

Interface inside (192.168.45.1): Normal (Waiting)

Interface outside (192.168.1.10): Normal (Waiting)

slot 1: snort rev (1.0) status (up)

slot 2: diskstatus rev (1.0) status (up)

Other host: Secondary - Standby Ready

Active time: 91512 (sec)

Interface diagnostic (0.0.0.0): Normal (Waiting)

Interface inside (0.0.0.0): Normal (Waiting)

Interface outside (0.0.0.0): Normal (Waiting)

slot 1: snort rev (1.0) status (up)

slot 2: diskstatus rev (1.0) status (up)

Stateful Failover Logical Update Statistics

Link : failover-link GigabitEthernet0/2 (up)

Stateful Obj	xmit	xerr	rcv	rerr
General	11797	0	76877	0

sys cmd	11574	0	11484	0
up time	0	0	0	0
RPC services	0	0	0	0
TCP conn	0	0	0	0
UDP conn	176	0	60506	0
ARP tbl	45	0	4561	0
Xlate_Timeout	0	0	0	0
IPv6 ND tbl	0	0	0	0
VPN IKEv1 SA	0	0	0	0
VPN IKEv1 P2	0	0	0	0
VPN IKEv2 SA	0	0	0	0
VPN IKEv2 P2	0	0	0	0
VPN CTCP upd	0	0	0	0
VPN SDI upd	0	0	0	0
VPN DHCP upd	0	0	0	0
SIP Session	0	0	0	0
SIP Tx	0	0	0	0
SIP Pinhole	0	0	0	0
Route Session	1	0	0	0
Router ID	0	0	0	0
User-Identity	0	0	30	0
CTS SGTNAME	0	0	0	0
CTS PAC	0	0	0	0
TrustSec-SXP	0	0	0	0
IPv6 Route	0	0	0	0
STS Table	0	0	0	0
Umbrella Device-ID	0	0	0	0
Rule DB B-Sync	0	0	30	0
Rule DB P-Sync	1	0	266	0
Rule DB Delete	0	0	0	0

Logical Update Queue Information

	Cur	Max	Total
Recv Q:	0	31	123591
Xmit Q:	0	1	12100

如果兩個FTD位於相同版本上，而HA狀態為正常，則升級已完成。

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）。