升級FTD HA（由FMC管理）

目錄

簡介

本文檔介紹由防火牆管理中心管理的高可用性思科安全防火牆威脅防禦的升級過程。

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
- 安全防火牆管理中心(FMC)配置
- 思科安全防火牆威脅防禦(FTD)組態

採用元件

本文檔中的資訊基於：

- 虛擬防火牆管理中心(FMC) 7.2.4版
- 虛擬思科防火牆威脅防禦(FTD)，版本7.0.1

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

FMC的工作方式是一次升級一個對等體。先是Standby（備用），然後是Active（活動），在Active（活動）升級完成之前執行故障切換。

背景資訊

升級前必須從software.cisco.com下載升級套件。

在CLI上，於作用中FTD中執行show high-availability config命令，以檢查高可用性的狀態。

```
> show high-availability config
Failover On
Failover unit Secondary
Failover LAN Interface: FAILOVER_LINK GigabitEthernet0/0 (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 1285 maximum
MAC Address Move Notification Interval not set
failover replication http
Version: Ours 9.16(2)5, Mate 9.16(2)5
Serial Number: Ours 9AJJSEGJS2T, Mate 9AVLW3FSSK8
Last Failover at: 00:37:48 UTC Jul 20 2023

        This host: Secondary - Standby Ready
                Active time: 4585 (sec)
                slot 0: ASAv hw/sw rev (/9.16(2)5) status (Up Sys)
                  Interface INSIDE (10.10.153.2): Normal (Monitored)
                  Interface diagnostic (0.0.0.0): Normal (Waiting)
                  Interface OUTSIDE (10.20.153.2): Normal (Monitored)
                slot 1: snort rev (1.0)  status (up)
                slot 2: diskstatus rev (1.0)  status (up)

        Other host: Primary - Active
                Active time: 60847 (sec)
                  Interface INSIDE (10.10.153.1): Normal (Monitored)
                  Interface diagnostic (0.0.0.0): Normal (Waiting)
                  Interface OUTSIDE (10.20.153.1): Normal (Monitored)
                slot 1: snort rev (1.0)  status (up)
                slot 2: diskstatus rev (1.0)  status (up)

Stateful Failover Logical Update Statistics

        Link : FAILOVER_LINK GigabitEthernet0/0 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         9192       0          10774      0
        sys cmd         9094       0          9092       0
…
        Rule DB B-Sync  0          0          0          0
        Rule DB P-Sync  0          0          204        0
        Rule DB Delete  0          0          1          0

        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       9       45336
        Xmit Q:         0       11      11572
```

如果未顯示錯誤，則繼續升級。

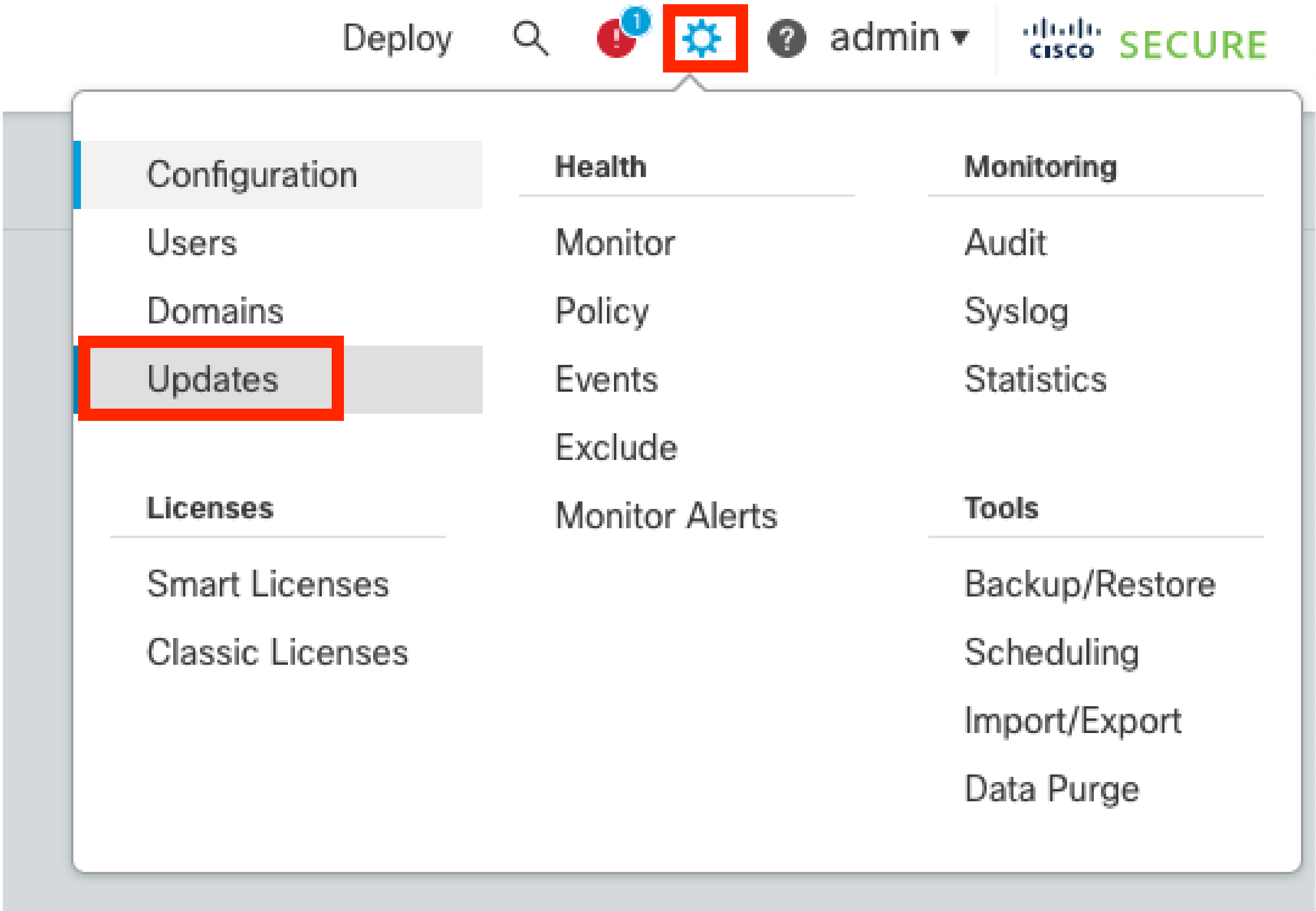
設定

步驟 1.上傳升級套件

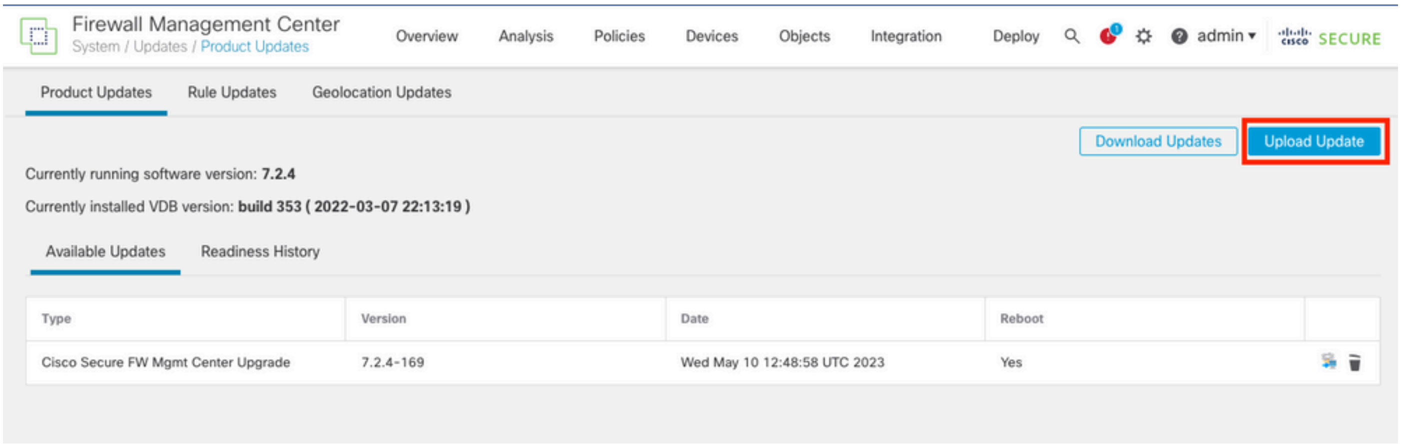
- 使用圖形使用者介面(GUI)將FTD升級套件上傳到FMC。
  之前必須根據FTD型號和想要的版本從思科軟體網站下載此套件。

警告：請確定FMC版本高於或等於要升級的新FTD版本。

系統>更新



- 選擇Upload Update。

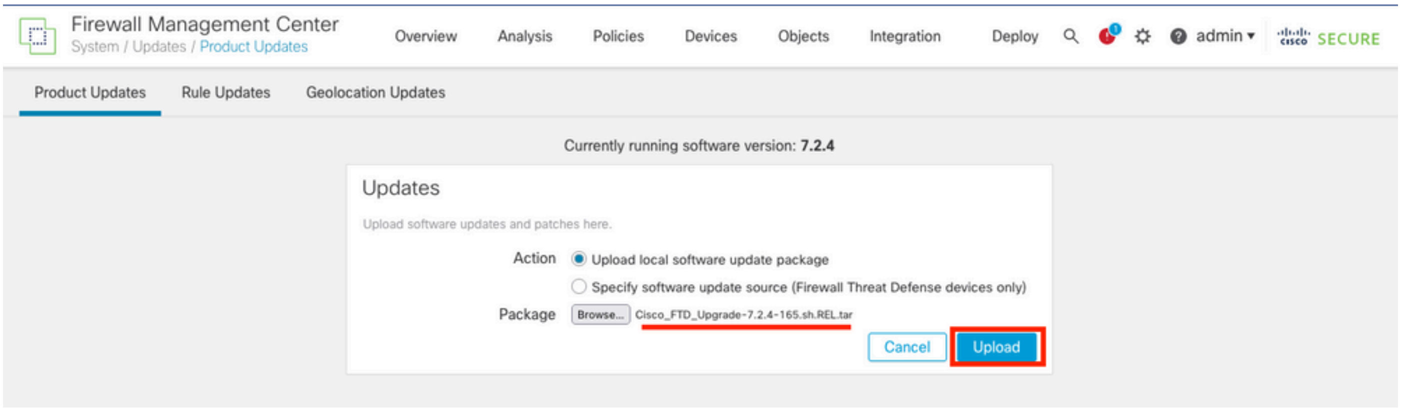


Currently running software version: **7.2.4**

Currently installed VDB version: **build 353 (2022-03-07 22:13:19)**

Type	Version	Date	Reboot
Cisco Secure FW Mgmt Center Upgrade	7.2.4-169	Wed May 10 12:48:58 UTC 2023	Yes

- 瀏覽找到先前下載的映象，然後選擇Upload。



Currently running software version: **7.2.4**

Updates

Upload software updates and patches here.

Action ● Upload local software update package

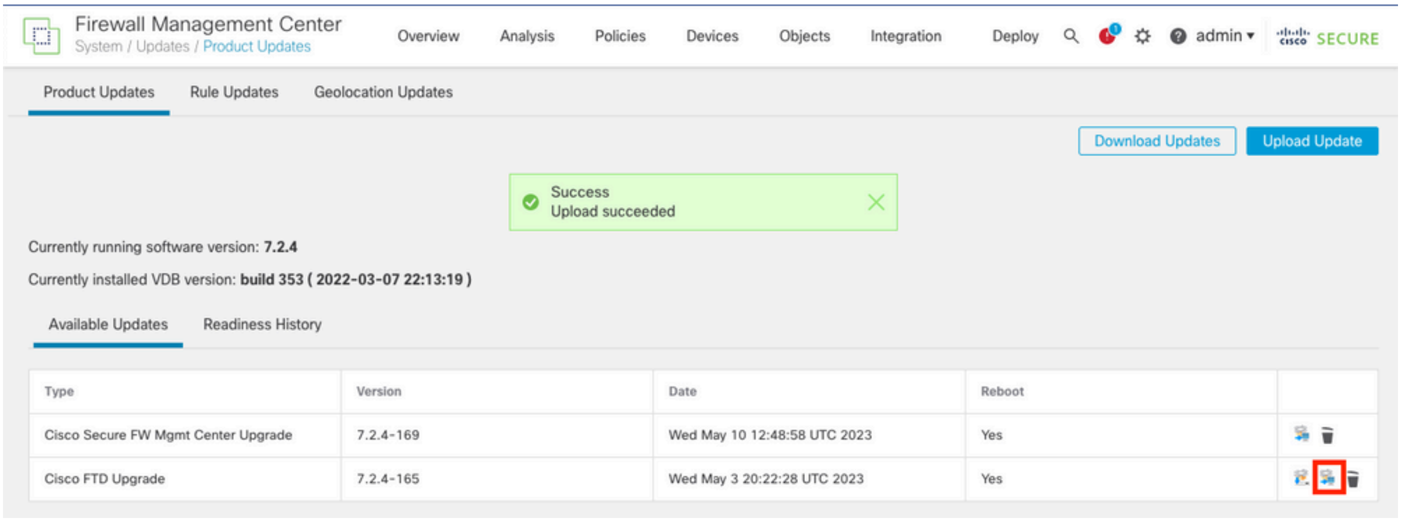
○ Specify software update source (Firewall Threat Defense devices only)

Package Cisco_FTD_Upgrade-7.2.4-165.sh.REL.tar

步驟 2.檢查就緒性

就緒性檢查可確認裝置是否已準備好繼續升級。

- 在正確的升級軟體套件中選擇Install選項。



Success
Upload succeeded

Currently running software version: **7.2.4**

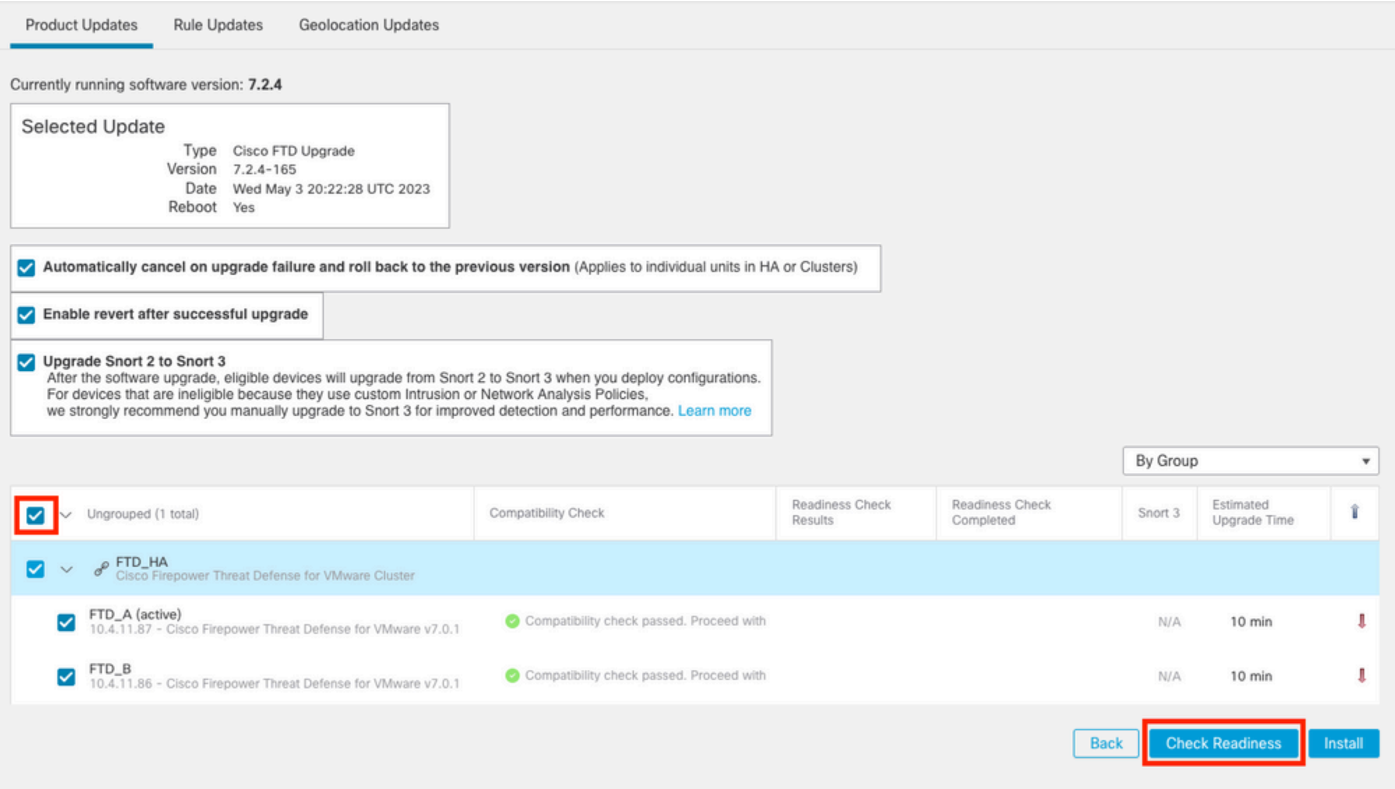
Currently installed VDB version: **build 353 (2022-03-07 22:13:19)**

Type	Version	Date	Reboot
Cisco Secure FW Mgmt Center Upgrade	7.2.4-169	Wed May 10 12:48:58 UTC 2023	Yes
Cisco FTD Upgrade	7.2.4-165	Wed May 3 20:22:28 UTC 2023	Yes

選擇您喜歡的升級。在本例中，選擇用於：

- 升級失敗時自動取消，並回滾到以前的版本。
- 在成功升級後啟用還原。
- 將Snort 2升級到Snort 3。

- 選擇FTD的HA群組並按一下Check Readiness。



Currently running software version: **7.2.4**

Selected Update

Type	Cisco FTD Upgrade
Version	7.2.4-165
Date	Wed May 3 20:22:28 UTC 2023
Reboot	Yes

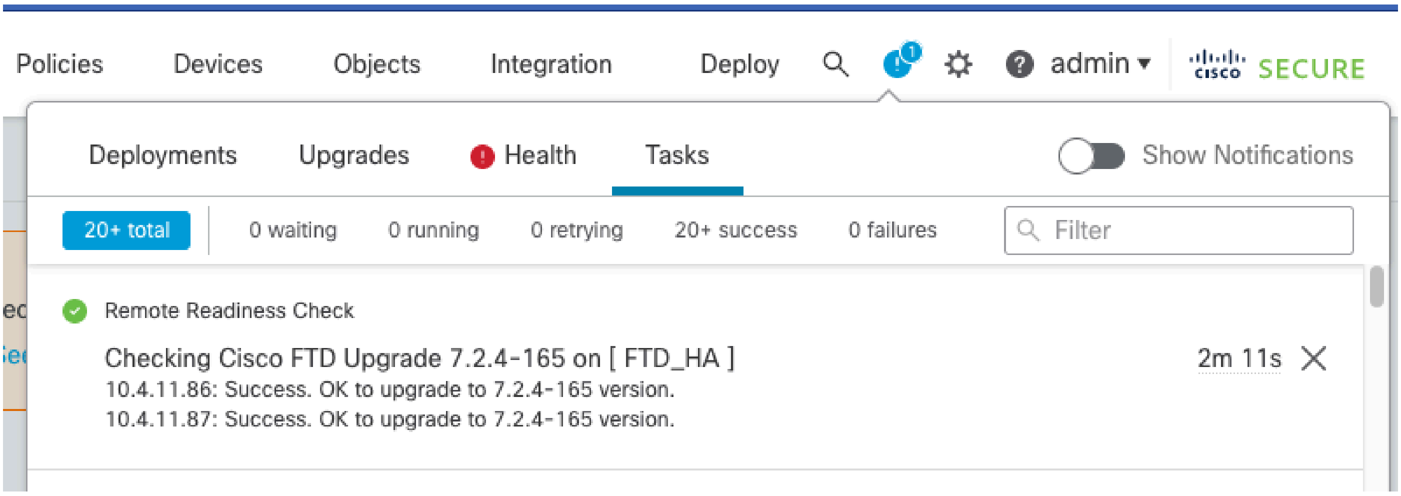
☑ **Automatically cancel on upgrade failure and roll back to the previous version** (Applies to individual units in HA or Clusters)

☑ **Enable revert after successful upgrade**

☑ **Upgrade Snort 2 to Snort 3**
After the software upgrade, eligible devices will upgrade from Snort 2 to Snort 3 when you deploy configurations.
For devices that are ineligible because they use custom Intrusion or Network Analysis Policies,
we strongly recommend you manually upgrade to Snort 3 for improved detection and performance. Learn more

☑ Ungrouped (1 total)	Compatibility Check	Readiness Check Results	Readiness Check Completed	Snort 3	Estimated Upgrade Time
☑ FTD_HA Cisco Firepower Threat Defense for VMware Cluster					
☑ FTD_A (active) 10.4.11.87 - Cisco Firepower Threat Defense for VMware v7.0.1	✓ Compatibility check passed. Proceed with			N/A	10 min
☑ FTD_B 10.4.11.86 - Cisco Firepower Threat Defense for VMware v7.0.1	✓ Compatibility check passed. Proceed with			N/A	10 min

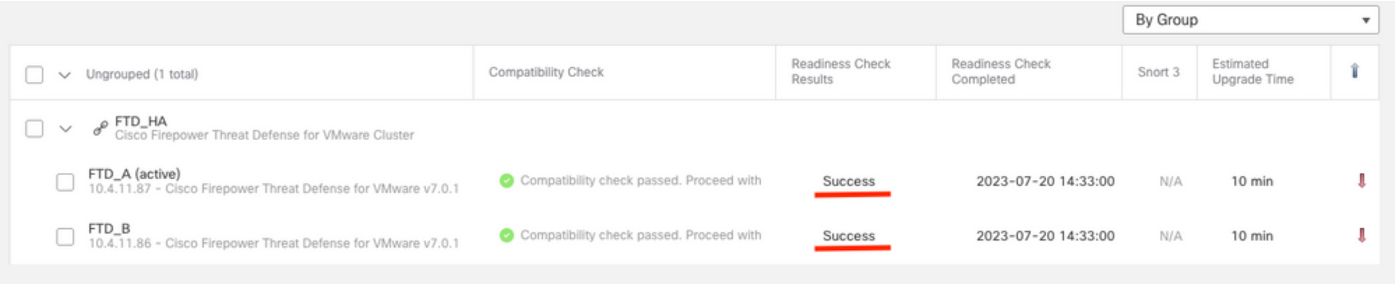
您可以在消息中心Messages > Tasks中檢查進度。



Remote Readiness Check

Checking Cisco FTD Upgrade 7.2.4-165 on [FTD_HA] 2m 11s
10.4.11.86: Success. OK to upgrade to 7.2.4-165 version.
10.4.11.87: Success. OK to upgrade to 7.2.4-165 version.

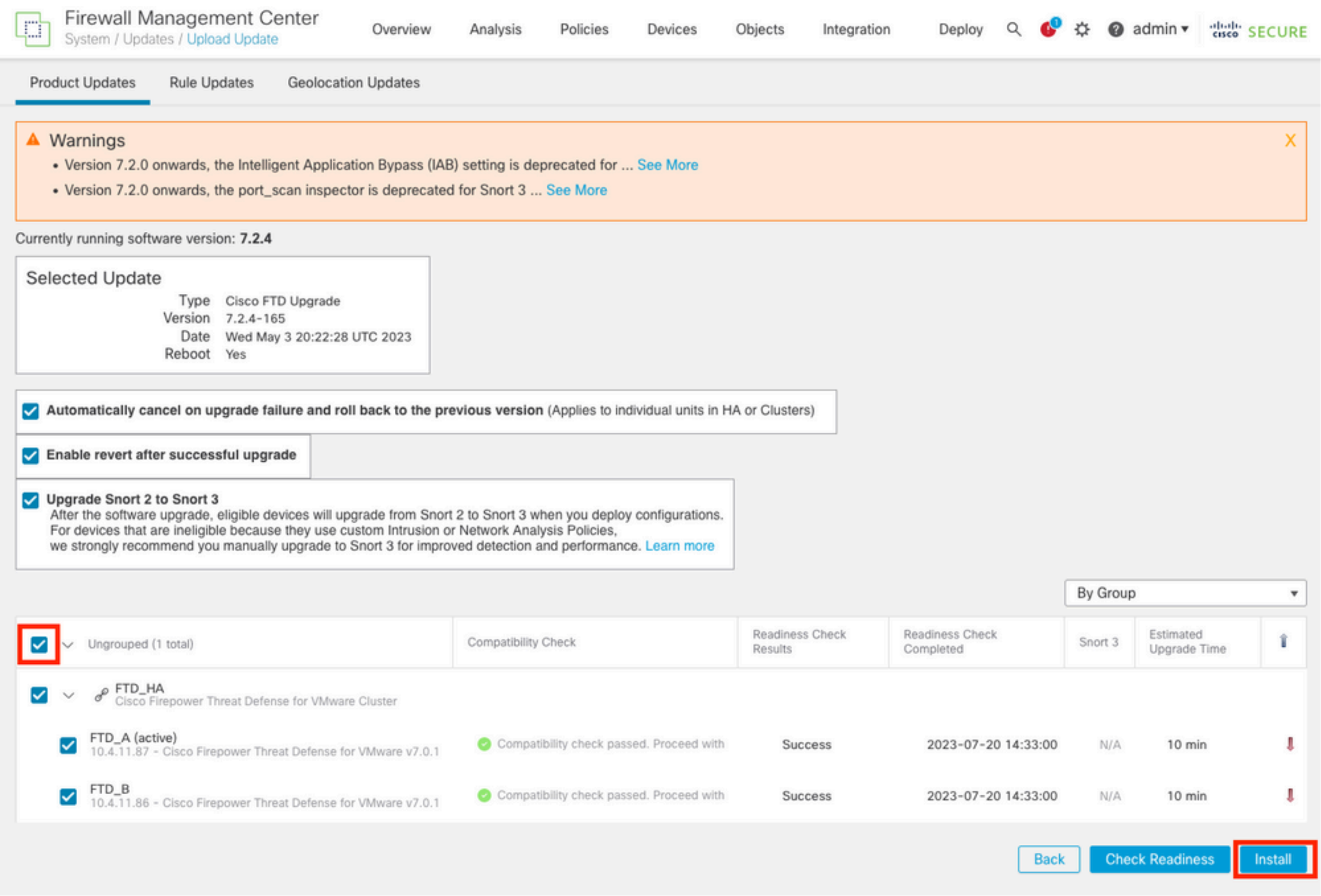
當FTD中完成整備檢查且結果為「成功」時，即可完成升級。



□ Ungrouped (1 total)	Compatibility Check	Readiness Check Results	Readiness Check Completed	Snort 3	Estimated Upgrade Time
□ FTD_HA Cisco Firepower Threat Defense for VMware Cluster					
□ FTD_A (active) 10.4.11.87 - Cisco Firepower Threat Defense for VMware v7.0.1	✓ Compatibility check passed. Proceed with	Success	2023-07-20 14:33:00	N/A	10 min
□ FTD_B 10.4.11.86 - Cisco Firepower Threat Defense for VMware v7.0.1	✓ Compatibility check passed. Proceed with	Success	2023-07-20 14:33:00	N/A	10 min

步驟 3.以高可用性升級FTD

- 選擇HA Pair並按一下Install。



Warnings

- Version 7.2.0 onwards, the Intelligent Application Bypass (IAB) setting is deprecated for ... See More
- Version 7.2.0 onwards, the port_scan inspector is deprecated for Snort 3 ... See More

Currently running software version: **7.2.4**

Selected Update

Type	Cisco FTD Upgrade
Version	7.2.4-165
Date	Wed May 3 20:22:28 UTC 2023
Reboot	Yes

☑ **Automatically cancel on upgrade failure and roll back to the previous version** (Applies to individual units in HA or Clusters)

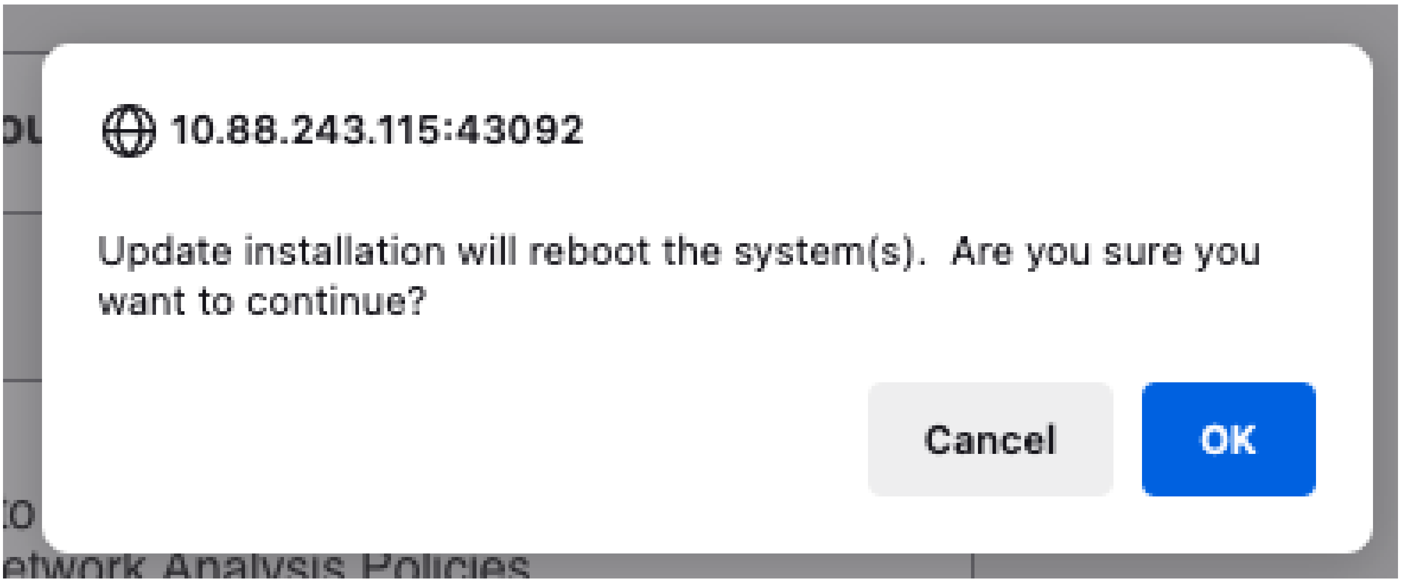
☑ **Enable revert after successful upgrade**

☑ **Upgrade Snort 2 to Snort 3**
After the software upgrade, eligible devices will upgrade from Snort 2 to Snort 3 when you deploy configurations.
For devices that are ineligible because they use custom Intrusion or Network Analysis Policies,
we strongly recommend you manually upgrade to Snort 3 for improved detection and performance. Learn more

By Group

☑ Ungrouped (1 total)	Compatibility Check	Readiness Check Results	Readiness Check Completed	Snort 3	Estimated Upgrade Time
☑ FTD_HA Cisco Firepower Threat Defense for VMware Cluster					
☑ FTD_A (active) 10.4.11.87 - Cisco Firepower Threat Defense for VMware v7.0.1	Compatibility check passed. Proceed with	Success	2023-07-20 14:33:00	N/A	10 min
☑ FTD_B 10.4.11.86 - Cisco Firepower Threat Defense for VMware v7.0.1	Compatibility check passed. Proceed with	Success	2023-07-20 14:33:00	N/A	10 min

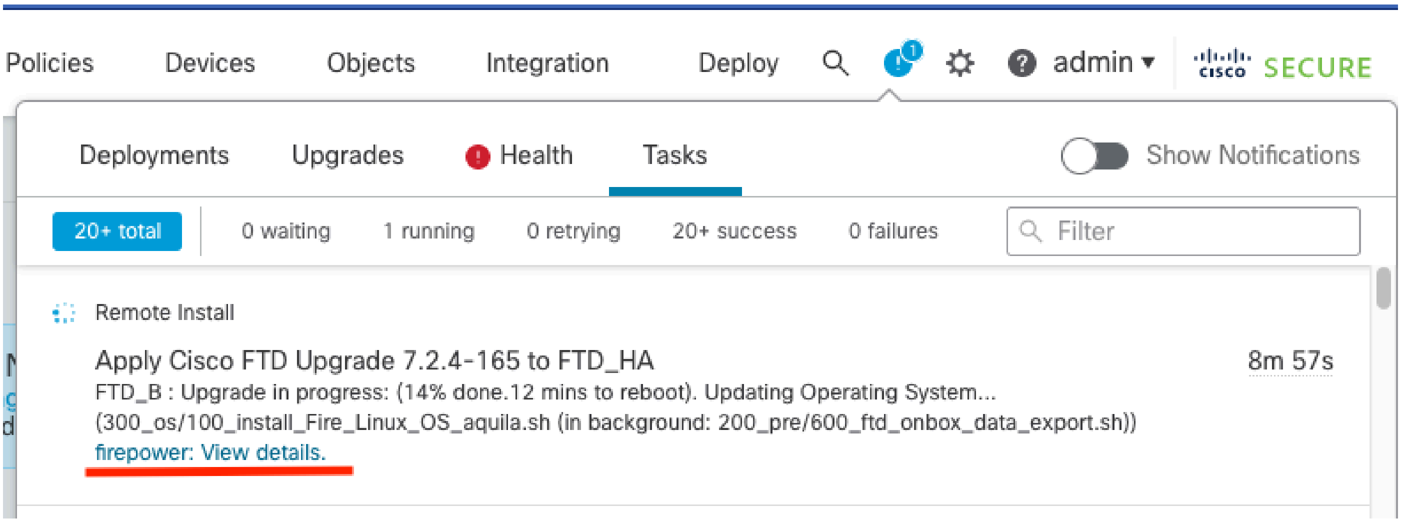
警告要繼續升級，系統會重新啟動以完成升級。選擇OK。



10.88.243.115:43092

Update installation will reboot the system(s). Are you sure you want to continue?

您可以在消息中心Messages > Tasks中檢查進度。

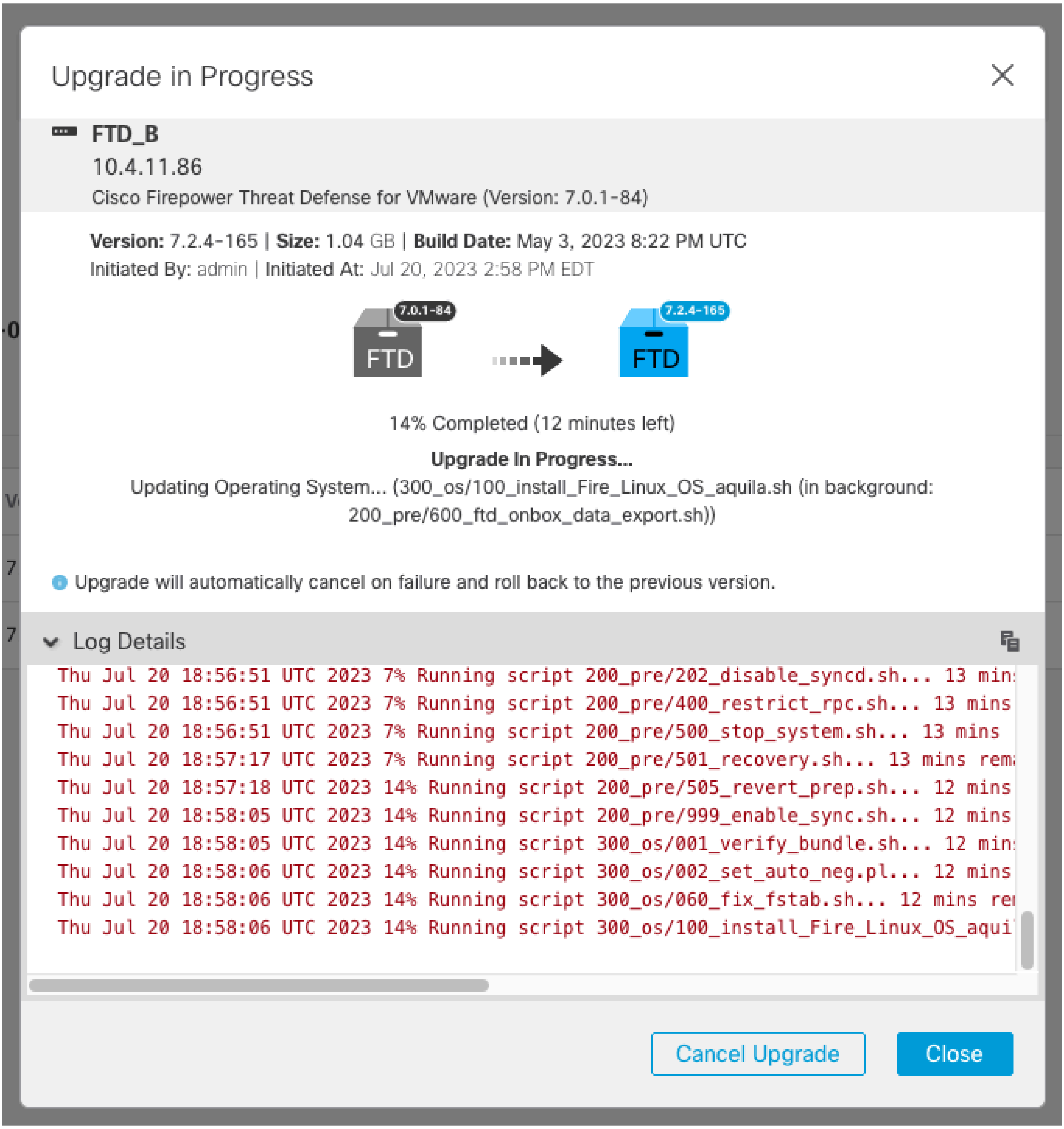


Remote Install

Apply Cisco FTD Upgrade 7.2.4-165 to FTD_HA 8m 57s

FTD_B : Upgrade in progress: (14% done.12 mins to reboot). Updating Operating System...
(300_os/100_install_Fire_Linux_OS_aquila.sh (in background: 200_pre/600_ftd_onbox_data_export.sh))
firepower: View details.

如果按一下firepower：檢視詳細資訊，則會以圖形方式顯示進度以及status.log的日誌。



Upgrade in Progress

FTD_B

10.4.11.86

Cisco Firepower Threat Defense for VMware (Version: 7.0.1-84)

Version: 7.2.4-165 | **Size:** 1.04 GB | **Build Date:** May 3, 2023 8:22 PM UTC

Initiated By: admin | Initiated At: Jul 20, 2023 2:58 PM EDT

14% Completed (12 minutes left)

Upgrade In Progress...

Updating Operating System... (300_os/100_install_Fire_Linux_OS_aquila.sh (in background: 200_pre/600_ftd_onbox_data_export.sh))

Upgrade will automatically cancel on failure and roll back to the previous version.

Log Details

```
Thu Jul 20 18:56:51 UTC 2023 7% Running script 200_pre/202_disable_syncd.sh... 13 min
Thu Jul 20 18:56:51 UTC 2023 7% Running script 200_pre/400_restrict_rpc.sh... 13 mins
Thu Jul 20 18:56:51 UTC 2023 7% Running script 200_pre/500_stop_system.sh... 13 mins
Thu Jul 20 18:57:17 UTC 2023 7% Running script 200_pre/501_recovery.sh... 13 mins rem
Thu Jul 20 18:57:18 UTC 2023 14% Running script 200_pre/505_revert_prep.sh... 12 mins
Thu Jul 20 18:58:05 UTC 2023 14% Running script 200_pre/999_enable_sync.sh... 12 mins
Thu Jul 20 18:58:05 UTC 2023 14% Running script 300_os/001_verify_bundle.sh... 12 min
Thu Jul 20 18:58:06 UTC 2023 14% Running script 300_os/002_set_auto_neg.pl... 12 mins
Thu Jul 20 18:58:06 UTC 2023 14% Running script 300_os/060_fix_fstab.sh... 12 mins re
Thu Jul 20 18:58:06 UTC 2023 14% Running script 300_os/100_install_Fire_Linux_OS_aqui
```

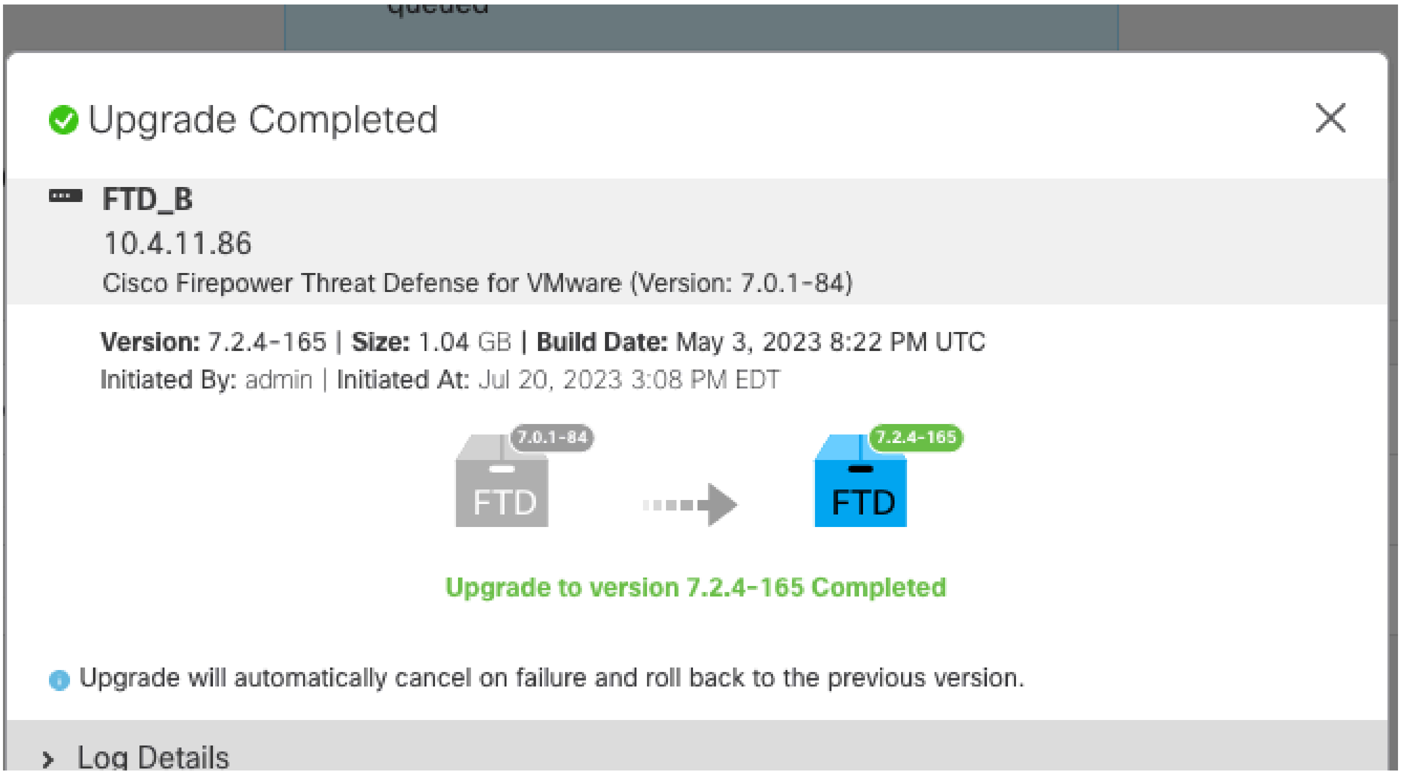
附註：每FTD升級約需20分鐘。

在CLI中，可以在升級資料夾/ngfw/var/log/sf中檢查進度；請轉到expert模式並輸入root 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-7.2.4

root@firepower:/ngfw/var/log/sf# cd Cisco_FTD_Upgrade-7.2.4

root@firepower:/ngfw/var/log/sf/Cisco_FTD_Upgrade-7.2.4# ls
000_start  AQ_UUID  DBCheck.log  finished_kickstart.flag  flags.conf  main_upgrade_script.log  status.l

root@firepower:/ngfw/var/log/sf/Cisco_FTD_Upgrade-7.2.4# tail -f status.log
state:running
ui:Upgrade has begun.
```

```
ui: Upgrade in progress: ( 0% done.14 mins to reboot). Checking device readiness... (000_start/000_00_r
…
ui: Upgrade in progress: (64% done. 5 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 (Thu Jul 20 19:05:20 2023):

System will reboot in 5 seconds due to system upgrade.

Broadcast message from root@firepower (Thu Jul 20 19:05:25 2023):

System will reboot now due to system upgrade.

Broadcast message from root@firepower (Thu Jul 20 19:05:34 2023):

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

升級狀態在GUI上標籤為已完成，並顯示後續步驟。



Upgrade Completed

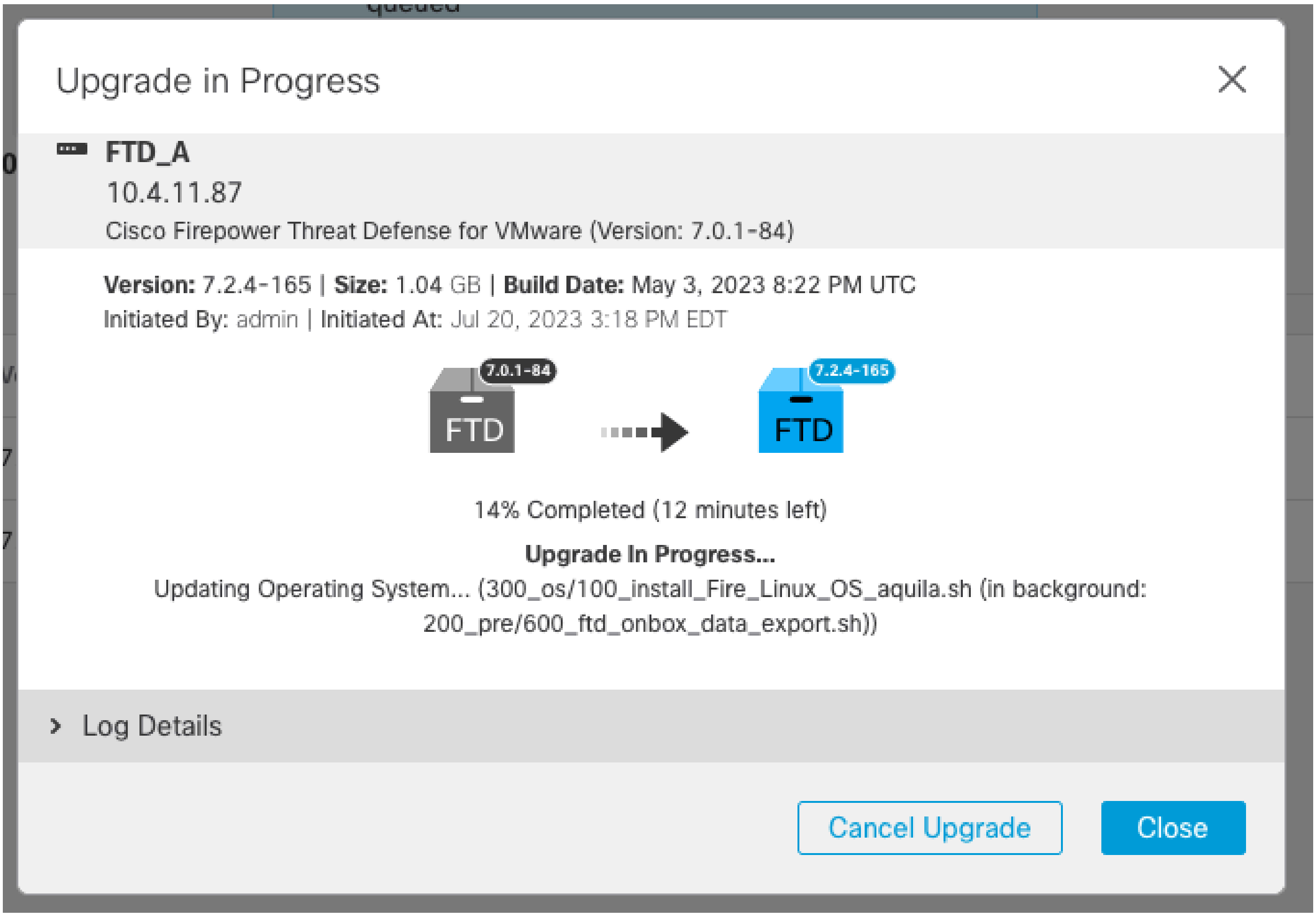
FTD_B
10.4.11.86
Cisco Firepower Threat Defense for VMware (Version: 7.0.1-84)

Version: 7.2.4-165 | **Size:** 1.04 GB | **Build Date:** May 3, 2023 8:22 PM UTC
Initiated By: admin | **Initiated At:** Jul 20, 2023 3:08 PM EDT

Upgrade to version 7.2.4-165 Completed

Upgrade will automatically cancel on failure and roll back to the previous version.

在備用裝置中完成升級後，它將在主用裝置中啟動。



Upgrade in Progress

FTD_A

10.4.11.87

Cisco Firepower Threat Defense for VMware (Version: 7.0.1-84)

Version: 7.2.4-165 | **Size:** 1.04 GB | **Build Date:** May 3, 2023 8:22 PM UTC

Initiated By: admin | Initiated At: Jul 20, 2023 3:18 PM EDT

14% Completed (12 minutes left)

Upgrade In Progress...

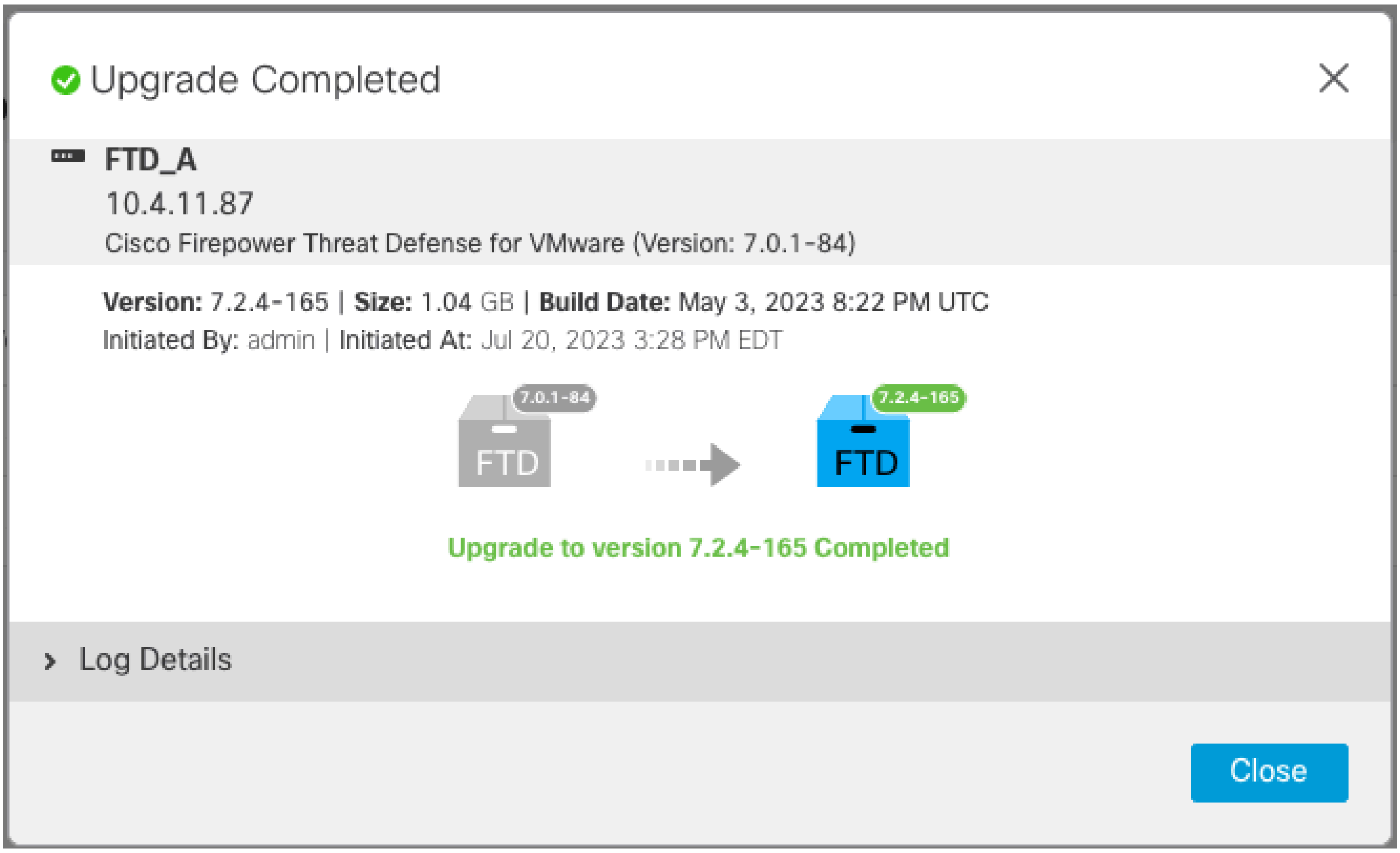
Updating Operating System... (300_os/100_install_Fire_Linux_OS_aquila.sh (in background: 200_pre/600_ftd_onbox_data_export.sh))

在CLI上，轉到LINA（系統支援diagnostic-cli），並使用命令show failover state檢查備用FTD上的故障切換狀態。

```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

firepower> enable
Password:
firepower# show failover state

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

====Configuration State===
        Sync Done - STANDBY
====Communication State===
        Mac set

firepower#
        Switching to Active
```

注意：在升級過程中，故障切換會自動發生。在作用中FTD重新啟動並完成升級之前。

升級完成時，需要重新開機：



Upgrade Completed

FTD_A

10.4.11.87

Cisco Firepower Threat Defense for VMware (Version: 7.0.1-84)

Version: 7.2.4-165 | **Size:** 1.04 GB | **Build Date:** May 3, 2023 8:22 PM UTC

Initiated By: admin | Initiated At: Jul 20, 2023 3:28 PM EDT

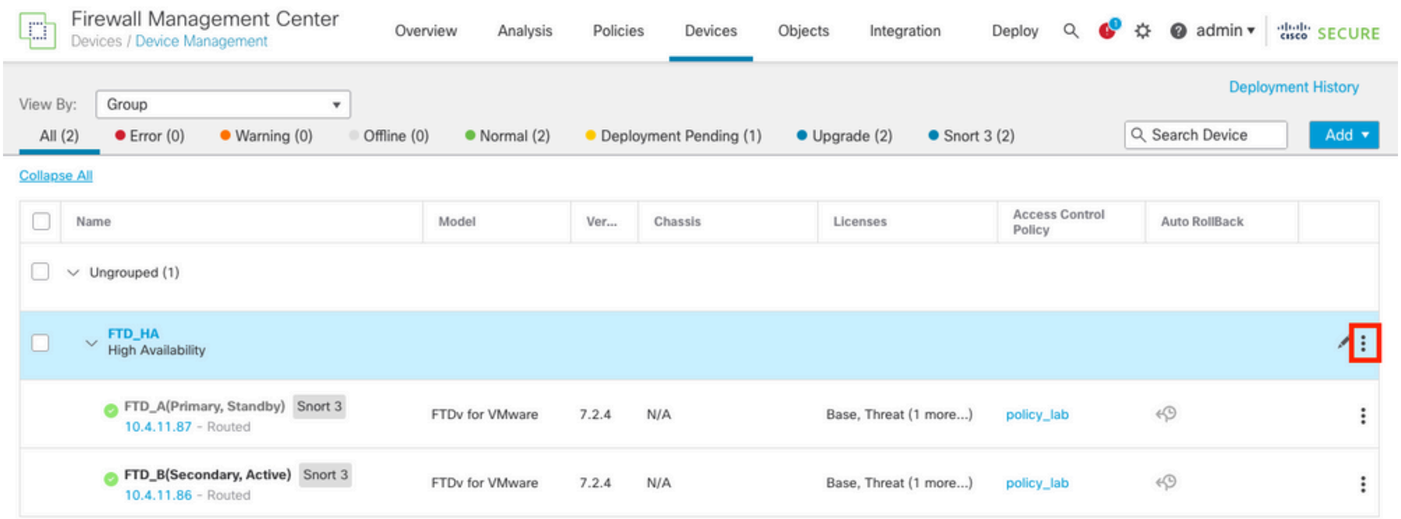
Upgrade to version 7.2.4-165 Completed

步驟 4.交換機活動對等體（可選）

註：如果輔助裝置處於活動狀態，則不會造成任何操作影響。
將主裝置設定為主裝置，將輔助裝置設定為備用裝置是幫助跟蹤可能發生的任何故障切換的最佳實踐。

在這種情況下，FTD Active現在為Standby，您可以使用手動容錯移轉將其設回Active。

- 導覽至編輯符號旁的三點。



Firewall Management Center
Devices / Device Management

Overview Analysis Policies Devices Objects Integration Deploy admin ▾ SECURE

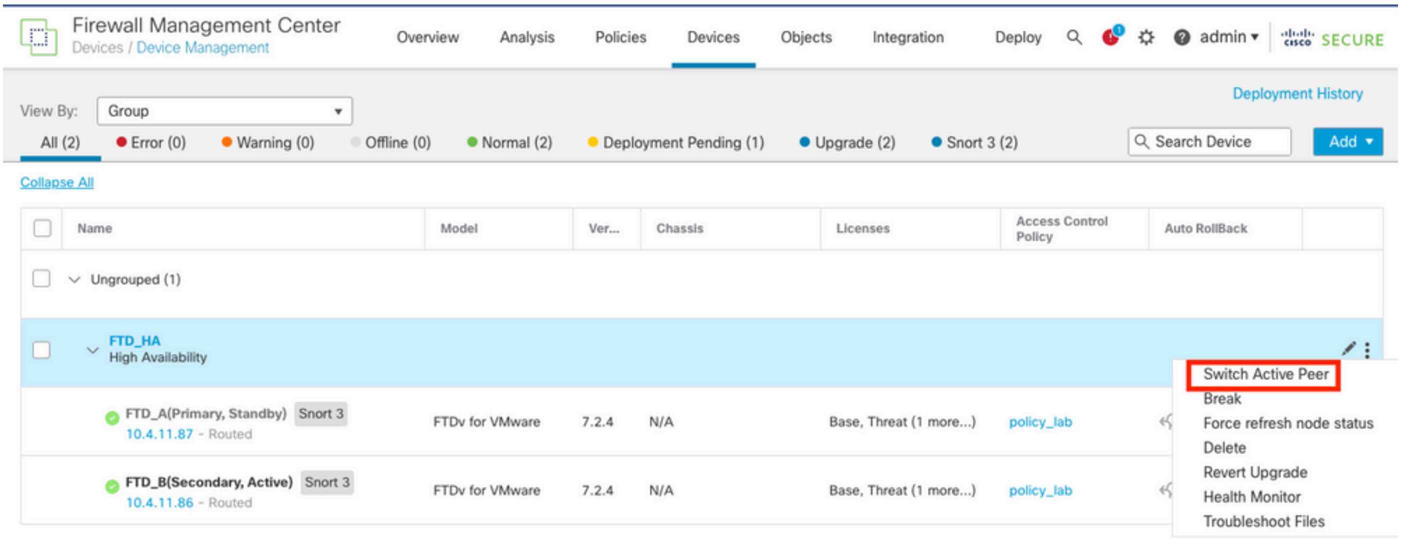
View By: Group ▾ Deployment History

All (2) ● Error (0) ● Warning (0) ● Offline (0) ● Normal (2) ● Deployment Pending (1) ● Upgrade (2) ● Snort 3 (2) Search Device Add ▾

Collapse All

□	Name	Model	Ver...	Chassis	Licenses	Access Control Policy	Auto RollBack	
□	∨ Ungrouped (1)							
□	∨ FTD_HA High Availability							⋮
	FTD_A(Primary, Standby) Snort 3 10.4.11.87 - Routed	FTDv for VMware	7.2.4	N/A	Base, Threat (1 more...)	policy_lab		⋮
	FTD_B(Secondary, Active) Snort 3 10.4.11.86 - Routed	FTDv for VMware	7.2.4	N/A	Base, Threat (1 more...)	policy_lab		⋮

- 選擇Switch Active Peer。



Firewall Management Center
Devices / Device Management

Overview Analysis Policies Devices Objects Integration Deploy admin ▾ SECURE

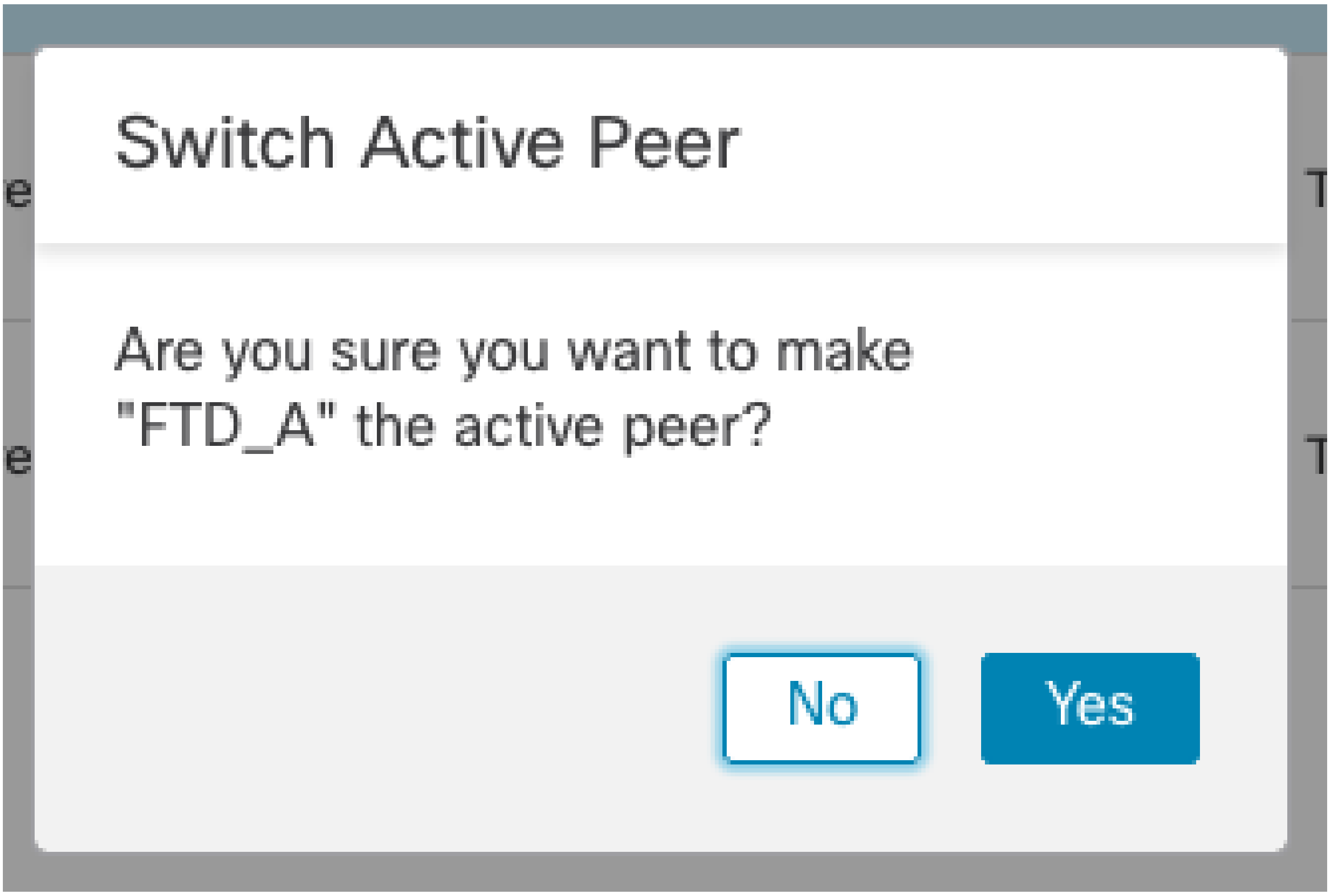
View By: Group ▾ Deployment History

All (2) ● Error (0) ● Warning (0) ● Offline (0) ● Normal (2) ● Deployment Pending (1) ● Upgrade (2) ● Snort 3 (2) Search Device Add ▾

Collapse All

□	Name	Model	Ver...	Chassis	Licenses	Access Control Policy	Auto RollBack	
□	∨ Ungrouped (1)							
□	∨ FTD_HA High Availability							⋮
	FTD_A(Primary, Standby) Snort 3 10.4.11.87 - Routed	FTDv for VMware	7.2.4	N/A	Base, Threat (1 more...)	policy_lab		
	FTD_B(Secondary, Active) Snort 3 10.4.11.86 - Routed	FTDv for VMware	7.2.4	N/A	Base, Threat (1 more...)	policy_lab		

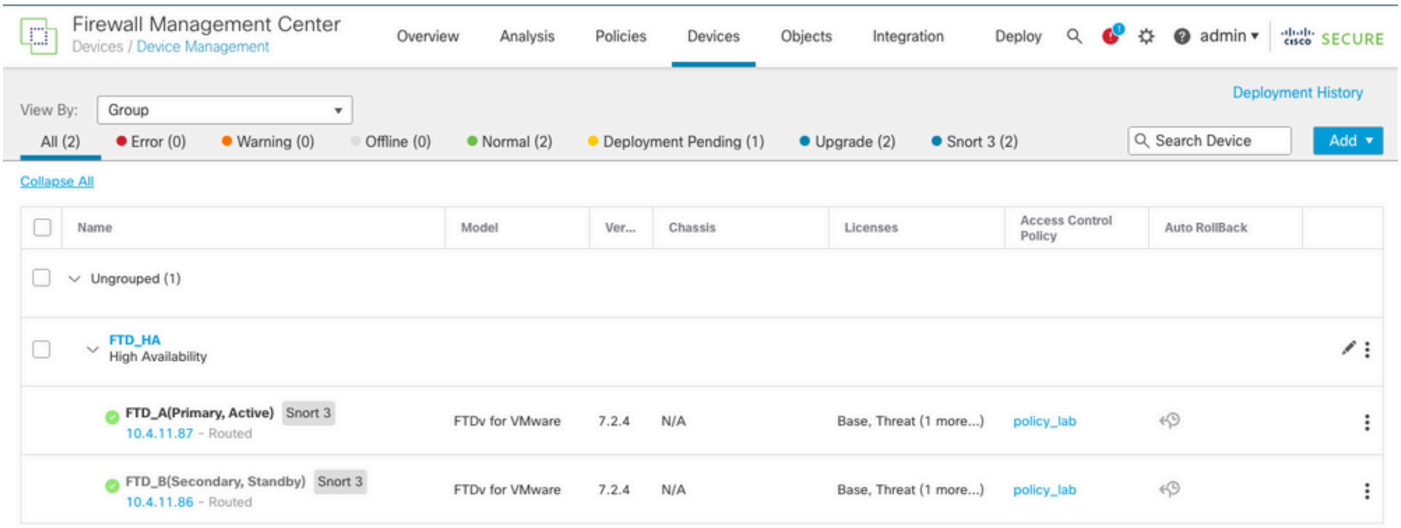
- 選擇YES以確認故障切換。



Switch Active Peer

Are you sure you want to make "FTD_A" the active peer?

升級結束時驗證高可用性狀態並完成故障轉移。
Devices > Device Management



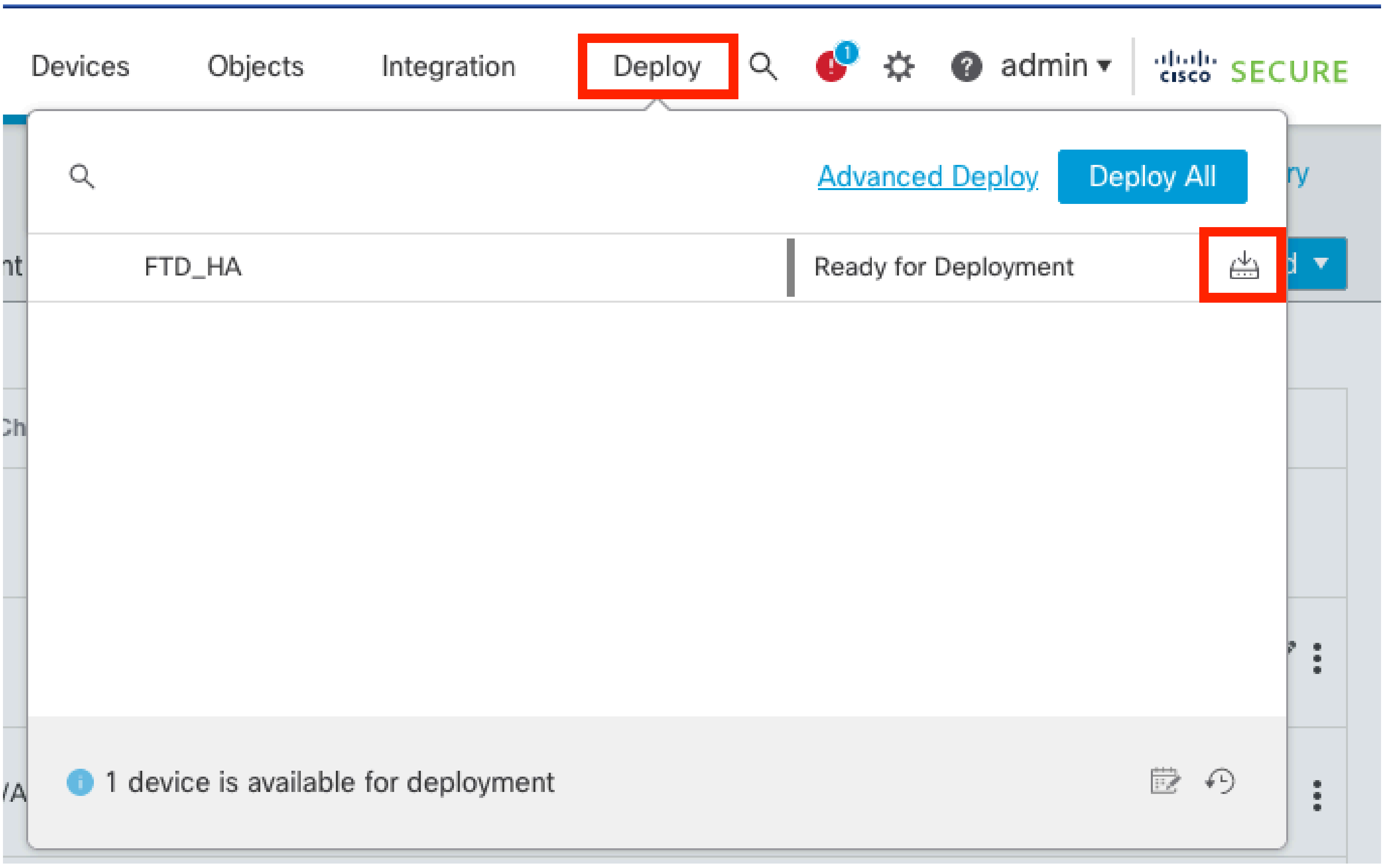
View By: Group

All (2) ● Error (0) ● Warning (0) ● Offline (0) ● Normal (2) ● Deployment Pending (1) ● Upgrade (2) ● Snort 3 (2)

□	Name	Model	Ver...	Chassis	Licenses	Access Control Policy	Auto RollBack
□	Ungrouped (1)						
□	FTD_HA High Availability						
	FTD_A(Primary, Active) Snort 3 10.4.11.87 - Routed	FTDv for VMware	7.2.4	N/A	Base, Threat (1 more...)	policy_lab	
	FTD_B(Secondary, Standby) Snort 3 10.4.11.86 - Routed	FTDv for VMware	7.2.4	N/A	Base, Threat (1 more...)	policy_lab	

步驟 5.最終部署

- 將策略部署到裝置Deploy > Deploy to this device。



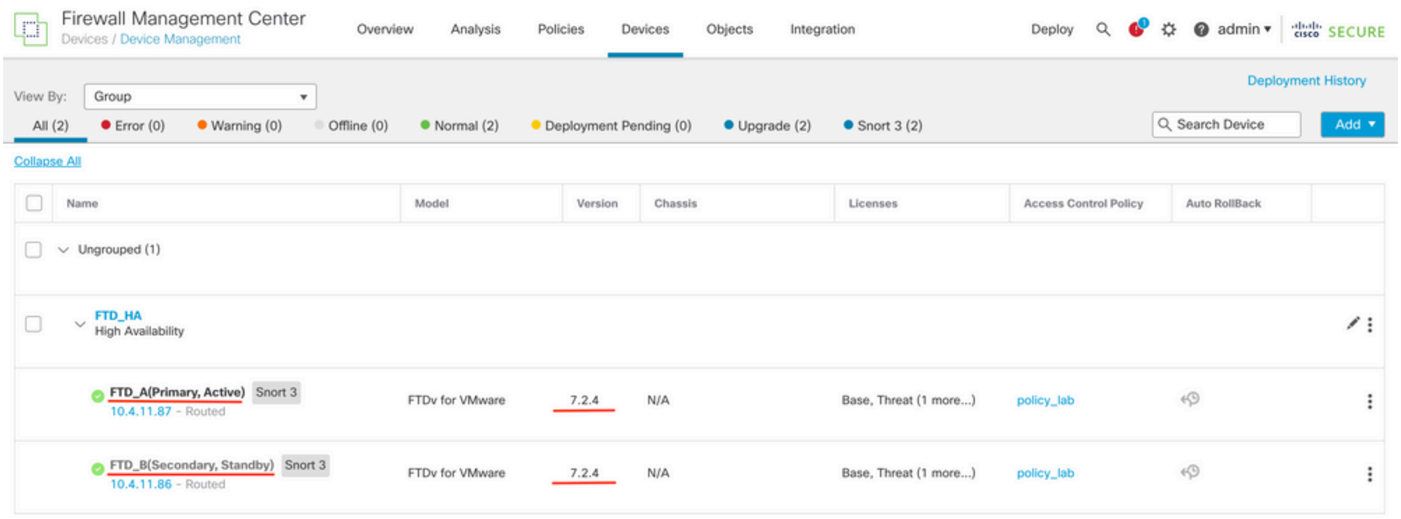
FTD_HA | Ready for Deployment

1 device is available for deployment

驗證

若要驗證高可用性狀態並完成升級，您需要確認狀態：
主要：活動
輔助：備用就緒
兩者都使用最近變更的版本（本範例中為7.2.4）。

- 在FMC GUI中，導航到Devices > Device Management。



Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack
Ungrouped (1)						
FTD_HA High Availability						
FTD_A(Primary, Active) Snort 3 10.4.11.87 - Routed	FTDv for VMware	7.2.4	N/A	Base, Threat (1 more...)	policy_lab	
FTD_B(Secondary, Standby) Snort 3 10.4.11.86 - Routed	FTDv for VMware	7.2.4	N/A	Base, Threat (1 more...)	policy_lab	

- 在CLI上，使用命令show failover state和show failover檢查故障切換狀態，瞭解更多詳細資訊。

```
Cisco Firepower Extensible Operating System (FX-OS) v2.12.0 (build 499)
Cisco Firepower Threat Defense for VMware v7.2.4 (build 165)

> show failover state

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

====Configuration State===
====Communication State===
        Mac set

> show failover
Failover On
Failover unit Primary
Failover LAN Interface: FAILOVER_LINK GigabitEthernet0/0 (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 1285 maximum
MAC Address Move Notification Interval not set
failover replication http
Version: Ours 9.18(3)39, Mate 9.18(3)39
Serial Number: Ours 9AVLW3FSSK8, Mate 9AJJSEGJS2T
Last Failover at: 19:56:41 UTC Jul 20 2023
        This host: Primary - Active
                Active time: 181629 (sec)
                slot 0: ASAv hw/sw rev (/9.18(3)39) status (Up Sys)
                  Interface INSIDE (10.10.153.1): Normal (Monitored)
                  Interface OUTSIDE (10.20.153.1): Normal (Monitored)
                  Interface diagnostic (0.0.0.0): 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: 2390 (sec)
                  Interface INSIDE (10.10.153.2): Normal (Monitored)
                  Interface OUTSIDE (10.20.153.2): Normal (Monitored)
                  Interface diagnostic (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 GigabitEthernet0/0 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         29336      0          24445      0
        sys cmd         24418      0          24393      0
...

        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       11      25331
        Xmit Q:         0       1       127887
```

如果兩個FTD位於相同版本中，且高可用性狀態正常，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）。