Upgrade FTD HA beheerd door FMC

Inhoud

Inleiding

Dit document beschrijft het upgradeproces voor een Cisco Secure Firewall Threat Defence in High Availability-software die wordt beheerd door een Firewall Management Center.

Voorwaarden

Vereisten

Cisco raadt u aan kennis van deze onderwerpen te hebben:

- Concepten en configuratie met hoge beschikbaarheid (HA)
- Configuratie van Secure Firewall Management Center (FMC)
- Cisco Secure Firewall Threat Defence (FTD)-configuratie

Gebruikte componenten

De informatie in dit document is gebaseerd op:

- Virtual Firewall Management Center (FMC), versie 7.2.4
- Virtual Cisco Firewall Threat Defence (FTD), versie 7.0.1

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Overzicht

Het VCC werkt door een peer per keer te upgraden. Eerst de Standby-modus, dan de Active-modus, een failover uitvoeren voordat de Active upgrade voltooid is.

Achtergrondinformatie

Upgradepakket moet vóór de upgrade worden gedownload van software.cisco.com.

Op CLI clish, voer de show high-Availability Config-opdracht in het actieve FTD uit om de status van de High Availability te controleren.

```
> 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
```

Als er geen fouten zichtbaar zijn, gaat u verder met de upgrade.

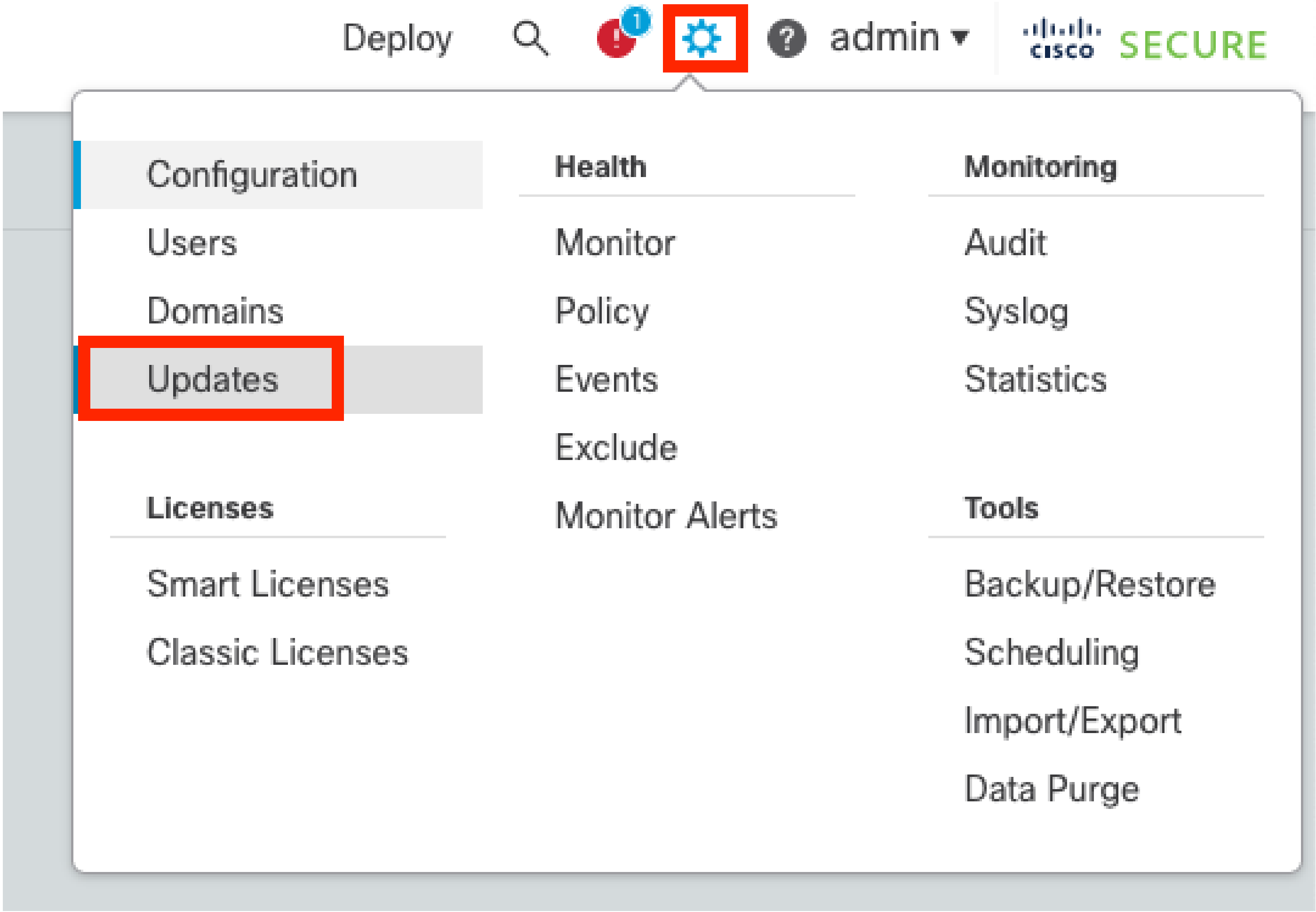
Configureren

Stap 1. Uploadupgrade-pakket

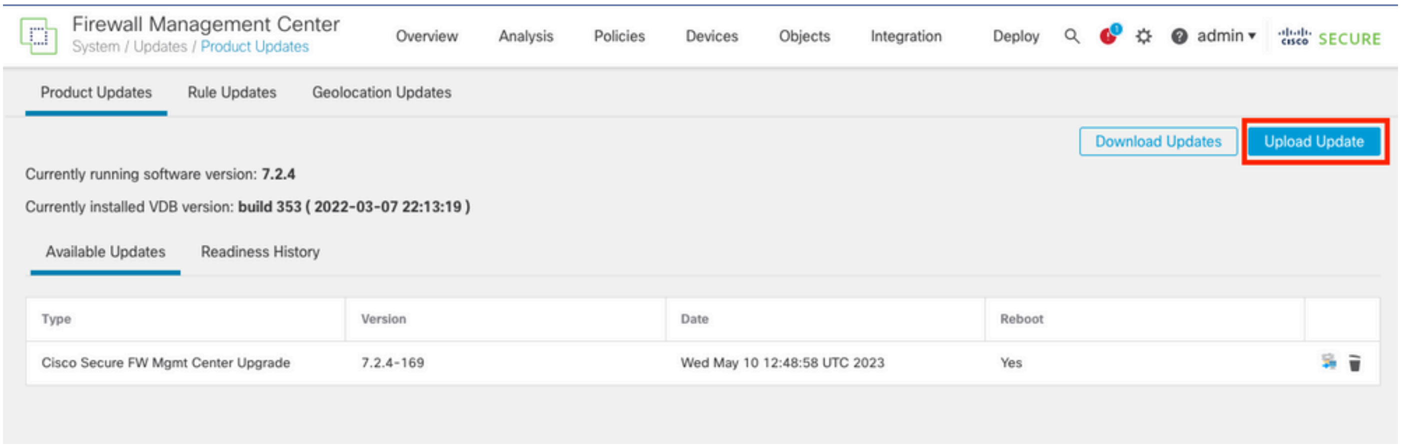
- Upload het FTD-upgradepakket naar het FMC via de grafische gebruikersinterface (GUI). Dit moet eerder worden gedownload van de Cisco-softwaresite op basis van het FTD-model en de gewenste versie.

Waarschuwing: zorg ervoor dat de FMC-versie hoger of gelijk is aan de te upgraden nieuwe FTD-versie.

Systeem > updates



- Selecteer Upload Update.

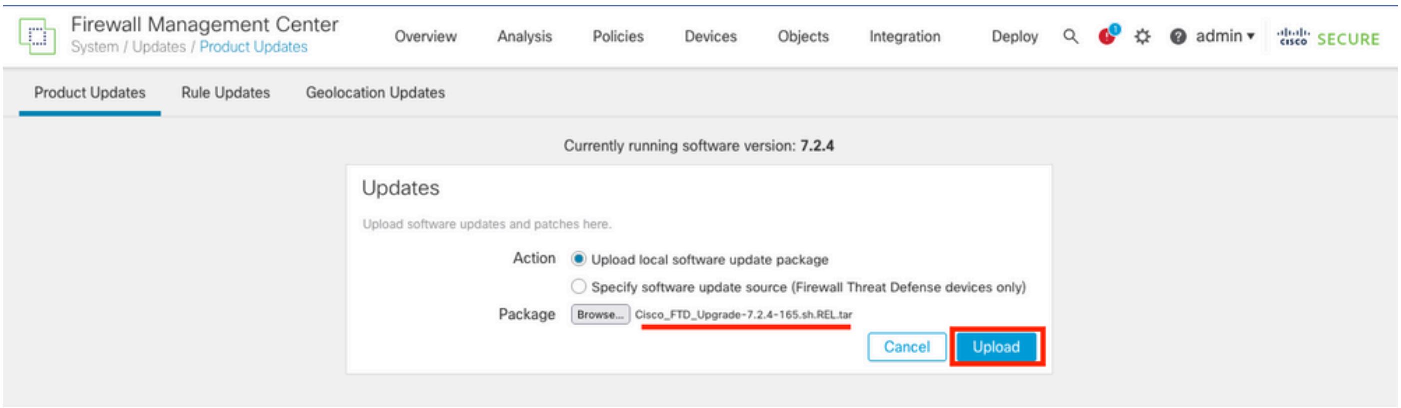


Currently running software version: **7.2.4**

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

- Blader naar de eerder gedownloade afbeelding en selecteer vervolgens Upload.



Currently running software version: **7.2.4**

Updates

Upload software updates and patches here.

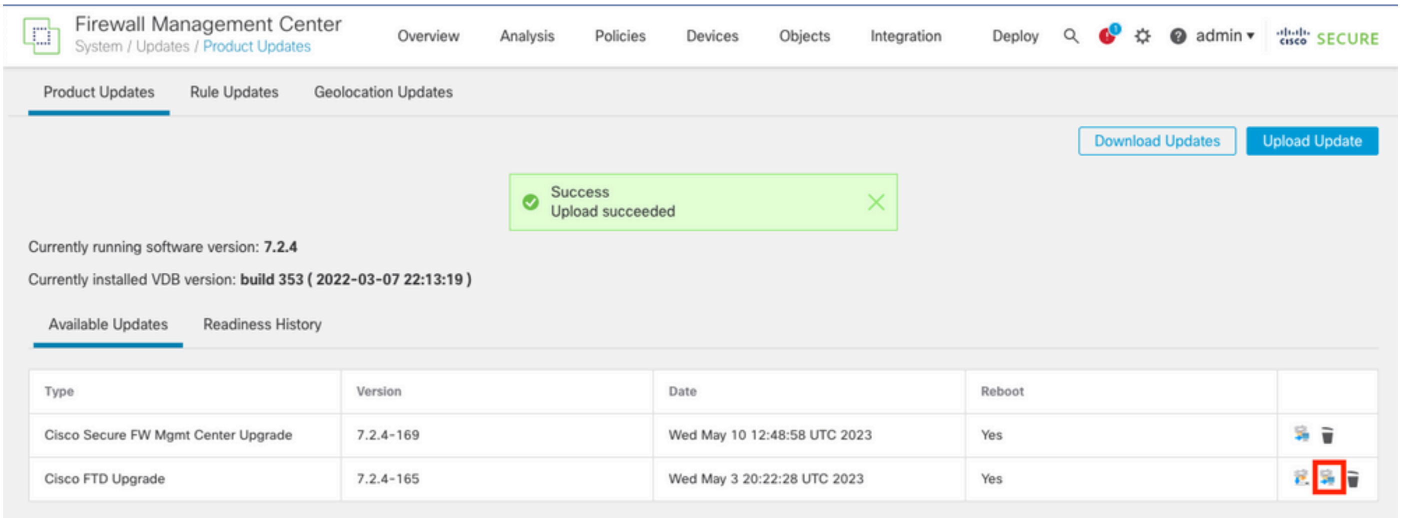
Action ● Upload local software update package
○ Specify software update source (Firewall Threat Defense devices only)

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

Stap 2. Gereedheid controleren

De controles van de bereidheid bevestigen of de apparaten klaar zijn om met verbetering te werk te gaan.

- Selecteer de optie Installeren in het juiste upgradepakket.



Success
Upload succeeded

Currently running software version: **7.2.4**

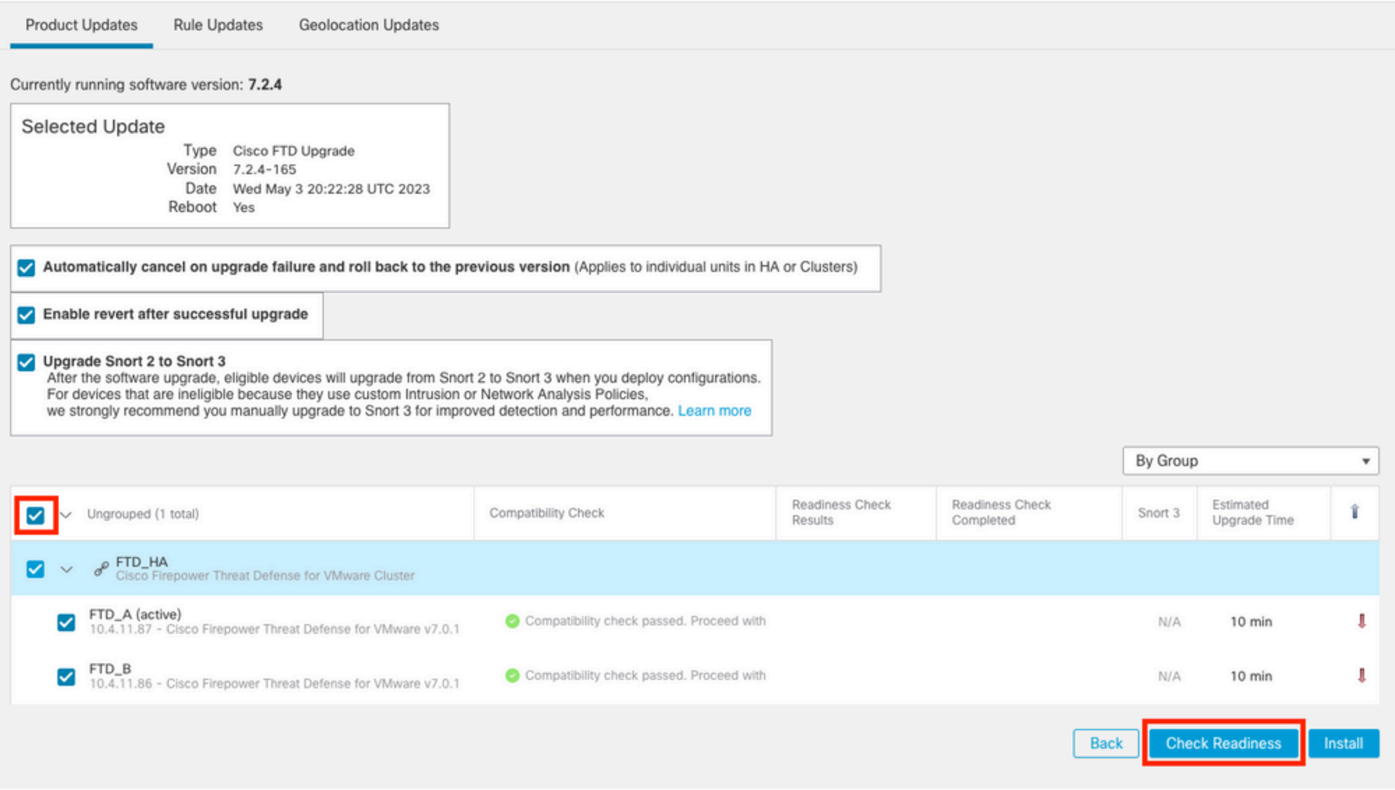
Currently installed VDB version: **build 353 (2022-03-07 22:13:19)**

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

Selecteer de gewenste upgrade. In dit geval is de selectie bedoeld voor:

- Annuleert automatisch bij een upgrade-fout en keert u terug naar de vorige versie.
- Schakel terugzetten na succesvolle upgrade in.
- Upgradesneltoets 2 naar sneltoets 3.

- Selecteer de HA-groep van FTD's en klik op Gereedheid controleren.



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)

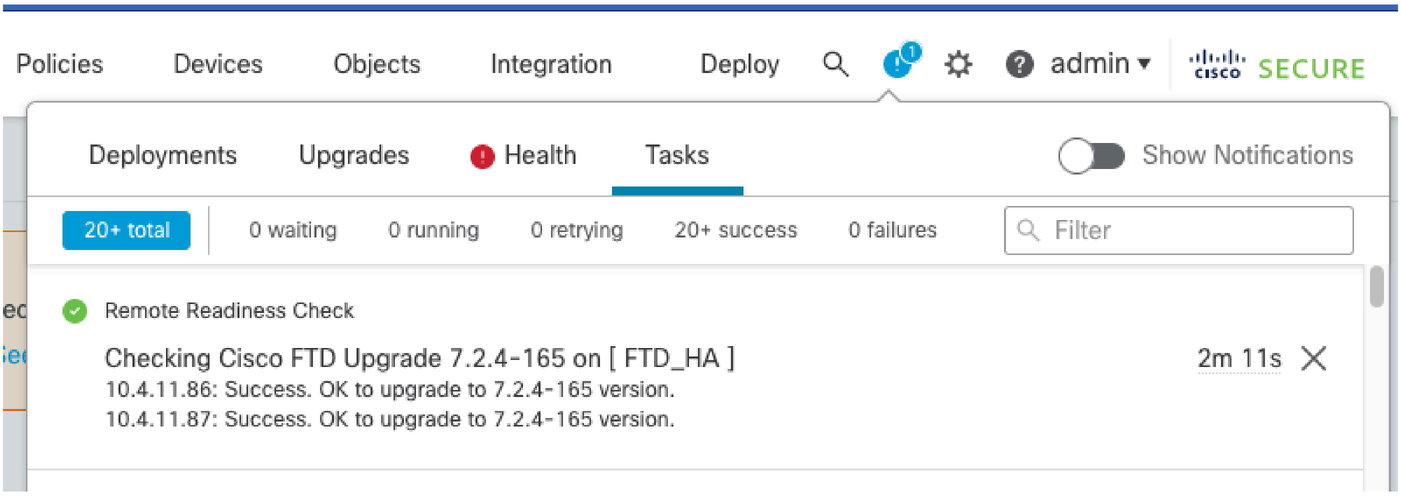
☑ **Enable revert after successful upgrade**

☑ **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			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	

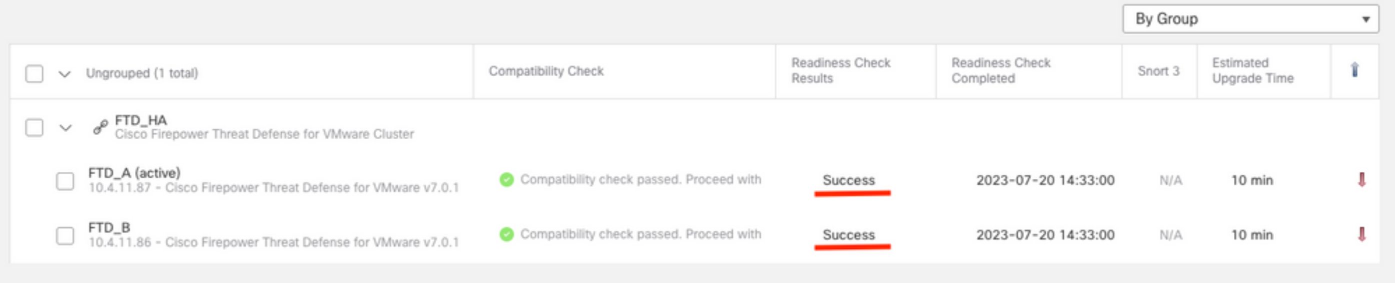
De voortgang kan worden gecontroleerd in het berichtencentrum Berichten > Taken.



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.

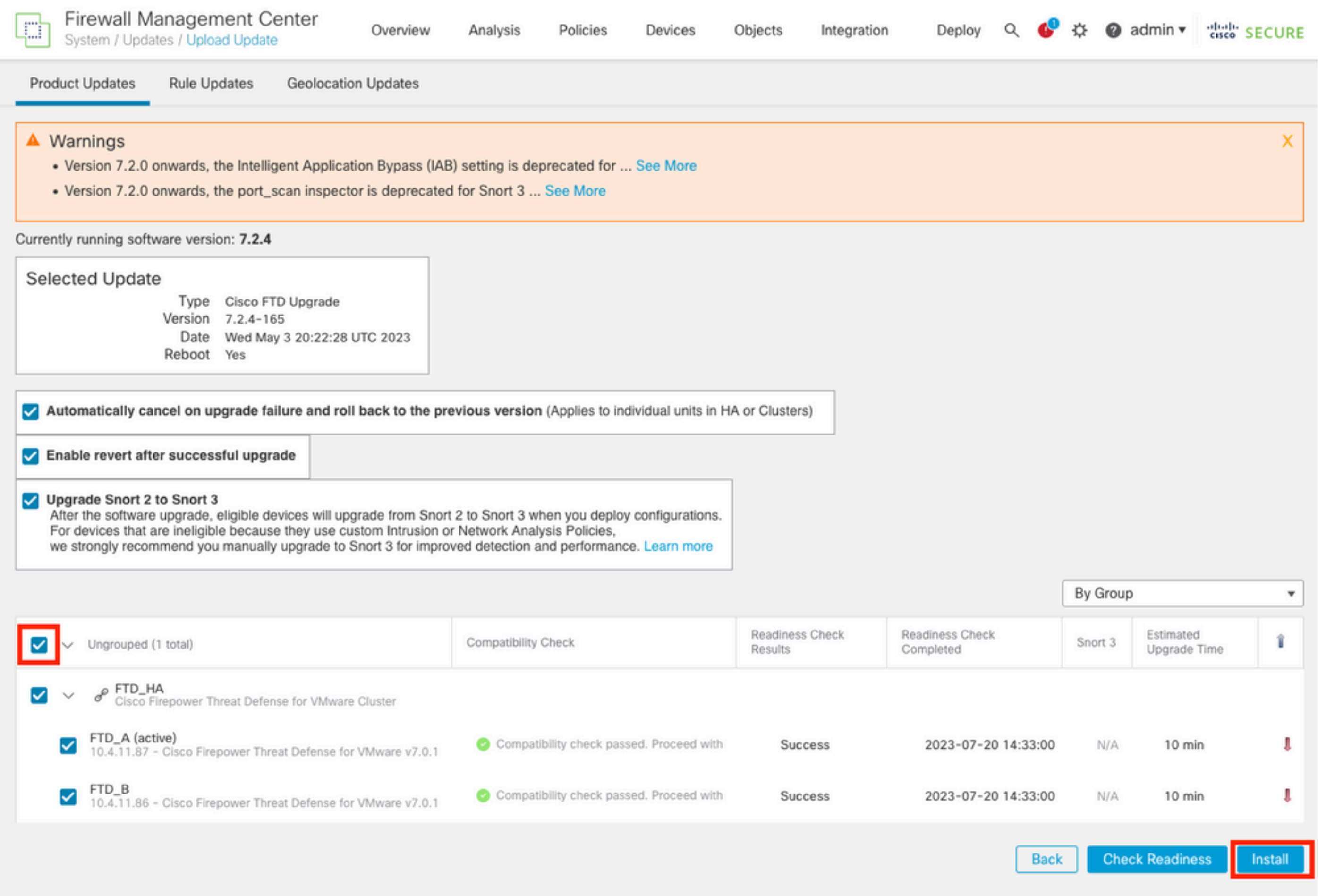
Wanneer de gereedheidscontrole voltooid is in zowel FTD als Resultaat is Success, kan de upgrade worden uitgevoerd.


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	

Stap 3. Upgrade FTD in hoge beschikbaarheid

- Selecteer het HA-paar en klik op Installeren.



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)

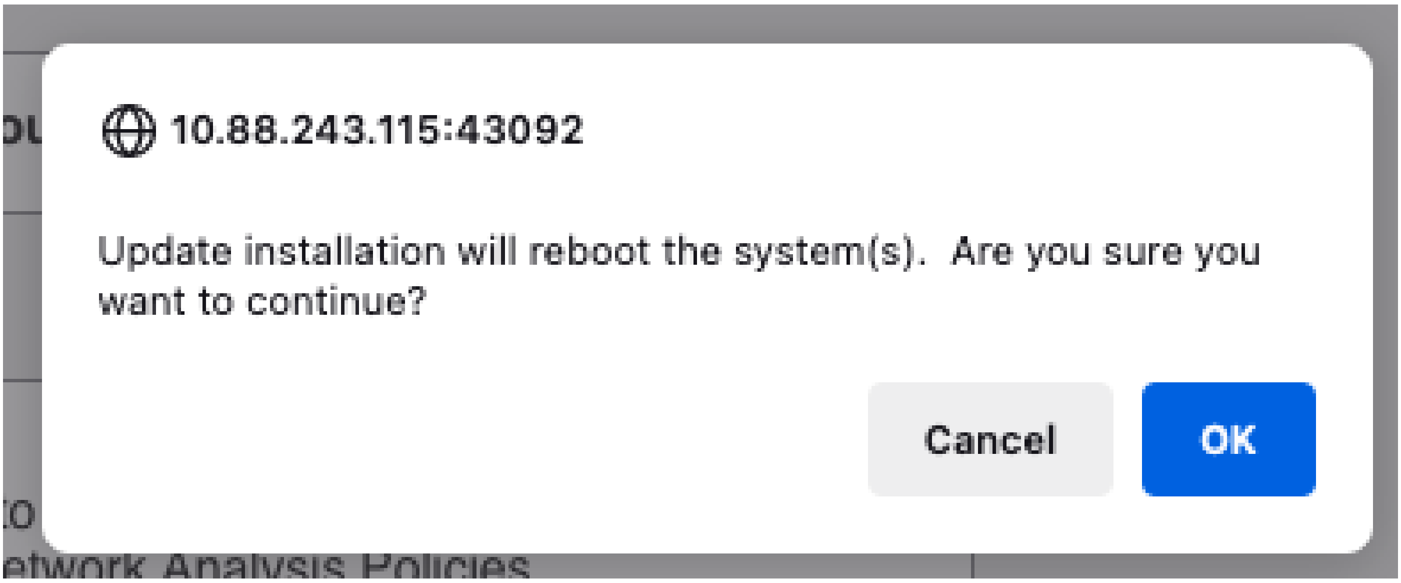
☑ **Enable revert after successful upgrade**

☑ **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

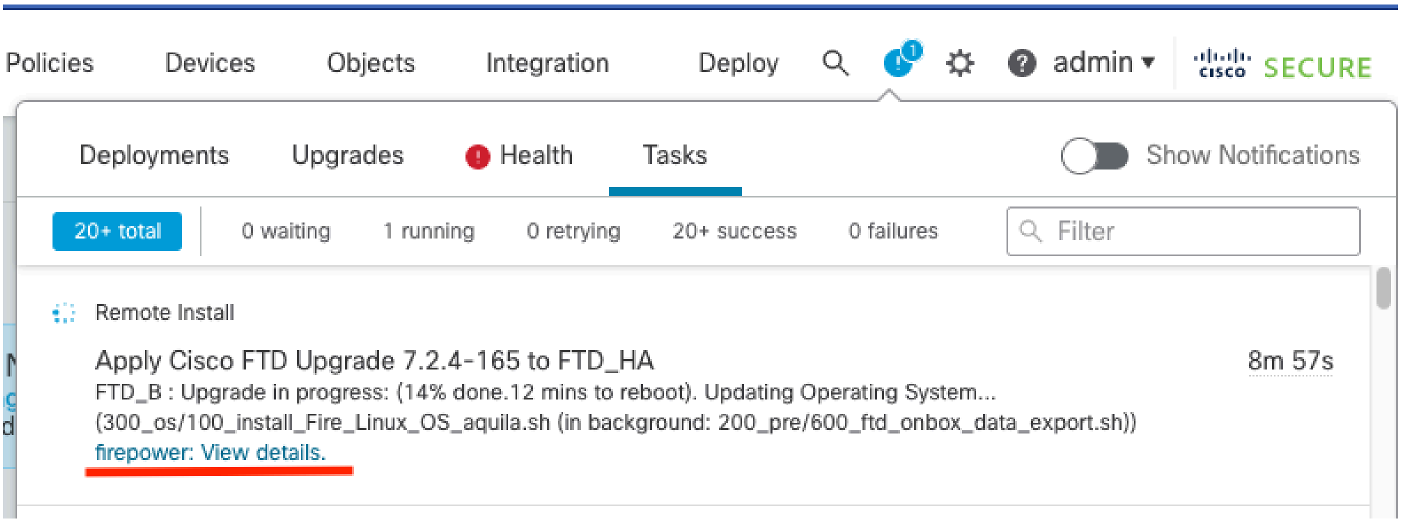
☑ Ungrouped (1 total)	Compatibility Check	Readiness Check Results	Readiness Check Completed	Snort 3	Estimated Upgrade Time
☑ FTD_HA Cisco Firepower Threat Defense for VMware Cluster					
☑ FTD_A (active) 10.4.11.87 - Cisco Firepower Threat Defense for VMware v7.0.1	✓ Compatibility check passed. Proceed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

Waarschuwing om door te gaan met de upgrade, het systeem wordt opnieuw opgestart om de upgrade te voltooien. Selecteer OK.


10.88.243.115:43092

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

De voortgang kan worden gecontroleerd in het berichtencentrum Berichten > Taken.

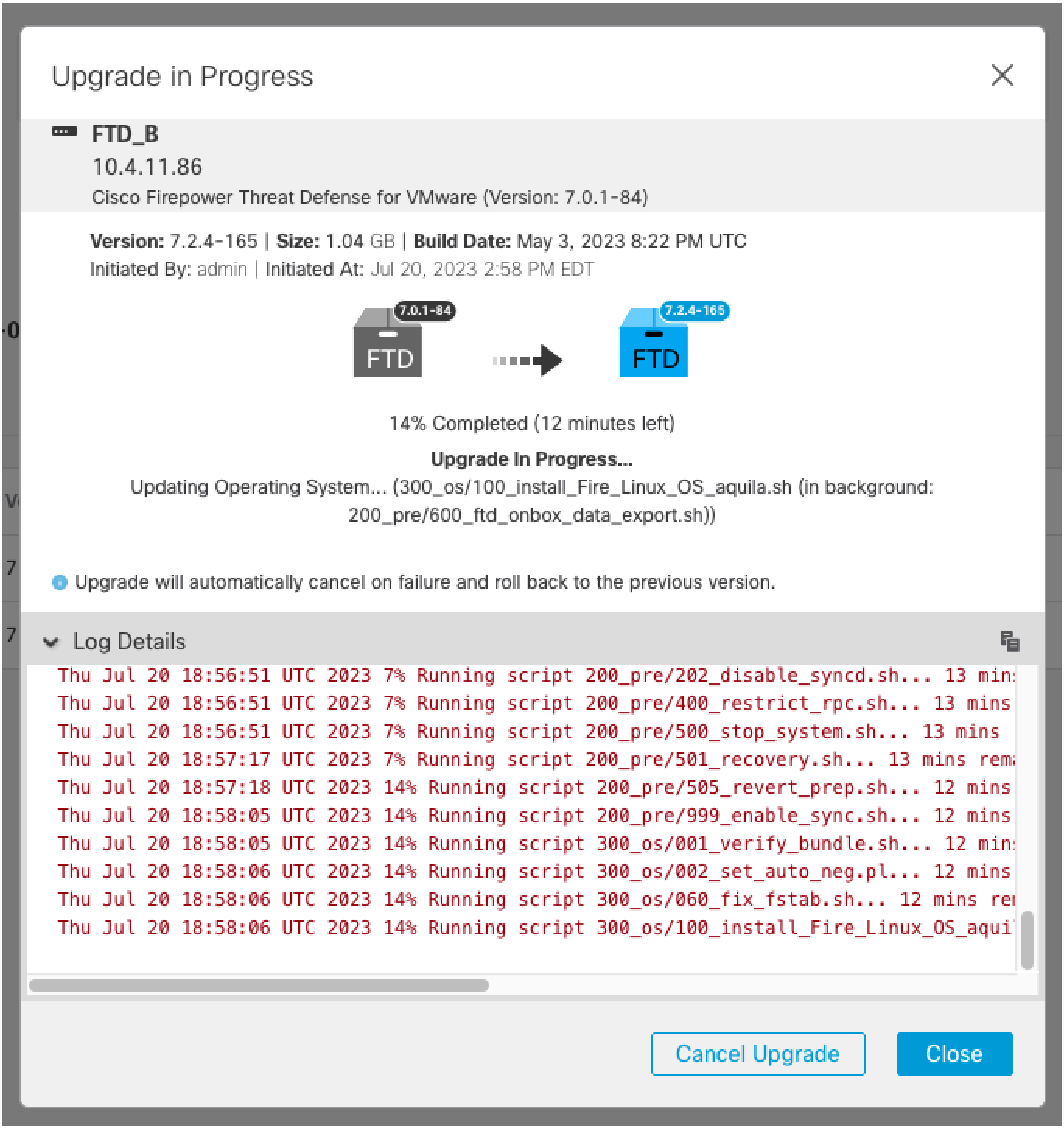


Remote Install

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.

Als u op vuurkracht klikt: Bekijk details, de voortgang wordt getoond op een grafische manier en de logboeken van status.log.



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.

```
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
```

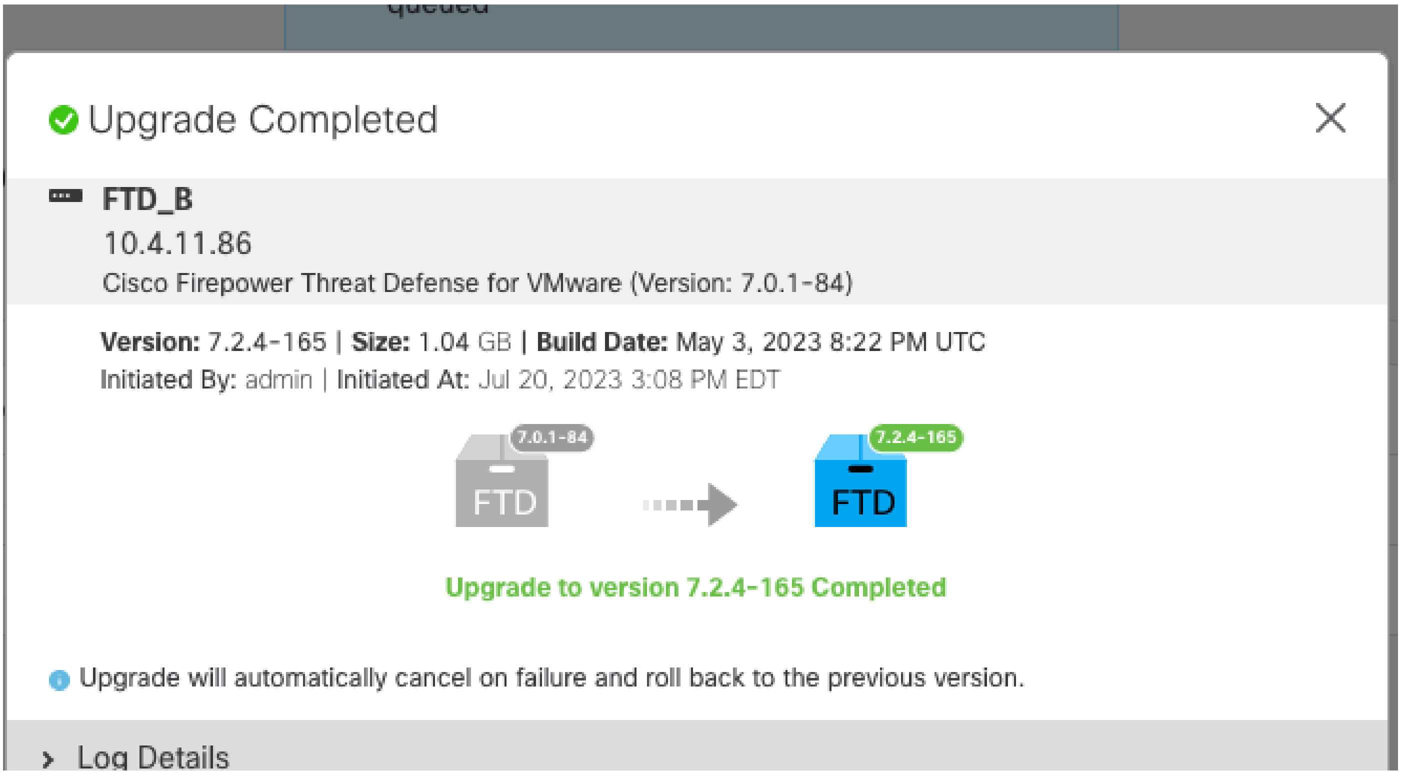
Opmerking: upgrade duurt ongeveer 20 minuten per FTD.

Bij CLI kan de voortgang worden gecontroleerd in upgrademap /ngfw/var/log/sf; ga naar de expert-modus en voer root-toegang in.

```
> 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_comp
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!
```

De upgrade-status wordt op de GUI aangeduid als voltooid en toont de volgende stappen.



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

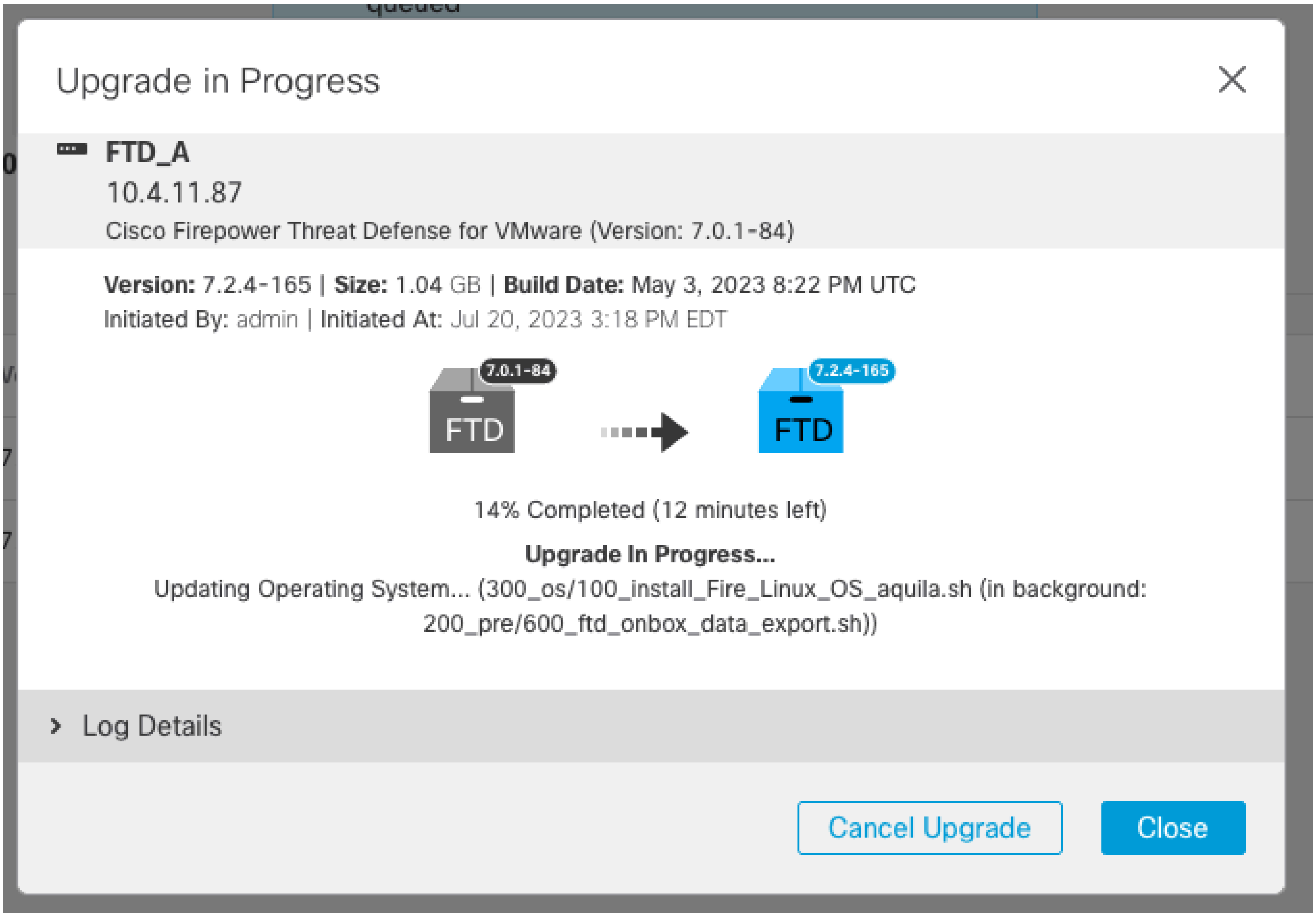
Initiated By: admin | Initiated At: Jul 20, 2023 3:08 PM EDT

Upgrade to version 7.2.4-165 Completed

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

› Log Details

Nadat de upgrade op het Standby-apparaat is voltooid, wordt gestart op het actieve apparaat.



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)

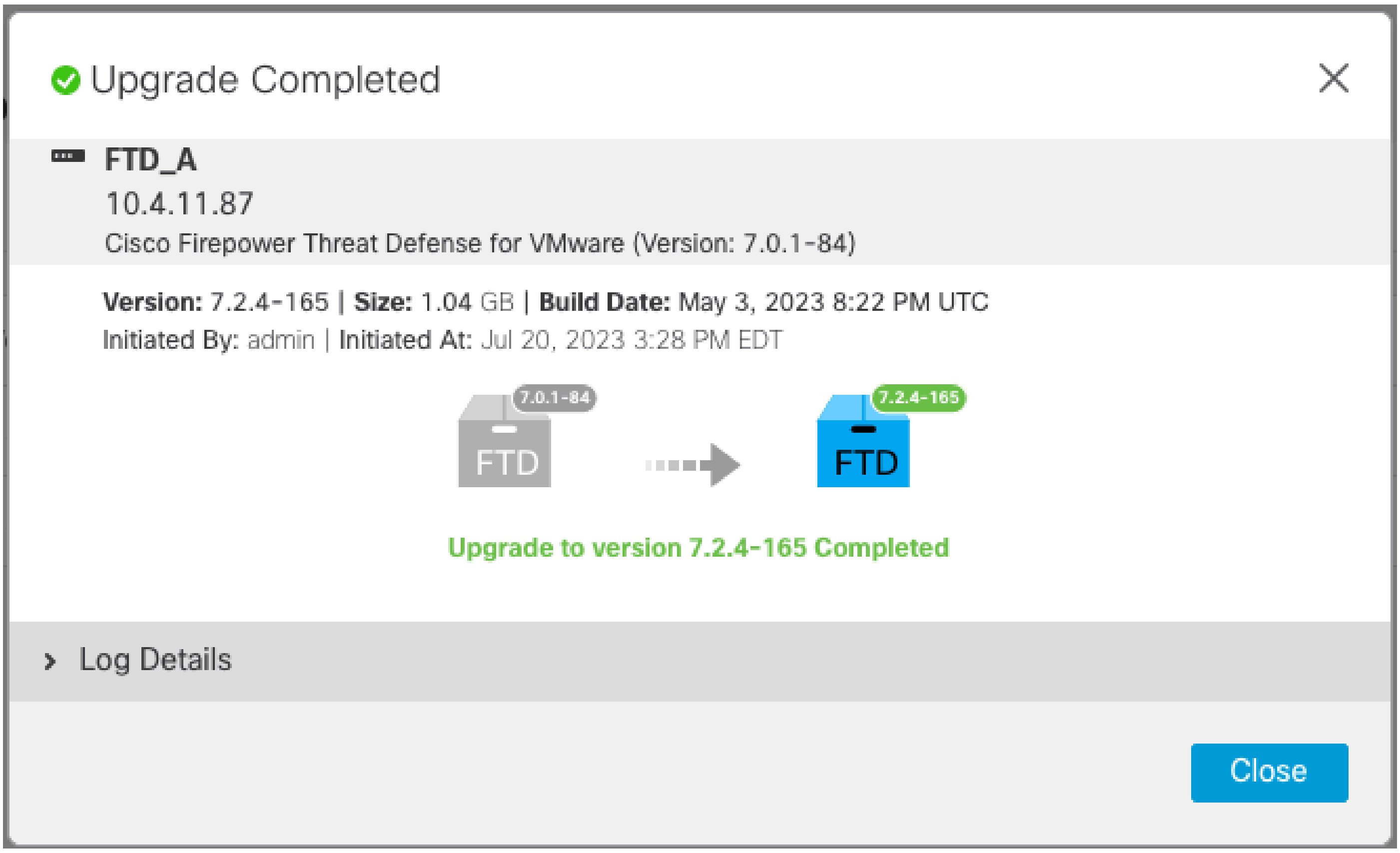
Upgrade In Progress...
Updating Operating System... (300_os/100_install_Fire_Linux_OS_aquila.sh (in background: 200_pre/600_ftd_onbox_data_export.sh))

Op CLI, verplaats naar LINA (system support diagnostic-cloud) en controleer de failover status op de Standby FTD met behulp van de opdracht failover status tonen.

```
> 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
```

Opmerking: de failover wordt automatisch uitgevoerd als onderdeel van de upgrade. Voor actieve FTD start en voltooi de upgrade.

Wanneer de upgrade is voltooid, moet de computer opnieuw worden opgestart:



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

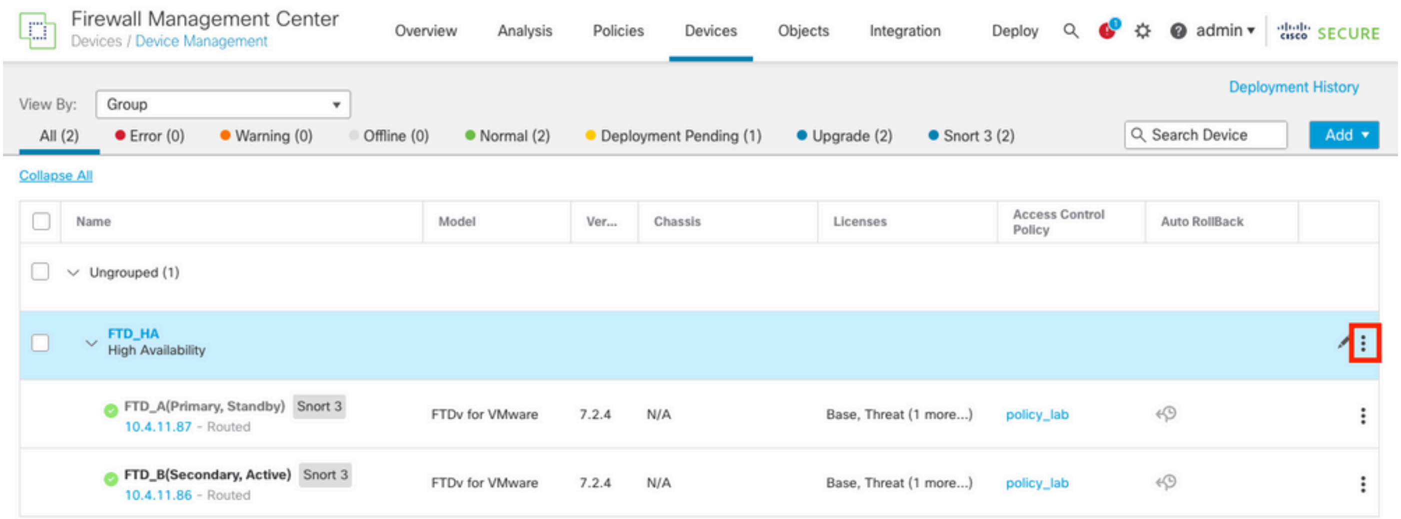
Upgrade to version 7.2.4-165 Completed

Stap 4. Switch actieve peer (optioneel)

Opmerking: als de hulpvoorziening actief is, heeft zij geen operationele gevolgen.
Het hebben van Primair apparaat zo Actief en Secundair als Standby is een beste praktijk die helpt het volgen van om het even welke failover die kan voorkomen.

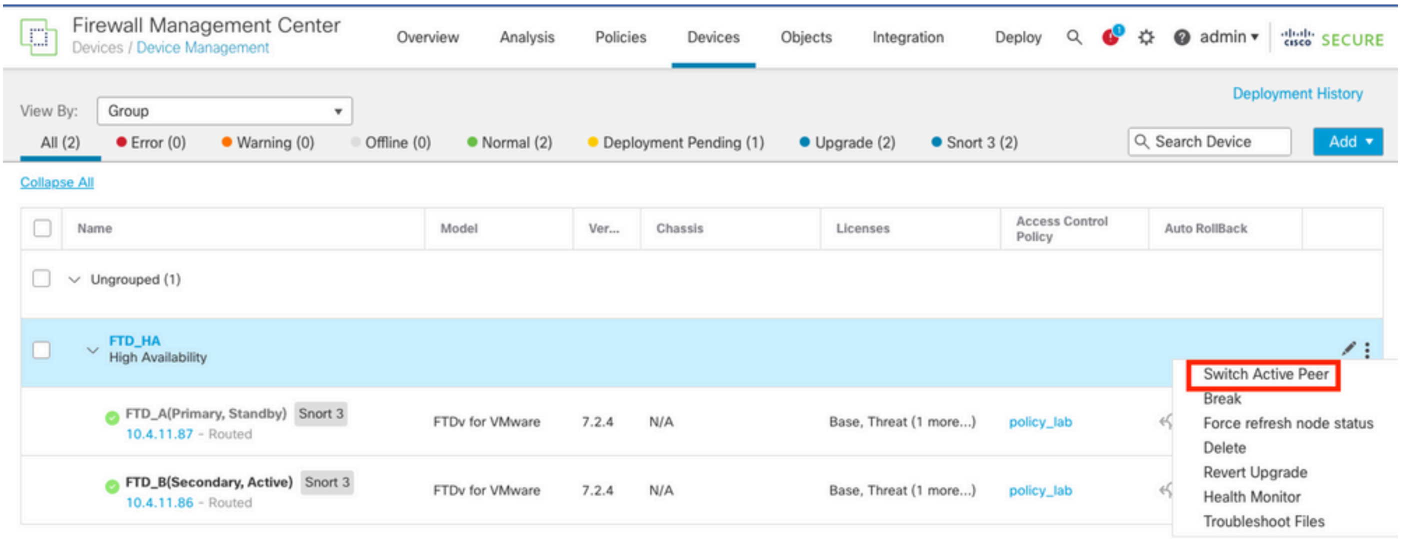
In dit geval is de FTD Active nu stand-by, kan een handmatige failover worden gebruikt om deze terug te zetten op Active.

- Navigeer naar de drie punten naast het bewerkingsteken.



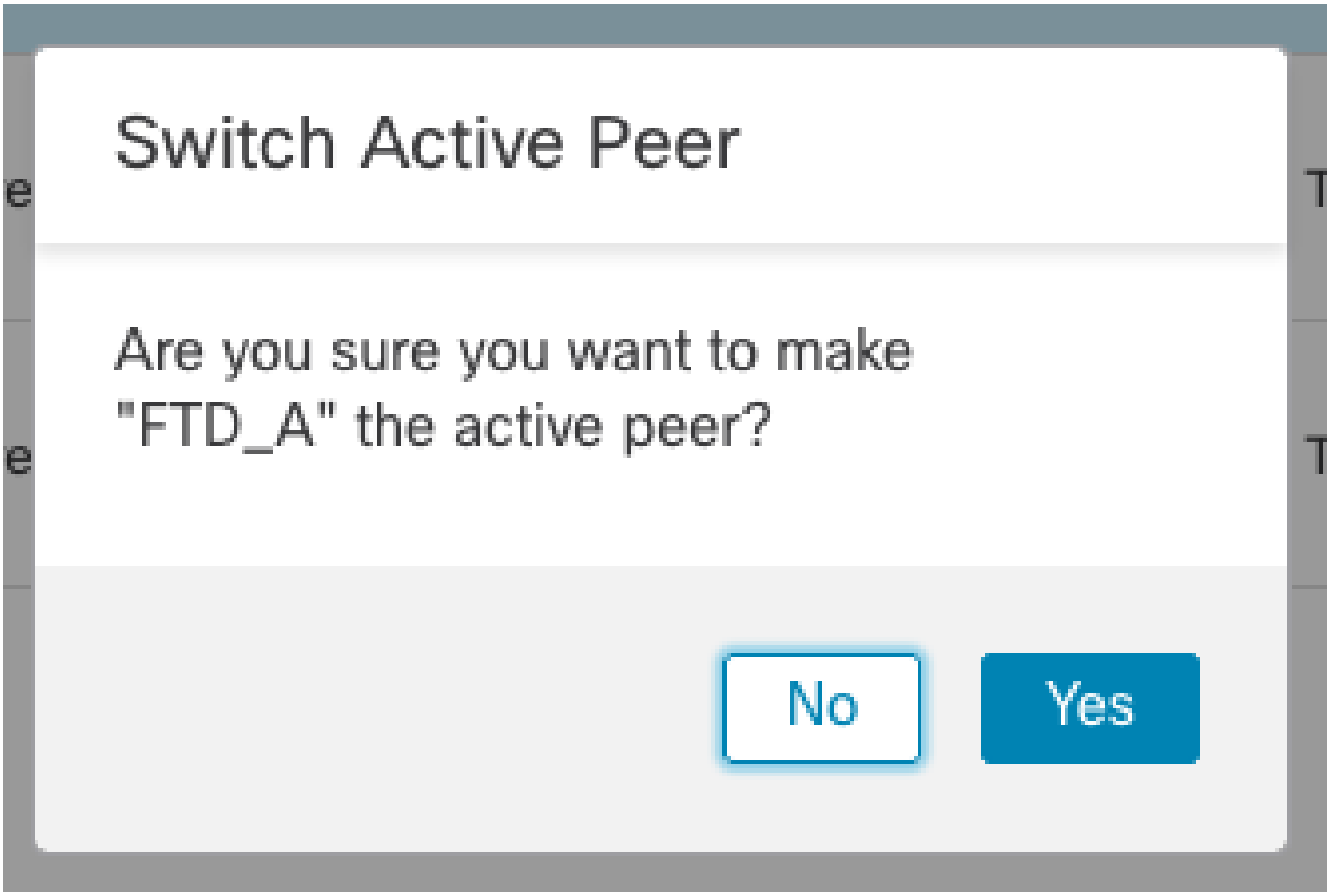
□	Name	Model	Ver...	Chassis	Licenses	Access Control Policy	Auto RollBack	
□	Ungrouped (1)							
□	FTD_HA High Availability							⋮
	FTD_A(Primary, Standby) Snort 3 10.4.11.87 - Routed	FTDv for VMware	7.2.4	N/A	Base, Threat (1 more...)	policy_lab		⋮
	FTD_B(Secondary, Active) Snort 3 10.4.11.86 - Routed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

- Selecteer Switch actieve peer.



□	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		

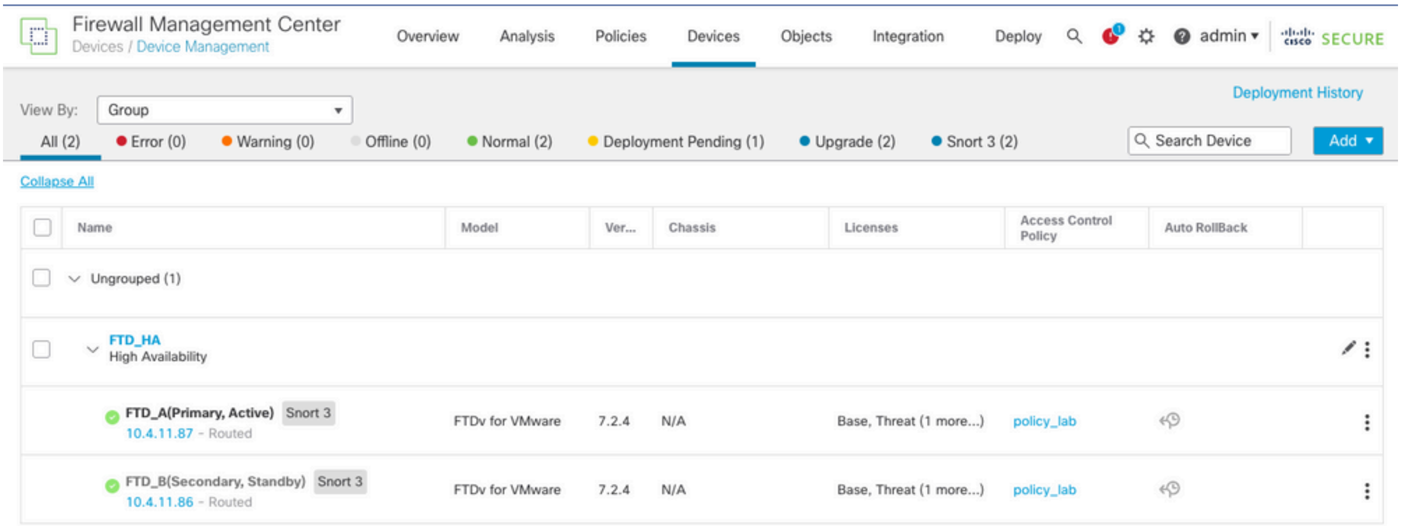
- Selecteer JA om de failover te bevestigen.



Switch Active Peer

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

Validatie van hoge beschikbaarheid status aan het eind van upgrade en failover gedaan.
Apparaten > Apparaatbeheer



Firewall Management Center
Devices / Device Management

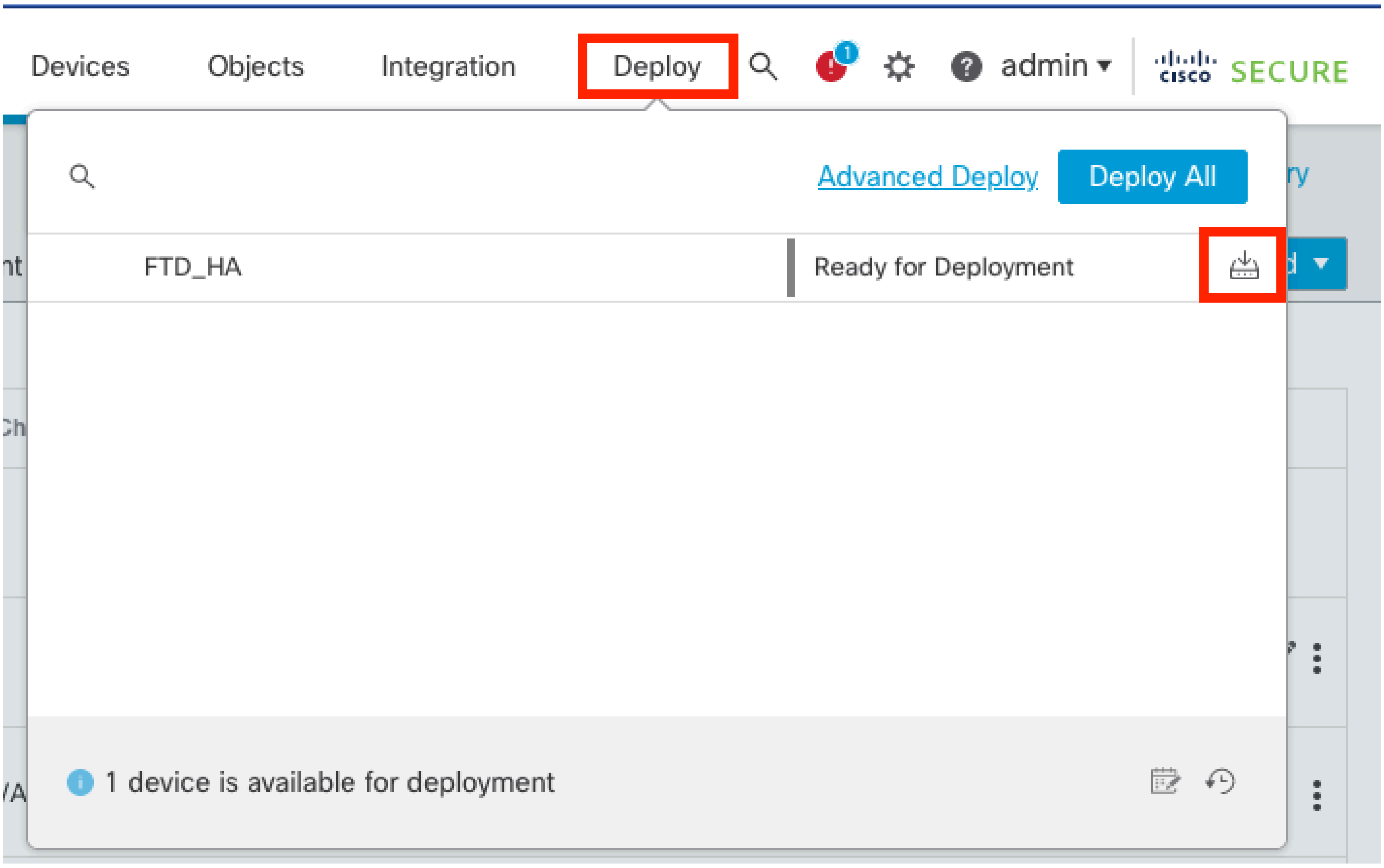
View By: Group ▾

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	

Stap 5. Definitieve implementatie

- Stel een beleid in om apparaten te implementeren > implementeren op dit apparaat.



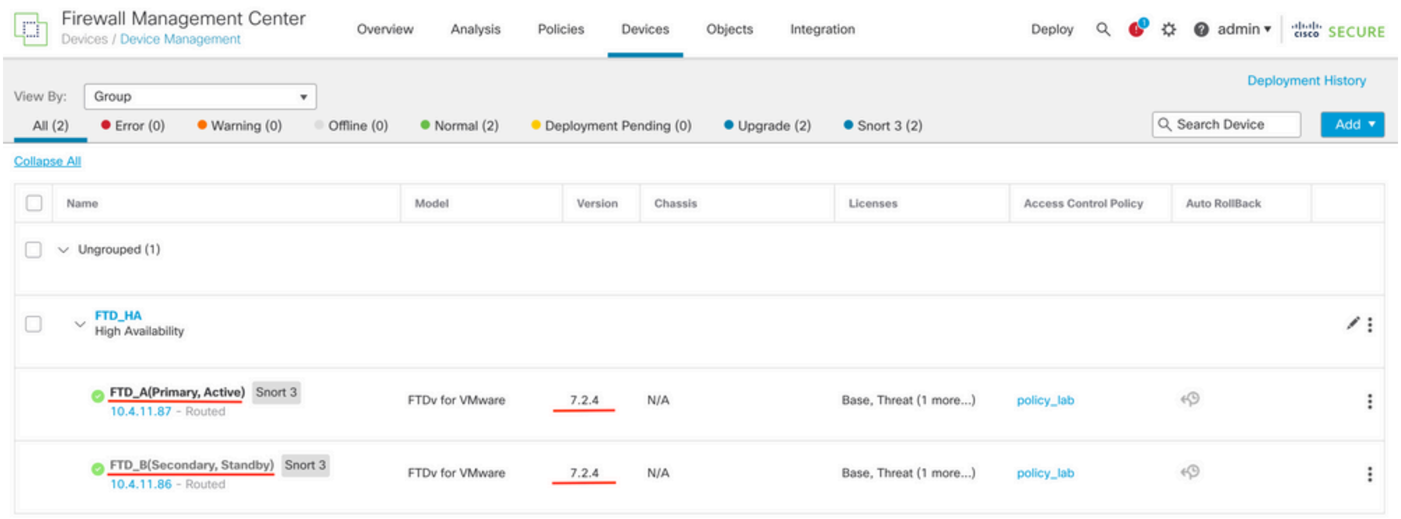
FTD_HA | Ready for Deployment

1 device is available for deployment

valideren

Om de status en upgrade van hoge beschikbaarheid te valideren, moet u de status bevestigen:
Primair: actief
Secundair: klaar voor stand-by
Beide staan onder de versie die onlangs is gewijzigd (7.2.4 in dit voorbeeld).

- In FMC GUI, navigeer naar Apparaten > Apparaatbeheer.



View By: Group

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

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	

- Over CLI clish, controleer de failover staat met de opdracht tonen failover staat en tonen failover een gedetailleerdere informatie.

```
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
```

Als beide FTDs op dezelfde versie zijn en de hoge beschikbaarheidsstatus gezond is, dan is de upgrade voltooid.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.