Actualización de FTD HA gestionado por FMC

Contenido

Introducción

Este documento describe el proceso de actualización para Cisco Secure Firewall Threat Defense en alta disponibilidad administrado por un centro de administración de firewall.

Prerequisites

Requirements

Cisco recomienda tener conocimientos de estos temas:

- Conceptos y configuración de alta disponibilidad (HA)
- Configuración de Secure Firewall Management Center (FMC)
- Configuración de Cisco Secure Firewall Threat Defence (FTD)

Componentes Utilizados

La información de este documento se basa en:

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

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Overview

El funcionamiento del FMC consiste en actualizar un par cada vez. Primero el Standby, luego el Active, haciendo una conmutación por fallas antes de que la actualización Active se complete.

Antecedentes

El paquete de actualización se debe descargar de software.cisco.com antes de la actualización.

En el clish de CLI, ejecute el comando show high-availability config en el FTD activo para verificar el estado de High Availability.

```
> 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
```

Si no hay errores visibles, continúe con la actualización.

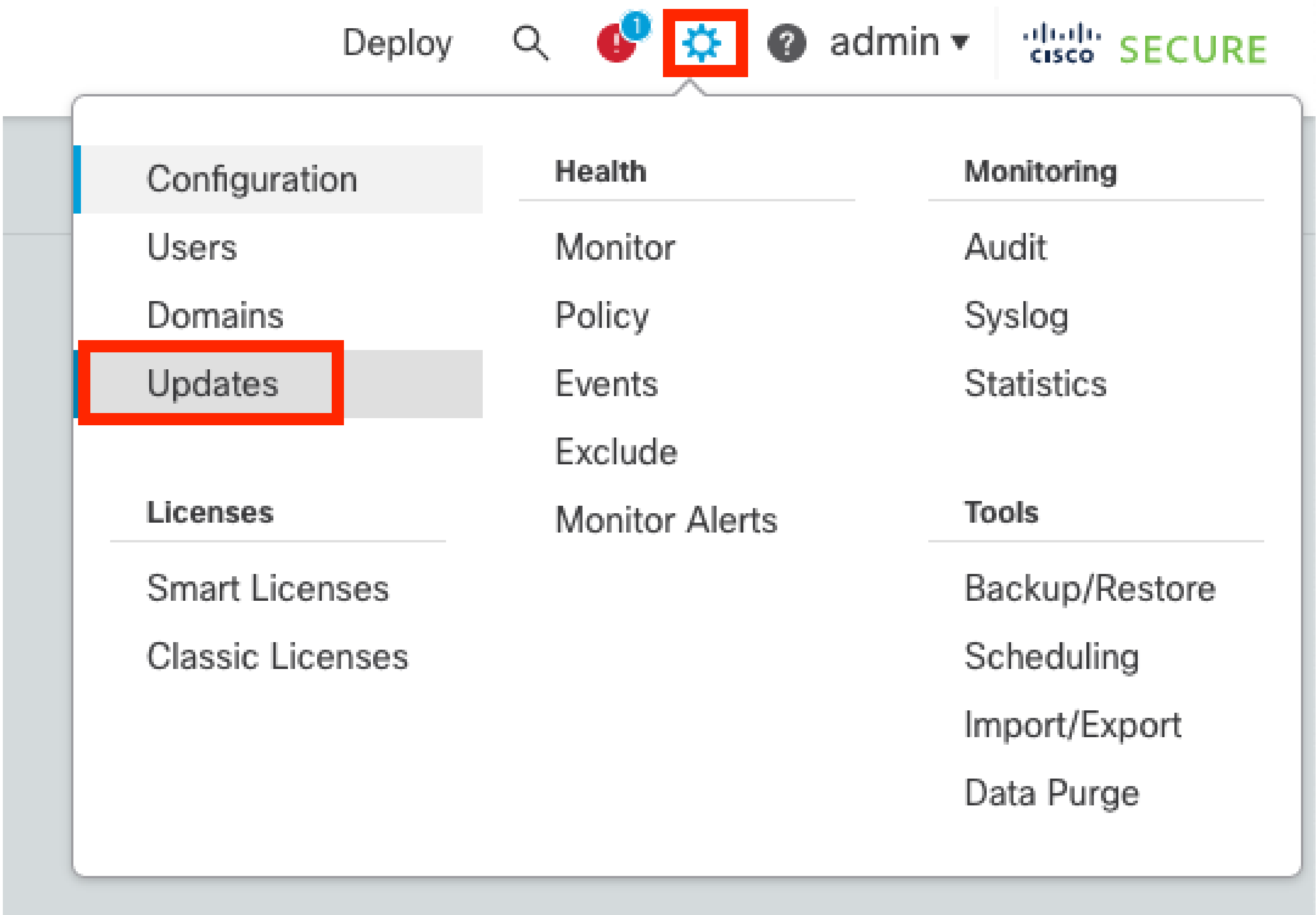
Configurar

Paso 1. Cargar paquete de actualización

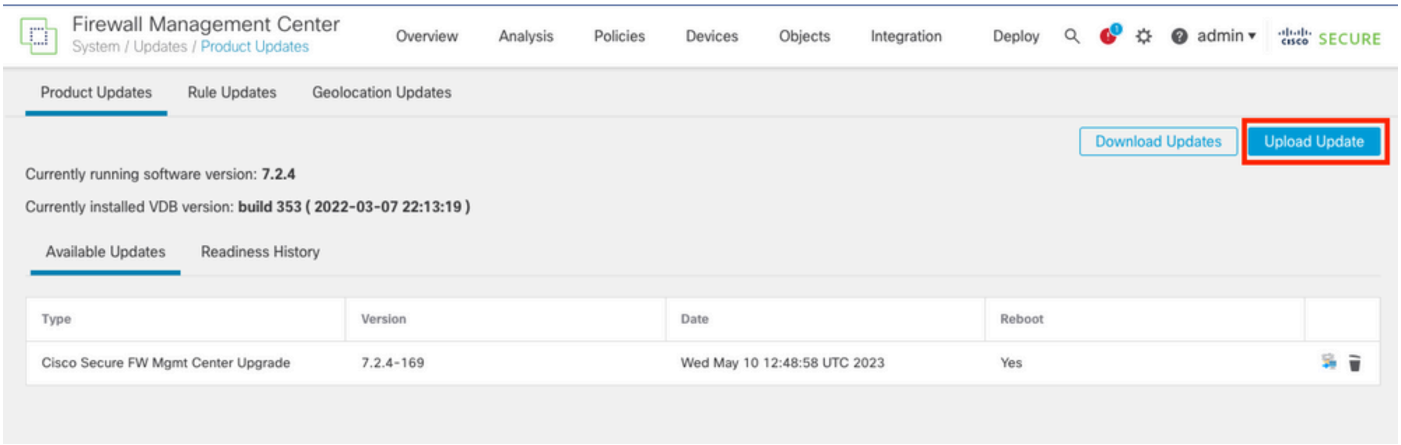
- Cargue el paquete de actualización del FTD en el FMC mediante la interfaz gráfica de usuario (GUI).
  Esto debe descargarse previamente del sitio de software de Cisco en función del modelo de FTD y de la versión deseada.

Advertencia: Asegúrese de que la versión del FMC es superior o igual a la nueva versión del FTD que se va a actualizar.

Sistema > Actualizaciones



- Seleccione Cargar actualización.

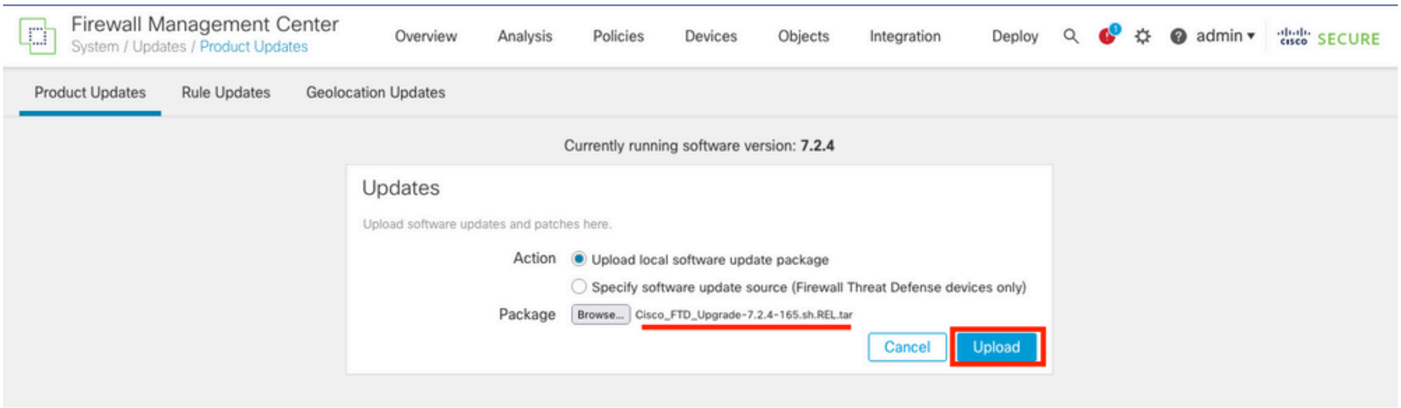


Currently running software version: **7.2.4**

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

- Busque la imagen descargada anteriormente y, a continuación, seleccione Cargar.



Currently running software version: **7.2.4**

Updates

Upload software updates and patches here.

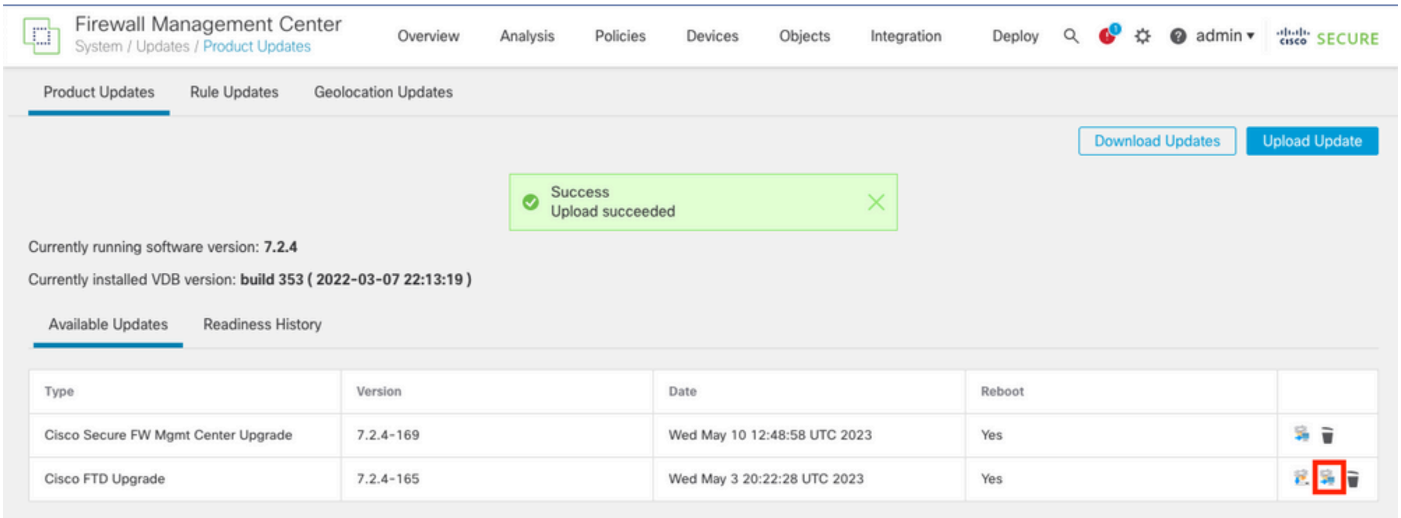
Action ● Upload local software update package
○ Specify software update source (Firewall Threat Defense devices only)

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

Paso 2. Comprobar preparación

Las comprobaciones de preparación confirman si los dispositivos están preparados para continuar con la actualización.

- Seleccione la opción Install en el paquete de actualización correcto.



Success
Upload succeeded

Currently running software version: **7.2.4**

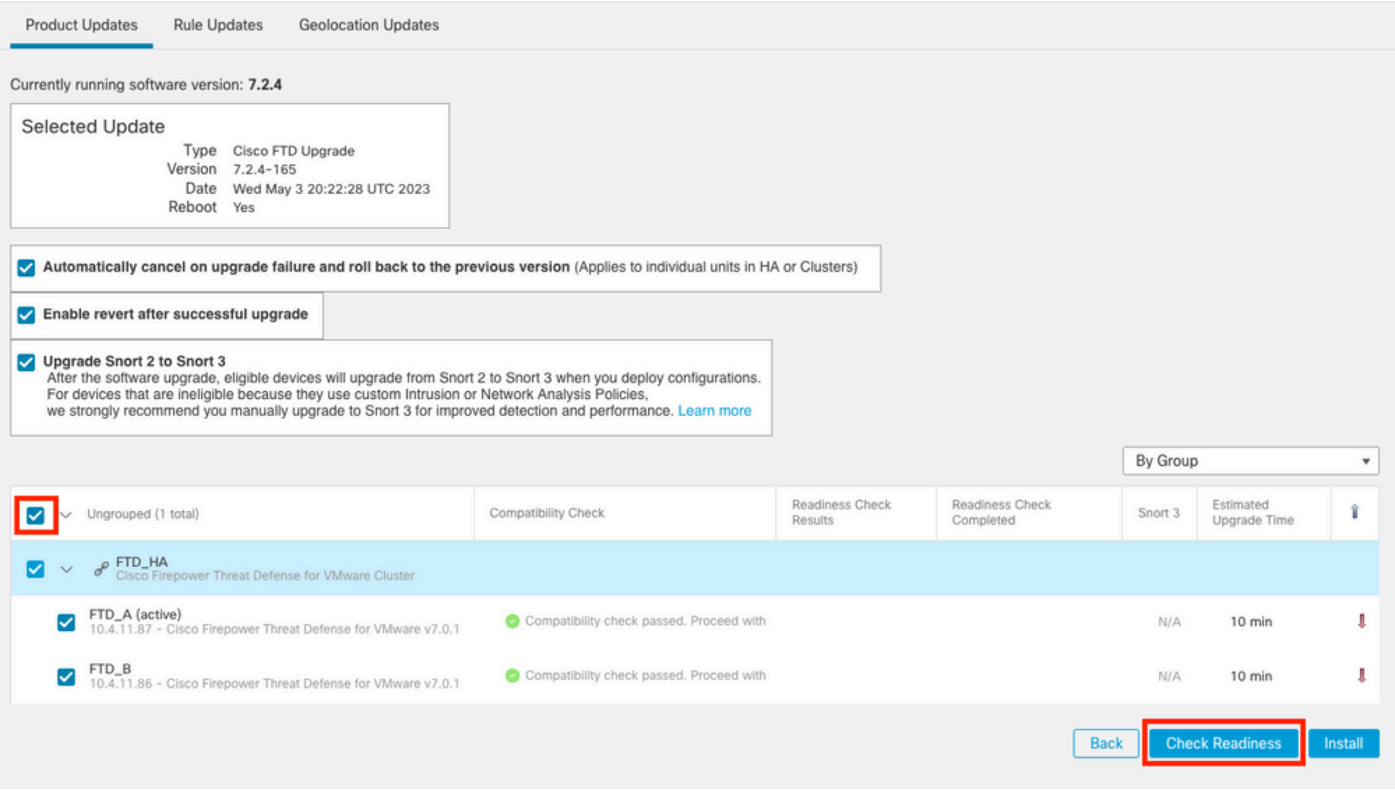
Currently installed VDB version: **build 353 (2022-03-07 22:13:19)**

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

Seleccione la actualización que prefiera. En este caso, la selección es para:

- Cancelar automáticamente en caso de fallo de actualización y revertir a la versión anterior.
- Habilitar la reversión después de una actualización correcta.
- Actualice Snort 2 a Snort 3.

- Seleccione el grupo HA de FTD y haga clic en 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)

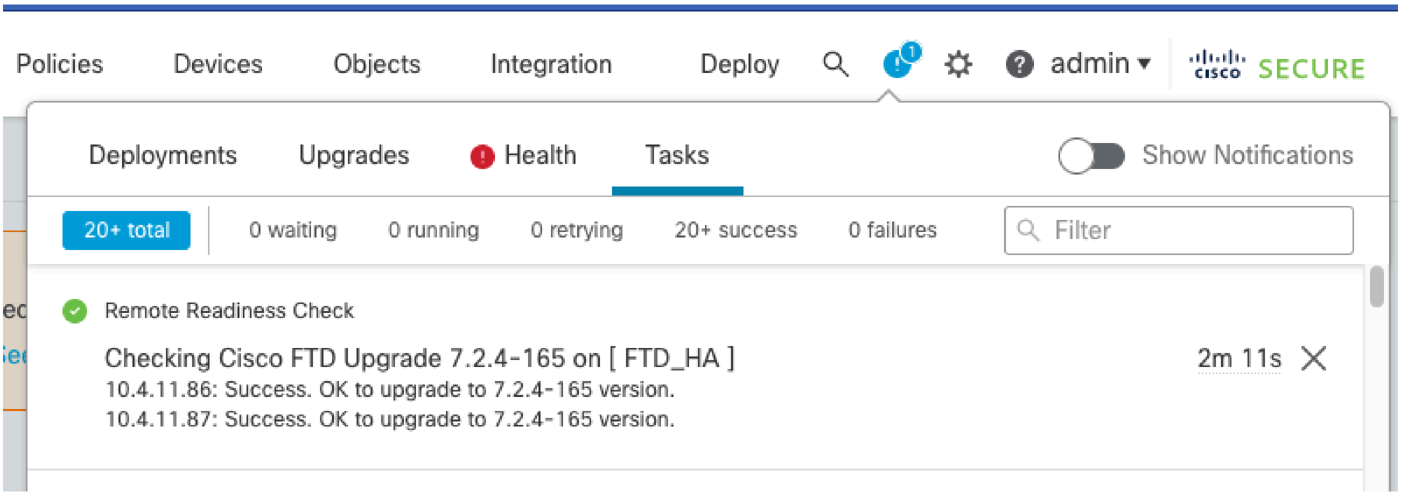
☑ **Enable revert after successful upgrade**

☑ **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

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

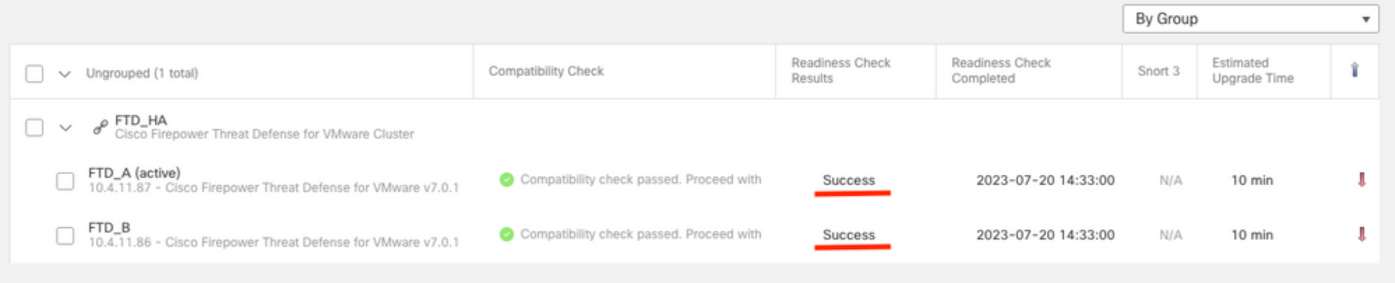
El progreso se puede verificar en el centro de mensajes Mensajes > Tareas.



✓ 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.

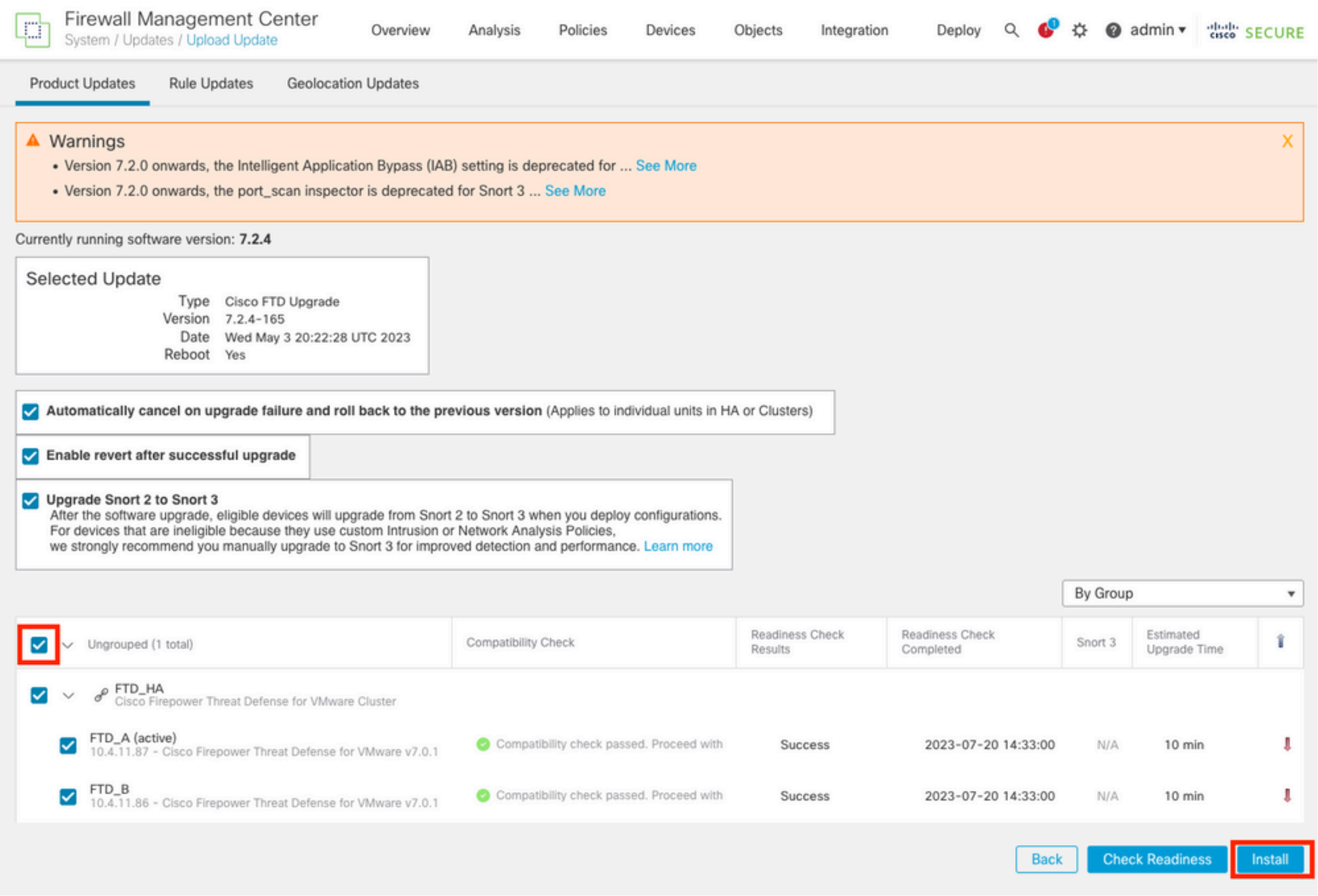
Una vez completada la comprobación de preparación en FTD y obtenido el resultado con éxito, se puede realizar la actualización.


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

Paso 3. Actualización de FTD en alta disponibilidad

- Seleccione el par HA y haga clic en 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)

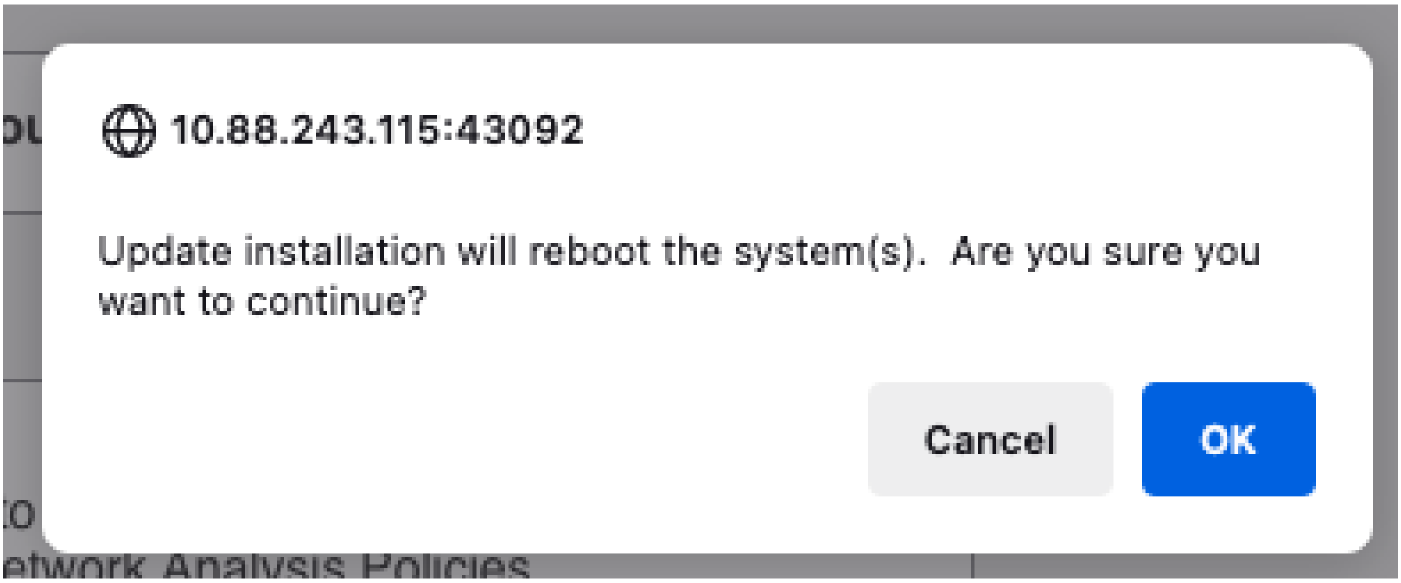
☑ **Enable revert after successful upgrade**

☑ **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

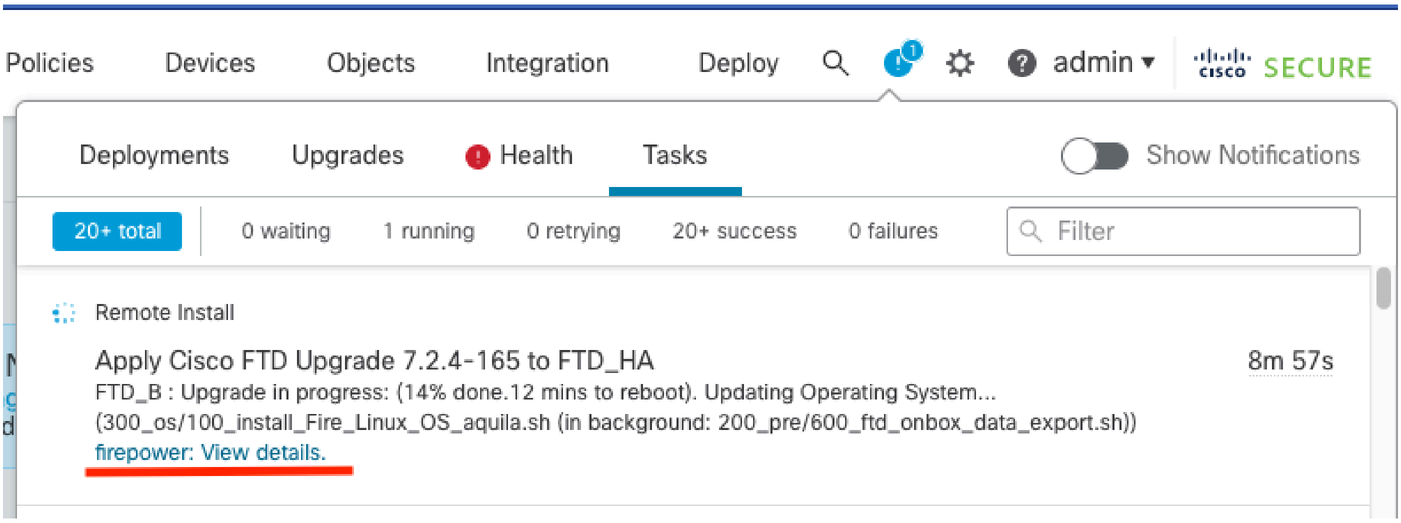
Advertencia para continuar con la actualización, el sistema se reinicia para completar la actualización. Seleccione Aceptar.



10.88.243.115:43092

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

El progreso se puede verificar en el centro de mensajes Mensajes > Tareas.



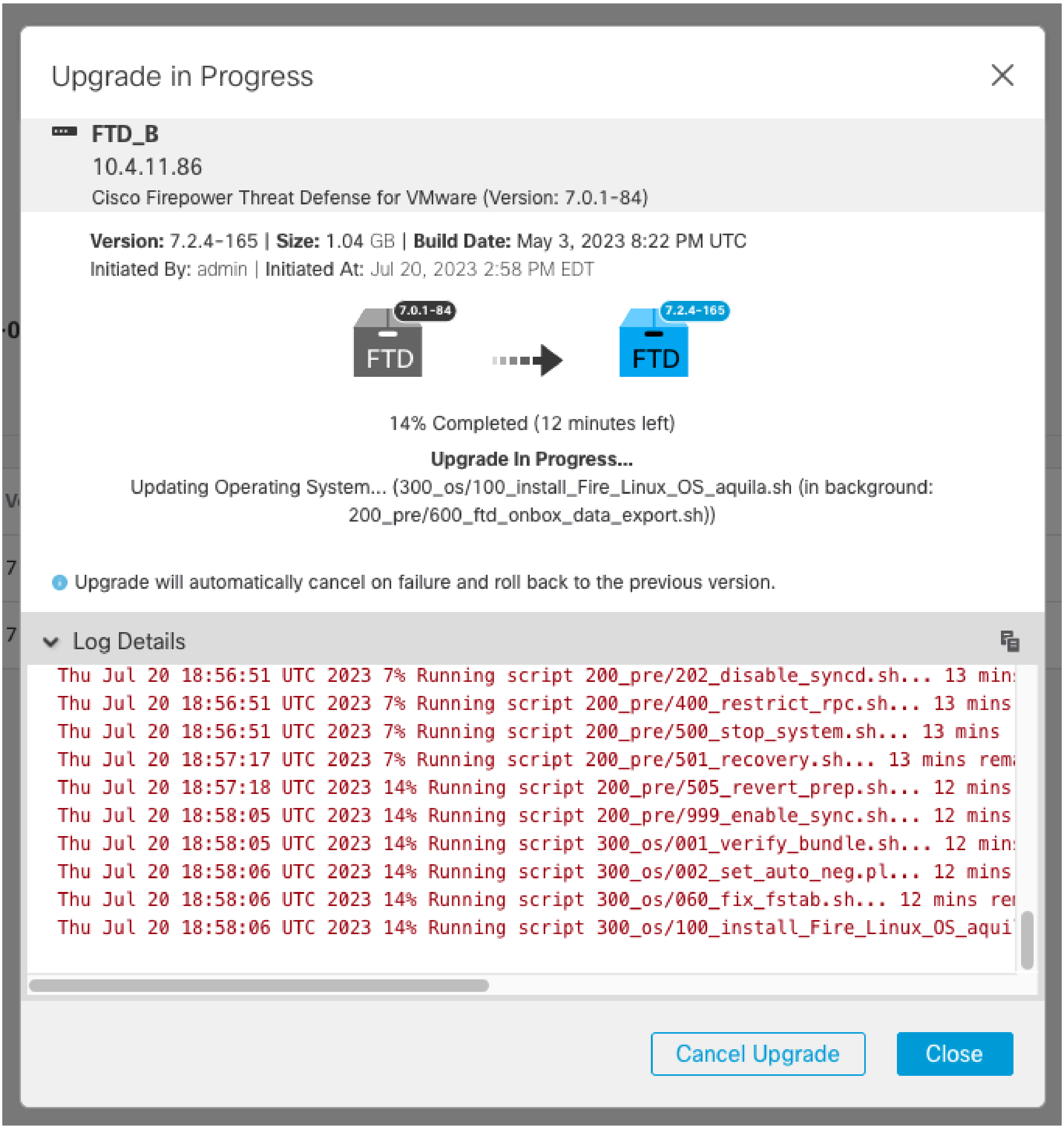
Remote Install

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.

Si hace clic en firepower: Ver detalles, el progreso se muestra de forma gráfica y los registros de status.log.



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
```

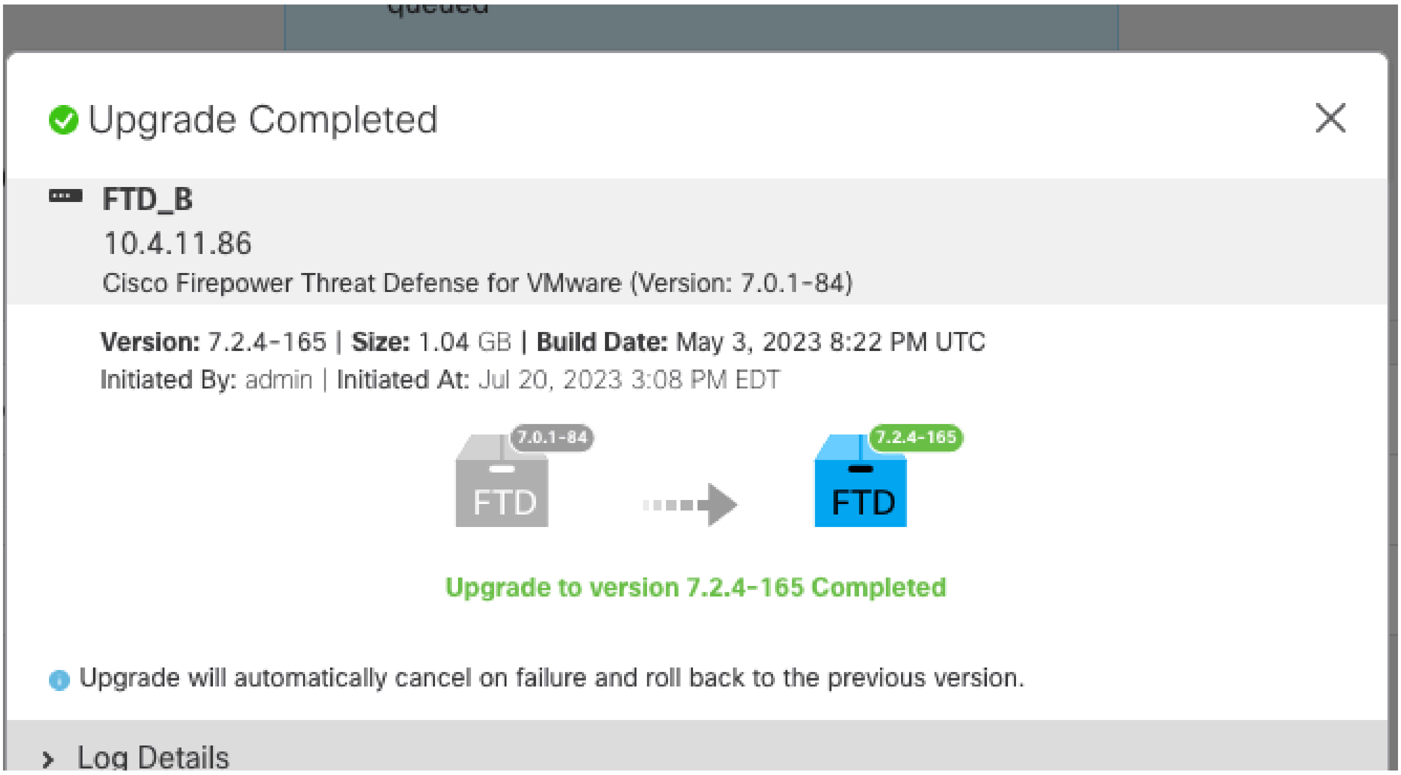
Nota: La actualización tarda unos 20 minutos por FTD.

En CLI, el progreso se puede verificar en la carpeta de actualización /ngfw/var/log/sf; pase al modo experto e ingrese al acceso raíz.

```
> 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!
```

El estado de actualización se marca como completado en la GUI y muestra los siguientes pasos.



queued

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

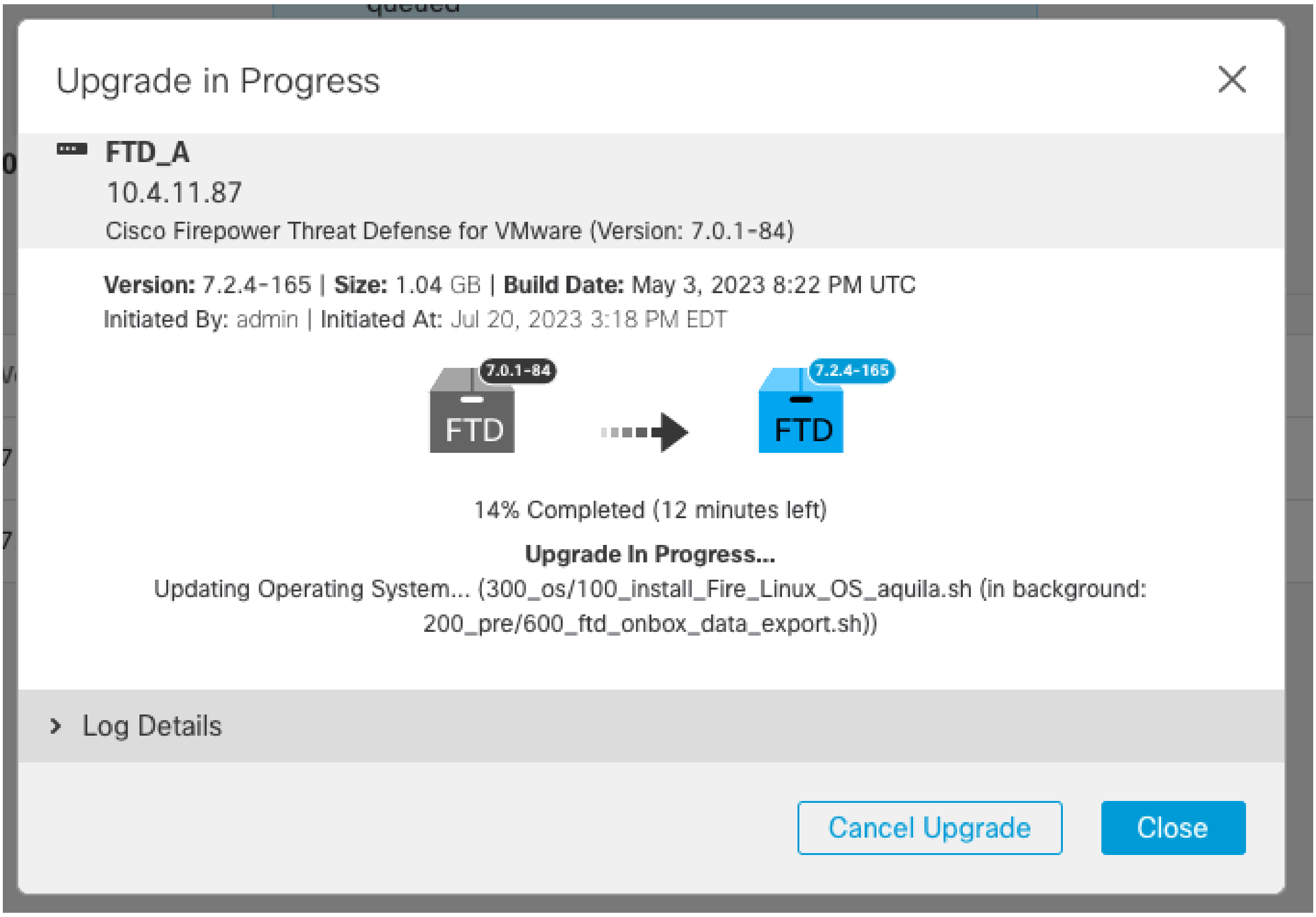
Initiated By: admin | Initiated At: Jul 20, 2023 3:08 PM EDT

Upgrade to version 7.2.4-165 Completed

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

Log Details

Una vez completada la actualización en el dispositivo en espera, se inicia en el dispositivo activo.



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...

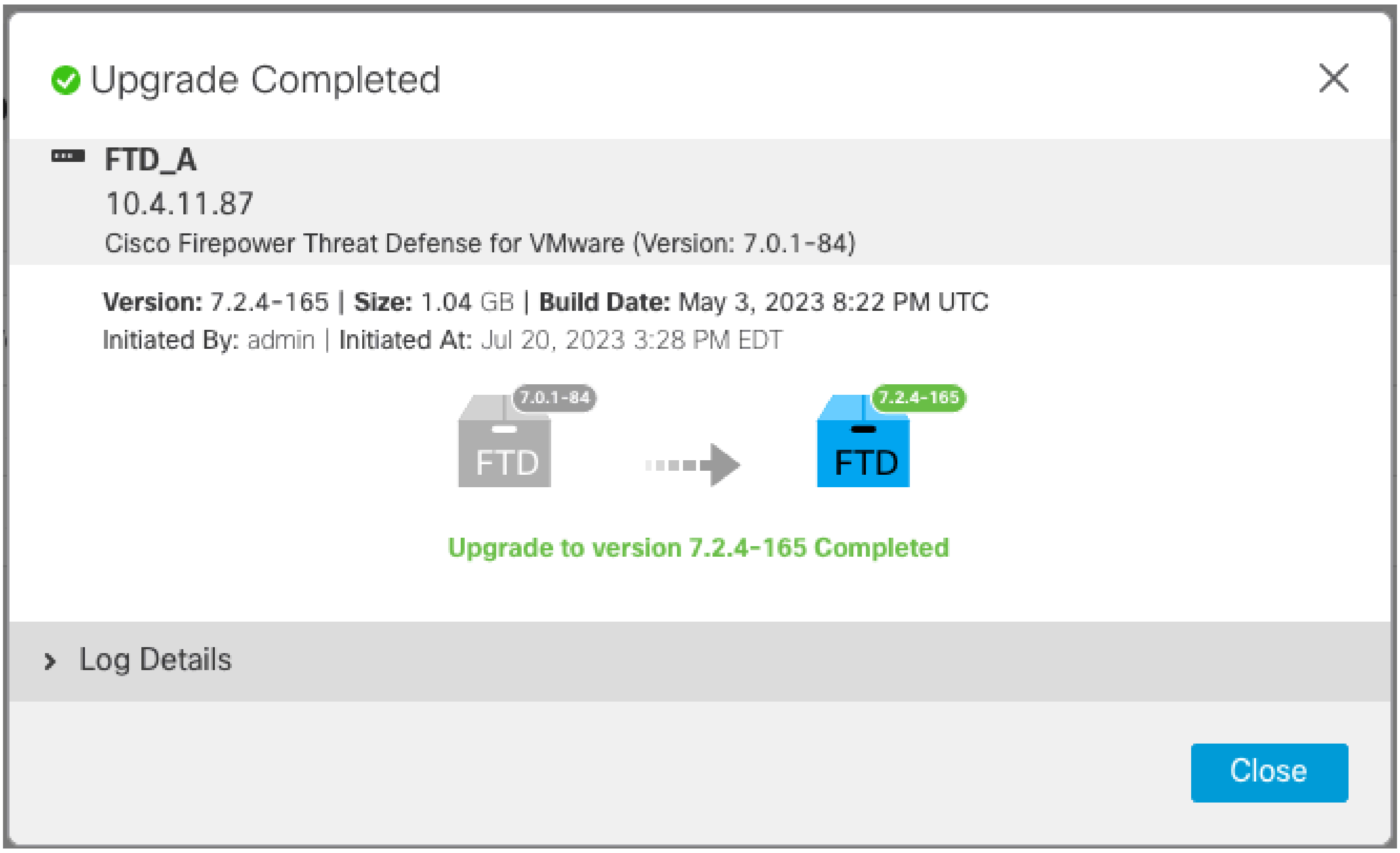
Updating Operating System... (300_os/100_install_Fire_Linux_OS_aquila.sh (in background: 200_pre/600_ftd_onbox_data_export.sh))

En CLI, vaya a LINA (system support diagnostic-cli) y verifique el estado de conmutación por fallas en el FTD en espera mediante el comando show failover state.

```
> 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
```

Nota: La conmutación por fallo se produce automáticamente como parte de la actualización. Antes de que el FTD activo se reinicie y complete la actualización.

Una vez completada la actualización, es necesario reiniciar:



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

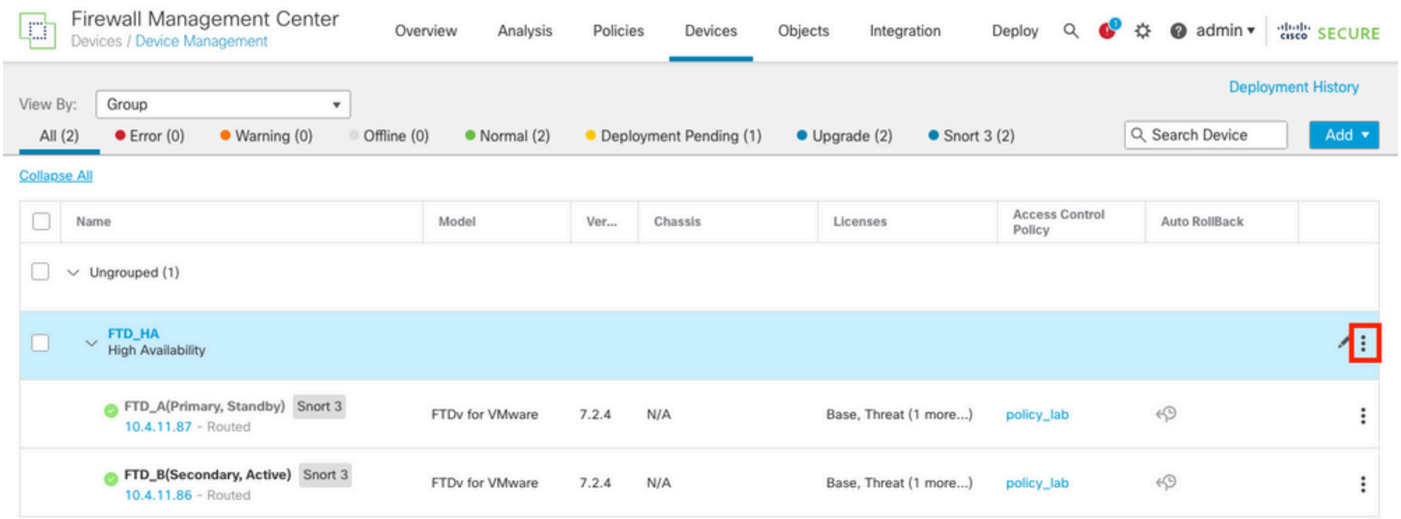
Upgrade to version 7.2.4-165 Completed

Paso 4. Switch Active Peer (Opcional)

Nota: si el dispositivo secundario está activo, no tiene ningún impacto en el funcionamiento.
Tener un dispositivo principal tan activo y secundario como en espera es una práctica recomendada que ayuda a realizar un seguimiento de cualquier fallo que se pueda producir.

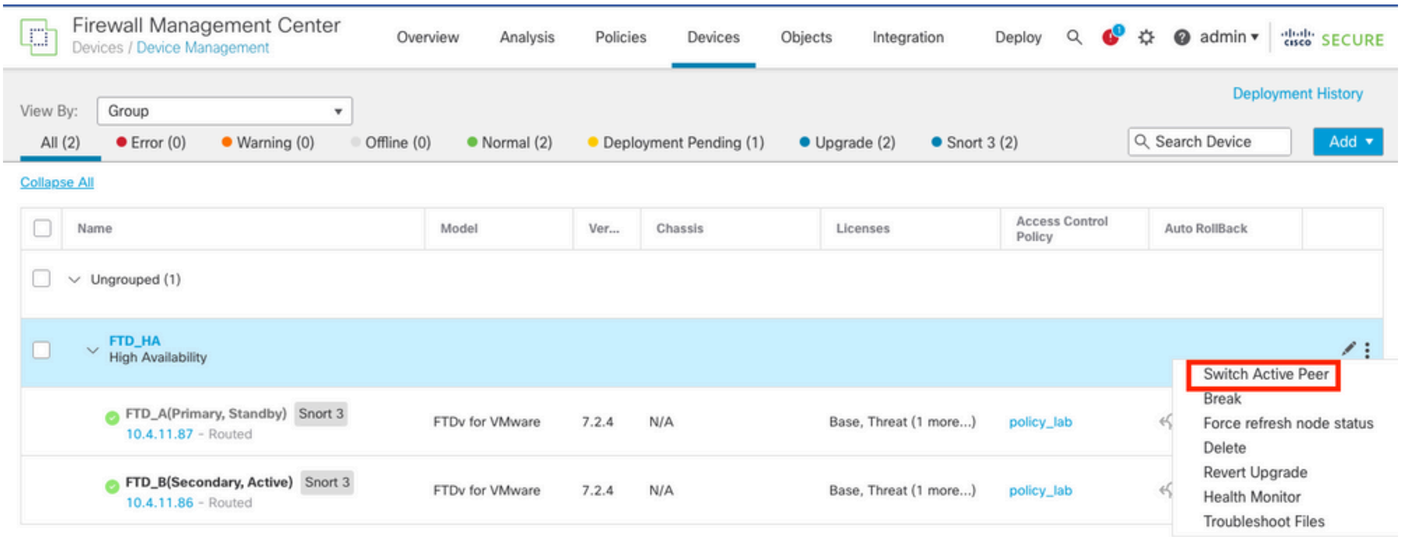
En este caso, el FTD activo está ahora en espera, se puede utilizar una conmutación por fallo manual para volver a activarlo.

- Desplácese hasta los tres puntos situados junto al signo de edición.



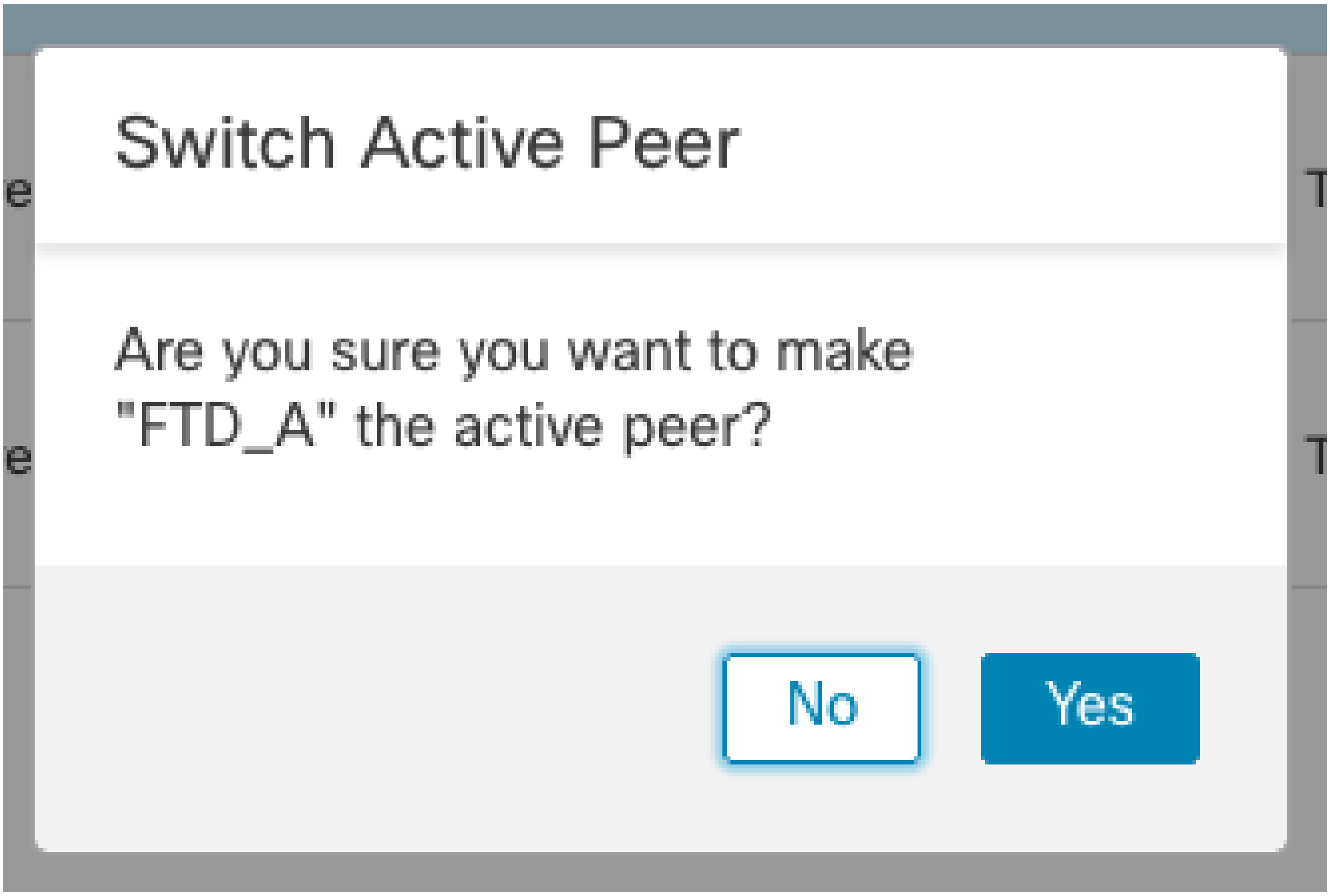
Name	Model	Ver...	Chassis	Licenses	Access Control Policy	Auto RollBack
Ungrouped (1)						
FTD_HA High Availability						
FTD_A(Primary, Standby) Snort 3 10.4.11.87 - Routed	FTDv for VMware	7.2.4	N/A	Base, Threat (1 more...)	policy_lab	
FTD_B(Secondary, Active) Snort 3 10.4.11.86 - Routed	FTDv for VMware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

- Seleccione Switch Active 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	

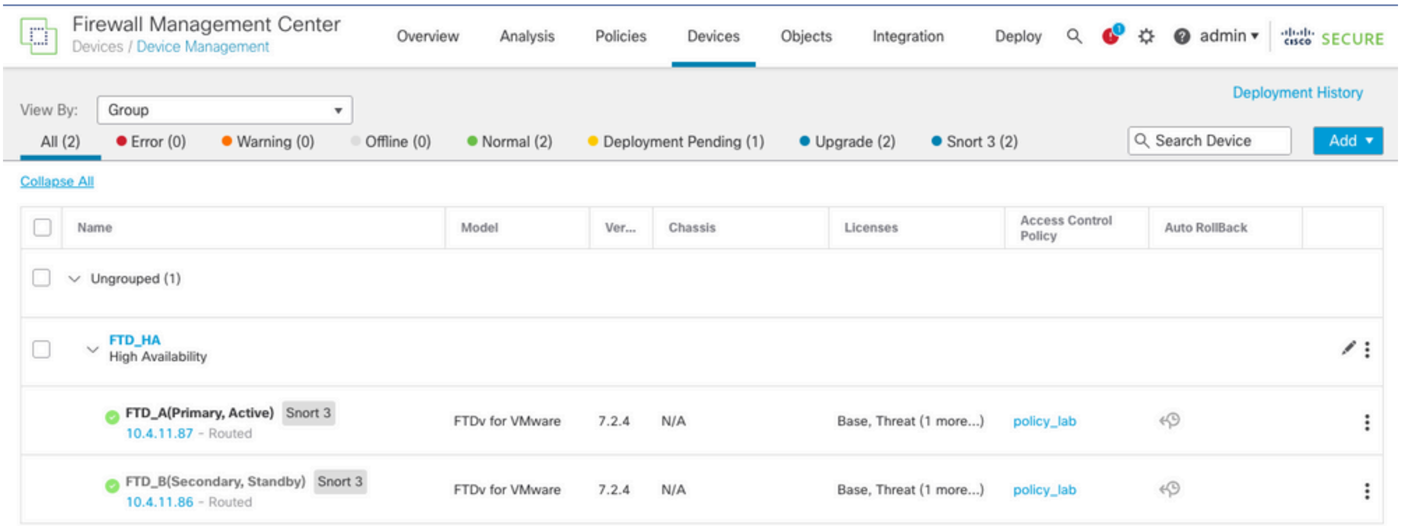
- Seleccione YES para confirmar la conmutación por error.



Switch Active Peer

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

Validación del estado de alta disponibilidad al final de la actualización y conmutación por fallo realizada.
Devices > Device Management



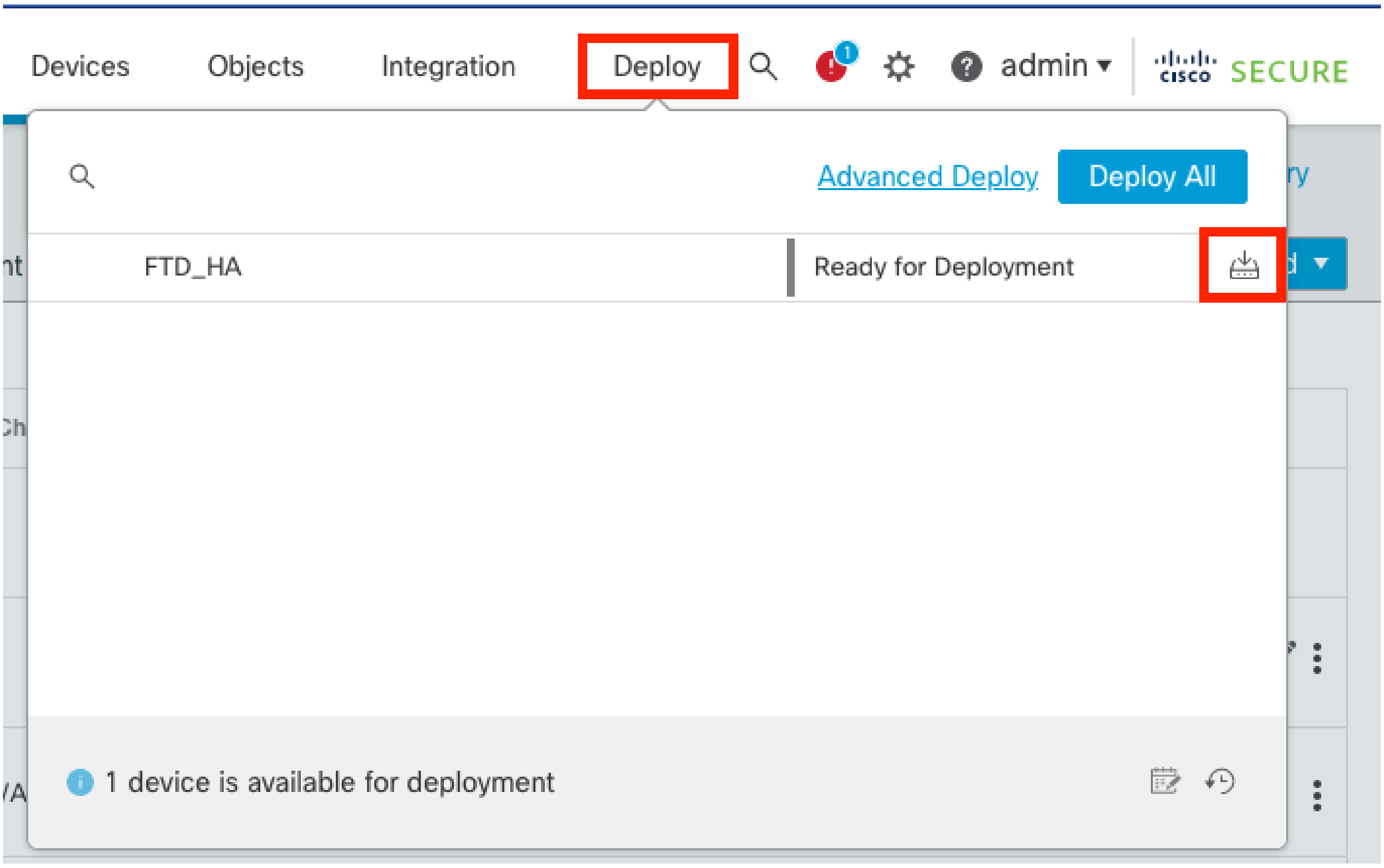
View By: Group

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	

Paso 5. Implementación final

- Implementar una política en dispositivos Implementar > Implementar en este dispositivo.



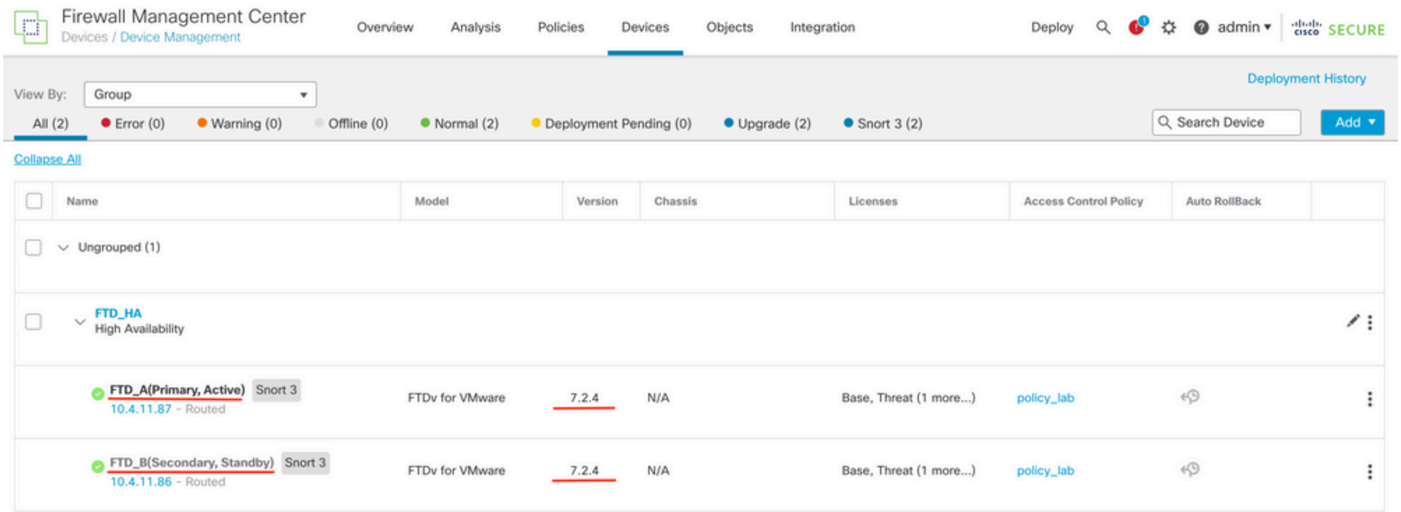
FTD_HA | Ready for Deployment

1 device is available for deployment

Validar

Para validar que el estado de alta disponibilidad y la actualización han finalizado, debe confirmar el estado:
Primario: Activo
Secundario: preparado en espera
Ambos se encuentran en la versión que es la que se ha cambiado recientemente (7.2.4 en este ejemplo).

- En FMC GUI, navegue hasta Devices > Device Management.



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	

- Durante el clish de CLI, verifique el estado de failover usando el comando show failover state y show failover para obtener información más detallada.

```
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
```

Si ambos FTD se encuentran en la misma versión y el estado de alta disponibilidad es correcto, la actualización ha finalizado.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).