

Mise à niveau FTD HA gérée par FMC

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Aperçu](#)

[Informations générales](#)

[Configurer](#)

[Étape 1. Télécharger le package de mise à niveau](#)

[Étape 2. Vérifier le niveau de préparation](#)

[Étape 3. Mettre à niveau FTD en haute disponibilité](#)

[Étape 4. Commutateur homologue actif \(facultatif\)](#)

[Étape 5. Déploiement final](#)

[Valider](#)

Introduction

Ce document décrit le processus de mise à niveau d'un pare-feu Cisco Secure Firewall Threat Defense en haute disponibilité géré par un Firewall Management Center.

Conditions préalables

Exigences

Cisco recommande de posséder des connaissances sur ces sujets :

- Concepts et configuration de la haute disponibilité (HA)
- Configuration de Secure Firewall Management Center (FMC)
- Configuration de Cisco Secure Firewall Threat Defense (FTD)

Composants utilisés

Les informations contenues dans ce document sont basées sur :

- Virtual Firewall Management Center (FMC), version 7.2.4
- Protection contre les menaces par pare-feu Cisco virtuel (FTD), version 7.0.1

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Aperçu

Le fonctionnement du FMC consiste à mettre à niveau un homologue à la fois. Commencez par le mode veille, puis le mode actif, en effectuant un basculement avant que la mise à niveau active ne soit terminée.

Informations générales

Le package de mise à niveau doit être téléchargé à partir du site software.cisco.com avant la mise à niveau.

Sur l'interférence CLI, exécutez la commande `show high-availability config` dans le FTD actif pour vérifier l'état de la haute disponibilité.

```
> 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 aucune erreur n'est visible, passez à la mise à niveau.

Configurer

Étape 1. Télécharger le package de mise à niveau

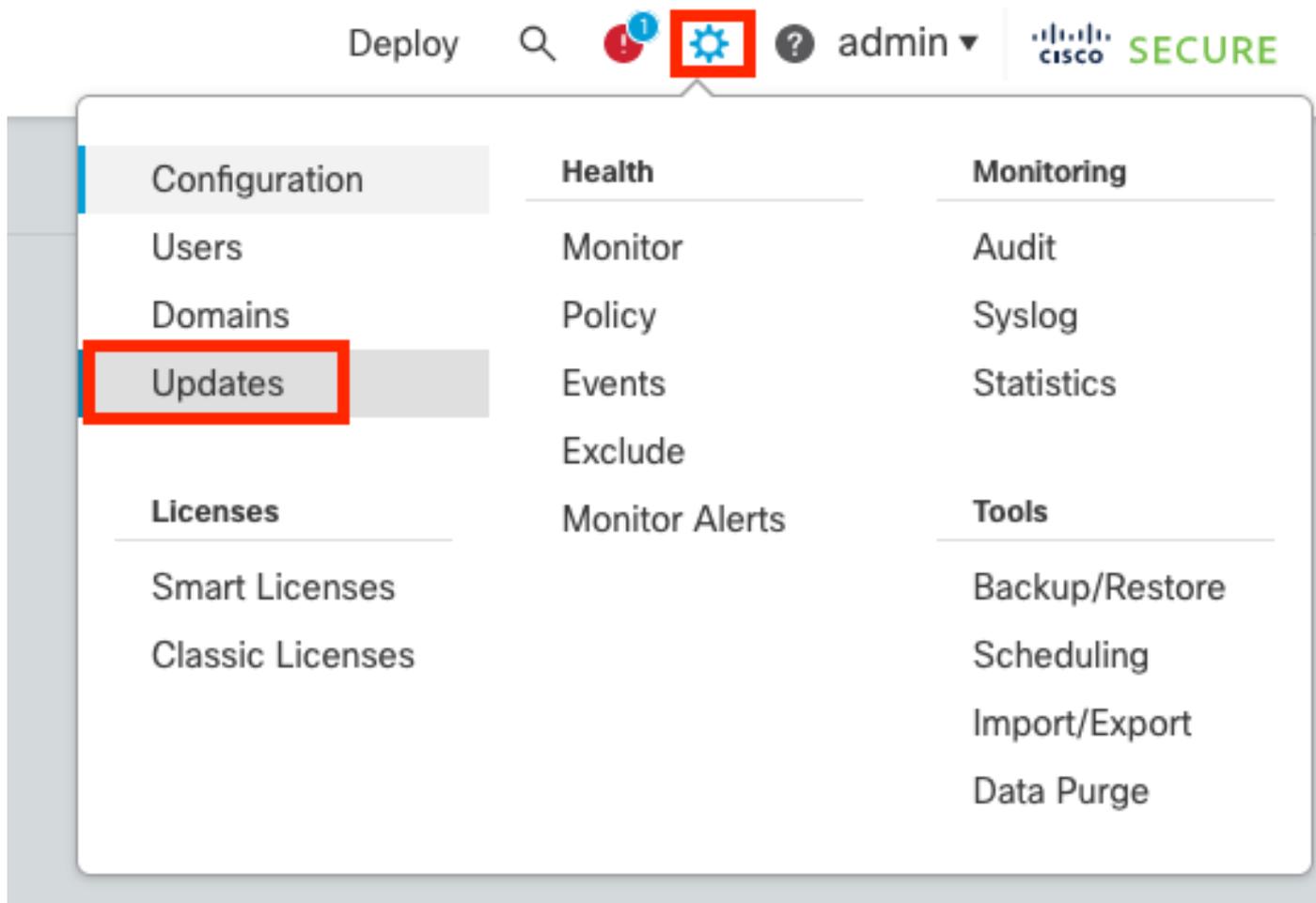
- Téléchargez le package de mise à niveau FTD sur le FMC à l'aide de l'interface graphique utilisateur (GUI).

Ce fichier doit être préalablement téléchargé à partir du site du logiciel Cisco en fonction du modèle FTD et de la version souhaitée.

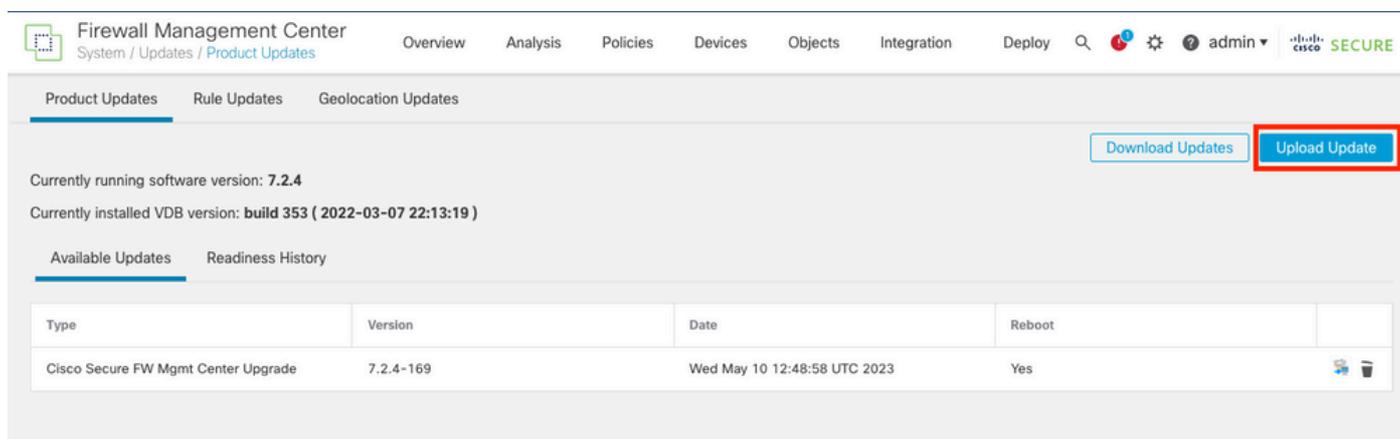


Avertissement : assurez-vous que la version FMC est supérieure ou égale à la nouvelle version FTD à mettre à niveau.

Système > Mises à jour



- Sélectionnez Upload Update.



- Recherchez l'image précédemment téléchargée, puis sélectionnez Upload.

Firewall Management Center
System / Updates / Product Updates

Overview Analysis Policies Devices Objects Integration Deploy

Product Updates Rule Updates Geolocation Updates

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

Cancel Upload

Étape 2. Vérifier le niveau de préparation

Les contrôles de préparation confirment que les appliances sont prêtes à être mises à niveau.

- Sélectionnez l'option Install dans le package de mise à niveau approprié.

Firewall Management Center
System / Updates / Product Updates

Overview Analysis Policies Devices Objects Integration Deploy

Product Updates Rule Updates Geolocation Updates

Download Updates Upload Update

Success
Upload succeeded

Currently running software version: 7.2.4
Currently installed VDB version: build 353 (2022-03-07 22:13:19)

Available Updates Readiness History

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	 

Sélectionnez la mise à niveau que vous préférez. Dans ce cas, la sélection porte sur :

- Annuler automatiquement en cas d'échec de la mise à niveau et revenir à la version précédente.
- Activer le rétablissement après une mise à niveau réussie.
- Passez de Snort 2 à Snort 3.
- Sélectionnez le groupe HA de FTDs et cliquez sur Check Readiness.

Product Updates Rule Updates Geolocation Updates

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 ▾

	Compatibility Check	Readiness Check Results	Readiness Check Completed	Snort 3	Estimated Upgrade Time	
<input checked="" type="checkbox"/> Ungrouped (1 total)						
<input checked="" type="checkbox"/> FTD_HA Cisco Firepower Threat Defense for VMware Cluster						
<input checked="" type="checkbox"/> 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	⚠
<input checked="" type="checkbox"/> FTD_B 10.4.11.86 - Cisco Firepower Threat Defense for VMware v7.0.1	✔ Compatibility check passed. Proceed with			N/A	10 min	⚠

La progression peut être vérifiée dans le centre de messages Messages > Tâches.

Policies Devices Objects Integration Deploy 🔍 📢 ⚙️ ? admin ▾ CISCO SECURE

Deployments Upgrades 🚨 Health **Tasks** 🏷️ Show Notifications

20+ total 0 waiting 0 running 0 retrying 20+ success 0 failures 🔍 Filter

✔ 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.

Lorsque la vérification du niveau de préparation est terminée dans FTD et que le résultat est Success, la mise à niveau peut être effectuée.

By Group ▾

	Compatibility Check	Readiness Check Results	Readiness Check Completed	Snort 3	Estimated Upgrade Time	
<input type="checkbox"/> Ungrouped (1 total)						
<input type="checkbox"/> FTD_HA Cisco Firepower Threat Defense for VMware Cluster						
<input type="checkbox"/> 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	⚠
<input type="checkbox"/> 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	⚠

Étape 3. Mettre à niveau FTD en haute disponibilité

- Sélectionnez la paire haute disponibilité et cliquez sur Installer.

Firewall Management Center
System / Updates / Upload Update

Overview Analysis Policies Devices Objects Integration Deploy 🔍 ⚙️ ? admin 🔒 cisco SECURE

Product Updates Rule Updates Geolocation Updates

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 ▾

<input checked="" type="checkbox"/>	Ungrouped (1 total)	Compatibility Check	Readiness Check Results	Readiness Check Completed	Snort 3	Estimated Upgrade Time	
<input checked="" type="checkbox"/>	FTD_HA Cisco Firepower Threat Defense for VMware Cluster						
<input checked="" type="checkbox"/>	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	⬇️
<input checked="" type="checkbox"/>	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	⬇️

Avertissement : pour poursuivre la mise à niveau, le système redémarre pour terminer la mise à niveau. Sélectionnez OK.

 10.88.243.115:43092

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

La progression peut être vérifiée dans le centre de messages Messages > Tâches.

20+ total

0 waiting

1 running

0 retrying

20+ success

0 failures

 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 vous cliquez sur firepower : View details, la progression est affichée de façon graphique et les journaux de status.log.

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 mins
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 mins
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
```

Cancel Upgrade

Close

Remarque : la mise à niveau prend environ 20 minutes par FTD.

Sur l'interface de ligne de commande, la progression peut être vérifiée dans le dossier de mise à niveau /ngfw/var/log/sf ; passez en mode expert et entrez l'accès racine.

```
> 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.log

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.

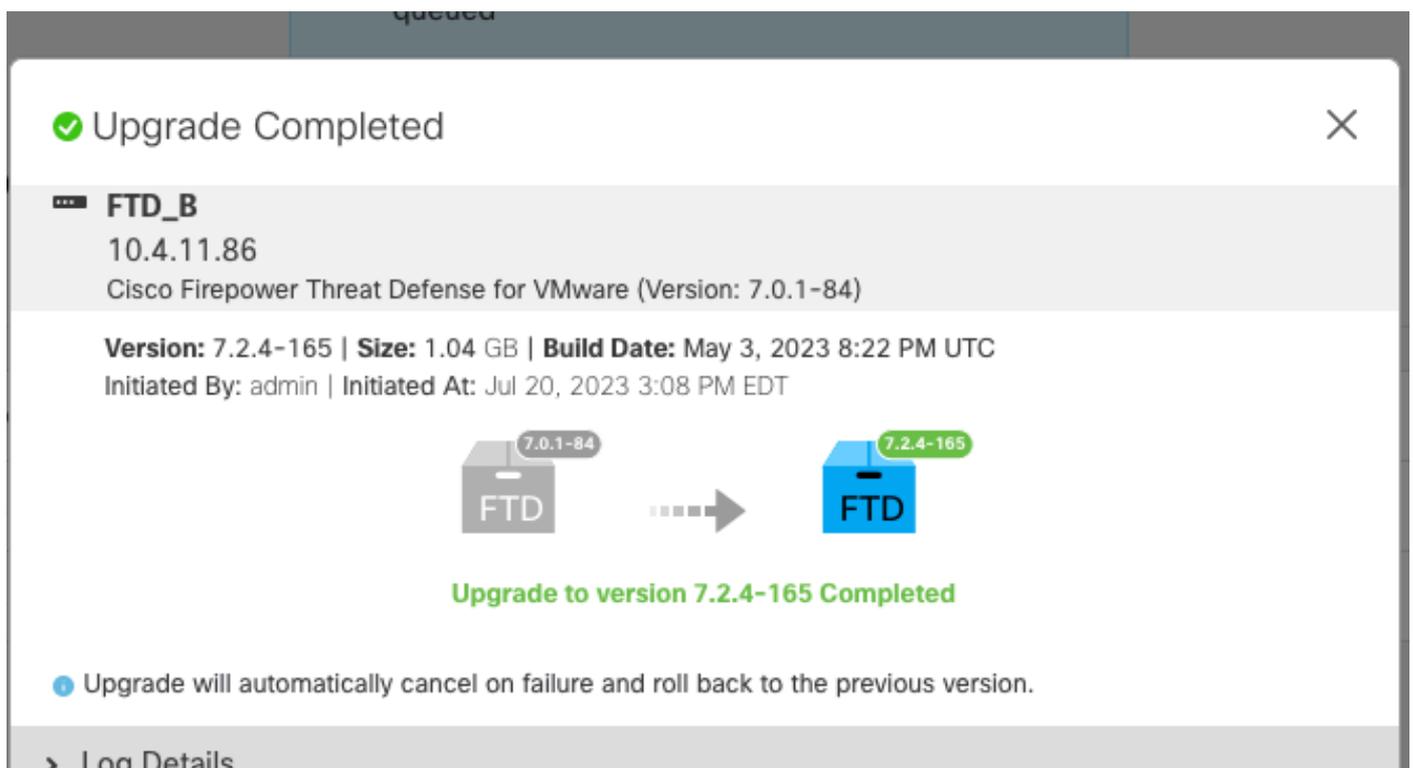
Broadcast message from root@firepower (Thu Jul 20 19:05:25 2023):

System will reboot now due to system upgrade.

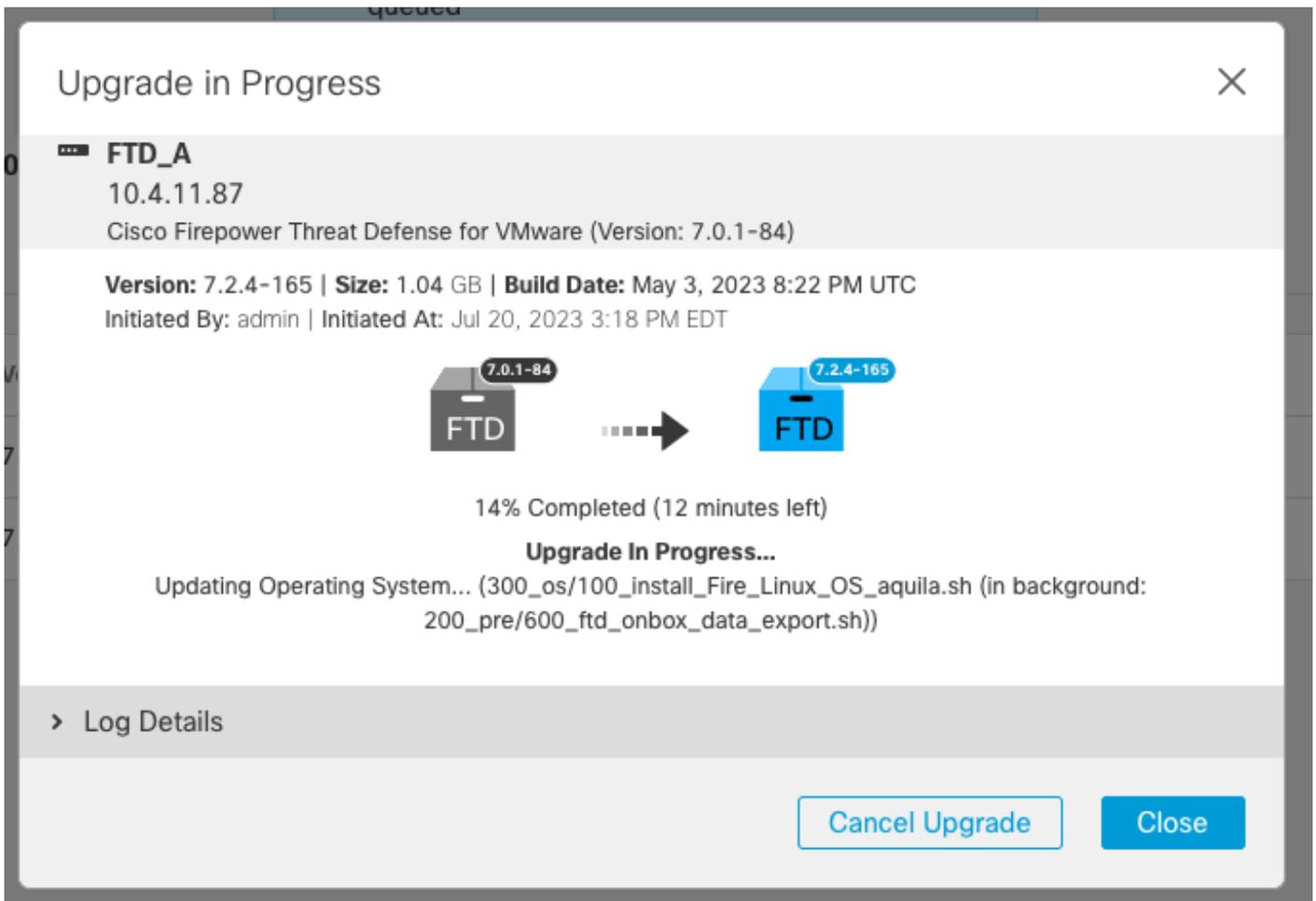
Broadcast message from root@firepower (Thu Jul 20 19:05:34 2023):

The system is going down for reboot NOW!

L'état de la mise à niveau est marqué comme terminé sur l'interface utilisateur graphique et indique les étapes suivantes.



Une fois la mise à niveau effectuée sur le périphérique en veille, elle démarre sur le périphérique actif.



Sur l'interface de ligne de commande, passez à LINA (system support diagnostic-cli) et vérifiez l'état de basculement sur le FTD de secours à l'aide de la commande show failover state.

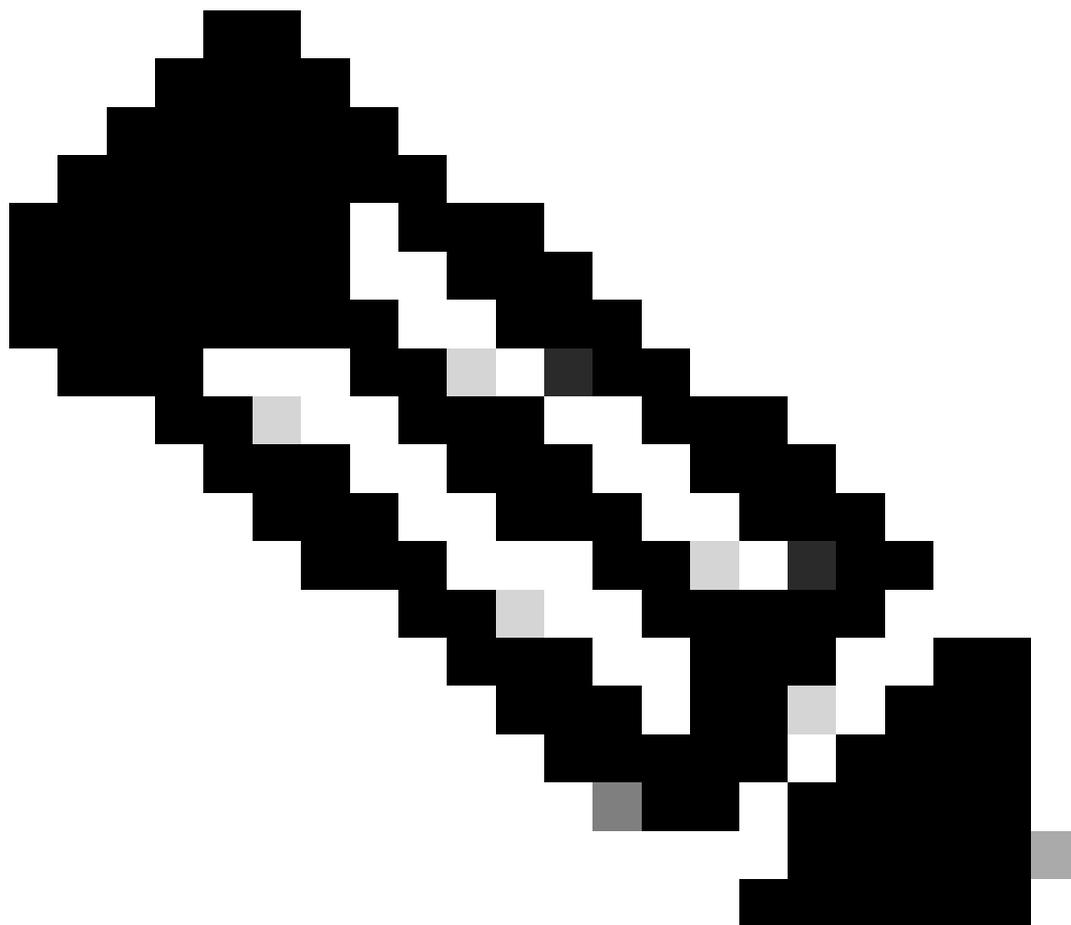
```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

firepower> enable
Password:
firepower# show failover state

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

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

firepower#
Switching to Active
```



Remarque : le basculement se produit automatiquement lors de la mise à niveau. Avant le redémarrage du FTD actif et la mise à niveau.

Une fois la mise à niveau terminée, un redémarrage est nécessaire :

✔ 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

> Log Details

Close

Étape 4. Commutateur homologue actif (facultatif)



Remarque : si le périphérique secondaire est actif, il n'a aucun impact opérationnel.
Le fait que le périphérique principal soit actif et le périphérique secondaire en veille est une bonne pratique qui permet de suivre tout basculement qui peut se produire.

Dans ce cas, le FTD actif est maintenant en veille, un basculement manuel peut être utilisé pour le redéfinir sur Actif.

- Naviguez jusqu'aux trois points situés à côté du signe de modification.

Firewall Management Center
Devices / Device Management

Overview Analysis Policies **Devices** Objects Integration Deploy 🔍 ⚙️ 👤 admin 🔒 **SECURE**

View By: Group

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

[Collapse All](#)

<input type="checkbox"/>	Name	Model	Ver...	Chassis	Licenses	Access Control Policy	Auto RollBack	
<input type="checkbox"/>	Ungrouped (1)							
<input type="checkbox"/>	FTD_HA High Availability							
●	FTD_A(Primary, Standby) 10.4.11.87 - Routed	FTDv for VMware	7.2.4	N/A	Base, Threat (1 more...)	policy_lab	↶	⋮
●	FTD_B(Secondary, Active) 10.4.11.86 - Routed	FTDv for VMware	7.2.4	N/A	Base, Threat (1 more...)	policy_lab	↶	⋮

- Sélectionnez Commutateur homologue actif.

Firewall Management Center
Devices / Device Management

Overview Analysis Policies **Devices** Objects Integration Deploy 🔍 ⚙️ 👤 admin 🔒 **SECURE**

View By: Group

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

[Collapse All](#)

<input type="checkbox"/>	Name	Model	Ver...	Chassis	Licenses	Access Control Policy	Auto RollBack	
<input type="checkbox"/>	Ungrouped (1)							
<input type="checkbox"/>	FTD_HA High Availability							
●	FTD_A(Primary, Standby) 10.4.11.87 - Routed	FTDv for VMware	7.2.4	N/A	Base, Threat (1 more...)	policy_lab	↶	<div style="border: 1px solid gray; padding: 5px;"> Switch Active Peer Break Force refresh node status Delete Revert Upgrade Health Monitor Troubleshoot Files </div>
●	FTD_B(Secondary, Active) 10.4.11.86 - Routed	FTDv for VMware	7.2.4	N/A	Base, Threat (1 more...)	policy_lab	↶	

- Sélectionnez YES pour confirmer le basculement.

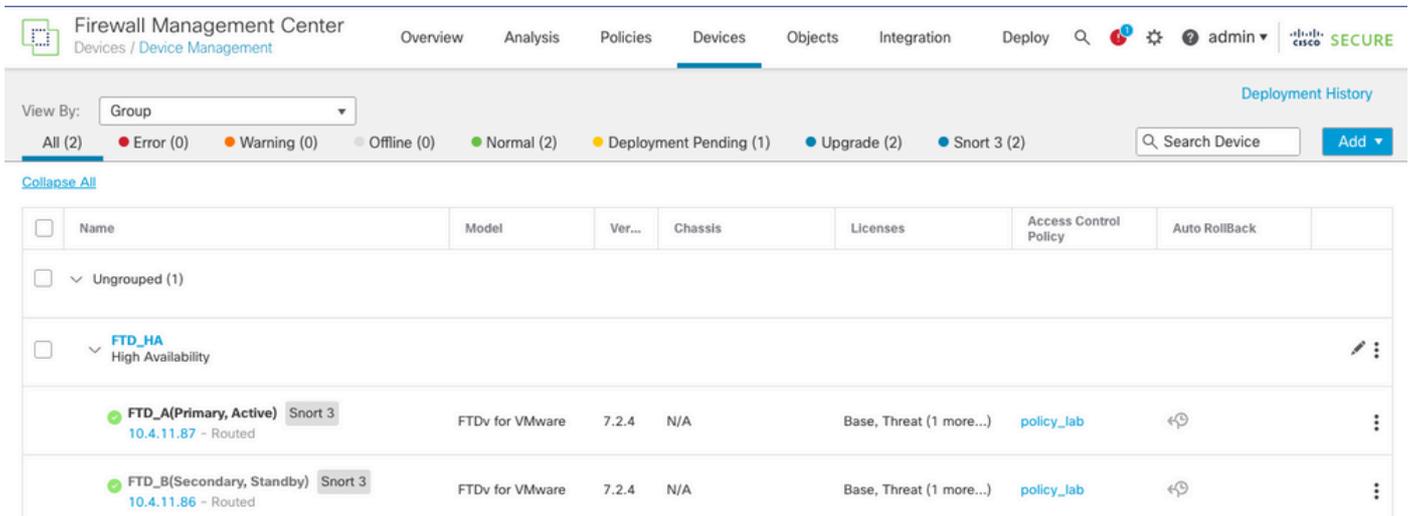
Switch Active Peer

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

No

Yes

Validation de l'état de haute disponibilité à la fin de la mise à niveau et du basculement effectuée.
Périphériques > Gestion des périphériques



Firewall Management Center
Devices / Device Management

Overview Analysis Policies **Devices** Objects Integration Deploy

View By: Group

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

Deployment History

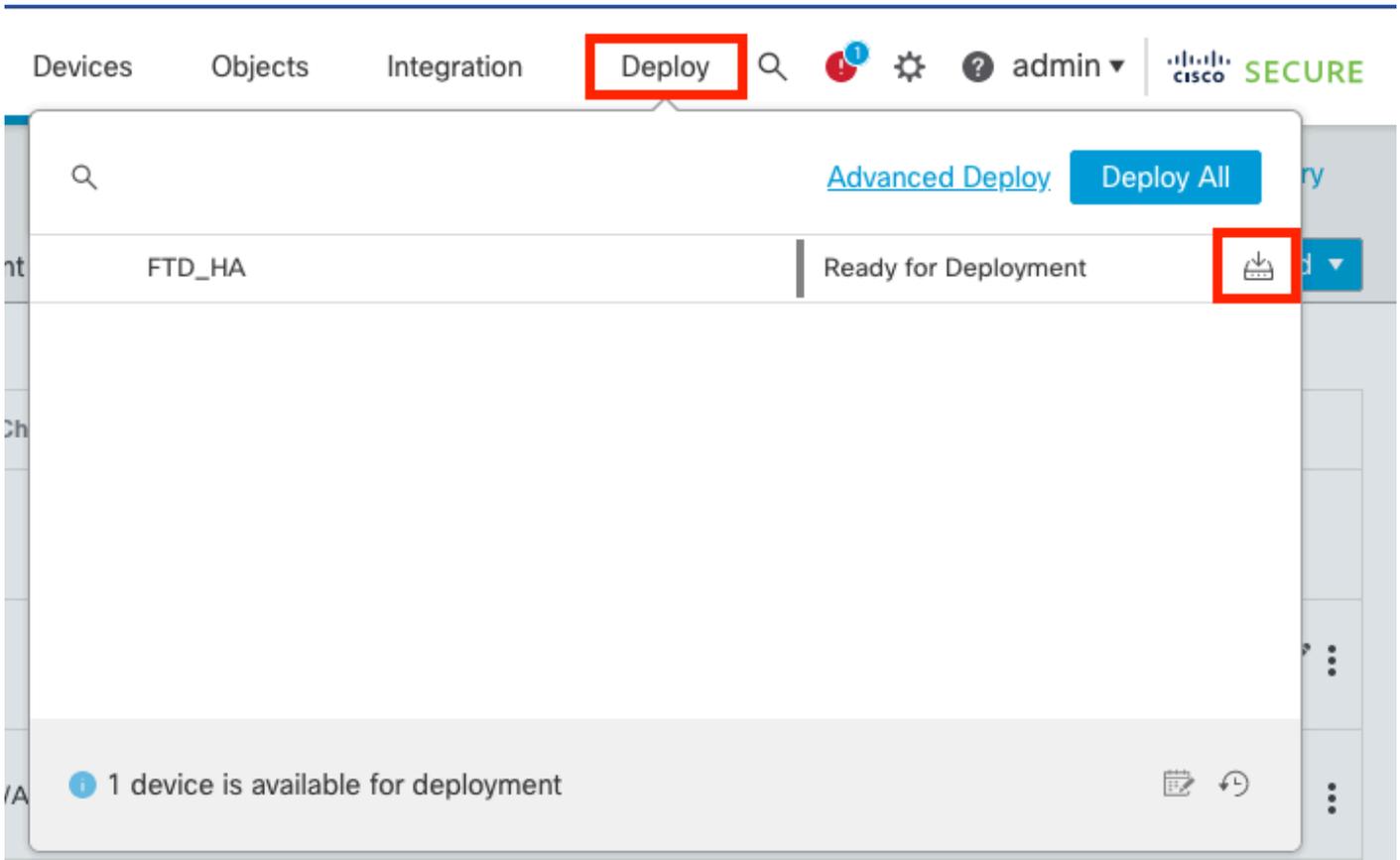
Search Device Add

Collapse All

<input type="checkbox"/>	Name	Model	Ver...	Chassis	Licenses	Access Control Policy	Auto RollBack	
<input type="checkbox"/>	Ungrouped (1)							
<input type="checkbox"/>	FTD_HA High Availability							
<input checked="" type="checkbox"/>	FTD_A(Primary, Active) 10.4.11.87 - Routed	FTDv for VMware	7.2.4	N/A	Base, Threat (1 more...)	policy_lab	↺	⋮
<input checked="" type="checkbox"/>	FTD_B(Secondary, Standby) 10.4.11.86 - Routed	FTDv for VMware	7.2.4	N/A	Base, Threat (1 more...)	policy_lab	↺	⋮

Étape 5. Déploiement final

- Déployer une stratégie sur les périphériques Déployer > Déployer sur ce périphérique.



Valider

Pour valider l'état de haute disponibilité et la mise à niveau, vous devez confirmer l'état :

Principal : actif

Secondaire : en veille

Les deux sont sous la version qui a été récemment modifiée (7.2.4 dans cet exemple).

- Dans l'interface utilisateur graphique de FMC, accédez à Périphériques > Gestion des périphériques.

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	↶

- Sur l'interface CLI, vérifiez l'état de basculement à l'aide des commandes show failover

state et show failover pour des informations plus détaillées.

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 les deux FTD sont sur la même version et que l'état de haute disponibilité est sain, la mise à niveau est terminée.

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.