Mise à niveau FTD HA gérée par FDM

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés
- Aperçu

Informations générales

Configurer

- Télécharger le package de mise à niveau
- Vérifier le niveau de préparation
- Mise à niveau FTD en haute disponibilité
- Commutateur homologue actif (facultatif)
- 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 Firepower Device Manager.

Conditions préalables

Exigences

Cisco vous recommande d'avoir des connaissances sur les sujets suivants :

- Concepts et configuration de la haute disponibilité (HA)
- Configuration de Cisco Secure Firepower Device Manager (FDM)
- Configuration de Cisco Secure Firewall Threat Defense (FTD)

Composants utilisés

Les informations contenues dans ce document sont basées sur Virtual Cisco FTD, version 7.2.8.

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 mode de fonctionnement de FDM consiste à mettre à niveau un homologue à la fois. Tout d'abord la mise en veille, puis la mise en service active, qui effectue un basculement avant le démarrage de la mise à niveau active.

Informations générales

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

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

```
> show high-availability config

Failover On

Failover unit Primary

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

Reconnect timeout 0:00:00

Unit Poll frequency 1 seconds, holdtime 15 seconds

Interface Poll frequency 5 seconds, holdtime 25 seconds

Interface Policy 1

Monitored Interfaces 3 of 311 maximum

MAC Address Move Notification Interval not set

failover replication http

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

Serial Number: Ours 9A1QUNFWPK1, Mate 9A45VNEHB5C

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

        This host: Primary - Active

                Active time: 507441 (sec)
```

```
            slot 0: ASAv hw/sw rev (/9.18(3)53) status (Up Sys)
              Interface diagnostic (0.0.0.0): Normal (Waiting)
              Interface inside (192.168.45.1): Normal (Waiting)
              Interface outside (192.168.1.10): Normal (Waiting)
            slot 1: snort rev (1.0)  status (up)
            slot 2: diskstatus rev (1.0)  status (up)
        Other host: Secondary - Standby Ready
            Active time: 8 (sec)
              Interface diagnostic (0.0.0.0): Normal (Waiting)
              Interface inside (0.0.0.0): Normal (Waiting)
              Interface outside (0.0.0.0): Normal (Waiting)
            slot 1: snort rev (1.0)  status (up)
            slot 2: diskstatus rev (1.0)  status (up)
```

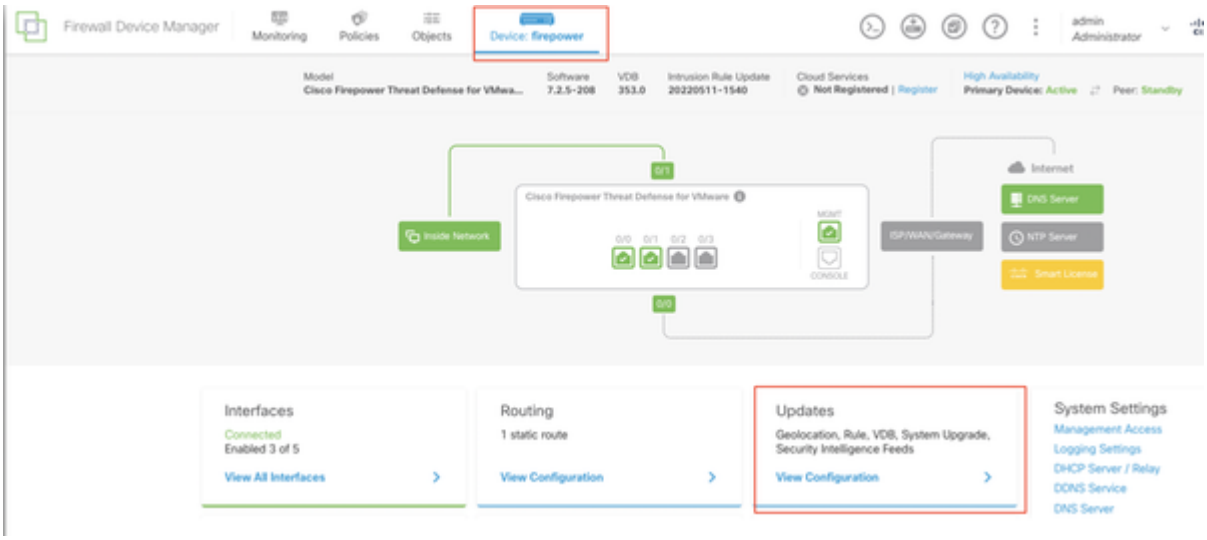
Si aucune erreur n'est visible, poursuivez la mise à niveau.

Configurer

Télécharger le package de mise à niveau

1. Téléchargez le package de mise à niveau FTD sur le FDM à l'aide de l'interface utilisateur graphique.

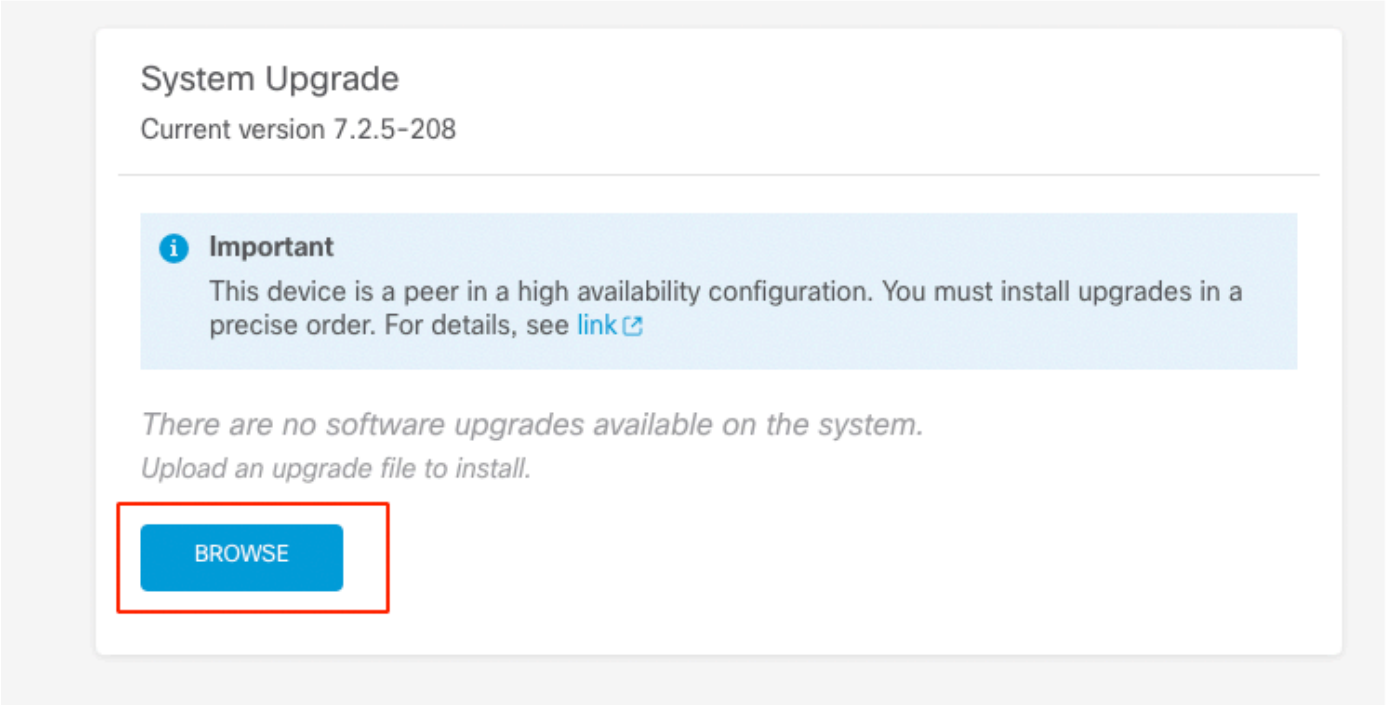
Ce fichier doit être préalablement téléchargé à partir du site du logiciel Cisco en fonction du modèle FTD et de la version souhaitée. Accédez à Device > Updates > System Upgrade :



Mises à jour

2. Recherchez l'image précédemment téléchargée, puis choisissez Télécharger.

Remarque : Téléchargez l'image sur les noeuds actifs et en veille.



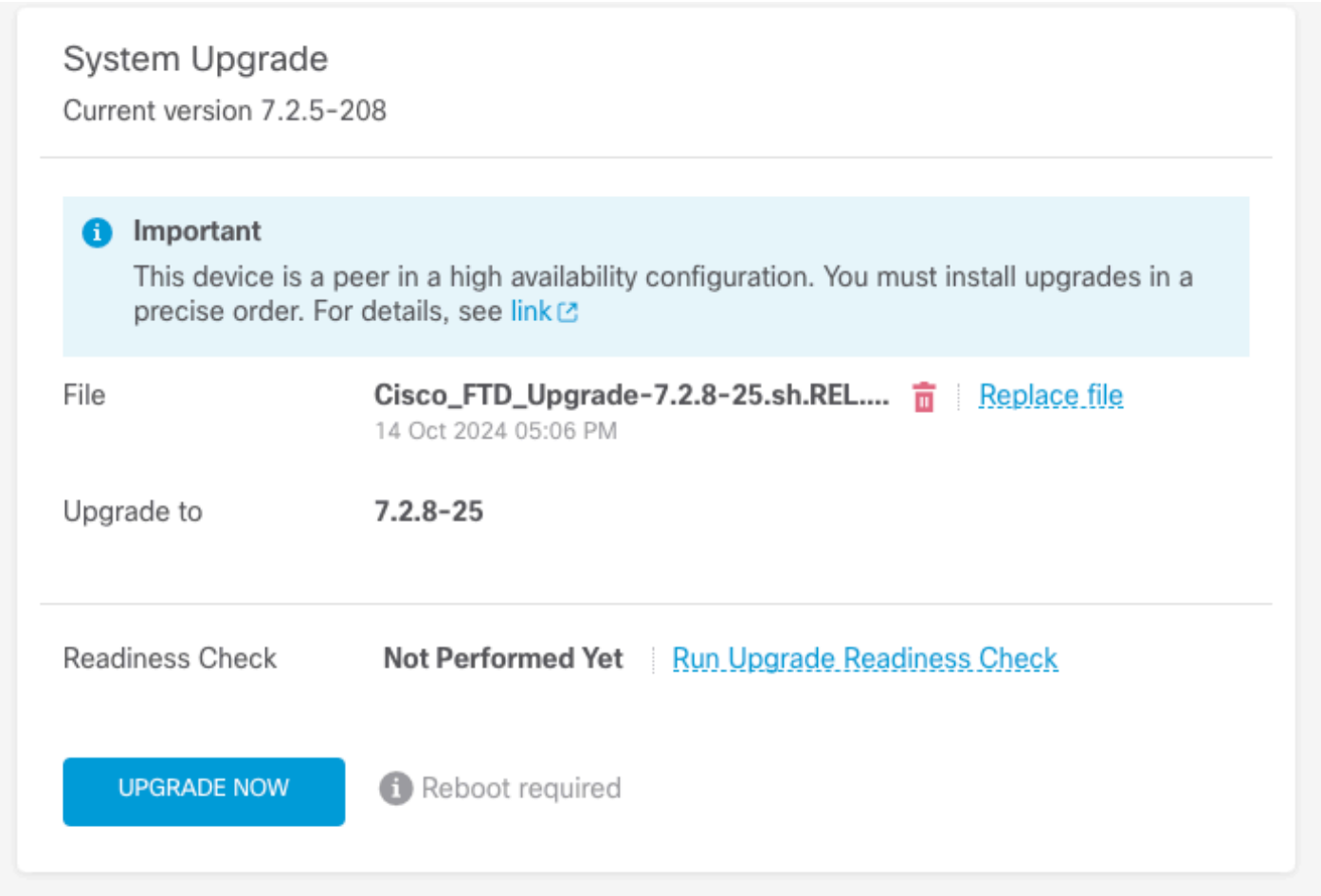
Exécuter la vérification du niveau de préparation

Vérifier le niveau de préparation

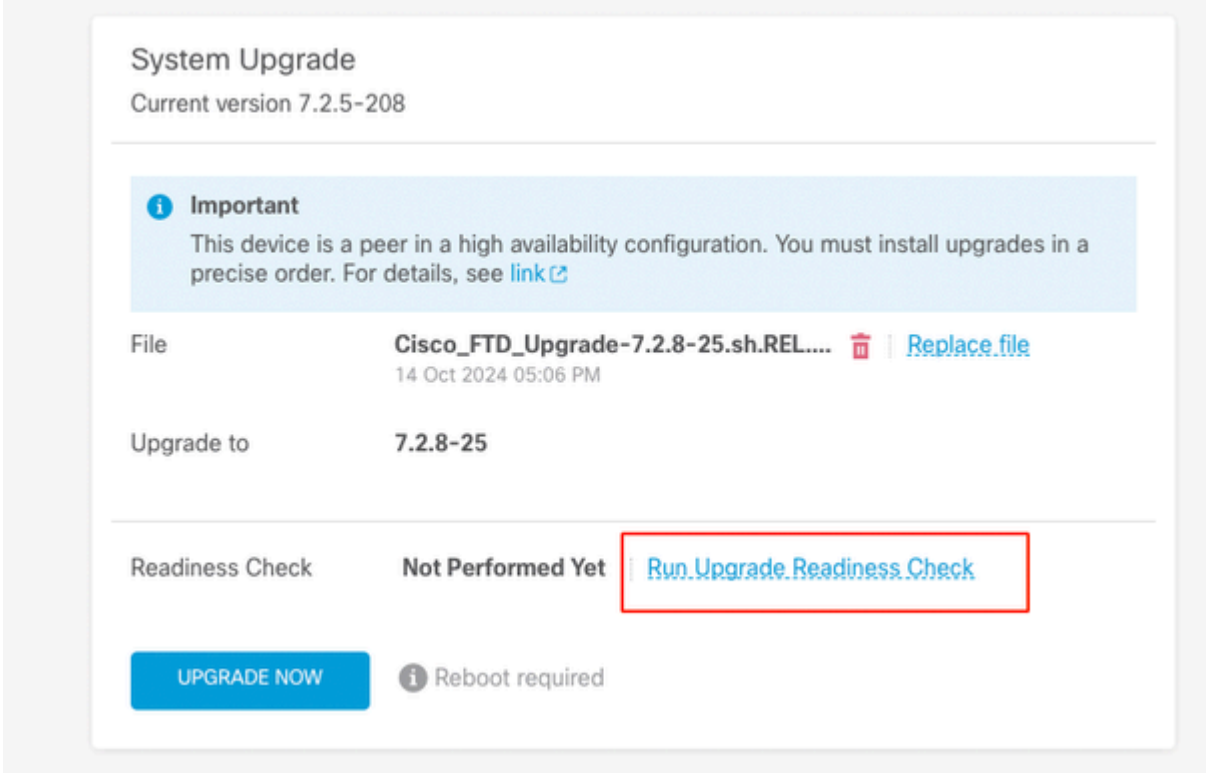
Les contrôles de préparation confirment que les appliances sont prêtes à poursuivre la mise à

niveau.

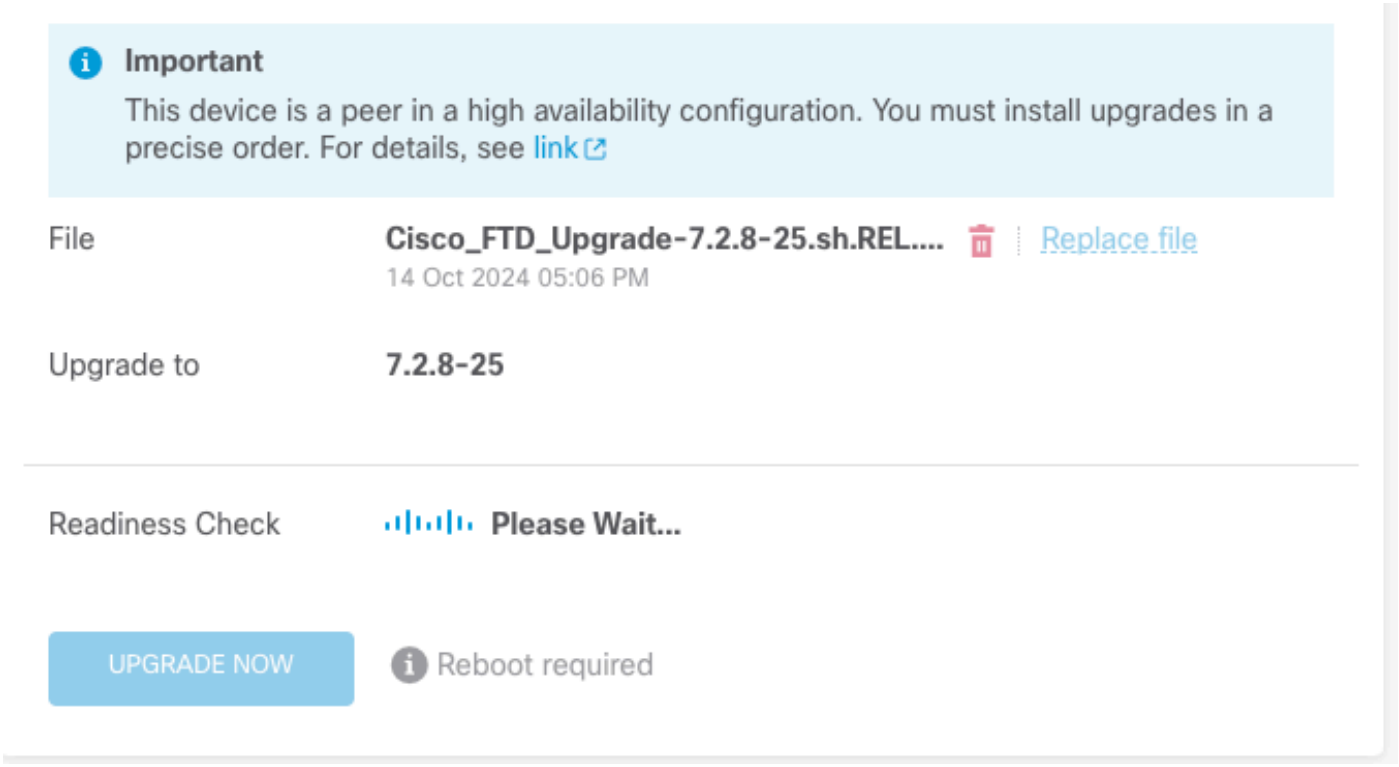
1. Sélectionnez Exécuter le contrôle de préparation à la mise à niveau.



Exécuter la vérification du niveau de préparation

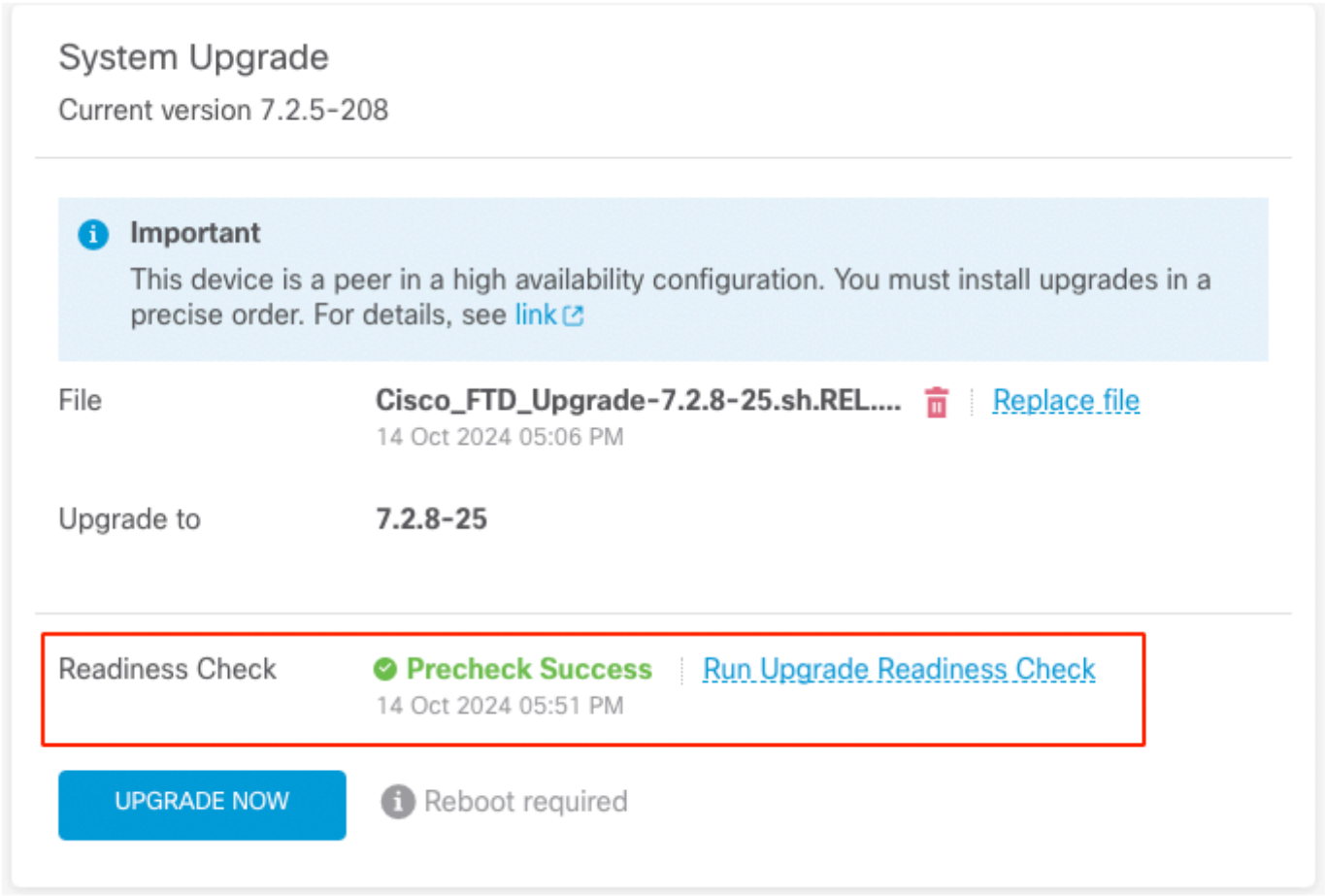


Exécuter le contrôle de préparation



Exécuter la vérification du niveau de préparation

2. Vous pouvez vérifier la progression en accédant à Système > Mise à niveau.

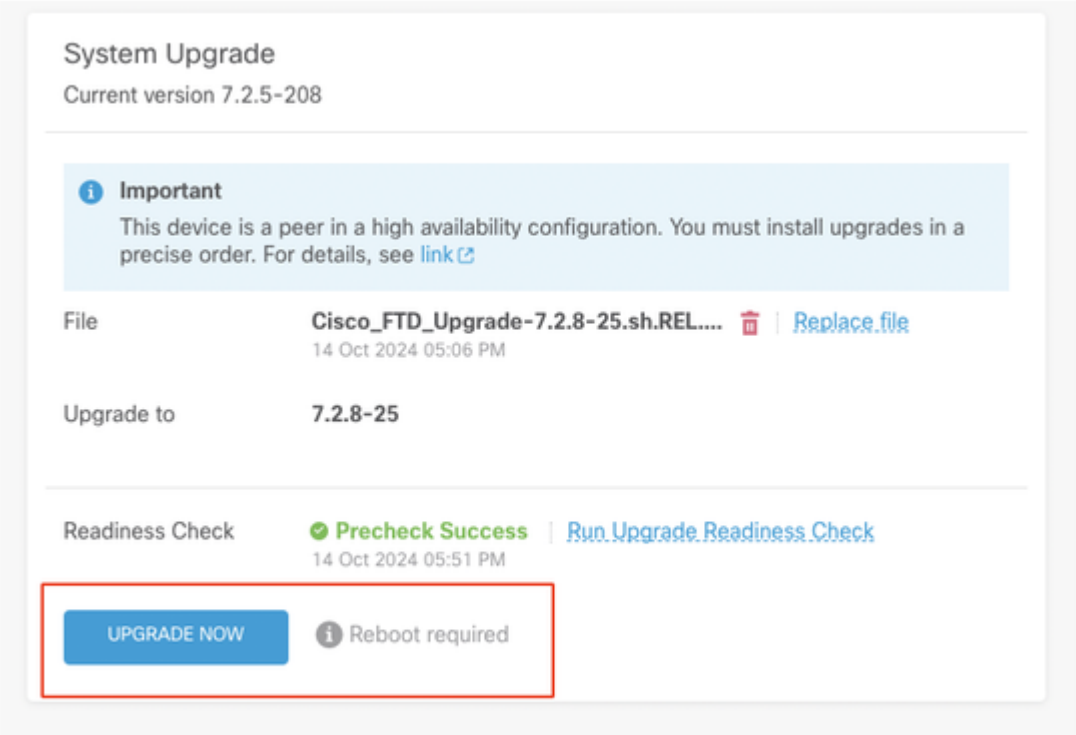


Exécuter la vérification du niveau de préparation

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

Mise à niveau FTD en haute disponibilité

1. Choisissez Standby FDM et cliquez sur Upgrade Now.

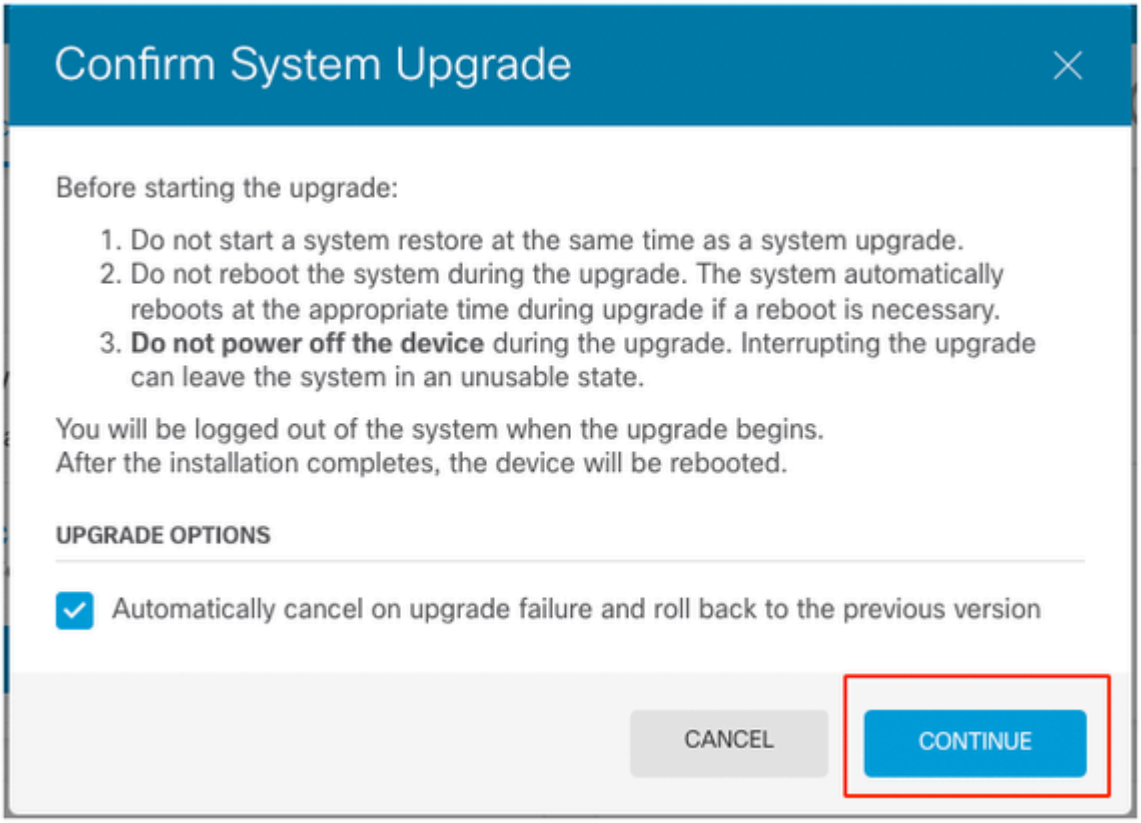


Mettre à niveau maintenant

2. Avant de commencer la mise à niveau :

- Ne démarrez pas une restauration du système en même temps qu'une mise à niveau du système.
- Ne redémarrez pas le système pendant la mise à niveau. Le système redémarre automatiquement au moment approprié pendant la mise à niveau, si un redémarrage est nécessaire.
- Ne mettez pas le périphérique hors tension pendant la mise à niveau. L'interruption de la mise à niveau peut rendre le système inutilisable.

3. Vous êtes déconnecté du système lorsque la mise à niveau commence.
4. Une fois l'installation terminée, le périphérique est redémarré.



Continuer

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

5. Sur CLI, la progression peut être vérifiée dans le dossier de mise à niveau /ngfw/var/log/sf ; passez en mode expert et entrez 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-7.2.8.



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

```
root@firepower:/ngfw/var/log/sf/Cisco_FTD_Upgrade-7.2.8# tail -f status.log
ui: Upgrade in progress: ( 8% done.22 mins to reboot). Preparing to upgrade... (200_pre/011_check_self.
ui: Upgrade in progress: ( 8% done.22 mins to reboot). Preparing to upgrade... (200_pre/015_verify_rpm.
ui: Upgrade in progress: ( 8% done.22 mins to reboot). Preparing to upgrade... (200_pre/100_check_dashb
ui: Upgrade in progress: ( 8% done.22 mins to reboot). Preparing to upgrade... (200_pre/100_get_snort_f
ui: Upgrade in progress: (12% done.21 mins to reboot). Preparing to upgrade... (200_pre/110_setup_upgra
ui: Upgrade in progress: (12% done.21 mins to reboot). Preparing to upgrade... (200_pre/120_generate_au
ui: Upgrade in progress: (12% done.21 mins to reboot). Preparing to upgrade... (200_pre/152_save_etc_sf

ui: Upgrade in progress: (79% done. 5 mins to reboot). Finishing the upgrade... (999_finish/999_zz_inst
ui: Upgrade in progress: (83% done. 4 mins to reboot). Finishing the upgrade... (999_finish/999_zzz_com
ui: Upgrade complete
ui: The system will now reboot.
ui: System will now reboot.

Broadcast message from root@firepower (Mon Oct 14 12:01:26 2024):
System will reboot in 5 seconds due to system upgrade.

Broadcast message from root@firepower (Mon Oct 14 12:01:31 2024):
System will reboot now due to system upgrade.

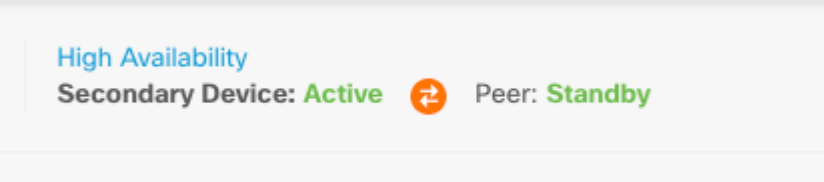
Broadcast message from root@firepower (Mon Oct 14 12:01:39 2024):
The system is going down for reboot NOW!
```

6. Mettez à niveau la deuxième unité.

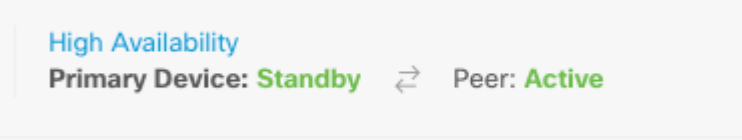
7. Changez de rôle afin de rendre ce périphérique actif : Choisissez Device > High Availability, puis choisissez Switch Mode dans le menu d'engrenages. Attendez que l'état de l'unité passe à

actif et vérifiez que le trafic circule normalement. Ensuite, déconnectez-vous.

8. Répétez les étapes précédentes afin de vous connecter à la nouvelle veille, de télécharger le package, de mettre à niveau le périphérique, de surveiller la progression et de vérifier la réussite.



Haute disponibilité



Haute disponibilité

9. 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.



primary_ha> enable

Password:

primary_ha# show failover state



               State          Last Failure Reason      Date/Time

This host  -   Primary

               Standby Ready  None

Other host -   Secondary

               Active         None
```

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

        Sync Skipped - STANDBY

====Communication State===

        Mac set


primary_ha#
```

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 pratique recommandée qui permet de suivre tout basculement pouvant survenir.

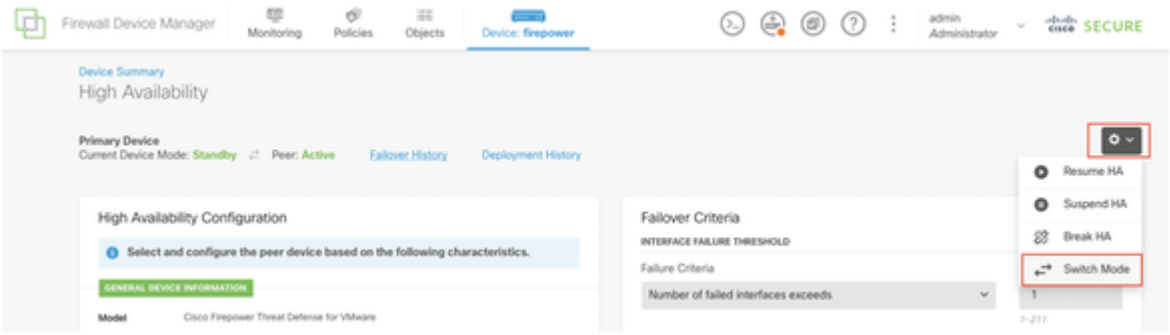
Dans ce cas, le FTD actif est maintenant en veille, un basculement manuel peut être utilisé pour le redéfinir sur Actif.

1. Accédez à Périphériques > Haute disponibilité.



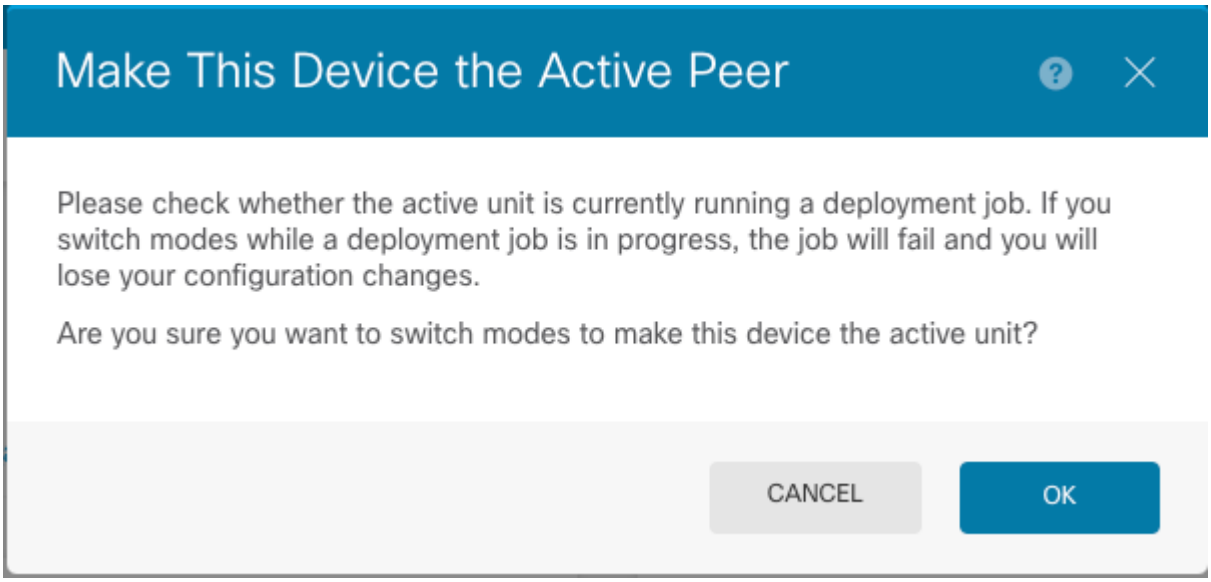
Haute disponibilité

2. Choisissez Switch Mode.



Mode de commutation

3. Cliquez sur OK afin de confirmer le basculement.



Homologue actif

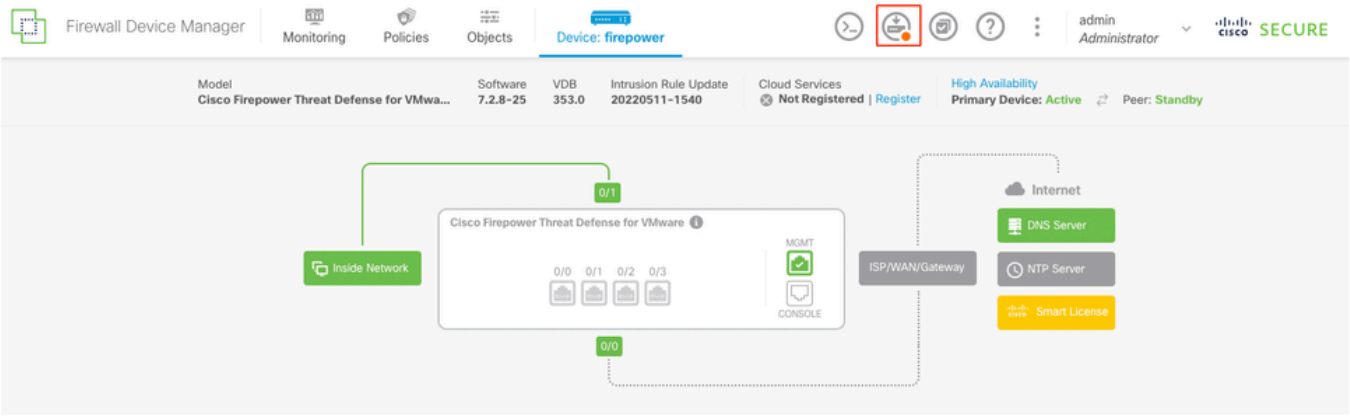
La validation de l'état de haute disponibilité à la fin de la mise à niveau et du basculement s'effectue comme indiqué :

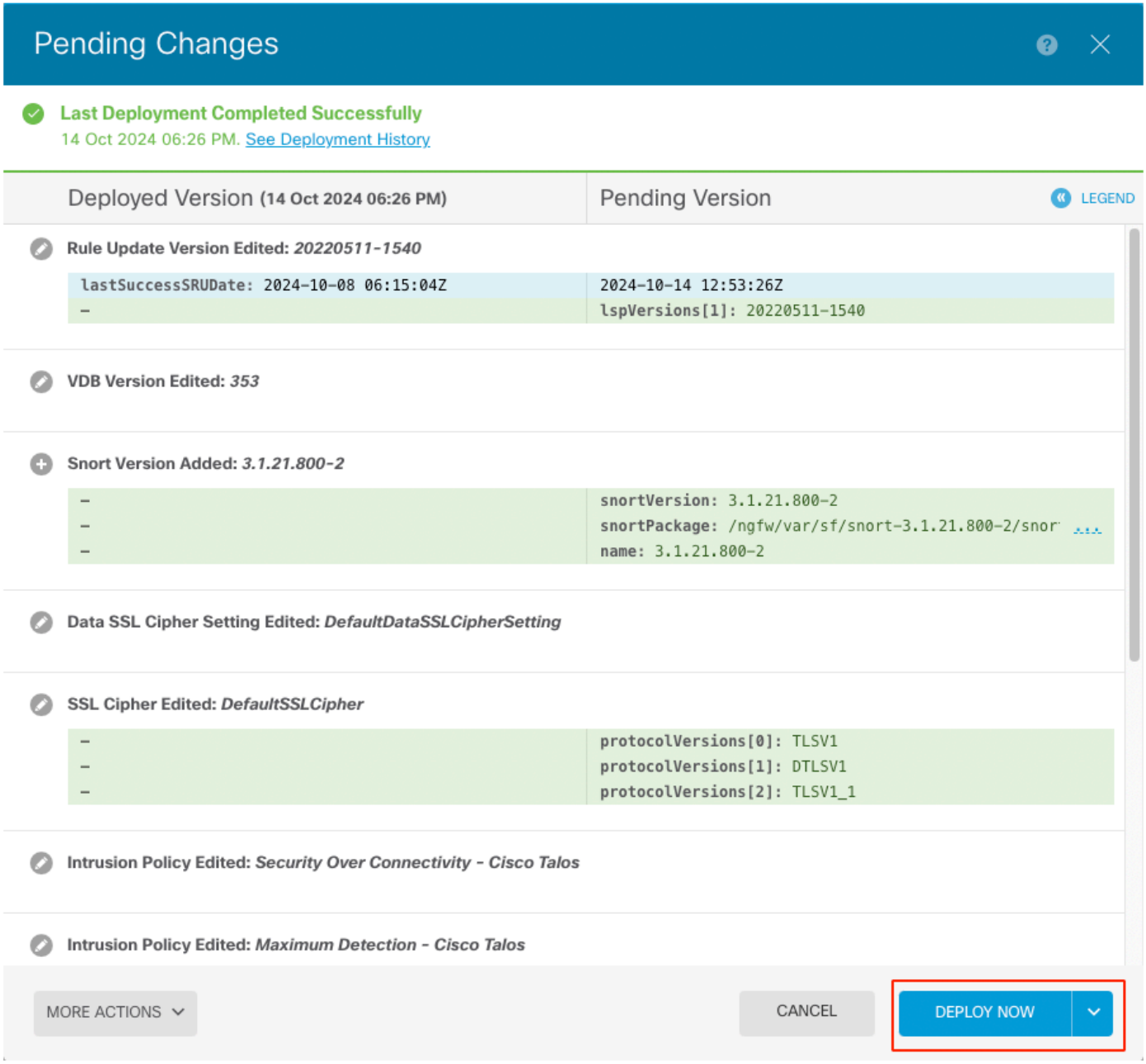


Périphériques

Déploiement final

Déployez la stratégie sur les périphériques en cliquant sur DEPLOY NOW sous l'onglet Deployment comme indiqué :





Déploiement des politiques

Valider

Afin de valider que l'état de haute disponibilité et la mise à niveau sont terminés, vous devez :

1. Confirmez le statut :
Principal : Actif
Secondaire : Veille prête

Les deux sont sous la version qui a été récemment modifiée (7.2.8 dans cet exemple) :



Basculement

2. Sur l'interférence CLI, vérifiez l'état de basculement à l'aide des commandes show failover state et show failover pour plus d'informations détaillées.

- Système d'exploitation extensible Cisco Firepower (FX-OS) v2.12.1 (build 73)
- Cisco Firepower Threat Defense pour VMware v7.2.8 (build 25)

```
> show failover state

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

====Configuration State===
        Sync Skipped
====Communication State===
        Mac set

> show failover
Failover On
Failover unit Primary
```

```
Failover LAN Interface: failover-link GigabitEthernet0/2 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 3 of 311 maximum
MAC Address Move Notification Interval not set
failover replication http
Version: Ours 9.18(4)210, Mate 9.18(4)210
Serial Number: Ours 9A1QUNFWPK1, Mate 9A45VNEHB5C
Last Failover at: 14:13:56 UTC Oct 15 2024
        This host: Primary - Active
                Active time: 580 (sec)
                slot 0: ASAv hw/sw rev (/9.18(4)210) status (Up Sys)
                  Interface diagnostic (0.0.0.0): Normal (Waiting)
                  Interface inside (192.168.45.1): Normal (Waiting)
                  Interface outside (192.168.1.10): Normal (Waiting)
                slot 1: snort rev (1.0)  status (up)
                slot 2: diskstatus rev (1.0)  status (up)
        Other host: Secondary - Standby Ready
                Active time: 91512 (sec)
                  Interface diagnostic (0.0.0.0): Normal (Waiting)
                  Interface inside (0.0.0.0): Normal (Waiting)
                  Interface outside (0.0.0.0): Normal (Waiting)
                slot 1: snort rev (1.0)  status (up)
                slot 2: diskstatus rev (1.0)  status (up)


Stateful Failover Logical Update Statistics
        Link : failover-link GigabitEthernet0/2 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         11797      0          76877      0
```

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

```
Logical Update Queue Information

                Cur     Max     Total

Recv Q:         0       31      123591

Xmit Q:         0       1       12100
```

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.