

Mise à niveau FTD HA gérée par FDM

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. Mise à niveau du 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 Firepower Device Manager.

Conditions préalables

Exigences

Cisco recommande de posséder des connaissances sur ces sujets :

- 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 l'interface CLI, exécutez la commande `show high-availability config` dans le FTD actif afin de vérifier l'état de la HA.

```
> 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)

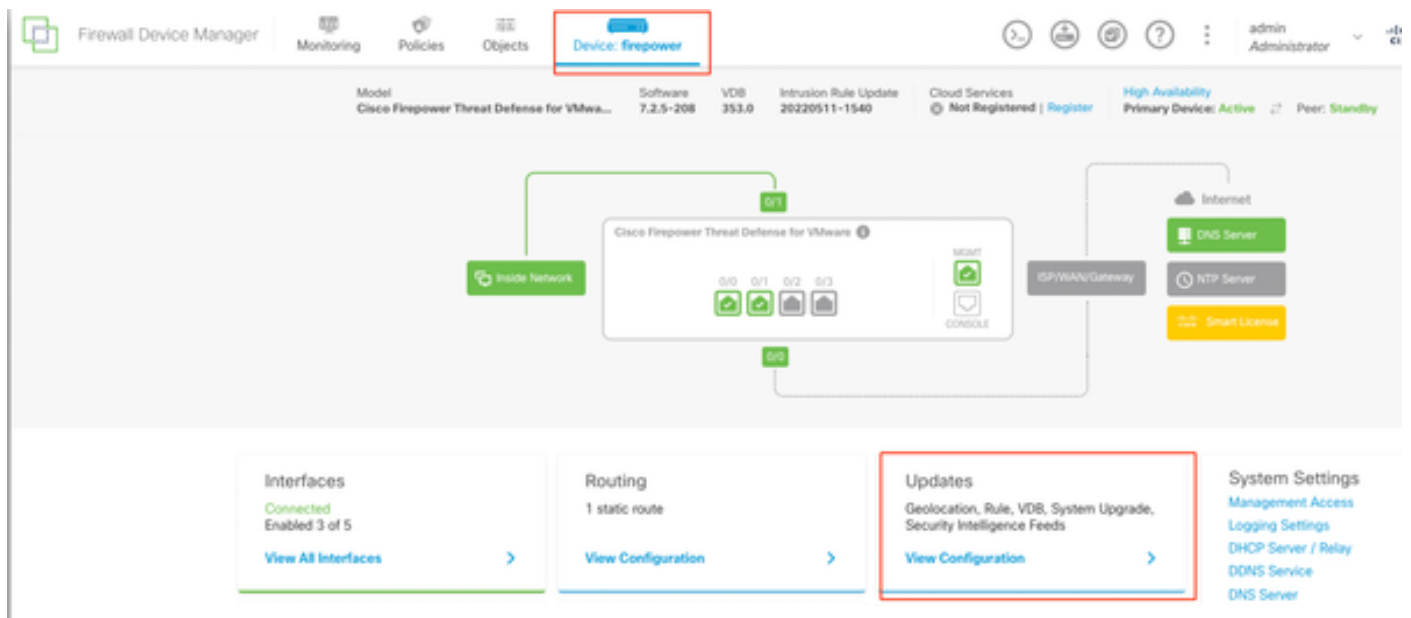
Si aucune erreur n'est visible, poursuivez la mise à niveau.

Configurer

Étape 1. Télécharger le package de mise à niveau

- 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

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



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

System Upgrade

Current version 7.2.5-208

i Important

This device is a peer in a high availability configuration. You must install upgrades in a precise order. For details, see [link](#)

There are no software upgrades available on the system.

Upload an upgrade file to install.

BROWSE

Exécuter la vérification du niveau de préparation

Étape 2. Vérifier le niveau de préparation

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


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

System Upgrade

Current version 7.2.5-208

i Important

This device is a peer in a high availability configuration. You must install upgrades in a precise order. For details, see [link](#)

File **Cisco_FTD_Upgrade-7.2.8-25.sh.REL....**  | [Replace file](#)
14 Oct 2024 05:06 PM

Upgrade to **7.2.8-25**

Readiness Check **Not Performed Yet** | [Run Upgrade Readiness Check](#)

UPGRADE NOW

i Reboot required

Exécuter la vérification du niveau de préparation

System Upgrade

Current version 7.2.5-208

i Important

This device is a peer in a high availability configuration. You must install upgrades in a precise order. For details, see [link](#)

File **Cisco_FTD_Upgrade-7.2.8-25.sh.REL....**  | [Replace file](#)
14 Oct 2024 05:06 PM

Upgrade to **7.2.8-25**


Readiness Check **Not Performed Yet** | [Run Upgrade Readiness Check](#)

UPGRADE NOW


i Reboot required

Exécuter le contrôle de préparation

i Important
This device is a peer in a high availability configuration. You must install upgrades in a precise order. For details, see [link](#)

File **Cisco_FTD_Upgrade-7.2.8-25.sh.REL....**  [Replace file](#)
14 Oct 2024 05:06 PM

Upgrade to **7.2.8-25**

Readiness Check  **Please Wait...**

UPGRADE NOW **i Reboot required**


Exécuter la vérification du niveau de préparation

Pour vérifier la progression, accédez à System > Upgrade.

System Upgrade

Current version 7.2.5-208

i Important
This device is a peer in a high availability configuration. You must install upgrades in a precise order. For details, see [link](#)

File **Cisco_FTD_Upgrade-7.2.8-25.sh.REL....**  [Replace file](#)
14 Oct 2024 05:06 PM

Upgrade to **7.2.8-25**

Readiness Check **✔ Precheck Success** [Run Upgrade Readiness Check](#)
14 Oct 2024 05:51 PM

UPGRADE NOW **i Reboot required**

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.

Étape 3. Mise à niveau du FTD en haute disponibilité

- Choisissez Standby FDM et cliquez sur Upgrade Now.

System Upgrade
Current version 7.2.5-208

Important
This device is a peer in a high availability configuration. You must install upgrades in a precise order. For details, see [link](#)

File: **Cisco_FTD_Upgrade-7.2.8-25.sh.REL....** | [Replace file](#)
14 Oct 2024 05:06 PM

Upgrade to: **7.2.8-25**

Readiness Check: **Precheck Success** | [Run Upgrade Readiness Check](#)
14 Oct 2024 05:51 PM

UPGRADE NOW | **Reboot required**

Mettre à niveau maintenant

Avant de commencer la mise à niveau :

1. Ne démarrez pas une restauration du système en même temps qu'une mise à niveau du système.
2. 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.
3. Ne mettez pas le périphérique hors tension pendant la mise à niveau. L'interruption de la mise à niveau peut rendre le système inutilisable.

Vous êtes déconnecté du système au début de la mise à niveau.
Une fois l'installation terminée, le périphérique est redémarré.

Confirm System Upgrade



Before starting the upgrade:

1. Do not start a system restore at the same time as a system upgrade.
2. Do not reboot the system during the upgrade. The system automatically reboots at the appropriate time during upgrade if a reboot is necessary.
3. **Do not power off the device** during the upgrade. Interrupting the upgrade can leave the system in an unusable state.

You will be logged out of the system when the upgrade begins.
After the installation completes, the device will be rebooted.

UPGRADE OPTIONS

- Automatically cancel on upgrade failure and roll back to the previous version

CANCEL

CONTINUE

Continuer



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 au mode expert et entrez en accès root.

```
> 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!
```

Mettez à niveau la deuxième unité.

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.

Mise à niveau: Répétez les étapes précédentes afin de vous connecter au nouveau périphérique de secours, de télécharger le package, de mettre à niveau le périphérique, de surveiller la progression et de vérifier la réussite.

High Availability

Secondary Device: **Active**  Peer: **Standby**

Haute disponibilité

High Availability

Primary Device: **Standby**  Peer: **Active**

Haute disponibilité

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#

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 pratique recommandée qui permet de suivre tout basculement pouvant survenir.

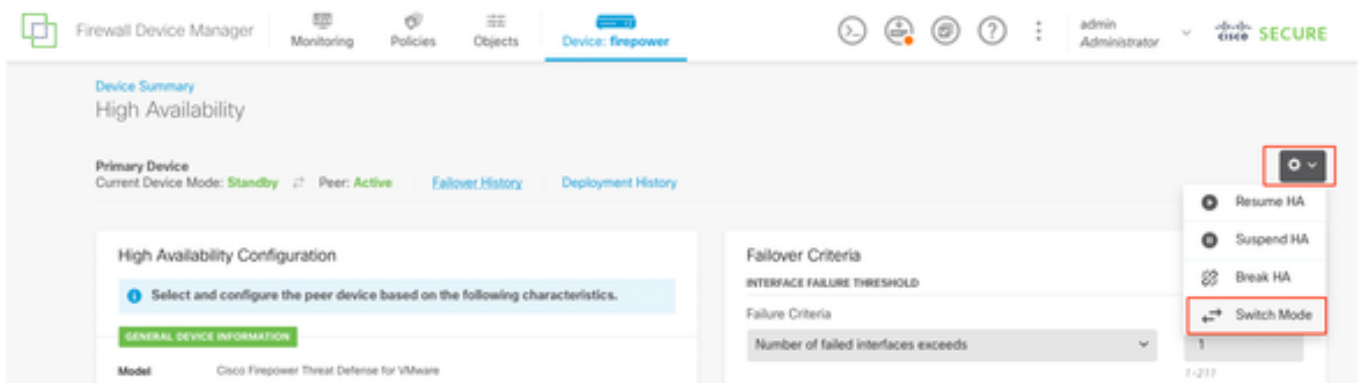
Dans ce cas, le FTD actif est maintenant en veille, un basculement manuel peut être utilisé pour le redéfinir sur Actif.

- Accédez à Périphériques > Haute disponibilité.



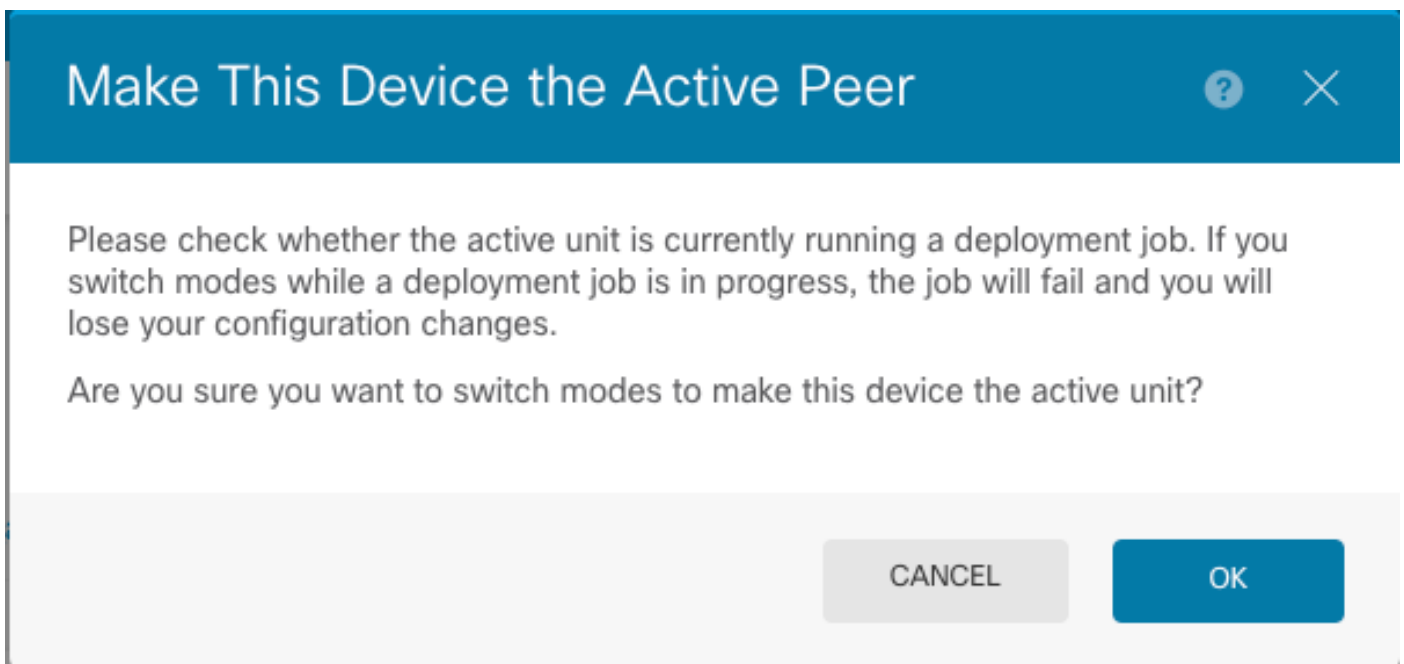
Haute disponibilité

- Sélectionnez Mode commutateur.



Mode de commutation

- Choisissez OK afin de confirmer le basculement.



Homologue actif

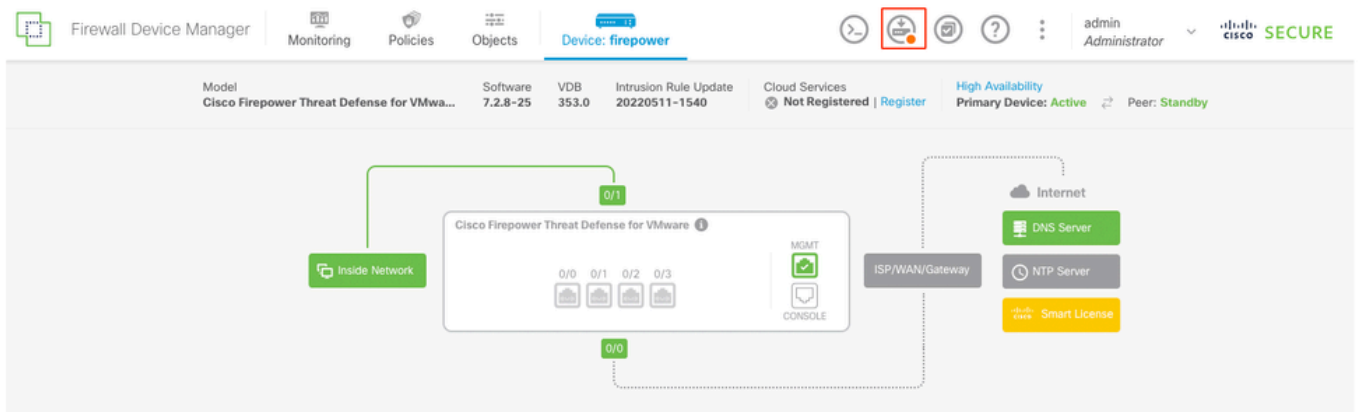
Validation de l'état de haute disponibilité à la fin de la mise à niveau et du basculement effectués.



Périphériques

Étape 5. Déploiement final

- Déployez la stratégie sur les périphériques en cliquant sur DEPLOY NOW sous l'onglet Deployment.



Pending Changes



✓ **Last Deployment Completed Successfully**
14 Oct 2024 06:26 PM. [See Deployment History](#)

Deployed Version (14 Oct 2024 06:26 PM)	Pending Version	LEGEND
Rule Update Version Edited: 20220511-1540		
<code>lastSuccessSRUDate: 2024-10-08 06:15:04Z</code>	<code>2024-10-14 12:53:26Z</code>	
<code>-</code>	<code>lspVersions[1]: 20220511-1540</code>	
VDB Version Edited: 353		
+ Snort Version Added: 3.1.21.800-2		
<code>-</code>	<code>snortVersion: 3.1.21.800-2</code>	
<code>-</code>	<code>snortPackage: /ngfw/var/sf/snort-3.1.21.800-2/snor...</code>	
<code>-</code>	<code>name: 3.1.21.800-2</code>	
Data SSL Cipher Setting Edited: DefaultDataSSLCipherSetting		
SSL Cipher Edited: DefaultSSLCipher		
<code>-</code>	<code>protocolVersions[0]: TLSV1</code>	
<code>-</code>	<code>protocolVersions[1]: DTLSV1</code>	
<code>-</code>	<code>protocolVersions[2]: TLSV1_1</code>	
Intrusion Policy Edited: Security Over Connectivity - Cisco Talos		
Intrusion Policy Edited: Maximum Detection - Cisco Talos		
MORE ACTIONS ▾	CANCEL	DEPLOY NOW ▾

Déploiement des politiques

Valider

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

Principal : Actif

Secondaire : Veille prête

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



Basculement

- Sur l'interférence CLI, vérifiez l'état de basculement en utilisant les 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.