Mise à niveau FTD HA via CLI gérée par FMC

Table des matières

Introduction

Ce document décrit une procédure détaillée pour mettre à niveau les périphériques Cisco Firepower Threat Defense (FTD) via l'interface de ligne de commande (CLI).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco Secure Firewall Management Center (FMC)
- Cisco Secure Firewall Threat Defense (FTD)

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco Secure Firewall Management Center v7.2.8

- Cisco Firepower Threat Defense pour VMWare v7.2.2

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.

Informations générales

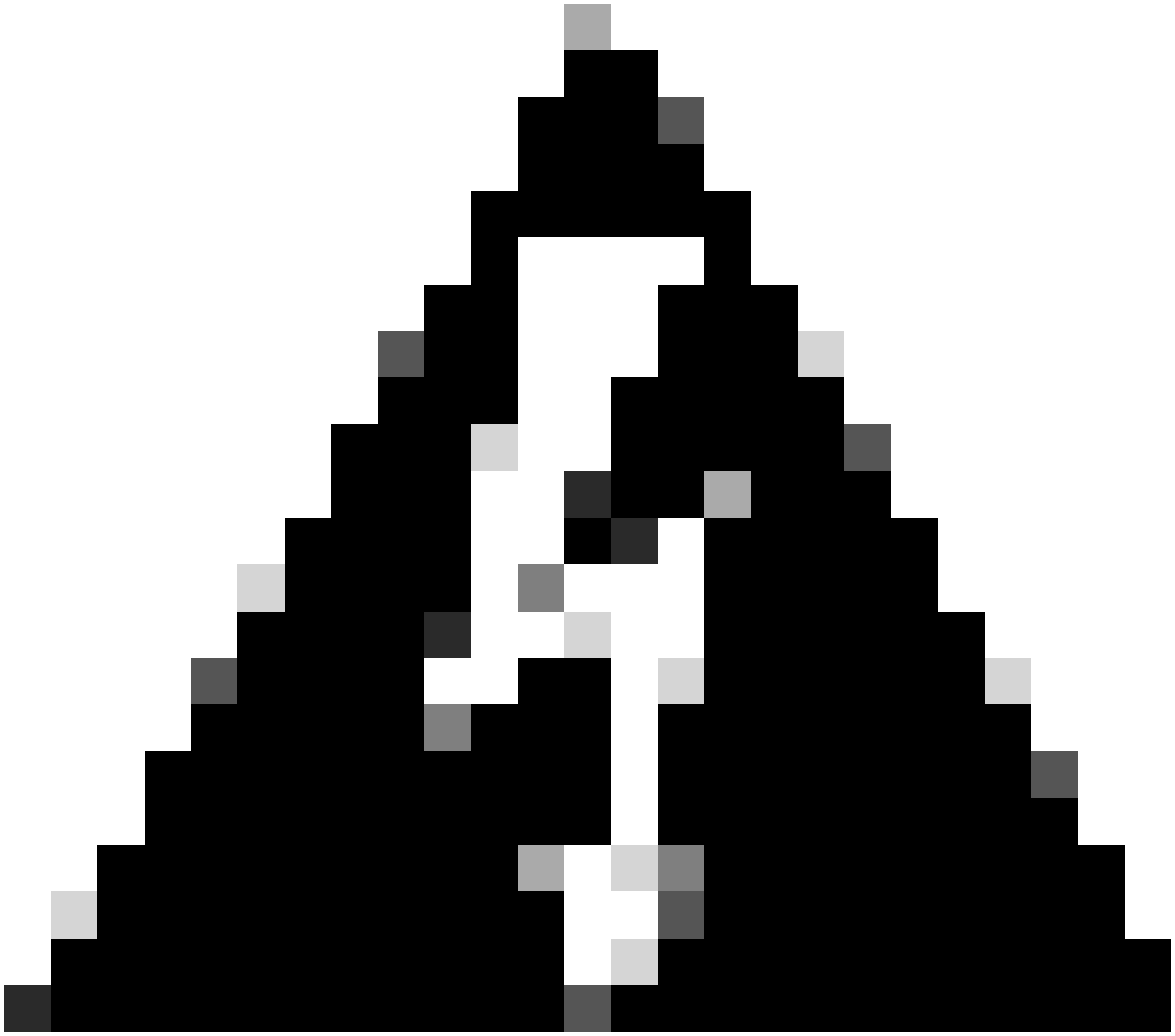
Les exigences spécifiques de ce document sont les suivantes :

- Cisco Secure Firewall Threat Defense version 7.2 ou ultérieure
- Cisco Secure Firewall Management Center version 7.2 ou ultérieure

Configurer

La mise à niveau d'une paire de périphériques FTD via l'interface de ligne de commande nécessite la présence du fichier de package de mise à niveau sur le périphérique. Il est essentiel de ne pas avoir de déploiements en attente comme condition préalable à une mise à niveau réussie via CLI.

Préparation de la mise à niveau



Avertissement : vérifiez l'ordre de mise à niveau, Standby / Active pour éviter toute interruption du trafic.

1. Commencez par le périphérique configuré en mode veille.

2. Accédez à l'interface de ligne de commande en mode expert en entrant expert suivi de sudo su en mode clish. Confirmez le mot de passe du périphérique pour élever les privilèges et passez en mode expert.

```
Copyright 2004-2022, Cisco and/or its affiliates. All rights reserved.
Cisco is a registered trademark of Cisco Systems, Inc.
All other trademarks are property of their respective owners.

Cisco Firepower Extensible Operating System (FX-OS) v2.12.0 (build 1104)
Cisco Firepower Threat Defense for VMware v7.2.2 (build 54)

> expert
admin@firepower:~$ sudo su

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

Password:
root@firepower:/home/admin#
root@firepower:/home/admin# cd
root@firepower:~#
root@firepower:~#
```

Vérifier l'état du basculement

Vérifiez l'état de basculement pour vous assurer que les étapes sont appliquées au FTD secondaire, qui peut être affiché comme Secondaire et Prêt pour la veille.

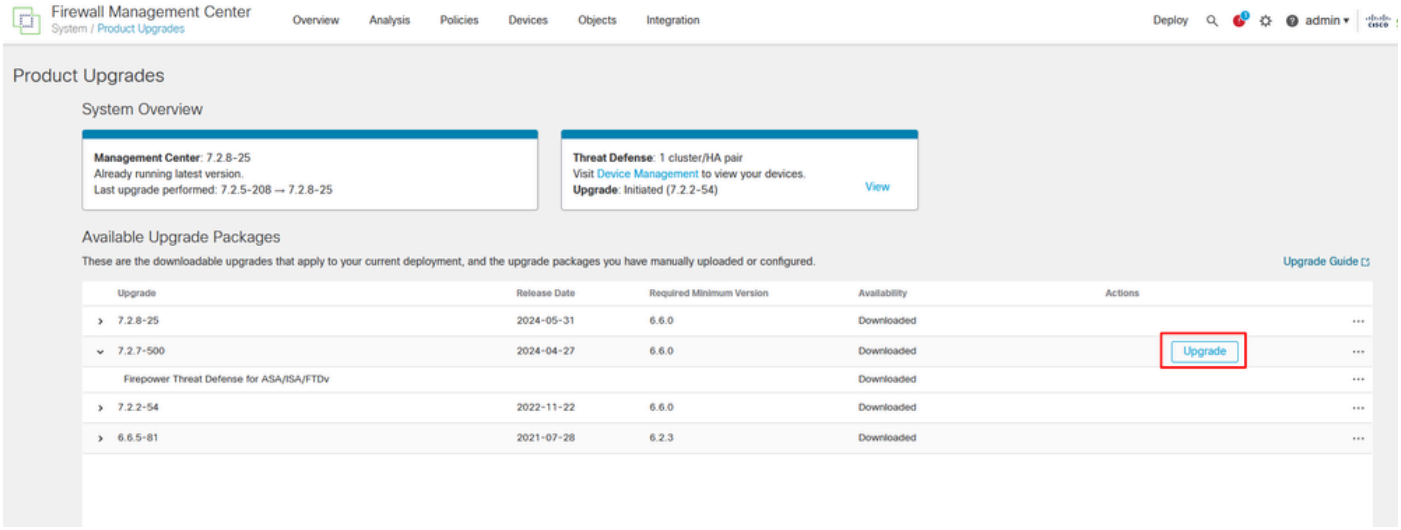
```
firepower#
firepower# sh failover state

               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#
firepower#
```

Télécharger le package de mise à niveau

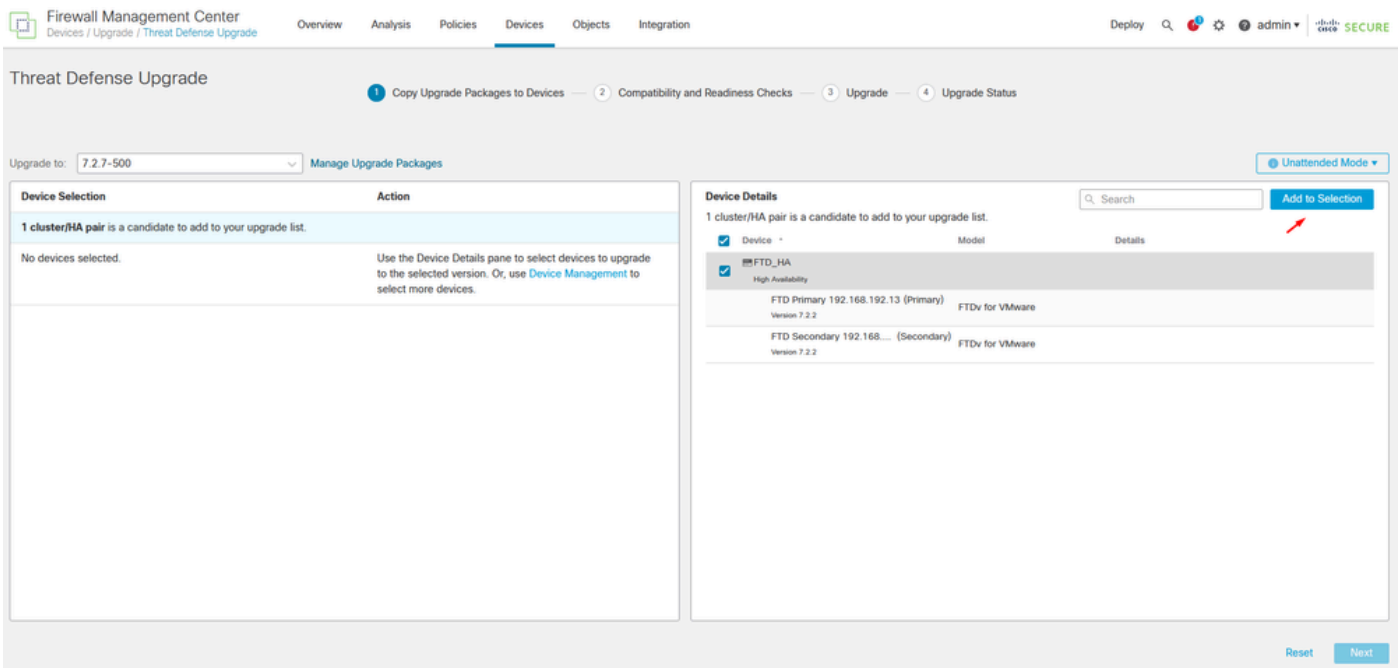
Téléchargez le package de mise à niveau vers les deux périphériques via le FMC en sélectionnant Settings > Updates > Product Updates > Upload local software update package. Sélectionnez le package précédemment téléchargé sur software.cisco.com et sélectionnez Upload.

Une fois que vous avez téléchargé le package Firepower sur le FMC, continuez avec le bouton Upgrade.



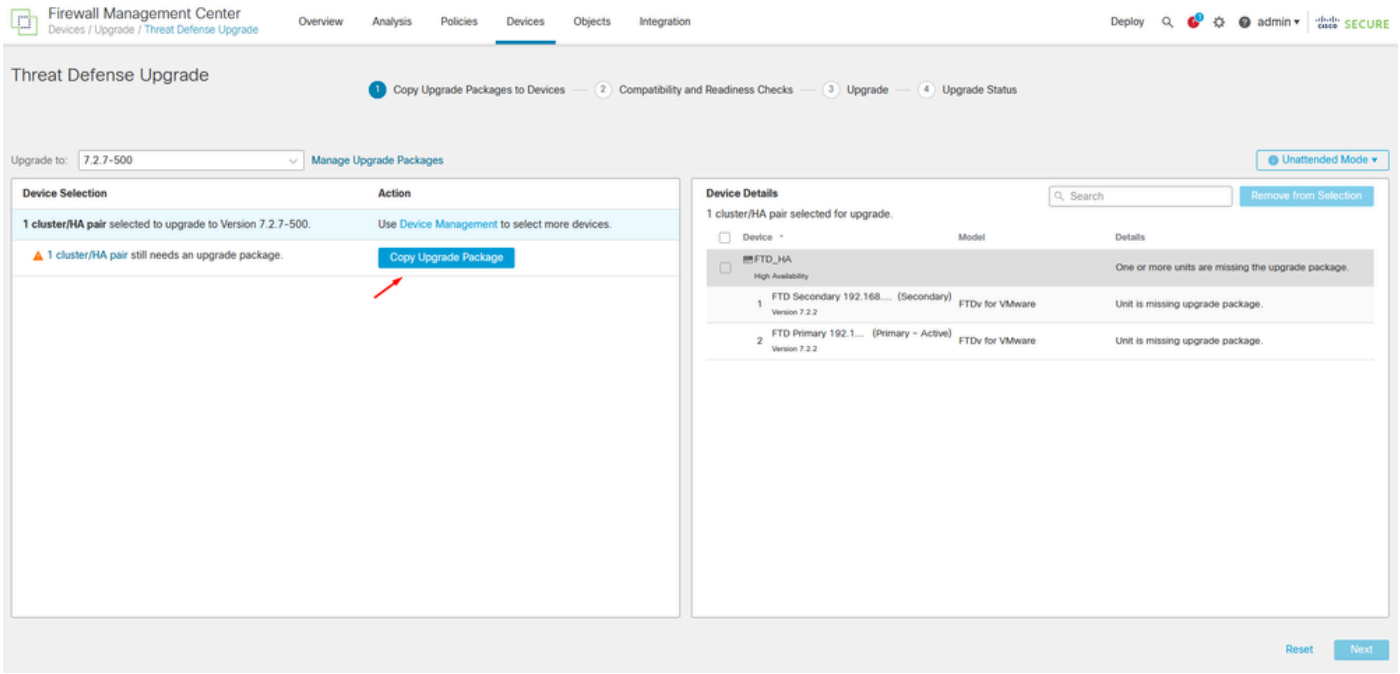
Bouton Upgrade

Dans l'assistant de mise à niveau, vous devez sélectionner les périphériques FTD HA, puis sélectionner les périphériques et cliquer sur Ajouter à la sélection.



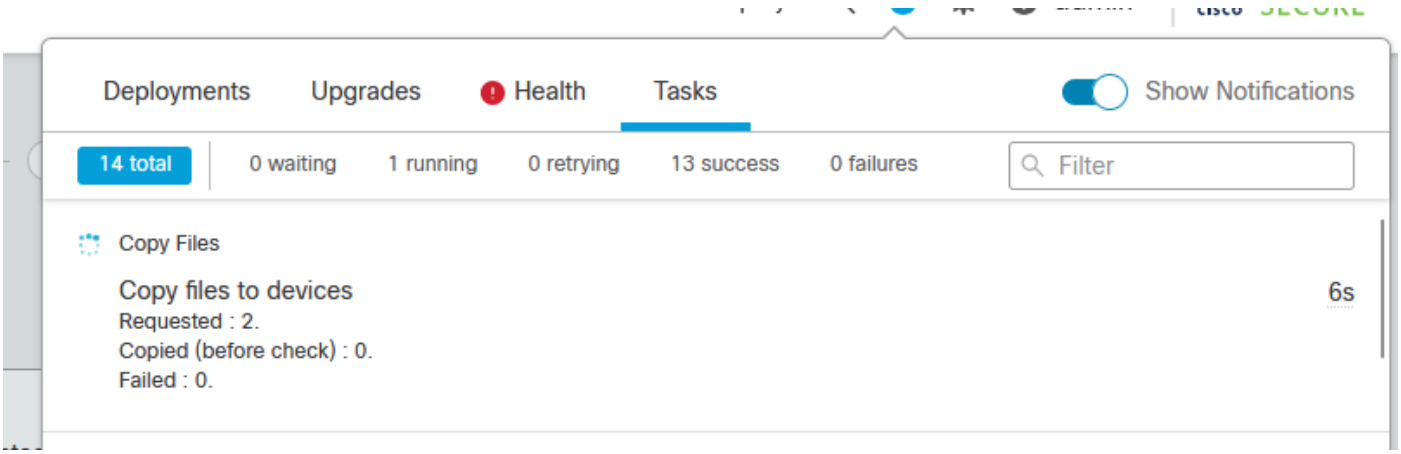
Ajouter à la sélection

Ensuite, vous pouvez copier le package de mise à niveau sur les périphériques, un message apparaît pour continuer les packages de mise à niveau.



Bouton Copier le package de mise à niveau

Dans la tâche Notification, vous pouvez trouver le travail de copie des fichiers sur le périphérique Une fois la tâche terminée, elle est terminée et a réussi.



Tâche Copie de fichiers vers des périphériques

Vous pouvez vérifier que le package est téléchargé vers les périphériques sur ce chemin :

```
root@firepower:/ngfw/var/sf/updates#
root@firepower:/ngfw/var/sf/updates# ls -l
total 2181772
-rw-r--r-- 1 root root 1110405120 Jul 18 01:08 Cisco_FTD_Upgrade-7.2.2-54.sh.REL.tar
-rw-r--r-- 1 root root        815 Jul 18 01:23 Cisco_FTD_Upgrade-7.2.2-54.sh.REL.tar.METADATA
-rw-r--r-- 1 root root 1123706880 Jul 18 02:36 Cisco_FTD_Upgrade-7.2.7-500.sh.REL.tar
-rw-r--r-- 1 root root        854 Jul 18 02:37 Cisco_FTD_Upgrade-7.2.7-500.sh.REL.tar.METADATA
```

```
root@firepower:/ngfw/var/sf/updates#
```

Vérification De L'État De Préparation

Exécutez la vérification de la préparation à partir de l'interface de ligne de commande sur le périphérique secondaire à l'aide de la commande suivante :

```
root@firepower:/ngfw/var/sf/updates# install_update.pl --detach --readiness-check /ngfw/var/sf/updates/
```

Voici un exemple :

```
root@firepower:/ngfw/var/sf/updates# install_update.pl --detach --readiness-check /ngfw/var/sf/updates/
ARGV[0] = --detach
ARGV[1] = --readiness-check
ARGV[2] = /ngfw/var/sf/updates/Cisco_FTD_Upgrade-7.2.7-500.sh.REL.tar
bundle_filepath: /ngfw/var/sf/updates/Cisco_FTD_Upgrade-7.2.7-500.sh.REL.tar
install_update.pl begins. bundle_filepath: /var/sf/updates/Cisco_FTD_Upgrade-7.2.7-500.sh.REL.tar
[Readiness-Info]filename : /var/sf/updates/Cisco_FTD_Upgrade-7.2.7-500.sh.REL.tar  at /usr/local/sf/lib
This was not run through the SF::System APIs at /usr/local/sf/lib/perl/5.24.4/SF/System/Wrappers.pm lin
Makeself GetUpdate Info params FILEPATH : /var/tmp/upgrade-patch/Cisco_FTD_Upgrade_Readiness-7.2.7-500.
FILEPATH directory name /var/tmp/upgrade-patch at /usr/local/sf/lib/perl/5.24.4/SF/Update/Makeself.pm l
Inside GetInfo FILEPATH :/var/tmp/upgrade-patch/Cisco_FTD_Upgrade_Readiness-7.2.7-500.sh at /usr/local/
root@firepower:/ngfw/var/sf/updates#
```

Surveillez le processus de vérification de la préparation selon le chemin suivant :

root@firepower:/ngfw/var/log/sf/Cisco_FTD_Upgrade-7.2.7/upgrade_readiness

```
root@firepower:/ngfw/var/log/sf/Cisco_FTD_Upgrade-7.2.7/upgrade_readiness# cat upgrade_readiness_status
TIMESTAMP:Thu Jul 18 02:43:05 UTC 2024 PERCENT: 0%  MESSAGE:Running script 000_start/000_00_run_cli_kic
TIMESTAMP:Thu Jul 18 02:43:05 UTC 2024 PERCENT: 5%  MESSAGE:Running script 000_start/000_check_platform
TIMESTAMP:Thu Jul 18 02:43:06 UTC 2024 PERCENT:10%  MESSAGE:Running script 000_start/100_start_messages
TIMESTAMP:Thu Jul 18 02:43:06 UTC 2024 PERCENT:14%  MESSAGE:Running script 000_start/101_run_pruning.pl
TIMESTAMP:Thu Jul 18 02:43:41 UTC 2024 PERCENT:19%  MESSAGE:Running script 000_start/105_check_model_nu
TIMESTAMP:Thu Jul 18 02:43:42 UTC 2024 PERCENT:24%  MESSAGE:Running script 000_start/106_check_HA_state
TIMESTAMP:Thu Jul 18 02:43:42 UTC 2024 PERCENT:29%  MESSAGE:Running script 000_start/107_version_check.
TIMESTAMP:Thu Jul 18 02:43:42 UTC 2024 PERCENT:33%  MESSAGE:Running script 000_start/108_clean_user_sta
TIMESTAMP:Thu Jul 18 02:43:43 UTC 2024 PERCENT:38%  MESSAGE:Running script 000_start/110_DB_integrity_c
TIMESTAMP:Thu Jul 18 02:43:47 UTC 2024 PERCENT:43%  MESSAGE:Running script 000_start/113_EO_integrity_c
TIMESTAMP:Thu Jul 18 02:43:50 UTC 2024 PERCENT:48%  MESSAGE:Running script 000_start/250_check_system_f
TIMESTAMP:Thu Jul 18 02:43:50 UTC 2024 PERCENT:52%  MESSAGE:Running script 000_start/410_check_disk_spa
TIMESTAMP:Thu Jul 18 02:43:55 UTC 2024 PERCENT:57%  MESSAGE:Running script 200_pre/001_check_reg.pl...
TIMESTAMP:Thu Jul 18 02:43:55 UTC 2024 PERCENT:62%  MESSAGE:Running script 200_pre/002_check_mounts.sh.
TIMESTAMP:Thu Jul 18 02:43:56 UTC 2024 PERCENT:67%  MESSAGE:Running script 200_pre/004_check_deploy_pac
TIMESTAMP:Thu Jul 18 02:43:56 UTC 2024 PERCENT:71%  MESSAGE:Running script 200_pre/005_check_manager.pl
TIMESTAMP:Thu Jul 18 02:43:56 UTC 2024 PERCENT:76%  MESSAGE:Running script 200_pre/006_check_snort.sh..
TIMESTAMP:Thu Jul 18 02:43:57 UTC 2024 PERCENT:81%  MESSAGE:Running script 200_pre/007_check_sru_instal
```

```
TIMESTAMP:Thu Jul 18 02:43:57 UTC 2024 PERCENT:86%  MESSAGE:Running script 200_pre/009_check_snort_prep
TIMESTAMP:Thu Jul 18 02:43:58 UTC 2024 PERCENT:90%  MESSAGE:Running script 200_pre/011_check_self.sh...
TIMESTAMP:Thu Jul 18 02:43:58 UTC 2024 PERCENT:95%  MESSAGE:Running script 200_pre/015_verify_rpm.sh...
TIMESTAMP:Thu Jul 18 02:44:00 UTC 2024 PERCENT:100%  MESSAGE:Readiness Check completed successfully.
root@firepower:/ngfw/var/log/sf/Cisco_FTD_Upgrade-7.2.7/upgrade_readiness#
```

Si la vérification de la préparation échoue, contactez le TAC Cisco.

Installation de mise à niveau

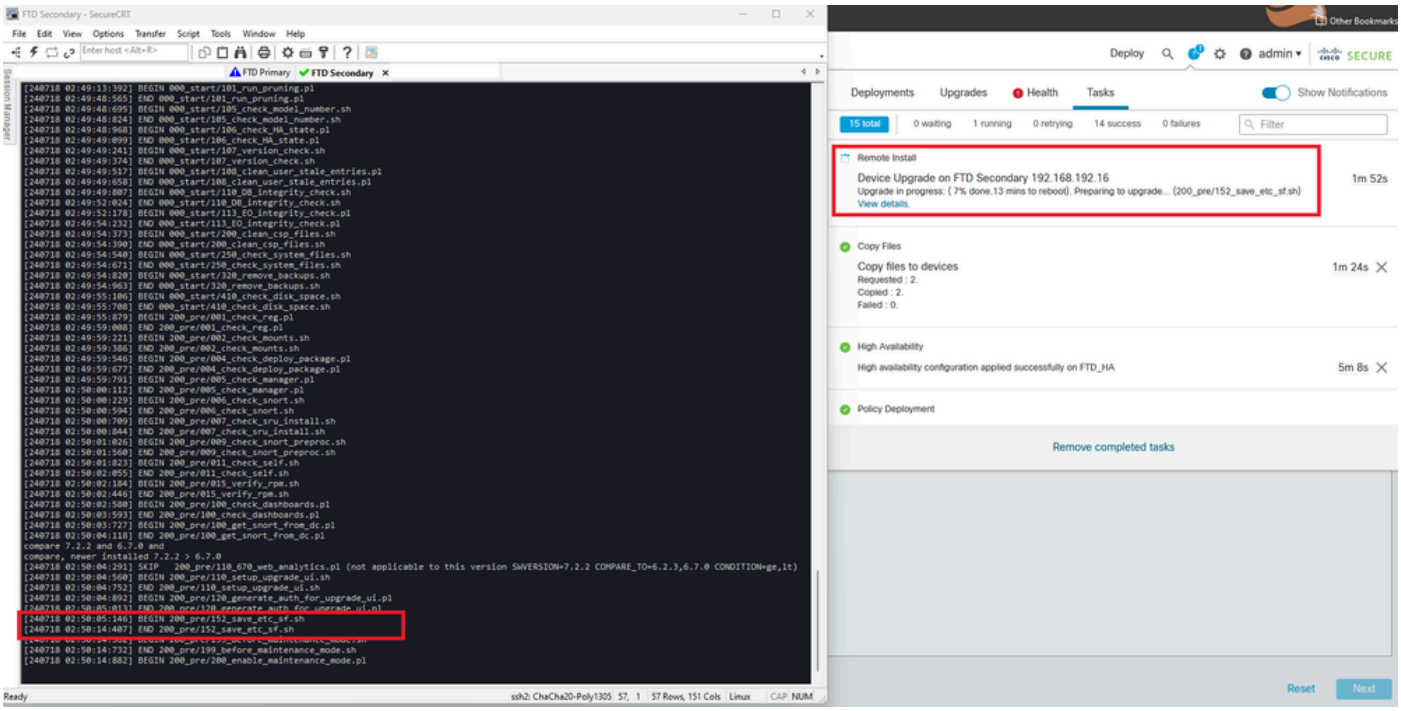
Poursuivez l'installation de la mise à niveau sur le FTD secondaire. Accédez au dossier contenant le fichier de mise à niveau et exécutez la commande d'installation :

```
root@firepower:/ngfw/var/sf/updates# install_update.pl --detach <FTD_Upgrade_Package.sh.REL.tar>
```

Une fois la mise à niveau exécutée, il y aura une sortie comme dans l'exemple suivant :

```
root@firepower:/ngfw/var/sf/updates# install_update.pl --detach Cisco_FTD_Upgrade-7.2.7-500.sh.REL.tar
ARGV[0] = Cisco_FTD_Upgrade-7.2.7-500.sh.REL.tar
bundle_filepath: Cisco_FTD_Upgrade-7.2.7-500.sh.REL.tar
updated absolute bundle_filepath: /ngfw/var/sf/updates/Cisco_FTD_Upgrade-7.2.7-500.sh.REL.tar
install_update.pl begins. bundle_filepath: /var/sf/updates/Cisco_FTD_Upgrade-7.2.7-500.sh.REL.tar
Makeself GetUpdate Info params FILEPATH : /var/tmp/upgrade-patch/Cisco_FTD_Upgrade-7.2.7-500.sh at /usr
FILEPATH directory name /var/tmp/upgrade-patch at /usr/local/sf/lib/perl/5.24.4/SF/Update/Makeself.pm l
Inside GetInfo FILEPATH :/var/tmp/upgrade-patch/Cisco_FTD_Upgrade-7.2.7-500.sh at /usr/local/sf/lib/per
Use of uninitialized value in string at /usr/local/sf/lib/perl/5.24.4/SF/Update/StatusProc.pm line 196.
Use of uninitialized value in string at /usr/local/sf/lib/perl/5.24.4/SF/Update/StatusProc.pm line 196.
Use of uninitialized value in string at /usr/local/sf/lib/perl/5.24.4/SF/Update/StatusProc.pm line 196.
Use of uninitialized value $in_container in string eq at /usr/local/sf/lib/perl/5.24.4/SF/Update/Status
Verifying archive integrity... All good.
Uncompressing Cisco FTD Upgrade / Sat Apr 27 04:09:29 UTC 2024.....................................
Entering is_fmc_managed
Device is FMC Managed
[240718 02:48:13:868] Found original ftd upgrade file /var/sf/updates/Cisco_FTD_Upgrade-7.2.7-500.sh.RE
[240718 02:48:16:990] MAIN_UPGRADE_SCRIPT_START
[240718 02:48:17:006] ########################################
[240718 02:48:17:007] # UPGRADE  STARTING
[240718 02:48:17:008] ########################################
compare 7.2.2 and 6.2.3 and
compare, newer installed 7.2.2 > 6.2.3
Entering create_upgrade_status_links...
Create upgrade_status.json and upgrade_status.log link in /ngfw/var/sf/sync/updates_status_logs
Running [ln -f /ngfw/var/log/sf/Cisco_FTD_Upgrade-7.2.7/upgrade_status.json /ngfw/var/sf/sync/updates_s
Link to JSON upgrade status file /ngfw/var/log/sf/Cisco_FTD_Upgrade-7.2.7/upgrade_status.json created i
Running [ln -f /ngfw/var/log/sf/Cisco_FTD_Upgrade-7.2.7/upgrade_status.log /ngfw/var/sf/sync/updates_st
Link to log upgrade status file /ngfw/var/log/sf/Cisco_FTD_Upgrade-7.2.7/upgrade_status.log created in
[240718 02:48:17:229] BEGIN 000_start/000_00_run_cli_kick_start.sh
[240718 02:48:18:421] END 000_start/000_00_run_cli_kick_start.sh
[240718 02:48:18:525] BEGIN 000_start/000_00_run_troubleshoot.sh
```

Sur le FMC, une tâche exécute la mise à niveau sur le périphérique secondaire :



Tâche exécutée sur FMC

Suivez l'état de la mise à niveau en suivant ce chemin :

```
root@firepower:/ngfw/var/log/sf/Cisco_FTD_Upgrade-X.X.X# tail -f upgrade_status.log
```

Voici un exemple de la sortie :

```
root@firepower:/ngfw/var/log/sf/Cisco_FTD_Upgrade-7.2.7# tail -f upgrade_status.log
TIMESTAMP:Thu Jul 18 02:50:25 UTC 2024 PERCENT:  7%  MESSAGE:Running script 200_pre/202_disable_syncd.sh
TIMESTAMP:Thu Jul 18 02:50:26 UTC 2024 PERCENT:  7%  MESSAGE:Running script 200_pre/400_restrict_rpc.sh.
TIMESTAMP:Thu Jul 18 02:50:26 UTC 2024 PERCENT:  7%  MESSAGE:Running script 200_pre/500_stop_system.sh..
TIMESTAMP:Thu Jul 18 02:50:53 UTC 2024 PERCENT:14%  MESSAGE:Running script 200_pre/501_recovery.sh... T
TIMESTAMP:Thu Jul 18 02:50:53 UTC 2024 PERCENT:14%  MESSAGE:Running script 200_pre/505_revert_prep.sh..
TIMESTAMP:Thu Jul 18 02:51:46 UTC 2024 PERCENT:14%  MESSAGE:Running script 200_pre/999_enable_sync.sh..
TIMESTAMP:Thu Jul 18 02:51:46 UTC 2024 PERCENT:14%  MESSAGE:Running script 300_os/001_verify_bundle.sh.
TIMESTAMP:Thu Jul 18 02:51:47 UTC 2024 PERCENT:14%  MESSAGE:Running script 300_os/002_set_auto_neg.pl..
TIMESTAMP:Thu Jul 18 02:51:47 UTC 2024 PERCENT:14%  MESSAGE:Running script 300_os/060_fix_fstab.sh... T
TIMESTAMP:Thu Jul 18 02:51:47 UTC 2024 PERCENT:14%  MESSAGE:Running script 300_os/100_install_Fire_Linu
```

Lorsque la mise à niveau sur le périphérique secondaire est terminée, le message suivant s'affiche :

```
240718 13:40:58:872] Attempting to remove upgrade lock
[240718 13:40:58:873] Success, removed upgrade lock
```

```
Upgrade lock /ngfw/tmp/upgrade.lock removed successfully.
[240718 13:40:58:882]
[240718 13:40:58:883] ############################################################
[240718 13:40:58:885] # UPGRADE  COMPLETE  #
[240718 13:40:58:887] ############################################################
Entering create_upgrade_status_links...
Create upgrade_status.json and upgrade_status.log link in /ngfw/Volume/root/ngfw/var/sf/sync/updates_st
Running [ln -f /ngfw/Volume/root/ngfw/var/log/sf/Cisco_FTD_Upgrade-7.2.7/upgrade_status.json /ngfw/Volu
Link to JSON upgrade status file /ngfw/Volume/root/ngfw/var/log/sf/Cisco_FTD_Upgrade-7.2.7/upgrade_stat
Running [ln -f /ngfw/Volume/root/ngfw/var/log/sf/Cisco_FTD_Upgrade-7.2.7/upgrade_status.log /ngfw/Volum
Link to log upgrade status file /ngfw/Volume/root/ngfw/var/log/sf/Cisco_FTD_Upgrade-7.2.7/upgrade_statu
Process 10677 exited.I am going away.
RC: 0
Update package reports success: almost finished...
Scheduling a reboot to occur in 5 seconds...
Process 12153 exited.I am going away.
root@firepower:/ngfw/var/sf/updates#
Broadcast message from root@firepower (Thu Jul 18 13:41:05 2024):

The system is going down for reboot NOW!
```

Une fois la mise à niveau du périphérique de secours terminée, le périphérique va être redémarré. Une fois les périphériques activés, vérifiez l'état de basculement pour vous assurer que tout reste comme configuré initialement.

Sur le FTD actif, vous pouvez trouver :

```
firepower# show failover state

               State          Last Failure Reason      Date/Time
This host  -   Primary
               Active         None
Other host -   Secondary
               Standby Ready  Comm Failure             13:24:46 UTC Jul 18 2024

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

firepower#
```

Sur Standby FTD, vous trouvez ceci :

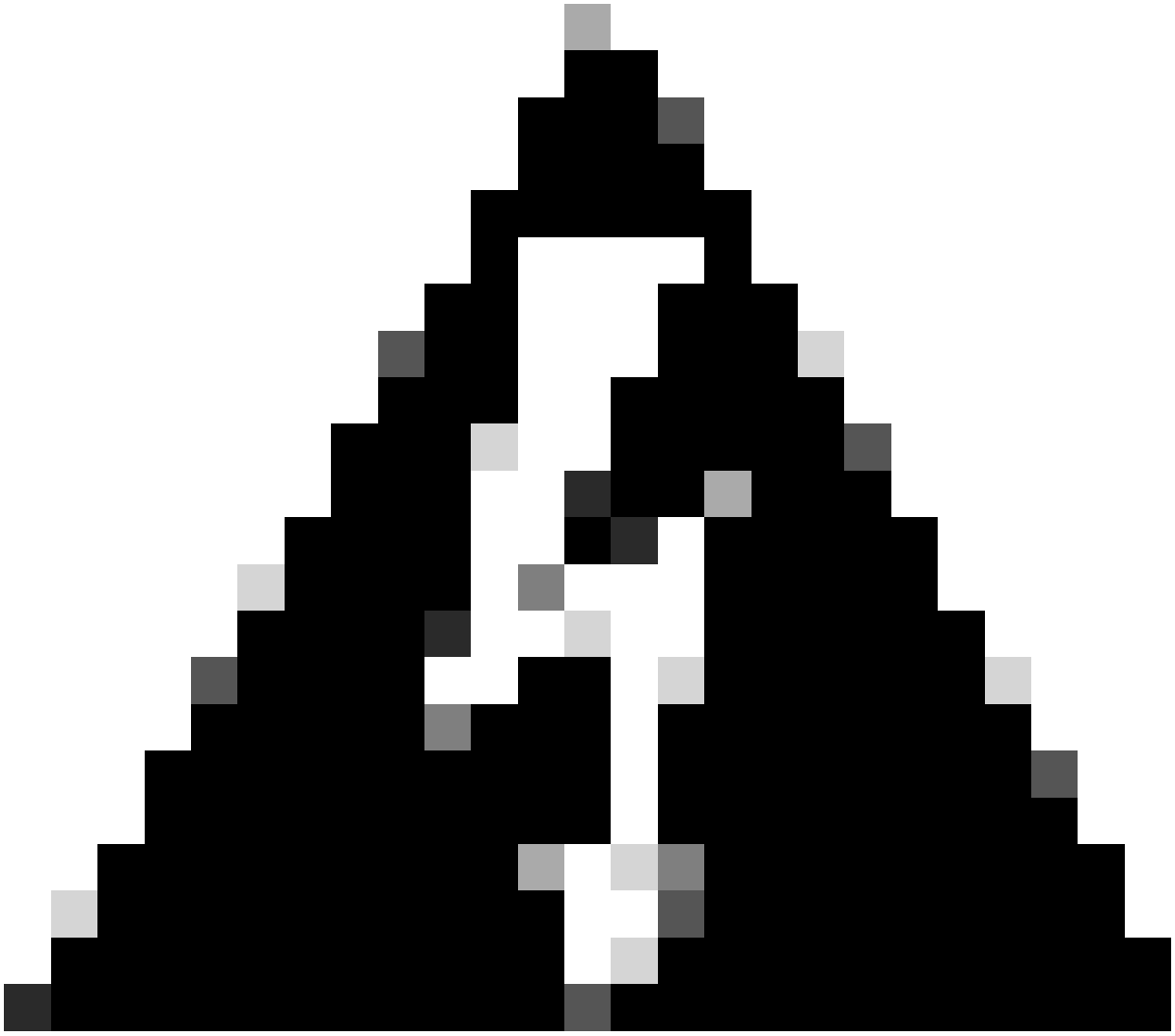
```
firepower#
firepower# sh failover state

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

```
====Configuration State===
        Sync Skipped - STANDBY
====Communication State===
        Mac set

firepower#
```

Il y aura un message indiquant que les versions ne sont pas identiques.

```
firepower#
*************WARNING****WARNING****WARNING*******************************
   Mate version 9.18(4)201 is not identical with ours 9.18(2)200
*************WARNING****WARNING****WARNING*******************************
```

Effectuez manuellement le basculement via l'interface de ligne de commande en utilisant la commande failover active sur le périphérique de secours. Le périphérique de secours devient alors actif.



Avertissement : à ce stade, le trafic est brièvement interrompu en cas de basculement.

```
firepower#
firepower# failover active

        Switching to Active
firepower#
firepower#
firepower# sh fail
firepower# sh failover state

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

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

```
firepower#
```

Une fois le basculement terminé, vous pouvez poursuivre la mise à niveau de l'autre périphérique. Suivez les mêmes étapes que celles décrites au début du document pour le périphérique qui était précédemment actif et qui est maintenant en veille.

Les deux périphériques sont désormais mis à niveau. Vous pouvez voir avec la commande show version sur le côté Lina. Pour le périphérique principal :

```
firepower#
firepower# 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

firepower#
```

Pour le périphérique secondaire :

```
firepower#
firepower# sh failover state

               State          Last Failure Reason      Date/Time
This host  -   Secondary
               Active         None
Other host -   Primary
               Standby Ready  Comm Failure             14:03:06 UTC Jul 18 2024

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

firepower#
```

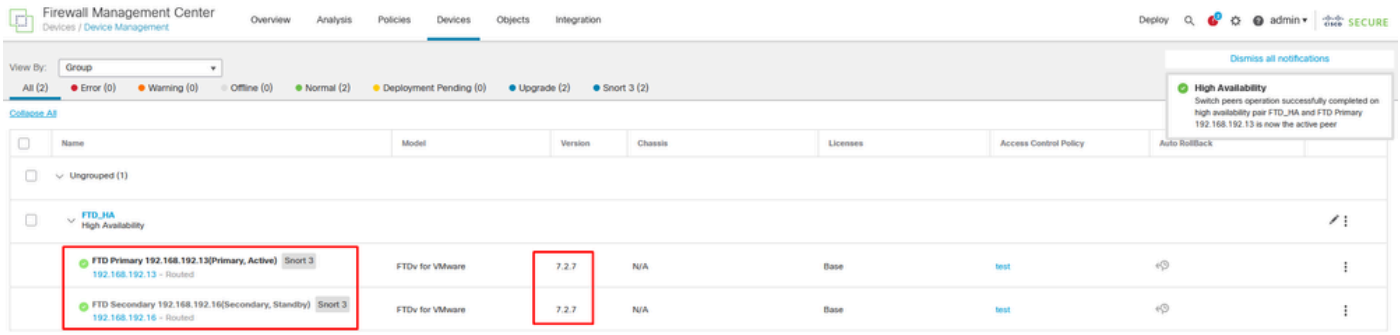
À ce stade, vous pouvez basculer les périphériques depuis FMC comme au début.

Vérifier

Après avoir réussi la mise à niveau des deux périphériques, vérifiez l'état dans le FMC et sur les deux FTD à l'aide de la commande show version.

```
firepower# show version
-------------------[ firepower ]--------------------
Model                     : Cisco Firepower Threat Defense for VMware (75) Version 7.2.7 (Build 500)
UUID                      : 0edf9f22-78e6-11ea-8ed0-e0e5abf334e2
LSP version               : lsp-rel-20240306-2015
VDB version               : 353
----------------------------------------------------
```

Sur le FMC, vous pouvez voir la mise à jour de version et êtes prêt à basculer comme vous l'aviez au début.



Homologues commutés de FMC

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.