Configurer la haute disponibilité FTD sur les appareils Firepower

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Tâche 1. Vérification des conditions

Tâche 2 : configuration de la haute disponibilité FTD

- Conditions

Tâche 3 : vérification de la haute disponibilité et de la licence FTD

Tâche 4. Changement des rôles de basculement

Tâche 5 : rupture de la paire haute disponibilité

Tâche 6. Suppression d'une paire haute disponibilité

Tâche 7. Suspension de la haute disponibilité

Foire aux questions (FAQ)

Informations connexes

Introduction

Ce document décrit comment configurer et vérifier la haute disponibilité (HA) de Firepower Threat Defense (FTD) sur les périphériques Firepower.

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

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

- 2 x Cisco Firepower 9300
- 2 x Cisco Firepower 4100 (7.2.8)
- Centre de gestion Firepower (FMC) (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.

Remarque : Sur un appareil FPR9300 avec FTD, vous pouvez configurer uniquement la haute disponibilité inter-châssis. Les deux unités d'une configuration haute disponibilité doivent remplir les conditions mentionnées ici.

Tâche 1. Vérification des conditions

Exigence de la tâche :

Vérifiez que les deux appareils FTD répondent aux exigences des notes et peuvent être configurés en tant qu'unités haute disponibilité.

Solution :

Étape 1 : connexion à l'adresse IP de gestion du FPR9300 et vérification du matériel du module

Vérifiez le matériel du FPR9300-1:

<#root>

```
KSEC-FPR9K-1-A#

show server inventory

Server Equipped PID Equipped VID Equipped Serial (SN) Slot Status      Ackd Memory (MB) Ackd Cores
------- ------------ ------------ -------------------- ---------------- ---------------- ----------
1/1     FPR9K-SM-36  V01          FLM19216KK6          Equipped                    262144         36
1/2     FPR9K-SM-36  V01          FLM19206H71          Equipped                    262144         36
1/3     FPR9K-SM-36  V01          FLM19206H7T          Equipped                    262144         36
KSEC-FPR9K-1-A#
```

Vérifiez le matériel du FPR9300-2:

<#root>

```
KSEC-FPR9K-2-A#

show server inventory

Server  Equipped PID Equipped VID Equipped Serial (SN) Slot Status      Ackd Memory (MB) Ackd Cores
------- ------------ ------------ -------------------- ---------------- ---------------- ----------
1/1     FPR9K-SM-36  V01          FLM19206H9T          Equipped                  262144         36
1/2     FPR9K-SM-36  V01          FLM19216KAX          Equipped                  262144         36
1/3     FPR9K-SM-36  V01          FLM19267A63          Equipped                  262144         36
KSEC-FPR9K-2-A#
```

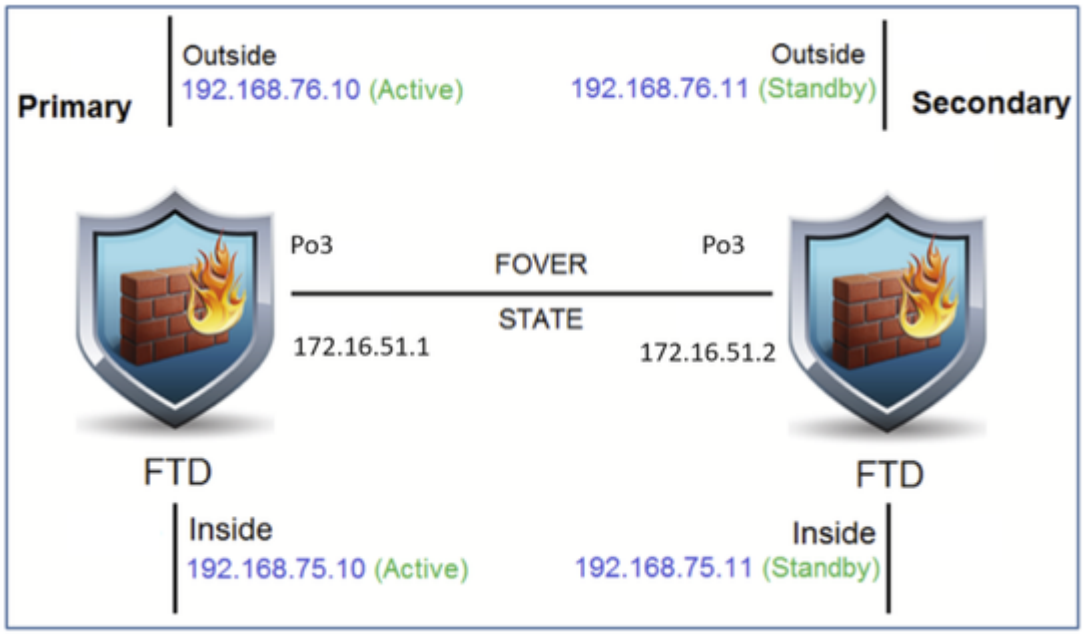
Étape 2. Connectez-vous au Gestionnaire de châssis FPR9300-1 et accédez à Logical Devices.

Étape 3 : vérification de la version du logiciel, du numéro et du type d'interface

Tâche 2 : configuration de la haute disponibilité FTD

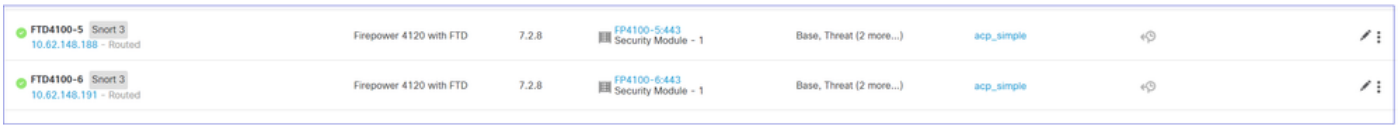
Exigence de la tâche :

Étape 1 : configuration du basculement actif/veille (HA) conformément au schéma Dans ce cas, une paire 41xx est utilisée.

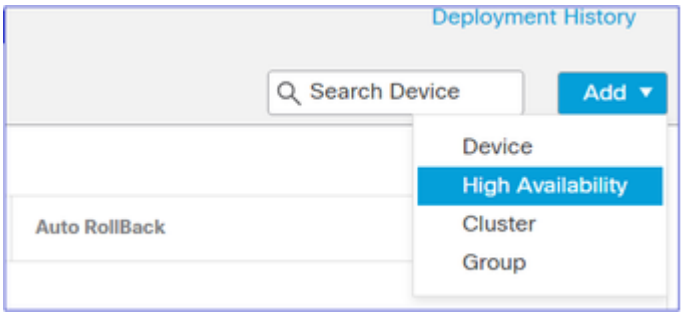


Solution

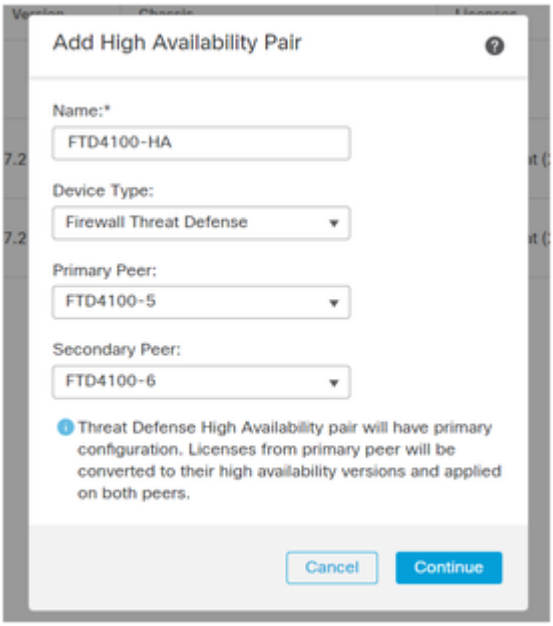
Les deux périphériques FTD sont enregistrés sur le FMC.



Étape 1. Pour configurer le basculement FTD, accédez à Périphériques > Gestion des périphériques et sélectionnez Ajouter une haute disponibilité.



Étape 2. Entrez l'homologue principal et l'homologue secondaire et cliquez sur Continuer.



Avertissement : Veillez à sélectionner l'unité appropriée comme unité principale. Toutes les configurations de l'unité principale sélectionnée sont répliquées sur l'unité FTD secondaire sélectionnée. Suite à la réplication, la configuration actuelle de l'unité secondaire peut être remplacée.

Conditions

Pour créer une haute disponibilité entre 2 périphériques FTD, les conditions suivantes doivent être remplies :

- Même modèle
- Même version, ceci s'applique à FXOS et à FTD - majeur (premier numéro), mineur (deuxième numéro) et maintenance (troisième numéro) doivent être égaux.
- Même nombre d'interfaces
- Même type d'interfaces
- Les deux périphériques font partie du même groupe/domaine dans FMC
- Disposent de configurations NTP (Network Time Protocol) identiques
- Doit être entièrement déployé sur le FMC sans modifications non validées
- Doit être dans le même mode de pare-feu : routé ou transparent

---



Remarque : Cela doit être vérifié à la fois sur les périphériques FTD et sur l'interface utilisateur graphique FMC, car il y a eu des cas où les FTD avaient le même mode, mais FMC ne reflète pas cela.

- Aucune interface n'est configurée avec le protocole DHCP/Point-to-Point Protocol over Ethernet (PPPoE).
- Nom d'hôte différent [nom de domaine complet (FQDN)] pour les deux châssis. Pour vérifier le nom d'hôte du châssis, accédez à FTD CLI et exécutez cette commande :

<#root>

```
firepower#

show chassis-management-url


https://

KSEC-FPR9K-1.cisco.com

:443//
```

 Remarque : Dans le FTD post 6.3, utilisez la commande show chassis detail.

<#root>

```
Firepower-module1#

show chassis detail



Chassis URL : https://FP4100-5:443//


Chassis IP : 10.62.148.187
Chassis IPv6 : ::
Chassis Serial Number : JAD19500BAB
Security Module : 1
```

Si les deux châssis portent le même nom, modifiez le nom en un avec cette commande :

<#root>

```
KSEC-FPR9K-1-A#

scope system

KSEC-FPR9K-1-A /system #

set name FPR9K-1new

Warning: System name modification changes FC zone name and redeploys them non-disruptively
KSEC-FPR9K-1-A /system* #

commit-buffer

FPR9K-1-A /system #

exit


FPR9K-1new-A

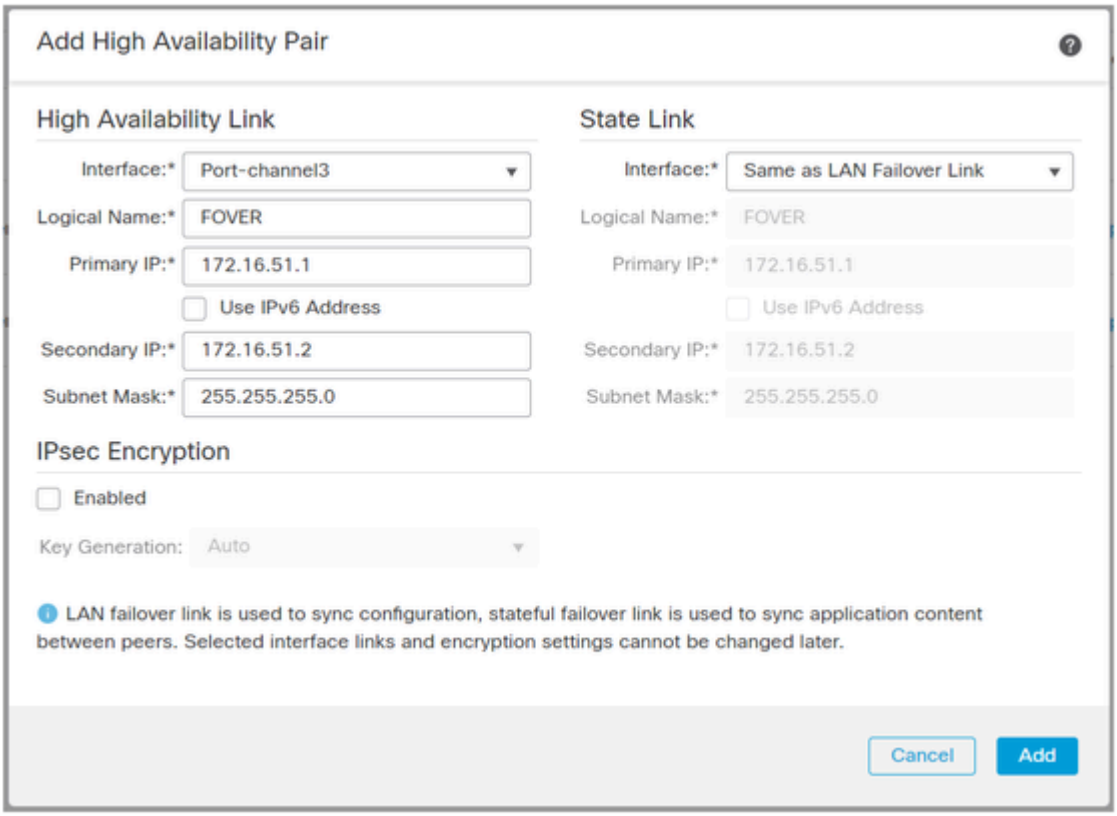
#
```

Après avoir modifié le nom du châssis, annulez l'enregistrement du FTD du FMC et enregistrez-le à nouveau. Procédez ensuite à la création de la paire à haute disponibilité.

Étape 3 : configuration de la haute disponibilité et définition des paramètres de liaison

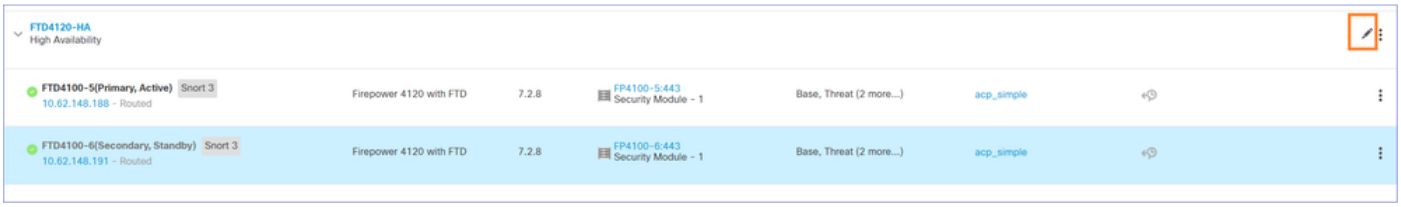
Dans ce cas, la liaison d'état possède les mêmes paramètres que la liaison de haute disponibilité.

Étape 4. Choisissez Add et attendez quelques minutes que la paire haute disponibilité soit déployée.

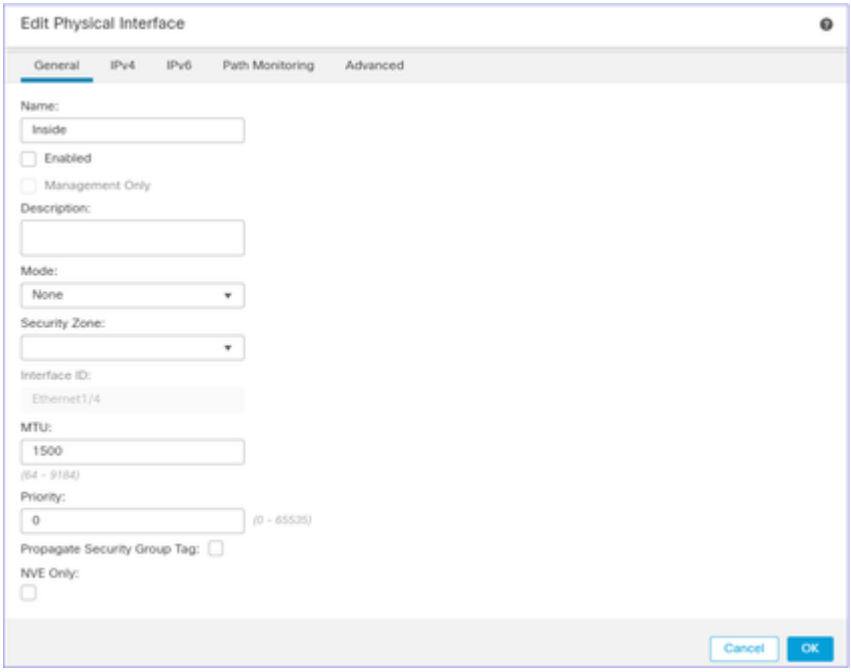


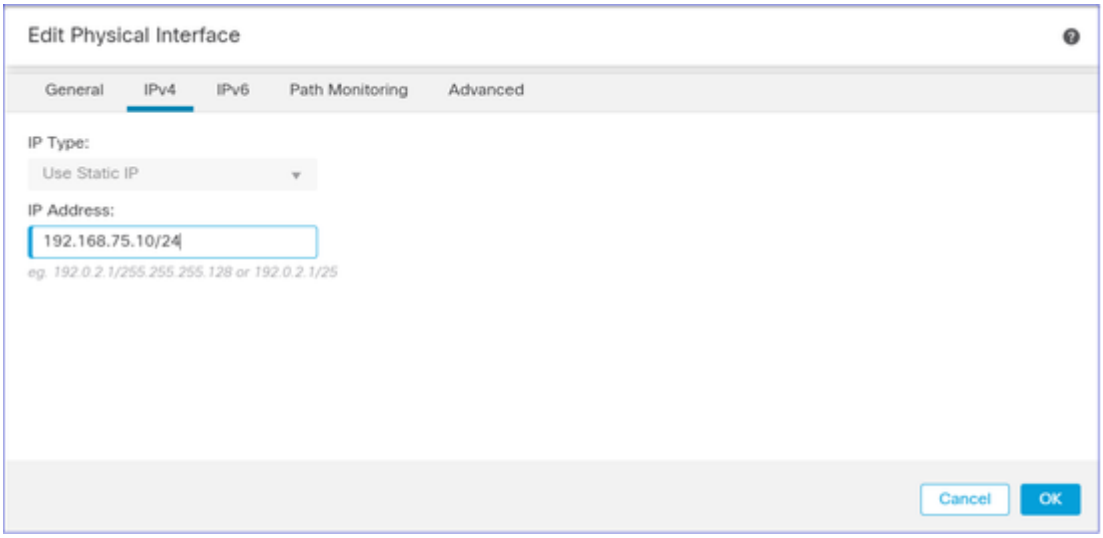
Étape 5 : configuration des interfaces de données (adresses IP principales et de secours)

Étape 6. Dans l'interface utilisateur graphique de FMC, sélectionnez HA Edit.

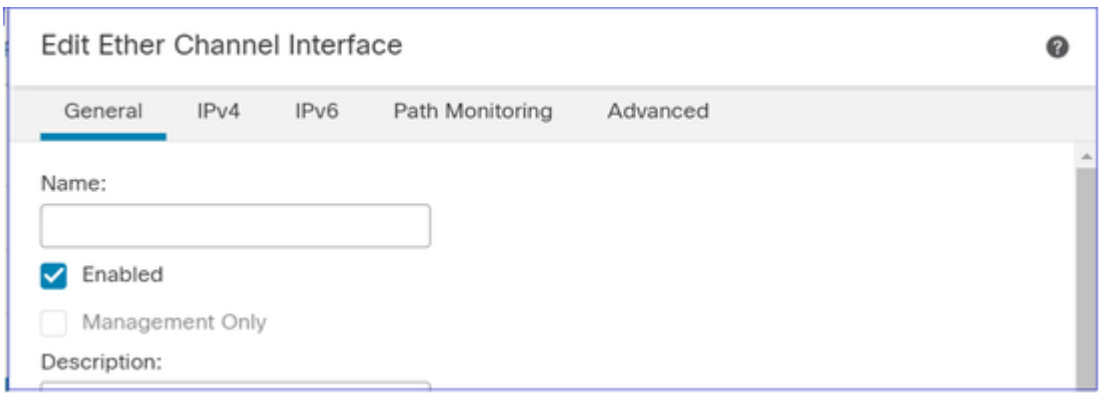


Étape 7. Configuration des paramètres d'interface :

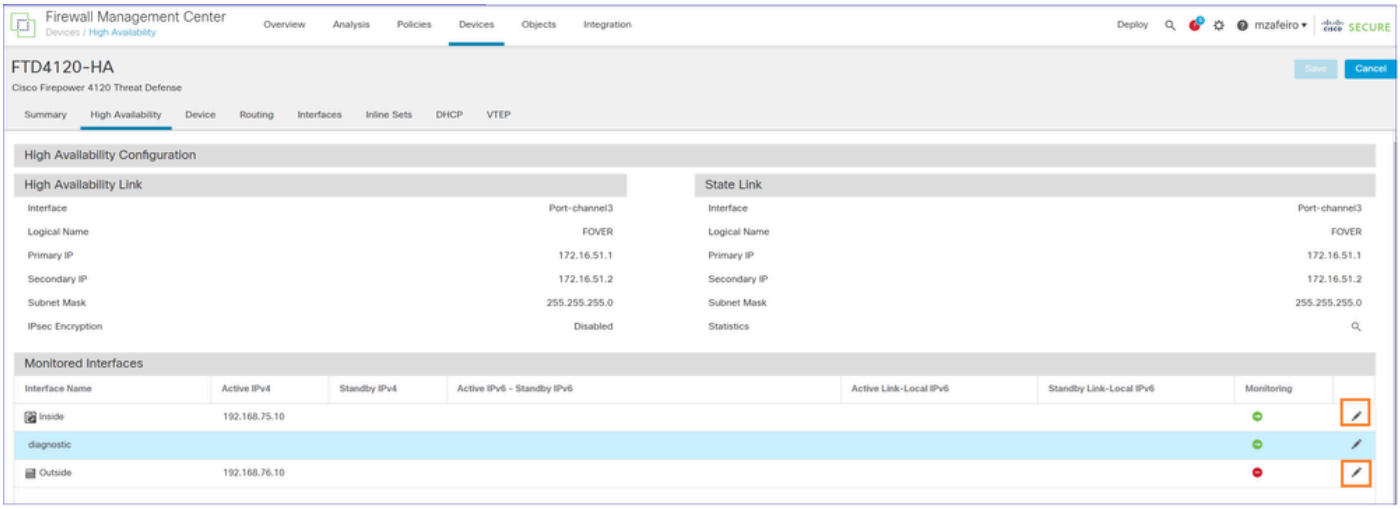


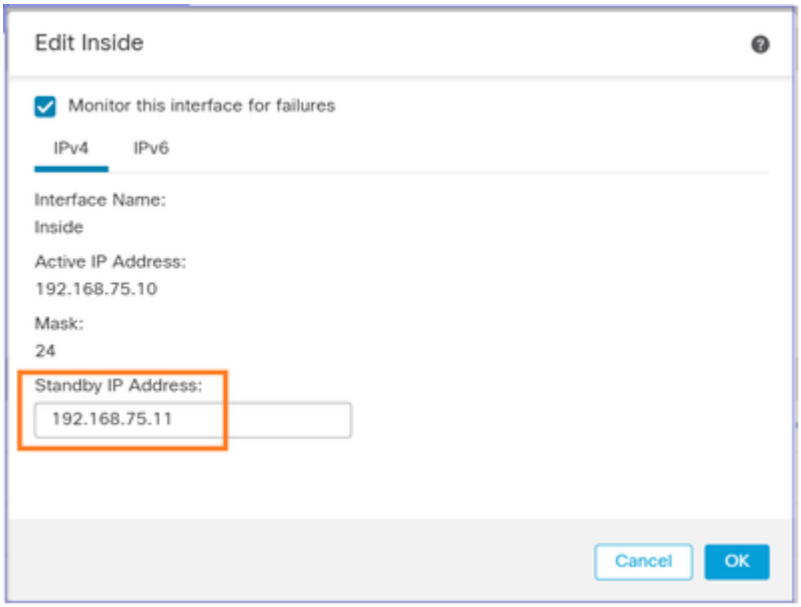


Dans le cas d'une sous-interface, vous devez activer l'interface parent :



Étape 8. Accédez à High Availability et choisissez le nom de l’interface, cliquez sur Edit pour ajouter les adresses IP de secours.



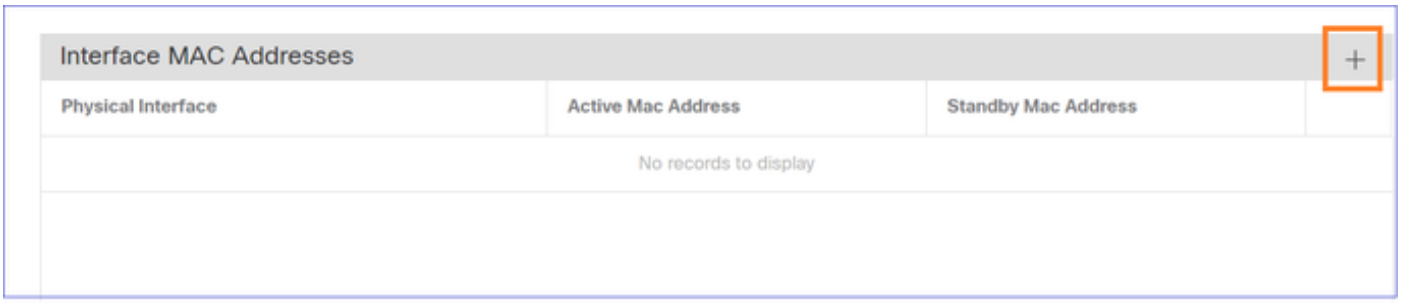


Étape 9. Effectuez les mêmes étapes pour l'interface externe.

Étape 10. Vérification des résultats



Étape 11. Restez dans l'onglet Haute disponibilité et configurez les adresses MAC virtuelles.



Étape 12. Image de l'interface interne



Étape 13. Effectuez les mêmes étapes pour l'interface externe.

Étape 14. Vérification des résultats



Étape 15. Après avoir configuré les modifications, choisissez Save and Deploy.

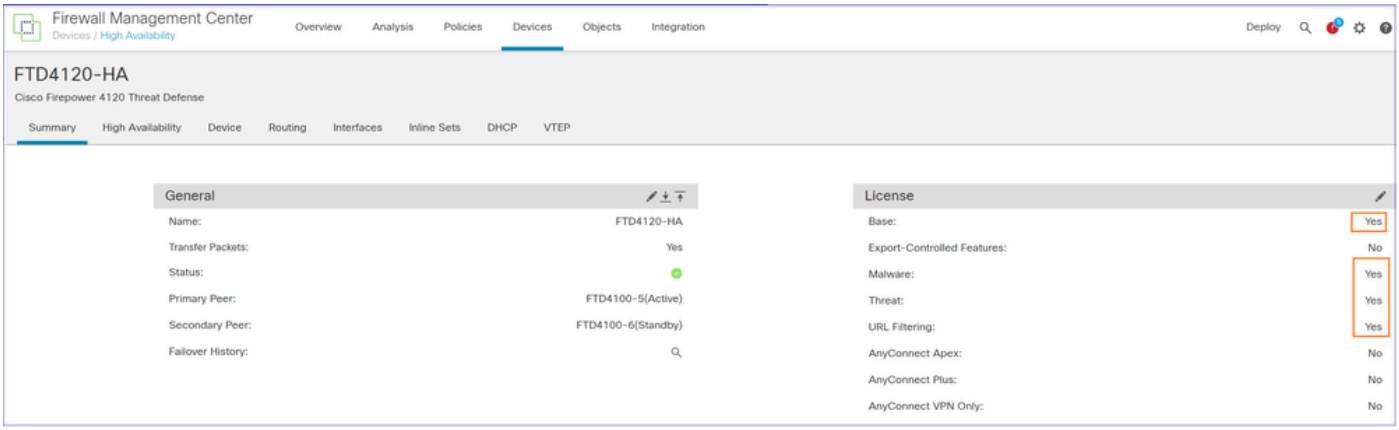
Tâche 3 : vérification de la haute disponibilité et de la licence FTD

Exigence de la tâche :

Vérifiez les paramètres FTD HA et activez les licences à partir de l'interface utilisateur graphique FMC et de l'interface de ligne de commande FTD.

Solution :

Étape 1. Accédez à Summary et vérifiez les paramètres HA et activez les licences.



Étape 2. À partir de l'ILC CLISH FTD, exécutez la commande show high-availability config ou show failover :

<#root>

>

show high-availability config

```
Failover On
Failover unit Primary
Failover LAN Interface: FOVER Port-channel3 (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 2 of 1291 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 FLM1949C5RR, Mate FLM2108V9YG
Last Failover at: 08:46:30 UTC Jul 18 2024
```

This host: Primary - Active

```
                Active time: 1999 (sec)
                slot 0: UCSB-B200-M3-U hw/sw rev (0.0/9.18(4)210) status (Up Sys)
                  Interface diagnostic (0.0.0.0): Normal (Waiting)
                  Interface Inside (192.168.75.10): Link Down (Shutdown)
                  Interface Outside (192.168.76.10): Normal (Not-Monitored)
                slot 1: snort rev (1.0) status (up)
                slot 2: diskstatus rev (1.0) status (up)
```

Other host: Secondary - Standby Ready

```
                Active time: 1466 (sec)
                slot 0: UCSB-B200-M3-U hw/sw rev (0.0/9.18(4)210) status (Up Sys)
                  Interface diagnostic (0.0.0.0): Normal (Waiting)
                  Interface Inside (192.168.75.11): Link Down (Shutdown)
                  Interface Outside (192.168.76.11): Normal (Not-Monitored)
                slot 1: snort rev (1.0) status (up)
                slot 2: diskstatus rev (1.0) status (up)

Stateful Failover Logical Update Statistics
<output omitted>
```

Étape 3. Effectuez les mêmes étapes sur le périphérique secondaire.

Étape 4. Exécutez la commande show failover state à partir de l'interface de ligne de commande LINA :

<#root>

```
firepower#
```

show failover state

```
               State          Last Failure Reason      Date/Time
This host  -   Primary
               Active         None
Other host -   Secondary
               Standby Ready  Comm Failure            18:32:56 EEST Jul 21 2016

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

firepower#
```

Étape 5. Vérifiez les paramètres de configuration de l'unité principale (ILC LINA) :

<#root>

```
>
```

show running-config failover

```
failover
failover lan unit primary
failover lan interface FOVER Port-channel3
failover replication http
failover mac address Ethernet1/4 aaaa.bbbb.1111 aaaa.bbbb.2222
failover mac address Port-channel2.202 aaaa.bbbb.3333 aaaa.bbbb.4444
failover link FOVER Port-channel3
failover interface ip FOVER 172.16.51.1 255.255.255.0 standby 172.16.51.2

>
```

show running-config interface

```
!
interface Port-channel2
no nameif
no security-level
no ip address
!
interface Port-channel2.202
vlan 202
nameif Outside
cts manual
propagate sgt preserve-untag
policy static sgt disabled trusted
security-level 0
ip address 192.168.76.10 255.255.255.0 standby 192.168.76.11
!
interface Port-channel3
description LAN/STATE Failover Interface
!
interface Ethernet1/1
management-only
nameif diagnostic
security-level 0
no ip address
!
interface Ethernet1/4
shutdown
nameif Inside
security-level 0
ip address 192.168.75.10 255.255.255.0 standby 192.168.75.11
>
```

Tâche 4. Changement des rôles de basculement

Exigence de la tâche :

À partir du contrôleur FMC, passez des rôles de basculement principal/actif, secondaire/veille à principal/veille, secondaire/actif.

Solution :

Étape 1. Sélectionnez l'icône.



Étape 2. Confirmez l'action.

Vous pouvez utiliser le résultat de la commande show failover history :

Sur le nouveau	Sur le r
> show failover history ========== Motif d'état à état ========== 09:27:11 UTC 18 juil. 2024 Standby Ready Just Active L'autre unité veut que je sois actif (Défini par la commande config) 09:27:11 UTC 18 juil. 2024 Juste Active Active Drain Une autre unité veut que je sois active (Défini par la commande config) 09:27:11 UTC 18 juil. 2024 Active Drain Active Application de la configuration Une autre unité veut que je sois actif (Défini par la commande config) 09:27:11 UTC 18 juil. 2024 Active Application Config Active Config Appliquée Une autre unité veut que je sois active (Défini par la commande config)	> show ====== Motif d' ====== 09:27:1 Active

09:27:11 UTC 18 juil. 2024 Active Config Appliqué Active Autre unité veut que je sois actif (Défini par la commande config)	

Étape 3. Après vérification, réactivez l'unité principale.

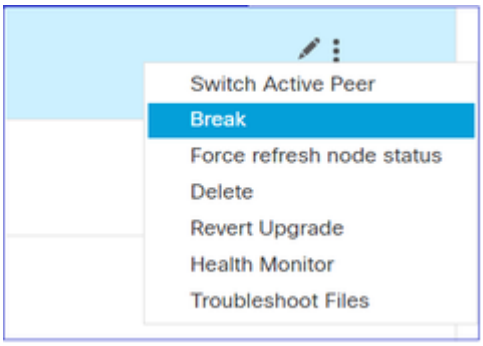
Tâche 5 : rupture de la paire haute disponibilité

Exigence de la tâche :

À partir du FMC, rompez la paire de basculement.

Solution :

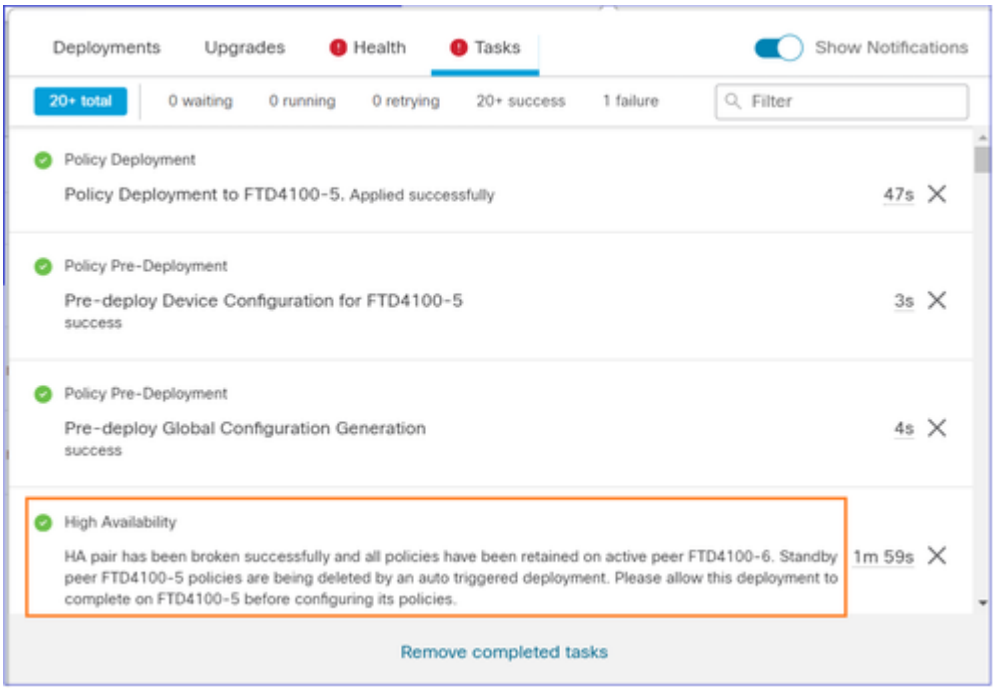
Étape 1. Sélectionnez l'icône.



Étape 2 : vérification de la notification



Étape 3. Notez le message.



Étape 4 : vérification des résultats de l'interface utilisateur graphique du FMC ou de l'interface de ligne de commande

Étape 5. Affichez la configuration en cours sur l'unité principale avant et après la coupure de haute disponibilité :

Unité principale/en veille avant la coupure HA	Unité principale après la coupure HA
> show running-config : Enregistré : : Numéro de série: FLM1949C5RR : Matériel : FPR4K-SM-24, 73850 Mo de RAM, processeur Xeon série E5 2 200 MHz, 2 processeurs (48 coeurs) : NGFW version 7.2.8 ! hostname puissance_feu enable password ***** chiffré strong-encryption-disable service-module 0 keepalive-timeout 4 service-module 0 keepalive-counter 6 noms no mac-address auto	> INFOS : Cette unité est actuellement en veille. En désactivant le basculement, cette unité reste en veille. > show running-config : Enregistré : : Numéro de série: FLM1949C5RR : Matériel : FPR4K-SM-24, 73850 Mo de RAM, processeur Xeon série E5 2 200 MHz, 2 processeurs (48 coeurs) : NGFW version 7.2.8 ! hostname puissance_feu enable password ***** chiffré strong-encryption-disable service-module 0 keepalive-timeout 4

```
!
interface Port-channel2
sans nom
manuel de l'organisme de contrôle des
transports aériens
propagate sgt preserve-untag
stratégie statique sgt désactivée approuvée
pas de niveau de sécurité
pas d'adresse ip
!
interface Port-channel2.202
vlan 202
nameif Extérieur
manuel de l'organisme de contrôle des
transports aériens
propagate sgt preserve-untag
stratégie statique sgt désactivée approuvée
niveau de sécurité 0
adresse ip 192.168.76.10 255.255.255.0 standby
192.168.76.11
!
interface Port-channel3
description Interface de basculement
LAN/STATE
!
interface Ethernet1/1
de gestion seulement
diagnostic de nameif
manuel de l'organisme de contrôle des
transports aériens
propagate sgt preserve-untag
stratégie statique sgt désactivée approuvée
niveau de sécurité 0
pas d'adresse ip
!
interface Ethernet1/4
nameif Inside
manuel de l'organisme de contrôle des
transports aériens
propagate sgt preserve-untag
stratégie statique sgt désactivée approuvée
niveau de sécurité 0
adresse ip 192.168.75.10 255.255.255.0 standby
192.168.75.11
!
ftp mode passive
service-module 0 keepalive-counter 6
noms
no mac-address auto

!
interface Port-channel2
shutdown
sans nom
pas de niveau de sécurité
pas d'adresse ip
!
interface Port-channel3
shutdown
sans nom
pas de niveau de sécurité
pas d'adresse ip
!
interface Ethernet1/1
de gestion seulement
shutdown
sans nom
pas de niveau de sécurité
pas d'adresse ip
!
interface Ethernet1/4
shutdown
sans nom
pas de niveau de sécurité
pas d'adresse ip
!
ftp mode passive
ngips conn-match vlan-id
object-group-search access-control
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ remark rule-id 9998
: STRATÉGIE DE PRÉFILTRE : Tunnel par
défaut et politique de priorité
access-list CSM_FW_ACL_ remark rule-id 9998
: RÈGLE : RÈGLE D'ACTION DE TUNNEL
PAR DÉFAUT
access-list CSM_FW_ACL_ advanced permit ip
any rule-id 9998
access-list CSM_FW_ACL_ advanced permit
udp any eq 3544 any range 1025 65535 rule-id
9998
access-list CSM_FW_ACL_ advanced permit
```

ngips conn-match vlan-id
object-group-search access-control
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ remark rule-id 9998 : STRATÉGIE DE PRÉFILTRE : Tunnel par défaut et politique de priorité
access-list CSM_FW_ACL_ remark rule-id 9998 : RÈGLE : RÈGLE D'ACTION DE TUNNEL PAR DÉFAUT
access-list CSM_FW_ACL_ advanced permit ip any rule-id 9998
access-list CSM_FW_ACL_ advanced permit udp any eq 3544 any range 1025 65535 rule-id 9998
access-list CSM_FW_ACL_ advanced permit udp any range 1025 65535 any eq 3544 rule-id 9998
access-list CSM_FW_ACL_ advanced permit 41 any any rule-id 9998
access-list CSM_FW_ACL_ advanced permit gre any any rule-id 9998
access-list CSM_FW_ACL_ remark rule-id 268434433 : POLITIQUE D'ACCÈS : acp_simple - Par défaut
access-list CSM_FW_ACL_ remark rule-id 268434433 : RÈGLE L4 : RÈGLE D'ACTION PAR DÉFAUT
access-list CSM_FW_ACL_ advanced permit ip any rule-id 268434433
!
tcp-map UM_STATIC_TCP_MAP
tcp-options range 6 7 allow
tcp-options range 9 18 allow
tcp-options range 20 255 allow
autorisation d'indicateur d'urgence
!
pas de pager
no logging message 106015
no logging message 313001
no logging message 313008
no logging message 106023
no logging message 710003
no logging message 106100
no logging message 302015
no logging message 302014
no logging message 302013
no logging message 302018
no logging message 302017
udp any range 1025 65535 any eq 3544 rule-id 9998
access-list CSM_FW_ACL_ advanced permit 41 any any rule-id 9998
access-list CSM_FW_ACL_ advanced permit gre any any rule-id 9998
access-list CSM_FW_ACL_ remark rule-id 268439552 : POLITIQUE D'ACCÈS : acp_simple - Obligatoire
access-list CSM_FW_ACL_ remark rule-id 268439552 : RÈGLE L7 : règle 1
access-list CSM_FW_ACL_ advanced permit ip any rule-id 268439552
!
tcp-map UM_STATIC_TCP_MAP
tcp-options range 6 7 allow
tcp-options range 9 18 allow
tcp-options range 20 255 allow
autorisation d'indicateur d'urgence
!
pas de pager
no logging message 106015
no logging message 313001
no logging message 313008
no logging message 106023
no logging message 710003
no logging message 106100
no logging message 302015
no logging message 302014
no logging message 302013
no logging message 302018
no logging message 302017
no logging message 302021
no logging message 302020
pas de basculement
<résultat omis>

no logging message 302016 no logging message 302021 no logging message 302020 mtu externe 1500 diagnostic mtu 1500 mtu Inside 1500 basculement failover lan unit primary failover lan interface FOVER Port-channel3 réplication de basculement http basculement adresse mac Ethernet1/4 aaaa.bbbb.111 aaaa.bbb.222 failover adresse mac Port-channel2.202 aaaa.bbb.333 aaaa.bbb.4444 liaison de basculement FOVER Port-channel3 failover interface ip FOVER 172.16.51.1 255.255.255.0 standby 172.16.51.2 <résultat omis>	

Unité secondaire/active avant la coupure HA	Unité secondaire après la coupure haute disponibilité
> show running-config : Enregistré : : Numéro de série: FLM2108V9YG : Matériel : FPR4K-SM-24, 73850 Mo de RAM, processeur Xeon série E5 2 200 MHz, 2 processeurs (48 coeurs) : NGFW version 7.2.8 ! hostname puissance_feu enable password ***** chiffré strong-encryption-disable service-module 0 keepalive-timeout 4 service-module 0 keepalive-counter 6 noms no mac-address auto ! interface Port-channel2 sans nom	> show running-config : Enregistré : : Numéro de série: FLM2108V9YG : Matériel : FPR4K-SM-24, 73850 Mo de RAM, processeur Xeon série E5 2 200 MHz, 2 processeurs (48 coeurs) : NGFW version 7.2.8 ! hostname puissance_feu enable password ***** chiffré strong-encryption-disable service-module 0 keepalive-timeout 4 service-module 0 keepalive-counter 6 noms no mac-address auto ! interface Port-channel2

pas de niveau de sécurité pas d'adresse ip ! interface Port-channel2.202 vlan 202 nameif Extérieur manuel de l'organisme de contrôle des transports aériens propagate sgt preserve-untag stratégie statique sgt désactivée approuvée niveau de sécurité 0 adresse ip 192.168.76.10 255.255.255.0 standby 192.168.76.11 ! interface Port-channel3 description Interface de basculement LAN/STATE ! interface Ethernet1/1 de gestion seulement diagnostic de nameif niveau de sécurité 0 pas d'adresse ip ! interface Ethernet1/4 nameif Inside niveau de sécurité 0 adresse ip 192.168.75.10 255.255.255.0 standby 192.168.75.11 ! ftp mode passive ngips conn-match vlan-id object-group-search access-control access-group CSM_FW_ACL_ global access-list CSM_FW_ACL_ remark rule-id 9998 : STRATÉGIE DE PRÉFILTRE : Tunnel par défaut et politique de priorité access-list CSM_FW_ACL_ remark rule-id 9998 : RÈGLE : RÈGLE D'ACTION DE TUNNEL PAR DÉFAUT access-list CSM_FW_ACL_ advanced permit ip any rule-id 9998 access-list CSM_FW_ACL_ advanced permit udp any eq 3544 any range 1025 65535 rule-id 9998 access-list CSM_FW_ACL_ advanced permit	sans nom pas de niveau de sécurité pas d'adresse ip ! interface Port-channel2.202 vlan 202 nameif Extérieur manuel de l'organisme de contrôle des transports aériens propagate sgt preserve-untag stratégie statique sgt désactivée approuvée niveau de sécurité 0 adresse ip 192.168.76.10 255.255.255.0 standby 192.168.76.11 ! interface Port-channel3 sans nom pas de niveau de sécurité pas d'adresse ip ! interface Ethernet1/1 de gestion seulement diagnostic de nameif niveau de sécurité 0 pas d'adresse ip ! interface Ethernet1/4 nameif Inside niveau de sécurité 0 adresse ip 192.168.75.10 255.255.255.0 standby 192.168.75.11 ! ftp mode passive ngips conn-match vlan-id object-group-search access-control access-group CSM_FW_ACL_ global access-list CSM_FW_ACL_ remark rule-id 9998 : STRATÉGIE DE PRÉFILTRE : Tunnel par défaut et politique de priorité access-list CSM_FW_ACL_ remark rule-id 9998 : RÈGLE : RÈGLE D'ACTION DE TUNNEL PAR DÉFAUT access-list CSM_FW_ACL_ advanced permit ip any rule-id 9998 access-list CSM_FW_ACL_ advanced permit udp any eq 3544 any range 1025 65535 rule-id

udp any range 1025 65535 any eq 3544 rule-id 9998 access-list CSM_FW_ACL_ advanced permit 41 any any rule-id 9998 access-list CSM_FW_ACL_ advanced permit gre any any rule-id 9998 access-list CSM_FW_ACL_ remark rule-id 268439552 : POLITIQUE D'ACCÈS : acp_simple - Obligatoire access-list CSM_FW_ACL_ remark rule-id 268439552 : RÈGLE L7 : règle 1 access-list CSM_FW_ACL_ advanced permit ip any rule-id 268439552 ! tcp-map UM_STATIC_TCP_MAP tcp-options range 6 7 allow tcp-options range 9 18 allow tcp-options range 20 255 allow autorisation d'indicateur d'urgence ! pas de pager no logging message 106015 no logging message 313001 no logging message 313008 no logging message 106023 no logging message 710003 no logging message 106100 no logging message 302015 no logging message 302014 no logging message 302013 no logging message 302018 no logging message 302017 no logging message 302016 no logging message 302021 no logging message 302020 mtu externe 1500 diagnostic mtu 1500 mtu Inside 1500 basculement failover lan unit secondary failover lan interface FOVER Port-channel3 réplication de basculement http liaison de basculement FOVER Port-channel3 failover interface ip FOVER 172.16.51.1 255.255.255.0 standby 172.16.51.2	9998 access-list CSM_FW_ACL_ advanced permit udp any range 1025 65535 any eq 3544 rule-id 9998 access-list CSM_FW_ACL_ advanced permit 41 any any rule-id 9998 access-list CSM_FW_ACL_ advanced permit gre any any rule-id 9998 access-list CSM_FW_ACL_ remark rule-id 268439552 : POLITIQUE D'ACCÈS : acp_simple - Obligatoire access-list CSM_FW_ACL_ remark rule-id 268439552 : RÈGLE L7 : règle 1 access-list CSM_FW_ACL_ advanced permit ip any rule-id 268439552 ! tcp-map UM_STATIC_TCP_MAP tcp-options range 6 7 allow tcp-options range 9 18 allow tcp-options range 20 255 allow autorisation d'indicateur d'urgence ! pas de pager no logging message 106015 no logging message 313001 no logging message 313008 no logging message 106023 no logging message 710003 no logging message 106100 no logging message 302015 no logging message 302014 no logging message 302013 no logging message 302018 no logging message 302017 no logging message 302016 no logging message 302021 no logging message 302020 mtu externe 1500 diagnostic mtu 1500 mtu Inside 1500 pas de basculement no monitor-interface Outside no monitor-interface service-module <résultat omis>

<résultat omis>	

Principaux points à noter pour la rupture de la haute disponibilité :

Unité principale/de secours	Unité secondaire/active
• Toutes les configurations de basculement sont supprimées. • Toute la configuration IP est supprimée	• Toutes les configurations de basculement sont supprimées. • Les adresses IP de secours sont conservées, mais elles seront supprimées lors du prochain déploiement

Étape 6. Une fois cette tâche terminée, recréez la paire haute disponibilité.

Tâche 6. Suppression d'une paire haute disponibilité

Cette tâche est basée sur une configuration haute disponibilité sur 41xx utilisant le logiciel 7.2.8. Dans ce cas, les périphériques se trouvaient initialement dans les états suivants :

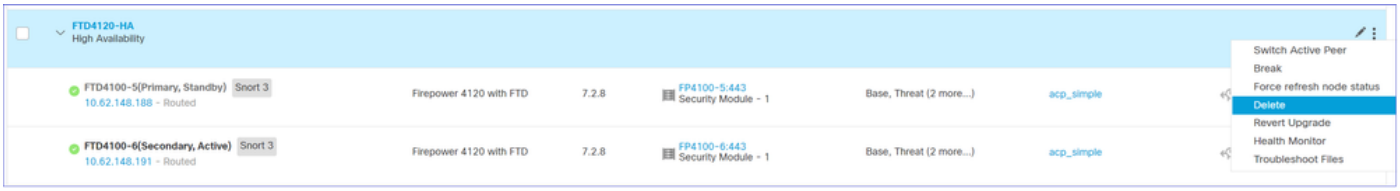
- Principal/veille
- Secondaire/actif

Exigence de la tâche :

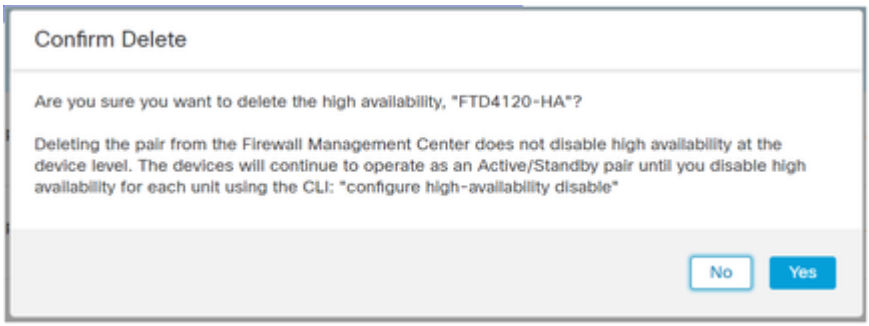
À partir du FMC, supprimez la paire de basculement.

Solution :

Étape 1. Cliquez sur l'icône.



Étape 2. Vérifiez la notification et confirmez.



Étape 3. Après la suppression de la haute disponibilité, les deux périphériques sont désinscrits (supprimés) du FMC.

Étape 4. Affichez le résultat running-config de l'interface de ligne de commande LINA :

Unité principale (veille)	Unité secondaire (active)
> show running-config : Enregistré : : Numéro de série: FLM1949C5RR : Matériel : FPR4K-SM-24, 73853 Mo de RAM, processeur Xeon série E5 2 200 MHz, 2 processeurs (48 coeurs) : NGFW version 7.2.8 ! nom_hôte Firepower-module1 enable password ***** chiffré strong-encryption-disable no asp inspect-dp ack-passthrough service-module 0 keepalive-timeout 4 service-module 0 keepalive-counter 6 noms no mac-address auto ! interface Port-channel2 sans nom pas de niveau de sécurité pas d'adresse ip ! interface Port-channel2.202 vlan 202	> show running-config : Enregistré : : Numéro de série: FLM2108V9YG : Matériel : FPR4K-SM-24, 73853 Mo de RAM, processeur Xeon série E5 2 200 MHz, 2 processeurs (48 coeurs) : NGFW version 7.2.8 ! nom_hôte Firepower-module1 enable password ***** chiffré strong-encryption-disable no asp inspect-dp ack-passthrough service-module 0 keepalive-timeout 4 service-module 0 keepalive-counter 6 noms no mac-address auto ! interface Port-channel2 sans nom pas de niveau de sécurité pas d'adresse ip ! interface Port-channel2.202 vlan 202

nameif NET202 manuel de l'organisme de contrôle des transports aériens propagate sgt preserve-untag stratégie statique sgt désactivée approuvée niveau de sécurité 0 adresse ip 172.16.202.1 255.255.255.0 standby 172.16.202.2 ! interface Port-channel2.203 vlan 203 nameif NET203 manuel de l'organisme de contrôle des transports aériens propagate sgt preserve-untag stratégie statique sgt désactivée approuvée niveau de sécurité 0 adresse ip 172.16.203.1 255.255.255.0 standby 172.16.203.2 ! interface Port-channel3 description Interface de basculement LAN/STATE ! interface Ethernet1/1 de gestion seulement diagnostic de nameif manuel de l'organisme de contrôle des transports aériens propagate sgt preserve-untag stratégie statique sgt désactivée approuvée niveau de sécurité 0 pas d'adresse ip ! interface Ethernet1/4 nameif NET204 manuel de l'organisme de contrôle des transports aériens propagate sgt preserve-untag stratégie statique sgt désactivée approuvée niveau de sécurité 0 adresse ip 172.16.204.1 255.255.255.0 standby 172.16.204.2 ! ftp mode passive ngips conn-match vlan-id	nameif NET202 manuel de l'organisme de contrôle des transports aériens propagate sgt preserve-untag stratégie statique sgt désactivée approuvée niveau de sécurité 0 adresse ip 172.16.202.1 255.255.255.0 standby 172.16.202.2 ! interface Port-channel2.203 vlan 203 nameif NET203 manuel de l'organisme de contrôle des transports aériens propagate sgt preserve-untag stratégie statique sgt désactivée approuvée niveau de sécurité 0 adresse ip 172.16.203.1 255.255.255.0 standby 172.16.203.2 ! interface Port-channel3 description Interface de basculement LAN/STATE ! interface Ethernet1/1 de gestion seulement diagnostic de nameif manuel de l'organisme de contrôle des transports aériens propagate sgt preserve-untag stratégie statique sgt désactivée approuvée niveau de sécurité 0 pas d'adresse ip ! interface Ethernet1/4 nameif NET204 manuel de l'organisme de contrôle des transports aériens propagate sgt preserve-untag stratégie statique sgt désactivée approuvée niveau de sécurité 0 adresse ip 172.16.204.1 255.255.255.0 standby 172.16.204.2 ! ftp mode passive ngips conn-match vlan-id

no object-group-search access-control access-group CSM_FW_ACL_ global access-list CSM_FW_ACL_ remark rule-id 9998 : STRATÉGIE DE PRÉFILTRE : Tunnel par défaut et politique de priorité access-list CSM_FW_ACL_ remark rule-id 9998 : RÈGLE : RÈGLE D'ACTION DE TUNNEL PAR DÉFAUT access-list CSM_FW_ACL_ advanced permit ip any rule-id 9998 access-list CSM_FW_ACL_ advanced permit udp any eq 3544 any range 1025 65535 rule-id 9998 access-list CSM_FW_ACL_ advanced permit udp any range 1025 65535 any eq 3544 rule-id 9998 access-list CSM_FW_ACL_ advanced permit 41 any any rule-id 9998 access-list CSM_FW_ACL_ advanced permit gre any any rule-id 9998 access-list CSM_FW_ACL_ remark rule-id 268434433 : POLITIQUE D'ACCÈS : acp_simple - Par défaut access-list CSM_FW_ACL_ remark rule-id 268434433 : RÈGLE L4 : RÈGLE D'ACTION PAR DÉFAUT access-list CSM_FW_ACL_ advanced permit ip any rule-id 268434433 ! tcp-map UM_STATIC_TCP_MAP tcp-options range 6 7 allow tcp-options range 9 18 allow tcp-options range 20 255 allow tcp-options md5 clear autorisation d'indicateur d'urgence ! pas de pager no logging message 106015 no logging message 313001 no logging message 313008 no logging message 106023 no logging message 710003 no logging message 106100 no logging message 302015 no logging message 302014 no logging message 302013	no object-group-search access-control access-group CSM_FW_ACL_ global access-list CSM_FW_ACL_ remark rule-id 9998 : STRATÉGIE DE PRÉFILTRE : Tunnel par défaut et politique de priorité access-list CSM_FW_ACL_ remark rule-id 9998 : RÈGLE : RÈGLE D'ACTION DE TUNNEL PAR DÉFAUT access-list CSM_FW_ACL_ advanced permit ip any rule-id 9998 access-list CSM_FW_ACL_ advanced permit udp any eq 3544 any range 1025 65535 rule-id 9998 access-list CSM_FW_ACL_ advanced permit udp any range 1025 65535 any eq 3544 rule-id 9998 access-list CSM_FW_ACL_ advanced permit 41 any any rule-id 9998 access-list CSM_FW_ACL_ advanced permit gre any any rule-id 9998 access-list CSM_FW_ACL_ remark rule-id 268434433 : POLITIQUE D'ACCÈS : acp_simple - Par défaut access-list CSM_FW_ACL_ remark rule-id 268434433 : RÈGLE L4 : RÈGLE D'ACTION PAR DÉFAUT access-list CSM_FW_ACL_ advanced permit ip any rule-id 268434433 ! tcp-map UM_STATIC_TCP_MAP tcp-options range 6 7 allow tcp-options range 9 18 allow tcp-options range 20 255 allow tcp-options md5 clear autorisation d'indicateur d'urgence ! pas de pager no logging message 106015 no logging message 313001 no logging message 313008 no logging message 106023 no logging message 710003 no logging message 106100 no logging message 302015 no logging message 302014 no logging message 302013

no logging message 302018 no logging message 302017 no logging message 302016 no logging message 302021 no logging message 302020 mtu NET202 1500 mtu NET203 1500 diagnostic mtu 1500 mtu NET204 1500 basculement failover lan unit primary failover lan interface FOVER Port-channel3 réplication de basculement http liaison de basculement FOVER Port-channel3 failover interface ip FOVER 172.16.51.1 255.255.255.0 standby 172.16.51.2 interface-moniteur NET202 NET203 interface-moniteur icmp unreachable rate-limit 1 burst-size 1 <résultat omis>	no logging message 302018 no logging message 302017 no logging message 302016 no logging message 302021 no logging message 302020 mtu NET202 1500 mtu NET203 1500 diagnostic mtu 1500 mtu NET204 1500 basculement failover lan unit secondary failover lan interface FOVER Port-channel3 réplication de basculement http liaison de basculement FOVER Port-channel3 failover interface ip FOVER 172.16.51.1 255.255.255.0 standby 172.16.51.2 interface-moniteur NET202 NET203 interface-moniteur icmp unreachable rate-limit 1 burst-size 1 <résultat omis>
> show ip Adresses IP système : Nom d'interface Adresse IP Masque de sous-réseau Méthode Port-channel2.202 NET202 172.16.202.1 255.255.255.0 CONFIG Port-channel2.203 NET203 172.16.203.1 255.255.255.0 CONFIG Port-channel3 FOVER 172.16.51.1 255.255.255.0 unset CONFIGURATION D'Ethernet1/4 NET204 172.16.204.1 255.255.255.0 Adresses IP actuelles : Nom d'interface Adresse IP Masque de sous-réseau Méthode Port-channel2.202 NET202 172.16.202.2 255.255.255.0 CONFIG Port-channel2.203 NET203 172.16.203.2 255.255.255.0 CONFIG Port-channel3 FOVER 172.16.51.1 255.255.255.0 unset CONFIGURATION D'Ethernet1/4 NET204 172.16.204.2 255.255.255.0	> show ip Adresses IP système : Nom d'interface Adresse IP Masque de sous-réseau Méthode Port-channel2.202 NET202 172.16.202.1 255.255.255.0 CONFIG Port-channel2.203 NET203 172.16.203.1 255.255.255.0 CONFIG Port-channel3 FOVER 172.16.51.1 255.255.255.0 unset CONFIGURATION D'Ethernet1/4 NET204 172.16.204.1 255.255.255.0 Adresses IP actuelles : Nom d'interface Adresse IP Masque de sous-réseau Méthode Port-channel2.202 NET202 172.16.202.1 255.255.255.0 CONFIG Port-channel2.203 NET203 172.16.203.1 255.255.255.0 CONFIG Port-channel3 FOVER 172.16.51.2 255.255.255.0 unset CONFIGURATION D'Ethernet1/4 NET204 172.16.204.1 255.255.255.0

> show failover Basculement activé Unité de basculement principale Interface LAN de basculement : FOVER Port-channel3 (up) Délai de reconnexion 0:00:00 Fréquence d'interrogation des unités 1 secondes, durée de conservation 15 secondes Fréquence d'interrogation d'interface 5 secondes, durée de conservation 25 secondes Politique d'interface 1 Interfaces surveillées 4 sur 1291 maximum Intervalle de notification de déplacement d'adresse MAC non défini réplication de basculement http Version : Notre 9.18(4)210, Mate 9.18(4)210 Numéro de série: Notre FLM1949C5RR, FLM2108V9YG Dernier basculement à : 13:56:37 UTC 16 juil. 2024 Cet hôte : Principal - Prêt pour la veille Durée active : 0 (s) logement 0 : UCSB-B200-M3-U hw/sw rev (0.0/9.18(4)210) status (Up Sys) Interface NET202 (172.16.202.2) : Normal (surveillé) Interface NET203 (172.16.203.2) : Normal (surveillé) Diagnostic d'interface (0.0.0.0) : Normal (En attente) Interface NET204 (172.16.204.2) : Normal (surveillé) logement 1 : état snort rev (1.0) (up) logement 2 : diskstatus rev (1.0) status (up) Autre hôte : Secondaire - Actif Durée active : 70293 (s) Interface NET202 (172.16.202.1) : Normal (surveillé) Interface NET203 (172.16.203.1) : Normal (surveillé) Diagnostic d'interface (0.0.0.0) : Normal (En attente) Interface NET204 (172.16.204.1) : Normal (surveillé) logement 1 : état snort rev (1.0) (up) logement 2 : diskstatus rev (1.0) status (up)	> show failover Basculement activé Unité de basculement secondaire Interface LAN de basculement : FOVER Port-channel3 (up) Délai de reconnexion 0:00:00 Fréquence d'interrogation des unités 1 secondes, durée de conservation 15 secondes Fréquence d'interrogation d'interface 5 secondes, durée de conservation 25 secondes Politique d'interface 1 Interfaces surveillées 4 sur 1291 maximum Intervalle de notification de déplacement d'adresse MAC non défini réplication de basculement http Version : Notre 9.18(4)210, Mate 9.18(4)210 Numéro de série: Notre FLM2108V9YG, Mate FLM1949C5RR Dernier basculement à : 13:42:35 UTC 16 juil. 2024 Cet hôte : Secondaire - Actif Durée active : 70312 (s) logement 0 : UCSB-B200-M3-U hw/sw rev (0.0/9.18(4)210) status (Up Sys) Interface NET202 (172.16.202.1) : Normal (surveillé) Interface NET203 (172.16.203.1) : Normal (surveillé) Diagnostic d'interface (0.0.0.0) : Normal (En attente) Interface NET204 (172.16.204.1) : Normal (surveillé) logement 1 : état snort rev (1.0) (up) logement 2 : diskstatus rev (1.0) status (up) Autre hôte : Principal - Prêt pour la veille Durée active : 0 (s) logement 0 : UCSB-B200-M3-U hw/sw rev (0.0/9.18(4)210) status (Up Sys) Interface NET202 (172.16.202.2) : Normal (surveillé) Interface NET203 (172.16.203.2) : Normal (surveillé) Diagnostic d'interface (0.0.0.0) : Normal (En attente) Interface NET204 (172.16.204.2) : Normal (surveillé)

<résultat omis>	logement 1 : état snort rev (1.0) (up) logement 2 : diskstatus rev (1.0) status (up) <résultat omis>

Étape 5. Les deux périphériques FTD n'ont pas été enregistrés auprès du FMC :

<#root>

```
> show managers

No managers configured.
```

Principaux points à noter pour l'option Disable HA (désactiver la haute disponibilité) dans le FMC :

Unité principale	Unité Secondaire
Le périphérique est retiré du FMC. Aucune configuration n'est supprimée du périphérique FTD.	Le périphérique est retiré du FMC. Aucune configuration n'est supprimée du périphérique FTD.

Scénario 1 :

Exécutez la commande configure high-availability disable pour supprimer la configuration de basculement du périphérique FTD actif :

<#root>

```
>

configure high-availability disable

 ?
Optional parameter to clear interfaces (clear-interfaces) optional parameter to clear interfaces (clear
<cr>
```

<#root>

```
>

configure high-availability disable
```

```
High-availability will be disabled. Do you really want to continue?
Please enter 'YES' or 'NO':

yes

Successfully disabled high-availability.
```

Le résultat :

Unité principale (hors veille)	Unité secondaire (ex-active)
> INFO: This unit is currently in standby state. By disabling failover, this unit will remain in standby state. > **show failover** **Failover Off (pseudo-Standby)** Failover unit Primary Failover LAN Interface: FOVER Port-channel3 (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 0 of 1291 maximum MAC Address Move Notification Interval not set failover replication http > **show ip** System IP Addresses: Interface Name IP address Subnet mask Method Port-channel3 FOVER 172.16.51.1 255.255.255.0 unset Current IP Addresses: Interface Name IP address Subnet mask Method Port-channel3 FOVER 172.16.51.1 255.255.255.0 unset	> **show failover** Failover Off Failover unit Secondary Failover LAN Interface: not Configured 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 4 of 1291 maximum MAC Address Move Notification Interval not set > **show ip** System IP Addresses: Interface Name IP address Subnet mask Method Port-channel2.202 NET202 172.16.202.1 255.255.255.0 CONFIG Port-channel2.203 NET203 172.16.203.1 255.255.255.0 CONFIG Ethernet1/4 NET204 172.16.204.1 255.255.255.0 CONFIG Current IP Addresses: Interface Name IP address Subnet mask Method Port-channel2.202 NET202 172.16.202.1 255.255.255.0 CONFIG Port-channel2.203 NET203 172.16.203.1 255.255.255.0 CONFIG Ethernet1/4 NET204 172.16.204.1 255.255.255.0 CONFIG
Principal (hors veille)	Secondaire (ex-actif)

> show running-config : Enregistré : : Numéro de série: FLM1949C5RR : Matériel : FPR4K-SM-24, 73853 Mo de RAM, processeur Xeon série E5 2 200 MHz, 2 processeurs (48 coeurs) : NGFW version 7.2.8 ! nom_hôte Firepower-module1 enable password ***** chiffré strong-encryption-disable no asp inspect-dp ack-passthrough service-module 0 keepalive-timeout 4 service-module 0 keepalive-counter 6 noms no mac-address auto ! interface Port-channel2 shutdown sans nom pas de niveau de sécurité no ip address <- Les adresses IP sont supprimées ! interface Port-channel3 description Interface de basculement LAN/STATE ! interface Ethernet1/1 de gestion seulement shutdown sans nom pas de niveau de sécurité pas d'adresse ip ! interface Ethernet1/4 shutdown sans nom pas de niveau de sécurité pas d'adresse ip ! ftp mode passive	> show running-config : Enregistré : : Numéro de série: FLM2108V9YG : Matériel : FPR4K-SM-24, 73853 Mo de RAM, processeur Xeon série E5 2 200 MHz, 2 processeurs (48 coeurs) : NGFW version 7.2.8 ! nom_hôte Firepower-module1 enable password ***** chiffré strong-encryption-disable no asp inspect-dp ack-passthrough service-module 0 keepalive-timeout 4 service-module 0 keepalive-counter 6 noms no mac-address auto ! interface Port-channel2 sans nom pas de niveau de sécurité pas d'adresse ip ! interface Port-channel2.202 vlan 202 nameif NET202 manuel de l'organisme de contrôle des transports aériens propagate sgt preserve-untag stratégie statique sgt désactivée approuvée niveau de sécurité 0 adresse ip 172.16.202.1 255.255.255.0 standby 172.16.202.2 ! interface Port-channel2.203 vlan 203 nameif NET203 manuel de l'organisme de contrôle des transports aériens propagate sgt preserve-untag stratégie statique sgt désactivée approuvée niveau de sécurité 0 adresse ip 172.16.203.1 255.255.255.0 standby

ngips conn-match vlan-id
no object-group-search access-control
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ remark rule-id 9998 : STRATÉGIE DE PRÉFILTRE : Tunnel par défaut et politique de priorité
access-list CSM_FW_ACL_ remark rule-id 9998 : RÈGLE : RÈGLE D'ACTION DE TUNNEL PAR DÉFAUT
access-list CSM_FW_ACL_ advanced permit ip any rule-id 9998
access-list CSM_FW_ACL_ advanced permit udp any eq 3544 any range 1025 65535 rule-id 9998
access-list CSM_FW_ACL_ advanced permit udp any range 1025 65535 any eq 3544 rule-id 9998
access-list CSM_FW_ACL_ advanced permit 41 any any rule-id 9998
access-list CSM_FW_ACL_ advanced permit gre any any rule-id 9998
access-list CSM_FW_ACL_ remark rule-id 268434433 : POLITIQUE D'ACCÈS : acp_simple - Par défaut
access-list CSM_FW_ACL_ remark rule-id 268434433 : RÈGLE L4 : RÈGLE D'ACTION PAR DÉFAUT
access-list CSM_FW_ACL_ advanced permit ip any rule-id 268434433
!
tcp-map UM_STATIC_TCP_MAP
tcp-options range 6 7 allow
tcp-options range 9 18 allow
tcp-options range 20 255 allow
tcp-options md5 clear
autorisation d'indicateur d'urgence
!
pas de pager
no logging message 106015
no logging message 313001
no logging message 313008
no logging message 106023
no logging message 710003
no logging message 106100
no logging message 302015
no logging message 302014
172.16.203.2
!
interface Port-channel3
sans nom
pas de niveau de sécurité
pas d'adresse ip
!
interface Ethernet1/1
de gestion seulement
diagnostic de nameif
manuel de l'organisme de contrôle des transports aériens
propagate sgt preserve-untag
stratégie statique sgt désactivée approuvée
niveau de sécurité 0
pas d'adresse ip
!
interface Ethernet1/4
nameif NET204
manuel de l'organisme de contrôle des transports aériens
propagate sgt preserve-untag
stratégie statique sgt désactivée approuvée
niveau de sécurité 0
adresse ip 172.16.204.1 255.255.255.0 standby 172.16.204.2
!
ftp mode passive
ngips conn-match vlan-id
no object-group-search access-control
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ remark rule-id 9998 : STRATÉGIE DE PRÉFILTRE : Tunnel par défaut et politique de priorité
access-list CSM_FW_ACL_ remark rule-id 9998 : RÈGLE : RÈGLE D'ACTION DE TUNNEL PAR DÉFAUT
access-list CSM_FW_ACL_ advanced permit ip any rule-id 9998
access-list CSM_FW_ACL_ advanced permit udp any eq 3544 any range 1025 65535 rule-id 9998
access-list CSM_FW_ACL_ advanced permit udp any range 1025 65535 any eq 3544 rule-id 9998
access-list CSM_FW_ACL_ advanced permit 41

no logging message 302013 no logging message 302018 no logging message 302017 no logging message 302016 no logging message 302021 no logging message 302020 pas de basculement failover lan unit primary failover lan interface FOVER Port-channel3 réplication de basculement http liaison de basculement FOVER Port-channel3 failover interface ip FOVER 172.16.51.1 255.255.255.0 standby 172.16.51.2 no monitor-interface service-module <résultat omis>	any any rule-id 9998 access-list CSM_FW_ACL_ advanced permit gre any any rule-id 9998 access-list CSM_FW_ACL_ remark rule-id 268434433 : POLITIQUE D'ACCÈS : acp_simple - Par défaut access-list CSM_FW_ACL_ remark rule-id 268434433 : RÈGLE L4 : RÈGLE D'ACTION PAR DÉFAUT access-list CSM_FW_ACL_ advanced permit ip any rule-id 268434433 ! tcp-map UM_STATIC_TCP_MAP tcp-options range 6 7 allow tcp-options range 9 18 allow tcp-options range 20 255 allow tcp-options md5 clear autorisation d'indicateur d'urgence ! pas de pager no logging message 106015 no logging message 313001 no logging message 313008 no logging message 106023 no logging message 710003 no logging message 106100 no logging message 302015 no logging message 302014 no logging message 302013 no logging message 302018 no logging message 302017 no logging message 302016 no logging message 302021 no logging message 302020 mtu NET202 1500 mtu NET203 1500 diagnostic mtu 1500 mtu NET204 1500 pas de basculement interface-moniteur NET202 NET203 interface-moniteur no monitor-interface service-module

Principaux points à noter pour désactiver la haute disponibilité à partir de l'interface de ligne de commande FTD active :

Unité active	Unité En Attente
• La configuration du basculement est supprimée • Les adresses IP de secours ne sont pas supprimées	• Les configurations d'interface sont supprimées. • La configuration du basculement n'est pas supprimée, mais le basculement est désactivé (pseudo-veille)

À ce stade, vous pouvez désactiver la haute disponibilité sur l'ex-unité en veille.

Scénario 2 (non recommandé)

Avertissement : Ce scénario conduit à une situation active/active, c'est pourquoi il n'est pas recommandé. Il est montré seulement pour la conscience.

Exécutez la commande 'configure high-availability disable' pour supprimer la configuration de basculement du périphérique FTD de secours :

```
<#root>

>

configure high-availability disable


High-availability will be disabled. Do you really want to continue?
Please enter 'YES' or 'NO':

YES


Successfully disabled high-availability.
```

Le résultat :

Principal (hors veille)	Secondaire (actif)
> show failover	> show failover

Basculement désactivé Unité de basculement secondaire Interface LAN de basculement : Non configuré Délai de reconnexion 0:00:00 Fréquence d'interrogation des unités 1 secondes, durée de conservation 15 secondes Fréquence d'interrogation d'interface 5 secondes, durée de conservation 25 secondes Politique d'interface 1 Interfaces surveillées 4 sur 1291 maximum Intervalle de notification de déplacement d'adresse MAC non défini > show ip Adresses IP système : Nom d'interface Adresse IP Masque de sous-réseau Méthode Port-channel2.202 NET202 172.16.202.1 255.255.255.0 manual <- Le périphérique utilise les mêmes adresses IP que le système ex-Active! Port-channel2.203 NET203 172.16.203.1 255.255.255.0 manuel Manuel d'Ethernet1/4 NET204 172.16.204.1 255.255.255.0 Adresses IP actuelles : Nom d'interface Adresse IP Masque de sous-réseau Méthode Port-channel2.202 NET202 172.16.202.1 255.255.255.0 manuel Port-channel2.203 NET203 172.16.203.1 255.255.255.0 manuel Manuel d'Ethernet1/4 NET204 172.16.204.1 255.255.255.0	Basculement activé <- Le basculement n'est pas désactivé Unité de basculement secondaire Interface LAN de basculement : FOVER Port-channel3 (up) Délai de reconnexion 0:00:00 Fréquence d'interrogation des unités 1 secondes, durée de conservation 15 secondes Fréquence d'interrogation d'interface 5 secondes, durée de conservation 25 secondes Politique d'interface 1 Interfaces surveillées 4 sur 1291 maximum Intervalle de notification de déplacement d'adresse MAC non défini réplication de basculement http Version : Notre 9.18(4)210, Mate 9.18(4)210 Numéro de série: Notre FLM2108V9YG, Mate FLM1949C5RR Dernier basculement à : 12:44:06 UTC 17 juil. 2024 Cet hôte : Secondaire - Actif Durée active : 632 (s) logement 0 : UCSB-B200-M3-U hw/sw rev (0.0/9.18(4)210) status (Up Sys) Diagnostic d'interface (0.0.0.0) : Normal (En attente) Interface NET204 (172.16.204.1) : Normal (surveillé) Interface NET203 (172.16.203.1) : Normal (surveillé) Interface NET202 (172.16.202.1) : Normal (surveillé) logement 1 : état snort rev (1.0) (up) logement 2 : diskstatus rev (1.0) status (up) Autre hôte : Principal - Désactivé Durée active : 932 (s) logement 0 : UCSB-B200-M3-U hw/sw rev (0.0/9.18(4)210) status (Up Sys) Diagnostic d'interface (0.0.0.0) : Inconnu (En attente) Interface NET204 (172.16.204.2) : Inconnu (surveillé) Interface NET203 (172.16.203.2) : Inconnu (surveillé) Interface NET202 (172.16.202.2) : Inconnu (surveillé)

	logement 1 : état snort rev (1.0) (up) logement 2 : diskstatus rev (1.0) status (up) > show ip Adresses IP système : Nom d'interface Adresse IP Masque de sous-réseau Méthode Port-channel2.202 NET202 172.16.202.1 255.255.255.0 manual <- Le périphérique utilise les mêmes adresses IP que l'ancien mode veille ! Port-channel2.203 NET203 172.16.203.1 255.255.255.0 manuel Port-channel3 FOVER 172.16.51.1 255.255.255.0 unset Manuel d'Ethernet1/4 NET204 172.16.204.1 255.255.255.0 Adresses IP actuelles : Nom d'interface Adresse IP Masque de sous-réseau Méthode Port-channel2.202 NET202 172.16.202.1 255.255.255.0 manuel Port-channel2.203 NET203 172.16.203.1 255.255.255.0 manuel Port-channel3 FOVER 172.16.51.2 255.255.255.0 unset Manuel d'Ethernet1/4 NET204 172.16.204.1 255.255.255.0

Principaux points à noter pour désactiver la haute disponibilité à partir de l'interface de ligne de commande FTD active :

Unité active	Unité En Attente
• La configuration du basculement n'est pas supprimée et reste activée • Le périphérique utilise les mêmes adresses IP que l'ancienne unité en veille	• La configuration du basculement est supprimée • Le périphérique utilise les mêmes adresses IP que l'unité active

Scénario 3 :

Exécutez la commande configure high-availability disable clear-interfaces pour supprimer la configuration de basculement du périphérique FTD actif :

```
<#root>

>

configure high-availability disable clear-interfaces


High-availability will be disabled. Do you really want to continue?
Please enter 'YES' or 'NO':

yes


Successfully disabled high-availability.

>
```

Le résultat :

Principal (hors veille)	Secondaire (ex-actif)
> show failover Basculement désactivé (pseudo-veille) Unité de basculement principale Interface LAN de basculement : FOVER Port-channel3 (up) Délai de reconnexion 0:00:00 Fréquence d'interrogation des unités 1 secondes, durée de conservation 15 secondes Fréquence d'interrogation d'interface 5 secondes, durée de conservation 25 secondes Politique d'interface 1 Interfaces surveillées 0 sur 1291 maximum Intervalle de notification de déplacement d'adresse MAC non défini réplication de basculement http > show ip Adresses IP système : Nom d'interface Adresse IP Masque de sous-réseau Méthode	> show failover Basculement désactivé Unité de basculement secondaire Interface LAN de basculement : Non configuré Délai de reconnexion 0:00:00 Fréquence d'interrogation des unités 1 secondes, durée de conservation 15 secondes Fréquence d'interrogation d'interface 5 secondes, durée de conservation 25 secondes Politique d'interface 1 Interfaces surveillées 0 sur 1291 maximum Intervalle de notification de déplacement d'adresse MAC non défini > show ip Adresses IP système : Nom d'interface Adresse IP Masque de sous-réseau Méthode Adresses IP actuelles : Nom d'interface Adresse IP Masque de sous-

Port-channel3 FOVER 172.16.51.1 255.255.255.0 unset Adresses IP actuelles : Nom d'interface Adresse IP Masque de sous-réseau Méthode Port-channel3 FOVER 172.16.51.1 255.255.255.0 unset **>**	réseau Méthode **>**

Points principaux à noter pour la désactivation de la haute disponibilité avec les interfaces clear-from Active FTD CLI :

Unité active	Unité En Attente
• La configuration du basculement est supprimée • Les adresses IP sont supprimées	• La configuration du basculement n'est pas supprimée, mais le basculement est désactivé (pseudo-veille) • Les adresses IP sont supprimées

Scénario 4

Exécutez la commande 'configure high-availability disable clear-interfaces' pour supprimer la configuration de basculement du périphérique FTD de secours :

<#root>

>

configure high-availability disable clear-interfaces

High-availability will be disabled. Do you really want to continue?
Please enter 'YES' or 'NO':

YES

Successfully disabled high-availability.

>

Le résultat :

Principal (hors veille)	Secondaire (actif)
> show failover Basculement désactivé Unité de basculement secondaire Interface LAN de basculement : Non configuré Délai de reconnexion 0:00:00 Fréquence d'interrogation des unités 1 secondes, durée de conservation 15 secondes Fréquence d'interrogation d'interface 5 secondes, durée de conservation 25 secondes Politique d'interface 1 Interfaces surveillées 0 sur 1291 maximum Intervalle de notification de déplacement d'adresse MAC non défini > show ip Adresses IP système : Nom d'interface Adresse IP Masque de sous-réseau Méthode Adresses IP actuelles : Nom d'interface Adresse IP Masque de sous-réseau Méthode >	> show failover Basculement activé Unité de basculement secondaire Interface LAN de basculement : FOVER Port-channel3 (up) Délai de reconnexion 0:00:00 Fréquence d'interrogation des unités 1 secondes, durée de conservation 15 secondes Fréquence d'interrogation d'interface 5 secondes, durée de conservation 25 secondes Politique d'interface 1 Interfaces surveillées 4 sur 1291 maximum Intervalle de notification de déplacement d'adresse MAC non défini réplication de basculement http Version : Notre 9.18(4)210, Mate 9.18(4)210 Numéro de série: Notre FLM2108V9YG, Mate FLM1949C5RR Dernier basculement à : 07:06:56 UTC 18 juil. 2024 Cet hôte : Secondaire - Actif Durée active : 1194 (s) logement 0 : UCSB-B200-M3-U hw/sw rev (0.0/9.18(4)210) status (Up Sys) Diagnostic d'interface (0.0.0.0) : Normal (En attente) Interface NET204 (172.16.204.1) : Normal (surveillé) Interface NET202 (172.16.202.1) : Normal (surveillé) Interface NET203 (172.16.203.1) : Normal (surveillé) logement 1 : état snort rev (1.0) (up) logement 2 : diskstatus rev (1.0) status (up) Autre hôte : Principal - Désactivé Durée active : 846 (s) logement 0 : UCSB-B200-M3-U hw/sw rev (0.0/9.18(4)210) status (Up Sys) Diagnostic d'interface (0.0.0.0) : Inconnu (En attente) Interface NET204 (172.16.204.2) : Inconnu

	(surveillé) Interface NET202 (172.16.202.2) : Inconnu (surveillé) Interface NET203 (172.16.203.2) : Inconnu (surveillé) logement 1 : état snort rev (1.0) (up) logement 2 : diskstatus rev (1.0) status (up) > show ip Adresses IP système : Nom d'interface Adresse IP Masque de sous-réseau Méthode Port-channel2.202 NET202 172.16.202.1 255.255.255.0 manuel Port-channel2.203 NET203 172.16.203.1 255.255.255.0 manuel Port-channel3 FOVER 172.16.51.1 255.255.255.0 unset Manuel d'Ethernet1/4 NET204 172.16.204.1 255.255.255.0 Adresses IP actuelles : Nom d'interface Adresse IP Masque de sous-réseau Méthode Port-channel2.202 NET202 172.16.202.1 255.255.255.0 manuel Port-channel2.203 NET203 172.16.203.1 255.255.255.0 manuel Port-channel3 FOVER 172.16.51.2 255.255.255.0 unset Manuel d'Ethernet1/4 NET204 172.16.204.1 255.255.255.0

Points principaux à noter pour désactiver la haute disponibilité avec les interfaces claires de l'interface de ligne de commande active FTD :

Unité active	Unité En Attente
• La configuration du basculement n'est pas supprimée • Les adresses IP ne sont pas supprimées	• La configuration du basculement est supprimée • Les adresses IP sont supprimées

Étape 6. Une fois cette tâche terminée, enregistrez les périphériques sur le FMC et activez la

paire haute disponibilité.

Tâche 7. Suspension de la haute disponibilité

Exigence de la tâche :

Suspendre la HA de l'interface CLI CLISH FTD.

Solution :

Étape 1. Sur le FTD principal, exécutez la commande et confirmez (tapez YES).

<#root>

> configure high-availability suspend

```
Please ensure that no deployment operation is in progress before suspending high-availability.
Please enter 'YES' to continue if there is no deployment operation in progress and 'NO' if you wish to
```

YES

```
Successfully suspended high-availability.
```

Étape 2 : vérification des modifications apportées à l'unité principale

<#root>

>

show high-availability config

Failover Off

```
Failover unit Primary
Failover LAN Interface: fover_link Ethernet1/4 (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 1 of 1041 maximum
MAC Address Move Notification Interval not set
failover replication http
```

Étape 3. Résultat sur l'unité secondaire :

<#root>

```
>

show high-availability config
Failover Off (pseudo-Standby)

Failover unit Secondary
Failover LAN Interface: fover_link Ethernet1/4 (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 1 of 1041 maximum
MAC Address Move Notification Interval not set
failover replication http
```

Étape 4. Reprise de la haute disponibilité sur l’unité principale :

<#root>

```
>

configure high-availability resume

Successfully resumed high-availablity.

> .

    No Active mate detected
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Beginning configuration replication: Sending to mate.
End Configuration Replication to mate

>
```

<#root>

```
>

show high-availability config

Failover On

Failover unit Primary
Failover LAN Interface: fover_link Ethernet1/4 (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 1 of 1041 maximum
MAC Address Move Notification Interval not set
failover replication http
```

Étape 5. Résultats sur l'unité secondaire après la reprise de la haute disponibilité :

<#root>

```
> ..
```

Detected an Active mate

```
Beginning configuration replication from mate.


WARNING: Failover is enabled but standby IP address is not configured for this interface.
WARNING: Failover is enabled but standby IP address is not configured for this interface.
End configuration replication from mate.

>
```

<#root>

```
>
```

show high-availability config

Failover On

```
Failover unit Secondary
Failover LAN Interface: fover_link Ethernet1/4 (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 1 of 1041 maximum
MAC Address Move Notification Interval not set
failover replication http
>
```

Foire aux questions (FAQ)

Q : Lorsque la configuration est répliquée, est-elle enregistrée immédiatement (ligne par ligne) ou à la fin de la réplication ?
R : À la fin de la réplication. La preuve se trouve à la fin du résultat de la commande debug fover sync, qui affiche la duplication de la configuration ou de la commande :

<#root>

```
cli_xml_server: frep_write_cmd: Cmd: access-list CSM_FW_ACL_ line 1506 remark rule-id 268442578: L7 RUL
cli_xml_server: frep_write_cmd: Cmd: access-list CSM_FW_ACL_ line 1507 advanced permit tcp object-group
cli_xml_server: frep_write_cmd: Cmd: access-list CSM_FW_ACL_ line 1508 remark rule-id 268442078: ACCESS
cli_xml_server: frep_write_cmd: Cmd: access-list CSM_FW_ACL_ line 1509 remark rule-id 268442078: L4 RUL
...
cli_xml_server: frep_write_cmd: Cmd: no access-list CSM_FW_ACL_ advanced permit tcp object-group group_
cli_xml_server: frep_write_cmd: Cmd: no access-list CSM_FW_ACL_ line 1510 remark rule-id 268442077: ACC
cli_xml_server: frep_write_cmd: Cmd: no access-list CSM_FW_ACL_ line 1510 remark rule-id 268442077: L7
cli_xml_server: frep_write_cmd: Cmd: no access-list CSM_FW_ACL_ advanced permit tcp object-group group_
cli_xml_server: frep_write_cmd: Cmd: no access-list CSM_FW_ACL_ line 1510 remark rule-id 268440577: ACC
cli_xml_server: frep_write_cmd: Cmd: no access-list CSM_FW_ACL_ line 1510 remark rule-id 268440577: L4
cli_xml_server: frep_write_cmd: Cmd: access-list CSM_FW_ACL_ advanced deny ip any any rule-id 268442078
cli_xml_server: frep_write_cmd: Cmd: crypto isakmp nat-traversal
cli_xml_server: frep_write_cmd: Cmd: no object-group network group_311
cli_xml_server: frep_write_cmd: Cmd: no object-group network group_433
cli_xml_server: frep_write_cmd: Cmd: no object-group network group_6
cli_xml_server: frep_write_cmd: Cmd: no object-group network group_2
cli_xml_server: frep_write_cmd: Cmd:

write memory        <--
```

Q : Que se passe-t-il si une unité est dans un pseudo état de veille (basculement désactivé) et que vous la rechargez alors que l'autre unité a le basculement activé et est active ?
R : Vous vous retrouvez dans un scénario Actif/Actif (bien que techniquement il s'agisse d'un Active/Failover-off). Plus précisément, une fois que l'unité est activée, le basculement est désactivé. Cependant, l'unité utilise les mêmes adresses IP que l'unité active. Donc, dans les faits, vous avez :

- Unité 1 : Actif
- Unité 2 : Le basculement est désactivé et l'unité utilise les mêmes adresses IP de données que l'unité 1, mais des adresses MAC différentes.

Q : Qu'arrive-t-il à la configuration du basculement si vous désactivez manuellement le basculement (configurez la suspension haute disponibilité), puis rechargez le périphérique ?
R : Lorsque vous désactivez le basculement, il ne s'agit pas d'une modification permanente (elle n'est pas enregistrée dans la configuration initiale, sauf si vous décidez de le faire explicitement).

Vous pouvez redémarrer/recharger l'unité de deux façons différentes et avec la deuxième façon, vous devez être prudent :

Cas 1. Redémarrage à partir de CLISH

Le redémarrage à partir de CLISH ne demande pas de confirmation. Par conséquent, la modification de configuration n'est pas enregistrée dans la configuration de démarrage :

```
<#root>

>

configure high-availability suspend

Please ensure that no deployment operation is in progress before suspending high-availability.
Please enter 'YES' to continue if there is no deployment operation in progress and 'NO' if you wish to

YES

Successfully suspended high-availability.
```

La configuration en cours a désactivé le basculement. Dans ce cas, l'unité était en veille et placée dans l'état pseudo-veille comme prévu pour éviter un scénario actif/actif :

```
<#root>

firepower#

show failover | include Failover

Failover Off (

pseudo-Standby

)
Failover unit Secondary
Failover LAN Interface: FOVER Ethernet1/1 (up)
```

La configuration de démarrage a toujours le basculement activé :

```
<#root>

firepower#
```

```
show startup | include failover
```

```
failover
```

```
failover lan unit secondary
failover lan interface FOVER Ethernet1/1
failover replication http
failover link FOVER Ethernet1/1
failover interface ip FOVER 192.0.2.1 255.255.255.0 standby 192.0.2.2
failover ipsec pre-shared-key *****
```

Redémarrez l'appareil à partir de la CLISH (commande reboot) :

```
<#root>
```

```
>
```

```
reboot
```

```
This command will reboot the system.  Continue?
Please enter 'YES' or 'NO':
```

```
YES
```

```
Broadcast message from root@
Threat Defense System: CMD=-stop, CSP-ID=cisco-ftd.6.2.2.81__ftd_001_JMX2119L05CYRIBVX1, FLAG=''
Cisco FTD stopping ...
```

Une fois l'unité sous tension, puisque le basculement est activé, l'appareil entre dans la phase de négociation de basculement et tente de détecter le pair distant :

```
<#root>
```

```
User enable_1 logged in to firepower
Logins over the last 1 days: 1.
Failed logins since the last login: 0.
Type help or '?' for a list of available commands.
firepower> .
```

```
Detected an Active mate
```

Cas 2. Redémarrage à partir de LINA CLI :

Redémarrez à partir de LINA (commande reload) et demandez confirmation. Ainsi, si vous sélectionnez Y (Yes) et que la modification de configuration est enregistrée dans la configuration de démarrage :

```
<#root>

firepower#

reload

System config has been modified. Save? [Y]es/[N]o:

Y  <-- Be careful. This disables the failover in the startup-config


Cryptochecksum: 31857237 8658f618 3234be7c 854d583a

8781 bytes copied in 0.940 secs
Proceed with reload? [confirm]
firepower#

show startup | include failover


no failover

failover lan unit secondary
failover lan interface FOVER Ethernet1/1
failover replication http
failover link FOVER Ethernet1/1
failover interface ip FOVER 192.0.2.1 255.255.255.0 standby 192.0.2.2
failover ipsec pre-shared-key *****
```

Une fois que l'unité est sous tension, le basculement est désactivé :

```
<#root>

firepower#

show failover | include Fail


Failover Off

Failover unit Secondary
Failover LAN Interface: FOVER Ethernet1/1 (up)
```

Remarque : Pour éviter ce scénario, assurez-vous que lorsque vous y êtes invité, vous

n'enregistrez pas les modifications apportées à la configuration de démarrage.

Informations connexes

- Reportez-vous à toutes les versions du guide de configuration de Cisco Firepower Management Center :

Navigation dans la documentation de Cisco Secure Firewall Threat Defense

- Reportez-vous à toutes les versions du guide de configuration FXOS Chassis Manager and CLI :

Navigation dans la documentation FXOS de Cisco Firepower 4100/9300

- Le centre d'assistance technique international (TAC) de Cisco recommande vivement ce guide visuel pour des connaissances pratiques approfondies sur les technologies de sécurité nouvelle génération Cisco Firepower :

Cisco Firepower Threat Defense (FTD) : Meilleures pratiques de configuration et de dépannage pour le pare-feu de nouvelle génération (NGFW), le système de prévention des intrusions de nouvelle génération (NGIPS) et Advanced Malware Protection (AMP)

- Reportez-vous à toutes les notes techniques de configuration et de dépannage relatives aux technologies Firepower :

Cisco Secure Firewall Management Center

- Assistance et documentation techniques - Cisco Systems

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.