Configurer la haute disponibilité FTD sur les appareils Firepower

Table des matières

Introduction
Conditions préalables
Exigences
Composants utilisés
Tâche 1. Vérifier les conditions
Tâche 2. Configurer la haute disponibilité FTD
Conditions
Tâche 3. Vérifier le FTD à haute disponibilité et la licence
Tâche 4. Modifier les rôles de basculement
<u>Tâche 5. Rompre la paire à haute disponibilité</u>
Tâche 6. Supprimer une paire haute disponibilité
Tâche 7. Suspendre la haute disponibilité
Foire aux questions (FAQ)
Informations connexes

Introduction

Ce document décrit comment configurer et vérifier Firepower Threat Defense (FTD) High Availability (HA) (basculement actif/veille) 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 à haute disponibilité doivent satisfaire aux conditions mentionnées dans le présent document.

Tâche 1. Vérifier les 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. Connectez-vous à l'adresse IP de gestion du FPR9300 et vérifiez le 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-F	PR9K-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	VOL	FLM19206H91	Equipped	262144	36
1/2	FPR9K-SM-36	V01	FLM19216KAX	Equipped	262144	36
1/3	FPR9K-SM-36	V01	FLM19267A63	Equipped	262144	36
KSEC-FP	R9K-2-A#					

Étape 2. Connectez-vous au gestionnaire de châssis du FPR9300-1 et accédez aux périphériques

logiques (Logical Devices).

Vérifiez la version du logiciel, le nombre et le type d'interfaces.

Tâche 2. Configurer la haute disponibilité FTD

Exigence de la tâche :

Configurez le basculement entre les modes actif/de secours (haute disponibilité) conformément à ce schéma. Dans ce cas, une paire 41xx est utilisée.



Solution

Les deux périphériques FTD sont déjà enregistrés sur le FMC, tel qu'il est illustré ci-dessous.

FTD4100-5 Snort 3 10.62.148.188 - Routed	Firepower 4120 with FTD	7.2.8	EP4100-5:443 Security Module - 1	Base, Threat (2 more)	acp_simple	Q>	1
FTD4100-6 Snort 3 10.62.148.191 - Routed	Firepower 4120 with FTD	7.2.8	EFP4100-6:443 Security Module - 1	Base, Threat (2 more)	acp_simple	Q9	1:

Étape 1. Afin de configurer le basculement FTD, naviguez vers Devices > Device Management et choisissez Add High Availability comme indiqué dans l'image.

	Deploym	ent History
Q Search De	evice	Add 🔻
	Device	•
	High A	vailability
Auto RollBack	Cluste	r
	Group	

Étape 2. Entrez le Pair principal et le Pair secondaire et choisissez Continue comme indiqué dans l'image.

Vern	lan Charala Hannay	-
	Add High Availability Pair	ľ
	Name:*	
7.2	FTD4100-HA	n (:
	Device Type:	
7.2	Firewall Threat Defense 🔹	nt (:
	Primary Peer:	
	FTD4100-5	
	Secondary Peer:	
	FTD4100-6	
	Threat Defense High Availability pair will have primary configuration. Licenses from primary peer will be converted to their high availability versions and applied on both peers.	
L	Cancel Continue	

Avertissement : assurez-vous de sélectionner l'unité correcte 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

Afin de 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 d'une configuration NTP (Network Time Protocol) identique.
- Être entièrement déployé sur le FMC sans modifications non validées.
- Être dans le même mode de pare-feu : routé ou transparent.



Remarque : cette option doit être vérifiée sur les périphériques FTD et sur l'interface utilisateur graphique FMC, car il est arrivé que les FTD aient le même mode, mais FMC ne le reflète pas.

- Aucune interface n'est configurée avec DHCP/Point-to-Point Protocol over Ethernet (PPPoE).
- Nom d'hôte différent [nom de domaine complet (FQDN)] pour les deux châssis. Afin de 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 de l'un d'eux en exécutant les commandes ci-dessous :

<#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 sur le FMC, puis enregistrez-le de nouveau. Procédez ensuite à la création de la paire à haute disponibilité.

Étape 3. Configurez la haute disponibilité et indiquez les paramètres des liens.

Dans votre cas, les paramètres du lien de l'état sont les mêmes que ceux du lien à haute disponibilité.

Choisissez Add et attendez quelques minutes que la paire haute disponibilité soit déployée, comme illustré dans l'image.

ligh Availabi	ility Link	State Link		
Interface:*	Port-channel3	Interface:*	Same as LAN Failover Link	Ŧ
ogical Name:*	FOVER	Logical Name:*	FOVER	
Primary IP:*	172.16.51.1	Primary IP:*	172.16.51.1	
l.	Use IPv6 Address		Use IPv6 Address	
Secondary IP:*	172.16.51.2	Secondary IP:*	172.16.51.2	
Subnet Mask:*	255.255.255.0	Subnet Mask:*	255.255.255.0	
Psec Encryp	tion			
(ey Generation:	Auto 👻			
LAN failover I between peers.	ink is used to sync configuration, statefu Selected interface links and encryption s	ul failover link is used settings cannot be cl	to sync application content hanged later.	

Étape 4. Configurez les interfaces de données (adresses IP principale et de secours).

Dans l'interface utilisateur graphique de FMC, choisissez HA Edit comme illustré dans l'image.

V FTD4120-HA High Availability							1
FTD4100-5(Primary, Active) Short 3 10.62.148.188 - Routed	Firepower 4120 with FTD	7.2.8	EP4100-5:443 Security Module - 1	Base, Threat (2 more)	acp_simple	c?	:
FTD4100-6(Secondary, Standby) Snort 3 10.62.148.191 - Routed	Firepower 4120 with FTD	7.2.8	FP4100-6:443 Security Module - 1	Base, Threat (2 more)	acp_simple	P	:

Étape 5. Configurez les paramètres d'interface :

Edit Physi	cal Inter	face						0
General	IPv4	IPv6	Path Monitoring	Advanced				
Name:								
Inside								
Enabled								
Manager	nent Only							
Description:								
Mode:								
None			*					
Security Zon	e:							
			¥					
Interface ID:								
Ethernet1/	4							
MTU:								
1500								
(64 - 9184)								
Priority:								
0			(0 - 65535)					
Propagate Si	ecurity Gro	oup Tag:						
NVE Only:								
							Cancel	ОК

General	IPv4	IPv6	Path Monitoring	Advanced		
P Type:						
Use Static	IP		v			
Address:						
192.168.7	5.10/24					
g. 192.0.2.1/2	255.255.255	5.128 or 19	2.0.2.1/25			
g. 192.0.2.1/3	255.255.255	5.128 or 19	2.0.2.1/25			
7. 192.0.2.1/2	255.255.255	5.128 or 19	2.0.2.1/25			
g. 192.0.2.1/J	255 255 251	5.128 or 19.	2.0.2.1/25			
g. 192.0.2.1/2	255.255.255	5.128 or 19	2.0.2.1/25			
rg. 192.0.2.1/2	255.255.25	i. 128 or 19	2.0.2.1/25			
ig. 192.0.2.1/2	255.255.25	5.128 or 19	2.0.2.1/25			

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

Edit Ether	Channe	el Interfa	ace		0
General	IPv4	IPv6	Path Monitoring	Advanced	
Name:	nent Only				

Étape 6. Accédez à High Availability et choisissez l'option Interface Name Edit pour ajouter les adresses IP de secours comme indiqué dans l'image.

Firewall Management Cen Devices / High Availability	ter _{Overview}	Analysis Policies	Devices Objects Integrati	'n			Deploy Q 🚱 🔅	mzafeiro •	teste SECURE
FTD4120-HA Cisco Firepower 4120 Threat Defense									Cancel
Summary High Availability Devic	e Routing Interfa	ces Inline Sets DF	ICP VTEP						
High Availability Configuration									
High Availability Link					State Link				
Interface			Port-channel3		Interface			Port	channel3
Logical Name			FOVER		Logical Name				FOVER
Primary IP			172.16.51.1		Primary IP			17	2.16.51.1
Secondary IP			172.16.51.2		Secondary IP			17	2.16.51.2
Subnet Mask			255.255.255.0		Subnet Mask			255.7	55.255.0
IPsec Encryption			Disabled		Statistics				٩
Monitored Interfaces									
Interface Name	Active IPv4	Standby IPv4	Active IPv6 - Standby IPv6			Active Link-Local IPv6	Standby Link-Local IPv6	Monitoring	
🗃 Inside	192.168.75.10							•	1
diagnostic								•	1
Outside	192.168.76.10							۰	1



Edit Inside	0
Monitor this interface for failures	
Interface Name: Inside Active IP Address: 192.168.75.10 Mask: 24	
Standby IP Address: 192.168.75.11	
Canc	el OK

Étape 8. Faites de même pour l'interface externe (Outside).

Étape 9. Vérifiez que le résultat est le même que celui sur l'image.

Monitored Interfaces							
Interface Name	Active IPv4	Standby IPv4	Active IPv6 - Standby IPv6	Active Link-Local IPv6	Standby Link-Local IPv6	Monitoring	
😭 Inside	192.168.75.10	192.168.75.11				•	/
diagnostic						•	/
Cutside	192.168.76.10	192.168.76.11				•	/

Étape 10. Restez dans l'onglet Haute disponibilité et configurez les adresses MAC virtuelles comme indiqué dans l'image.

Interface MAC Addresses				
Physical Interface	Active Mac Address	Standby Mac Address		
	No records to display			

Add Interface Mac Address
Physical Interface:*
Ethernet1/4
Active Interface Mac Address:*
aaaa.bbbb.1111
Standby Interface Mac Address:*
aaaa.bbbb.2222
Enter the Mac addresses in hexadecimal format such as 0123.4567.89ab
Cancel OK

Étape 12. Faites de même pour l'interface externe (Outside).

Étape 13. Vérifiez que le résultat est le même que celui sur l'image.

Interface MAC Addresses			+
Physical Interface	Active Mac Address	Standby Mac Address	
Ethernet1/4	aaaa.bbbb.1111	aaaa.bbbb.2222	/1
Port-channel2.202	aaaa.bbbb.3333	aaaa.bbbb.4444	/1

Étape 14. Après avoir configuré les modifications, choisissez Save and Deploy.

Tâche 3. Vérifier le FTD à haute disponibilité et la licence

Exigence de la tâche :

Vérifiez les paramètres du FTD à haute disponibilité et les licences activées à partir de la GUI du FMC et de la CLI du FTD.

Solution :

Étape 1. Rendez-vous au récapitulatif (Summary) et vérifiez les paramètres de haute disponibilité et les licences activées en vous fiant à l'image.

									_
Firewall Manag Devices / High Availa	gement Center Overview An bility	nalysis Policies Devices	Objects Integration	n		Deploy C	λ 🌀	¢	0
FTD4120-HA									
Cisco Firepower 4120 Threa	t Defense								
Summary High Avail	ability Device Routing Interfaces	Inline Sets DHCP VTEP							
	General		/±∓		License				1
	Name:		FTD4120-HA		Base:			1	/es
	Transfer Packets:		Yes		Export-Controlled Features:				No
	Status:		0		Malware:			1	res
	Primary Peer:		FTD4100-5(Active)		Threat:			1	res
	Secondary Peer:		FTD4100-6(Standby)		URL Filtering:			1	res
	Failover History:		٩		AnyConnect Apex:				No
					AnyConnect Plus:				No
					AnyConnect VPN Only:				No

Étape 2. À partir de l'interface de ligne de commande FTD CLISH, 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. Faites de même sur le périphérique secondaire.

Étape 4. Exécutez la commande show failover state à partir de la CLI LINA :

<#root> firepower# show failover state State Last Failure Reason Date/Time This host -Primary None Active Other host -Secondary 18:32:56 EEST Jul 21 2016 Standby Ready Comm Failure ====Configuration State=== Sync Done ====Communication State=== Mac set firepower#

Étape 5. Vérifiez la configuration de l'unité principale (CLI 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 1 interface Port-channel3 description LAN/STATE Failover Interface interface Ethernet1/1 management-only nameif diagnostic security-level 0 no ip address Т 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. Modifier les rôles de basculement

Exigence de la tâche :

À partir du FMC, basculez les rôles de basculement de Primary/Active (principal/actif), Secondary/Standby (secondaire/de secours) à Primary/Standby (principal/de secours), Secondary/Active (secondaire/actif).

Solution :

Étape 1. Sélectionnez l'icône illustrée ci-dessous.

FTD4120-HA High Availability							Switch Active Peer
FTD4100-5(Primary, Active) Short 3 10.62.148.188 - Routed	Firepower 4120 with FTD	7.2.8	FP4100-5:443 Security Module - 1	Base, Threat (2 more)	acp_simple	۰Ø	Break Force refresh node status Delete Revert Upgrade
FTD4100-6(Secondary, Standby) Short 3 10.62.148.191 - Routed	Firepower 4120 with FTD	7.2.8	EFP4100-6:443 Security Module - 1	Base, Threat (2 more)	acp_simple	40	Health Monitor Troubleshoot Files

Étape 2. Confirmez l'action.

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

Sur le nouveau				
> 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 config)	(Défini par la commande			
09:27:11 UTC 18 juil. 2024 Juste Active Active Drain Une autre unité veut que je sois active config)	(Défini par la commande	> show ===== Motif d' ======		
09:27:11 UTC 18 juil. 2024 Active Drain Active Application de la configuration Une autre unité veut config)	t que je sois actif (Défini par la commande	09:27:1 Active		
09:27:11 UTC 18 juil. 2024 Active Application Config Active Config Appliquée Une autre unité veut config)	t que je sois active (Défini par la commande			
09:27:11 UTC 18 juil. 2024 Active Config Appliqué Active Autre unité veut que je sois actif config)	(Défini par la commande			

Étape 4. Après la vérification, réactivez l'unité principale.

Tâche 5. Rompre la paire à haute disponibilité

Exigence de la tâche :

À partir du FMC, rompez la paire de basculement.

Solution :

Étape 1. Sélectionnez l'icône illustrée ci-dessous.

/ E
Switch Active Peer
Break
Force refresh node status
Delete
Revert Upgrade
Health Monitor
Troubleshoot Files

Étape 2. Vérifiez la notification illustrée ci-dessous.



Étape 3. Prenez note du message illustré ci-dessous.

	Deployments Upgrades 0 Health 0 Tasks Sho	w Notific	ation	s
	0 waiting 0 running 0 retrying 20+ success 1 failure . Filter]
0	Policy Deployment Policy Deployment to FTD4100-5. Applied successfully	<u>47s</u>	×	
0	Policy Pre-Deployment Pre-deploy Device Configuration for FTD4100-5 success	35	×	
0	Policy Pre-Deployment Pre-deploy Global Configuration Generation success	4s	×	
0	High Availability HA pair has been broken successfully and all policies have been retained on active peer FTD4100-6. Standby peer FTD4100-5 policies are being deleted by an auto triggered deployment. Please allow this deployment to complete on FTD4100-5 before configuring its policies.	1m 59s	×	
	Remove completed tasks			

Étape 4. Vérifiez le résultat à partir de l'interface utilisateur graphique du FMC ou de l'interface de ligne de commande

Commande show running-config sur l'unité principale avant et après la rupture de la haute

disponibilité :

Unité principale/en veille avant la coupure HA	Unité principale après la coupure HA
> show running-config : enregistré	> INFO : cette unité est actuellement en veille. En désactivant le basculement, cette unité reste en veille.
: Numéro de série : FLM1949C5RR Matériel : FPR4K-SM-24, 73850 Mo de RAM, processeur Xeon série E5 200 MHz, 2 processeurs (48 coeurs)	> show running-config : enregistré : : Numéro de série : FLM1949C5RR
NGFW version 7.2.8 ! hostname puissance_feu	Matériel : FPR4K-SM-24, 73850 Mo de RAM, processeur Xeon série E5 200 MHz, 2 processeurs (48 coeurs)
enable password ***** chiffré strong-encryption-disable service-module 0 keepalive-timeout 4	: NGFW version 7.2.8 !
service-module 0 keepalive-counter 6 noms no mac-address auto	hostname puissance_feu enable password ***** chiffré strong-encryption-disable
! interface Port-channel2 sans nom	service-module 0 keepalive-counter 6 noms no mac-address auto
manuel de l'organisme de contrôle des transports aériens propagate sgt preserve-untag	! interface Port-channel2
stratégie statique sgt désactivée approuvée pas de niveau de sécurité pas d'adresse ip	snutdown sans nom pas de niveau de sécurité pas d'adresse ip
interface Port-channel2.202 vlan 202 nameif Extérieur	! interface Port-channel3 shutdown
manuel de l'organisme de contrôle des transports aériens propagate sgt preserve-untag	sans nom pas de niveau de sécurité pas d'adresse ip !
niveau de sécurité 0 adresse ip 192.168.76.10 255.255.255.0 standby 192.168.76.11	interface Ethernet1/1 de gestion seulement shutdown
! interface Port-channel3	pas de niveau de sécurité

description Interface de basculement	pas d'adresse ip
LAN/STATE	!
!	interface Ethernet1/4
interface Ethernet1/1	shutdown
de gestion seulement	sans nom
diagnostic de nameif	pas de niveau de sécurité
manuel de l'organisme de contrôle des	pas d'adresse ip
transports aériens	!
propagate sgt preserve-untag	ftp mode passive
stratégie statique sgt désactivée approuvée	ngips conn-match vlan-id
niveau de sécurité 0	object-group-search access-control
pas d'adresse ip	access-group CSM_FW_ACL_ global
!	access-list CSM_FW_ACL_ remark rule-id 9998
interface Ethernet1/4	: PREFILTER POLICY : politique de priorité et
nameif Inside	de tunnel par défaut
manuel de l'organisme de contrôle des	access-list CSM_FW_ACL_ remark rule-id 9998
transports aériens	: RULE : DEFAULT TUNNEL ACTION RULE
propagate sgt preserve-untag	access-list CSM_FW_ACL_ advanced permit ip
stratégie statique sgt désactivée approuvée	any rule-id 9998
niveau de sécurité 0	access-list CSM_FW_ACL_ advanced permit
adresse ip 192.168.75.10 255.255.255.0 standby	udp any eq 3544 any range 1025 65535 rule-id
192.168.75.11	9998
!	access-list CSM_FW_ACL_ advanced permit
ftp mode passive	udp any range 1025 65535 any eq 3544 rule-id
ngips conn-match vlan-id	9998
object-group-search access-control	access-list CSM_FW_ACL_ advanced permit 41
access-group CSM_FW_ACL_ global	any any rule-id 9998
access-list CSM_FW_ACL_ remark rule-id 9998 :	access-list CSM_FW_ACL_ advanced permit
PREFILTER POLICY : politique de priorité et de	gre any any rule-id 9998
tunnel par défaut	access-list CSM_FW_ACL_ remark rule-id
access-list CSM_FW_ACL_ remark rule-id 9998 :	268439552 : ACCESS POLICY : acp_simple -
RULE : DEFAULT TUNNEL ACTION RULE	Obligatoire
access-list CSM_FW_ACL_ advanced permit ip	access-list CSM_FW_ACL_ remark rule-id
any rule-id 9998	268439552 : L7 RULE : rule1
access-list CSM_FW_ACL_ advanced permit udp	access-list CSM_FW_ACL_ advanced permit ip
any eq 3544 any range 1025 65535 rule-id 9998	any rule-id 268439552
access-list CSM_FW_ACL_ advanced permit udp	!
any range 1025 65535 any eq 3544 rule-id 9998	tcp-map UM_STATIC_TCP_MAP
access-list CSM_FW_ACL_ advanced permit 41	tcp-options range 6 7 allow
any any rule-id 9998	tcp-options range 9 18 allow
access-list CSM_FW_ACL_ advanced permit gre	tcp-options range 20 255 allow
any any rule-id 9998	autorisation d'indicateur d'urgence
access-list CSM_FW_ACL_ remark rule-id	!
268434433 : POLITIQUE D'ACCÈS : acp_simple	pas de pager
- Par défaut	no logging message 106015
access-list CSM_FW_ACL_ remark rule-id	no logging message 313001

268434433 : L4 RULE : DEFAULT ACTION RULE access-list CSM_FW_ACL_ advanced permit ip any rule-id 268434433	no logging message 313008 no logging message 106023 no logging message 710003 no logging message 106100
	no logging message 302015
	no logging message 302014
tcp-options range 6 7 allow	no logging message 302013
tcp-options range 9 18 allow	no logging message 302018
tcp-options range 20 255 allow	no logging message 302017
autorisation d'indicateur d'urgence	no logging message 302016
<u>!</u>	no logging message 302021
pas de pager	no logging message 302020
no logging message 106015	pas de basculement
no logging message 313001	<résultat omis=""></résultat>
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 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=""></résultat>	
Unité secondaire/active avant la coupure HA	Unité secondaire après la coupure haute disponibilité

> show running-config : enregistré :	> show running-config : enregistré
: Numéro de série : FLM2108V9YG Matériel : FPR4K-SM-24, 73850 Mo de RAM, processeur Xeon série E5 200 MHz, 2 processeurs (48 coeurs) :	: : Numéro de série : FLM2108V9YG Matériel : FPR4K-SM-24, 73850 Mo de RAM, processeur Xeon série E5 200 MHz, 2 processeurs (48 coeurs)
NGFW version 7.2.8	: NGEW vorsion 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	<pre>INGFW Version 7.2.8 I hostname puissance_feu enable password ***** chiffré strong-encryption-disable service-module 0 keepalive-timeout 4 service-module 0 keepalive-counter 6 noms</pre>
	no mac-address auto
	! interface Port channel?
sans nom pas de niveau de sécurité	
pas d'adresse in	pas de niveau de sécurité
!	pas d'adresse ip
interface Port-channel2.202	!
vlan 202	interface Port-channel2.202
nameif Extérieur	vlan 202
manuel de l'organisme de contrôle des	nameif Extérieur
transports aériens	manuel de l'organisme de contrôle des
propagate sgt preserve-untag	transports aériens
stratégie statique sgt désactivée approuvée	propagate sgt preserve-untag
niveau de sécurité 0	stratégie statique sgt désactivée approuvée
adresse ip 192.168.76.10 255.255.255.0	Iniveau de securite U
standby 192.168.76.11	adresse Ip 192.168.76.10 255.255.255.0
interface Port-channel3	
description Interface de basculement	interface Port-channel3
LAN/STATE	sans nom
!	pas de niveau de sécurité
interface Ethernet1/1	pas d'adresse ip
de gestion seulement	!
diagnostic de nameif	interface Ethernet1/1
niveau de sécurité 0	de gestion seulement
pas d'adresse ip	diagnostic de nameif
!	niveau de sécurité 0

interface Ethernet1/4	pas d'adresse ip
nameif Inside	!
niveau de sécurité 0	interface Ethernet1/4
adresse ip 192.168.75.10 255.255.255.0	nameif Inside
standby 192.168.75.11	niveau de sécurité 0
!	adresse ip 192.168.75.10 255.255.255.0
ftp mode passive	standby 192.168.75.11
ngips conn-match vlan-id	!
object-group-search access-control	ftp mode passive
access-group CSM_FW_ACL_ global	ngips conn-match vlan-id
access-list CSM_FW_ACL_ remark rule-id 9998	object-group-search access-control
: PREFILTER POLICY : politique de priorité et	access-group CSM_FW_ACL_ global
de tunnel par défaut	access-list CSM_FW_ACL_ remark rule-id 9998
access-list CSM_FW_ACL_ remark rule-id 9998	: PREFILTER POLICY : politique de priorité et
: RULE : DEFAULT TUNNEL ACTION RULE	de tunnel par défaut
access-list CSM_FW_ACL_ advanced permit ip	access-list CSM_FW_ACL_ remark rule-id 9998
any rule-id 9998	: RULE : DEFAULT TUNNEL ACTION RULE
access-list CSM_FW_ACL_ advanced permit	access-list CSM_FW_ACL_ advanced permit ip
udp any eq 3544 any range 1025 65535 rule-id	any rule-id 9998
9998	access-list CSM_FW_ACL_ advanced permit
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
9998	access-list CSM_FW_ACL_ advanced permit
access-list CSM_FW_ACL_ advanced permit 41	udp any range 1025 65535 any eq 3544 rule-id
any any rule-id 9998	9998
access-list CSM_FW_ACL_ advanced permit gre	access-list CSM_FW_ACL_ advanced permit 41
any any rule-id 9998	any any rule-id 9998
access-list CSM_FW_ACL_ remark rule-id	access-list CSM_FW_ACL_ advanced permit gre
268439552 : ACCESS POLICY : acp_simple -	any any rule-id 9998
Obligatoire	access-list CSM_FW_ACL_ remark rule-id
access-list CSM_FW_ACL_ remark rule-id	268439552 : ACCESS POLICY : acp_simple -
268439552 : L7 RULE : rule1	Obligatoire
access-list CSM_FW_ACL_ advanced permit ip	access-list CSM_FW_ACL_ remark rule-id
any rule-id 268439552	268439552 : L7 RULE : rule1
!	access-list CSM_FW_ACL_ advanced permit ip
tcp-map UM_STATIC_TCP_MAP	any rule-id 268439552
tcp-options range 6 7 allow	!
tcp-options range 9 18 allow	tcp-map UM_STATIC_TCP_MAP
tcp-options range 20 255 allow	tcp-options range 6 7 allow
autorisation d'indicateur d'urgence	tcp-options range 9 18 allow
!	tcp-options range 20 255 allow
pas de pager	autorisation d'indicateur d'urgence
no logging message 106015	
no logging message 313001	pas de pager
no logging message 313008	no logging message 106015
no logging message 106023	no logging message 313001

no logging message 710003	no logging message 313008
no logging message 106100	no logging message 106023
no logging message 302015	no logging message 710003
no logging message 302014	no logging message 106100
no logging message 302013	no logging message 302015
no logging message 302018	no logging message 302014
no logging message 302017	no logging message 302013
no logging message 302016	no logging message 302018
no logging message 302021	no logging message 302017
no logging message 302020	no logging message 302016
mtu externe 1500	no logging message 302021
diagnostic mtu 1500	no logging message 302020
mtu Inside 1500	mtu externe 1500
basculement	diagnostic mtu 1500
failover lan unit secondary	mtu Inside 1500
failover lan interface FOVER Port-channel3	pas de basculement
réplication de basculement http	no monitor-interface Outside
liaison de basculement FOVER Port-channel3	no monitor-interface service-module
failover interface ip FOVER 172.16.51.1	
255.255.255.0 standby 172.16.51.2	<resultat omis=""></resultat>
<résultat omis=""></résultat>	

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 5. Une fois cette tâche terminée, recréez la paire à haute disponibilité.

Tâche 6. Supprimer 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/En veille
- Secondaire/actif

Exigence de la tâche :

À partir du FMC, supprimez la paire de basculement.

Solution :

Étape 1. Choisissez l'icône comme indiqué dans l'image :

FTD4120-HA High Availability							Switch Active Peer
FTD4100-5(Primary, Standby) Short 3 10.62.148.188 - Routed	Firepower 4120 with FTD	7.2.8	FP4100-5:443 Security Module - 1	Base, Threat (2 more)	acp_simple	45	Break Force refresh node status Delete
FTD4100-6(Secondary, Active) Snort 3 10.62.148.191 - Routed	Firepower 4120 with FTD	7.2.8	EP4100-6:443 Security Module - 1	Base, Threat (2 more)	acp_simple	45	Health Monitor Troubleshoot Files

Étape 2. Vérifiez la notification illustrée ci-dessous et confirmez-la:

Confirm Delete
Are you sure you want to delete the high availability, "FTD4120-HA"? Deleting the pair from the Firewall Management Center does not disable high availability at the device level. The devices will continue to operate as an Active/Standby pair until you disable high availability for each unit using the CLI: "configure high-availability disable"
No Yes

Étape 3. Une fois que vous avez supprimé la haute disponibilité, l'enregistrement des deux périphériques sur le FMC est annulé (ils sont supprimés).

Le résultat de la commande show running-config de la CLI LINA est conforme au tableau cidessous :

Unité principale (veille)	Unité secondaire (active)
> show running-config	> show running-config
: enregistré	: enregistré
:	:
: Numéro de série : FLM1949C5RR	: Numéro de série : FLM2108V9YG
Matériel : FPR4K-SM-24, 73853 Mo de RAM,	Matériel : FPR4K-SM-24, 73853 Mo de RAM,
processeur Xeon série E5 200 MHz, 2	processeur Xeon série E5 200 MHz, 2
processeurs (48 coeurs)	processeurs (48 coeurs)
NGFW version 7.2.8	NGFW version 7.2.8
!	!
nom_hôte Firepower-module1	nom_hôte Firepower-module1

	-
enable password ***** chiffré	enable password ***** chiffré
strong-encryption-disable	strong-encryption-disable
no asp inspect-dp ack-passtbrough	no asp inspect-dp ack-passtbrough
service-module 0 keepalive-timeout 4	service-module 0 keepaliye-timeout 4
service-module 0 keepalive-counter 6	service-module 0 keepalive-counter 6
noms	noms
no mac-address auto	no mac-address auto
!	<u>!</u>
interface Port-channel2	interface Port-channel2
sans nom	sans nom
pas de niveau de sécurité	pas de niveau de sécurité
pas d'adresse ip	pas d'adresse ip
!	
interface Port-channel2.202	interface Port-channel2.202
vlan 202	vlan 202
nameif NET202	nameif NET202
manuel de l'organisme de contrôle des	manuel de l'organisme de contrôle des
transports aériens	transports aériens
propagate sgt preserve-untag	propagate sgt preserve-untag
stratégie statique sgt désactivée approuvée	stratégie statique sgt désactivée approuvée
niveau de sécurité 0	niveau de sécurité 0
adresse ip 172.16.202.1 255.255.255.0 standby	adresse ip 172.16.202.1 255.255.255.0 standby
172.16.202.2	172.16.202.2
!	!
interface Port-channel2.203	interface Port-channel2.203
vlan 203	vlan 203
nameif NET203	nameif NET203
manuel de l'organisme de contrôle des	manuel de l'organisme de contrôle des
transports aériens	transports aériens
propagate sgt preserve-untag	propagate sgt preserve-untag
stratégie statique sgt désactivée approuvée	stratégie statique sgt désactivée approuvée
niveau de sécurité 0	niveau de sécurité 0
adresse ip 1/2.16.203.1 255.255.255.0 standby	adresse ip 1/2.16.203.1 255.255.255.0 standby
172.16.203.2	172.16.203.2
interface Port-channel3	interface Port-channel3
description Interface de basculement	description Interface de basculement
LAN/STATE	LAN/STATE
!	!
interface Ethernet1/1	interface Ethernet1/1
de gestion seulement	de gestion seulement
diagnostic de nameif	diagnostic de nameif
manuel de l'organisme de contrôle des	manuel de l'organisme de contrôle des
transports aériens	transports aériens
propagate sgt preserve-untag	propagate sgt preserve-untag

stratégie statique sgt désactivée approuvée	stratégie statique sgt désactivée approuvée
niveau de sécurité 0	niveau de sécurité 0
pas d'adresse ip	pas d'adresse ip
!	!
interface Ethernet1/4	interface Ethernet1/4
nameif NET204	nameif NET204
manuel de l'organisme de contrôle des	manuel de l'organisme de contrôle des
transports aeriens	transports aeriens
propagate sgt preserve-untag	propagate sgt preserve-untag
strategie statique sgt desactivee approuvee	strategie statique sgt desactivee approuvee
niveau de securite U	niveau de securite U
adresse ip 172.16.204.1 255.255.255.0 standby	adresse ip 172.10.204.1 255.255.255.0 standby
172.10.204.2	172.10.204.2
! ftp mode peoplike	! ftp mode possive
ngins conn-match vlan-id	ngins conn-match vlan-id
ng object_group_search access_control	ngips committee wanted
access-group CSM FW ACL global	access-group CSM EW ACL global
access-list CSM_EW_ACIremark rule-id 9998	access-list CSM_EW_ACL_remark rule-id 9998
· PREFILTER POLICY · politique de priorité et	· PREFILTER POLICY · politique de priorité et
de tunnel par défaut	de tunnel par défaut
access-list CSM FW ACL remark rule-id 9998	access-list CSM FW ACL remark rule-id 9998
: RULE : DEFAULT TUNNEL ACTION RULE	: RULE : DEFAULT TUNNEL ACTION RULE
access-list CSM_FW_ACL_ advanced permit ip	access-list CSM_FW_ACL_ advanced permit ip
any rule-id 9998	any rule-id 9998
access-list CSM_FW_ACL_ advanced permit	access-list CSM_FW_ACL_ advanced permit
udp any eq 3544 any range 1025 65535 rule-id	udp any eq 3544 any range 1025 65535 rule-id
9998	9998
access-list CSM_FW_ACL_ advanced permit	access-list CSM_FW_ACL_ advanced permit
udp any range 1025 65535 any eq 3544 rule-id 9998	udp any range 1025 65535 any eq 3544 rule-id 9998
access-list CSM_FW_ACL_ advanced permit 41	access-list CSM_FW_ACL_ advanced permit 41
any any rule-id 9998	any any rule-id 9998
access-list CSM_FW_ACL_ advanced permit gre	access-list CSM_FW_ACL_ advanced permit gre
any any rule-id 9998	any any rule-id 9998
access-list CSM_FW_ACL_ remark rule-id	access-list CSM_FW_ACL_ remark rule-id
268434433 : POLITIQUE D'ACCÈS :	268434433 : POLITIQUE D'ACCÈS :
acp_simple - Par défaut	acp_simple - Par défaut
access-list CSM_FW_ACL_ remark rule-id	access-list CSM_FW_ACL_ remark rule-id
268434433 : L4 RULE : DEFAULT ACTION	268434433 : L4 RULE : DEFAULT ACTION
RULE	RULE
access-list CSM_FW_ACL_ advanced permit ip	access-list CSM_FW_ACL_ advanced permit ip
any rule-id 268434433	any rule-id 268434433
tcp-map UM_STATIC_TCP_MAP	tcp-map UM_STATIC_TCP_MAP
tcp-options range 6 / allow	tcp-options range 6 / allow

tcp-options range 9 18 allow	tcp-options range 9 18 allow
tcp-options range 20 255 allow	tcp-options range 20 255 allow
tcp-options md5 clear	tcp-options md5 clear
autorisation d'indicateur d'urgence	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 302015 no logging message 302015 no logging message 302014 no logging message 302018 no logging message 302017 no logging message 302016 no logging message 302021	! 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 302015 no logging message 302014 no logging message 302018 no logging message 302017 no logging message 302016 no logging message 302021
no logging message 302021	no logging message 302021
no logging message 302020	no logging message 302020
mtu NET202 1500	mtu NET202 1500
mtu NET203 1500	mtu NET203 1500
diagnostic mtu 1500	diagnostic mtu 1500
mtu NET204 1500	mtu NET204 1500
basculement	basculement
failover lan unit primary	failover lan unit secondary
failover lan interface FOVER Port-channel3	failover lan interface FOVER Port-channel3
réplication de basculement http	réplication de basculement http
liaison de basculement FOVER Port-channel3	liaison de basculement FOVER Port-channel3
failover interface ip FOVER 172.16.51.1	failover interface ip FOVER 172.16.51.1
255.255.255.0 standby 172.16.51.2	255.255.255.0 standby 172.16.51.2
interface-moniteur NET202	interface-moniteur NET202
NET203 interface-moniteur	NET203 interface-moniteur
icmp unreachable rate-limit 1 burst-size 1	icmp unreachable rate-limit 1 burst-size 1
<resultat omis=""></resultat>	<resultat omis=""></resultat>
> show ip	> show ip
Adresses IP système :	Adresses IP système :
Nom d'interface Adresse IP Masque de sous-	Nom d'interface Adresse IP Masque de sous-
réseau Méthode	réseau Méthode
Port-channel2.202 NET202 172.16.202.1	Port-channel2.202 NET202 172.16.202.1
255.255.255.0 CONFIG	255.255.255.0 CONFIG
Port-channel2.203 NET203 172.16.203.1	Port-channel2.203 NET203 172.16.203.1
255.255.255.0 CONFIG	255.255.255.0 CONFIG

Т

Γ

Port-channel3 FOVER 172.16.51.1	Port-channel3 FOVER 172.16.51.1
255.255.255.0 unset	255.255.255.0 unset
CONFIGURATION D'Ethernet1/4 NET204	CONFIGURATION D'Ethernet1/4 NET204
172.16.204.1 255.255.255.0	172.16.204.1 255.255.255.0
Adresses IP actuelles :	Adresses IP actuelles :
Nom d'interface Adresse IP Masque de sous-	Nom d'interface Adresse IP Masque de sous-
réseau Méthode	réseau Méthode
Port-channel2.202 NET202 172.16.202.2	Port-channel2.202 NET202 172.16.202.1
255.255.255.0 CONFIG	255.255.255.0 CONFIG
Port-channel2.203 NET203 172.16.203.2	Port-channel2.203 NET203 172.16.203.1
255.255.255.0 CONFIG	255.255.255.0 CONFIG
Port-channel3 FOVER 172.16.51.1	Port-channel3 FOVER 172.16.51.2
255.255.255.0 unset	255.255.255.0 unset
CONFIGURATION D'Ethernet1/4 NET204	CONFIGURATION D'Ethernet1/4 NET204
172.16.204.2 255.255.255.0	172.16.204.1 255.255.255.0
 > show failover Basculement activé Unité de basculement principale Interface LAN de basculement : FOVER Port-	 > 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	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 15 secondes Fréquence d'interrogation d'interface 5
secondes, durée de conservation 25 secondes Politique d'interface 1 Interfaces surveillées 4 sur 1291 maximum Interfaces MAC non défini réplication de basculement http Version : Notre 9.18(4)210, Mate 9.18(4)210 Numéro de série : Ours FLM1949C5RR, Mate FLM2108V9YG Dernier basculement à : 13:56:37 UTC Jul 16 2024	secondes, durée de conservation 25 secondes Politique d'interface 1 Interfaces surveillées 4 sur 1291 maximum Interfaces MAC non défini réplication de basculement http Version : Notre 9.18(4)210, Mate 9.18(4)210 Numéro de série : Ours FLM2108V9YG, Mate FLM1949C5RR Dernier basculement à : 13:42:35 UTC Jul 16 2024
Cet hôte : Principal - Prêt pour la veille	Cet hôte : secondaire - actif
Durée active : 0 (s)	Durée active : 70312 (s)
logement 0 : état UCSB-B200-M3-U hw/sw rev	logement 0 : état UCSB-B200-M3-U hw/sw rev
(0.0/9.18(4)210) (Up Sys)	(0.0/9.18(4)210) (Up Sys)
Interface NET202 (172.16.202.2) : normale	Interface NET202 (172.16.202.1) : normale
(surveillée)	(surveillée)
Interface NET203 (172.16.203.2) : normale	Interface NET203 (172.16.203.1) : normale
(surveillée)	(surveillée)
Diagnostic de l'interface (0.0.0.0) : Normal (En	Diagnostic de l'interface (0.0.0.0) : Normal (En
attente)	attente)

Т

Interface NET204 (172.16.204.2) : normale	Interface NET204 (172.16.204.1) : normale
(surveillée)	(surveillée)
logement 1 : état snort rev (1.0) (up)	logement 1 : état snort rev (1.0) (up)
logement 2 : diskstatus rev (1.0) status (up)	logement 2 : diskstatus rev (1.0) status (up)
Autre hôte : secondaire - actif	Autre hôte : principal - Prêt pour la veille
Durée active : 70293 (s)	Durée active : 0 (s)
Interface NET202 (172.16.202.1) : normale	logement 0 : état UCSB-B200-M3-U hw/sw rev
(surveillée)	(0.0/9.18(4)210) (Up Sys)
Interface NET203 (172.16.203.1) : normale	Interface NET202 (172.16.202.2) : normale
(surveillée)	(surveillée)
Diagnostic de l'interface (0.0.0.0) : Normal (En	Interface NET203 (172.16.203.2) : normale
attente)	(surveillée)
Interface NET204 (172.16.204.1) : normale	Diagnostic de l'interface (0.0.0.0) : Normal (En
(surveillée)	attente)
logement 1 : état snort rev (1.0) (up)	Interface NET204 (172.16.204.2) : normale
logement 2 : diskstatus rev (1.0) status (up)	(surveillée)
	logement 1 : état snort rev (1.0) (up)
<resultat omis=""></resultat>	logement 2 : diskstatus rev (1.0) status (up)
	<resultat omis=""></resultat>

Étape 4. L'enregistrement des deux périphériques FTD sur le FMC a été annulé :

<#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.	Le périphérique est retiré du FMC.
Aucune configuration n'est supprimée du périphérique FTD.	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 :

>

configure high-availability disable

?

Optional parameter to clear interfaces (clear-interfaces) optional parameter to clear interfaces (clear <<r>

<#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 Failover unit Secondary
	Failover LAN Interface: not Configured Reconnect timeout 0:00:00 Unit Poll frequency 1 seconds, holdtime 15
> show failover Failover Off (pseudo-Standby) Failover unit Primary	seconds Interface Poll frequency 5 seconds, holdtime 25 seconds
Failover LAN Interface: FOVER Port-channel3 (up) Reconnect timeout 0:00:00 Unit Poll frequency 1 seconds, holdtime 15	Interface Policy 1 Monitored Interfaces 4 of 1291 maximum MAC Address Move Notification Interval not set
Interface Poll frequency 5 seconds, holdtime 25 seconds	> show in
Interface Policy 1	System IP Addresses:
Monitored Interfaces 0 of 1291 maximum	Interface Name IP address Subnet mask Method
MAC Address Move Notification Interval not set	Port-channel2.202 NET202 172.16.202.1
failover replication http	255.255.255.0 CONFIG
	Port-channel2.203 NET203 172.16.203.1
> show ip System IP Addresses:	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	Interface Name IP address Subnet mask Method
Port-channel3 FOVER 172.16.51.1 255.255.255.0	Port-channel2.202 NET202 172.16.202.1
unset	255.255.255.0 CONFIG
Current IP Addresses:	Port-channel2.203 NET203 172.16.203.1
Interface Name IP address Subnet mask Method	255.255.255.0 CONFIG
Port-channel3 FOVER 172.16.51.1 255.255.255.0	Ethernet1/4 NET204 172.16.204.1 255.255.255.0
unset	CONFIG
Principal (hors veille)	Secondaire (ex-actif)
> show running-config	> show running-config
: enregistré	: enregistré
:	:
: Numéro de série : FLM1949C5RR	: Numéro de série : FLM2108V9YG
Matériel : FPR4K-SM-24, 73853 Mo de RAM,	Matériel : FPR4K-SM-24, 73853 Mo de RAM,
processeur Xeon série E5 200 MHz, 2	processeur Xeon série E5 200 MHz, 2
processeurs (48 coeurs)	processeurs (48 coeurs)
NGFW version 7.2.8	NGFW version 7.2.8
!	!
nom_hôte Firepower-module1	nom_hôte Firepower-module1
enable password ***** chiffré	enable password ***** chiffré
strong-encryption-disable	strong-encryption-disable
no asp inspect-dp ack-passthrough	no asp inspect-dp ack-passthrough
service-module 0 keepalive-timeout 4	service-module 0 keepalive-timeout 4
service-module 0 keepalive-counter 6	service-module 0 keepalive-counter 6
noms	noms
no mac-address auto	no mac-address auto
<pre>! 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 LANUSTATE</pre>	! 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
interface Ethernet1/1 de gestion seulement	propagate sgt preserve-untag stratégie statique sgt désactivée approuvée niveau de sécurité 0

shutdown	adresse ip 172.16.202.1 255.255.255.0 standby
sans nom	172.16.202.2
pas de niveau de sécurité	!
pas d'adresse ip	interface Port-channel2.203
!	vlan 203
interface Ethernet1/4	nameif NET203
shutdown	manuel de l'organisme de contrôle des
sans nom	transports aériens
pas de niveau de sécurité	propagate sgt preserve-untag
pas d'adresse ip	stratégie statique sgt désactivée approuvée
!	niveau de sécurité 0
ftp mode passive	adresse ip 172.16.203.1 255.255.255.0 standby
ngips conn-match vlan-id	172.16.203.2
no object-group-search access-control	!
access-group CSM_FW_ACL_ global	interface Port-channel3
access-list CSM_FW_ACL_ remark rule-id 9998	sans nom
: PREFILTER POLICY : politique de priorité et	pas de niveau de sécurité
de tunnel par défaut	pas d'adresse ip
access-list CSM_FW_ACL_ remark rule-id 9998	!
: RULE : DEFAULT TUNNEL ACTION RULE	interface Ethernet1/1
access-list CSM_FW_ACL_ advanced permit ip	de gestion seulement
any rule-id 9998	diagnostic de nameif
access-list CSM_FW_ACL_ advanced permit	manuel de l'organisme de contrôle des
udp any eq 3544 any range 1025 65535 rule-id	transports aériens
9998	propagate sqt preserve-untag
access-list CSM FW ACL advanced permit	stratégie statigue sqt désactivée approuvée
udp any range 1025 65535 any eg 3544 rule-id	niveau de sécurité 0
9998	pas d'adresse ip
access-list CSM FW ACL advanced permit 41	· · · ·
any any rule-id 9998	interface Ethernet1/4
access-list CSM FW ACL advanced permit gre	nameif NET204
anv anv rule-id 9998	manuel de l'organisme de contrôle des
access-list CSM FW ACL remark rule-id	Itransports aériens
268434433 : POLITIQUE D'ACCÈS :	propagate sot preserve-untag
acp simple - Par défaut	stratégie statigue sot désactivée approuvée
access-list CSM_FW_ACL_remark rule-id	niveau de sécurité 0
268434433 · I 4 RULE · DEFAULT ACTION	adresse in 172 16 204 1 255 255 255 0 standby
RUIF	172 16 204 2
access-list CSM_EW_ACL_advanced permit in	1
any rule-id 268434433	' Iftp mode passive
	ngips conn-match vlan-id
r tcp-map LIM_STATIC_TCP_MAP	no object-group-search access-control
tcp-options range 6 7 allow	access-group CSM FW ACL global
tcp-options range 9 18 allow	access-list CSM_FW_ACIremark rule_id 9998
tcp-options range 20 255 allow	· PREFILTER POLICY · nolitique de priorité et
tcn-ontions md5 clear	de tunnel nar défaut

autorisation d'indicateur d'urgence	access-list CSM_FW_ACL_ remark rule-id 9998
!	: RULE : DEFAULT TUNNEL ACTION RULE
pas de pager	access-list CSM_FW_ACL_ advanced permit ip
no logging message 106015	any rule-id 9998
no logging message 313001	access-list CSM_FW_ACL_ advanced permit
no logging message 313008	udp any eq 3544 any range 1025 65535 rule-id
no logging message 106023	9998
no logging message 710003	access-list CSM_FW_ACL_ advanced permit
no logging message 106100	udp any range 1025 65535 any eq 3544 rule-id
no logging message 302015	9998
no logging message 302014	access-list CSM_FW_ACL_ advanced permit 41
no logging message 302013	any any rule-id 9998
no logging message 302018	access-list CSM_FW_ACL_ advanced permit gre
no logging message 302017	any any rule-id 9998
no logging message 302016	access-list CSM FW ACL remark rule-id
no logging message 302021	268434433 : POLITIQUE D'ACCÈS :
no logging message 302020	acp_simple - Par défaut
pas de basculement	access-list CSM FW ACL remark rule-id
failover lan unit primary	268434433 : L4 RULE : DEFAULT ACTION
failover lan interface FOVER Port-channel3	RULE
réplication de basculement http	access-list CSM FW ACL advanced permit ip
liaison de basculement FOVER Port-channel3	any rule-id 268434433
failover interface ip FOVER 172.16.51.1	!
255.255.255.0 standby 172.16.51.2	tcp-map UM_STATIC_TCP_MAP
no monitor-interface service-module	tcp-options range 6 7 allow
	tcp-options range 9 18 allow
<résultat omis=""></résultat>	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 la désactivation de la haute disponibilité à partir de l'ILC 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 également désactiver la haute disponibilité sur l'unité ex-Standby.

Scénario 2 (non recommandé)

Avertissement : ce scénario mène à une situation active/active, il n'est donc 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)
Principal (hors veille) > show failover Basculement désactivé Unité de basculement secondaire Interface LAN de basculement : non configurée 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 Adresses IP actuelles : Nom d'interface Adresse IP Masque de sous- réseau Méthode Port-channel2.202 NET202 172.16.204.1 255.255.255.0 Adresses IP actuelles : Nom d'interface Adresse IP Masque de sous- réseau Méthode Port-channel2.203 NET203 172.16.203.1 255.255.255.0 Manuel Port-channel2.203 NET203 172.16.203.1 255.255.255.0 Manuel d'Ethernet1/4 NET204 172.16.204.1 255.255.255.0 Manuel Manuel d'Ethernet1/4 NET204 172.16.204.1 255.255.255.0	Secondaire (actif) > show failover 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 : Ours FLM2108V9YG, Mate FLM1949C5RR Dernier basculement à : 12:44:06 UTC Jul 17 2024 Cet hôte : secondaire - actif Durée active : 632 (s) logement 0 : état UCSB-B200-M3-U hw/sw rev (0.0/9.18(4)210) (Up Sys) Diagnostic de l'interface (0.0.0.0) : Normal (En attente) Interface NET204 (172.16.203.1) : normale (surveillée) Interface NET202 (172.16.202.1) : normale (surveillée) Interface NET203 (172.16.203.1) : normale (surveillée) Interface NET203 (172.16.203.1) : normale (surveillée) Interface NET202 (172.16.202.1) : normale (surveillée) Interface NET202 (172.16.202.1) : normale (surveillée) Interface NET203 (172.16.203.1) : normale (surveillée) Interface NET203 (172.16.203.1) : normale (surveillée) Interface NET203 (172.16.203.1) : normale (surveillée) Interface NET202 (172.16.202.1) : normale (surveillée) Interface NET203 (172.16.203.1) : normale (surveillée) Interface NET203 (172.
	attente)

Interface NET204 (172.16.204.2) : inconnue
(surveillée)
Interface NET203 (172.16.203.2) : inconnue
(surveillée)
Interface NET202 (172.16.202.2) : inconnue
(surveillée)
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 1/2.16.51.1
255.255.255.0 unset
Manuel d'Ethernet1/4 NE1204 1/2.16.204.1
255.255.255.0
Adresses IP actuelles :
Nom d'interface Adresse IP Masque de sous-
Port-channel2.202 NET202 172.16.202.1
255.255.255.0 manuel
Port-channel2.203 NET203 172.16.203.1
200.200.200.0 manuel Dort channel 2 EOV/ED 172.16.51.2
255 255 255 0 upget
200.200.200.0 UIISEL Manual d'Ethornat1/4 NET204 472 46 204 4
NIAHUELU EULEHIELI/4 NET204 1/2.10.204.1
200.200.200.0

Principaux points à noter pour la désactivation de la haute disponibilité à partir de l'ILC FTD active :

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

mêmes adresses IP que	l'unité active
l'ancienne unité en veille	

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

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

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

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 configurée 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 : Ours FLM2108V9YG, Mate FLM1949C5RR Dernier basculement à : 07:06:56 UTC 18 juillet 2024 Cet hôte : secondaire - actif Durée active : 1 194 (s) logement 0 : état UCSB-B200-M3-U hw/sw rev (0.0/9.18(4)210) (Up Sys) Diagnostic de l'interface (0.0.0.0) : Normal (En attente) Interface NET204 (172.16.204.1) : normale (surveillée) Interface NET203 (172.16.203.1) : normale (surveillée) Interface NET204 (172.16.204.2) : inconnu (en attente) Interface NET204 (172.16.204.2) : inconnue

(surveillée)
Interface NET202 (172.16.202.2) : inconnue
(surveillée)
Interface NET203 (172.16.203.2) : inconnue
(surveillée)
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 la désactivation de la haute disponibilité avec les interfaces clearinterfaces 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 la tâche terminée, enregistrez les périphériques sur le FMC et activez la paire à

haute disponibilité.

Tâche 7. Suspendre la haute disponibilité

Exigence de la tâche :

Suspendez la haute disponibilité la CLI CLISH du FTD.

Solution :

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

<#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. Vérifiez les modifications sur 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. Le 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. Réactivez la haute disponibilité sur l'unité principale :

<#root>

>

configure high-availability resume

Successfully resumed high-availablity.

> .

>

<#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. Résultat sur l'unité secondaire après la réactivation 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)

Lorsque la configuration est répliquée, est-elle enregistrée immédiatement (ligne par ligne) ou à la fin de la réplication ?

À la fin de la duplication. 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: 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_ line 1510 remark rule-id 268442077: L7
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_ line 1510 remark rule-id 268440577: L7
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: ACC
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: no access-list CSM_FW_ACL_ line 1510 remark rule-id 268440577: L4
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 <--</pre>
```

Que se passe-t-il si une unité est dans un état pseudo-veille (basculement désactivé) et que vous la rechargez alors que l'autre unité est activée et active ?

Vous vous retrouvez dans un scénario Actif/Actif (bien que techniquement il s'agisse d'un scénario Actif/Basculement désactivé). Plus précisément, une fois l'unité sous tension, le basculement est désactivé, mais l'unité utilise les mêmes adresses IP que l'unité active. Donc, dans les faits, vous avez :

- Unité-1 : active
- Unit-2 : le basculement est désactivé. L'unité utilise les mêmes adresses IP de données que l'unité 1, mais des adresses MAC différentes.

Qu'arrive-t-il à la configuration du basculement si vous désactivez manuellement le basculement (configurez la suspension haute disponibilité), puis rechargez le périphérique ? Lorsque vous désactivez le basculement, il ne s'agit pas d'une modification permanente (qui n'est pas enregistrée dans la configuration initiale, sauf si vous décidez de le faire explicitement). Vous pouvez redémarrer/recharger l'unité de 2 façons différentes et avec la deuxième façon, vous devez être prudent :

Cas 1 . Redémarrer à partir de CLISH

Le redémarrage à partir de CLISH ne demande pas de confirmation. Ainsi, la modification de la 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 est passée à l'état pseudo-veille comme prévu afin d'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 192.0.2.1 255.255.0 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 . Redémarrer à partir de la CLI LINA

Le redémarrage à partir de LINA (commande reload) demande une confirmation. Par conséquent, si vous sélectionnez Y (Yes), la modification de configuration est enregistrée dans startup-config :

```
<#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

• Vous trouverez ici toutes les versions du guide de configuration de Cisco Firepower Management Center.

Navigation dans la documentation de Cisco Secure Firewall Threat Defense

• Vous trouverez ici toutes les versions des guides de configuration du gestionnaire de châssis FXOS et de la 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 :

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

Pour toutes les notes techniques de configuration et de dépannage relatives aux technologies Firepower

Cisco Secure Firewall Management Center

<u>Assistance et documentation techniques - Cisco Systems</u>

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.