Configuration de la haute disponibilité multiinstance FTD sur Firepower 4100

Table des matières

Conditions préalables Exigences Composants utilisés Informations générales Diagramme du réseau Configurations Étape 1. Pré-configuration des interfaces Étape 2. Ajoutez 2 profils de ressources pour les instances de conteneur. Étape 3. (Facultatif) Ajoutez un préfixe de pool MAC d'adresse MAC virtuelle pour les interfaces d'instance de conteneur. Étape 5. Configuration des interfaces Étape 6. Ajoutez Une Paire Haute Disponibilité Pour Chaque Instance. Vérifier Dépannage Référence	Introduction
Exigences Composants utilisés Informations générales Diagramme du réseau Composants utilisés Étape 1. Pré-configuration des interfaces Étape 2. Ajoutez 2 profils de ressources pour les instances de conteneur. Étape 3. (Facultatif) Ajoutez un préfixe de pool MAC d'adresse MAC virtuelle pour les interfaces d'instance de conteneur. Étape 4. Ajouter une instance autonome. Étape 5. Configuration des interfaces Étape 6. Ajoutez Une Paire Haute Disponibilité Pour Chaque Instance. Vérifier Depannage Référence	Conditions préalables
Composants utilisés Informations générales Diagramme du réseau Composants utilisés gitage 1. Pré-configuration des interfaces Étape 1. Pré-configuration des interfaces Étape 2. Ajoutez 2 profils de ressources pour les instances de conteneur. Étape 3. (Facultatif) Ajoutez un préfixe de pool MAC d'adresse MAC virtuelle pour les interfaces d'instance de conteneur. Étape 5. Configuration des interfaces Étape 6. Ajoutez Une Paire Haute Disponibilité Pour Chaque Instance. Vérifier Dépannage Référence	Exigences
Informations générales Diagramme du réseau Configurations Étape 1. Pré-configuration des interfaces Étape 2. Ajoutez 2 profils de ressources pour les instances de conteneur. Étape 3. (Facultatif) Ajoutez un préfixe de pool MAC d'adresse MAC virtuelle pour les interfaces d'instance de conteneur. Étape 4. Ajouter une instance autonome. Étape 5. Configuration des interfaces Étape 6. Ajoutez Une Paire Haute Disponibilité Pour Chaque Instance. Vérifier Dépannage Référence	Composants utilisés
Diagramme du réseau Configurations Étape 1. Pré-configuration des interfaces Étape 2. Ajoutez 2 profils de ressources pour les instances de conteneur. Étape 3. (Facultatif) Ajoutez un préfixe de pool MAC d'adresse MAC virtuelle pour les interfaces d'instance de conteneur. Étape 4. Ajouter une instance autonome. Étape 5. Configuration des interfaces Étape 6. Ajoutez Une Paire Haute Disponibilité Pour Chaque Instance. Vérifier Dépannage Référence	Informations générales
Configurations Étape 1. Pré-configuration des interfaces Étape 2. Ajoutez 2 profils de ressources pour les instances de conteneur. Étape 3. (Facultatif) Ajoutez un préfixe de pool MAC d'adresse MAC virtuelle pour les interfaces d'instance de conteneur. Étape 4. Ajouter une instance autonome. Étape 5. Configuration des interfaces Étape 6. Ajoutez Une Paire Haute Disponibilité Pour Chaque Instance. Vérifier Dépannage Référence	Diagramme du réseau
Étape 1. Pré-configuration des interfaces Étape 2. Ajoutez 2 profils de ressources pour les instances de conteneur. Étape 3. (Facultatif) Ajoutez un préfixe de pool MAC d'adresse MAC virtuelle pour les interfaces d'instance de conteneur. Étape 4. Ajouter une instance autonome. Étape 5. Configuration des interfaces Étape 6. Ajoutez Une Paire Haute Disponibilité Pour Chaque Instance. Vérifier Dépannage Référence	Configurations
Étape 2. Ajoutez 2 profils de ressources pour les instances de conteneur. Étape 3. (Facultatif) Ajoutez un préfixe de pool MAC d'adresse MAC virtuelle pour les interfaces d'instance de conteneur. Étape 4. Ajouter une instance autonome. Étape 5. Configuration des interfaces Étape 6. Ajoutez Une Paire Haute Disponibilité Pour Chaque Instance. Vérifier Dépannage Référence	Étape 1. Pré-configuration des interfaces
<u>Étape 3. (Facultatif) Ajoutez un préfixe de pool MAC d'adresse MAC virtuelle pour les interfaces</u> d'instance de conteneur. <u>Étape 4. Ajouter une instance autonome.</u> <u>Étape 5. Configuration des interfaces</u> <u>Étape 6. Ajoutez Une Paire Haute Disponibilité Pour Chaque Instance.</u> <u>Vérifier</u> <u>Dépannage</u> <u>Référence</u>	Étape 2. Ajoutez 2 profils de ressources pour les instances de conteneur.
Étape 4. Ajouter une instance autonome. Étape 5. Configuration des interfaces Étape 6. Ajoutez Une Paire Haute Disponibilité Pour Chaque Instance. Vérifier Dépannage Référence	Étape 3. (Facultatif) Ajoutez un préfixe de pool MAC d'adresse MAC virtuelle pour les interfaces d'instance de conteneur.
<u>Étape 5. Configuration des interfaces</u> <u>Étape 6. Ajoutez Une Paire Haute Disponibilité Pour Chaque Instance.</u> <u>Vérifier</u> <u>Dépannage</u> <u>Référence</u>	Étape 4. Ajouter une instance autonome.
Étape 6. Ajoutez Une Paire Haute Disponibilité Pour Chaque Instance. Vérifier Dépannage Référence	Étape 5. Configuration des interfaces
<u>Vérifier</u> Dépannage Référence	Étape 6. Ajoutez Une Paire Haute Disponibilité Pour Chaque Instance.
Dépannage Référence	Vérifier
Référence	<u>Dépannage</u>
	Référence

Introduction

Ce document décrit comment configurer le basculement dans les instances de conteneur FTD (multi-instance).

Conditions préalables

Exigences

Cisco vous recommande de connaître Firepower Management Center et Firewall Threat Defense.

Composants utilisés

Cisco Firepower Management Center Virtual 7.2.5 Périphérique de pare-feu de nouvelle génération Cisco Firepower 4145 (FTD) 7.2.5 Système d'exploitation extensible Firepower (FXOS) 2.12 (0.498) Windows 10

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.

Avant de déployer FTD Multi-Instance, il est important de comprendre l'impact que cela peut avoir sur les performances de votre système et de planifier en conséquence. Reportez-vous toujours à la documentation officielle de Cisco ou consultez un représentant technique Cisco pour garantir un déploiement et une configuration optimaux.

Informations générales

Multi-Instance est une fonctionnalité de Firepower Threat Defense (FTD) qui est similaire au mode de contexte multiple ASA. Il vous permet d'exécuter plusieurs instances de conteneur distinctes de FTD sur un seul composant matériel. Chaque instance de conteneur permet une séparation des ressources matérielles, une gestion de la configuration séparée, des rechargements séparés, des mises à jour logicielles distinctes et une prise en charge complète des fonctions de défense contre les menaces. Cela est particulièrement utile pour les entreprises qui ont besoin de politiques de sécurité différentes pour différents services ou projets, mais qui ne souhaitent pas investir dans plusieurs appliances matérielles distinctes. La fonctionnalité Multi-Instance est actuellement prise en charge sur les appliances de sécurité des gammes Firepower 4100 et 9300 exécutant FTD 6.4 et versions ultérieures.

Ce document utilise Firepower4145 qui prend en charge un maximum de 14 instances de conteneur. Pour connaître le nombre maximal d'instances prises en charge dans l'appliance Firepower, veuillez vous reporter à <u>Nombre maximal d'instances de conteneur et ressources par modèle.</u>

Diagramme du réseau

Ce document présente la configuration et la vérification de la haute disponibilité dans Multi-Instance sur ce schéma.



Diagramme de configuration logique



Schéma de configuration physique

Configurations

Étape 1. Pré-configuration des interfaces

a. Accédez à Interfaces sur FCM. Définissez 2 interfaces de gestion. Dans cet exemple, Ethernet1/3 et Ethernet1/7.

Overview Interfac	Logical Devices	Security Engine	Platform Settings						Syste	m Tools Help	o admin
			Network Module 1								
All Interfaces Hardwa	are Bypass									1 Ober	
Interface	Туре	Admin Speed	Operational Speed	Instances	VLAN	Admin Duplex	Auto Negotiation	Operation State	Admin State	riter.	
М мбмт	Management										
Port-channel48	cluster	10gbps	indeterminate			Full Duplex	no	admin-down		J 🗊	
Ethernet1/1	data	1gbps	lgbps			Full Duplex	yes	up		ø	
Ethernet1/2	data	1gbps	lgbps			Full Duplex	yes	up	\frown	ø	
Ethernet1/3	mgmt	lgbps	lgbps			Full Duplex	yes	up	$\overline{}$	ø	
Ethernet1/4	data	1gbps	1gbps			Full Duplex	yes	up	$\overline{}$	ø	
Ethernet1/5	data	1gbps	lgbps			Full Duplex	yes	up	\frown	ø	
Ethernet1/6	data	1gbps	lgbps			Full Duplex	yes	up	\frown	ø	
Ethernet1/7	mgmt	1gbps	lgbps			Full Duplex	yes	up		ø	
Ethernet1/8	data	1gbps	lgbps			Full Duplex	yes	up		Ø	

Pré-configuration des interfaces

Étape 2. Ajoutez 2 profils de ressources pour les instances de conteneur.

a. Accédez à Platform Settings > Resource Profiles > Add on FCM. Définissez le 1er profil de ressource.

Dans cet exemple : ·Nom : Instance01 · Nombre de coeurs : 10



Remarque : pour la haute disponibilité d'une paire d'instances de conteneur, ils doivent utiliser les mêmes attributs de profil de ressource.

Définissez le nom du profil entre 1 et 64 caractères. Notez que vous ne pouvez pas modifier le nom de ce profil après l'avoir ajouté.

Définissez le nombre de coeurs pour le profil, entre 6 et le maximum.

Overview Interfaces Logi	cal Devices Security Engine Platfe	orm Settings			System Tools Help admin
NTP SSH				Add	
SNMP	Name	Description	Cores		
HTTPS AAA	Default-Small	Auto-created application resource-profile with 6 cpu-cores	6	/ 6	
Syslog DNS					
FIPS and Common Criteria					
Access List MAC Pool		Add Resource Profile			
Resource Profiles		Name:* Instance01			
Network Control Policy		Description:			
Chassis URL		Number of Cores:* 10 Range: 6 to 86			
		• Specify even value for number of cores.			
		OK Cancel			

b. Répétez la procédure a. à l'étape 2, pour configurer le 2e profil de ressources.

Dans cet exemple : ·Nom : Instance02 · Nombre de coeurs : 20

	Overview I	Interfaces	Logica	Devices Security Engine	Platform Settings	System Tools Help admin
	NTP SSH				O Add	
	SNMP			Name	Description Cores	
	HTTPS			Default-Small	Auto-created application resource-profile with 6 cpu-cores 6 🥒 🔒	
	Syslog			Instance01	10 🥒 🗊	
	DNS					
	FIPS and Cor	mmon Criteria			Add Baseyrae Brefile	
	Access List				Add Resource Profile	
	MAC Pool				Name:* Instance02	
	Resource Pr	rofiles				
	Network Con	trol Policy			Description:	
U	Chassis URL				Number of Cores:* 20 Range: 6 to 86	
					Specify even value for number of cores.	
l					OK Cancel	

Ajouter un 2e profil de ressources

c. Vérifiez que 2 profils de ressources ont bien été ajoutés.

Oven	view Interfaces L	ogical	Devices	Security Engin	ne <mark>P</mark> l	latform	Settings														1	System	Tools	Help	admin
NTP																			~	A-64					
SNE	IP								_	Provide la						0		U	<u> </u>	~~~					
нтт	PS		Name	Canall						Descrip	ption	Fighting of		file with discou		Cor	es								
AAA			Default	Smail						Auto-cre	eated app	plication re	esource-pro	rile with 6 cpu	u-cores	0	_			6					
Sys	og		Instance	101												10				J 🖯					
DNS	and Common Criteria		Instance	102												20				a 🖉					
Acc	ess List																_								
MAG	Pool																								
Res	ource Profiles																								
Net	vork Control Policy																								
Cha	ssis URL																								

Confirmer le profil de ressource

Étape 3. (Facultatif)Ajoutez un préfixe de pool MAC d'adresse MAC virtuelle pour les interfaces d'instance de conteneur.

Vous pouvez définir manuellement l'adresse MAC virtuelle pour l'interface active/veille. Si les adresses MAC virtuelles ne sont pas définies pour la fonctionnalité multi-instance, le châssis génère automatiquement des adresses MAC pour les interfaces d'instance et garantit qu'une interface partagée dans chaque instance utilise une adresse MAC unique.

Veuillez vérifier <u>Ajouter un préfixe de pool MAC et Afficher les adresses MAC pour les interfaces</u> <u>d'instance de conteneur</u> pour plus de détails sur l'adresse MAC.

Étape 4. Ajouter une instance autonome.

a. Accédez à Logical Devices > Add Standalone. Définissez la 1ère instance.

Dans cet exemple : · Nom du périphérique : FTD01

· Type d'instance : conteneur



Remarque : la seule façon de déployer une application conteneur est de prédéployer une instance d'application avec le type d'instance défini sur Conteneur. Assurez-vous de sélectionner Container.

Vous ne pouvez pas modifier ce nom après avoir ajouté le périphérique logique.

Overview Interfaces Logical Devices Security Engine	Platform Settings			System Tools Help admi
Logical Device List	(0 instances) 100% (86 of 86) Cor	es Available		C Refresh Add
No logical devices available. Click on Add Device to add a new logical device.				
	Add Standalone			
	Device Name:	FTD01		
	Template:	Cisco Secure Firewall Threat Defense	¥	
	Image Version:	7.2.5.208	~	
	Instance Type:	Container	~	
	Before you add t the security mod formatting. You of	he first container instance, you must reinit ule/engine so that the disk has the correct only need to perform this action once.	alize	
		ок	ancel	

Ajouter une instance

Étape 5. Configuration des interfaces

a. Définissez Profil de ressource, Interface de gestion, IP de gestion pour Instance01.

Dans cet exemple :

- · Profil de ressource : Instance01
- · Interface de gestion : Ethernet1/3
- ·IP de gestion : x.x.1.1

Overview Interfaces Logical Devices Security Engine Platform	Settings	System Tools Help admin
Provisioning - FTD01 Standalone Cisco Secure Firewall Threat Defense 7.2.5.208	Cisco Secure Firewall Threat Defense - Bootstrap Configuration 🖭	Save Cancel
Data Ports	General Information Settings Agreement	
Ethernet1/1 Ethernet1/2 Ethernet1/4 Ethernet1/5 Ethernet1/6 Ethernet1/6	SM 1 - 86 Cores Available Resource Profile: Instance01 Interface Information Management Interface: Ethernet1/3 Address Type: IP+4 only IP+4 Management IP: 1::::::: Network Mask: 255.0.0.0 Network Gateway: 1.^^	
Application Version Resource Profile	rt Status	
G FTD 7.2.5.208		
	OK Cancel	

Configuration du profil/interface de gestion/IP de gestion

b. Définissez les interfaces de données.

Dans cet exemple :

- ·Ethernet1/1 (utilisé pour l'intérieur)
- ·Ethernet1/2 (utilisé pour l'extérieur)
- ·Ethernet1/4 (utilisé pour la liaison haute disponibilité)

c	overview Interfaces	Logical Devices Secu	rity Engine Platform Set	tings				System Tools	Help admin
P S	rovisioning - FTD01 itandalone Cisco Sec	ure Firewall Threat Defense	e 7.2.5.208					Save	Cancel
	ata Ports Ethernet1/1 Ethernet1/2 Ethernet1/4 Ethernet1/6 Ethernet1/6			Ethernet1, Ethernet1, Ethernet1,] 11 12 12 14	FTD - 7.2.5.206 Etheretic Click to configure	3 1		
ł	Application	Version	Resource Profile	Management IP	Gateway	Management Port	Status		
•	FTD	7.2.5.208	Instance01	1.100.1	1.0	Ethernet1/3			
	Interface Name Ethernet1/1 Ethernet1/2 Ethernet1/4	2		Type data data data					

Définition des interfaces de données

c. Accédez à Logical Devices. Attente du démarrage de l'instance.

	Overview	Interfaces	Logical Devices	Security Engine	Platform Setting	s				System Tools Help admin
Lo	ogical Devic	e List		c	1 Container instanc	e) 100% (86 of 86) Cores Ava	ilable			C Refresh O Ads •
	FTD01			Standalone	Status:ok					₽ :
	Applicat	ion	Version	Resource F	Profile	Management IP	Gateway	Management Port	Status	
	FTD		7.2.5.208	Instance01		1	1.0-0-000	Ethernet1/3	🐝 Installing	💷 🎼 C 🕍

Confirmer l'état de Instance01

d. Répétez a. aux étapes 4.a et 5.a à c pour ajouter la 2e instance et définir les détails correspondants.

Dans cet exemple :

•Nom du périphérique : FTD11 •Type d'instance : Conteneur

Profil de ressource : Instance02Interface de gestion : Ethernet1/7IP de gestion : x.x.10.1

•Ethernet1/5 = interne

·Ethernet1/6 = extérieur

·Ethernet1/8 = liaison haute disponibilité

e. Confirmez que 2 instances sont en ligne sur FCM.

Overview	Interfaces	Logical Devices	Security Engine	Platform Settin	gs				System Tools Help admin
Logical Devi	ce List			2 Container instan	ces) 66% (56 of 86) C	ores Available			C Refresh 💽 Add -
FTD11			Standalone	Status:ok					
Applica	tion	Version	Resource I	Profile	Management IP	Gateway	Management Port	Status	
B FTD		7.2.5.208	Instance02]		1/2-2-22	Ethernet1/7	Online	💌 🎘 c 🔬
FTD01			Standalone	Status:ok					Ø :
Applica	tion	Version	Resource I	Profile	Management IP	Gateway	Management Port	Status	
H FTD		7.2.5.208	Instance01]	C a.i	1.	Ethernet1/3	1 Online	🕶 🕅 c 🖾

Confirmer l'état des instances dans le périphérique principal

f. (Facultatif) Exécutez scope ssa, scope slot 1 et show app-Instance commande pour confirmer que 2 instances sont en ligne sur l'interface de ligne de commande Firepower.

<#root> FPR4145-ASA-K9# scope ssa FPR4145-ASA-K9 /ssa # scope slot 1 FPR4145-ASA-K9 /ssa/slot # show app-Instance Application Instance: App Name Identifier Admin State Oper State Running Version Startup Version Deploy Online 7.2.5 208 7.2.5 208 Container No Instance01 Not Applicable None --> FTD01 Instance is Online ftd FTD11 online 7.2.5 208 7.2.5 208 Container No Instance02 Not Applicable None --> FTD11 Instance is Online

g. Procédez de la même manière sur le périphérique secondaire. Confirmez que 2 instances ont l'état En ligne.

Overview	Interfaces	Logical Devices	Security Engine	Platform Setting	js				System Tools Help admin
Logical Devi	ice List		c	2 Container instanc	es) 66% (56 of 86) Cores A	vailable			C Refresh 🕢 Add •
FTD12]		Standalone	Status:ok					2 I
Applica	ation	Version	Resource P	rofile	Management IP	Gateway	Management Port	Status	
# FTD		7.2.5.208	Instance02		10.2	1.1	Ethernet1/7	Online	💌 🕅 🕫
FTD02]		Standalone	Status:ok					1
Applica	ation	Version	Resource P	rofile	Management IP	Gateway	Management Port	Status	
B FTD		7.2.5.208	Instance01			1.6	Ethernet1/3	nline 🕜	💌 🕅 🕬

Confirmer l'état de l'instance dans le périphérique secondaire

Étape 6. Ajoutez Une Paire Haute Disponibilité Pour Chaque Instance.

a. Accédez à **Devices** > **Add Device** sur FMC. Ajoutez toutes les instances à FMC.

Dans cet exemple :

Nom d'affichage pour Instance01 de FTD1 : FTD1_FTD01
Nom d'affichage pour Instance02 de FTD1 : FTD1_FTD11
Nom d'affichage pour Instance01 de FTD2 : FTD2_FTD02
Nom d'affichage pour Instance02 de FTD2 : FTD2_FTD12

Cette image présente le paramètre de FTD1_FTD01.



Ajouter une instance FTD à FMC

b. Vérifiez que toutes les instances sont normales.

Firewall Management Center Overview Analysis Polic Devices / Device Management Overview	cies Devices Objects II	ntegration			Deploy	Q 📀 🌣 🚱 admin 🔹	dada SECURE
View By: Group v						Deployr	ment History
All (4) • Error (0) • Warning (0) • Offline (0) • Normal (4) • De	ployment Pending (0) • Upgrade	(0) • Snort 3	(4)			Q, Search Device	Add •
Collapse All							
Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack	
Ungrouped (4)							
C FTD1_FTD01_Snort 3 (An(),1,1 - Routed	Firepower 4145 with FTD	7.2.5	FPR4145-ASA-K9-443 Security Module - 1 (Container)	Base, Threat (2 more)	acpirule	10 10	1
Cites 10.1 + Routed	Firepower 4145 with FTD	7.2.5	EPR4145-ASA-K9-443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	4Q	1
FTD2_FTD02 Snort 3 Smot3.1.2 - Routed	Firepower 4145 with FTD	7.2.5	IIII Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	4Q	1
FTD2_FTD12 Snort 3 Circle 2.10.2 - Routed	Firepower 4145 with FTD	7.2.5	IIII Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	40	11

Confirmer l'état des instances dans FMC

c. Accédez à **Devices** > **Add High Availability**. Définissez la 1ère paire de basculement.

Dans cet exemple :

·Nom: FTD01_FTD02_HA

· Homologue principal : FTD1_FTD01

· Homologue secondaire : FTD2_FTD02



Remarque : assurez-vous de sélectionner l'unité appropriée comme unité principale.

Firewall Management Center Overview Analysis Po Devices / Device Management	olicies Devices Objects I	integration			Deploy	익 📀 🌣 📵 admin •	dide SECURE
View By: Group						Deplo	ment History
All (4) • Error (0) • Warning (0) • Offline (0) • Normal (4) • E	Deployment Pending (0)	(0) • Snort 3	(4)			Q, Search Device	Add v
Collapse All							
Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack	
Ungrouped (4)		Add High A	vailability Pair				
FTD1_FTD01_Snort.3	Firepower 4145 with FTD	Name:* FTD01_FTD0	2_HA	Base, Threat (2 more)	acp-rule	4Q	1
FTD1_FTD1 Sect 3	Firepower 4145 with FTD	Device Type: Firewall Three	it Defense 👻	Base, Threat (2 more)	acp-rule	49	1
FTD2_FTD2_Snort_3	Firepower 4145 with FTD	Primary Peer: FTD1_FTD01	•	Base, Threat (2 more)	acp-rule	4Q	1
FTD2_FTD12_Snort 3 FT02_FT0.2 - Routed	Firepower 4145 with FTD	Secondary Pee FTD2_FTD02	a. •	Base, Threat (2 more)	acp-rule	e©	1
		 Threat Defe configuration converted to on both per 	nse High Availability pair will have primary n. Licenses from primary peer will be their high availability versions and applied rs.				
			Cancel Continue				

Ajouter la première paire de basculement

d. Définissez l'adresse IP du lien de basculement dans la première paire de basculement.

Dans cet exemple :

- · Liaison haute disponibilité : Ethernet1/4
- · Liaison d'état : Ethernet1/4
- · IP principale : 192.168.90.1/24

· IP secondaire : 192.168.90.2/24

Firewall Management Center Overview Analysis Policies Devices Objects Integration Depico Aragement Devices / Devices											
Max Br. Group					Deple	syment History					
All (4) Error (0) Warning (0) Offline (0) Normal (4)	Deployment P	Pending (0) Upgrade (0) Snort 3 (4)			Q, Search Device	Add 🔻					
Collacse All											
Name	Model	Addutes Australian Data		Access Control Policy	Auto RollBack						
Ungrouped (4)		Add High Availability Pair	0								
		High Availability Link	State Link								
FTD1_FTD01 Snort 3	Firepowe	Interface:* Ethernet1/4 +	Interface:* Ethernet1/4 +	acp-rule	4(3)	11					
		Logical Name:* ha_link	Logical Name:*								
FTD1_FTD11 Short 3	Firepowe	Primary IP:* 192.168.90.1	Primary IP:* Use IPv6 Address	acp-rule	49	1					
C FTD2_FTD02 Snort 3	E	Secondary IP:* 192.168.90.2	Secondary IP:*								
1.2 - Routed	Pirepowe	Subnet Mask:* 255.255.255.0	Subnet Mask:*		459	1					
FTD2_FTD12 Snort 3	Firepowe	IPsec Encryption		acp-rule	e9+	11					
		Enabled									
		Key Generation: Auto v									
		LAN failover link is used to sync configuration, stated	ful failover link is used to sync application content								
		www.peers. arecord interace into and encryption	antenga carena de crangeo aner.								
			Cancel Add								

Définir l'interface haute disponibilité et IP pour la première paire de basculement

e. Confirmer l'état du basculement

·FTD1_FTD01 : Primaire, actif

·FTD2_FTD02 : secondaire, veille

- Fire	wall Management Center												
Devic	ces / Device Management Overview Analysis	Policies Devices Object	s Integration	n			Deploy Q 📀 🔅	admin databi secure					
View By:	Group +							Deployment History					
All (4)	Error (0) Warning (0) Offline (0) Normal (4)	 Deployment Pending (0) 	pgrade (0)	Snort 3 (4)			Q, 1	Search Device Add •					
Collapse All	College All												
	Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack						
	Ungrouped (3)												
0	FID01_FID02_HA High Availability							/1					
	FTD1_FTD01{Primary, Active} Short 3	Firepower 4145 with FTD	7.2.5	EPR4145-ASA-K9-443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	4(9	ı					
	FTD2_FTD02(Secondary, Standby) Snott 3 FTJ1.12 - Routed	Firepower 4145 with FTD	7.2.5	Firepower4KHG.cisco.com:443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	«Ģ	:					
	FTD1_FTD11 Snort 3	Firepower 4145 with FTD	7.2.5	FPR4145-ASA-K9:443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	¢9	11					
	FTD2_FTD12 Snort 3 t1102 - Routed	Firepower 4145 with FTD	7.2.5	Firepower4KHG.cisco.com:443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	¢9	1					

Confirmer l'état de la première paire de basculement

f. Accédez à **Devices** > **Cliquez sur FTD01_FTD02_HA** (dans cet exemple) > **Interfaces.** Définissez l'adresse IP active pour l'interface de données.

Dans cet exemple :

Ethernet1/1 (interne) : 192.168.10.254/24
Ethernet1/2 (extérieur) : 192.168.20.254/24

·Ethernet1/3 (diagnostic) : 192.168.80.1/24

Cette image montre le paramètre de l'adresse IP active d'Ethernet1/1.

Firewall Management Center Overview Analysis Devices / Secure Prevall Interfaces	Policies Devices Objects Integration		Deploy Q 🧬 🌣 🔕 admin 🕶 🕬 SECURE
FTD1_FTD01			You have unsaved changes Save Cancel
Summary High Availability Device Routing Interfaces Inline	Edit Physical Interface	Edit Physical Interface	Asiable for use. A
	General IPv4 IPv6 Path Monitoring Advanced	General IPv4 IPv6 Path Monitoring Advanced	Add Interfaces 👻
Interface Logi	inside	Use Static IP v	
Ethernet1/1 inside	Enabled Management Only	192.168.10.254/24	
Ethernet1/2 outside	Description:		
Ethernet1/4	Mode:		
	Security Zone:		
	Inside_zone		Cancel
	Ethernet1/1 MTU:		
	(54 - 9184)		
	Priority: 0 (0 - 65535)		
	Propagate Security Group Tag:		
	0		
		Cancel	

Définir l'adresse IP active pour l'interface de données

g. Accédez à **Devices** > **Cliquez sur FTD01_FTD02_HA** (dans cet exemple) > **High Availability.** Définissez l'IP de secours pour l'interface de données.

Dans cet exemple : •Ethernet1/1 (interne) : 192.168.10.253/24 •Ethernet1/2 (extérieur) : 192.168.20.253/24 •Ethernet1/3 (diagnostic) : 192.168.80.2/24

Cette image montre le paramètre de l'adresse IP de secours d'Ethernet1/1.

Firewall Management Center Overview Analysis Policies Devices / High Availability Devices / High Availability Devices / High Availability Devices / High Availability												
FTD01_FTD02_HA Sovo Cancel Cisco Firepower 4145 Threat Defense Summary High Availability Device Routing Interfaces DHCP VTEP												
IPsec Encryption	Edit inside	0	itics					٩				
Monitored Interfaces	Monitor this interface for failures											
Interface Name	IPv4 IPv6			Active Link-Local IPv6	Standby Link	Local IPv6	Monitoring					
outside	Interface Name:						٢	1				
diagnostic	Active IP Address:						•	1				
inside	192.168.10.254 Mask:				•			1				
	24 Standby IP Address:											
Failover Trigger Criteria	192.168.10.253		face MAC Add	resses				+				
Failure Limit			cal Interface	Active Mac Ac	idress	Standby Ma	c Address					
Peer Poll Time		Cancel	et1/1	1234.1234.00	01	1234.1234.0	0002	/1				
Peer Hold Time												

Définir l'IP de secours pour l'interface de données

h. Répétez les étapes 6.c à g pour ajouter une deuxième paire de basculement.

Dans cet exemple :

Nom : FTD11_FTD12_HA
Pair principal : FTD1_FTD11
Homologue secondaire : FTD2_FTD12
Liaison haute disponibilité : Ethernet1/8
Liaison d'état : Ethernet1/8

·Ethernet1/8 (ha_link Active) : 192.168.91.1/24

·Ethernet1/5 (interne actif) : 192.168.30.254/24

·Ethernet1/6 (extérieur actif) : 192.168.40.254/24

·Ethernet1/7 (diagnostic actif) : 192.168.81.1/24

·Ethernet1/8 (ha_link Standby) : 192.168.91.2/24

·Ethernet1/5 (en veille) : 192.168.30.253/24

·Ethernet1/6 (hors veille) : 192.168.40.253/24

·Ethernet1/7 (diagnostic Standby) : 192.168.81.2/24

i. Accédez à Logical Devices > Add Standalone. Définissez la règle ACP pour autoriser le trafic de l'intérieur vers l'extérieur.

Ę	Firewall Ma Policies / Acces	anagement C ss Control / Policy	Center Editor	Overview	Analysis	Policies	Devices	Objects	Integration					Deploy	Q 🗳 🌣	🛛 adm	nin •	daaba SEC	CURE
•	acp-rule Try New UI Layout (Analyze Hit Counts Seeve Cancel Enter Description																		
	Rules Security Intelligence HTTP Responses Logging Advanced Prefitter Policy: Default Prefitter Policy: Default Prefitter Policy: None Identity Policy: None																		
Eit	er by Device	Search Rules											×	Show Rule Con	flicts 🛛 +	Add Cate	gory	+ Add	Rule
	Name	Source Zones	Dest Zones	Source Networks	De	est Networks	VLAN Tags	Users	Applications	Source Ports	Dest Ports	URLs	Source Dynamic Attributes	Destination Dynamic Attributes	Action	15 O	ធ្ រាវ	-	¢
$\sim N$	landatory - acp-rule	(1-1)		_															
1	ftd_ha_acp	inside_zone	outside_zone	Any	An		Any	Any	Any	Any	Any	,Any	Any	Any	Allow	15. U	B. 2 (i 🖬 🛛	11
∨ D	✓ Default - acp-rule (-)																		
The	re are no rules in thi	is section. Add Ru	le or Add Categ	jory															

j. Déployez le paramètre sur FTD.

k. Confirmer le statut HA dans CLI

L'état de haute disponibilité de chaque instance est également confirmé dans l'interface de ligne de commande Firepower, qui est identique à ASA.

Exécutez show running-config failover et show failover exécutez la commande pour confirmer l'état de haute disponibilité de FTD1_FTD01 (instance principale01).

<#root>

// confrim HA status of FTD1_FTD01 (Instance01 of Primary Device) >

show running-config failover

failover failover lan unit primary failover lan interface ha_link Ethernet1/4 failover replication htt

show failover

Failover On Failover unit Primary Failover LAN Interface: ha_link Ethernet1/4 (up) This host: P Other host: Secondary - Standby Ready <---- InstanceO1 of FPRO2 is Standby Interface diagnostic

Exécutez **show running-config failover** et **show failover** exécutez la commande pour confirmer l'état de haute disponibilité de FTD1_FTD11 (instance principale02).

<#root>

// confrim HA status of FTD1_FTD11 (Instance02 of Primary Device) >

show running-config failover

failover failover lan unit primary failover lan interface ha_link Ethernet1/8 failover replication htt

show failover

Failover On Failover unit Primary Failover LAN Interface: ha_link Ethernet1/8 (up) This host: P Other host: Secondary - Standby Ready <---- Instance02 of FPR02 is Standby Interface diagnostic (192.16

Exécutez show running-config failover et show failover exécutez la commande pour confirmer l'état de haute disponibilité de FTD2_FTD02 (instance secondaire01).

<#root>

// confrim HA status of FTD2_FTD02 (Instance01 of Secondary Device) >

show running-config failover

failover failover lan unit secondary failover lan interface ha_link Ethernet1/4 failover replication h

show failover

Failover On Failover unit Secondary Failover LAN Interface: ha_link Ethernet1/4 (up) This host:

Other host: Primary - Active <---- InstanceO1 of FPRO1 is Active Active time: 31651 (sec) slot 0: UCSB-

Exécutez show running-config failover la show failover commande permettant de confirmer l'état de haute disponibilité de FTD2_FTD12 (instance secondaire02).

<#root>

// confrim HA status of FTD2_FTD12 (Instance02 of Secondary Device) >

show running-config failover

failover failover lan unit secondary failover lan interface ha_link Ethernet1/8 failover replication h Other host: Primary - Active <---- Instance02 of FPR01 is Active Active time: 31275 (sec) slot 0: UCSB-

l. Confirmer la consommation de licence

Toutes les licences sont utilisées par moteur/châssis de sécurité et non par instance de conteneur.

· Les licences de base sont automatiquement attribuées : une par moteur/châssis de sécurité.

• Les licences de fonction sont attribuées manuellement à chaque instance, mais vous ne consommez qu'une seule licence par moteur/châssis de sécurité. Pour une licence de fonction spécifique, vous n'avez besoin que d'une licence au total, quel que soit le nombre d'instances utilisées.

Ce tableau montre comment les licences sont utilisées dans ce document.

RP01	Instance01	Base, filtrage des URL, programmes malveillants, menace
	Instance02	Base, filtrage des URL, programmes malveillants, menace
RP02	Instance01	Base, filtrage des URL, programmes malveillants, menace
	Instance02	Base, filtrage des URL, programmes malveillants, menace

Base	Filtrage des URL	Programme malveillant	Menace
2	2	2	2

Confirmez le nombre de licences consommées dans l'interface utilisateur graphique FMC.

Smart Licenses			Filter Devices	×	Edit Performance Tier	Edit Licenses
License Type/Device Name	License Status	Device Type		Domain	Group	
∨ Base (2)	 In-Compliance 					1
FTD01_FTD02_HA (2) Cisco Firepower 4145 Threat Defense Threat Defense High Availability	 In-Compliance 	High Availability - Cisco Firepower 4145 Th	reat Defense	Global	N/A	
FTD11_FTD12_HA (2) Cisco Firepower 4145 Threat Defense Threat Defense High Availability	 In-Compliance 	High Availability - Cisco Firepower 4145 Th	reat Defense	Global	N/A	
Mahware (2)	In-Compliance					
FTD01_FTD02_HA (2) Cisco Firepower 4145 Threat Defense Threat Defense High Availability	In-Compliance	High Availability - Cisco Firepower 4145 Th	reat Defense	Global	N/A	
FTD11_FTD12_HA (2) Clsco Firepower 4145 Threat Defense Threat Defense High Availability	 In-Compliance 	High Availability - Cisco Firepower 4145 Th	reat Defense	Global	N/A	
∨ Threat (2)	In-Compliance					
FTD01_FTD02_HA (2) Cisco Firepower 4145 Threat Defense Threat Defense High Availability	 In-Compliance 	High Availability - Cisco Firepower 4145 Th	reat Defense	Global	N/A	
FTD11_FTD12_HA (2) Cisco Firepower 4145 Threat Defense Threat Defense High Availability	 In-Compliance 	High Availability - Cisco Firepower 4145 Th	reat Defense	Global	N/A	
✓ URL Filtering (2)	 In-Compliance 					-
FTD01_FTD02_HA (2) Cisco Firepower 4145 Threat Defense Threat Defense High Availability	In-Compliance	High Availability - Cisco Firepower 4145 Thr	eat Defense	Global	N/A	
FTD11_FTD12_HA (2) Cisco Firepower 4145 Threat Defense Threat Defense High Availability	In-Compliance	High Availability - Cisco Firepower 4145 Thr	eat Defense	Global	N/A	

Confirmer les licences consommées

Vérifier

En cas de panne sur FTD1_FTD01 (instance principale01), le basculement de l'instance01 est déclenché et les interfaces de données côté veille prennent le relais de l'adresse IP/MAC de l'interface active d'origine, assurant ainsi le passage continu du trafic (connexion FTP dans ce document) par Firepower.



Avant le crash



Pendant le crash



Le basculement est déclenché

Étape 1. Lancez la connexion FTP de Win10-01 à Win10-02.

Étape 2. Exécutez la show conn commande pour confirmer que la connexion FTP est établie dans les deux instances de Instance01.

<#root>

// Confirm the connection in Instance01 of FPR01 >

show conn

TCP outside 192.168.20.1:21 inside 192.168.10.1:49723, idle 0:00:11, bytes 529, flags UIO N1 // Confirm

show conn

TCP outside 192.168.20.1:21 inside 192.168.10.1:49723, idle 0:00:42, bytes 530, flags UIO N1

Étape 3. Lancez la connexion FTP de Win10-03 à Win10-04.

Étape 4. Exécutez la show conn commande pour confirmer que la connexion FTP est établie dans les deux instances de Instance02.

<#root>

// Confirm the connection in Instance02 of FPR01 >

show conn

```
TCP outside 192.168.40.1:21 inside 192.168.30.1:52144, idle 0:00:02, bytes 530, flags UIO N1 // Confirm show conn
```

TCP outside 192.168.40.1:21 inside 192.168.30.1:52144, idle 0:00:13, bytes 530, flags UIO N1

Étape 5. Exécutez connect ftd FTD01 et entrez system support diagnostic-cli la commande dans l'interface de ligne de commande ASA. Exécuter enable et **crashinfo force watchdog** commander pour forcer la panne Instance01 dans l'unité principale/active.

<#root>

```
Firepower-module1>
connect ftd FTD01
    s
system support diagnostic-cli
    FTD01>
enable
Password: FTD01# FTD01#
crashinfo force watchdog
reboot. Do you wish to proceed? [confirm]:
```

Étape 6. Le basculement se produit dans Instance01 et la connexion FTP n'est pas interrompue. Exécutez show failover et show conn la commande pour confirmer l'état de Instance01 dans FPR02.

<#root>

```
>
```

show failover

Failover On Failover unit Secondary Failover LAN Interface: ha_link Ethernet1/4 (up) This host: Other host: Primary - Failed Interface diagnostic (192.168.80.2): Unknown (Monitored) Interface inside

show conn

TCP outside 192.168.20.1:21 inside 192.168.10.1:49723, idle 0:02:25, bytes 533, flags U N1

Étape 7. Le plantage survenu dans Instance01 n'a eu aucun effet sur Instance02. Exécutez show failover et show conn la commande pour confirmer l'état d'Instance02.

<#root>

>

show failover

Failover On Failover unit Secondary Failover LAN Interface: ha_link Ethernet1/8 (up) This host: Other host: Primary - Active Interface diagnostic (192.168.81.1): Normal (Monitored) Interface inside (1

show conn

TCP outside 192.168.40.1:21 inside 192.168.30.1:52144, idle 0:01:18, bytes 533, flags UIO N1

Étape 8. Accédez à Devices > All sur FMC. Confirmez l'état HA.

·FTD1_FTD01 : principal, veille

·FTD2_FTD02 : secondaire, actif

Fin Dev	ewall Management Center Overview Analysis	Policies Devices Objec	ts Integratio	'n			Deploy Q	admin • 🗟 🕹 SECURE					
View By:	Group							Deployment History					
All (4)	Error (0) Warning (0) Offline (0) Normal (4)	Deployment Pending (0)	Jpgrade (0)	 Snort 3 (4) 				Q, Search Device Add •					
Collapse All	All control of the second s												
	Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack						
	 Ungrouped (2) 												
	 FTD01_FTD02_HA High Availability 							11					
	FTD1_FTD01(Primary, Standby) Snort 3	Firepower 4145 with FTD	7.2.5	III Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	49	:					
	FTD2_FTD02(Secondary, Active) Snort 3	Firepower 4145 with FTD	7.2.5	IIII Firepower4KHG cisco.com 443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	49	:					
	V FTD11_FTD12_HA High Availability							11					
	FTD1_FTD11(Primary, Active) Short 3 Short 3 Short 3	Firepower 4145 with FTD	7.2.5	III Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	49	:					
	FTD2_FTD12(Secondary, Standby) Short 3 T11	Firepower 4145 with FTD	7.2.5	Firepower4KHG cisco com 443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	49	:					

Confirmer l'état HA

Étape 9. (Facultatif)Une fois que l'Instance01 de FPR01 est revenue à la normale, vous pouvez changer manuellement l'état de la haute disponibilité. Cela peut être effectué par l'interface graphique FMC ou l'interface de ligne de commande FRP.

Sur FMC, accédez à **Devices** > **All**. Cliquez sur **Commuter l'homologue actif** pour commuter l'état de haute disponibilité pour **FTD01_FTD02_HA**.

C) 5	Firewall Management Center Overview Analysis Policies Devices / De											
View By: All (4)	Group • • Error (0) • Warning (0) • Offline (0) • Normal (4)	Deployment Pending (0)	lpgrade (0)	Snort 3 (4)				Deployment History Q, Search Device Add •				
Golisen Al												
	Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack					
	 Ungrouped (2) 											
	V FT001_FT002_HA High Availability							Switch Active Peer				
	FTD1_FTD01(Primary, Stansby) Snort 3 Critic 3.1.1 - Routed	Firepower 4145 with FTD	7.2.5	FPR4145-ASA-K9.443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	κ۵	Force refresh node status Delete Revert Upgrade				
	FTD2_FTD02(Secondary, Active) Snort 3 Control 1.2 - Routed	Firepower 4145 with FTD	7.2.5	Firepower4KHG cisco com:443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	«Ø	Health Monitor Troubleshoot Files				
	V High Availability							11				
	C FTD1_FTD11(Primary, Active) Snort 3 C C 1, 10, 3 - Routed	Firepower 4145 with FTD	7.2.5	EPR4145-ASA-K9.443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	¢۶	1				
	FTD2_FTD12(Secondary, Standby) Short 3 Fortp3.10.2 - Routed	Firepower 4145 with FTD	7.2.5	Firepower4KHG.cisco.com.443 Security Module - 1 (Container)	Base, Threat (2 more)	acpirule	¢۵	1				

État HA du commutateur

Sur l'interface de ligne de commande Firepower, exécutez connect ftd FTD01 et system support diagnostic-cli la commande pour entrer dans

l'interface de ligne de commande ASA. Exécutez enable et la **failover active** commande pour commuter la haute disponibilité pour FTD01_FTD02_HA.

<#root>

Firepower-module1>

connect ftd FTD01

>

system support diagnostic-cli

Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach. Type help or '?' for a list of available

enable

firepower#

failover active

Dépannage

Afin de valider l'état du basculement, exécutez show failover et show failover history commande.

<#root>

>

show failover

Failover On Failover unit Secondary Failover LAN Interface: ha_link Ethernet1/8 (up) This host: Other host: Primary - Active Interface diagnostic (192.168.81.1): Normal (Monitored) Interface inside (2

>

show failover history

Exécutez la commande debug fover <option> pour activer le journal de débogage du basculement.

<#root>

>

debug fover

auth Failover Cloud authentication cable Failover LAN status cmd-exec Failover EXEC command execution of

Référence

https://www.cisco.com/c/en/us/support/docs/security/firepower-management-center/212699-configure-ftd-high-availability-on-firep.html https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/multi-Instance/multi-Instance solution.html

https://www.cisco.com/c/en/us/support/docs/availability/high-availability/217763-troubleshoot-firepower-threat-defense-hi.html#toc-hId-46641497

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.