Configurer la haute disponibilité sur FMC

Table des matières

ntroduction
Conditions préalables
Exigences
Composants utilisés
nformations générales
Avant de commencer
Configurer
Configuration du FMC secondaire
Configuration du FMC principal
<u>Vérification</u>

Introduction

Ce document décrit un exemple de configuration de haute disponibilité (HA) sur un centre de gestion des pare-feu (FMC).

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

Les informations contenues dans ce document sont basées sur Secure FMC pour VMware v7.2.5.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Les exigences spécifiques de ce document sont les suivantes :

- Les deux homologues FMC doivent être sur la même version logicielle, la même mise à jour de règle d'intrusion, la même base de données de vulnérabilité et le même package de sécurité léger
- Les deux homologues FMC doivent avoir la même capacité ou la même version matérielle
- Les deux FMC nécessitent une licence distincte

Pour connaître l'ensemble des conditions requises, vous pouvez consulter le <u>Guide</u> <u>d'administration</u>.



Avertissement : En cas de non-correspondance dans les exigences répertoriées, vous ne pouvez pas configurer la haute disponibilité.

Cette procédure est prise en charge sur toutes les appliances matérielles.

Avant de commencer

- · Garantir un accès administrateur aux deux FMC
- Assurer la connectivité entre les interfaces de gestion
- Prenez le temps de vérifier les versions logicielles et assurez-vous que toutes les mises à niveau nécessaires sont effectuées

Configurer

Configuration du FMC secondaire

Étape 1. Connectez-vous à l'interface utilisateur graphique (GUI) du périphérique du FMC qui va jouer le rôle de secondaire/veille.



Se connecter à FMC

Étape 2. Accédez à l'onglet Intégration.

Firewall Management Center Overview / Dashboards / Dashboard	Overview	Analysis I	Policies	Devices	Objects	Integration	De	ploy Q	o 🔉	🛿 admin 🔻	cisco SECURE
											Reporting
Summary Dashboard (which dashboard) Provides a summary of activity on the appliance											
Network \times Threats Intrusion Events	Status Geo	plocation	QoS	+				Show the Last	1 hour		• II
											Add Widgets
 Unique Applications over Time 	$-\times$	► Top Web	Applicatio	ns Seen		$-\times$	► Top Clie	nt Application	ns Seen		$-\times$
No Data				No Date					No Da	ata	
No devices registered.			N	lo devices reg	istered.			No	devices re	egistered.	
Click here to register a device.			Click	here to regist	er a device.			Click h	ere to regi	ster a device.	
Last updated 3 minutes ago		Last updated 3	3 minutes ag	10			Last updated	3 minutes ago			
Traffic by Application Risk	- ×	Top Serv	er Applicat	tions Seen		- ×	► Top Ope	rating System	ns Seen		- ×
No Data											

Accéder à l'intégration

Étape 3. Cliquez sur Autres intégrations.

Integration	Deploy	Q 📀 🌣 🕜 admin ▼ 👊
SecureX Security Analytics & L Other Integrations	ogging	Intelligence Incidents Sources
AMP		Elements Settings
AMP Management Dynamic Analysis Cor	nnections	

Accédez à Autre intégration

Étape 4. Accédez à l'onglet Haute disponibilité.

Integration / Other In	tegrations / Cloud Services	Overview	Analysis	Policies	Devices	Objects	Integration
Cloud Services Realr	Identity Sources	High Availability	eStreamer	Host Input (Client	Smart Software I	Manager On-Prem

Accédez à Haute disponibilité

Étape 5. Cliquez sur Secondaire.

Firewall Integration	Manager Other Integr	ment Center rations / High Availabili	Overview	Analysis	Policies	Devices	Objects	Integration	Deploy	Q	0 <	> 0	admin 🔻	cisco SECURE
														Peer Manager
Cloud Services	Realms	Identity Sources	High Availability	eStreamer	Host Input	Client Sm	art Software I	Aanager On-Prem						
Select a role for Role For This Firev Standalone (N	this Manag vall Manager o High Availa	gement Center and ment Center: ability)	specify peer detai	ls to setup hiç	gh availability	ſ.								
O Primary														
 Secondary 														

Entrez les informations et sélectionnez le rôle souhaité pour le FMC actuel.

Étape 6. Entrez les informations relatives à l'homologue principal/actif et cliquez sur Register.

							Peer Manager
Cloud Services	Realms	Identity Sources	High Availability	eStreamer	Host Input Client	Smart Software Manager On-Prem	
Select a role for	this Manag	ement Center and	specify peer details	s to setup high	n availability.		
Role For This Firev	vall Managem o High Availal	ent Center: bility)					
O Primary							
 Secondary 							
Peer Details:							
After Firewall Man	agement Cen	ter high availability is	configured in virtual o	r cloud environr	ment, each registered	Firewall Threat Defense consumes an additional Firepower MCv Device license.	
Primary Firewall M	anagement C	enter Host:					
10.18.19.31							
Registration Key*:							
cisco123							
Unique NAT ID:							
Register							
+ Either host or NAT I	D is required.						



Remarque : Prenez note de la clé d'enregistrement, car elle sera utilisée sur le FMC actif.

Warning

This operation may affect critical processes running in the background. Do you want to continue?





Remarque : Assurez-vous qu'aucune autre tâche n'est en cours d'exécution car pendant la création de HA, l'interface utilisateur redémarre.

Étape 8. Confirmez que vous souhaitez enregistrer l'homologue principal.



Do you want to register primary peer: 10.18.19.31?





Avertissement : Toutes les informations sur les périphériques/la stratégie/la configuration vont être supprimées du FMC secondaire une fois que la haute disponibilité aura été créée.

Étape 9. Vérifiez que l'état du contrôleur FMC secondaire est en attente.

Firewall Manag	ement Center egrations / Peer Manager	Overview	Analysis	Policies	Devices	Objects	Integration	Deploy	Q	0	≎	🕜 admin 🕶	cisco SE	ECURE
Cloud Services Realn	Identity Sources	High Availability	eStreamer	Host Input (Client	Smart Softwar	e Manager On-Prem							
Host	Last Mod	lified			S	Status				s	tate			
10.18.19.31	2023-05	-28 13:53:56			P	ending Registratio	n				0		1	Ŵ

Configuration du FMC principal

Répétez les étapes 1 à 4 sur le FMC principal/actif.

Étape 5. Cliquez sur Principal.

Firewall Integration /	Manager Other Integr	nent Center ations / High Availabilit	Overview y	Analysis	Policies	Devices	Objects	Integration	Deploy	۹	0	🕜 admin 🕇	cisco SECURE
Cloud Services	Realms	Identity Sources	High Availability	eStreamer	Host Input	: Client Sr	nart Software M	Manager On-Pren	1				Peer Manager
Select a role for	this Manaç	gement Center and	specify peer detai	ils to setup hig	gh availabilit	ty.							
Role For This Firew	all Managen High Availa	nent Center: bility)											
Primary													
Secondary													
Peer Details:													
Configure the seco After Firewall Mana Secondary Firewal	ndary Mana Igement Cer Manageme	gement Center with d tter high availability is nt Center Host:	etails of the primary configured in virtual	before registrati or cloud enviror	ion. nment, each r	egistered Fire	wall Threat Def	énse consumes a	n additional Fire	power N	ICv Devi	ce license.	
Registration Key*:													
Unique NAT ID:													
Register † Either host or NAT II	D is required.												

Étape 6. Entrez les informations relatives à Secondary FMC et cliquez sur Register.

Cloud Services	Realms	Identity Sources	High Availability	eStreamer	Host Input Client	Peer Mar Smart Software Manager On-Prem	hager
Select a role for	this Manaç	gement Center and	specify peer detai	ls to setup hig	gh availability.		
Role For This Firev	vall Manager o High Availa	nent Center: ibility)					
Primary							
Secondary							
Peer Details:							
Configure the second After Firewall Man Secondary Firewa	ondary Mana agement Cer Il Manageme	gement Center with o nter high availability is nt Center Host:	letails of the primary l configured in virtual	before registrati or cloud enviror	on. Iment, each registereo	d Firewall Threat Defense consumes an additional Firepower MCv Device license.	
10.18.19.32							
Registration Key*:							
cisco123							
Unique NAT ID:							
Register † Either host or NAT	D is required.						



Remarque : Utilisez la même clé d'enregistrement que le contrôleur FMC secondaire.

Étape 7. Cet avertissement vous demande de confirmer, cliquez sur yes.

Warning

This operation may affect critical processes running in the background. Do you want to continue?





Remarque : Vérifiez qu'aucune autre tâche n'est en cours d'exécution.

Étape 8. Confirmez que vous souhaitez vous inscrire au FMC secondaire.

Warning

Secondary peer configuration and policies will be removed. After Firewall Management Center high availability is configured in virtual or cloud environment, each registered Firewall Threat Defense consumes an additional Firepower MCv Device license. Do you want to register secondary peer: 10.18.19.32?





Remarque : Assurez-vous qu'il n'y a aucune information critique sur le FMC secondaire, car accepter cette invite supprime toutes les configurations du FMC.

La synchronisation entre le principal et le secondaire commence ; la durée dépend de la configuration et des périphériques. Ce processus peut être surveillé à partir des deux unités.

	Firewall I Integration /	Managen Other Integra	nent Cent ations / High A	er wailability	Overview	Analysis	Policies	Devices	Objects	Integration	Deploy	۹ (\$	🕜 admin	eisco SECURE
															Peer Manager
Cloud \$	Services	Realms	Identity Sou	irces	High Availability	eStreamer	Host Input	t Client Sr	mart Software M	Manager On-Pre	m				
										Switch Peer R	oles 🗳	Break HA		II Pause Sy	vnchronization
				High ava These oj Databas	ilability operations and perations include file e files synchronization	re in progress. The copy which may t n: 100% of 379MI	e status messa ake time to co 8 transferred	ages and alerts omplete.	on this page are	a temporary. Plea	se check after high	availabilit	ty opera	ions are compl	ete. ×
	Summa	ry						S	ystem Statu	s					
	Status		A Tem	porarily	degraded- high ava	ailability operation p	ns are in rogress.				Local Active - Primary (10.18.19.31)		Stan	Remote dby - Seconda (10.18.19.32)	ary
	Synchron	nization				4	Failed	C	perating Syste	m	7.2.5			7.2.5	
	Active Sy	/stem				10.1	8.19.31	s	oftware Version	n	7.2.5-208			7.2.5-208	
	Standby	System				10.1	8.19.32	Μ	lodel	Secur	e Firewall Manag Center for VMwar	ement e	S Mana	ecure Firewall gement Cente VMware	r for



Remarque : Pendant la synchronisation, attendez-vous à voir l'état Failed et Temporary degraded. Cet état s'affiche jusqu'à ce que le processus soit terminé.

Vérification

Une fois la synchronisation terminée, le résultat attendu est Status Healthy et Synchronization OK.

Firewal Integration	I Manage	ment Center grations / High Availability	Overview	Analysis	Policies	Devices	Objects	Integration	Deploy	Q	Ø	🕜 admin 🕇	cisco SE
													Peer Mana
oud Services	Realms	Identity Sources	High Availability	eStreamer	Host Input	Client Sr	mart Software N	lanager On-Prem					
							\$	Switch Peer Roles	\$ \$	Break H/		II Pause Sy	nchronization
Summ	nary					S	ystem Statu	S					
Status				O H	lealthy			Act	Local		Stan	Remote	
Synchr	ronization				OK			ACI (10.18.19.31)		Stan	(10.18.19.32)	У
Active	System			10.18	.19.31	C	perating System	n	7.2.5			7.2.5	
Standb	by System			10.18	.19.32	s	oftware Versior	1	7.2.5-208			7.2.5-208	
						N	lodel	Secure F Cen	irewall Manag ter for VMwar	ement e	Mana	Secure Firewall agement Center VMware	for

Le principal et le secondaire continuent de se synchroniser ; this is normal.

Firewall Management Center Integration / Other Integrations / High Availability	Devices Integration		۹ (☆
Olaud Candona – Ulab Augliability – «Steamer	Heat have Oliver			Peer Manager
Cloud Services High Availability eStreamer	Host Input Client			
		Switc	h Peer Roles 🛛 🐢 Break HA	Pause Synchronization
Summary		System Status		
Status	Synchronization task is in progress		Local	Remote
Synchronization	OK 📀		(10.18.19.32)	(10.18.19.31)
Active System	10.18.19.31	Operating System	7.2.5	7.2.5
Standby System	10.18.19.32	Software Version	7.2.5-208	7.2.5-208
		Model	Secure Firewall Management Center for VMware	Secure Firewall Management Center for VMware

Prenez quelques instants pour vérifier que vos périphériques s'affichent correctement sur le principal et le secondaire.

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.