Konfigurieren von hoher Verfügbarkeit auf FMC

Inhalt

Einleitung
Voraussetzungen
Anforderungen
Verwendete Komponenten
Hintergrundinformationen
Vorbereitungen
Konfigurieren
Sekundäres FMC konfigurieren
Primäres FMC konfigurieren
Verifizierung

Einleitung

Dieses Dokument beschreibt ein Konfigurationsbeispiel für Hochverfügbarkeit (HA) in einem Firewall Management Center (FMC).

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Secure FMC für VMware v7.2.5.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Spezifische Anforderungen für dieses Dokument:

- Beide FMC-Peers müssen dieselbe Softwareversion, dasselbe Update für Angriffsregeln, dieselbe Schwachstellendatenbank und dasselbe Lightweight Security Package verwenden.
- Beide FMC-Peers müssen dieselbe Kapazität oder Hardwareversion aufweisen.
- Beide FMCs erfordern eine separate Lizenz.

Eine vollständige Liste der Anforderungen finden Sie im Administrationshandbuch.



Warnung: Wenn die aufgelisteten Anforderungen nicht übereinstimmen, kann die HA-Funktion nicht konfiguriert werden.

Dieses Verfahren wird auf allen Hardware-Appliances unterstützt.

Vorbereitungen

- Administratorzugriff auf beide FMCs gewährleisten
- Gewährleistung der Verbindung zwischen Verwaltungsschnittstellen
- Nehmen Sie sich einen Moment Zeit, um die Softwareversionen zu überprüfen und sicherzustellen, dass alle erforderlichen Upgrades durchgeführt werden.

Konfigurieren

Sekundäres FMC konfigurieren

Schritt 1: Melden Sie sich bei der grafischen Benutzeroberfläche (GUI) des Geräts des FMC an, das die Rolle des sekundären/Standby-Geräts übernehmen soll.



Bei FMC anmelden

Schritt 2: Navigieren Sie zur Registerkarte Integration.

Firewall Management Center Overview / Dashboards / Dashboard	Overview	Analysis Policies	Devices	Objects In	tegration	Deploy Q	📀 🔅 🕜 admin	stituli: SECURE
								Reporting
Summary Dashboard (switch dashboard) Provides a summary of activity on the appliance								
Network \times Threats Intrusion Events	Status Geo	location QoS	+			Show the Last	1 hour	• II
								Add Widgets
Unique Applications over Time	$-\times$	Top Web Applica	ations Seen		$-\times$	Top Client Application	ns Seen	- ×
No Data			No Data				No Data	
No devices registered.			No devices regis	stered.		No	devices registered.	
Click here to register a device.		CI	ick here to registe	r a device.		Click h	ere to register a device	
Last updated 3 minutes ago		Last updated 3 minutes	ago			Last updated 3 minutes ago		
 Traffic by Application Risk 	$-\times$	 Top Server Appli 	cations Seen		-×	Top Operating System	ms Seen	- ×
No Dete								
No Data	1	1				1		1

Zur Integration navigieren

Schritt 3: Klicken Sie auf Weitere Integrationen.

Integration	Deploy	ୟ 📀 🌣 🕜 admin▼ '	ılı.ılı. cısco
SecureX Security Analytics & Other Integrations	Logging	Intelligence Incidents Sources	
AMP		Elements Settings	
AMP Management Dynamic Analysis Co	onnections		

Zur anderen Integration navigieren

Schritt 4: Navigieren Sie zur Registerkarte "Hohe Verfügbarkeit".

Firewall	Manager Other Integr	nent Center ations / Cloud Service:	Overview	Analysis	Policies	Devices	Objects	Integration
Cloud Services	Realms	Identity Sources	High Availability	eStreamer	Host Input	Client	Smart Software	Manager On-Prem

Navigation zur Hochverfügbarkeit

Schritt 5: Klicken Sie auf Sekundär.

Firewall Integration /	Manager Other Integr	ment Center rations / High Availabili	Overview	Analysis	Policies	Devices	Objects	Integration	Deploy	۹	0	¢	🕜 admin 🕇	cisco SECURE
														Peer Manager
Cloud Services	Realms	Identity Sources	High Availability	eStreamer	Host Input	Client Sn	hart Software I	Aanager On-Prem						
Select a role for Role For This Firew Standalone (No	this Manag vall Manager o High Availa	gement Center and ment Center: ability)	specify peer detai	ls to setup hiç	gh availability	t.								
O Primary														
 Secondary 														

Informationen eingeben und gewünschte Rolle für aktuelles FMC auswählen

Schritt 6: Geben Sie Informationen zum primären/aktiven Peer ein, und klicken Sie auf Register.

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



Anmerkung: Beachten Sie den Registrierungsschlüssel, da er für das aktive FMC verwendet wird.

Warning

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





Anmerkung: Stellen Sie sicher, dass kein anderer Task ausgeführt wird, da die GUI neu gestartet wird, während HA erstellt wird.

Schritt 8: Bestätigen Sie, dass Sie den primären Peer registrieren möchten.



Do you want to register primary peer: 10.18.19.31?





Warnung: Alle Informationen auf den Geräten/Richtlinien/Konfigurationen werden aus dem sekundären FMC entfernt, sobald die HA erstellt wurde.

Schritt 9: Überprüfen Sie, ob der Status des sekundären FMC "Ausstehend" lautet.

Fil Inte	rewall N egration / (/lanagem Other Integra	tions / Peer Mana	Overview ger	Analysis	Policies	Devices	Objects	Integration	Deploy	Q	0	¢	🕜 admin 🕶	cisco SECURE
Cloud Se	ervices	Realms	Identity Sourc	s High Availability	eStreamer	Host Inp	ut Client	Smart Softwar	e Manager On-Prem						
Host			Last	Aodified			s	itatus				S	tate		
10.18.19	9.31		2023	-09-28 13:53:56			P	ending Registratio	in			•			/ 1

Primäres FMC konfigurieren

Wiederholen Sie die Schritte 1 bis 4 für das primäre/aktive FMC.

Schritt 5: Klicken Sie auf Primär.

Firewall Ma	anagement Center ler Integrations / High Availabili	Overview	Analysis	Policies	Devices	Objects	Integration	Deploy	Q	o 🜣	🕜 admin 🔻	cisco SECURE
Cloud Services Re	ealms Identity Sources	High Availability	eStreamer	Host Input	Client Sn	nart Software I	Manager On-Prem					Peer Manager
Select a role for this	Management Center and	specify peer detail	ils to setup hig	gh availabilit	у.							
Role For This Firewall N	Management Center: gh Availability)											
Primary												
 Secondary 												
Peer Details:												
Configure the secondar After Firewall Managen Secondary Firewall Mar	ary Management Center with o ment Center high availability is inagement Center Host:	letails of the primary configured in virtual	before registrati or cloud enviror	on. nment, each r	egistered Fire	wall Threat Def	fense consumes an	additional Fire	power N	//Cv Devi	e license.	
Registration Key*:												
Unique NAT ID:												
Register † Either host or NAT ID is re	required.											

Schritt 6: Geben Sie die Informationen zum sekundären FMC ein, und klicken Sie auf Registrieren.

Cloud Services	Realms	Identity Sources	High Availability	eStreamer	Host Input Client	Peer Ma Smart Software Manager On-Prem	nager
Select a role for	this Manag	ement Center and	specify peer detai	ls to setup hig	h availability.		
Role For This Firev	vall Managen o High Availa	nent Center: bility)					
Primary							
Secondary							
Peer Details:							
Configure the second After Firewall Man Secondary Firewal	ondary Mana agement Cer I Manageme	gement Center with d nter high availability is nt Center Host:	letails of the primary to configured in virtual	pefore registration or cloud environ	on. Iment, each registerec	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 I	D is required.						



Anmerkung: Verwenden Sie denselben Registrierungsschlüssel wie das sekundäre FMC.

Schritt 7. Diese Warnung fordert Sie zur Bestätigung auf, klicken Sie auf Yes.

Warning

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





Anmerkung: Stellen Sie sicher, dass kein anderer Task ausgeführt wird.

Schritt 8: Bestätigen Sie, dass Sie sich für das sekundäre FMC registrieren möchten.

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?





Anmerkung: Stellen Sie sicher, dass keine kritischen Informationen zum sekundären FMC vorliegen, da bei Annahme dieser Aufforderung alle Konfigurationen aus dem FMC entfernt werden.

Synchronisierung zwischen primärem und sekundärem Start Die Dauer hängt von der Konfiguration und den Geräten ab. Dieser Vorgang kann von beiden Einheiten aus überwacht werden.

	Firewall I Integration /	Managen Other Integra	nent Cent ations / High /	er Availability	Overview	Analysis	Policies	Devices	Objects	Integration	Deploy	Q	\$	🛿 admin 🔻	cisco SECURE
															Peer Manager
Cloud	Services	Realms	Identity Sou	urces	High Availability	eStreamer	Host Input	t Client Sr	nart Software I	Manager On-Pre	m				
									5	Switch Peer Ro	oles 🔅 I	Break HA		II Pause Syr	nchronization
				High ava These of Database	ilability operations ar perations include file e files synchronizatio	re in progress. The copy which may t n: 100% of 379MI	e status messa take time to co B transferred	ages and alerts omplete.	on this page are	e temporary. Pleas	se check after high	availabili	ty operat	ions are comple	te. ×
	Summa	ary						S	ystem Statu	S					
	Status		🔺 Ten	nporarily (degraded- high ava	ilability operation p	ns are in progress.			1	Local Active - Primary (10.18.19.31)		Stan	Remote dby - Seconda (10.18.19.32)	ry
	Synchror	nization					Failed	C	perating Syste	m	7.2.5			7.2.5	
	Active Sy	ystem				10.1	18.19.31	s	oftware Versio	n	7.2.5-208			7.2.5-208	
	Standby	System				10.1	18.19.32	Ν	lodel	Secur	e Firewall Manag Center for VMwar	ement e	S Mana	ecure Firewall gement Center VMware	for



Anmerkung: Erwarten Sie während der Synchronisierung den Status Failed (Fehlgeschlagen) und Temporary degraded (Temporär). Dieser Status wird angezeigt, bis der Prozess abgeschlossen ist.

Verifizierung

Nach Abschluss der Synchronisierung lautet die erwartete Ausgabe Status fehlerfrei und Synchronisierung OK.

Firewall	/ Other Integ	ment Center rations / High Availability	Overview	Analysis	Policies	Devices	o Objects	Integration	Deploy	۹ (\$	🕜 admin 🕇	cisco SEC
													Peer Manag
oud Services	Realms	Identity Sources	High Availability	eStreamer	Host Input	Client	Smart Software M	lanager On-Pi	em				
							4	Switch Peer	Roles 🏟 I	Break HA		II Pause Sy	nchronization
Summ	ary					11	System Status	6					
Status				O H	lealthy				Local		Stan	Remote	
Synchro	onization				OK 📀				(10.18.19.31)		Stan	(10.18.19.32)	u y
Active	System			10.18	.19.31		Operating System	n	7.2.5			7.2.5	
Standb	y System			10.18	.19.32		Software Version		7.2.5-208			7.2.5-208	
							Model	Sec	ure Firewall Manag Center for VMwar	ement e	S Mana	ecure Firewall gement Center VMware	for

Die primäre und sekundäre Synchronisierung wird fortgesetzt. das ist normal.

	Firewall	Management (Other Integrations /	Center High Availability	Devices	Integration					۹	0	¢	0	admi	n •	alialia cisco	SECURE
																Peer M	anager
Cloud S	Services	High Availability	eStreamer	Host Input Client													
							Switch P	eer Roles	42	Break H	łA		П	Pause	Sync	hroniza	ation
	Summa	ary				System S	tatus										
	Status			Synchroniza	tion task is in progress			Loc Standby - 5	cal Seconda	arv		Act	Rer	note Prima	arv.		
	Synchro	nization			OK			(10.18	.19.32)			(10.18	3.19.31)		
	Active S	ystem			10.18.19.31	Operating S	System	7.3	2.5				7.	.2.5			
	Standby	System			10.18.19.32	Software Ve	ersion	7.2.5	5-208				7.2.	5-208			
						Model		Secure Firewa Center fo	ill Manag or VMwar	ement e	,	S€ Manag	ecure geme VM	Firew ent Cen	all iter fo	r	

Nehmen Sie sich einen Moment Zeit, um zu überprüfen, ob Ihre Geräte sowohl in der primären als auch in der sekundären Anzeige korrekt sind.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.