Hoge beschikbaarheid op FMC configureren

Inhoud

iding	Inleidir
prwaarden	Voorwa
Vereisten	Vere
Gebruikte componenten	Geb
itergrondinformatie	Achter
ordat u begint	Voorda
nfigureren	<u>Config</u>
Secundair VCC configureren	<u>Sec</u>
Primair VCC configureren	Prim
ificatie	<u>Verifica</u>

Inleiding

Dit document beschrijft een configuratievoorbeeld van High Availability (HA) op een Firewall Management Center (FMC).

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op het beveiligde FMC voor VMware v7.2.5.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Specifieke eisen voor dit document zijn onder meer:

- Beide FMC-peers moeten op dezelfde softwareversie, inbraakregelupdate, kwetsbaarheidsdatabase en lichtgewicht security pakket staan
- Beide FMC-peers moeten dezelfde capaciteit of hardwareversie hebben
- · Beide VCC's hebben een afzonderlijke vergunning nodig

Voor een volledige reeks vereisten kunt u de beheershandleiding bezoeken.



Waarschuwing: Als de vereisten niet overeenkomen, kunt u HA niet configureren.

Deze procedure wordt op alle hardwareapparatuur ondersteund.

Voordat u begint

- Ervoor zorgen dat de beheerder toegang heeft tot beide VCC's
- Zorg voor connectiviteit tussen beheerinterfaces
- Neem even de tijd om de softwareversies te bekijken en zorg ervoor dat alle benodigde upgrades uitgevoerd worden

Configureren

Secundair VCC configureren

Stap 1. Log in op de grafische gebruikersinterface (GUI) van het apparaat van het VCC dat de rol van Secundair/Standby zal vervullen.



Inloggen bij VCC

Stap 2. Navigeer naar het tabblad Integratie.

Firewall Management Center Overview / Dashboards / Dashboard	Overview	Analysis Policies	Devices	Objects	Integration	Deploy	२ 📀 🌣	🕜 admin 🔻	cisco 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	tions Seen		$-\times$	Top Client Applic	ations Seen		$-\times$
No Data			No Data				No E	ata	
No devices registered. Click here to register a device.		Cli	No devices regist	tered.		CI	No devices	registered.	
Last updated 3 minutes ago		Last updated 3 minutes	ago			Last updated 3 minutes	ago		
 Traffic by Application Dick 	- >								
	- ^	 Top Server Applie 	cations Seen		- ×	Top Operating Sy	stems Seen		- ×
No Data									

Naar integratie navigeren

Stap 3. Klik op Overige integraties.

Integration	Deploy	Q	0	₽	?	admin 🔻	cisco
SecureX Security Analytics & Lo Other Integrations AMP	ogging	I S S	ntellige ncider Source Elemer Setting	ence nts es nts gs			
AMP Management Dynamic Analysis Con	nections						

Naar andere integraties navigeren

Stap 4. Navigeer naar het tabblad Hoge beschikbaarheid.

Firewall Management Center Integration / Other Integrations / Cloud Services	Overview	Analysis	Policies	Devices	Objects	Integration
Cloud Services Realms Identity Sources High	igh Availability	eStreamer	Host Input C	lient Sn	nart Software N	Manager On-Prem
Naar hoge beschikbaarheid navigeren						
Stap 5. Klik op Secundair.						
Firewall Management Center Integration / Other Integrations / High Availability Overview Anal	lysis Policies Dev	vices Objects	Integration	Deploy	० 📀 🌣 🔞	admin • alada SECURE
Cloud Services Realms Identity Sources High Availability eStrea	amer Host Input Client	Smart Software	Manager On-Prem			Peer Manager
Select a role for this Management Center and specify peer details to set Role For This Firewall Management Center:	tup high availability.					

Firewall	Manager / Other Integr	ment Center rations / High Availabilit	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 Sm	hart Software I	Manager On-Prem						
Select a role for	r this Manag wall Manager	gement Center and	specify peer detai	Is to setup hig	gh availability	y.								
 Standalone (N 	lo High Availa	ability)												
O Primary														
Secondary														

Invoer informatie en selecteer de gewenste rol voor het huidige VCC

Stap 6. Voer informatie in van de primaire/actieve peer en klik op Register.

Cloud Services	Realms	Identity Sources	High Availability	eStreamer	Host Input Client	Smart Software Manager On-Prem	r oci managor
Select a role for	this Manag	ement Center and	specify peer detail	s to setup hig	h availability.		
Role For This Firev	vall Managen o High Availa	ent Center: bility)					
O Primary							
 Secondary 							
Peer Details:							
After Firewall Man Primary Firewall M 10.18.19.31	agement Cer anagement (ter high availability is center Host:	configured in virtual o	or cloud environ	ment, 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.						



Opmerking: Neem nota van de registratiesleutel, aangezien deze op het actieve VCC zal worden gebruikt.

Warning

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





Opmerking: Zorg ervoor dat er geen andere taak wordt uitgevoerd terwijl HA wordt gemaakt, de GUI wordt opnieuw gestart.

Stap 8. Bevestig dat u de primaire peer wilt registreren.



Do you want to register primary peer: 10.18.19.31?





Waarschuwing: Alle informatie over de Apparaten/Beleid/Configuratie zal worden verwijderd uit Secundair FMC zodra HA wordt gemaakt.

Stap 9. Controleer of de status van het secundaire VCC hangende is.

Firev Integra	vall Manage tion / Other Integ	ment Cen grations / Peer	ter Manager	Overview	Analysis	Policies	Devices	Objects	Integration	Deploy	Q	0	≎	🕜 admin 🔻	alialia cisco	SECURE
Cloud Servi	ces Realms	Identity S	Sources	High Availability	eStreamer	Host Inp	ut Client	Smart Softwar	e Manager On-Prem							
Host			Last Modifi	ed			s	Status				S	tate			
10.18.19.31			2023-09-2	28 13:53:56			P	ending Registratio	n				0			1

Primair VCC configureren

Herhaal stap 1 t/m 4 op het primaire/actieve VCC.

Stap 5. Klik op Primair.

Firewall Ma Integration / Oth	anagement her Integrations /	Center / High Availability	Overview	Analysis	Policies	Devices	Objects	Integration	Deploy	Q	0	¢ 6	admin 🔹	cisco SECURE
Cloud Services Re	ealms Iden	tity Sources	High Availability	eStreamer	Host Input	Client Sn	nart Software M	Aanager On-Prem						Peer Manager
Select a role for this	s Managemen	t Center and s	specify peer detail	s to setup hig	gh availability	у.								
Role For This Firewall N	Management Ce gh Availability)	enter:												
Primary														
 Secondary 														
Peer Details: Configure the seconda After Firewall Managen Secondary Firewall Ma	ary Managemen ment Center hig anagement Cent	t Center with de h availability is o ter Host:	atails of the primary b configured in virtual c	efore registrati or cloud enviror	on. nment, each re	egistered Fire	wall Threat Def	ense consumes an a	dditional Fire	power	MCv D	evice li	icense.	
Registration Key*:]												
Unique NAT ID:]												
Register † Either host or NAT ID is r	required.													

Stap 6. Voer de informatie over het secundaire VCC in en klik op Registreren.

							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 detai	ls to setup hig	h availability.		
Role For This Firev	vall Managem	nent Center:					
 Standalone (Network) 	o High Availa	bility)					
Primary							
 Secondary 							
Peer Details:							
Configure the seco	ondary Manag	gement Center with d	letails of the primary I	before registratio	on.	Eircurall Threat Defense consumes on additional Eirconnuer MCu Device license	
Secondary Firewal	I Managemer	nt Center Host:	conligured in virtual	or cloud environ	ment, each registered	a Prewait Threat befense consumes an additional Prepower MCV bevice license.	
10.18.19.32							
Registration Key*:							
cisco123							
Unique NAT ID:							
Register							
† Either host or NAT I	D is required.						



Opmerking: Gebruik dezelfde registratiesleutel die als secundair VCC wordt gebruikt.

Stap 7. Met deze waarschuwing kunt u dit bevestigen door te klikken op yes.

Warning

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





Opmerking: Zorg ervoor dat er geen andere taak wordt uitgevoerd.

Stap 8. Bevestig dat u zich wilt registreren voor secundair FMC.

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?





Opmerking: Zorg ervoor dat er geen kritieke informatie over het secundaire VCC is, aangezien het aanvaarden van deze prompt alle configuraties uit het VCC verwijdert.

synchronisatie tussen primaire en secundaire start; de duur hangt af van de configuratie en de apparaten. Dit proces kan vanaf beide eenheden worden gevolgd.

	Firewall Integration /	Managen Other Integra	nent Cent ations / High A	er vailability	Overview	Analysis	Policies	Devices	Objects	Integration	Deploy	Q	¢	🛿 admin 🕇	cisco SECURE
															Peer Manager
Cloud	Services	Realms	Identity Sou	rces	High Availability	eStreamer	Host Input	t Client Si	mart Software M	Manager On-Prer	m				
										Switch Peer Ro	oles 🏟	Break H/		II Pause Sy	nchronization
				High ava These op Database	ilability operations a perations include file e files synchronization	re in progress. The copy which may t on: 100% of 379Mi	e status messa ake time to co 8 transferred	ages and alerts omplete.	on this page are	e temporary. Pleas	e check after hig	h availabil	ty operat	ions are comple	te. ×
	Summa	ary						S	ystem Statu	IS					
	Status		A Tem	porarily	degraded- high ava	ailability operation p	ns are in rogress.			1	Local Active - Primary (10.18.19.31)	,	Stand	Remote Iby - Seconda (10.18.19.32)	ry
	Synchron	nization				4	Failed	c	perating Syste	m	7.2.5			7.2.5	
	Active S	ystem				10.1	8.19.31	s	oftware Versio	n	7.2.5-208			7.2.5-208	
	Standby	System				10.1	8.19.32	Ν	lodel	Secure	e Firewall Mana Center for VMwa	gement re	S Mana	ecure Firewall gement Center VMware	for



Opmerking: Terwijl de synchronisatie plaatsvindt, verwacht dat de status Mislukt en Tijdelijk gedegradeerd wordt. Deze status wordt weergegeven totdat het proces is voltooid.

Verificatie

Zodra de synchronisatie is voltooid, is de verwachte uitvoer Status Gezond en Synchronisatie OK.

Firewal	II Manage	ment Center rations / High Availability	Overview	Analysis	Policies	Devices	o Objects	Integration	Deploy	Q	0	\$	🛛 admin	• diale SEC
														Peer Manag
Cloud Services	Realms	Identity Sources	High Availability	eStreamer	Host Input	Client	Smart Software M	lanager On-Pr	em					
							4	Switch Peer I	Roles 🏟	Break H	łA	חר	II Pause S	ynchronization
Sumn	nary					11	System Status	S						
Status				O H	lealthy				Local			Standb	Remote	201
Synch	ronization				OK				(10.18.19.31)	y	,	(10	.18.19.32)	ai y
Active	System			10.18	3.19.31		Operating System	n	7.2.5				7.2.5	
Standt	by System			10.18	.19.32		Software Version	i.	7.2.5-208			7	2.5-208	
							Model	Secu	re Firewall Mana Center for VMwa	gement ire	N	Seci Manage	ure Firewal ment Cente /Mware	r for

De primaire en secundaire synchronisatie behouden; dit is normaal.

Firewall Management Center Integration / Other Integrations / High Availability	Devices Integration		٩	ວ 🌣 🕜 admin ▾ 🖓🖑 SECURE
Cloud Services High Availability eStreamer	Host Input Client			Peer Manager
		Switc	ch Peer Roles 🛛 🏟 Break HA	II Pause Synchronization
Summany		System Status		
Status	Synchronization task is in progress	oystem otatus	Local	Remote
Synchronization	📀 ОК		(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

Neem even de tijd om te bekijken of uw apparaten correct worden weergegeven op zowel Primair als Secundair.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.