Secure Firewall Management Center in HA-Paar ersetzen

Inhalt

Einleitung Voraussetzungen Anforderungen Verwendete Komponenten Konfigurieren Lösung 1 Verfahren zum Ersetzen einer fehlerhaften Einheit durch ein Backup Lösung 2 Verfahren zum Austausch einer fehlerhaften Einheit ohne Backup Verifizierung Fehlerbehebung Zugehörige Informationen

Einleitung

In diesem Dokument wird beschrieben, wie ein fehlerhaftes Secure Firewall Management Center in einem Hochverfügbarkeitspaar ersetzt wird.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie dieses Thema kennen:

Cisco Secure Firewall Management Center (FMC)

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

• Cisco Secure Firewall Management Center (FMC) mit Version 7.2.5 (1) im HA-Modus

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.

Konfigurieren

Lösung 1

Verfahren zum Ersetzen einer fehlerhaften Einheit durch ein Backup

Schritt 1: Zuweisen der Betriebseinheit als aktiv. Weitere Informationen finden Sie unter <u>Switching</u> <u>Peers in the Management Center High Availability Pair.</u>

Firew Integrate	rall Managen	ent Center fors / High Availabili	y Devices	Integration					Q 🧬 Ö 🙆 admin	• toto secure
Cloud Services	s Hich Availa	sibv eStreamer	Host Incut Clier	at a						Peer Manager
								Switch Peer Role	s Ø Break HA II Pause S	ynchronization
	Summary						System Status			
	Status				Degraded- Synchronization income (No connection between high availability Management Cent	plete ters)		Local Standby - Secondary (10.28.1.150)	Remote Active - Primary (10.28.1.149)	
	Synchronization				▲ F	ailed	Operating System	7.2.5	7.2.5	
	Active System				10.28.1 (HA synchronization time : Thu Apr 11 20:31:24 20	024)	Software Version	7.2.5.1-29	7.2.5.1-29	
	Standby System	1			10.28.1 (HA synchronization time : Thu Apr 11 20:30:08 20	1.150 024)	Model	Secure Firewall Management Center for VMware	Secure Firewall Management Center for VMware	
Firew	vall Manager	nent Center	Devices	Integration					ද 💕 ඊ 🛚 admin	- dut SECURE
					•					
Cloud Service	s High Avails	bilty eStreame	Host Input Clie	nt						Peer Manager
								Switch Peer Role		nchronization
	Summary						System Status			
	Status		(No connecti	on between hig	Degraded - Synchronization incom h availability Management Centers , Database is not running in availability m	plete high ode)		Local Standby - Secondary (10.28.1.150)	Remote Active - Primary (10.28.1.149)	
	Synchronizatio				🔺 F	alled	Operating System	7.2.5	7.2.5	
	Active System				10.28.1 (HA synchronization time : Thu Apr 11 20:31:24 20	024)	Software Version	7.2.5.1-29	7.2.5.1-29	
	Standby Syste				10.28.1 (HA synchronization time : Thu Apr 11 20:30:08 20	1.150 024)	Model	Secure Firewall Management Center for VMware	VMware	
								Switching Roles	ø	
					We The	larning is operation may affect o background. Do you wi	nikal processes running in et to continue?	Active Management Center is unavailable. Making this Managem Center active will cause split brain when the old active comes up. Do want to continue?	ent you OK	

Schritt 2: Erstellen Sie ein neues Image des neuen Geräts, das mit der Softwareversion des aktiven Geräts übereinstimmt. Weitere Informationen finden Sie unter <u>Reimage a Hardware Model</u> of a Cisco Secure Firewall Management Center (Hardware-Modell eines Cisco Secure Firewall Management Center neu erstellen).

Schritt 3: Stellen Sie die Datensicherung vom ausgefallenen Gerät im neuen Verwaltungscenter wieder her. Navigieren Sie zu System > Backup/Restore (System > Sichern/Wiederherstellen), laden Sie die Sicherungsdatei hoch, und stellen Sie sie auf dem neuen Gerät wieder her.

Firewall Management Center System / Tools / Backup/Restore / Backup Management Overview Analysis	Policies Devices Objects	Integration			D	eploy Q 💕 Ö 😡	admin •	SECURE	
Backup Management Backup Profiles								emote Storage	
				Firewall Manage	ment Backu	D Managed Device Bac	kup Upi	and Backup	
		Info New backups found on system. Importing Xackup information.							
Firewall Management Backups									
System Information	Date Created	File Name	VDB Version	Location	Size (M8)	Configurations	Events	TID	
Secure Firewall Management Center for VMware v7.2.5.1	2024-04-11 16:50:31	Backup_Active_00-2024-04-10T23-07-42.tar	build 353	Local	250	Yes	Yes	Yes	
Impower Green Firewall Management Center for VMware v7.2.5.1	2024-04-11 16:22:24	Backup_NewUnit_00-2024-04-11120-17-36.tar	build 353	Local	236	Yes	Yes	Yes	
Restore Download Delete More Storage Location: Anriht/backup/ (Disk Usage: 9%) Storage Location: Anriht/backup/ (Disk Usage: 9%)									
Firewall Management Center Overvew Anayss Posces	Devices Objects Integration				L	xepnoy Q, GF Q, G	admin • ;	note Storage	
		Info 9 You are about to replace or modify key yushes likes. The system will be reborted at the end of the restore process.							
	Restore Replace	Backup Bane Backup.Active_00-2024-04-10123-07-42.ter Configuration Data Restore Found Data Thread-Intelligence Director Data							

Schritt 4: Aktualisieren Sie ggf. die gleiche Version der Geolocation-Datenbank-Updates (GeoDB), der Schwachstellendatenbank-Updates (VDB) und der Systemsoftware-Updates wie die aktive Einheit, um die Konsistenz sicherzustellen.

New Unit

Active Unit

× X disco SECURE cisco SECURE Firewall Management Center Firewall Management Center Version 7.2.5.1 (build 29) Version 7.2.5.1 (build 29) Secure Firewall Management Center for VMware Model Secure Firewall Management Center for VMware Model Serial Number None Serial Number None 2.9.20 (Build 5100) 3.1.21.501 (Build 26) 2.9.20 (Build 5100) Snort Version Snort Version
 Los 20 (bitle 5100)

 Snort3 Version
 3.1.21.501 (Build 26)

 Rule Pack Version
 2655

 Module Pack Version
 3019

 LSP Version
 Isp-rel-20220511-1540
 Snort3 Version Rule Pack Version 2655 Module Pack Version 3019 LSP Version lsp-rel-20220511-1540 VDB Version build 353 (2022-03-07 22:13:19) VDB Version build 353 (2022-03-07 22:13:19) Rule Update Version 2022-01-06-001-vrt Rule Update Version 2022-01-06-001-vrt Geolocation Update Version Country Code: 2022-05-11-103, IP: None Geolocation Update Version Country Code: 2022-05-11-103, IP: None Cisco Firepower Extensible Operating System (FX-OS) 0S OS Cisco Firepower Extensible Operating System (FX-OS) 2.12.0 (build 519) 2.12.0 (build 519) Hostname firepower Hostname firepower m questions, email tac@cisco.com phone: 1-800-553-2447 or email tac@cisco.com phone: 1-800-553-2447 or 1-408-526-7209. Copyright 2004-2023, Cisco and/or its affiliates. All rights rese 1-408-526-7209. Copyright 2004-2023, Cisco and/or its affliates. All rights reserved. Copy Close Copy Close

Schritt 5: Sobald die Updates abgeschlossen sind, können beide Geräte einen aktiven Status anzeigen, was zu einem HA-Split-Brain-Zustand führen kann.

Schritt 6: Setzen Sie das Gerät, das kontinuierlich in Betrieb war, manuell als aktiv ein. Dadurch kann die neueste Konfiguration mit der Ersatzeinheit synchronisiert werden.

Firew	vall Manager ton / Other Integ	ment Center	Overview	Analysis	Policies	Devices	Objects	Integration	n						Deploy	a 🛷	o e adr	nin + SECUR
Cloud Service	s Realms	Identity Sources	High Availability	eStreamer	Host Inp	ut Client Sm	art Software	e Manager On-i	Prem									Peer Manager
														E2 Moke Me Ad	5×0	Brook HA	II Paul	e Synchronization
								n	This high availabili	ility pair is in split bra	in. Make one Management Ce	enter active by clic	king 'Make Me Active'. >	¢				
	Summary								_		System Status							
	Status				▲ Sp	it Brain - Manag (Database	ement Cent	ter is active on t gured for high a	both peers. evaluability)				Local Split Brain - S	econdary	50	Remote lit Brain - Prime	ry.	
	Synchronizatio	on .				(A Failed				(10.28.1	1500		(10.28.1.149)		
	Active System					H& supchronizati	ion time : T	1 Avr 11 21 00	0.28.1.150		Software Version		7.25.1	-29		7.2.5		
	Standby Syste	m				HA synchronized	ion time : Th	1 hu Apr 11 21:03	10.28.1.149 3:00 2024)		Model	9	ecure Firewall Managem	ent Center for VMware	Secure Fire	wali Manageme VMware	nt Center for	
High Av	vailability	eStreamer	Host Input Clier	nt Sr	mart Softw	are Manager	r On-Prer	m										
															Make M	e Active	4	Break HA
							This !	high availabil	lity pair is in t	split brain. Mak	te one Management C	enter active b	y clicking 'Make Me	Active'. 🗙				
										Syste	em Status							
			🔺 Split Brail (n - Mana Database	gement Ce e is not co	enter is active infigured for I	e on both high avail	a peers. lability)					Spl	Local it Brain - Second (10.28.1.150)	lary		Sp	Remote lit Brain - Primar (10.28.1.149)
							4	Failed		Opera	ating System			7.2.5				7.2.5
			(HA syr	nchroniza	ition time :	Thu Apr 11	10.20 21:03:25	8.1.150		Softw	are Version			7.2.5.1-29				7.2.5.1-29
			(HA sy	nchroniza	ition time :	Thu Apr 11	10.20 21:03:00	8.1.149 2024)		Mode	ı		Secure Firewal	Management Ce	inter for VMv	vare Se	cure Fire	vall Management VMware
							P						Make Me	Active		0		
								Warning					Do you war Center acti	nt to make this ve and peer st	Managem andby?	ent		
This optime bac other pr overwritistandby			This operati the backgro other peer v overwrite co standby pee	ion may affe bund. The lo will become onfiguration er. Do you w	ect critical pro ocal peer will t e a standby. Th n and policies p want to continu	cesses running in the active and the the active peer will present on the ue?			Q	insel	ОК							
							L			(No							

Schritt 7: Navigieren Sie bei erfolgreicher Synchronisierung, die einige Zeit in Anspruch nehmen kann, zur Webschnittstelle der aktiven Einheit. Ändern Sie dann die Rollen, und positionieren Sie die neue Einheit als aktive Appliance.

Lösung 2

Verfahren zum Austausch einer fehlerhaften Einheit ohne Backup

Schritt 1: Zuweisen der Betriebseinheit als aktiv. Weitere Informationen finden Sie unter <u>Switching</u> <u>Peers in the Management Center High Availability Pair.</u>

Firewall Management Center	Devices Integration			Q 💕 Ø 🛛 admin •
Cloud Services High Availability eStreamer	Host Input Client			Peer Manager
			Switch Peer Role	6 Preak HA II Pause Synchronization
Summary		System Status	/	
Status	▲ Degraded - Synchronization incomplete (No connection between high availability Management Centers , Database is not running in high availability mode)		Local Standby - Primary (10.28.1.149)	Remote Active - Secondary (10.28.1.150)
Synchronization	🔺 Failed	Operating System	7.2.5	7.2.5
Active System	10.28.1.150	Software Version	7.2.5.1-29	7.2.5.1-29
Standby System	(HA synchronization time : Thu Apr 11 21:55:43 2024) 10.28.124 (HA synchronization time : Thu Apr 11 27:56:42 2021	Model	Secure Firewall Management Center for VMware	Secure Finewall Management Center for VMware
	Warning			
	This operation may affect critical pro the background. Do you want to cor	ocesses running in ntinue?		_
			Switching Roles	
			Active Management Center is unavailable. Making this Management Center active will cause spill brain, when the old active comes up. Do you want to continue?	
			Cancel	

Schritt 2: Erstellen Sie ein neues Image des neuen Geräts, das mit der Softwareversion des aktiven Geräts übereinstimmt. Weitere Informationen finden Sie unter <u>Rimage a Hardware Model</u> of a Cisco Secure Firewall Management Center (Hardware-Modell eines Cisco Secure Firewall Management Center neu erstellen).

Schritt 3: Aktualisieren Sie ggf. dieselbe Version der Geolocation-Datenbank-Updates (GeoDB), der Schwachstellendatenbank-Updates (VDB) und der Systemsoftware-Updates wie die aktive Einheit, um die Konsistenz sicherzustellen.

Operational Unit

× × cisco SECURE cisco SECURE Firewall Management Center Firewall Management Center Version 7.2.5.1 (build 29) Version 7.2.5.1 (build 29) Secure Firewall Management Center for VMware Model Secure Firewall Management Center for VMware Model Serial Number None Serial Number None Snort Version 2.9.20 (Build 5100) 2.9.20 (Build 5100) Snort Version 3.1.21.501 (Build 26) Snort3 Version Snort3 Version 3.1.21.501 (Build 26) 2655 3019 Rule Pack Version 2655 Rule Pack Version Module Pack Version Module Pack Version 3019 lsp-rel-20220511-1540 LSP Version LSP Version lsp-rel-20220511-1540 VDB Version build 353 (2022-03-07 22:13:19) build 353 (2022-03-07 22:13:19) VDB Version Rule Update Version 2022-01-06-001-vrt Rule Update Version 2022-01-06-001-vrt Geolocation Update Version Country Code: 2022-05-11-103, IP: None Geolocation Update Version Country Code: 2022-05-11-103, IP: None 05 Cisco Firepower Extensible Operating System (FX-OS) 0S Cisco Firepower Extensible Operating System (FX-OS) 2.12.0 (build 519) 2.12.0 (build 519) Hostname frecower Hostname frepower mail tac@cisco.com phone: 1-800-553-2447 or For technical/system questions, email tac@cisco.com phone: 1-800-553-2447 or 1-408-526-7209. Copyright 2004-2023, Cisco and/or its affiliates. All rights reserved. Cisco.com phone: 1-800-553-2447 or 1-408-526-7209. Copyright 2004-2023, Cisco and/or its affiliates. All rights rese Copy Copy

Schritt 4: Verwenden Sie die Webschnittstelle des aktiven Management Centers, um die hohe Verfügbarkeit zu unterbrechen. Wenn Sie dazu aufgefordert werden, wählen Sie die Option zum Verwalten registrierter Geräte von dieser Konsole aus.

Replacement

Firev	vall Management Center tion / Other Integrations / High Avail	ability Overview Analysis Policies Devices Object	s Integration			Deploy Q 💕 Ö 🛛 admin •
Cloud Service	s Realms Identity Source	s High Availability eStreamer Host Input Client Smart Softwa	re Manager On-Prem			Peer Manager
					Switch Peer Rol	es Break HA II Pause Synchronization
	Summary			System Status		
	Status	Degraded- (No connection between high availability Management Centers , Da	Synchronization incomplete tabase is not configured for high availability)		Local Active - Primary (10.28.1.149)	Remote Standby - Secondary (10.28.1.150)
	Synchronization		A Failed	Operating System	7.2.5	7.2.5
	Active System	[MA surchmentation time -	10.28.1.149	Software Version	7.2.5.1-29	7.2.5.1-29
	Standby System	(HA synchronization time :	Break HA	0	Secure Firewall Management Center for VMware	Secure Firewall Management Center for VMware
			How do you want to manager	devices after breaking high availability? vices from this console.		
			All devices will be unregistere	d from peer console.		

Schritt 5: Konfigurieren Sie die HA des Management Centers neu, indem Sie das Management Center als primäre und die Ersatzeinheit als sekundäre Einheit konfigurieren. Ausführliche Anweisungen finden Sie unter <u>Einrichten der Hochverfügbarkeit von Management Center.</u>



Hinweis: Wenn die hohe Verfügbarkeit wiederhergestellt ist, wird die aktuelle Konfiguration des primären Management Centers mit dem sekundären Management Center synchronisiert. Sowohl Classic- als auch Smart-Lizenzen sind für eine reibungslose Integration konzipiert.

Verifizierung

Verwenden Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

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

Firewall Management Center Integration / Other Integrations / High Availability	Overview Analysis	Policies Devices Objects Integration			Deploy Q 🥙 🖄 🙆 admin 🔹 👬 SECURI
Cloud Services Realms Identity Sources High A	Availability eStreamer	Host Input Client Smart Software Manager On-Prem			Peer Manager
				Switch Peer Rol	es 🛛 🖶 Break HA 🛛 🔢 Pause Synchronization
Summary			System Status		
Status		Healthy		Local Active - Primary	Remote Standby - Secondary
Synchronization		O OK		(10.28.1.149)	(10.28.1.150)
Active System		10.28.1.149	Operating System	7.2.5	7.2.5
		(HA synchronization time : Thu Apr 11 20:11:21 2024)	Software Version	7.2.5.1-29	7.2.5.1-29
Standby System		10.28.1.150 (HA synchronization time : Thu Apr 11 20:10:03 2024)	Model	Secure Firewall Management Center for VMware	Secure Firewall Management Center for VMware

Da dieser Vorgang einige Zeit in Anspruch nehmen kann, werden die primären und sekundären Einheiten noch synchronisiert. Stellen Sie während dieses Zeitraums sicher, dass Ihre Geräte sowohl in der primären als auch in der sekundären Einheit korrekt aufgeführt sind.

Darüber hinaus kann die Überprüfung über die CLI durchgeführt werden. Erreicht wird dies durch die Verbindung mit der CLI, den Wechsel in den Expertenmodus, die Erweiterung der Berechtigungen und die Ausführung der folgenden Skripte:

<#root> fmc1:/Volume/home/admin# troubleshoot_HADC.pl 1 Show HA Info Of FMC 2 Execute Sybase DBPing 3 Show Arbiter Status Check Peer Connectivity 4 Print Messages of AQ Task 5 Show FMC HA Operations History (ASC order) 6 Dump To File: FMC HA Operations History (ASC order) 7 8 Last Successful Periodic Sync Time (When it completed) Print HA Status Messages 9 10 Compare active and standby device list 11 Check manager status of standby missing devices 12 Check critical PM processes details 13 Help

0 Exit

<#ro	ot>
------	-----

fmc1:/Volume/home/admin#

troubleshoot_HADC.pl

1 Show HA Info Of FMC

2 Execute Sybase DBPing 3 Show Arbiter Status 4 Check Peer Connectivity 5 Print Messages of AQ Task 6 Show FMC HA Operations History (ASC order) 7 Dump To File: FMC HA Operations History (ASC order) 8 Help 0 Exit

Weitere Informationen finden Sie unter <u>Überprüfen des FirePOWER-Modus, der Instanz, der</u> <u>Hochverfügbarkeit und der Skalierbarkeitskonfiguration.</u>

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

- <u>Cisco Secure Firewall Management Center Administrationshandbuch, 7.4. Hohe</u> <u>Verfügbarkeit</u>
- <u>Technischer Support und Downloads von Cisco</u>

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.