識別和分析FMC上的FTD故障轉移事件

目錄

<u>簡介</u>
<u>必要條件</u>
<u>需求</u>
<u>採用元件</u>
<u>背景資訊</u>
<u>FMC上的故障轉移事件</u>
<u>步驟 1.運行狀況策略配置</u>
<u>步驟 2.策略分配</u>
<u>步驟3.故障轉移事件警報</u>
步驟4.歷史故障轉移事件
<u>步驟 5.高可用性儀表板</u>
步驟 6.威脅防禦CLI

<u>相關資訊</u>

簡介

本文檔介紹如何識別和分析安全防火牆管理中心GUI上安全防火牆威脅防禦的故障轉移事件。

必要條件

需求

思科建議您瞭解以下主題:

- 適用於思科安全防火牆威脅防禦(FTD)的高可用性(HA)設定
- 思科防火牆管理中心(FMC)的基本可用性

採用元件

本文中的資訊係根據以下軟體和硬體版本:

- Cisco FMC v7.2.5
- Cisco Firepower 9300系列v7.2.5

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路運作中,請確保您瞭解任何指令可能造成的影響。

背景資訊

FMC不僅是Firepower裝置的管理中心,而且除了管理和配置選項之外,它還提供了一個圖形介面

,有助於即時分析日誌和事件。

當談到故障切換時,介面有了新的改進,有助於分析故障切換事件以瞭解故障。

FMC上的故障轉移事件

步驟 1.運行狀況策略配置

預設情況下,模組集群/HA Failure Status在運行狀況策略上啟用,但您也可以啟用Split-brain檢查 選項。

若要啟用運行狀況策略中的HA選項,請導航至 System > Health > Policy > Firewall Threat Defense Health Policy > High Avilability.

此映像描述運行狀況策略的HA配置:

System / Hea	Management Center	Overview	Analysis	Policies	Devices	Objects	Integration
Initial_Health_ Initial Health Policy	Policy 2023-08-29 15:2	6:44 🖋					
Health Modules		Disk Usage Monitors disk us Warning threes 85 % Warning Three 97 %	age shold shold (second	ary HD)	Critical thres 90 % Critical Thres 99 %	hold shold (secondary	(HD)
		 High Availa Cluster/HA Monitors cluster Firewall Thread Monitors Firewal Integration 	Ability Failure Statu and HA member eat Defense	IS rs for their availat HA (Split-b HA for split-brai	pility failure rain check) n (Both HA mer	mbers are in active :	state)

高可用性運行狀況設定

步驟 2.策略分配

確保將運行狀況策略分配給要從FMC監控的HA對。

要分配策略,請導航至 System > Health > Policy > Firewall Threat Defense Health Policy > Policy Assignments & Deploy.

此圖顯示如何將運行狀況策略分配給HA配對:



HA分配

分配並儲存策略後,FMC會自動將其應用到FTD。

步驟 3.故障轉移事件警報

根據HA的配置,一旦觸發了故障切換事件,將顯示描述故障切換故障的彈出警報。

此圖顯示生成的故障切換警報:

Devices	Objects Integ	ration		Deploy	Q 🧐 🌣 Ø admin ▼ 🔤 🐯 SECURE
					Dismiss all notifications
t Pending (0)	Upgrade (0) Version	Chassis	Licenses	Access Control Pe	Cluster/Failover Status - 10.82.141.169 × SECONDARY (FLM1946BCEX) FAILOVER_STATE_ACTIVE (Inspection engine in other unit has failed(My failed services Peer failed services-diskstatus)) PRIMARY (FLM19389LQR) FAILOVER_STATE_STANDBY (Check peer event for reason)
with FTD	7.2.5	IIII F241-24-04-FPR9K-1.cisco.com;443 Security Module - 1	Essentials, IPS (2 more)	FTD HA	Cluster/Failover Status - 10.82.141.171 × PRIMARY (FLM19389LQR) FAILOVER_STATE_STANDBY (Other unit wants me Standby) PRIMARY (FLM19389LQR) FAILOVER_STATE_STANDBY_FAILED (Detect Inspection engine failure(My failed services- diskstatus Peer failed services-)
with FTD	7.2.5	F241-F241-24-4-FPR9K-2.cisco.com:4 III Security Module - 1	Essentials, IPS (2 more)	FTD HA	Bisk Usage - 10.82.141.171 × /ngfw using 98%: 186G (5.5G Avail) of 191G

故障切換警報

您也可以導航至 Notifications > Health 以便視覺化故障切換運行狀況警報。

此圖顯示了通知下的故障切換警報:

Firewall Management Center Overview Analy Devices / Device Management Overview	sis Policies Devices	Objects	Integration	Deploy Q 🥙 🌣 🕢 admin 🔹 🕬
View By: Group • All (2) • Error (2) • Warning (0) • Offline (0) • Normal	(0) • Deployment Pending	(0) • Upgr	ade (0)	Deployments Upgrades Health Tasks Show Notifications 209-total 15 warnings 7 critical 0 errors Q. Filter
Collacte All Image: Collacte All Image: Collacte All	Model	Version	Chassis	Smart License Monitor Smart Agent is not registered with Smart Licensing Cloud URL Filtering Monitor URL Filtering registration failure
 Ungrouped (1) FTD-HA 				Devices 10.82.141.169 Interface Status Interface 'Ethernet1/2' is not receiving any packets Interface 'Ethernet1/3' is not receiving any packets
10.82.141.169(Secondary, Active) 10.82.141.169 - Routed	Firepower 9300 with FTD	7.2.5	E241-24-04-FPR9K-1 Security Module - 1	Interface "Ethernet1/4" is not receiving any packets 10.82.141.171 Disk Usage /ngfw using 98%: 1866 (5.46 Avail) of 191G Interface Status Interface "Ethernet1/2" is not receiving any packets
10.82.141.171(Primary, Failed)	Firepower 9300 with FTD	7.2.5	E241-F241-24-4-FPR Security Module - 1	Interface "Ethernet1/3" is not receiving any packets Interface "Ethernet1/4" is not receiving any packets

HA通知

步驟 4.歷史故障轉移事件

FMC提供了一種顯示過去發生的故障切換事件的方式。要過濾事件,請導航至 System > Health > Events > Edit Search 並指定Module Name為Cluster/Failover Status。此外,還可以根據狀態應用過濾器。

此圖顯示如何過濾故障轉移事件:

Module Name	Cluster/Failover Status	Disk Status, Interface Status
Value		25
Description		Sample Description
Units		unit
Status	Warning	Critical, Warning, Normal, Recovered

故障轉移篩選器消息

您可以調整時間設定以顯示特定日期和時間的事件。要修改時間設定,請導航至 System > Health > Events > Time.

此圖顯示如何編輯時間設定:

																	Bookmark This Page Re	porting	Workflows,	View Bookmarks Sear
																		11 2023	3-09-27 11:02:0	0 - 2023-09-28 11:08 Expand
Search Constraints (Edit Search Sa	ve Search)										20	23-09	28 11	14						
ealth Monitor Table View of He	alth Events	A Not	Secure	http	is://10	.82.14	1.165	/date/tin	ne_rang	e.cgi?	page	_type=	lealti	%201	Ionitor	ing&formnam	e=eventform&start_end=169582692	-		
		Healt	h Moni	toring	Time \	Windo	w	Prefere	ences											
Module Name ×	Test Name ×					_	_	_										×	Status ×	Device ×
Cluster/Failover Status	Cluster/Failover Status	Exp	anding	Time \	Windo	w													4	10.82.141.171
Cluster/Failover Status	Cluster/Failover Status	Start 1	Time						End	lime	7		_	_	_	Presets			4	10.82.141.169
Cluster/Failover Status	Cluster/Failover Status	2023	3-09-2	7 11:02		11 .	7.6	2 -	202	3-09-	28 11	:14	100			Last	Current.			10.82.141.169
Cluster/Failover Status	Cluster/Failover Status								1000			7001222				Last	Current		A	10.82.141.171
Cluster/Failover Status	Cluster/Failover Status	1< <		Septer	mber	2023		>>	1<	<	Sep	stembe	2023	h i	>>	1 nour	Day			10.82.141.171
Cluster/Failover Status	Cluster/Failover Status	SU	MO	TU	WE	TH	FR	SA	SI	MO	TR	J WE	TH	FR	SA	t day	Marth		4	10.82.141.169
Cluster/Failover Status	Cluster/Failover Status	27	28	29	30	31	1	2	23		33	10.30			283	1 wook	Supplication with		*	10.82.141.171
Cluster/Failover Status	Cluster/Failover Status	3	4	5	6	7	8	9		- 14			12	8)	2.9.1	2 wooks	Synchronize with		*	10.82.141.171
Cluster/Failover Status	Cluster/Failover Status	10	11	12	13	14	15	16			1.13		3.4			1 month	Fuents Time Mindow			10.82,141,169
Cluster/Failover Status	Cluster/Failover Status	17	18	19	20	21	22	23				3) 20	21				Events rang window			10.82.141.169
Cluster/Failover Status	Cluster/Failover Status	24	25	26	21	28	2900	30					- 280	29						10.82.141.171
Cluster/Failover Status	Cluster/Failover Status		2.	3	A.	-0	0	<u>^</u> ,		- 2		4	- 5	0]	Any changes made will take effect	0.00	A	10.82.141.171
Cluster/Failover Status	Cluster/Failover Status												1 da	y, 12 r	ninute	5	on the next page load			10.82.141.169
Cluster/Failover Status	Cluster/Failover Status																	10	A	10.82.141.171

時間篩選器

一旦識別出事件,為了確認事件的原因,請將游標指向「說明」下。

此圖顯示如何得知容錯移轉的原因。

Firewall Management C System / Health / Events	Center Overview	Analysis Policies	Devices	Objects Inte	ration	De	ploy Q	6 0	admin 🔻 ;	diada SECURE
						Bookmark This Pag	e Reporting	Workflows ₊	View Bookm	arks Search
Search Constraints (Edit Search Sav	e Search)						11 202	3-09-27 11:1	1:00 - 2023-0	9-28 12:38:42 Expanding
Health Monitor Table View of Hea	ith Events			-						
Module Name ×	Test Name ×	↓ Time ×		Description ×		Value ×	Units ×	Status ×	Device ×	
Cluster/Failover Status	Cluster/Failover Status	2023-09-28 11:4	1:52	PRIMARY (ELM1938	LOR) FAILOVER_STATE_STANDBY_FAIL PRIMARY (FLM19880.08) FAILOVES_STATE_STANDBYFAIL Impection engine failure(My failed diskatatus. Peer failed services-)).	D (Detect services-		*	10.82.14	11.171

步驟 5.高可用性儀表板

監視故障轉移的另一種方法位於 System > Health Montitor > Select Active or Standby Unit.

HA監控器會提供有關HA和狀態連結、受監控介面、ROL的狀態以及每個裝置上的警報狀態的資訊 。

此圖顯示HA監控器:

Firewall Managemen System / Health / Monitor	t Center Overview Analysis Policies Devices	Objects Integration	Deploy Q 🧬 🌣 🕢 admin 🕶 🖏 SECURE
Monitoring) Gi Home	Health: 10.82.141.169(Active) Critical View System & Toubleshoot Dettals Overview CPU Memory Interfaces Connections	Snort ASP drops	Last 1 hour V 2023-09-28 11:47 - 2023-09-28 12:47
 Hrewal Management Center Devices (2) FTD-HA 10.82.141.169 Active 10.82.141.171 Starting + Inc. 	CPU Data collection for CPU module is disabled in the health policy, partial or no data may be shown. No Data Available	Memory Date Plane Avg 17 %; 11435555 Snort Avg 21 %; 2513736 System Avg 19 %; 2513736 100 %	Avg - all interfaces > Input Rate Avg 1-32 kbgs Output Rate Avg 1-32 kbgs Output Rate Avg 1-32 kbgs Output Rate Avg 1-32 kbgs Avg 1-32 kbgs Output Rate Avg 1-32 kbgs Output Rate Avg 1-32 kbgs Avg 1-3
	Connection Statistics Connections Ard 0.3.3 PAG 5.3.3 PAG 5.3.3.3 PAG 5.3.3 PAG 5.3	Process Health Critical Processes All Processes	High Availability Manage HA

運行狀況圖形

要直觀顯示警報,請導航至 System > Health Montitor > Select Active or Standby Unit > Select the Alerts.

Firewall Management Ce System / Health / Monitor	nter Overview	Analysis	Policies	Devices	Ob
Monitoring The Home Firewall Management Center Devices (2) FTD-HA 10.82.141.169 Active 10.82.141.171 Standby - F	Ith: 10.82.141.171 (System & Troubleshoot Det erview CPU U Data collection for CPU or no data may be show	(Standby - Failed) FTD-HA (HA-Stand 10.82.141.171 - Alerts: 2 / 4 Top 5 Alerts 9 Disk Usage 9 Interface Status 9 Firewall Threat D 9 Snort Identity M 9 Configuration Re	Critical Critical Critical O 17 Defense HA (Spl emory Usage esource Utilization	it-brain check) on View all alerts	Snc
	N	lo Data Availa	able		-

此映像顯示導致故障切換的磁碟狀態:

Hea	alth Alerts - 10.	82.141.17	'1			×
Di Di /nç	19 total sk Usage gfw using 98%: 186G (2 critical 5.4G Avail) of 1	0 warnings 91G see less	7 normal	Export Sep 28, 20	Run All 23 12:47 PM
	Local Disk Partition S Mount /mnt/boot /opt/cisco/config /opt/cisco/platform/l /var/data/cores /opt/cisco/csp /ngfw	tatus Size Free 7.5G 7.3G 1.9G 1.8G ogs 4.6G 4.3G 46G 43G 684G 4980 191G 5.4G	Used Percent 208M 3% 3.4M 1% 19M 1% 823M 2% 187G 28% 186G 98%			
Int Int Int Int	terface Status erface 'Ethernet1/2' is erface 'Ethernet1/3' is erface 'Ethernet1/4' is	not receiving a not receiving a not receiving a	ny packets ny packets ny packets see m	iore	Sep 28, 20	23 12:47 PM
o Ap All	opliance Heartbeat appliances are sending	g heartbeats co	prrectly.		Sep 28, 20	23 12:47 PM
	Itomatic Application	Dunace Stat	110		Son 20 20	22 12 47 DM

步驟 6.威脅防禦CLI

最後,為了收集有關FMC的其他資訊,您可以導航至 Devices > Troubleshoot > Threat Defense CLI. 配置引數 (如裝置和要執行的命令),然後按一下 Execute.

此圖顯示命令範例 show failover history 可以在FMC上執行,您可以在其中識別故障切換故障。



故障切換歷史記錄

相關資訊

- <u>FTD的高可用性</u>
- <u>在 Firepower 設備上設定 FTD 高可用性</u>
- <u>技術支援與文件 Cisco Systems</u>

關於此翻譯

思科已使用電腦和人工技術翻譯本文件,讓全世界的使用者能夠以自己的語言理解支援內容。請注 意,即使是最佳機器翻譯,也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準 確度概不負責,並建議一律查看原始英文文件(提供連結)。