Identifier et analyser les événements de basculement FTD sur FMC

Table des matières

Introduction Conditions préalables Exigences Composants utilisés Informations générales Événements de basculement sur FMC Étape 1. Configuration de la stratégie de santé Étape 2. Affectation de stratégie Étape 3. Alertes d'événements de basculement Étape 4. Événements de basculement Étape 5. Tableau de bord haute disponibilité Étape 6. CLI Threat Defense

Introduction

Ce document décrit comment identifier et analyser les événements de basculement pour Secure Firewall Threat Defense sur l'interface utilisateur graphique de Secure Firewall Management Center.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration haute disponibilité (HA) pour Cisco Secure Firewall Threat Defense (FTD)
- Facilité d'utilisation de base de Cisco Firewall Management Center (FMC)

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco FMC v7.2.5
- Gamme Cisco Firepower 9300 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

Le FMC n'est pas seulement le centre administratif des périphériques Firepower, au-delà des options de gestion et de configuration, il fournit également une interface graphique qui permet d'analyser les journaux et les événements en temps réel et passé.

En matière de basculement, l'interface présente de nouvelles améliorations qui permettent d'analyser les événements de basculement afin de comprendre les pannes.

Événements de basculement sur FMC

Étape 1. Configuration de la stratégie de santé

Le module Cluster/HA Failure Status est activé par défaut sur la politique d'intégrité, mais en outre, vous pouvez activer l'option Split-brain check.

Afin d'activer les options pour la haute disponibilité dans la politique de santé, accédez à System > Health > Policy > Firewall Threat Defense Health Policy > High Avilability.

Cette image décrit la configuration haute disponibilité de la politique d'intégrité :

Firewall Manage System / Health / Policy	ement Center	Overview	Analysis	Policies	Devices	Objects	Integration
Initial_Health_Policy 2 Initial Health Policy	2023-08-29 15:26	6:44 🖋					
Health Modules Run Tin	ne Intervals						
		Disk Usage Monitors disk usa Warning thresl 85 % Warning Thres 97 %	^{age} hold shold (seconda	ary HD)	Critical threshu 90 % Critical Thresh 99 %	old old (secondary	• HD)
	F	High Availa	bility				
		Cluster/HA F Monitors cluster a	Failure Status and HA members	S for their availat	pility failure		
		Firewall Three Monitors Firewall	eat Defense Threat Defense H	HA (Split-b HA for split-brai	r ain check) n (Both HA memb	pers are in active s	state)
	v	Integration					



Étape 2. Affectation de stratégie

Assurez-vous que la politique d'intégrité est attribuée aux paires haute disponibilité que vous souhaitez surveiller à partir du FMC.

Afin d'attribuer la stratégie, accédez à System > Health > Policy > Firewall Threat Defense Health Policy > Policy Assignments & Deploy.

Cette image montre comment attribuer la stratégie d'intégrité à la paire haute disponibilité :

ſ	Policy Assignments & Deploy			×
Ľ	Select devices to which the policy has to	be app	blied.	
	Available Devices	- F	Selected Devices	
			✓ FTD-HA (HA)	1
			10.82.141.169	
			10.82.141.171	
aila				
- 6		\rightarrow		
bra				
		<<		
ce				
ı Fi				
Ŀ				
n c			Cancel	Apply

Affectation haute disponibilité

Une fois la stratégie attribuée et enregistrée, le FMC l'applique automatiquement au FTD.

Étape 3. Alertes d'événements de basculement

Selon la configuration de la haute disponibilité, une fois qu'un événement de basculement est déclenché, les alertes contextuelles qui décrivent l'échec du basculement s'affichent.

Cette image présente les alertes de basculement générées :

					Dismiss all notifications
t Pending (0)	• Upgrade (0)				Cluster/Failover Status - 10.82.141.169 × SECONDARY (FLM1946BCEX) FAILOVER_STATE_ACTIVE (Inspection engine in other unit has failed(My failed services Peer
	Version	Chassis	Licenses	Access Control Pe	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- diskstature Poser failed engines)
with FTD	(0) ● Upgrade (0) Version Chassis 7.2.5 Image: F241-24-04-FPR9K-1.cisco.com:4 Security Module - 1 7.2.5 Image: F241-24-4-FPR9K-2.cisco.com	III F241-F241-24-4-FPR9K-2.cisco.com:4 IIII Security Module - 1	Essentials, IPS (2 more)	FTD HA	Disk Usage - 10.82.141.171 × /ngfw using 98%: 186G (5.5G Avail) of 191G

Alertes de basculement

Vous pouvez également accéder à Notifications > Health afin de visualiser les alertes d'intégrité de basculement.

Cette image présente les alertes de basculement sous les notifications :

View By: Group 👻				Deployments Upgrades Health Tasks Show Not
All (2) • Error (2) • Warning (0) • Offline (0) • Norma	I (0) Deployment Pending (0) • Upgr	rade (0)	20+ total 15 warnings 7 critical 0 errors
Collapse All				Smart License Monitor Smart Agent is not registered with Smart Licensing Cloud UII Elizades Meeter
Name	Model	Version	Chassis	OKL Hitering Monitor OKL Hitering registration failure
✓ Ungrouped (1)				Devices 10.82.141.169
✓ FTD-HA High Availability				Interface Status Interface "Etherner(1)2" is not receiving any packets Interface "Etherner(1)3" is not receiving any packets Interface "Etherner(1)4" is not receiving any packets
▲ 10.82.141.169(Secondary, Active) 10.82.141.169 - Routed	Firepower 9300 with FTD	7.2.5	EIII F241-24-04-FPR9K-1 Security Module - 1	10.82.141.171 Image: Disk Usage /ngfw using 98%: 186G (5.4G Avail) of 191G Image: Disk Usage /ngfw using 98%: 186G (s.4G Avail) of 191G Image: Disk Usage /ngfw using 98%: 186G (s.4G Avail) of 191G
10.82.141.171(Primary, Failed)	Firepower 9300 with FTD	7.2.5	F241-F241-24-4-FPR	Interface "Ethernet1/3" is not receiving any packets Interface "Ethernet1/4" is not receiving any packets

Notifications HA

Étape 4. Événements de basculement historiques

Le FMC permet de visualiser les événements de basculement qui se sont produits dans le passé. Pour filtrer les événements, accédez à System > Health > Events > Edit Search et spécifiez le nom du module en tant qu'état de cluster/basculement. En outre, le filtre peut être appliqué en fonction de l'état.

Cette image montre comment filtrer les événements de basculement :

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

Messages de filtre de basculement

Vous pouvez ajuster les paramètres d'heure afin d'afficher les événements pour une date et une heure spécifiques. Pour modifier les paramètres d'heure, accédez à System > Health > Events > Time.

Cette image montre comment modifier les paramètres d'heure :

Firewall Management Center Overview System / Health / Events	Analysis Policies Devices Object	ts Integration	Deploy	Q 💕 🌣 🙆 admin 🔹 🖏 SECURE
			Bookmark This Page R	eporting Workflows, View Bookmarks Search II 2023-09-27 11:02:00 - 2023-09-28 11:08:13 Expanding
 Search Constraints (Edit Search Save Search) 	•••	2023-09-28 11:14		
Health Monitor Table View of Health Events	A Not Secure https://10.82.141.165/date/	time_range.cgi?page_type=Health%20Monitorin	g&formname=eventform&start_end=169582692	Land Land Land Land Land Land Land Land
Module Name × Test Name ×	Health Monitoring Time Window Prefe	erences		× Status × Device ×
Cluster/Failover Status Cluster/Failover Status	Expanding Time Window •			A 10.82.141.171
Cluster/Failover Status Cluster/Failover Status	Start Time	End Time	Presets	A 10.82.141.169
Cluster/Failover Status Cluster/Failover Status	2023-09-27 11:02	2023-09-28 11:14	Last Current	4 10.82.141.169
Cluster/Failover Status Cluster/Failover Status			1 hour Day	A 10.82.141.171
Cluster/Failover Status Cluster/Failover Status	I< September 2023 > >I	< September 2023 >>	6 hours Week	10.82.141.171
Cluster/Fallover Status Cluster/Fallover Status	SU MO TU WE TH FR SA	SU MO TU WE TH FR SA	1 day Month	A 10.82.141.169
Cluster/Failover Status Cluster/Failover Status	27 28 29 30 31 1 2	27 28 29 30 31 1 2	1 week Sunchronize with	A 10.82.141.171
Cluster/Failover Status Cluster/Failover Status	3 4 5 6 7 8 9	3 4 5 6 7 8 9	2 weeks Audit Log Time Window	A 10.82.141.171
Cluster/Failover Status Cluster/Failover Status	10 11 12 13 14 15 16	10 11 12 13 14 15 16	1 month Events Time Window	A 10.82.141,169
Cluster/Failover Status Cluster/Failover Status	17 18 19 20 21 22 23	17 18 19 20 21 22 23	Events Time Window	A 10.82.141.169
Cluster/Failover Status Cluster/Failover Status	24 25 26 27 28 29 30	24 25 26 27 28 29 30		A 10.82.141.171
Cluster/Failover Status Cluster/Failover Status	1 2 3 4 5 6 7	1 2 3 4 5 6 7	Any changes made will take effect	10.82.141.171
Cluster/Failover Status Cluster/Failover Status		1 day, 12 minutes	on the next page load	4 10.82.141.169
Cluster/Failover Status Cluster/Failover Status	-			A 10.82.141.171
Cluster/Failover Status Cluster/Failover Status			Reset Apply	A 10.82.141.171

Filtre de temps

Une fois que les événements ont été identifiés, afin de confirmer la raison de l'événement, pointez le curseur sous Description.

Cette image montre comment la raison du basculement peut être vue.

P	Firewall Management System / Health / Events	Center Overview	Analysis	Policies	Devices	Objects	Integration		Dep	iloy Q	6 0	admin 🔻	esco SECURE
								Boo	kmark This Page	Reporting	Workflows ₊	View Book	kmarks Search
► S He	earch Constraints (Edit Search Se alth Monitor Table View of He	ve Search) aith Events								11 202:	8-09-27 11:1:	:00 - 2023-	-09-28 12:38:42 Expanding
	Module Name ×	Test Name ×	+	Time ×		Description	ç		Value ×	Units ×	Status ×	Device	×
٠	Cluster/Failover Status	Cluster/Failover Status	20	23-09-28 11:4	1:52	PRIMARY.(E	.M19389LOR) FAILOVER_STATE_STANDBY_F/ PRIMARY_[FL FAILOVER_ST Inspection en disketatus, Pa	Allent M19389LQR) :ATE_STANDBY_FAILED (Detect rgine failure(My failed services- rec failed services-)).	0		-	10.82.	.141.171

détails du basculement

Étape 5. Tableau de bord haute disponibilité

Une autre méthode de surveillance du basculement est disponible sous System > Health Montitor > Select Active or Standby Unit.

Le moniteur de haute disponibilité fournit des informations sur l'état de la haute disponibilité et de la liaison d'état, des interfaces surveillées, du ROL et de l'état des alertes sur chaque unité.

Cette image montre le moniteur haute disponibilité :



Graphiques de santé

Afin de visualiser les alertes, accédez à System > Health Montitor > Select Active or Standby Unit > Select the Alerts.



Alertes

Pour obtenir plus de détails sur les alertes, sélectionnez View all alerts > see more.

Cette image montre l'état du disque à l'origine du basculement :

19 total	2 critical	0 warnings	7 normal	Export	Run All
Disk Usage				Sep 28, 20	023 12:47 PN
/ngfw using 98%: 186G (5.4G Avail) of 1	91G see less			
Local Disk Partition S	tatus				
Mount	Size Free	Used Percent			
/mnt/boot	7.5G 7.3G	208M 3%			
/opt/cisco/config	1.9G 1.8G	3.4M 1%			
/opt/cisco/platform/l	ogs 4.6G 4.3G	19M 1%			
/var/data/cores	46G 43G	823M 2%			
/opt/cisco/csp	684G 4980	G 187G 28%			
/ngfw	191G 5.4G	186G 98%			
Interface Status				Sep 28, 20	023 12:47 PN
Interface 'Ethernet1/2' is	not receiving a	ny packets			
Interface 'Ethernet1/3' is	not receiving a	ny packets			
Interface 'Ethernet1/4' is	not receiving a	ny packets see m	nore		
Appliance Heartbeat				Sep 28, 20	023 12:47 PN
All appliances are sending	g heartbeats co	orrectly.			
Automatic Application	Runace Stat	110		Son 28 20	122 12-47 DK

Étape 6. CLI Threat Defense

Enfin, afin de collecter des informations supplémentaires sur FMC, vous pouvez accéder à Devices > Troubleshoot > Threat Defense CLI. Configurez les paramètres tels que Device et la commande à exécuter, puis cliquez sur Execute.

Cette image présente un exemple de la commande show failover history qui peut être exécuté sur le FMC où vous pouvez identifier l'échec du basculement.

Firewall Management Center Devices / Troubleshcot / Threat Defense CLI	Overview Analysis	Policie	es Devices	Objects Int	egration	
	De Co	evice	10.82.141.169 show	• •	Parameter	failover history
	Ou	utput other uni	t has failed			due to disk failure
		05:28:05 Active Dr other uni	UTC Sep 28 2023 ain t has failed	Active Appl	ying Config	Inspection engine in due to disk failure
		05:28:05 Active Ap other uni	UTC Sep 28 2023 plying Config t has failed	Active Conf	ig Applied	Inspection engine in due to disk failure
	0 4 0	05:28:05 Active Co other uni	UTC Sep 28 2023 nfig Applied t has failed	Active		Inspection engine in due to disk failure
				Back	Execute	

historique de basculement

Informations connexes

- Haute disponibilité pour FTD
- <u>Configurer la haute disponibilité FTD sur les appareils Firepower</u>
- <u>Assistance et documentation techniques Cisco Systems</u>

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.