Identificar e analisar eventos de failover de FTD no FMC

Contents Introdução Pré-requisitos Requisitos Componentes Utilizados Informações de Apoio Eventos de failover no FMC Etapa 1. Configuração de Política de Integridade

Etapa 2. Atribuição de política Etapa 3. Alertas de eventos de failover Etapa 4. Eventos Históricos de Failover Etapa 5. Painel de Alta Disponibilidade Etapa 6. Defesa contra ameaças CLI

Informações Relacionadas

Introdução

Este documento descreve como identificar e analisar eventos de failover para Secure Firewall Threat Defense na GUI do Secure Firewall Management Center.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Configuração de alta disponibilidade (HA) para Cisco Secure Firewall Threat Defense (FTD)
- Utilização básica do Cisco Firewall Management Center (FMC)

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

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

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto

potencial de qualquer comando.

Informações de Apoio

O FMC não é apenas o centro administrativo de dispositivos Firepower, além do gerenciamento e das opções de configuração, ele também fornece uma interface gráfica que ajuda a analisar logs e eventos em tempo real e passado.

Ao falar sobre failover, a interface tem novas melhorias que ajudam a analisar os eventos de failover para entender as falhas.

Eventos de failover no FMC

Etapa 1. Configuração de Política de Integridade

O módulo Cluster/HA Failure Status (Status de falha de HA/cluster) é ativado por padrão na Health Policy (Política de integridade), mas, além disso, você pode ativar a opção Split-brain check (Dividir cérebro).

Para habilitar as opções de HA na política de integridade, navegue até System > Health > Policy > Firewall Threat Defense Health Policy > High Avilability.

Esta imagem descreve a configuração de HA da Política de Integridade:

Firewall Management Center System / Health / Policy	Overview	Analysis	Policies	Devices	Objects	Integration
Initial_Health_Policy 2023-08-29 15:2 Initial Health Policy	6:44 🖋					
Health Modules Run Time Intervals		nao, generatoro a		0.00		
	Disk Usage Monitors disk us Warning thres 85 % Warning Thres 97 %	^{age} hold shold (second	ary HD)	Critical thresh 90 % Critical Thresh 99 %	old Iold (secondar	y HD)
	High Availa	ability				
	Cluster/HA Monitors cluster	Failure Statu and HA member	I S s for their availa	bility failure		
	Firewall Three Monitors Firewall	eat Defense I Threat Defense	HA (Split-I HA for split-bra	orain check) ain (Both HA memi	oers are in active	state)
~	Integration					

Configurações de Integridade de Alta Disponibilidade

Etapa 2. Atribuição de política

Certifique-se de que a Política de integridade esteja atribuída aos pares de alta disponibilidade que você deseja monitorar do FMC.

Para atribuir a regra, navegue até System > Health > Policy > Firewall Threat Defense Health Policy > Policy Assignments & Deploy.

Esta imagem mostra como atribuir a política de integridade ao par HA:

ſ	Policy Assignments & Deplo	у	×
Ľ	Select devices to which the policy l	has to be applied.	
	Available Devices	Selected Devices	
		✓ FTD-HA (HA) 10.82.141.169 10.82.141.171	1
aila : - k bra		>>	
ce			
Fi			
n c		Cancel	Apply

atribuição HA

Uma vez atribuída e salva a política, o FMC a aplica automaticamente ao FTD.

Etapa 3. Alertas de eventos de failover

Dependendo da configuração do HA, quando um evento de failover é acionado, os alertas pop-up que descrevem a falha de failover são mostrados.

Esta imagem mostra os alertas de failover gerados:

					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)
					Cluster/Failover Status - 10.82.141.171 × PRIMARY (FLM19389LQR) FAILOVER_STATE_STANDBY (Other unit wants me Standby) PRIMARY (FLM19389LQR) FAILOVER_STATE_STANDBY_FAILED (Detect
with FTD	7.2.5	F241-24-04-FPR9K-1.cisco.com:443 Escurity Module - 1	Essentials, IPS (2 more)	FTD HA	Inspection engine failure(My failed services- diskstatus. Peer failed services-))
with FTD	7.2.5	F241-F241-24-4-FPR9K-2.cisco.com:4 Executive Module - 1	Essentials, IPS (2 more)	FTD HA	S Disk Usage - 10.82.141.171 X /ngfw using 98%: 186G (5.5G Avail) of 191G

Alertas de failover

Você também pode navegar para Notifications > Health para visualizar os alertas de integridade de failover.

Esta imagem mostra os alertas de failover em notificações:

View By: Group +				Deployments Upgrades Health Tasks.
All (2) • Error (2) • Warning (0) • Offline (0) • Normal	(0) • Deployment Pending (0) 🔹 Upg	rade (0)	20+ total 15 warnings 7 critical 0 errors Q Filter
Collacue All				Smart License Monitor Smart Agent is not registered with Smart Licensing Cloud UDI Elitedion Monitor UDI Elitedion conference onlines
Name	Model	Version	Chassis	One Price ing Monitor One Price ing registration tanking
 Ungrouped (1) FTD-HA High Availability 				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	E F241-24-04-FPR9K-1 Security Module - 1	10.82,141.171 Interface 'Ethernet1/4' is not receiving any packets 10.82,141.171 Disk Usage /ngfw using 98%: 186G (5.4G Avail) of 191G Interface Status Interface 'Ethernet1/2' is not receiving any packets
10.82.141.171(Primary, Falled) 10.82.141.171 - Routed	Firepower 9300 with FTD	7.2.5	ER F241-F241-24-4-FPR	Interface "Ethernet1/3" is not receiving any packets Interface "Ethernet1/4" is not receiving any packets

Notificações HA

Etapa 4. Eventos Históricos de Failover

O FMC fornece uma maneira de visualizar eventos de failover que ocorreram no passado. Para filtrar os eventos, navegue até System > Health > Events > Edit Search e especifique o Nome do módulo como Status do cluster/failover. Além disso, o filtro pode ser aplicado com base no Status.

Esta imagem mostra como filtrar eventos de failover:

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

Mensagens de filtro de failover

Você pode ajustar as configurações de hora para exibir os eventos de uma data e hora específicas. Para modificar as configurações de hora, navegue até System > Health > Events > Time.

Esta imagem mostra como editar as configurações de hora:

Firewall Management Center Overview System / Health / Events	Analysis Policies Devices Objects Integration		Deploy	ର 🔮 🌣 🚳 ା	Idmin • tiste SECURE
 Search Constraints (Edit Search Save Search) 	• • • 2023-09-	-28 11:14	Bookmark This Page Rep	sorting Workflows, 2023-09-27 11:02:0	View Bookmarks Search 30 - 2023-09-28 11:08:13 Expanding
Health Monitor Table View of Health Events	Not Secure https://10.82.141.165/date/time_range.cgi7page_type= Health Monitoring Time Window Preferences	4ealth%20Monitoring&formname=e	ventform&start_end=169582692	x Status X	Device ×
Cluster/Fallover Status Cluster/Fallover Status Cluster/Fallover Status Cluster/Fallover Status Cluster/Fallover Status Cluster/Fallover Status	Start Time End Time	Presets			10.82.141.171 10.82.141.169 10.82.141.169
Cluster/Failover Status Cluster/Failover Status Cluster/Failover Status	2023-09-27 11:02 11 ▼ : 02 ▼ 2023-09-28 11:14 I<	2023 >> Last	Current Day Week		10.82.141.171
Cluster/Fallover Status Cluster/Fallover Status Cluster/Fallover Status Cluster/Fallover Status Cluster/Fallover Status Cluster/Fallover Status	SU MO TU WE TH FR SA SU MO TU WE 27 28 29 30 31 1 2 27 28 29 30 3 4 5 6 7 8 9 3 4 5 6	TH FR SA 31 1 2 1 day 7 8 0 1 week	Month Synchronize with	-	10.82.141.169 10.82.141.171 10.82.141.171
Cluster/Fallover Status Cluster/Fallover Status Cluster/Fallover Status	10 11 12 13 14 15 16 10 11 12 13 17 18 19 20 21 22 23 17 18 19 20 21 22 23 17 18 19 20 21 22 23 17 18 19 20 21 22 23 17 18 19 20 21 22 23 17 18 19 20 21 22 23 17 18 19 20 21 22 23 17 18 19 20 21 22 23 17 18 19 20 21 22 23 17 18 19 20 24 25 26 27 28 29 20 24 25 26 27 24 25 26 27 28 29 20 24 25 26 27 28 </td <td>14 15 16 2 weeks 21 22 23 1 month 28 29 30</td> <td>Audit Log Time Window Events Time Window</td> <td></td> <td>10.82.141.169 10.82.141.169</td>	14 15 16 2 weeks 21 22 23 1 month 28 29 30	Audit Log Time Window Events Time Window		10.82.141.169 10.82.141.169
Cluster/Fallover Status Cluster/Fallover Status Cluster/Fallover Status Cluster/Fallover Status Cluster/Fallover Status Cluster/Fallover Status	1 2 3 4 5 6 7 1 2 3 4 5 6 7	5 6 7	Any changes made will take effect on the next page load.		10.82.141.171 10.82.141.171 10.82.141.169
Cluster/Failover Status Cluster/Failover Status Cluster/Failover Status			Reset		10.82.141.171 10.82.141.171

Filtro de tempo

Uma vez identificados os eventos, para confirmar a razão do evento, aponte o cursor em Descrição.

Esta imagem mostra como o motivo do failover pode ser visto.

þ	Firewall Management C System / Health / Events	enter _{Overview}	Analysis	Policies	Devices	Objects	Integration		Dep	iloy Q	6 0	admin 🔻	esco SECURE
								Book	mark This Page	Reporting	Workflows	View Bookn	narks Search
 Set Heal 	rch Constraints (Edit Search Save	Search) th Events								II 2023	-09-27 11:19	:00 - 2023-0	09-28 12:38:42 Expanding
	Module Name ×	Test Name ×	÷	Time ×		Description			Value ×	Units ×	Status ×	Device >	<
*	Cluster/Failover Status	Cluster/Failover Status	205	23-09-28 11:41	1:52	PRIMARY.(E	M19389LOR) FAILOVER_STATE_STANDBY_ PRIMARY (7 FAILOVER, 1 Inspector diskstatus, 1	Allwas LM19389LQR) TATE_STANDBY_FAILED (Detect ngine failure(fb tailed services- teer failed services-)).	0		*	10.82.1	41.171

detalhes de failover

Etapa 5. Painel de Alta Disponibilidade

Outra maneira de monitorar o failover pode ser encontrada em System > Health Montitor > Select Active or Standby Unit.

O monitor HA fornece informações sobre o status do HA e do link de estado, interfaces monitoradas, ROL e o status dos alertas em cada unidade.

Esta imagem mostra o Monitor HA:



Gráficos de integridade

Para visualizar os alertas, navegue até System > Health Montitor > Select Active or Standby Unit > Select the Alerts.



Alertas

Para obter mais detalhes sobre os alertas, escolha View all alerts > see more.

Esta imagem mostra o status do disco que causou o failover:

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	191G see less			
Local Disk Partition S	tatus				
Mount	Size Free	Used Percent			
/mnt/boot	7.5G 7.3G	i 208M 3%			
/opt/cisco/config	1.9G 1.8G	i 3.4M 1%			
/opt/cisco/platform/l	ogs 4.6G 4.3G	i 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	ore		
Appliance Heartbeat				Sep 28, 20	023 12:47 PN
All appliances are sending	g heartbeats co	orrectly.			
Automatic Application	Runace Stat	110		Son 28 21	122 12-47 DA

Etapa 6. Defesa contra ameaças CLI

Por último, para recolher informações adicionais sobre o CVP, pode Devices > Troubleshoot > Threat Defense CLI. Configure os parâmetros como Dispositivo e o comando a ser executado e clique em Execute.

Esta imagem mostra um exemplo do comando show failover history que pode ser executado no FMC, onde você pode identificar a falha de failover.



histórico de failover

Informações Relacionadas

- Alta disponibilidade para FTD
- <u>Configurar a alta disponibilidade do FTD em dispositivos Firepower</u>
- Suporte Técnico e Documentação Cisco Systems

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.