# 识别和分析FMC上的FTD故障切换事件

### 目录

 節介

 先决条件

 要求

 使用的组件

 背景信息

 FMC上的故障切换事件

 步骤1:运行状况策略配置

 第二步:策略分配

 第三步:故障切换事件警报

 第五步:高可用性控制面板

 第六步:威胁防御CLI

 相关信息

### 简介

本文档介绍如何在安全防火墙管理中心GUI上识别和分析安全防火墙威胁防御的故障转移事件。

### 先决条件

#### 要求

Cisco 建议您了解以下主题:

- 思科安全防火墙威胁防御(FTD)的高可用性(HA)设置
- 思科防火墙管理中心(FMC)的基本可用性

#### 使用的组件

本文档中的信息基于以下软件和硬件版本:

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

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果您的网络处于活动状态,请确保您了解所有命令的潜在影响。

#### 背景信息

FMC不仅是Firepower设备的管理中心,而且除了管理和配置选项之外,它还提供了一个图形界面

,有助于实时和以前分析日志和事件。

当谈到故障切换时,接口有了新的改进,有助于分析故障切换事件以便了解故障。

### FMC上的故障切换事件

#### 步骤1:运行状况策略配置

默认情况下,模块Cluster/HA Failure Status在Health Policy上启用,但您也可以启用Split-brain检 查选项。

要在运行状况策略中启用HA选项,请导航至 System > Health > Policy > Firewall Threat Defense Health Policy > High Avilability.

#### 此映像描述运行状况策略的HA配置:

Firewall Management Center System / Health / Policy	Overview	Analysis	Policies	Device	s Objects	Integration
Initial_Health_Policy 2023-08-29 15:20 Initial Health Policy	6:44 🖋					
Health Modules Run Time Intervals						
	Disk Usage Monitors disk usa Warning thres 85 % Warning Thres 97 %	age shold shold (seconda	ary HD)	Critical thr 90 Critical Th 99	reshold % reshold (secondary H %	T ال
	High Availa	ability				
	Cluster/HA I Monitors cluster	Failure Status and HA members	<b>S</b> for their availa	bility failure		
	Firewall Three Monitors Firewall	eat Defense I Threat Defense I	<b>HA (Split-b</b> HA for split-bra	<b>orain cheo</b> in (Both HA r	<b>:k)</b> nembers are in active sta	te)
~	Integration					

高可用性运行状况设置

第二步:策略分配

确保将运行状况策略分配给要从FMC监控的HA对。

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

此图显示如何将运行状况策略分配给HA对:



HA分配

分配并保存策略后,FMC会自动将其应用到FTD。

第三步:故障切换事件警报

根据HA的配置,一旦触发了故障切换事件,将显示描述故障切换故障的弹出警报。

下图显示生成的故障切换警报:

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

故障切换警报

您也可以导航至 Notifications > Health 以便可视化故障切换运行状况警报。

#### 下图显示通知下的故障切换警报:

Firewall Management Center Overview Analy Devices / Device Management Overview	vsis Policies Devices	Objects	Integration	Deploy Q 🥙 🌣 🚱 admin 🔹 🕬 SECUR
View By: Group All (2)	(0) • Deployment Pending (i	)) 🔹 Upgri	ade (0)	Deployments         Upgrades         Health         Tasks         Show Notifications           20+ total         15 warnings         7 critical         0 errors         Q. Filter
Collapse All				Smart License Monitor     Smart Agent is not registered with Smart Licensing Cloud
Name	Model	Version	Chassis	URL Filtering Monitor     URL Filtering registration failure
<ul> <li>Ungrouped (1)</li> </ul>				Devices 10.82.141.169
✓ FTD-HA High Availability				Interface Status     Interface 'Ethernet1/2' is not receiving any packets     Interface 'Ethernet1/3' is not receiving any packets     Interface 'Ethernet1/4' is not receiving any packets
10.82.141.169(Secondary, Active) 10.82.141.169 - Routed	Firepower 9300 with FTD	7.2.5	E Security Module - 1	10.82.141.171     /ngfw using 98%: 186G (5.4G Avail) of 191G       Disk Usage     /ngfw using 98%: 186G (5.4G Avail) of 191G       Interface Status     Interface "Ethernel1/2" is not receiving any packets       Interface "Ethernel1/2" is not receiving any usekets
10.82.141.171(Primary, Falled) 10.82.141.171 - Routed	Firepower 9300 with FTD	7.2.5	F241-F241-24-4-FPR Security Module - 1	Interface Externet (73 is not receiving any packets Interface "Ethernet1/4" is not receiving any packets

HA通知

#### 第四步:历史故障切换事件

FMC提供了一种可视化过去发生的故障切换事件的方式。要过滤事件,请导航至 System > Health > Events > Edit Search 并将Module Name指定为Cluster/Failover Status。此外,可以根据状态应用过滤器。

此图显示如何过滤故障切换事件:

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

故障切换过滤器消息

您可以调整时间设置以显示特定日期和时间的事件。要修改时间设置,请导航至 System > Health > Events > Time.

#### 此图显示如何编辑时间设置:

																	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	C			10.82.141.169
Cluster/Failover Status	Cluster/Failover Status								1000			7001222				Last	Current		<b>A</b>	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	<b>A</b>	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

时间过滤器

确定事件后,为了确认事件的原因,请将光标指向Description下。

#### 此图显示如何查看故障切换的原因。

Firewall Management Ce System / Health / Events	enter Overview	Analysis	Policies	Devices	Objects	Integration		D	ploy Q	6 0	admin • dealer SECURE
							Во	okmark This Pa	ge   Reporting	Workflows <sub>+</sub>	View Bookmarks   Search
									11 2023	8-09-27 11:19:	00 - 2023-09-28 12:38:42 Expanding
Search Constraints (Edit Search Save	Search)										
Health Monitor Table View of Healt	h Events										
Module Name ×	Test Name ×	+	Time ×		Description	¢		Value ×	Units ×	Status ×	Device ×
Cluster/Failover Status	Cluster/Failover Status	20	23-09-28 11:4	1:52	PRIMARY (	M19389LOR) FAILOVER_STA	ATE_STANDBY_FAIL	0		-	10.82.141.171
							PRIMARY (FLM19389LQR) FAILOVER_STATE_STANDBY_FAILED (Detect Inspection engine failure(My failed services- diskstatus. Peer failed services-)).				

第五步:高可用性控制面板

监控故障转移的另一种方法位于 System > Health Montitor > Select Active or Standby Unit.

HA监视器提供有关HA和状态链路、受监控接口、ROL的状态以及每台设备上警报状态的信息。 此图显示HA监控器:

Hire Wall Managemer System / Health / Monitor Monitoring (응) 없 Home	It Center         Overview         Analysis         Policies         Devices           Health: 10.82.141.169 (Active)         © Critical         View System & Toubleshoot Details         Overview         CPU         Memory         Interfaces         Connections	Objects Integration	Deploy Q 6 2 admin • diversion SECURE
<ul> <li>Frewall Management Center</li> <li>Devices (2)</li> <li>FTD-HA</li> <li>10.82.141.169 Across</li> <li>10.82.141.171 Standy Film</li> </ul>	CPU Data collection for CPU module is disabled in the health policy, partial or no data may be shown. No Data Available	Memory         Data Plane         Avg 17.%         Snort         Avg 21.%         System         Avg 19.%         Source           144.55 G8         17% - 17%         100.47 G8 27.% - 21.%         System         Avg 19.%         System	Throughput         Avg 1.42 kbps         Avg - all interfaces           Input Rate         Avg 1.42 kbps         Output Rate         Avg 1.74 kbps           28 k         Set bps - 2.64 kbps         Output Rate         Avg 1.74 kbps           13 k         Avg 1.92 kbps         Output Rate         Avg 1.74 kbps           13 k         Avg 1.92 kbps         Avg 1.92 kbps         Avg 1.74 kbps           13 k         Avg 1.92 kbps         Avg 1.92 kbps         Avg 1.92 kbps           199         11.95 kbps         12.95 kbps         12.95 kbps         12.95 kbps
	Connection Statistics Connections <sup>Avg0,0,3,31</sup> <sup>11</sup> <sup>12</sup> <sup>13</sup> <sup>14</sup> <sup>15</sup> <sup>14</sup> <sup>15</sup> <sup>15</sup> <sup>15</sup> <sup>15</sup> <sup>15</sup> <sup>15</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup> <sup>16</sup>	Process Health Critical Processes All Processes AddP Date Plane Narry Of Date Services Servic	High Availability Manage HA Primary Standby State Link Monitored Interfaces (4/4) Monitored Interfaces

运行状况图形

要将警报可视化,请导航至 System > Health Montitor > Select Active or Standby Unit > Select the Alerts.

Firewall Management Center System / Health / Monitor	Overview	Analysis	Policies	Devices	Ob
Monitoring	10.82.141.171 (s a & Troubleshoot Det CPU collection for CPU data may be show	Standby - Failed) FTD-HA (HA-Stand 10.82.141.171 Alerts: 2   4 Fop 5 Alerts Disk Usage Interface Status Firewall Threat Snort Identity M Configuration R	Critical Critical Critical Critical O T Critical O T Critical O T Critical C C C C C C C C C C C C C C C C C C C	lit-brain check) on View all alerts	Snc
	No	o Data Avail	able		ŀ

风险通告

要获取警报的更多详细信息,请选择 View all alerts > see more.

此映像显示导致故障切换的磁盘状态:

Health Alerts - 10.	82.141.17	1		×
<ul> <li>19 total</li> <li>Disk Usage /ngfw using 98%: 186G (19)</li> </ul>	2 critical 5.4G Avail) of 19	0 warnings 1G see less	7 normal	Export Run All Sep 28, 2023 12:47 PM
Local Disk Partition S	itatus			
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/	logs 4.6G 4.3G	19M 1%		
/var/data/cores	46G 43G	823M 2%		
/opt/cisco/csp	684G 498G	187G 28%		
/ngfw	191G 5.4G	186G 98%		
Interface Status	1 11,020	28. E		Sep 28, 2023 12:47 PM
Interface 'Ethernet1/2' is	not receiving an	y packets		
Interface 'Ethernet1/3' is	not receiving an	y packets	0.070	
Appliance Ethernet1/4 IS	not receiving an	y packets see n	lore	C 20. 2002 12 17 DI
Appliance Heartbeat All appliances are conding	a hoorthoote cou	roctly		Sep 28, 2023 12:47 PM
All appliances are sending	g near beats con	recuy.		D 00 0000 40 47 PM
	KUNASS STATI			Non 78 7073 17/17 DM

第六步:威胁防御CLI

最后,为了收集有关FMC的其他信息,您可以导航至 Devices > Troubleshoot > Threat Defense CLI.配置要执行的参数(如设备和命令),然后单击 Execute.

下图显示了命令的示例 show failover history 可在FMC上执行,您可以在其中识别故障切换故障。



故障切换历史记录

## 相关信息

- <u>FTD的高可用性</u>
- 在 Firepower 设备上配置 FTD 高可用性
- <u>技术支持和文档 Cisco Systems</u>

#### 关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言,希望全球的用户都能通过各 自的语言得到支持性的内容。

请注意:即使是最好的机器翻译,其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任,并建议您总是参考英文原始文档(已提供 链接)。