FTD에 대한 장애 조치 상태 메시지 이해

목차

소개

이 문서에서는 FTD(Secure Firewall Threat Defense)에서 장애 조치 상태 메시지를 이해하는 방법 에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco Secure FTD의 고가용성(HA) 설정
- Cisco FMC(Firewall Management Center)의 기본 사용 편의성

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

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

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바 이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

장애 조치 상태 모니터링 개요:

FTD 디바이스는 전체 상태 및 인터페이스 상태에 대해 각 유닛을 모니터링합니다. FTD는 Unit Health Monitoring 및 Interface Monitoring을 기반으로 각 유닛의 상태를 결정하기 위해 테스트를 수 행합니다. HA 쌍의 각 유닛의 상태를 확인하는 테스트가 실패할 경우 장애 조치 이벤트가 트리거됩 니다.

장애 조치 상태 메시지

활용 사례 - 장애 조치 없이 데이터 링크 중단

FTD HA에서 인터페이스 모니터링이 활성화되지 않은 경우 및 데이터 링크 실패의 경우 인터페이 스에 대한 상태 모니터 테스트가 수행되지 않으므로 장애 조치 이벤트가 트리거되지 않습니다.

이 이미지에서는 데이터 링크 실패의 경고를 설명하지만 장애 조치 경고가 트리거되지 않습니다.

Analysis Policies Devi	ices Objects	Integration		Deploy Q 🧉	🕈 🌣 🕜 admin	• cisco SECURE
					Dismiss all notific	ations
ormal (2)	ding (1) 🔹 Up	grade (0)		S Inter Interf	face Status - 10.82. ace "Ethernet1/3" is not r ace "Ethernet1/3" has no	141.171 × receiving any packets link
Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack	
						11
Firepower 9300 with FTD	7.2.5	F241-24-04-FPR9K-1.cisco.com:4 Security Module - 1	Essentials, IPS (2 more)	FTD HA	49	i
Firepower 9300 with FTD	7.2.5	F241-F241-24-4-FPR9K-2.cisco.cr EXAMPLE A Security Module - 1	Essentials, IPS (2 more)	FTD HA	4D	:

링크 다운 알림

데이터 링크의 상태 및 상태를 확인하려면 다음 명령을 사용합니다.

• show failover - 각 유닛 및 인터페이스의 장애 조치 상태에 대한 정보를 표시합니다.

Monitored Interfaces 1 of 1291 maximum ... This host: Primary - Active Active time: 3998 (sec) slot 0: UCSB-B200-M3-U hw/sw rev (0.0/9.18(3)53) status (Up Sys) Interface DMZ (192.168.10.1): Normal (Waiting) Interface INSIDE (172.16.10.1): No Link (Not-Monitored) Interface OUTSIDE (192.168.20.1): Normal (Waiting) Interface diagnostic (0.0.0.0): Normal (Not-Monitored)
...
Other host: Secondary - Standby Ready
Active time: 0 (sec)
slot 0: UCSB-B200-M3-U hw/sw rev (0.0/9.18(3)53) status (Up Sys)
Interface DMZ (192.168.10.2): Normal (Waiting)
Interface INSIDE (172.16.10.2): Normal (Waiting)
Interface OUTSIDE (192.168.20.2): Normal (Waiting)
Interface diagnostic (0.0.0.0): Normal (Not-Monitored)

인터페이스의 상태가 'Waiting'인 경우 인터페이스가 가동 중이지만 피어 유닛의 해당 인터페이스에 서 hello 패킷을 아직 받지 못했음을 의미합니다.

반면, 'No Link (Not-Monitored)' 상태는 인터페이스의 물리적 링크가 중단되었지만 장애 조치 프로 세스에서 모니터링되지 않음을 의미합니다.

중단을 방지하려면 해당 대기 IP 주소를 사용하는 모든 민감한 인터페이스에서 인터페이스 상태 모 니터를 활성화하는 것이 좋습니다.

Interface Monitoring을 활성화하려면Device > Device Management > High Availability > Monitored Interfaces.

이 그림에서는 Monitored Interfaces 탭을 보여 줍니다.

Monitored Interfaces	-						
Interface Name	Active IPv4	Standby IPv4	Active IPv6 - Standby IPv6	Active Link-Local IPv6	Standby Link-Local IPv6	Monitoring	
DMZ	192.168.10.1	192.168.10.2				0	1
OUTSIDE	192.168.20.1	192.168.20.2				0	1
diagnostic						0	1
INSIDE	172.16.10.1	172.16.10.2				0	1

모니터링되는 인터페이스

모니터링되는 인터페이스 및 대기 IP 주소의 상태를 확인하려면 다음 명령을 실행합니다.

• show failover - 각 유닛 및 인터페이스의 장애 조치 상태에 대한 정보를 표시합니다.

```
Monitored Interfaces 3 of 1291 maximum
. . .
This host: Primary - Active
Active time: 3998 (sec)
slot 0: UCSB-B200-M3-U hw/sw rev (0.0/9.18(3)53) status (Up Sys)
Interface DMZ (192.168.10.1): Normal (Monitored)
Interface INSIDE (172.16.10.1): No Link (Monitored)
Interface OUTSIDE (192.168.20.1): Normal (Monitored)
Interface diagnostic (0.0.0.0): Normal (Waiting)
. . .
Other host: Secondary - Standby Ready
Active time: 0 (sec)
slot 0: UCSB-B200-M3-U hw/sw rev (0.0/9.18(3)53) status (Up Sys)
Interface DMZ (192.168.10.2): Normal (Monitored)
Interface INSIDE (172.16.10.2): Normal (Monitored)
Interface OUTSIDE (192.168.20.2): Normal (Monitored)
Interface diagnostic (0.0.0.0): Normal (Waiting)
```

활용 사례 - 인터페이스 상태 오류

한 유닛에서 모니터링되는 인터페이스의 hello 메시지를 15초 동안 수신하지 않고 한 유닛에서 인터 페이스 테스트가 실패하고 다른 유닛에서 작동하는 경우 인터페이스가 실패한 것으로 간주됩니다.

장애가 발생한 인터페이스 수에 대해 정의한 임계값이 충족되고 액티브 유닛에 스탠바이 유닛보다 장애가 발생한 인터페이스가 많은 경우 장애 조치가 발생합니다.

인터페이스 임계값을 수정하려면 Devices > Device Management > High Availability > Failover Trigger Criteria.

이 이미지에서는 인터페이스 장애 시 생성되는 경고에 대해 설명합니다.

Ana	lysis Policies D	evices Objects	Integration		Deploy	Q 💕 🌣 🕜 admin ▼ 號 SECURE
					[Dismiss all notifications
Norma	I (2) • Deployment P	Pending (0) • Up	ograde (0) • Snort 3 (2)			▲ Cluster/Failover Status - 10.82.141.169 × SECONDARY (FLM1946BCEX)
						FAILOVER_STATE_STANDBY_FAILED (Interface check) SECONDARY (FLM1946BCEX)
	Model	Version	Chassis	Licenses	Access Contro	FAILOVER_STATE_STANDBY (Interface check) SECONDARY (FLM1946BCEX)
						FAILOVER_STATE_ACTIVE (Other unit wants me
						Interface Status - 10.82.141.171 X Interface 'Ethernet 1/4' has no link
						▲ Cluster/Failover Status - 10.82.141.171 ×
	Firepower 9300 with FTD	7.2.5	F241-24-04-FPR9K-1.cisco.com:4- Security Module - 1	Essentials, IPS (2 more)	FTD HA	SECONDARY (FLM1946BCEX) FAILOVER_STATE_STANDBY (Check peer event for reason) SECONDARY (FLM1946BCEX)
	Firepower 9300 with FTD	7.2.5	Executive Module - 1	Essentials, IPS (2 more)	FTD HA	FAILOVER_STATE_STANDBY (Check peer event for reason) PRIMARY (FLM19389LQR)

링크 다운이 있는 장애 조치 이벤트

실패 이유를 확인하려면 다음 명령을 사용합니다.

• show failover state - 이 명령은 두 유닛의 장애 조치 상태 및 마지막으로 보고된 장애 조치 사유를 표시합니다.

<#root>

firepower#

show failover state

This host -	Primary						
	Active	Ifc Failure	19:14:54	UTC	Sep	26	2023
Other host	- Secondary						
	Failed	Ifc Failure	19:31:35	UTC	Sep	26	2023
		OUTSIDE: No Link					

• show failover history - 장애 조치 기록을 표시합니다. 장애 조치 내역은 과거 장애 조치 상태 변경

사항 및 상태 변경 사유를 표시합니다.

<#root>

firepower#

show failover history

From State	To State	Reason
19:31:35 UTC Sep 26 2023 Active	Failed	Interface check This host:1 single_vf: OUTSIDE Other host:0

활용 사례 - 높은 디스크 사용량

액티브 유닛의 디스크 공간이 90% 이상 찼을 경우 장애 조치 이벤트가 트리거됩니다.

이 이미지는 디스크가 가득 찰 때 생성되는 경고에 대해 설명합니다.

Analy	vsis Policies	Devices	Objects	Integration		Deploy	् 🚱 🌣 🕐 admin 🔹 ीडिके SECURE
						[Dismiss all notifications
Normal	(2) • Deploymen	t Pending (0)	• Upgra	de (0) • Snort 3 (2)			Cluster/Failover Status - 10.82.141.169 × PRIMARY (FLM19389LQR) FAILOVER_STATE_STANDBY (Check peer event for reason)
	Model		Version	Chassis	Licenses	Access Contro	SECONDARY (FLM1946BCEX) FAILOVER_STATE_ACTIVE (Inspection engine in other unit has failed(My failed services Peer failed services-diskstatus))
							Cluster/Failover Status - 10.82.141.171 × PRIMARY (FLM19389LQR) FAILOVER_STATE_STANDBY (Other unit wants me Standby) PRIMARY (FLM19389LQR)
	Firepower 9300 with F	TD	7.2.5	Executive Module - 1	Essentials, IPS (2 more)	FTD HA	FAILOVER_STATE_STANDBY_FAILED (Detect Inspection engine failure(My failed services- diskstatus. Peer failed services-))
	Firepower 9300 with F	TD	7.2.5	Executive Module - 1	Essentials, IPS (2 more)	FTD HA	Disk Usage - 10.82.141.171 × /ngfw using 98%: 186G (4.8G Avail) of 191G

장애 조치(디스크 사용량 포함)

실패 이유를 확인하려면 다음 명령을 사용합니다.

• show failover history - 장애 조치 기록을 표시합니다. 장애 조치 내역은 과거 장애 조치 상태 변경 사 항 및 상태 변경 사유를 표시합니다.

<#root>

firepower#

show failover history

From State	To State	Reason
20:17:11 UTC Sep 26 2023 Active	Standby Ready	 Other unit wants me Standby Inspection engine in other unit ha
20:17:11 UTC Sep 26 2023. Active	Standby Ready	Failed Detect Inspection engine fa due to disk failure

• show failover - 각 유닛의 장애 조치 상태에 대한 정보를 표시합니다.

<#root>

firepower#

show failover | include host|disk

This host: Primary - Failed slot 2: diskstatus rev (1.0) status (down) Other host: Secondary - Active slot 2: diskstatus rev (1.0) status (up)

• df-h - 전체 크기, 사용된 공간, 사용 비율 및 마운트 지점을 포함하여 마운트된 모든 파일 시스 템에 대한 정보를 표시합니다.

<#root>

admin@firepower:/ngfw/Volume/home\$

df -h /ngfw

Filesystem Size Used Avail Use% Mounted on /dev/sda6 191G 186G 4.8G 98% /ngfw

활용 사례 - Lina Traceback

lina traceback의 경우 장애 조치 이벤트를 트리거할 수 있습니다.

이 이미지에서는 lina traceback의 경우 생성된 경고에 대해 설명합니다.

Analysis	Policies Devices C	oy 🔍 🚱 🌣 🕲 admin 🕶 💼 secure				
						Dismiss all notifications
lormal (2)	 Deployment Pending (0) 	• Upgrade (0)				Cluster/Failover Status - 10.82.141.171 × PRIMARY (FLM19389LQR) FAILOVER_STATE_ACTIVE (HELLO not heard from peer)
	Model	Version	Chassis	Licenses	Access Control I	olleur Auto DollDack
						Interface Status - 10.82.141.171 × Interface "Ethernet1/1" is not receiving any packets Interface "Ethernet1/2" is not receiving any packets Interface "Ethernet1/3" is not receiving any packets Interface "Ethernet1/4" is not receiving any packets
						S Appliance Heartbeat - F241.24.04- X FMC4600
	Firepower 9300 with FTD	7.2.5	F241-24-04-FPR9K-1.cisco.com:443 Security Module - 1	Essentials, IPS (2 more)	FTD HA	Appliance 10.82.141.169 is not sending heartbeats.
	Firepower 9300 with FTD	7.2.5	F241-F241-24-4-FPR9K-2.cisco.com:4 Becurity Module - 1	Essentials, IPS (2 more)	FTD HA	Process Status - 10.82.141.169 Iina exited 2 time(s).

lina traceback을 사용한 장애 조치

실패 이유를 확인하려면 다음 명령을 사용합니다.

• show failover history - 장애 조치 기록을 표시합니다. 장애 조치 내역은 과거 장애 조치 상태 변경 사 항 및 상태 변경 사유를 표시합니다.

<#root>

firepower#

show failover history

From State	To State	Reason
8:36:02 UTC Sep 27 2023		
Standby Ready	Just Active	HELLO not heard from peer (failover link up, no response from pee
18:36:02 UTC Sep 27 2023		
Just Active	Active Drain	HELLO not heard from peer (failover link up, no response from pee
18:36:02 UTC Sep 27 2023 Active Drain	Active Applying Config	HELLO not heard from peer (failover link up, no response from pee
18:36:02 UTC Sep 27 2023 Active Applying Config	Active Config Applied	HELLO not heard from peer (failover link up, no response from pee
18:36:02 UTC Sep 27 2023 Active Config Applied	Active	HELLO not heard from peer (failover link up, no response from pee

lina traceback의 경우 다음 명령을 사용하여 코어 파일을 찾습니다.

```
root@firepower:/opt/cisco/csp/applications#
```

cd /var/data/cores

root@firepower:/var/data/cores#

ls -1

```
total 29016
-rw----- 1 root root 29656250 Sep 27 18:40 core.lina.11.13995.1695839747.gz
```

lina traceback의 경우 문제 해결 파일을 수집하고 Core 파일을 내보낸 다음 Cisco TAC에 문의하는 것이 좋습니다.

활용 사례 - Snort 인스턴스 다운

액티브 유닛에서 Snort 인스턴스의 50% 이상이 다운된 경우 장애 조치가 트리거됩니다.

이 그림에서는 snort 실패 시 생성되는 경고에 대해 설명합니다.

Analy	sis Policies Devices	Objects	Integration		Deploy	Q 💕 🌣 Ø admin▼ distit- cisco SI	ECURE
					Γ	Dismiss all notifications	
Jormal	(0) • Deployment Pending	(0) • Upgra	de (0) • Snort 3 (2) Chassis	Licenses	Access Control	Cluster/Failover Status - 10.82.141.1 SECONDARY (FLM1946BCEX) FAILOVER_STATE_STANDBY (Other unit wai Standby) SECONDARY (FLM1946BCEX) FAILOVER_STATE_STANDBY_FAILED (Deteiling)	nts me
						Inspection engine failure(My failed services- Peer failed services-))	·snort.
						Process Status - 10.82.141.169 The Primary Detection Engine process termi unexpectedly 1 time(s).	X
	Firepower 9300 with FTD	7.2.5	E241-24-04-FPR9K-1.cisco.com:44 Security Module - 1	Essentials, IPS (2 more)	FTD HA	Q>>	:
	Firepower 9300 with FTD	7.2.5	EXAMPLE 1	Essentials, IPS (2 more)	FTD HA	e?»	:

snort traceback을 통한 장애 조치

를 위해 실패 원인을 확인하려면 다음 명령을 사용합니다.

• show failover history - 장애 조치 기록을 표시합니다. 장애 조치 내역은 과거 장애 조치 상태 변경 사 항 및 상태 변경 사유를 표시합니다.

<#root>		
firepower#		
show failover history		
From State	To State	Reason

21:22:03 UTC Sep 26 2023 Standby Ready	Just Active	Inspection engine in other unit has failed due to snort failure
21:22:03 UTC Sep 26 2023	Just Active	Active Drain Inspection engine in other unit due to snort failure
21:22:03 UTC Sep 26 2023	Active Drain	Active Applying Config Inspection engine in o due to snort failure
21:22:03 UTC Sep 26 2023	Active	Applying Config Active Config Applied Inspect due to snort failure

• show failover - 유닛의 장애 조치 상태에 대한 정보를 표시합니다.

<#root>

firepower#

show failover | include host|snort

This host: Secondart - Active slot 1: snort rev (1.0) status (up) Other host: Primary - Failed slot 1: snort rev (1.0) status (down) Firepower-module1#

snort traceback의 경우 다음 명령을 사용하여 crashinfo 또는 core 파일을 찾습니다.

<#root>

For snort3:
root@firepower#

cd /ngfw/var/log/crashinfo/

root@firepower:/ngfw/var/log/crashinfo#

ls -1

```
total 4
-rw-r--r-- 1 root root 1052 Sep 27 17:37 snort3-crashinfo.1695836265.851283
```

For snort2:
root@firepower#

cd/var/data/cores

root@firepower:/var/data/cores#

```
ls -al
```

```
total 256912
-rw-r--r-- 1 root root 46087443 Apr 9 13:04 core.snort.24638.1586437471.gz
```

snort traceback의 경우 문제 해결 파일을 수집하고 Core 파일을 내보낸 다음 Cisco TAC에 문의하는 것이 좋습니다.

활용 사례 - 하드웨어 또는 전원 장애

FTD 디바이스는 hello 메시지가 포함된 장애 조치 링크를 모니터링하여 다른 유닛의 상태를 확인합 니다. 유닛에서 장애 조치 링크에 대한 3개의 연속 hello 메시지를 수신하지 못하고 모니터링된 인터 페이스에서 테스트가 실패할 경우 장애 조치 이벤트를 트리거할 수 있습니다.

이 그림에서는 정전이 있을 때 생성되는 경고에 대해 설명합니다.

Analysis Policies	Devices	Objects Integration		Deploy	Q 🔮 🌣 🍘 admin ▼ 號co	SECURE
					Dismiss all notifications	
Normal (2)	t Pending (0)	• Upgrade (0) • Snort 3 (2)			Interface Status - 10.82.141.171 Interface 'Ethernet1/1' has no link Interface 'Ethernet1/2' has no link	×
Model	Version	Chassis	Licenses	Access Cor	Cluster/Failover Status - 10.82.14 CLUSTER_STATE_GENERAL_FAILURE (Fill Stateful link down) CLUSTER_STATE_GENERAL_FAILURE (Fill LAN link down) PRIMARY (FLM19389LQR) FAILOVER_STATE_ACTIVE (HELLO not he peer)	1.171 × ailover ailover eard from
Firepower 9300 with FTD	7.2.5	E241-24-04-FPR9K-1.cisco.cor Security Module - 1	Essentials, IPS (2 more)	FTD HA	49	:
Firepower 9300 with FTD	7.2.5	EXAMPLE 1	Essentials, IPS (2 more)	FTD HA	Q>	:

전원 장애 시 장애 조치

를 위해 실패 원인을 확인하려면 다음 명령을 사용합니다.

• show failover history - 장애 조치 기록을 표시합니다. 장애 조치 내역은 과거 장애 조치 상태 변경 사 항 및 상태 변경 사유를 표시합니다.

<#root>					
firepower#					
show failover history					
From State	To State	Reason			
	Just Active	HELLO not heard from peer			

		(failover link down)
22:14:42 UTC Sep 26 2023		
Just Active	Active Drain	HELLO not heard from peer (failover link down
22:14:42 UTC Sep 26 2023		
Active Drain	Active Applying Config	HELLO not heard from peer (failover link down
22:14:42 UTC Sep 26 2023		
Active Applying Config	Active Config Applied	HELLO not heard from peer (failover link down)
22:14:42 UTC Sep 26 2023		
Active Config Applied	Active	HELLO not heard from peer (failover link down)

• show failover state - 이 명령은 두 유닛의 장애 조치 상태 및 마지막으로 보고된 장애 조치 사유를 표시합니다.

<#root>

firepower#

show failover state

	State	Last Failure Reason	Date/Time
This host -	- Primary		
	Active	None	
Other host -	- Secondary		
	Failed	Comm Failure	22:14:42 UTC Sep 26 2023

활용 사례 - MIO-Hearbeat 장애(하드웨어 장치)

애플리케이션 인스턴스는 수퍼바이저에 하트비트를 주기적으로 전송합니다. 하트비트 응답이 수신 되지 않으면 장애 조치 이벤트가 트리거될 수 있습니다.

를 위해 실패 원인을 확인하려면 다음 명령을 사용합니다.

• show failover history - 장애 조치 기록을 표시합니다. 장애 조치 내역은 과거 장애 조치 상태 변경 사 항 및 상태 변경 사유를 표시합니다.

<#root>				
firepower#				
show failover history				
From State	To State	Reason		
02:35:08 UTC Sep 26 2023 Active	Failed	MIO-blade heartbeat failure		

02:35:12 UTC Sep 26 2023 Failed	Negotiation	MIO-blade heartbeat recovered
02:37:02 UTC Sep 26 2023		
Sync File	System Bulk Sync	Detected an Active mate
02:37:14 UTC Sep 26 2023		
Bulk Sync	Standby Ready	Detected an Active mate

MIO-hearbeat가 실패할 경우 문제 해결 파일을 수집하고 FXOS의 기술 로그를 표시하고 Cisco TAC에 문의하는 것이 좋습니다.

firepower 4100/9300의 경우 show tech-support 섀시 및 show tech-support 모듈을 수집합니다.

FPR1000/2100 및 Secure Firewall 3100/4200의 경우 show tech-support 양식을 수집합니다.

관련 정보

- <u>FTD의 고가용성</u>
- Firepower 어플라이언스에서 FTD 고가용성 설정
- <u>firepower 파일 생성 절차 문제 해결</u>
- <u>비디오 FXOS에서 Show Tech-Support 파일을 생성하는 방법</u>
- <u>기술 지원 및 문서 Cisco Systems</u>

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번 역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.