ASA 장애 조치 시 스플릿 브레인 문제 해결

목차

소개

이 문서에서는 Cisco ASA(Adaptive Security Appliance) 장애 조치 또는 FTD(Firepower Threat Defense) HA(High Availability) 쌍에서 발생하는 일반적인 스플릿 브레인 문제를 해결하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 ASA/FTD High Availability Pair(Failover)의 작동 방식 대해 알고 있는 것이 좋습니다(정보).

사용되는 구성 요소

이 문서는 특정 소프트웨어 또는 하드웨어 버전으로 제한되지 않으며 장애 조치에서 지원되는 모든 ASA/FTD 구축에 적용됩니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참조하십시오.

스플릿 브레인(Split-Brain)이란 무엇입니까?

스플릿 브레인(Split-brain)은 ASA/FTD HA의 유닛이 네트워크에서 서로를 탐지할 수 없으므로 둘 다 활성 역할을 수행하는 시나리오입니다. 이렇게 하면 유닛이 동일한 인터페이스 IP 주소와 MAC 주소를 가지며 네트워크에 심각한 불일치를 일으켜 서비스가 손실될 수 있습니다.

HA가 스플릿 브레인(split-brain)에 있는지 확인하려면 두 유닛 모두에서 **show failover state** 명령을 실행하고 두 상자가 모두 활성 상태인지 확인합니다.

스플릿 브레인 예시:

기본 단위:

```
ciscoasa1/act/pri# show failover state

State Last Failure Reason Date/Time
This host - Primary
 Active None
Other host - Secondary
Failed Comm Failure 02:39:43 UTC Jan 10 2022

====Configuration State===
 Sync Done - STANDBY
====Communication State==
```

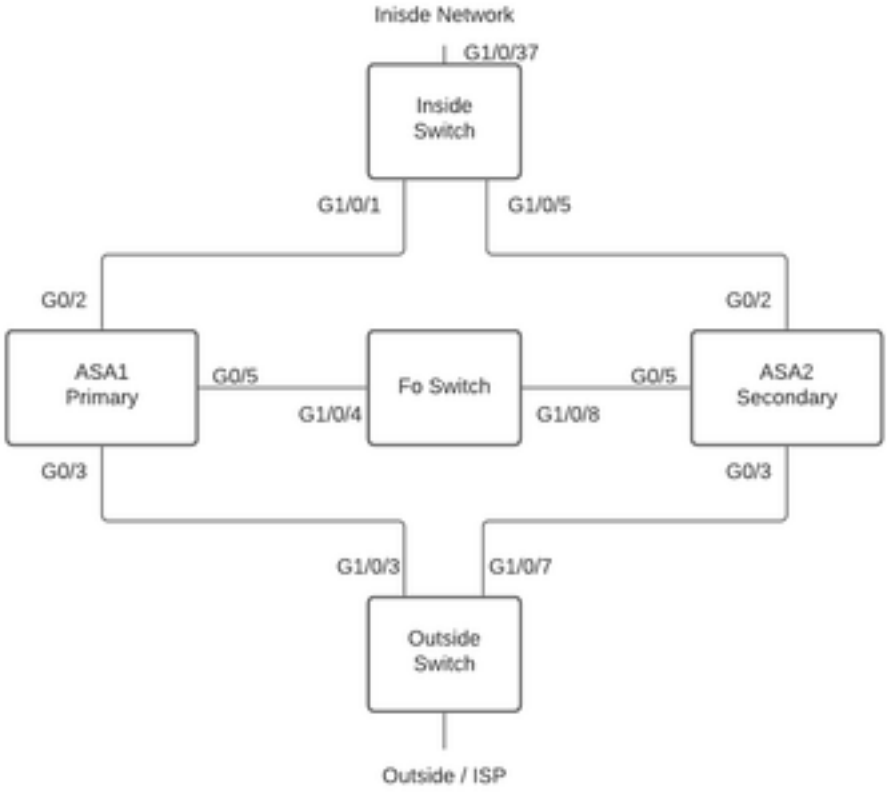
보조 유닛:

```
ciscoasa2/act/sec# show failover state

State Last Failure Reason Date/Time
This host - Secondary
 Active None
Other host - Primary
Failed Comm Failure 02:39:40 UTC Jan 10 2022

====Configuration State===
  Sync Done
 Sync Done - STANDBY
====Communication State==
```

연결된 디바이스의 활성 IP 주소에 대해 학습된 MAC 주소가 모두 동일한 유닛이 아닐 경우 스플릿 브레인(split-brain)이 중단될 수 있습니다. 예를 들어, 네트워크 토폴로지를 고려하십시오.



랩 토폴로지

VMAC는 다음과 같이 인터페이스에 할당되었으며, 이는 **mac 주소 테이블**을 쉽게 이해할 수 있도록 하기 위해 수행되었습니다.

```
Inside (G0/2)    : Active MAC    - 00c1.1000.aaaa
                         Standby MAC - 00c1.1000.bbbb

Outside (G0/4) : Active MAC    - 00c1.2000.aaaa

                         Standby MAC - 00c1.2000.bbbb
```

참고: VMAC이 구성되지 않은 경우 활성 디바이스는 항상 기본 유닛 인터페이스에 대해 MAC을 사용하며 스탠바이는 보조 MAC를 사용합니다.

HA가 정상인 경우 스위치의 MAC 주소 테이블:

```
Switch#show mac address-table

Mac Address Table
-------------------------------------------
Vlan Mac Address Type Ports
---- ----------- -------- -----
100 00c1.1000.aaaa DYNAMIC Gi1/0/5
100 00c1.1000.bbbb DYNAMIC Gi1/0/1
300 00c1.64bc.c508 DYNAMIC Gi1/0/4
300 00d7.8f38.8424 DYNAMIC Gi1/0/8
200 00c1.2000.aaaa DYNAMIC Gi1/0/7
200 00c1.2000.bbbb DYNAMIC Gi1/0/3
```

장애 조치 링크에 장애가 발생하면 액티브 유닛은 활성 상태를 유지하고 스탠바이 유닛은 대기 상

태를 유지합니다. 유닛이 장애 조치 링크에서 세 개의 연속 HELLO 메시지를 수신하지 않을 경우, 유닛은 장애 조치 링크를 비롯한 각 데이터 인터페이스에서 LANTEST 메시지를 전송하여 피어가 응답하는지 여부를 검증합니다. ASA에서 수행하는 작업은 다른 유닛의 응답에 따라 달라집니다.

가능한 작업은 다음과 같습니다.

- ASA가 장애 조치 링크에서 응답을 수신하면 장애 조치가 수행되지 않습니다.
- ASA가 장애 조치 링크에 대한 응답을 수신하지 않지만 데이터 인터페이스에서 응답을 수신하면 유닛이 장애 조치를 수행하지 않습니다. 장애 조치 링크가 실패한 것으로 표시됩니다. 장애 조치 링크가 중단된 동안에는 유닛에서 스탠바이 유닛으로 장애 조치를 수행할 수 없으므로 최대한 빨리 장애 조치 링크를 복원해야 합니다.
- ASA가 어떤 인터페이스도 응답을 받지 못하면 스탠바이 유닛은 액티브 모드로 전환되고 다른 유닛은 실패한 것으로 분류합니다. 이것은 스플릿 브레인 시나리오로 이어질 것이다.

이 단계에서는 두 방화벽의 모든 데이터 인터페이스가 액티브 유닛처럼 작동합니다. 따라서 액티브 및 스탠바이 방화벽의 인터페이스는 동일한 IP 및 MAC 주소를 사용합니다. 그러면 포이즌 arp 항목으로 인해 일관성 없는 MAC 주소 테이블이 생성되어 중단이 발생합니다.

> **참고:** 장애 조치 링크는 장애 조치 쌍(Failover Pair): 유닛 상태(액티브/스탠바이), hello 메시지, 네트워크 링크 상태, MAC 주소 교환, 구성 복제 및 동기화 간의 이 데이터 통신을 담당합니다.

장애 조치 문제를 사전에 대비하는 방법

스플릿 브레인(Split-brain) 상태에 대해 사전에 대비하려면

- Cisco Recommended Golden Release - 특정 조건에서 메모리 누수 등의 문제로 인해 스플릿 브레인(split-brain)도 발생할 수 있습니다. Cisco Recommended 릴리스를 사용하면 이러한 상황에 대한 노출을 크게 줄일 수 있습니다.
- Network Topology(네트워크 토폴로지) - 데이터 인터페이스와 장애 조치 링크의 경로가 다르므로 모든 인터페이스가 동시에 실패할 가능성이 줄어듭니다.
- 장애 조치 인터페이스에 포트 채널 인터페이스 사용 - 방화벽에 사용되지 않는 인터페이스가 있는 경우 이를 페어링하여 포트 채널을 구성하고 장애 조치 링크로 사용하면 링크 신뢰성이 향상되고 SPOF(Single Point of Failure)가 제거됩니다.
- 장애 조치 인터페이스에 너무 많은 레이턴시가 발생하지 않도록 하십시오. - ASA 구성 가이드 "장거리 장애 조치를 사용할 때 최적의 성능을 얻으려면 상태 링크의 레이턴시는 10밀리초 미만이고 250밀리초까지만 허용됩니다. 레이턴시가 10밀리초 이상인 경우 장애 조치 메시지의 재전송으로 인해 일부 성능 저하가 발생합니다."
- 구축에 따라 폴링 타이머/보류 타이머 값 조정 - 장애 조치 타이머에 대한 모든 접근 방식에 맞는 사이즈는 없습니다. 일반적으로 타이머를 낮추면 불필요한 장애 조치(특히 레이턴시가 있는 경우)가 발생할 수 있으며 값이 너무 높으면 장애 조치가 발생하는 시간이 증가할 수 있습니다. 따라서 장애 조치가 두드러집니다. 보류 타이머 값은 5x 폴링 타이머 값이어야 합니다.
- 인터페이스에 대해 가상 MAC 주소 구성 - "보조 유닛이 기본 유닛을 탐지하지 않고 부팅하는 경우, 보조 유닛은 액티브 유닛이 되고 기본 유닛 MAC 주소를 알지 못하므로 자체 MAC 주소를 사용합니다. 기본 유닛을 사용할 수 있게 되면 보조(활성) 유닛에서는 MAC 주소를 기본 유닛의 주소로 변경하며, 네트워크 트래픽이 중단될 수 있습니다. 마찬가지로, 기본 유닛을 새 하드웨어로 교체하면 새 MAC 주소가 사용됩니다." 가상 MAC는 시작 시 활성 MAC 주소를 보조 유닛

에 알려주고 새 기본 유닛 하드웨어의 경우 그대로 유지하므로 이 중단에 대한 차단을 보호합니다. 가상 MAC 주소를 구성하지 않으면 연결된 라우터에서 ARP 테이블을 지워 트래픽 흐름을 복원해야 할 수 있습니다." 자세한 내용은 장애 조치의 MAC 주소 및 IP 주소를 참조하십시오.
- 두 유닛에 대한 ASA/FTD 로그를 외부 Syslog 서버로 전송 - 이 단계는 문제 서비스 가용성을 위한 것입니다.

스플릿 브레인 이유

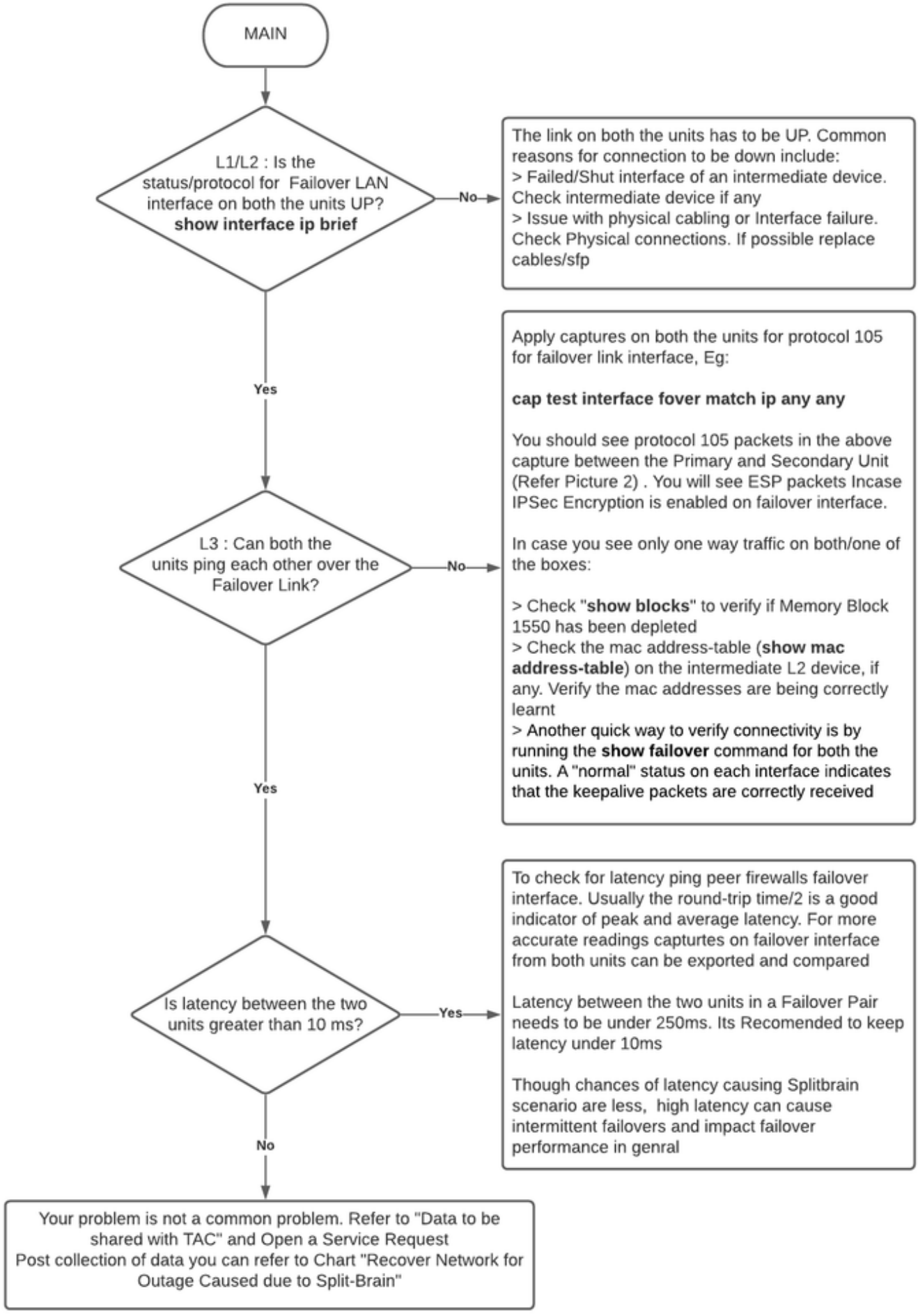
이미 언급했듯이, 장애 조치 링크 인터페이스 간의 통신이 다운될 때(단방향 또는 양방향으로) 스플릿 브레인(split-brain)이 발생합니다. 가장 일반적인 이유는 다음과 같습니다.

- L1 문제 - 케이블/SFP/인터페이스 오류
- 중간 장치의 문제
- ASA/FTD의 메모리 또는 CPU 리소스 부족 **참고:** ASA/Lina Engine은 1550바이트 메모리 블록을 사용하여 처리를 위해 패킷을 저장합니다. 이 크기의 사용 가능한 블록이 없는 경우 ASA/FTD는 더 이상 장애 조치 패킷을 처리할 수 없게 됩니다. show blocks를 실행하여 블록 감소를 확인합니다.

문제 해결 절차 - 순서도

스플릿 브레인 시나리오를 트러블슈팅하고 해결하려면 이 순서도를 사용하여 **Main**으로 표시된 상자에서 시작합니다. 여기서 해결할 수 없는 문제가 있습니다. 이러한 경우 Cisco 기술 지원에 대한 링크가 제공됩니다. 서비스 요청을 열려면 유효한 서비스 계약이 있어야 합니다.

참고: FTD 구축에서 이 차트의 단계는 "**system support diagnostics-cli**"에서 따라야 합니다.


MAIN
L1/L2 : Is the status/protocol for Failover LAN interface on both the units UP? show interface ip brief
No
The link on both the units has to be UP. Common reasons for connection to be down include:
> Failed/Shut interface of an intermediate device. Check intermediate device if any
> Issue with physical cabling or Interface failure. Check Physical connections. If possible replace cables/sfp
Yes
Apply captures on both the units for protocol 105 for failover link interface, Eg:
cap test interface fover match ip any any
You should see protocol 105 packets in the above capture between the Primary and Secondary Unit (Refer Picture 2) . You will see ESP packets Incase IPSec Encryption is enabled on failover interface.
L3 : Can both the units ping each other over the Failover Link?
No
In case you see only one way traffic on both/one of the boxes:
> Check "show blocks" to verify if Memory Block 1550 has been depleted
> Check the mac address-table (show mac address-table) on the intermediate L2 device, if any. Verify the mac addresses are being correctly learnt
> Another quick way to verify connectivity is by running the show failover command for both the units. A "normal" status on each interface indicates that the keepalive packets are correctly received
Yes
Is latency between the two units greater than 10 ms?
Yes
To check for latency ping peer firewalls failover interface. Usually the round-trip time/2 is a good indicator of peak and average latency. For more accurate readings capturtes on failover interface from both units can be exported and compared
Latency between the two units in a Failover Pair needs to be under 250ms. Its Recomended to keep latency under 10ms
Though chances of latency causing Splitbrain scenario are less, high latency can cause intermittent failovers and impact failover performance in genral
No
Your problem is not a common problem. Refer to "Data to be shared with TAC" and Open a Service Request
Post collection of data you can refer to Chart "Recover Network for Outage Caused due to Split-Brain"

문제 해결 흐름도

스플릿 브레인 응급 복구

스플릿 브레인(split-brain)에서 네트워크를 복구하려면 트래픽이 두 방화벽 중 하나에 도달하는지, 즉 활성 IP에 대해 학습된 MAC 주소가 모두 단일 유닛을 가리키도록 해야 합니다. 이렇게 하려면 유닛에서 장애 조치를 비활성화하거나 네트워크를 완전히 차단할 수 있습니다.

1. 트래픽을 전달하지 않는 유닛에서 장애 조치 비활성화: ASA 플랫폼에서 CLI를 통해 컨피그레이션 터미널로 이동하고 no failover 명령을 입력합니다.FTD Platform의 Clish 모드에서 configure **high-availability suspend** 명령을 입력합니다.
2. ASA의 경우 데이터 인터페이스를 종료합니다. FTD의 경우 연결된 디바이스의 인터페이스를 종료합니다. 또는 인터페이스를 물리적으로 분리할 수도 있습니다. 또한 디바이스의 전원을 끌 수 있지만, 이렇게 하면 디바이스 관리가 제한됩니다. 이 작업을 수행하는 단계에 대한 디바이스 컨피그레이션 가이드를 참조하십시오.

   참고: 앞서 언급한 단계를 수행한 후에도 연결 문제가 발생하면 연결된 디바이스에 오래된 arp 항목이 있을 수 있습니다. 업스트림 및 다운스트림 디바이스에서 arp 항목을 확인합니다. 이 문제를 해결하려면 이러한 항목을 플러시하거나 작업 중인 ASA/FTD에서 문제가 있는 인터페이스 IP에 대한 패킷 패킷을 전송하도록 강제할 수 있습니다. 이렇게 하려면 enable 모드에서 명령을 실행합니다(시스템의 FTD는 diagnostics-cli를 지원) - debug **menu ipaddrutl 6 <interface ip address>**.

   주의: 스플릿 브레인 관련 문제에 대해 TAC와 함께 지원 티켓을 열 경우 이 문서에서 **"TAC 서비스 요청에 대해 수집할 데이터"** 섹션에 언급된 정보를 공유하십시오.

TAC와 공유할 데이터

TAC 서비스 요청을 열어야 할 경우에 대비하여 언급된 데이터를 공유하십시오.

1. ASA/FTD-HA 및 인접 디바이스와의 물리적 연결을 보여 주는 토폴로지 다이어그램(장애 조치 인터페이스 포함).
2. ASA의 **show tech-support** 또는 FTD를 실행하는 플랫폼의 문제 해결 파일에 대한 출력입니다.
3. 문제가 발생한 경우 +/- 5분 동안 Syslogs와 타임스탬프가 함께 제공됩니다.
4. FXOS 문제 해결 파일(하드웨어가 FPR 어플라이언스인 경우).

FTD 또는 FXOS에 대한 문제 해결 파일을 생성하려면 Firepower Troubleshoot File Generation Procedures를 참조하십시오. TAC SR을 엽니다.