높은 액세스 목록 요소 수로 인한 보안 방화벽 FTD 높은 메모리

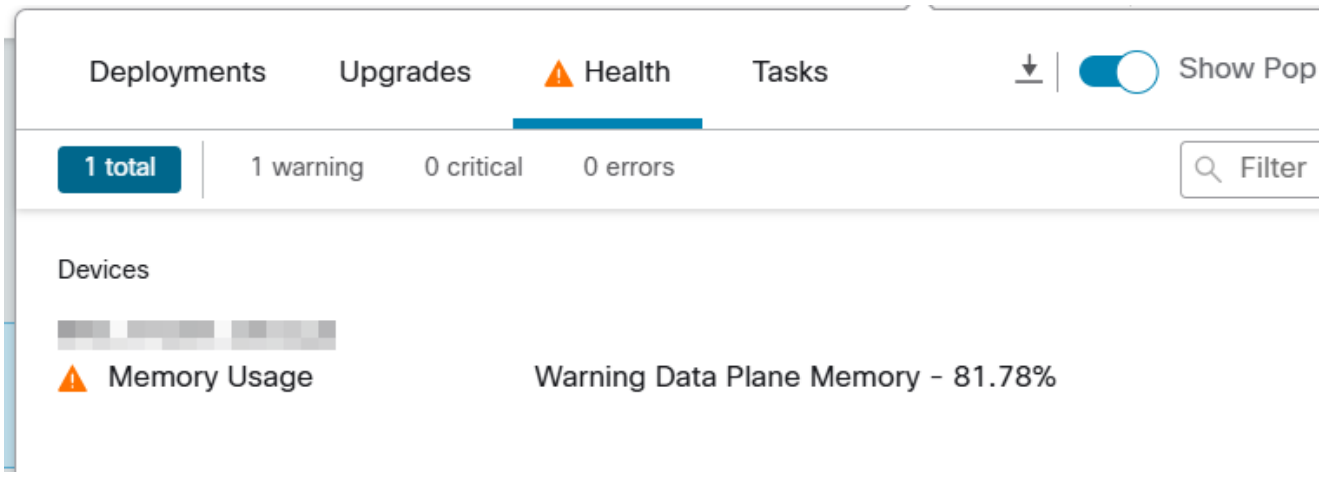
목차

문제

FTD는 지속적으로 높은 데이터 플레인 메모리 사용률 경고를 80% 이상 표시합니다. 액세스 목록 요소 수가 플랫폼이 수용할 수 있는 것보다 훨씬 더 많이 증가하는 정책 구축 후에도 메모리 사용률이 이 높은 수준에 머물러 있습니다.

FTD High Availability 컨피그레이션에서 이 문제는 두 유닛에 영향을 미치지만 활성 FTD의 메모리 사용량이 더 높습니다.

- FMC 경고는 FTD의 데이터 플레인에서 높은 메모리 사용량을 보여줍니다.



- FTD CLI는 또한 높은 메모리 사용량을 확인합니다.

<#root>

```
firepower# show memory
Free memory:        2590897856 bytes (18%)
Used memory:       11746269504 bytes (82%)

-------------      ------------------
Total memory:      14337167360 bytes (100%)
```

- access-list element count는 FTD CLI에서 100만 개 이상의 요소를 보여줍니다.

<#root>

```
firepower# show access-list element-count
```

Total number of access-list elements: 3223691

- FTD에 대한 FMC 상태 모니터링 그래프에서는 ACE 구축과 관련된 메모리가 크게 증가했습니다.



- 고가용성 피어 FTD에서 메모리 사용이 지워지지 않은 메모리로 인해 높은 수준으로 중단될 수 있습니다.

<#root>

```
firepower# failover exec standby show memory
Free memory:         3278441368 bytes (23%)
```

Used memory: 11058725992 bytes (77%)

```
-------------      -------------------
Total memory:       14337167360 bytes (100%)
```

환경

- 고가용성 구성의 Cisco Firepower 2130 Threat Defense
- FTD 소프트웨어 버전: 7.4.2
- FMC 소프트웨어 버전: 7.6.2
- 액세스 목록 요소가 100만 개 이상 많음

해결

1. FTD High Availability(FTD 고가용성) 컨피그레이션에서 사전 계획된 시간 동안 피어 FTD를 재부팅하여 이전에 누적되었을 수 있는 보존된 메모리 저장소를 지웁니다.

2. 재부팅 후 다음을 확인합니다.

- 피어 FTD가 고가용성 쌍으로 올바르게 다시 동기화됩니다.
- 메모리 사용률이 정상 수준을 나타냅니다.
- FTD 메모리 알림은 FMC UI에서 지워집니다.

3. Devices(디바이스) > Device Management(디바이스 관리)로 이동하고 FTD에 대한 Edit(편집) 아이콘을 클릭합니다.

4. 왼쪽 상단 근처의 장치 탭(FTD HA의 요약 탭)을 클릭하고 고급 설정 섹션까지 아래로 스크롤한 다음 편집 아이콘을 클릭합니다.

5. 이 기능을 사용하려면 객체 그룹 검색 확인란을 선택하고 저장을 클릭합니다.

6. FTD HA 쌍에 컨피그레이션 변경 사항을 구축하고 상태 모니터를 몇 분 동안 모니터링하여 메모리 사용량 변경 사항을 관찰합니다.

<#root>

```
firepower# show memory
Free memory:        6948343576 bytes (48%)
```

```
Used memory:        7388823784 bytes (52%)


-------------     --------------------------
Total memory:      14337167360 bytes (100%)
```

추가 고려 사항

Object Group Search를 활성화한 후에도 메모리 사용률이 지속적인 성능 문제가 될 경우 다음과 같은 최적화 전략을 고려하십시오.

- FMC 연결 이벤트를 사용하여 상위 적중 횟수 규칙 검토
- 신뢰할 수 있는 대용량 트래픽에 대한 불필요한 검사 감소
- 모든 규칙에 침입 검사가 필요한지 여부 평가
- 대용량 Firepower 플랫폼(FPR4K 또는 FPR9K 시리즈)으로 플랫폼 업그레이드를 고려 중입니다.

원인

데이터 플레인 메모리 사용률이 높은 이유는 FTD의 보존된 메모리와 정책 구축 후 액세스 목록 요소 처리 오버헤드의 증가로 인해 발생합니다. 중요한 access-list 요소 수는 메모리 사용률 급증과 직접적으로 연관됩니다. 개체 그룹 검색 최적화 없이 ACL 처리 요구 사항이 크게 증가하면 높은 메모리 사용이 지속됩니다.

관련 콘텐츠

- FMC CLI를 사용하여 ACE(Access List Element) 수 계산
- Cisco Secure Firewall Management Center Device Configuration Guide, 7.4: 액세스 제어 규칙의 모범 사례
- Cisco Secure Firewall Management Center Device Configuration Guide, 7.4: 객체 그룹 검색 구성

- firepower 위협 방어를 위한 명령 참조
- Cisco 기술 지원 및 다운로드

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 번역 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.