연결 이벤트가 FireSIGHT Management Center에서 사라짐

목차

소개

이 문서에서는 시스템이 며칠 동안 실행된 후 FireSIGHT Management Center에서 연결 이벤트가 사라질 때 근본 원인을 파악하고 문제를 해결하는 방법에 대해 설명합니다.관리 센터의 컨피그레이션 설정으로 인해 발생할 수 있습니다.

사전 요구 사항

요구 사항

FireSIGHT Management Center에 대해 알고 있는 것이 좋습니다.

사용되는 구성 요소

이 문서의 정보는 다음 하드웨어 및 소프트웨어 버전을 기반으로 합니다.

- FireSIGHT Management Center
- 소프트웨어 버전 5.2 이상

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

문제 해결

1단계:저장된 이벤트 수 확인

FireSIGHT Management Center에 저장된 연결 이벤트 수를 확인하려면

1. Analysis **> Connections > Table View of Connection Events를 선택합니다**.
2. Time Window(시간 창)를 모든 현재 이벤트를 포함하는 넓은 범위로 확장합니다(예: 12개월).
3. 페이지 하단에 있는 총 행 수를 확인합니다.마지막 페이지를 클릭하고 마지막으로 사용 가능한 연결 이벤트의 타임스탬프를 확인합니다.

이 정보는 현재 컨피그레이션과 연결 이벤트를 유지할 수 있는 시간 및 기간에 대한 정보를 제공합니다.

2단계:로깅 옵션 결정

로깅되는 연결 및 연결이 로깅되는 플로우의 위치를 검토합니다.조직의 보안 및 규정 준수 요구 사항에 따라 연결을 로깅해야 합니다.생성하는 이벤트 수를 제한하는 것이 목표인 경우 분석에 중요한 규칙에 대해서만 로깅을 활성화합니다.그러나 네트워크 트래픽의 광범위한 보기를 원하는 경우 추가 액세스 제어 규칙 또는 기본 작업에 대한 로깅을 활성화할 수 있습니다.Connection Events를 장기간 보존할 수 있도록 중요하지 않은 트래픽에 대해 Connection Logging을 비활성화할 수 있습니다.

팁:성능을 최적화하려면 연결의 시작 또는 종료 중 하나만 로깅하는 것이 좋습니다.

참고:단일 연결의 경우 연결 종료 이벤트에는 연결 시작 이벤트의 모든 정보와 세션 동안 수집된 정보가 포함됩니다.신뢰 및 허용 규칙의 경우 연결 종료를 사용하는 것이 좋습니다.

이 차트에서는 각 규칙 작업에 사용할 수 있는 다양한 로깅 옵션에 대해 설명합니다.

규칙 작업 또는 로깅 옵션	시작 시 로그	끝에 로그
신뢰 기본 작업:신뢰	X	X
허용 기본 작업:침입	X	X
기본 작업:검색 모니터		X(필수)
차단 차단 후 재설정	X	
기본 작업:차단 인터랙티브 차단 인터랙티브 차단 및 재설정	X	X(우회된 경우)
보안 인텔리전스	X	

3단계:연결 데이터베이스의 크기 조정

연결 이벤트는 시스템 정책의 최대 연결 이벤트 설정에 따라 정리됩니다.설정을 변경하려면 다음을

수행합니다.

1. System(**시스템) > Local(로컬) > System Policy(시스템 정책)를 선택합니다**.
2. 현재 적용된 정책을 수정하려면 *연필* 아이콘을 클릭합니다.
3. Database **> Connection Database > Maximum Connection Events를 선택합니다**.
4. Maximum Connection Events(**최대 연결 이벤트**)의 값을 **변경합니다**.
5. Save **Policy and Exit를** 클릭한 다음 **Apply** the policy to your appliances를 클릭합니다.

저장할 수 있는 연결 이벤트의 최대 양은 Management Center 모델에 따라 달라집니다.

> **참고:**최대 이벤트 제한은 연결 이벤트와 보안 인텔리전스 이벤트 간에 공유됩니다.두 이벤트에 대해 구성된 최대값의 합계가 최대 이벤트 제한을 초과할 수 없습니다.

관리 센터 모델	**최대 이벤트 수**
FS750, DC750	5,000만
FS1500, DC1500	1억
FS2000	3억
FS3500, DC3500	5억
FS4000	10억
가상 어플라이언스	1,000만

> **주의:**데이터베이스 제한이 증가하면 디바이스에 부정적인 성능이 영향을 미칠 수 있습니다.성능을 향상시키려면 이벤트 제한을 정기적으로 작업하는 이벤트 수에 맞게 조정해야 합니다.

시간 범위 동안 이벤트 수를 표시하는 위젯의 경우 이벤트 뷰어에서 자세한 데이터를 사용할 수 있는 이벤트 수가 총 이벤트 수를 반영하지 않을 수 있습니다.이는 디스크 공간 사용량을 관리하기 위해 오래된 이벤트 세부 정보가 삭제되는 경우가 있기 때문입니다.이벤트 세부 정보 정리 발생을 최소화하기 위해 구축에서 가장 중요한 이벤트만 기록하도록 이벤트 로깅을 미세 조정할 수 있습니다
.

관련 정보

- 데이터베이스 이벤트 제한 구성
- 기술 지원 및 문서 – Cisco Systems