보안 엔드포인트 Linux 커넥터 오류 트러블슈팅

목차

소개

이 문서에서는 Cisco Secure Endpoint Linux Connector가 정상적인 작동에 영향을 주는 조건을 알리기 위해 사용하는 결함에 대해 설명합니다.

배경 정보

Cisco Secure Endpoint Linux 커넥터는 커넥터의 적절한 기능에 영향을 주는 조건을 감지하면 Fault Raised(결함 발생) 이벤트로 알립니다. 마찬가지로, Fault Cleared 이벤트는 조건이 더 이상 존재하지 않음을 알려줍니다.

보안 엔드포인트 Linux 커넥터 결함 테이블

이 표에서는 결함 및 관련 진단 단계에 대해 설명합니다.

결함 ID	설명	문제 해결/해결
5	스캔 서비스 사용자를 사용할 수 없음	커넥터가 파일 스캔 프로세스를 실행할 사용자를 만들지 못했습니다. 커넥터는 루트 사용자를 사용하여 파일 스캔을 해결합니다. 이는 의도한 설계에서 벗어나 예상하지 못한 것이다. 이 `cisco-amp-scan-svc` 사용자 또는 그룹이 삭제되었거나 사용자 및 그룹의 구성이 변경된 경우 커넥터를 다시 설치하여 필요한 구성으로 사용자 및 그룹을 다시 만들 수 있습니다. 자세한 내용은 /var/log/cisco/ampdaemon.log. /etc/login.defs의 설정을 통해 사용자 그룹 생성이 제한되는 경우, 사용자와 그룹을 생성할 수 있도록 설치 프로그램을 실행하는 동안 이 파일을 임시로 변경해야 합니다. 이렇게 하려면 usergroups_enab를 no에서 yes로 변경합니다. 이 결함은 다른 프로그램이 커넥터의 디렉터리 권한 중 하나(즉, /opt/cisco 또는 하위 디렉터리)를 수정한 경우 Linux 커넥터 1.15.1 이상에서 발생할 수 있습니다. 이 문제를 해결하려면 변경된 디렉터리 사용 권한을 다시 기본값(예:

		0755)으로 설정하고, 이후 프로그램에서 /opt/cisco 디렉터리(또는 자식 디렉터리)를 수정하지 않도록 하고, 커넥터 서비스를 다시 시작해야 합니다.
6	자주 서비스 검사 다시 시작	커넥터 파일 검사 프로세스에서 오류가 반복되었으며, 오류를 지우기 위해 커넥터가 다시 시작되었습니다. 시스템에 있는 하나 이상의 파일이 스캔 시 스캔 알고리즘이 충돌할 수 있습니다. 커넥터는 최선형(best-effort) 기반으로 스캔을 계속합니다. 커넥터가 시작된 후 10분 이내에 이 결함이 자동으로 제거되지 않을 경우, 이는 추가적인 사용자 개입이 필요하며 커넥터에서 스캔을 수행하는 기능이 저하됨을 나타냅니다. 자세한 내용은 /var/log/cisco/ampdaemon.log 및 /var/log/cisco/ampscansvc.log을 참조하십시오.
7	스캔 서비스를 시작하지 못했습니다.	커넥터의 파일 스캔 프로세스를 시작하지 못했으며 오류를 지우기 위해 커넥터가 다시 시작되었습니다. 이 결함이 제기되는 동안 파일 스캔 기능을 사용할 수 없습니다. 이 실패는 새로 설치된 바이러스 정의 파일(.cvd 파일)을 로드할 때 오류가 발생한 경우 트리거될 수 있습니다. 커넥터는 이 오류를 방지하기 위해 새 .cvd 파일을 활성화하기 전에 여러 무결성 및 안정성 검사를 수행합니다. 다시 시작할 때 커넥터는 잘못된 .cvd 파일을 제거하여 커넥터를 다시 시작할 수 있도록 합니다. 커넥터가 재시작될 때 이 결함이 제거되지 않으면 사용자 개입이 추가로 필요함을 나타냅니다. 이 오류가 각 .cvd 업데이트와 함께 반복되면 잘못된 .cvd 파일이 커넥터의 .cvd 파일 무결성 검사에서 제대로 탐지되지 않음을 나타냅니다. 이 오류는 시스템이 사용 가능한 메모리가 부족하고 스캐너 서비스를 시작할 수 없는 경우 Linux 커넥터에서 트리거될 수 있습니다. Linux의 최소 시스템 요구 사항은 "Secure Endpoint(이전의 AMP for Endpoints) 사용자 가이드"를 참조하십시오. 자세한 내용은 /var/log/cisco/ampdaemon.log 및 /var/log/cisco/ampscansvc.log을 참조하십시오.
8	실시간 파일 시스템 모니터를 시작하지 못했습니다.	실시간 파일 시스템 활동 모니터링을 제공하는 커널 모듈이 로드되지 않았고 커넥터 정책에서 "파일 복사 및 이동 모니터링"을 사용하도록 설정했습니다. 이 결함이 제기되는 동안에는 커넥터에서 이러한 모니터링 기능을 사용할 수 없습니다. 이 결함은 Secure Endpoint 커넥터가 파일 시스템 활동 모니터링에 필요한 기본 커널 모듈을 로드할 수 없을 때 제기됩니다. 시스템에서 UEFI 보안 부팅을 비활성화해야 합니다.

		Secure Boot(보안 부팅)가 비활성화된 경우, 이 결함은 Secure Endpoint 커넥터가 제공하는 ampavflt 또는 ampfsm 커널 모듈과 시스템에 설치된 시스템 커널 또는 기타 서드파티 커널 모듈 간의 비호환성 때문에 발생할 수 있습니다. 자세한 내용은 /var/log/messages를 참조하십시오. 이 결함은 커넥터에서 지원하지 않는 커널 버전을 실행할 때도 발생할 수 있습니다. 이 경우 현재 실행 중인 시스템 커널에 대해 사용자 정의 ampfsm 커널 모듈을 구축하여 제거할 수 있습니다. (Linux 커넥터 버전 1.16.0 이상에만 적용 가능) 커스텀 커널 모듈 구축에 대한 자세한 내용은 다음을 참조하십시오. Cisco Secure Endpoint Linux Connector 커널 모듈 구축
9	실시간 네트워크 모니터를 시작하지 못했습니다.	실시간 네트워크 활동 모니터링을 제공하는 커널 모듈이 로드되지 않았고 커넥터 정책에서 "Enable Device Flow Correlation"을 사용하도록 설정했습니다. 이 결함이 제기되는 동안에는 커넥터에서 이 모니터링 기능을 사용할 수 없습니다. 이 결함은 Secure Endpoint 커넥터가 파일 시스템 활동 모니터링에 필요한 기본 커널 모듈을 로드할 수 없을 때 제기됩니다. 시스템에서 UEFI 보안 부팅을 비활성화해야 합니다. Secure Boot(보안 부팅)가 비활성화된 경우, 이 결함은 Secure Endpoint 커넥터가 제공하는 ampavflt 또는 ampfsm 커널 모듈과 시스템에 설치된 시스템 커널 또는 기타 서드파티 커널 모듈 간의 비호환성 때문에 발생할 수 있습니다. 자세한 내용은 /var/log/messages를 참조하십시오. 이 결함은 커넥터에서 지원하지 않는 커널 버전을 실행할 때도 발생할 수 있습니다. 이 경우 현재 실행 중인 시스템 커널에 대해 사용자 정의 ampfsm 커널 모듈을 구축하여 제거할 수 있습니다. (Linux 커넥터 버전 1.16.0 이상에만 적용 가능) 커스텀 커널 모듈 구축에 대한 자세한 내용은 다음을 참조하십시오. Cisco Secure Endpoint Linux Connector 커널 모듈 구축
11	필요한 커널 수준 패키지가 없습니다.	Secure Endpoint 커넥터는 eBPF 모듈을 사용하여 파일 시스템, 프로세스 및 네트워크 활동을 모니터링합니다. 커넥터에서 이러한 eBPF 모듈을 로드하고 실행하려면 특정 패키지를 시스템에서 사용할 수 있어야 합니다. 이 오류를 해결하려면 아래 설명된 대로 Linux 배포판에 필요한 패키지를 설치하고 커넥터를 다시 시작하십시오. Red Hat 기반 배포의 경우 이 결함은 커널 레벨 패키지가 없을 때 제기됩니다. 커널 레벨 패키지를 설치하고 커넥터를 다시 시작합니다. (Linux 커넥터 버전 1.13.0 이상에만 적용 가능) Oracle Linux UEK 6 이상의 경우 이 결함은 kernel-uek-devel에서 제기됩니다패키지가 없습니다. kernel-uek-dev 패키지를 설치하고 커넥터를 다시 시작합니다. (Linux 커넥터 버전 1.18.0 이상에만 적용 가능) 데비안 기반 배포의 경우 이 결함은 linux-headers 패키지가 없을 때 제기됩니다. linux-headers 패키지를 설치하고 커넥터를 다시 시작합니다. (Linux 커

		넥터 버전 1.15.0 이상에만 적용 가능) 자세한 내용은 다음을 참조하십시오. Linux 커널 레벨 결합
16	호환되지 않는 커널	현재 실행 중인 커널이 현재 실행 중인 커넥터와 호환되지 않으며 커넥터 정책에 "Monitor File Copies and Moves(파일 복사 및 이동 모니터링)" 또는 "Enable Device Flow Correlation(디바이스 흐름 상관관계 활성화)"이 활성화되어 있습니다. 커널을 지원되는 버전으로 다운그레이드하거나 커넥터를 이 커널을 지원하는 최신 버전으로 업그레이드합니다. 지원되는 커널 버전에 대한 자세한 내용은 다음을 참조하십시오. Cisco Secure Endpoint Linux Connector OS 호환성
18	커넥터 이벤트 모니터링이 오버로드되었습니다.	이 결함은 시스템 이벤트가 너무 많아 커넥터의 부하가 높을 때 발생합니다. 시스템 보호가 제한되어 있으며, 전체 시스템 활동이 줄어들 때까지 커넥터는 소규모 시스템 중요 이벤트를 모니터링합니다. 이 결함은 악의적인 시스템 활동을 나타내거나 시스템에서 매우 활성화된 애플리케이션을 나타낼 수 있습니다. 활성 애플리케이션이 사용자가 신뢰하는 안전한 경우, 커넥터의 모니터링 부하를 줄이기 위해 프로세스 제외 세트에 추가할 수 있습니다. 이 작업은 결함을 제거하는 데 충분할 수 있습니다. 무해한 프로세스로 인해 부하가 많이 발생하지 않는 경우, 일부 조사를 통해 악의적인 프로세스로 인해 활동이 증가했는지 확인해야 합니다. 커넥터가 과부하 상태에서 단기간에 있는 경우 이 결함이 스스로 제거될 수 있습니다. 이 결함이 자주 제기되고 로드가 과중한 정상적인 프로세스가 없으며 악의적인 프로세스가 검색되지 않은 경우, 무거운 로드를 처리하기 위해 시스템을 다시 프로비저닝해야 합니다.
19	SELinux 정책이 없거나 비활성화되었습니다.	이 결함은 시스템의 SELinux(Secure Enterprise Linux) 정책에서 Connector가 시스템 활동을 모니터링할 수 없게 될 때 제기됩니다. SELinux가 활성화되어 있고 적용 모드에 있는 경우 Connector는 SELinux 정책에서 다음 규칙을 필요로 합니다. `allow unconfined_service_t self:bpf { map_create map_read map_write prog_load prog_run };` RHEL 7 및 Oracle Linux 7을 비롯한 Red Hat 기반 시스템에서는 이 규칙이 기본 SELinux 정책에 없습니다. 설치 또는 업그레이드 중에 Connector는

		SELinux Policy Module이라는 이름의 설치를 통해 이 규칙을 추가하려고 합니다 `cisco 보안 bpf`. 경우 `cisco 보안 bpf` 설치 및 로드에 실패하거나 비활성화되면 결함이 제기됩니다. 결함을 해결하려면 시스템 패키지 policycoreutils-python이 설치되어 있어야 합니다. Connector를 다시 설치하거나 업그레이드하여 `cisco-secure-bpf`의 설치를 트리거하거나, 기존 SELinux 정책에 규칙을 수동으로 추가하고 Connector를 다시 시작합니다. 이 결함을 해결하기 위해 SELinux 정책을 수정하는 방법에 대한 자세한 지침은 SELinux 정책 결함을 참조하십시오.

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.