Cisco Secure Endpoint Mac Connector 결함

목차

소개

커넥터는 커넥터의 적절한 기능에 영향을 주는 조건을 탐지할 경우 Fault Raised 이벤트를 알려줄 수 있습니다.마찬가지로 Fault Cleared 이벤트는 해당 조건이 더 이상 존재하지 않음을 알립니다.

커넥터 결함 테이블

다음 표에서는 결함 및 해당 진단 단계에 대해 설명합니다.

결함 ID	포털 텍스트	엔드포인트 설명	문제 해결/해결
1	커널 모듈이 인증되지 않음	시스템 확장이 인증되지 않음	Connector의 시스템 확장이 실행되지 않도록 차단되었습니다. 보안 및 개인 정보 보호 시스템 기본 설정을 열고 확장을 승인합니다. 또는 MDM(Mobile Device Management) 프로파일을 사용하여 원격으로 시스템을 승인할 수 있습니다.
2	버전 불일치	시스템 확장 버전이 일치하지 않습니다.	설치된 커넥터 소프트웨어가 손상되었습니다.커넥터를 다시 설치합니다. 참고: Mac Connector 버전 1.14.0 이상을 실행하는 경우 컴퓨터를 다시 시작하여 결함의 일부 발생을 제거할 수 있습니다.
3	디스크 액세스가 허용되지 않음	전체 디스크 액세스가 허용되지 않음	커넥터가 검사를 위해 사용자 파일에 액세스할 수 없습니다.Security and Privacy System Preferences(보안 및 개인 정보 보호 시스템 기본 설정)를 열고 AMP 서에 대한 전체 디스크 액세스 권한을 부여합니다. 1.14.0 이전 버전의 Mac Connector의 경우 이 프로세스의 이름은 */opt/cisco/amp/ampdaemon입니다*. Mac Connector 버전 1.14.0 이상의 경우 다음 두 응용 프로그램은 macOS 버전라 전체 디스크 액세스가 필요합니다. • *AMP for Endpoints 서비스*(모든 macOS 버전에 필요) • *AMP 보안 확장* (macOS 10.15.5 이상에서 필요) Mac Connector 버전 1.14.1 이상의 경우 다음 두 응용 프로그램은 macOS 버전라 전체 디스크 액세스가 필요합니다. • *AMP for Endpoints 서비스*(모든 macOS 버전에 필요) • *AMP 보안 확장* (macOS 11 이상에서 필요) 자세한 내용은 이 기술 참고에 나와 있습니다.
4	커널 모듈이 로드되지 않았습니다.	시스템 확장을 로드할 수 없습니다.커넥터 재설치	Mac Connector 버전 1.14.0 이전 또는 macOS 10.14 또는 10.15에서 실행하는 이 결함은 커넥터의 시스템 확장이 올바른 버전이며 실행을 위해 승인되었지만 히 로드되지 않았음을 나타냅니다.자세한 *내용은 /Library/Logs/Cisco/ampdaemon.log*를 참조하십시오.커넥터를 제거하고 다시 하면 이 결함이 지워질 수도 있습니다.
5	스캔	스캔 서비스	커넥터가 파일 스캔 프로세스를 실행할 사용자를 만들지 못했습니다.Connecto

	서비스 사용자를 사용할 수 없음	사용자를 사용할 수 없음	트 사용자를 사용하여 파일 검사를 수행하여 이 문제를 해결합니다.이는 의도한 와 다르며 예상되지 않습니다. 이(가) `cisco-amp-scan-svc` 사용자 또는 그룹이 삭제되었거나 사용자 및 그룹의 구 이 변경되었습니다. 커넥터를 다시 설치하면 사용자 및 그룹이 필요한 구성으로 만들어집니다.자세한 내용은 */Library/Logs/Cisco/ampdaemon.log*.
6	스캔 서비스가 자주 다시 시작됩니다.	스캔 서비스가 자주 다시 시작됩니다.	Connector의 파일 스캔 프로세스에서 오류가 반복적으로 발생했고, 오류를 지우 Connector가 다시 시작되었습니다.시스템에 있는 하나 이상의 파일이 스캔될 때 캔 알고리즘이 충돌할 수 있습니다.커넥터는 최선의 방법으로 스캔을 계속합니 커넥터가 시작된 후 10분 이내에 이 결함이 자동으로 지워지지 않으면 추가 사용 개입이 필요하며 Connector의 스캔 수행 능력이 저하될 것임을 나타냅니다. 검토 */Library/Logs/Cisco/ampdaemon.log* 및 */Library/Logs/Cisco/ampscansvc.* 세한 내용을 참조하십시오.
7	스캔 서비스를 시작하지 못했습니다.	스캔 서비스를 시작하지 못했습니다.	Connector의 파일 스캔 프로세스를 시작하지 못했습니다. 이 오류를 지우려고 터가 다시 시작되었습니다.이 결함이 발생하는 동안 파일 스캔 기능이 비활성화 다. 새로 설치된 바이러스 정의 파일(.cvd 파일)을 로드할 때 오류가 발생하면 이 오 트리거할 수 있습니다. 이 오류를 방지하기 위해 Connector는 새 .cvd 파일을 활 하기 전에 여러 무결성 및 안정성 검사를 수행합니다.다시 시작하면 커넥터가 다 시작할 수 있도록 잘못된 .cvd 파일이 모두 제거됩니다. 커넥터를 다시 시작할 때 이 결함이 지워지지 않으면 추가 사용자 개입이 필요함 나타냅니다.이 오류가 각 .cvd 업데이트와 함께 반복되면 Connector의 .cvd 파일 결성 검사에서 잘못된 .cvd 파일이 제대로 탐지되지 않음을 나타냅니다. 검토 */Library/Logs/Cisco/ampdaemon.log* 및 */Library/Logs/Cisco/ampscansvc.* 세한 내용을 참조하십시오.
10	커널 모듈 또는 시스템 확장을 로드하려면 재부팅해야 합니다.	시스템 확장을 로드하려면 재부팅해야 합니다.	시스템을 재부팅합니다. Mac Connector 버전 1.11.1 및 1.14.0의 경우 시스템 확장을 로드할 수 없는 경우 결함이 발생할 수 있습니다.이 경우 Connector를 다시 설치하여 이 결함을 제거 있습니다. 시스템에 너무 많은 Network Content Filter 시스템 확장이 설치되어 있는 경우 Connector 1.14.1 이상에서 이 결함이 발생할 수 있습니다.컴퓨터를 재부팅해도 결함이 제거되지 않는 경우 자세한 내용은 아래의 결함 13 지침을 참조하십시오
12	네트워크 필터가 허용되지 않음	네트워크 필터가 허용되지 않음	네트워크 필터는 정책의 'Enable Device Flow Correlation' 기능에 필요합니다.이 함을 지우려면 'AMP for Endpoints Service'가 엔드포인트에서 네트워크 콘텐츠 터링하도록 허용합니다. Agent(에이전트) 메뉴에 나열된 활성 fault를 클릭하고 제공된 지침에 따라 네트 필터를 허용하도록 macOS 대화 상자를 액세스할 수 있습니다. 네트워크 필터의 원격 권한 부여를 위한 MDM 프로필 설정을 비롯한 추가 세부 는 이 기술 노트.
13	네트워크 콘텐츠	네트워크 콘텐츠 필터 시스템 확장	Mac Connector 1.14.0의 경우 네트워크 콘텐츠 필터 시스템 확장을 시작할 때 macOS 버그로 인해 이 결함이 자주 발생합니다.컴퓨터를 재부팅하면 이 결함이 워집니다.

	필터 시스템 확장이 너무 많습니다.	이 너무 많습니다.	정책의 'Enable Device Flow Correlation' 기능을 사용하려면 방화벽 등급 macO 트워크 콘텐츠 필터를 사용해야 합니다.MacOS 실행할 수 있는 네트워크 콘텐츠 터 수를 제한합니다. 이 결함이 제기되고 컴퓨터를 재부팅하여 제거되지 않은 경우를 눌러 더 이상 필 지 않은 방화벽 등급 네트워크 콘텐츠 필터를 제거하고 커넥터를 다시 시작합니
14	엔드포인트 보안 시스템 확장이 너무 많습니다.	엔드포인트 보안 시스템 확장이 너무 많습니다.	MacOS는 실행 가능한 엔드포인트 보안 시스템 확장 수를 제한합니다.Mac Connector에는 정책에서 '파일 복사 및 이동 모니터링' 및 '프로세스 실행 모니터 기능을 위한 이러한 엔드포인트 보안 시스템 확장 중 하나가 필요합니다. 이 오류를 지우려면 더 이상 필요하지 않은 엔드포인트 보안 시스템 확장을 제거 커넥터를 다시 시작하십시오.
15	시스템 확장에 전체 디스크 액세스 필요	시스템 확장에 전체 디스크 액세스 필요	Mac Connector의 macOS System Extensions가 스캔을 위해 사용자 파일에 액 할 수 없습니다.Security & Privacy System Preferences(보안 및 개인 정보 보호 템 기본 설정)를 열고 *AMP Security Extension(AMP 보안 확장)에* 대한 전체 디 액세스 권한을 *부여합니다*. 시스템 확장이 포함된 전체 디스크 액세스의 원격 권한 부여를 위한 MDM 프로 정을 포함한 추가 세부 정보는 이 기술 참고에서 확인할 수 있습니다. macOS 11.0.0의 버그로 인해 전체 디스크 액세스 설정이 부여된 후 다시 부팅할 즉시 지워질 수 있습니다. 이 버그는 macOS 11.0.1에서 수정되었습니다.
17	궤도 전체 디스크 액세스가 허용되지 않음	궤도 전체 디스크 액세스가 허용되지 않음	Orbeability는 쿼리를 위해 보호된 파일 및 디렉토리에 액세스하기 위한 전체 디 액세스를 필요로 합니다.Security & Privacy System Preferences(보안 및 개인 보호 시스템 기본 설정)를 열고 *Cisco Orbeability*(*Cisco Orbeability)에* 대한 전체 스크 액세스 권한을 *부여합니다*.