# SUSE Linux 보안 엔드포인트에서 결함 ID 11 문제 해결

## 목차



## 소개

이 문서에서는 해결 프로세스에 대해 설명합니다. Fault ID 11/1 Secure Endpoint on SUSE Linux Enterprise 15 SP2 .

### 요구 사항

명령줄 인터페이스(CLI일부 명령의 가용성은 정책 컨피그레이션 및/또는 루트 권한에 따라 달라지지만, 시스템의 모든 사용자가 사용할 수 있습니다. 이에 종속된 명령은 이 기사 전반에 걸쳐 개시되어 있다.

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Linux Command Line
- Secure Endpoint

### 사용되는 구성 요소

문서에서 사용되는 정보는 다음 소프트웨어 버전을 기반으로 합니다.

- Secure Endpoint 1.20
- SUSE Linux Enterprise 15 SP2 커널 버전 5.3.18-24.96-default

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

## 배경 정보

On SUSE Linux Enterprise 15 Service Pack (SP) 2, 커널 버전이 5.3.18 이상인 경우 커넥터 사용 eBPF 실시간 파일 시스템 및 네트워크 모니터링용 모듈 이 eBPF Linux를 대체하는 모듈 Kernel 실행할 때 사용되는 모듈 RHEL 6, RHEL 7, Oracle Linux 7 RHCK, Oracle Linux 7 UEK 5 및 이전 버전에서는 Amazon Linux 2 kernel 4.14

이전. 대상 Ubuntu 18.04 이상 Debian 10세 이상 eBPF 모듈은 기본입니다.

적절한 호환성을 위해 커넥터는 eBPF 시스템에서 커넥터가 로드되고 실행되기 전에 커넥터에서 사용하는 모듈입니다. 이 컴파일을 사용하려면 현재에 해당하는 커널 개발 헤더 파일이 필요합니다 kernel-devel 을(를) 설치합니다. 실시간 filesystem 네트워크 모니터링이 활성화되면 커넥터는 eBPF 모듈은 커넥터가 시작될 때마다 또는 정책 업데이트의 일환으로 이러한 기능이 활성화될 때 실시간으로 실행됩니다.

시스템이 현재 커널 레벨 패키지를 놓치면 커넥터가 Fault ID 11(실시간 네트워크 및 파일 모니터링을 사용할 수 없음)을 제기합니다. 현재 실행 중인 커널에 대한 커널 레벨 패키지를 설치한 다음 Connector를 다시 시작합니다. 이 결함의 문제는 Linux 커넥터가 성능이 저하된 상태로 실행된다는 것입니다. 즉, 결함이 해결될 때까지 정상적으로 작동하지 않습니다.

# 문제 해결

결함 11이 제기되면 다음 오류 로그가 나타납니다.

- 시스템 로그에서 로그 줄 찾기 /var/log/messages 다음과 같은 특징이 있습니다.

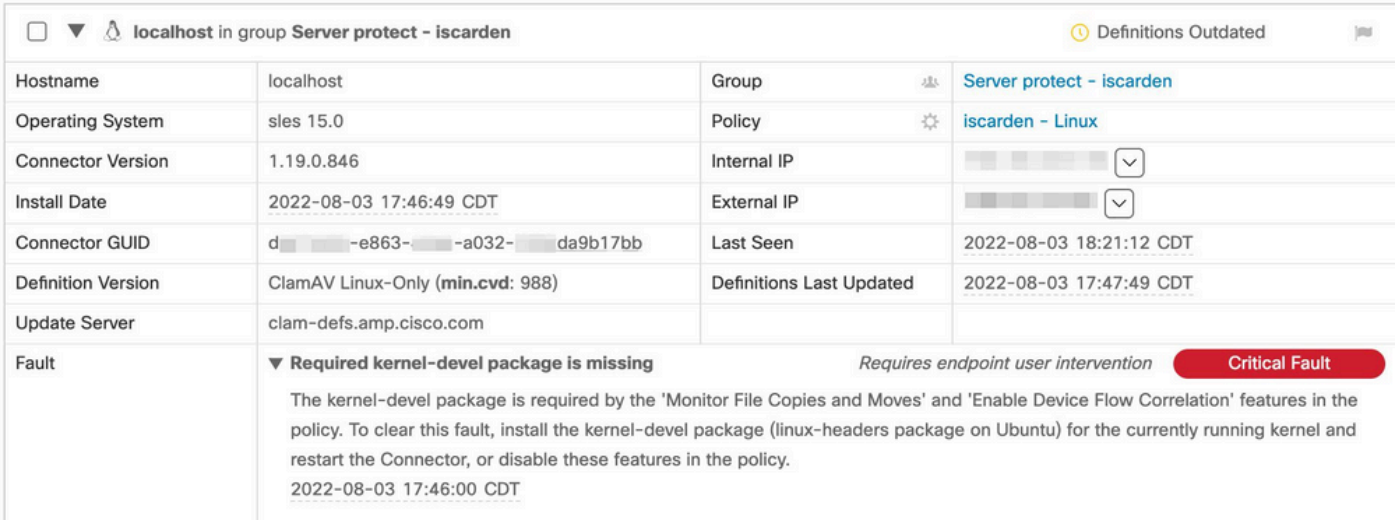
init: cisco-amp pre-start: AMP kernel modules are not required on this kernel version '5.3.18-24.96-default'; skipping reinstalling kernel modules
이 로그는 컴퓨터의 현재 커널 버전이 다음에 대한 커널 모듈을 사용하지 않음을 나타냅니다 filesystem 네트워크 모니터링이 포함됩니다. 4.18보다 크거나 같은 커널 버전에서 filesystem 네트워크를 모니터링하려면 eBPF 모듈.

## 없는 커널 헤더를 식별하는 방법

커널 헤더가 없는 컴퓨터에서 커넥터가 실행되면 Fault ID 11 (Realtime network and file monitoring is unavailable), 커넥터는 성능 저하 상태에서 filesystem 네트워크 모니터링도 가능합니다.
이러한 단계들은 커넥터가 있는지를 식별하기 위해 터미널 윈도우로부터 수행될 수 있다 kernel-header 이(가) 있거나 없습니다.

1단계. 영향을 받는 디바이스에서 커넥터가 Fault ID 11 :

# /opt/cisco/amp/bin/ampcli # status [logger] Set minimum reported log level to notice Trying to connect... Connected. Status: Connected Mode: Degraded Scan: Ready for scan Last Scan: 2022-08-03 06:31:42 PM Policy: iscarden - Linux (#22192) Command-line: Enabled Orbital: Disabled Faults: 1 Critical Fault IDs: 11 ID 11 - Critical: Realtime network and file monitoring is unavailable. Install the kernel-devel package for the currently running kernel, then, restart the Connector.
Secure Endpoint(보안 엔드포인트) 콘솔에서 영향을 받는 디바이스를 찾고 세부 정보를 확장하여 Fault(결함) 섹션을 확인합니다.




2단계. 다음 명령을 사용하여 현재 커널을 확인합니다.

$ uname -r 5.3.18-150200.24.115-default

3단계. 커널 헤더의 설치 여부를 확인하려면 다음을 수행합니다.

# zypper se -s kernel-default-devel | grep $(uname -r | sed "s/-default//") # zypper se -s kernel-devel | grep $(uname -r | sed "s/-default//")

출력은 다음과 같아야 합니다.

```
isaac@localhost:~> zypper se -s kernel-default-devel | grep $(uname -r | sed "s/-default//")
i+ | kernel-default-devel | package | 5.3.18-24.96.1   | x86_64 | SLE-Module-Basesystem15-SP2-Updates
```

여기서 i+는 패키지가 설치되었음을 나타냅니다. 왼쪽 열이 v 또는 **비어** 있는 경우 패키지를 설치해야 합니다.

이 SUSE 컴퓨터는 커널 헤더를 설치하는 데 적합하며 다음 사항이 모두 참인 경우

- 커넥터에 Fault ID 11이 있습니다.
- 최소 kernel 버전은 5.3.18입니다.
- 이 kernel 헤더가 설치되지 않았습니다.

# 해결

이 SUSE 시스템에 필요한 커널 헤더가 없으면 이 절차를 사용하여 시스템에 필요한 커널 헤더를 설치할 수 있습니다.

1단계. 필요한 커널 헤더를 설치합니다.

# sudo zypper install --oldpackage kernel-default-devel=$(uname -r | sed 's/-default//') # sudo zypper install --oldpackage kernel-devel=$(uname -r | sed 's/-default//')

2단계. 커넥터를 다시 시작합니다.

# sudo systemctl stop cisco-amp # sudo systemctl start cisco-amp

3단계. 결함이 제거되었는지 확인합니다.

# /opt/cisco/amp/bin/ampcli # status Trying to connect... Connected. ampcli> status Status: Connected Mode: Normal Scan: Ready for scan Last Scan: 2022-08-05 01:29:47 PM Policy: iscarden - Linux (#22201) Command-line: Enabled Orbital: Disabled Faults: None ampcli > quit

# 다음을 확인합니다.

커널 헤더가 현재 설치되어 있는지 확인하려면 다음 명령을 실행합니다.

# zypper se -s kernel-default-devel | grep $(uname -r | sed "s/-default//") # zypper se -s kernel-devel | grep $(uname -r | sed "s/-default//")

해결 방법을 수행하기 전에 다음과 유사한 출력이 표시되었습니다.

```
isaac@localhost:~> zypper se -s kernel-default-devel | grep $(uname -r | sed 's/
-default//') $ zypper se -s kernel-devel | grep $(uname -r | sed 's/-default//')
isaac@localhost:~>
```

해결 방법을 수행한 후 출력은 다음과 유사해야 합니다.

```
isaac@localhost:~> zypper se -s kernel-default-devel | grep $(uname -r | sed "s/-default//")
i+ | kernel-default-devel | package | 5.3.18-24.96.1   | x86_64 | SLE-Module-Basesystem15-SP2-Updates
isaac@localhost:~> zypper se -s kernel-devel | grep $(uname -r | sed "s/-default//")
i | kernel-devel | package | 5.3.18-24.96.1   | noarch | SLE-Module-Basesystem15-SP2-Updates
isaac@localhost:~>
```

# 관련 정보

- 보안 엔드포인트 Linux 커넥터 OS 호환성 확인
- Linux 커널 레벨 결함
- Cisco Secure Endpoint Linux Connector 커널 모듈 구축

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.