Cisco Secure Endpoint Linux Connector Kernel Module 구축

목차

소개

이 문서에서는 Cisco Secure Endpoint Linux 커넥터의 파일 시스템 및 네트워크 모니터링에 필요한 사전 컴파일된 커널 모듈을 현재 실행 중인 시스템 커널에서 사용할 수 없는 시기 및 파일 시스템 및 네트워크 모니터링이 작동하도록 커널 모듈을 수동으로 컴파일하는 절차를 식별하는 방법에 대해 설명합니다.

이 문서에서 "지원되지 않는 커널"은 Linux 커넥터에서 지원하는 커널 버전이지만 커널 버전에 필요한 특정 미리 컴파일된 커널 모듈은 커넥터 설치 패키지에 포함되지 않으므로 수동으로 컴파일해야 합니다. 이는 Amazon Linux 2와 같은 롤링 릴리스 업데이트를 사용하는 운영 체제에서 실행되는 지정된 Linux 커넥터 릴리스의 경우일 수 있습니다.

모든 Linux 배포판 및 커널 버전이 컴파일된 커널 모듈을 실행하는 것은 지원하지 않습니다. 이 문서는 커널 모듈을 수동으로 컴파일할 때 사용할 수 있는 시기를 파악하는 데 도움이 됩니다.

사전 요구 사항

요구 사항

- RHEL 기반 시스템의 경우 배포 제공 gcc가 설치되어 있습니다. 현재 실행 중인 커널에 대해 kernel-devel이 설치되었습니다.
- UEK(Unbreakable Enterprise Kernel)을 사용하는 시스템의 경우 배포 제공 gcc가 설치됨 현재 실행 중인 커널에 대해 kernel-uek-devel이 설치되었습니다.

적용 가능성

운영 체제

- RHEL/CentOS 7
- Oracle Linux 7 RHCK(Red Hat Compatible Kernel)
- Oracle Linux 7 UEK 5 이하

- Amazon Linux 2

커널 버전

- 네트워크 모니터링 커널 모듈은 커널 버전 2.6~4.14에 대해 컴파일할 수 있습니다.
- 파일 시스템 모니터링 커널 모듈은 커널 버전 3.10~4.14에 대해 컴파일할 수 있습니다.

참고:

- 커널 버전 2.6에서 3.10까지 연결되면 커넥터는 사용자 지정 컴파일에 적용되지 않는 파일 시스템 모니터링에 redirfs(out-of-tree 커널 모듈)를 사용합니다.
- 4.14에서 4.19 사이의 커널 버전은 커넥터와 호환되지 않으며 사용자 지정 컴파일에도 적용되지 않습니다.
- 커널 버전 4.19 이상의 경우 커넥터는 파일 시스템 및 네트워크 모니터링에 eBPF 모듈을 사용합니다. 해당 커널 버전에서 이 결함을 해결하는 방법에 대한 자세한 내용은 Linux Kernel-Devel Fault 문서를 참조하십시오.

커넥터 버전

- 1.16.0 이상
- 사용자 지정 UEK 커널 모듈 생성을 위한 1.18.0 이상

커넥터가 지원되지 않는 커널이 있는 컴퓨터에서 실행 중인 경우 결함 8(실시간 파일 시스템 모니터 시작 실패) 및 결함 9(실시간 네트워크 모니터 시작 실패)가 제기되며 커넥터는 파일 시스템이나 네트워크 모니터링 없이 성능 저하 상태로 실행됩니다.

커넥터가 지원되지 않는 커널에서 실행 중인지 확인하기 위해 터미널 창에서 다음 단계를 수행할 수 있습니다.

1. 커넥터에 결함 8 및/또는 결함 9가 있는지 확인합니다.

   ```
   $ /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: none Policy: unsupported kernel example (#7607) Command-line: Enabled Faults: 2 Critical Fault IDs: 8, 9 ID 8 - Critical: Realtime filesystem monitor failed to start. ID 9 - Critical: Realtime network monitor failed to start.
   ```
2. 현재 실행 중인 커널이 2.6에서 4.14 사이이고 포함되며 미리 컴파일된 커널 모듈 버전과 일치하지 않는지 확인합니다.
   다음 명령은 현재 실행 중인 커널 버전을 표시합니다.

   ```
   $ uname -r 4.14.97-90.72.amzn2.x86_64
   ```
   커넥터와 함께 패키지로 제공되는 미리 컴파일된 커널 모듈 버전은 다음 명령을 사용하여 나열됩니다.
3.
   ```
   $ ls /opt/cisco/amp/bin/modules/ 4.14.186-146.268.amzn2.x86_64 4.14.198-152.320.amzn2.x86_64 4.14.209-160.335.amzn2.x86_64 4.14.219-161.340.amzn2.x86_64 4.14.225-169.362.amzn2.x86_64 4.14.192-147.314.amzn2.x86_64 4.14.200-155.322.amzn2.x86_64 4.14.209-160.339.amzn2.x86_64 4.14.219-164.354.amzn2.x86_64 4.14.231-173.360.amzn2.x86_64 4.14.193-
   ```

```
149.317.amzn2.x86_64 4.14.203-156.332.amzn2.x86_64 4.14.214-160.339.amzn2.x86_64 4.14.225-168.357.amzn2.x86_64 4.14.231-173.361.amzn2.x86_64
```

위 예에서 커널 버전 4.14.97-90.72.amzn2.x86_64은 사용 가능한 커널 모듈 목록에 포함되지 않습니다.

다음 사항이 모두 참인 경우 Linux 커넥터는 맞춤형 커널 모듈을 컴파일하는 데 적합합니다.

- 커넥터에는 결함 8 및/또는 9이 제기됩니다.
- 현재 커널 버전은 2.6에서 4.14 사이이며 포함적입니다.
- 현재 커널 버전은 미리 컴파일된 커널 모듈 `/opt/cisco/amp/bin/module` 목록에 포함되지 않습니다.

해결

Linux 커넥터가 지원되지 않는 커널에서 실행 중인 경우 다음 절차를 사용하여 시스템에 대한 사용자 지정 커널 모듈을 컴파일할 수 있습니다.

1. 필요한 시스템 종속성 설치:

   ```
   $ yum install gcc
   ```

   `gcc`는 특정 옵션으로 커널 모듈을 컴파일하려면 필요합니다.RHEL 기반 커널을 사용하는 시스템에서 다음 명령을 사용하여 필요한 커널 패키지를 설치합니다.

   ```
   $ yum install kernel-devel-$(uname -r)
   ```

   UEK를 사용하는 시스템에서 다음 명령을 사용하여 필요한 커널 패키지를 설치합니다.

   ```
   $ yum install kernel-uek-devel-$(uname -r)
   ```

   시스템에 따라 현재 실행 중인 커널에 대한 커널 모듈을 컴파일하려면 `kernel-devel-$(uname -r)  kernel-uek-devel-$(uname -r)`이 필요합니다.
2. 루트 권한이 있는 compile_kmods.sh 스크립트를 실행합니다.

   ```
   $ sudo /opt/cisco/amp/bin/compile_kmods.sh
   ```

   compile_kmods.sh 스크립트는 현재 실행 중인 커널 버전에 대한 파일 시스템 및 네트워킹 모니터링 커널 모듈을 컴파일하려고 시도합니다. 사용자 지정 커널 모듈은 `/opt/cisco/amp/extras/modules` 디렉터리에 저장할 수 있습니다. 실행이 끝나면 스크립트는 새로 컴파일된 커널 모듈을 시스템에 로드할 수 있도록 커넥터를 자동으로 다시 시작합니다.
3. 결함 8 및 9가 지워졌는지 확인합니다.

   ```
   $ /opt/cisco/amp/bin/ampcli status [logger] Set minimum reported log level to notice Trying to connect... Connected. Status: Connected Mode: Normal Scan: Ready for scan Last Scan: 2021-06-14 05:53 PM Policy: unsupported kernel example (#7607) Command-line: Enabled Faults: None
   ```

추가 명령

compile_kmods.sh 실행 파일은 Secure Endpoint Linux 커넥터 버전 1.16.0 이상에서 사용할 수 있으며 호환 OS 배포에 자동으로 설치됩니다. compile_kmods.sh 실행 파일은 UEK의 사용자 지정 컴파일을 지원하도록 Secure Endpoint Linux 커넥터 버전 1.18.0 이상에서 개선되었습니다.

네트워크 모니터링을 위한 사용자 지정 컴파일 커널 모듈은 커널 버전 2.6~4.14에서 지원되지만, 커널 버전 3.10~4.14에서는 파일 시스템 모니터링을 위한 사용자 지정 컴파일 커널 모듈이 지원됩니다.

사용 가능한 명령

참고: compile_kmods.sh 실행 파일은 루트 특권 집합과 함께 실행해야 합니다.

- `-h/—help` 옵션은 사용 가능한 옵션의 전체 목록을 표시합니다.

```
$ /opt/cisco/amp/bin/compile_kmods.sh --help Usage: compile_kmods [OPTIONS] OPTIONS: -f, --force force overwriting compiled kmod -h, --help show help
```

- `-f/ - force` 옵션을 사용하여 현재 실행 중인 커널에 대해 이전에 컴파일된 사용자 지정 커널 모듈을 덮어쓸 수 있습니다. 이 기능은 현재 사용자 지정 커널 모듈이 이전 버전의 커넥터로 빌드된 경우 사용해야 하며 업데이트된 버전의 커넥터로 다시 컴파일해야 합니다. 커넥터 업데이트 프로세스는 고객 커널 모듈을 업데이트의 일부로 재컴파일하지 않습니다.

문제 해결

장애 발생 8 및/또는 9가 여전히 *해결* 다음 단계를 수행하여 문제를 자세히 조사할 수 있습니다.

- 시스템 로그`/var/log/messages`에서 다음과 유사한 로그 라인을 찾습니다. 다음 로그는 컴퓨터에서 현재 실행 중인 커널 버전이 파일 시스템 및 네트워크 모니터링에 커널 모듈을 사용하지 않는다고 설명합니다. 4.18보다 크거나 같은 커널 버전에서 eBPF 모듈을 사용하여 파일 시스템 및 네트워크를 모니터링합니다.

```
init: cisco-amp pre-start: AMP kernel modules are not required on this kernel version '5.4.117-58.216.amzn2.x86_64'; skipping reinstalling kernel modules
```

다음 로그는 미리 컴파일된 커널 모듈 디렉토리에 커널 버전이 없다는 것을 나타냅니다. `/opt/cisco/amp/bin/modules`, 현재 실행 중인 커널 버전과 호환됩니다.

```
init: cisco-amp pre-start: finding compatible kernel modules in /opt/cisco/amp/bin/modules to install init: cisco-amp pre-start: failed to find kernel versions init: cisco-amp pre-start: failed to install and load all required kernel modules in /opt/cisco/amp/bin/modules, continuing without some modules loaded
```

다음 로그는 사용자 지정 컴파일된 커널 모듈 디렉토리에 커널 버전이 없다는 것을 나타냅니다. `/opt/cisco/amp/extra/modules`, 현재 실행 중인 커널 버전과 호환됩니다.

```
init: cisco-amp pre-start: finding compatible kernel modules in /opt/cisco/amp/extra/modules to install init: cisco-amp pre-start: failed to find kernel versions init: cisco-amp pre-start: failed to install and load all required kernel modules in /opt/cisco/amp/extra/modules, continuing without some modules loaded
```

- Secure Endpoint Linux 커넥터 파일 시스템 및 네트워크 모니터링 커널 모듈이 로드되었는지 확인합니다.

```
$ lsmod | grep ampfsm ampfsm 24576 0
```

```
$ lsmod | grep ampnetworkflow ampnetworkflow 65536 0
```

- 사용 가능한 경우 Secure Endpoint Linux 커넥터를 최신 버전으로 업그레이드합니다.