Building Cisco Secure Endpoint Linux Connector Kernel Modules

Contents

Introduction

This article explains how to identify when precompiled kernel modules required for the Cisco Secure Endpoint Linux connector's filesystem and network monitoring are not available for the currently running system kernel, and the procedure for manually compiling kernel modules so that filesystem and network monitoring will be operational.

For the purpose of this article, an "unsupported kernel" is a kernel version that is supported by the Linux connector but the specific precompiled kernel modules required for the kernel version are not included in the connector install package and therefore have to be manually compiled. This can be the case for a given Linux connector release running on an operating system that uses a rolling release update, such as Amazon Linux 2.

Not all Linux distributions and kernel version support running compiled kernel modules. This article will assist in identifing when manually compiling kernel modules can be used.

Prerequisites

Requirements

- For RHEL based systems, distribution-provided gcc installed; kernel-devel installed for currently running kernel.
- For systems using an Unbreakable Enterprise Kernel (UEK), distribution-provided gcc installed; kernel-uek-devel installed for currently running kernel.

Applicability

Operating System

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

- Oracle Linux 7 UEK 5 and earlier
- Amazon Linux 2

Kernel Versions

- The network monitoring kernel module can be compiled for kernel versions 2.6 through 4.14 inclusive.
- The filesystem monitoring kernel module can be compiled for kernel versions 3.10 through 4.14 inclusive.

NOTES:

- On kernel versions 2.6 up until 3.10, the connector uses redirfs (an out-of-tree kernel module) for filesystem monitoring which is not applicable for custom compiling.
- Kernel versions between 4.14 and 4.19 are not compatible with the connector and are also not applicable for custom compiling.
- For kernel versions 4.19 and newer, the connector uses eBPF modules for filesystem and network monitoring. Refer to the Linux Kernel-Devel Fault article for details on resolving this fault on those kernel versions.

Connector Versions

- 1.16.0 and newer
- 1.18.0 and newer for creating custom UEK kernel modules

Diagnosing an Unsupported Kernel

When the connector is running on a computer with an unsupported kernel, fault 8 (Realtime filesystem monitor failed to start) and fault 9 (Realtime network monitor failed to start) will be raised and the connector will run in a degraded state without filesystem or network monitoring.

The following steps can be performed from a terminal window in order to identify whether the connector is running on an unsupported kernel:

1. Verify that the connector has fault 8 and/or fault 9 raised:

   ```
   $ /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. Check that the current running kernel is between 2.6 and 4.14, inclusively, and that it does not match any of the precompiled kernel module versions.
   The following command displays the current running kernel version:

   ```
   $ uname -r 4.14.97-90.72.amzn2.x86_64
   ```
   The available precompiled kernel module versions packaged with the connector are listed using the following command:
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
```

In the above example, kernel version 4.14.97-90.72.amzn2.x86_64 is not included in the list of available kernel modules.

The Linux connector is suitable for compiling custom kernel modules if all of the following are true:

- The connector has fault(s) 8 and/or 9 raised.
- The current kernel version is between 2.6 and 4.14, inclusively.
- The current kernel version is not included in the list of precompiled kernel modules `/opt/cisco/amp/bin/modules`

Resolution

If a Linux connector is running on an unsupported kernel, then the following procedure can be used to compile custom kernel modules for the system:

1. Install required system dependencies:

   ```
   $ yum install gcc
   ```

   `gcc` is required in order to compile the kernel modules with specific options.On systems using a RHEL based kernel, use the following command to install the required kernel package:

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

   On systems using UEK, use the following command to install the required kernel package:
   `$ yum install kernel-uek-devel-$(uname -r)`
   Depending on your system,`kernel-devel-$(uname -r)` or`kernel-uek-devel-$(uname -r)`is required in order to compile the kernel modules for the current running kernel.
2. Run the compile_kmods.sh script with root priviledges:
   `$ sudo /opt/cisco/amp/bin/compile_kmods.sh`
   The compile_kmods.sh script will attempt to compile filesystem and networking monitoring kernel modules for the current running kernel version. The custom kernel modules will be created under the `/opt/cisco/amp/extras/modules` directory. At the end of execution, the script will restart the connector automatically so that the newly compiled kernel modules can be loaded on the system.
3. Confirm that faults 8 and 9 have been cleared:

   ```
   $ /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
   ```

More Commands

The compile_kmods.sh executable is available in Secure Endpoint Linux connector versions 1.16.0 and newer, and it is installed automatically on compatible OS distributions. The compile_kmods.sh executable was improved in Secure Endpoint Linux connector version 1.18.0

and newer to support the custom compilation of UEKs.

Custom compiling kernel modules for network monitoring is supported on kernel versions 2.6 through 4.14, while custom compiling kernel modules for filesystem monitoring is supported on kernel versions 3.10 through 4.14.

Available Commands

NOTE: the compile_kmods.sh executable must be run with root priviledges.

- The `-h/--help` option displays the full list of available options:

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

- The `-f/--force` option can be used to force a previously compiled custom kernel module for the currently running kernel to be overwritten. This should be used when the current custom kernel module was built with an older version of the connector and needs to be re-compiled with an updated version of the connector. The connector update process does not recompile customer kernel modules as part of the update.

Troubleshooting

If fault(s) 8 and/or 9 are still raised after the *Resolution* steps are followed, then the following steps can be performed to further investigate the issue:

- Look for log lines in the system log `/var/log/messages` that are similar to the following: The following log states that the current running kernel version on the computer does not use kernel modules for filesystem and network monitoring. On kernel versions greater than or equal to 4.18, the filesystem and network are monitored using eBPF modules.

```
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
```

  The following log states that there are no kernel versions found in the precompiled kernel modules directory, `/opt/cisco/amp/bin/modules`, that are compatible with the current running kernel version:

```
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
```

  The following log states that there are no kernel versions found in the custom compiled kernel modules directory, `/opt/cisco/amp/extra/modules`, that are compatible with the current running kernel version:

```
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
```

- Check if Secure Endpoint Linux connector filesystem and network monitoring kernel modules are loaded:

```
$ lsmod | grep ampfsm ampfsm 24576 0

$ lsmod | grep ampnetworkflow ampnetworkflow 65536 0
```

- Upgrade the Secure Endpoint Linux connector to a newer version, if available.