构建思科安全终端Linux连接器内核模块

目录

简介

本文说明如何确定当前运行的系统内核无法使用思科安全终端Linux连接器的文件系统和网络监控所需的预编译内核模块，以及手动编译内核模块以使文件系统和网络监控可运行的过程。

在本文中，“不支持的内核”是Linux连接器支持的内核版本，但内核版本所需的特定预编译内核模块不包括在连接器安装软件包中，因此必须手动编译。在使用滚动版本更新（例如Amazon Linux 2）的操作系统上运行的给定Linux连接器版本可能会出现这种情况。

并非所有Linux发行版和内核版本都支持运行编译的内核模块。本文将帮助识别在手动编译内核模块时可以使用的功能。

先决条件

要求

- 对于基于RHEL的系统，安装分布式提供的gcc;为当前运行的内核安装的内核级。
- 对于使用Unbreakable Enterprise Kernel(UEK)的系统，安装分布式提供的gcc;为当前运行的内核安装的kernel-uek-devel。

适用性

操作系统

- RHEL/CentOS 7
- Oracle Linux 7 Red Hat兼容内核(RHCK)
- Oracle Linux 7 UEK 5及更低版本
- Amazon Linux 2

内核版本

- 网络监控内核模块可针对内核版本2.6到4.14（含4.14）进行编译。

- 文件系统监控内核模块可针对内核版本3.10到4.14（含4.14）进行编译。

注意：

- 在内核版本2.6至3.10中，连接器使用redirfs（树外内核模块）进行文件系统监控，但不适用于自定义编译。
- 4.14和4.19之间的内核版本与连接器不兼容，也不适用于自定义编译。
- 对于4.19及更高版本的内核，连接器使用eBPF模块进行文件系统和网络监控。有关解决这些内核版本上的此故障的详细信息，请参阅Linux内核级故障文章。

连接器版本

- 1.16.0及更高版本
- 1.18.0及更高版本，用于创建自定义UEK内核模块

当连接器在具有不受支持内核的计算机上运行时，将引发故障8（实时文件系统监视器无法启动）和故障9（实时网络监视器无法启动），并且连接器将在没有文件系统或网络监视的情况下以降级状态运行。

可以从终端窗口执行以下步骤，以确定连接器是否在不受支持的内核上运行：

1. 验证连接器是否出现故障8和/或故障9:

```
$ /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. 检查当前运行的内核是否介于2.6和4.14之间（含2.6和4.14），以及它是否与任何预编译的内核模块版本都不匹配。
   以下命令显示当前运行的内核版本：

```
$ uname -r 4.14.97-90.72.amzn2.x86_64
```

   使用以下命令列出与连接器打包的可用预编译内核模块版本：

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
```

   在上例中，可用内核模块列表中未包含内核版本4.14.97-90.72.amzn2.x86_64。

如果以下所有情况均属实，则Linux连接器适于编译自定义内核模块：

- 连接器出现8和/或9故障。
- 当前内核版本介于2.6和4.14之间（含2.6和4.14）。
- 预编译的内核模块/opt/cisco/amp/bin/modules列表中不

分辨率

如果Linux连接器在不受支持的内核上运行，则可以使用以下过程为系统编译自定义内核模块：

1. 安装所需的系统依赖项：

   ```
   $ yum install gcc
   ```

   gcc在使用基于RHEL的内核的系统上，使用以下命令安装所需的内核包：

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

   在使用UEK的系统上，使用以下命令安装所需的内核包：

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

   根据您的系统，`kernel-devel-$(uname -r)`或kernel-uek-devel-$(uname -r)是编译当前运行内核的内核模块所必需的。
2. 运行具有根权限的compile_kmods.sh脚本：

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

   compile_kmods.sh脚本将尝试为当前运行的内核版本编译文件系统和网络监控内核模块。自定义内核模块将在 `/opt/cisco/amp/extras/modules` 的双曲余切值。在执行结束时，脚本将自动重新启动连接器，以便新编译的内核模块可以加载到系统上。
3. 确认故障8和9已清除：

   ```
   $ /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
   ```

更多命令

compile_kmods.sh可执行文件在安全终端Linux连接器版本1.16.0及更高版本中可用，并自动安装在兼容的OS发行版中。在安全终端Linux连接器版本1.18.0及更高版本中，compile_kmods.sh可执行文件得到了改进，以支持UEK的自定义编译。

内核版本2.6到4.14支持用于网络监控的自定义编译内核模块，而内核版本3.10到4.14支持用于文件系统监控的自定义编译内核模块。

可用命令

NOTE:compile_kmods.sh可执行文件必须使用根权限运行。

- `-h/–help`选项显示可用选项的完整列表：

  ```
  $ /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`项可用于强制覆盖以前编译的当前运行内核的自定义内核模块。当当前自定义内核模块使用较旧版本的连接器构建，并且需要使用更新版本的连接器重新编译时，应使用此模块。连接器更新过程不会在更新过程中重新编译客户内核模块。

故障排除

如果故障8和/或9仍在 *分辨率* 然后执行以下步骤以进一步调查问题：

- 在系统日志/var/log/`messages`以下内容类似的日志行： 以下日志表明计算机上当前运行的内核版本不使用内核模块进行文件系统和网络监控。在大于或等于4.18的内核版本上，使用eBPF模块监控文件系统和网络。

  ```
  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
  ```

  以下日志表明在预编译的内核模块目录中找不到内核版本， `/opt/cisco/amp/bin/modules`，与当前运行的内核版本兼容：

  ```
  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
  ```

  以下日志表明在自定义编译的内核模块目录中找不到内核版本，
  `/opt/cisco/amp/extra/modules`，与当前运行的内核版本兼容：

  ```
  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
  ```

- 检查是否加载了安全终端Linux连接器文件系统和网络监控内核模块：

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

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

- 将Secure Endpoint Linux连接器升级到更新版本（如果可用）。