Creación de módulos de núcleo de conector Linux de terminales seguros de Cisco

Contenido

Introducción

Este artículo explica cómo identificar cuando los módulos del núcleo precompilados requeridos para el sistema de archivos del conector de Linux Secure Endpoint de Cisco y el monitoreo de red no están disponibles para el núcleo del sistema que se está ejecutando actualmente, y el procedimiento para compilar manualmente los módulos del núcleo de modo que el sistema de archivos y el monitoreo de red estén operativos.

A los efectos de este artículo, un "kernel no soportado" es una versión del kernel soportada por el conector Linux pero los módulos específicos del kernel precompilado requeridos para la versión del kernel no están incluidos en el paquete de instalación del conector y por lo tanto deben ser compilados manualmente. Este puede ser el caso de una versión de conector Linux dada que se ejecuta en un sistema operativo que utiliza una actualización de versión continua, como Amazon Linux 2.

No todas las distribuciones de Linux y la versión del núcleo soportan la ejecución de módulos del núcleo compilados. Este artículo ayudará a identificar cuando se puedan utilizar módulos del núcleo compilados manualmente.

Prerequisites

Requirements

- Para los sistemas basados en RHEL, se instaló el gcc proporcionado por la distribución; kernel-devel instalado para el kernel que se está ejecutando actualmente.
- Para los sistemas que utilizan un núcleo empresarial irrompible (UEK), se instaló un gcc proporcionado por distribución; kernel-uek-devel instalado para el núcleo que se está ejecutando actualmente.

Aplicabilidad

Sistema operativo

- RHEL/CentOS 7
- Núcleo Compatible con Red Hat de Oracle Linux 7 (RHCK)
- Oracle Linux 7 UEK 5 y versiones anteriores
- Amazon Linux 2

Versiones del núcleo

- El módulo del núcleo de monitoreo de red puede ser compilado para las versiones del kernel 2.6 a 4.14 inclusive.
- El módulo del kernel de monitoreo del sistema de archivos puede ser compilado para las versiones del kernel 3.10 a 4.14 inclusive.

NOTAS:

- En las versiones 2.6 hasta la 3.10 del núcleo, el conector utiliza redirfs (un módulo kernel fuera del árbol) para monitorear el sistema de archivos que no es aplicable para la compilación personalizada.
- Las versiones del núcleo entre 4.14 y 4.19 no son compatibles con el conector y tampoco son aplicables para la compilación personalizada.
- Para las versiones 4.19 y posteriores del kernel, el conector utiliza módulos eBPF para el monitoreo del sistema de archivos y la red. Refiérase al artículo Linux Kernel-Devel Fault para obtener detalles sobre la resolución de este fallo en esas versiones del kernel.

Versiones de conectores

- 1.16.0 y posterior
- 1.18.0 y posterior para crear módulos UEK personalizados

DIAGruido un núcleo no admitido

Cuando el conector se está ejecutando en un equipo con un núcleo no admitido, se provoca el error 8 (el monitor del sistema de archivos en tiempo real no se pudo iniciar) y el error 9 (el monitor de red en tiempo real no se pudo iniciar) y el conector se ejecutará en un estado degradado sin el control del sistema de archivos o de la red.

Los siguientes pasos se pueden realizar desde una ventana de terminal para identificar si el conector se está ejecutando en un núcleo no admitido:

1. Verifique que el conector tenga la falla 8 o la falla 9 provocada:

```
$ /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. Verifique que el núcleo en ejecución actual esté entre 2.6 y 4.14, inclusive, y que no coincida

con ninguna de las versiones precompiladas del módulo del núcleo.
El siguiente comando muestra la versión actual del kernel en ejecución:

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

Las versiones precompiladas disponibles del módulo kernel empaquetadas con el conector se enumeran usando el siguiente comando:

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
```

En el ejemplo anterior, la versión 4.14.97-90.72.amzn2.x86_64 del núcleo no está incluida en la lista de módulos del núcleo disponibles.

El conector Linux es adecuado para compilar módulos kernel personalizados si todo lo siguiente es cierto:

- El conector tiene una(s) falla(s) 8 y/o 9 provocada(s).
- La versión actual del kernel está entre 2.6 y 4.14, inclusive.
- La versión actual del kernel no está incluida en la lista de módulos del kernel precompilados `/opt/cisco/amp/bin/module`

Resolución

Si un conector Linux se ejecuta en un núcleo no admitido, entonces se puede utilizar el siguiente procedimiento para compilar módulos kernel personalizados para el sistema:

1. Instale las dependencias del sistema necesarias:

   ```
   $ yum install gcc
   ```

   `gcc` es necesario para compilar los módulos del kernel con opciones específicas.En los sistemas que utilizan un núcleo basado en RHEL, utilice el siguiente comando para instalar el paquete de kernel necesario:

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

   En sistemas que utilizan UEK, utilice el siguiente comando para instalar el paquete de kernel necesario:
   `$ yum install kernel-uek-devel-$(uname -r)`
   Dependiendo de su sistema, `kernel-devel-$(uname -r) orkernel-uek-devel-$(uname -r)` es necesario para compilar los módulos del núcleo para el núcleo en ejecución actual.
2. Ejecute el script compile_kmods.sh con privilegios de root:
   `$ sudo /opt/cisco/amp/bin/compile_kmods.sh`
   La secuencia de comandos compile_kmods.sh intentará compilar los módulos del núcleo de monitoreo de redes y del sistema de archivos para la versión actual del núcleo en ejecución. Los módulos de kernel personalizados se crearán bajo el `/opt/cisco/amp/extras/modules` directorio. Al final de la ejecución, el script reiniciará el conector automáticamente para que los módulos del núcleo recién compilados puedan cargarse en el sistema.
3. Confirme que se han borrado los errores 8 y 9:

```
$ /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
```

Más comandos

El ejecutable compile_kmods.sh está disponible en las versiones 1.16.0 y posteriores del conector de Linux de terminal seguro, y se instala automáticamente en distribuciones de SO compatibles. El ejecutable compile_kmods.sh fue mejorado en Secure Endpoint Linux Connector versión 1.18.0 y posterior para soportar la compilación personalizada de UEK.

Los módulos de compilación personalizada del núcleo para el monitoreo de red se soportan en las versiones 2.6 a 4.14 del núcleo, mientras que los módulos de compilación personalizada para el monitoreo del sistema de archivos se soportan en las versiones 3.10 a 4.14 del núcleo.

Comandos disponibles

NOTE: el ejecutable compile_kmods.sh se debe ejecutar con privilegios raíz.

- La opción `-h/–help` muestra la lista completa de opciones disponibles:

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

- La opción `-f/–force` se puede utilizar para forzar la sobrescritura de un módulo de kernel personalizado previamente compilado para el núcleo que se ejecuta actualmente. Esto debería usarse cuando el módulo del núcleo personalizado actual se construyó con una versión anterior del conector y necesita ser re-compilado con una versión actualizada del conector. El proceso de actualización del conector no vuelve a compilar los módulos del núcleo del cliente como parte de la actualización.

Resolución de problemas

Si los fallos 8 y/o 9 siguen apareciendo después de *Resolución* se siguen los pasos siguientes y, a continuación, se pueden realizar los siguientes pasos para investigar más a fondo el problema:

- Busque líneas de registro en el log del sistema `/var/log/messages` que sean similares a las siguientes: El siguiente registro indica que la versión actual del kernel en ejecución en el equipo no utiliza módulos kernel para el monitoreo del sistema de archivos y de la red. En las versiones del núcleo mayores o iguales a 4.18, el sistema de archivos y la red se monitorean usando módulos eBPF.

```
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
```

  El siguiente registro indica que no hay versiones del núcleo encontradas en el directorio de módulos del núcleo precompilado, `/opt/cisco/amp/bin/modules`, que son compatibles con la versión actual del kernel en ejecución:

```
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
```

El siguiente registro indica que no hay versiones del kernel encontradas en el directorio de módulos del kernel compilado personalizado, `/opt/cisco/amp/extra/modules`, que son compatibles con la versión actual del kernel en ejecución:

```
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
```

- Verifique si el sistema de archivos del conector Linux Secure Endpoint y los módulos del núcleo de monitoreo de red están cargados:

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

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

- Actualice el conector Secure Endpoint Linux a una versión más reciente, si está disponible.