Falla de Linux Kernel-Devel

Contenido

Overview

En Red Hat Enterprise Linux (RHEL) 8 y variantes, Oracle Linux 8 Red Hat Compatible Kernel (RHCK), Oracle Linux 7 y 8, Unbreakable Enterprise Kernel (UEK) 6, así como Amazon Linux 2 que se ejecuta en un kernel de sistema 4.19 o posterior, el conector Cisco Secure Endpoint Linux no podrá supervisar los movimientos de archivos ni habilitar la correlación de flujo de dispositivos (supervisión de red) cuando el paquete kernel-devel, o paquete kernel-uek-devel en Oracle Linux UEK, no existe para el kernel que se está ejecutando actualmente. El conector generará el ID de falla 11 "Falta el paquete requerido kernel-devel" en esta situación. Para Debian y Ubuntu esta falla puede ser provocada cuando falta el paquete linux-encabezados.

A partir de RHEL 8, Oracle Linux 8 RHCK, Oracle Linux 7 y 8 UEK 6, y Amazon Linux 2 kernel 4.19 o posterior, el conector utilizará módulos eBPF para el sistema de archivos en tiempo real y la supervisión de la red. Los módulos eBPF sustituyen a los módulos del núcleo Linux utilizados cuando se ejecutan en RHEL 6, RHEL 7, Oracle Linux 7 RHCK, Oracle Linux 7 UEK 5 y anteriores, y el núcleo Amazon Linux 2 4.14 o anterior. Para Ubuntu 18.04 y posteriores, así como para Debian 10 y posteriores, los módulos eBPF son nativos.

Para una compatibilidad más amplia, el conector compilará automáticamente los módulos eBPF utilizados por el conector antes de cargarlos y ejecutarlos en el sistema. Esta compilación requiere que se instalen los archivos de encabezado de desarrollo del núcleo correspondientes al núcleo que se está ejecutando actualmente. El conector intentará compilar y cargar los módulos eBPF cada vez que se inicie el conector

Ocasionalmente, este fallo puede aparecer en Oracle Linux con UEK instalado a pesar de que los paquetes kernel-devel están presentes en la máquina. Esto se debe a un fallo durante el proceso de instalación en el que el conector no puede configurar SELinux para aceptar sondas eBPF utilizadas para monitorear la actividad en el terminal.

Aplicabilidad

La falla se generará típicamente después de instalar un nuevo conector Secure Endpoint Linux o después de actualizar el kernel del sistema.

Sistemas operativos

- RHEL/CentOS/Rocky Linux/AlmaLinux 8

- Oracle Linux 8 RHCK
- Oracle Linux 7 y 8 UK 5 y 6
- Ubuntu 18.04 y posterior
- Debian 10 y posteriores
- Amazon Linux 2

Versiones del conector

- Linux 1.13.0 y versiones posteriores

RHEL Linux

El paquete kernel-devel instala los archivos de encabezado de desarrollo del núcleo necesarios en el directorio /usr/src/kernels, organizados según su versión del núcleo.

Causas

Falta el paquete kernel-devel necesario para el sistema de archivos en tiempo real y la supervisión de la actividad de la red.

Resolución

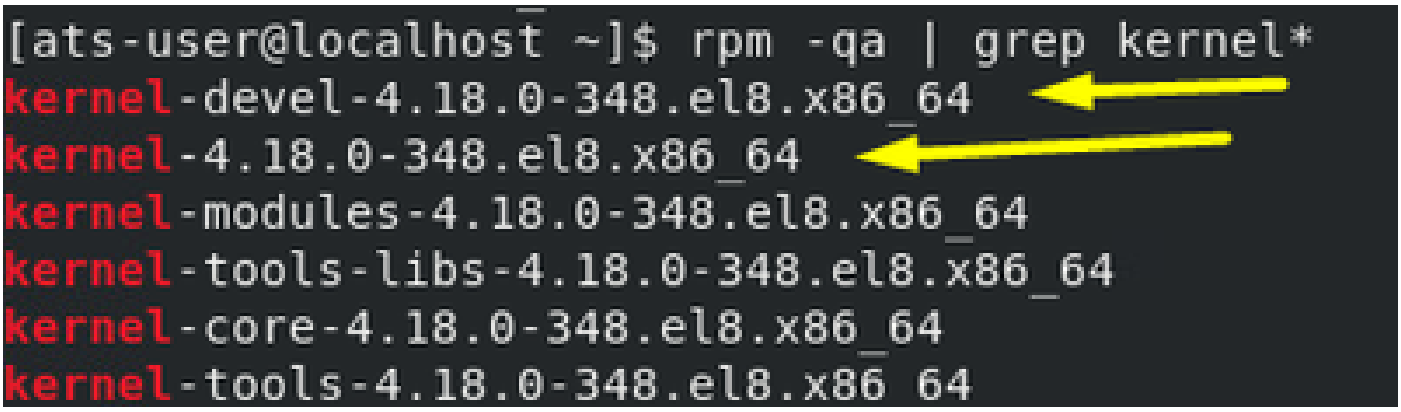
Instale el paquete `kernel-devel` que coincida con el núcleo que se está ejecutando actualmente.

Procedimiento

El paquete 'kernel-devel' debe coincidir con el núcleo que se está ejecutando actualmente. Para verificar si el paquete 'kernel-devel' actual está instalado y/o falta, ejecute lo siguiente:

```
rpm -qa | grep kernel*
```

El siguiente es un ejemplo de salida que ilustra el paquete 'kernel-devel' que coincide con el núcleo que se está ejecutando actualmente.



Para instalar el paquete kernel-devel correspondiente al núcleo que se está ejecutando actualmente, ejecute lo siguiente.

```
dnf install -y kernel-devel-$(uname -r)
```

El conector debe recuperarse y borrar el fallo en un minuto. Si el fallo no se borra en el plazo de un minuto, reinicie manualmente el conector. El fallo debe ser borrado dentro de un minuto después del reinicio.

NOTA: Si el comando anterior falla con un error "No match for argument" (No hay coincidencia para el argumento), es posible que la versión actual del núcleo ya no sea soportada y que el mantenedor del sistema operativo haya eliminado el paquete del repositorio dnf. En este caso, el paquete .rpm necesario para el desarrollo del núcleo se puede descargar manualmente de los archivos del sistema operativo del proveedor y, a continuación, se puede instalar manualmente, o bien el núcleo se puede actualizar a una versión compatible y el comando anterior se puede volver a intentar.

Por ejemplo, si no es posible utilizar CentOS y actualizar el núcleo a una versión compatible con la distribución, los paquetes .rpm antiguos de desarrollo de núcleo para CentOS se pueden descargar manualmente desde http://vault.centos.org. El nombre del archivo que se va a descargar viene dado por la salida del siguiente comando bash.

```
echo kernel-devel-$(uname -r).rpm
```

Una vez descargado, el paquete kernel-devel se puede instalar ejecutando el siguiente comando bash en el directorio donde se guarda el archivo .rpm descargado.

```
dnf install -y kernel-devel-$(uname -r).rpm
```

Oracle Linux

Oracle Linux distribuye con dos alternativas de kernel diferentes, RHCK y UEK. Los paquetes kernel-devel y kernel-uek-devel instalan los archivos de encabezado de desarrollo del núcleo necesarios en el directorio /usr/src/kernels en RHCK y UEK, respectivamente. Los archivos de desarrollo del núcleo están organizados en /usr/src/kernels según su versión del núcleo.

Oracle Linux RHCK

El procedimiento para identificar el paquete de kernel faltante y resolver el ID de falla 11 en Oracle Linux RHCK es idéntico al de RHEL Linux. Consulte la sección anterior de RHEL Linux para obtener más información.

UEK de Oracle Linux

El procedimiento para identificar el paquete de kernel faltante y resolver el ID de falla 11 en Oracle Linux UEK es similar pero no idéntico al de RHEL Linux. Consulte la sección anterior de RHEL Linux para obtener más información, pero reemplace cada instancia de "kernel-devel" por "kernel-uek-devel". Para ser específico, `reemplace kernel-devel-$(uname -r)` con kernel-uek-devel-$(uname -r)para cada comando relevante.

NOTA: Si el paquete kernel-uek-devel .rpm necesario no se puede encontrar al intentar instalar desde el repositorio dnf, el paquete se puede descargar e instalar manualmente desde los archivos de Oracle en https://yum.oracle.com/.

Debian/Ubuntu Linux

El paquete linux-encabezados instala los archivos de encabezado necesarios en el directorio /usr/src, organizados según su versión del núcleo.

Causas

Falta el paquete linux-encabezados requerido para el sistema de archivos en tiempo real y el monitoreo de actividad de la red.

Puede confirmar los encabezados instalados en el directorio /usr/src.

Resolución

El paquete linux-encabezados se puede instalar con el siguiente comando:

```
sudo apt install linux-headers-$(uname -r)
```

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).