

Linux Kernel-Devel Fault

Contents

Overview

On Red Hat Enterprise Linux (RHEL) 8 and variants, Oracle Linux 8 Red Hat Compatible Kernel (RHCK), Oracle Linux 7 and 8, Unbreakable Enterprise Kernel (UEK) 6, as well as Amazon Linux 2 running on a 4.19 or newer system kernel, the Cisco Secure Endpoint Linux connector will not be able to monitor file moves or enable Device Flow Correlation (network monitoring) when the kernel-devel package, or kernel-uek-devel package on Oracle Linux UEK, is missing for the currently running kernel. The connector will raise fault ID 11 "Required kernel-devel package is missing" in this situation. For Debian and Ubuntu this fault may be raised when the linux-headers package is missing.

Starting with RHEL 8, Oracle Linux 8 RHCK, Oracle Linux 7 and 8 UEK 6, and Amazon Linux 2 kernel 4.19 or newer the connector will use eBPF modules for realtime file system and network monitoring. The eBPF modules replace the Linux Kernel Modules used when running on RHEL 6, RHEL 7, Oracle Linux 7 RHCK, Oracle Linux 7 UEK 5 and earlier, and Amazon Linux 2 kernel 4.14 or earlier. For Ubuntu 18.04 and later as well as Debian 10 and later, eBPF modules are native.

For widest compatibility the connector will automatically compile the eBPF modules used by the connector before loading and running them on the system. This compilation requires that kernel development header files corresponding to the currently running kernel be installed. The connector will attempt to compile and load the eBPF modules each time the connector is started

Occasionally, this fault may appear on Oracle Linux with UEK installed despite the kernel-devel packages being present on the machine. This is caused by a fault during the installation process where the connector is unable to configure SELinux to accept eBPF probes used to monitor activity on the endpoint.

Applicability

The fault will typically be raised after a fresh Secure Endpoint Linux connector install or after updating the system kernel.

Operating Systems

- RHEL/CentOS/Rocky Linux/AlmaLinux 8
- Oracle Linux 8 RHCK
- Oracle Linux 7 and 8 UEK 5 and 6
- Ubuntu 18.04 and later
- Debian 10 and later
- Amazon Linux 2

Connector Versions

- Linux 1.13.0 and later

RHEL Linux

The kernel-devel package installs the needed kernel development header files in the /usr/src/kernels directory, organized according to their kernel version.

Causes

The kernel-devel package required for realtime filesystem and network activity monitoring is missing.

Resolution

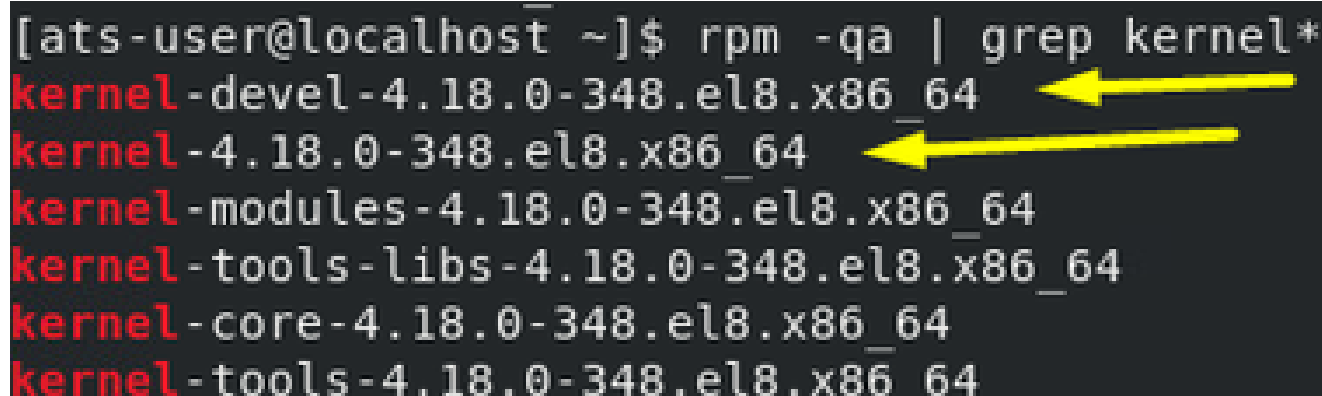
Install the `kernel-devel` package matching the currently running kernel.

Procedure

The 'kernel-devel' package needs to match the currently running kernel. To verify if the current 'kernel-devel' package is installed and/or missing, run the following:

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

The following is a sample output illustrating the 'kernel-devel' package matching the currently running kernel.



```
[ats-user@localhost ~]$ rpm -qa | grep kernel*
kernel-devel-4.18.0-348.el8.x86_64
kernel-4.18.0-348.el8.x86_64
kernel-modules-4.18.0-348.el8.x86_64
kernel-tools-libs-4.18.0-348.el8.x86_64
kernel-core-4.18.0-348.el8.x86_64
kernel-tools-4.18.0-348.el8.x86_64
```

To install the kernel-devel package corresponding to the currently running kernel, run the following.

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

The connector should recover and clear the fault within a minute. If the fault does not clear within one minute then manually restart the connector. The fault should then be cleared within one minute after the restart.

NOTE: If the above command fails with an error "No match for argument" then it's possible that the current

kernel version is no longer supported and the OS maintainer has removed the package from the dnf repository. In this case the needed kernel-devel .rpm package can be manually downloaded from the vendor's OS archives and then manually installed, or the kernel can be updated to a supported version and the above command tried again.

As an example, if using CentOS and updating the kernel to a version supported by the distribution is not possible, old kernel-devel .rpm packages for CentOS can be manually downloaded from <http://vault.centos.org>. The name of the file to download is given by the output from the following bash command.

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

Once downloaded, the kernel-devel package can be installed by running the following bash command in the directory where the downloaded .rpm file is saved.

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

Oracle Linux

Oracle Linux distributes with two different kernel alternatives, RHCK and UEK. The kernel-devel and kernel-uek-devel packages install the needed kernel development header files in the /usr/src/kernels directory on RHCK and UEK, respectively. The kernel development files are organized in /usr/src/kernels according to their kernel version.

Oracle Linux RHCK

The procedure for identifying the missing kernel package and resolving fault ID 11 on Oracle Linux RHCK is identical to that of RHEL Linux. Please refer to the RHEL Linux section above for more information.

Oracle Linux UEK

The procedure for identifying the missing kernel package and resolving fault ID 11 on Oracle Linux UEK is similar but not identical to that of RHEL Linux. Please refer to the RHEL Linux section above for more information but replace every instance of "kernel-devel" with "kernel-uek-devel." To be specific, replace `kernel-devel-$(uname -r)` with `kernel-uek-devel-$(uname -r)` for every relevant command.

NOTE: If the needed kernel-uek-devel .rpm package cannot be found when attempting to install from the dnf repository then the package can be manually downloaded and installed from the Oracle archives at <https://yum.oracle.com/>.

Debian/Ubuntu Linux

The linux-headers package installs the needed header files in the /usr/src directory, organized according to their kernel version.

Causes

The linux-headers package required for realtime filesystem and network activity monitoring is missing.

You can confirm the headers installed in the /usr/src directory.

Resolution

The linux-headers package can be installed with the following command:

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