Linux内核级故障

目录

概述

在Red Hat Enterprise Linux(RHEL)8和变体、Oracle Linux 8 Red Hat Compatible Kernel(RHCK)、Oracle Linux 7和8、Unbreakable Enterprise Kernel(UEK)6以及运行在4.19或更高版本系统内核上的Amazon Linux 2上，Cisco Secure Endpoint Linux连接器将无法监控文件移动或启用设备流关联（网络监控），因为当前运行的内核缺少内核级软件包或Oracle Linux UEK上的内核级软件包。 在这种情况下，连接器将引发故障ID 11“Required kernel-devely package is missing(必需的内核级软件包缺失)”。对于Debian和Ubuntu，当缺少linux-headers软件包时，可能会引发此故障。

从RHEL 8、Oracle Linux 8 RHCK、Oracle Linux 7和8 UEK 6以及Amazon Linux 2内核4.19或更高版本开始，连接器将使用eBPF模块进行实时文件系统和网络监控。eBPF模块替换在RHEL 6、RHEL 7、Oracle Linux 7 RHCK、Oracle Linux 7 UEK 5及更低版本以及Amazon Linux 2内核4.14或更低版本上运行时使用的Linux内核模块。 对于Ubuntu 18.04及更高版本以及Debian 10及更高版本，eBPF模块是本地模块。

为了获得最广泛的兼容性，连接器将在系统上加载和运行连接器所使用的eBPF模块之前自动编译这些模块。此编译要求安装与当前运行的内核相对应的内核开发头文件。每次启动连接器时，连接器将尝试编译和加载eBPF模块

有时，在安装了UEK的Oracle Linux上可能会出现此故障，尽管计算机上存在内核级程序包。这是由于在安装过程中发生错误，连接器无法将SELinux配置为接受用于监控终端上的活动的eBPF探测器。

适用范围

在全新安全终端Linux连接器安装之后或在更新系统内核之后，通常会发生故障。

操作系统

- RHEL/CentOS/Rocky Linux/AlmaLinux 8
- Oracle Linux 8 RHCK
- Oracle Linux 7和8 UEK 5和6
- Ubuntu 18.04及更高版本
- Debian 10及更高版本
- Amazon Linux 2

连接器版本

- Linux 1.13.0及更高版本

RHEL Linux

内核级软件包将所需的内核开发头文件安装在/usr/src/kernels目录中，这些文件根据其内核版本进行组织。

原因

缺少实时文件系统和网络活动监控所需的内核级软件包。

分辨率

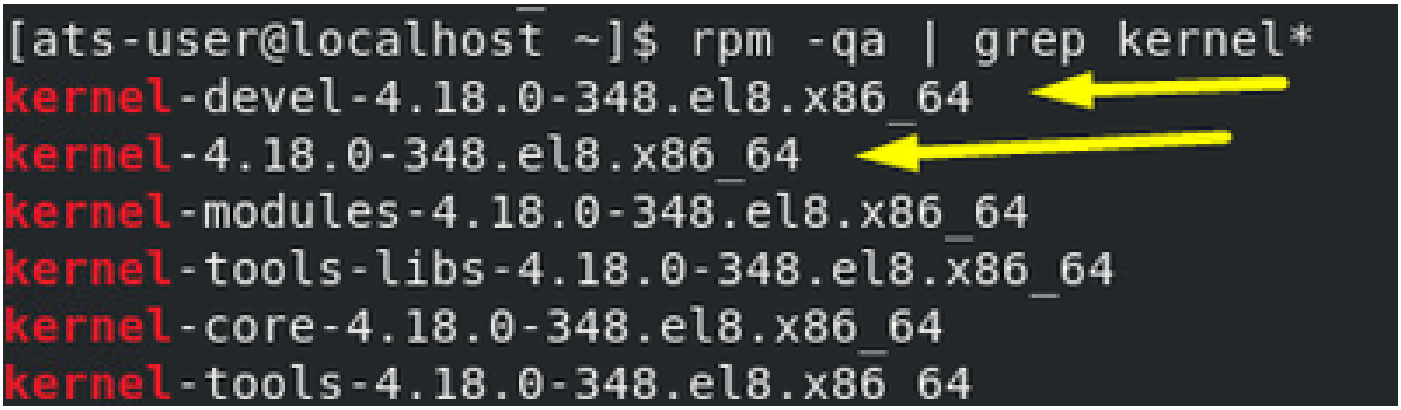
安装与当前运行的内核匹配的“kernel-level”程序包。

步骤

“kernel-level”软件包需要与当前运行的内核匹配。 要验证当前的“kernel-level”软件包是否已安装和/或丢失，请运行以下命令：

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

以下是一个示例输出，说明与当前运行的内核匹配的“kernel-level”程序包。



要安装与当前运行的内核相对应的内核级软件包，请运行以下命令。

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

连接器应该在一分钟内恢复和清除故障。如果故障在一分钟内未清除，请手动重新启动连接器。然

后，应在重新启动后1分钟内清除故障。

注意：如果上述命令失败，并出现错误“No match for argument”，则可能不再支持当前内核版本，并且操作系统维护者已从dnf存储库中删除该软件包。在这种情况下，所需内核级.rpm软件包可以从供应商的OS存档中手动下载，然后手动安装，或者内核可以更新为受支持的版本，然后再次尝试上述命令。

例如，如果无法使用CentOS并将内核更新为发行版支持的版本，则可以从http://vault.centos.org手动下载用于CentOS的旧内核级.rpm包。以下bash命令的输出给出了要下载的文件的名称。

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

下载后，可以在保存下载的.rpm文件的目录中运行以下bash命令，安装内核级软件包。

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

Oracle Linux

Oracle Linux与两种不同的内核替代产品RHCK和UEK一起发布。内核级和内核级软件包分别在RHCK和UEK的/usr/src/kernels目录中安装所需的内核开发头文件。内核开发文件根据其内核版本在/usr/src/kernels中组织。

Oracle Linux RHCK

在Oracle Linux RHCK上识别缺失的内核包和解决故障ID 11的过程与RHEL Linux的过程相同。有关详细信息，请参阅上面的RHEL Linux部分。

Oracle Linux UEK

在Oracle Linux UEK上识别缺失的内核包和解决故障ID 11的过程与RHEL Linux类似，但不相同。有关详细信息，请参阅上面的RHEL Linux部分，但请将每个“kernel-devel”实例替换为“kernel-uek-devel”。 具体来说，对于每个相关命令，用kernel-uek-devel-$(uname -r)替换`kernel-devel-$(uname -r)`。

注：如果在尝试从dnf存储库进行安装时找不到所需的内核级.rpm软件包，则可以从Oracle归档文件(https://yum.oracle.com/)中手动下载并安装该软件包。

Debian/Ubuntu Linux

linux-headers软件包将所需的头文件安装在/usr/src目录中，并根据其内核版本进行组织。

原因

缺少实时文件系统和网络活动监控所需的linux-headers软件包。

您可以确认/usr/src目录中安装的标头。

分辨率

可以使用以下命令安装linux-headers软件包：

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

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。