Linux核心級故障

目錄

概觀

在Red Hat Enterprise Linux(RHEL)8和變體、Oracle Linux 8 Red Hat Compatible Kernel(RHCK)、Oracle Linux 7和8、Unbreakable Enterprise Kernel(UEK)6以及運行在4.19或更高版本系統核心上的Amazon Linux 2上，Cisco Secure Endpoint Linux聯結器將無法在當前運行的核心級軟體包或Oracle Linux UEK上的核心級軟體包缺失時監控檔案移動或啟用裝置流關聯（網路監控）。 在這種情況下，聯結器將提出故障ID 11「Required kernel-devely package is missing」。對於Debian和Ubuntu，當缺少linux-headers包時，可能會引發此故障。

從RHEL 8、Oracle Linux 8 RHCK、Oracle Linux 7和8 UEK 6以及Amazon Linux 2核心4.19或更高版本開始，聯結器將使用eBPF模組進行即時檔案系統和網路監控。eBPF模組取代在RHEL 6、RHEL 7、Oracle Linux 7 RHCK、Oracle Linux 7 UEK 5及更低版本以及Amazon Linux 2 kernel 4.14或更低版本上運行時使用的Linux核心模組。 對於Ubuntu 18.04及更高版本以及Debian 10及更高版本，eBPF模組是本地模組。

為了獲得最廣泛的相容性，聯結器將在系統上載入和運行聯結器所使用的eBPF模組之前自動編譯這些模組。此編譯要求安裝與當前運行的核心相對應的核心開發標頭檔案。每次啟動聯結器時，聯結器將嘗試編譯和載入eBPF模組

有時，儘管電腦上存在核心級軟體包，但安裝了UEK的Oracle Linux上可能會出現此故障。這是由於在安裝過程中發生錯誤，聯結器無法將SELinux配置為接受用於監視端點上的活動的eBPF探測器。

適用性

在安裝新的Secure Endpoint Linux聯結器或更新系統核心之後，通常會引發故障。

作業系統

- 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

聯結器版本

- Linux 1.13.0及更高版本

RHEL Linux

核心開發包將所需的核心開發標頭檔案安裝在/usr/src/kernels目錄中，該檔案根據其核心版本進行組織。

原因

缺少即時檔案系統和網路活動監控所需的核心級軟體包。

解析

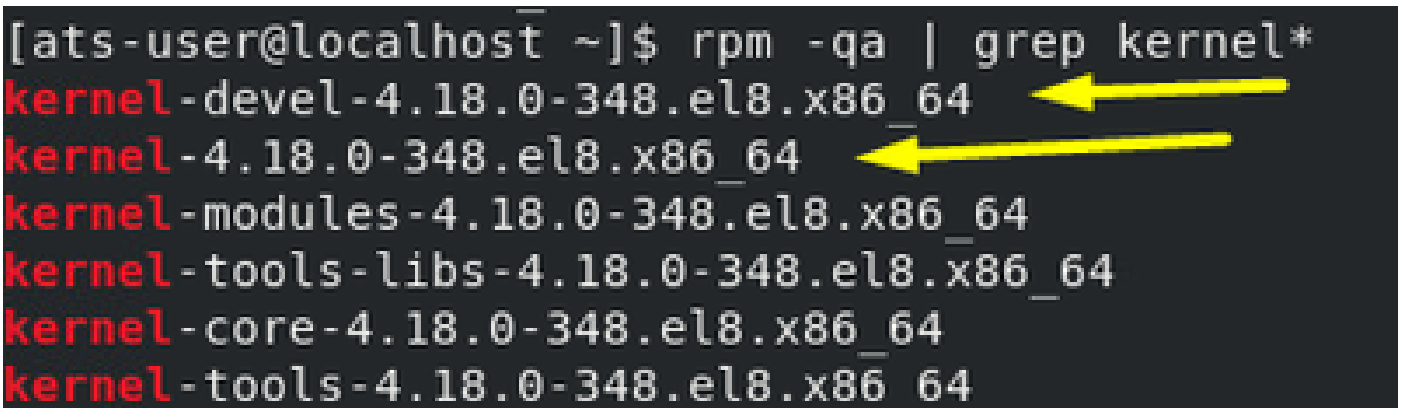
安裝與當前運行的核心匹配的「kernel-level」程式包。

程式

「kernel-level」包需要與當前運行的核心匹配。 要驗證當前的「kernel-level」軟體包是否已安裝和/或丟失，請運行以下命令：

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

以下是說明與當前運行的核心匹配的「kernel-version」軟體包的示例輸出。



要安裝與當前運行的核心相對應的核心級軟體包，請運行以下命令。

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

聯結器應在一分鐘內恢復並清除故障。如果故障在一分鐘內未清除，請手動重新啟動聯結器。然後

，應在重新啟動後1分鐘內清除故障。

注意：如果上述命令失敗，並出現錯誤「No match for arguments」，則可能不再支援當前核心版本，並且作業系統維護者已從dnf儲存庫中刪除該軟體包。在這種情況下，所需的核心級.rpm軟體包可以從供應商的OS歸檔中手動下載，然後手動安裝，或者核心可以更新為受支援的版本，然後再次嘗試上述命令。

例如，如果無法使用CentOS並將核心更新為發行版支援的版本，則可以從http://vault.centos.org手動下載用於CentOS的舊核心級.rpm包。要下載的檔案的名稱由以下bash命令的輸出給出。

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

下載後，可以在儲存下載的.rpm檔案的目錄中運行以下bash命令，安裝核心級軟體包。

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

Oracle Linux

Oracle Linux使用兩種不同的核心替代方案RHCK和UEK。核心級和核心級軟體包分別在RHCK和UEK的/usr/src/kernels目錄中安裝所需的核心開發標頭檔案。核心開發檔案根據其核心版本組織在/usr/src/kernels中。

Oracle Linux RHCK

在Oracle Linux RHCK上識別缺失的核心包和解決故障ID 11的過程與RHEL Linux的過程相同。有關詳細資訊，請參閱上面的RHEL Linux部分。

Oracle Linux UEK

在Oracle Linux UEK上識別缺失的核心包和解決故障ID 11的過程與RHEL Linux類似，但不完全相同。請參閱上面的RHEL Linux部分瞭解更多資訊，但將每個「kernel-devel」例項替換為「kernel-uek-devel」。 具體來說，對於每個相關命令，用`kernel-uek-devel-$(uname -r)`replace`kernel-devel-$(uname -r)`。

註：如果在嘗試從dnf資料檔案庫安裝時找不到所需的核心級別.rpm程式包，則可以從Oracle歸檔檔案(位於https://yum.oracle.com/)手動下載並安裝該程序包。

Debian/Ubuntu Linux

linux-headers軟體包將所需的標頭檔案安裝在/usr/src目錄中，並根據其核心版本進行組織。

原因

缺少即時檔案系統和網路活動監控所需的linux-headers軟體包。

您可以確認/usr/src目錄中安裝的標頭。

解析

可以使用以下命令安裝linux-headers程式包：

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

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。