Linux Kernel-Devel Fault

Inhoud

[Overzicht](#)
[Toepasselijkheid](#)
[Besturingssystemen](#)
[Aansluitversies](#)
[RHEL Linux](#)
[oorzaken](#)
[Resolutie](#)
[Procedure](#)
[Oracle Linux](#)
[Oracle Linux RHCK](#)
[Oracle Linux UEK](#)
[Debian/Ubuntu Linux](#)
[oorzaken](#)
[Resolutie](#)

Overzicht

Op Red Hat Enterprise Linux (RHEL) 8 en varianten, Oracle Linux 8 Red Hat-compatibele Kernel (RHCK), Oracle Linux 7 en 8 Unbreakable Enterprise Kernel (UEK) 6, evenals Amazon Linux 2 op een 4.19 of nieuwer systeemkernel, kan de Cisco Secure Endpoint Linux-connector niet bestandsbewegingen bewaken of ApparaatFlow Correlatie mogelijk maken (netwerkbewaking) wanneer het kernel-stap-pakket, of het pakket kernel-stap-stap op Oracle Linux UEK, ontbreekt voor de momenteel draaiende kern. De connector zal fout-ID 11 "Vereiste pakket kernel-graden" in deze situatie opheffen. Voor Debian en Ubuntu kan deze fout veroorzaken bij het ontbreken van een linux-headerpakket.

Om te beginnen met RHEL 8, Oracle Linux 8 RHCK, Oracle Linux 7 en 8 UEK 6 en Amazon Linux 2 kernel 4.19 of nieuwer gebruikt de connector eBPF modules voor realtime bestands systeem en netwerkbewaking. De eBPF-modules vervangen de Linux Kernel-modules die gebruikt worden bij gebruik op RHEL 6, RHEL 7, Oracle Linux 7 RHCK, Oracle Linux 7 UEK 5 en hoger en Amazon Linux 2 kernel 4.14 of eerder. Voor Ubuntu 18.04 en later, maar ook voor Debian 10 en later, zijn eBPF-modules eigen.

Voor een zo breed mogelijke compatibiliteit stelt de connector automatisch de eBPF-modules samen die door de connector worden gebruikt, alvorens deze op het systeem te laden en uit te voeren. Deze compilatie vereist dat de kabelontwikkelingsbestanden die corresponderen met het momenteel draaiende kern, worden geïnstalleerd. Als realtime bestands- en netwerkbewaking is ingeschakeld, stelt de connector de eBPF-modules samen telkens als de connector wordt gestart, of in realtime als deze functies zijn ingeschakeld als onderdeel van een beleidsupdate.

Toepasselijkheid

De fout wordt normaal gesproken groter nadat een nieuwe Secure Endpoint Linux-connector is geïnstalleerd of nadat deze de systeemkern heeft bijgewerkt.

Besturingssystemen

- RHEL/CentOS/Rocky Linux/AlmaLinux 8
- Oracle Linux 8 RHCK
- Oracle Linux 7 en 8 UEK 6
- Ubuntu 18.04 en later
- 10 debiërs en later
- Amazon Linux 2

Aansluitversies

- Linux 1.13.0 en hoger

RHEL Linux

Het pakket met kernel-graden installeert de benodigde bestanden van de pannenontwikkelingsheader in de map /usr/src/kernels, georganiseerd volgens hun kernelversie.

oorzaken

Het kernel-develpakket dat nodig is voor de controle van het realtime systeem en de netwerkactiviteit ontbreekt en het verbindingsbeleid heeft 'Monitor File Copies and Moves' of 'Enable Devices Flow Correlatief inschakelen' ingeschakeld.

Resolutie

Installeer het "kernel-vel"-pakket dat overeenkomt met de huidige kern.

In de zeldzame situatie dat er geen real-time bestands- en netwerkbewaking nodig is, kan deze fout ook worden geklaard door zowel 'Monitor File Copies and Moves' als 'Enable Devices Flow Correlatie inschakelen' in het beleid uit te schakelen. Merk op dat de connector geen realtime-bescherming van het systeem biedt als deze functies worden uitgeschakeld.

Procedure

Als u het pakket voor het aanpassen van de punten wilt installeren dat overeenkomt met de momenteel draaiende kern, voert u het volgende uit.

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

De connector moet binnen een minuut herstellen en de fout verwijderen. Als de fout niet binnen een minuut verdwijnt, moet u de connector handmatig opnieuw opstarten. De fout dient vervolgens

binnen één minuut na het opnieuw opstarten gewist te worden.

OPMERKING: Als de bovenstaande opdracht faalt met een fout "Geen partij voor argument" dan is het mogelijk dat de huidige kernelversie niet langer wordt ondersteund en de OS-houder het pakket uit de dnf-opslagplaats heeft verwijderd. In dit geval kan het benodigde kernel-devel .rpm pakket handmatig worden gedownload van de OS-archieven van de verkoper en handmatig worden geïnstalleerd, of kan het kanaal worden bijgewerkt naar een ondersteunde versie en heeft de bovenstaande opdracht opnieuw geproefd.

Als het niet mogelijk is om CentOS te gebruiken en de kern bij te werken naar een versie die door de distributie wordt ondersteund, kunnen de oude kernel-devel .rpm pakketten voor CentOS handmatig van http://vault.centos.org worden gedownload. De naam van het te downloaden bestand wordt gegeven door de uitvoer van de volgende basisopdracht.

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

Nadat u het bestand hebt gedownload, kan het kernel-vel-pakket worden geïnstalleerd door de volgende basisopdracht in de map uit te voeren waar het gedownload .rpm-bestand wordt opgeslagen.

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

Oracle Linux

Oracle Linux distribueert met twee verschillende kernel alternatieven, RHCK en UEK. Het kernel-vel- en het kernel-Ondevel-pakketten installeren de noodzakelijke dossiers van de kernelontwikkelingskoppen in de /usr/src/kernels folder op RHCK en UEK, respectievelijk. De pit-ontwikkelingsbestanden worden volgens hun kernelversie in /usr/src/kernels georganiseerd.

Oracle Linux RHCK

De procedure voor het identificeren van het ontbrekende kerelpakket en het oplossen van fout-ID 11 op Oracle Linux RHCK is identiek aan die van RHEL Linux. Raadpleeg het gedeelte RHEL Linux hierboven voor meer informatie.

Oracle Linux UEK

De procedure voor het identificeren van het ontbrekende kerelpakket en het oplossen van fout-ID 11 op Oracle Linux UEK is vergelijkbaar maar niet identiek aan die van RHEL Linux. Raadpleeg het gedeelte RHEL Linux voor meer informatie maar vervang elk exemplaar van "kernel-devel" door "kernel-uek-devel". Wilt u dit specifiek doen, dan `stelt u ter vervanging van ekernel-devel-$(uname-r) met een extra-devel-$(uname-r)` voor elke relevante opdracht.

OPMERKING: Als het benodigde pakket voor het juiste toetsenbord-niveau.rpm niet gevonden kan worden wanneer u probeert te installeren vanaf de gegevensbank, kan het pakket handmatig worden gedownload en geïnstalleerd vanaf de Oracle-archieven op https://yum.oracle.com/.

Debian/Ubuntu Linux

Het linux-headerpakket installeert de benodigde headerbestanden in de /usr/src folder, georganiseerd volgens hun kernel versie.

oorzaken

Het linux-headerpakket vereist voor controle van realtime bestanden en netwerkactiviteit ontbreekt en het verbindingsbeleid heeft 'Monitor File Copies and Moves' of 'Enable Devices Flow Correling inschakelen' ingeschakeld.

Resolutie

Het linux-headerpakket kan met de volgende opdracht worden geïnstalleerd:

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