# Défaillance du noyau Linux

## Table des matières

## Aperçu

Sur Red Hat Enterprise Linux (RHEL) 8 et ses variantes, Oracle Linux 8 Red Hat Compatible Kernel (RHCK), Oracle Linux 7 et 8, Unbreakable Enterprise Kernel (UEK) 6, ainsi qu'Amazon Linux 2 exécuté sur un noyau système 4.19 ou plus récent, le connecteur Cisco Secure Endpoint Linux ne pourra pas surveiller les déplacements de fichiers ou activer la corrélation de flux de périphérique (surveillance réseau) lorsque le package kernel-devel ou kernel-uek-devel sur Oracle Linux UEK est manquant pour le noyau en cours d'exécution. Dans cette situation, le connecteur soulèvera l'ID d'erreur 11 « Le package kernel-devel requis est manquant ». Pour Debian et Ubuntu, cette erreur peut être soulevée lorsque le paquet linux-headers est manquant.

À partir de RHEL 8, Oracle Linux 8 RHCK, Oracle Linux 7 et 8 UEK 6 et le noyau Amazon Linux 2 4.19 ou version ultérieure, le connecteur utilisera des modules eBPF pour la surveillance en temps réel du système de fichiers et du réseau. Les modules eBPF remplacent les modules de noyau Linux utilisés lors de l'exécution sur RHEL 6, RHEL 7, Oracle Linux 7 RHCK, Oracle Linux 7 UEK 5 et versions antérieures, et le noyau Amazon Linux 2 4.14 ou versions antérieures.  Pour Ubuntu 18.04 et versions ultérieures, ainsi que pour Debian 10 et versions ultérieures, les modules eBPF sont natifs.

Pour une compatibilité maximale, le connecteur compilera automatiquement les modules eBPF utilisés par le connecteur avant de les charger et de les exécuter sur le système. Cette compilation nécessite que les fichiers d'en-tête de développement du noyau correspondant au noyau en cours d'exécution soient installés. Le connecteur tente de compiler et de charger les modules eBPF à chaque démarrage du connecteur

Parfois, cette erreur peut apparaître sur Oracle Linux avec UEK installé malgré la présence des paquets kernel-devel sur la machine. Cela est dû à une erreur au cours du processus d'installation, lorsque le connecteur ne parvient pas à configurer SELinux pour accepter les sondes eBPF utilisées pour surveiller l'activité sur le point d'extrémité.

## Applicabilité

La défaillance sera généralement soulevée après une nouvelle installation du connecteur Secure Endpoint Linux ou après la mise à jour du noyau du système.

### Systèmes d'exploitation

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

### Versions des connecteurs

- Linux 1.13.0 et versions ultérieures

# Linux RHEL

Le paquet kernel-devel installe les fichiers d'en-tête de développement du noyau nécessaires dans le répertoire /usr/src/kernels, organisés selon leur version de noyau.

### Causes

Le paquet kernel-devel requis pour la surveillance en temps réel du système de fichiers et de l'activité du réseau est manquant.

### Résolution

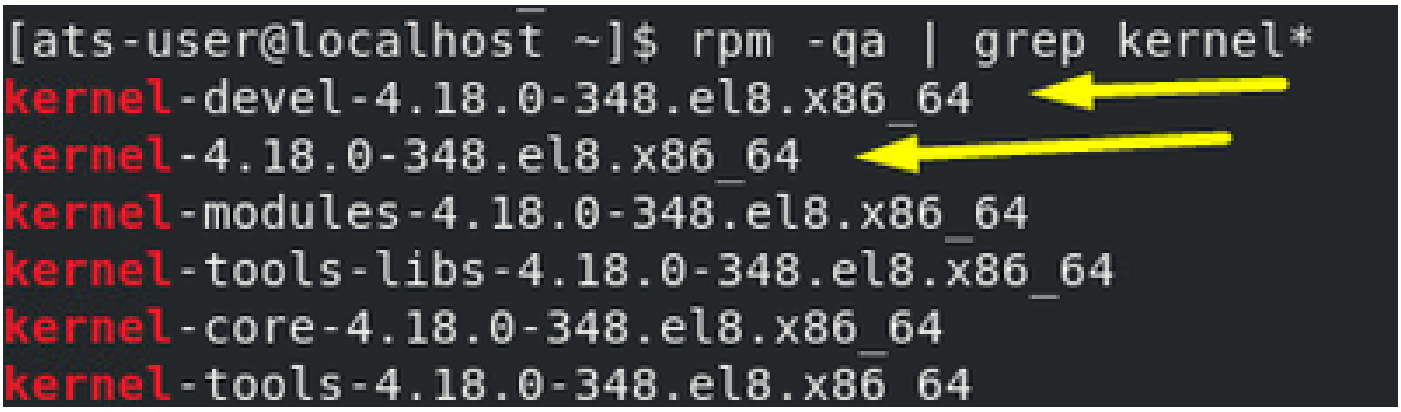
Installez le paquet « kernel-devel » correspondant au noyau en cours d'exécution.

### Procédure

Le paquet « kernel-devel » doit correspondre au noyau en cours d'exécution.  Pour vérifier si le paquet 'kernel-devel' actuel est installé et/ou manquant, exécutez la commande suivante :

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

Voici un exemple de sortie illustrant le paquet « kernel-devel » correspondant au noyau en cours d'exécution.




Pour installer le paquet kernel-devel correspondant au noyau en cours d'exécution, exécutez la commande suivante.

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

Le connecteur doit être rétabli et effacé dans la minute qui suit. Si le problème ne disparaît pas dans la minute qui suit, redémarrez manuellement le connecteur. La panne doit ensuite être résolue dans la minute qui suit le redémarrage.

REMARQUE : Si la commande ci-dessus échoue avec l'erreur "No match for argument", alors il est possible que la version actuelle du noyau ne soit plus prise en charge et que le responsable du système d'exploitation ait supprimé le paquet du dépôt dnf. Dans ce cas, le paquet kernel-devel .rpm nécessaire peut être téléchargé manuellement à partir des archives du système d'exploitation du fournisseur, puis installé manuellement, ou le noyau peut être mis à jour vers une version prise en charge et la commande ci-dessus essayée à nouveau.

Par exemple, si l'utilisation de CentOS et la mise à jour du noyau vers une version prise en charge par la distribution ne sont pas possibles, les anciens paquets .rpm kernel-devel pour CentOS peuvent être téléchargés manuellement à partir de http://vault.centos.org. Le nom du fichier à télécharger est donné par le résultat de la commande bash suivante.

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

Une fois téléchargé, le paquet kernel-devel peut être installé en exécutant la commande bash suivante dans le répertoire où le fichier .rpm téléchargé est enregistré.

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

# Oracle Linux

Oracle Linux distribue avec deux alternatives de noyau différentes, RHCK et UEK. Les paquets kernel-devel et kernel-uek-devel installent les fichiers d'en-tête de développement du noyau nécessaires dans le répertoire /usr/src/kernels sur RHCK et UEK, respectivement. Les fichiers de développement du noyau sont organisés dans /usr/src/kernels en fonction de leur version.

## Oracle Linux RHCK

La procédure d'identification du package noyau manquant et de résolution de l'ID de panne 11 sur Oracle Linux RHCK est identique à celle de RHEL Linux. Pour plus d'informations, reportez-vous à la section RHEL Linux ci-dessus.

## Oracle Linux UEK

La procédure d'identification du paquet de noyau manquant et de résolution de l'ID de panne 11 sur Oracle Linux UEK est similaire mais pas identique à celle de RHEL Linux. Reportez-vous à la section Linux de RHEL ci-dessus pour plus d'informations mais remplacez chaque instance de « kernel-devel » par « kernel-uek-devel ». Pour être plus précis, `remplacez kernel-devel-$(uname -r) par kernel-uek-devel-$(uname -r)` pour chaque commande appropriée.

REMARQUE : si le package kernel-uek-devel .rpm nécessaire est introuvable lors de la tentative d'installation à partir du référentiel dnf, vous pouvez le télécharger manuellement et l'installer à partir des archives Oracle à l'adresse https://yum.oracle.com/.

# Debian/Ubuntu Linux

Le paquet linux-headers installe les fichiers d'en-tête nécessaires dans le répertoire /usr/src, organisés selon leur version de noyau.

## Causes

Le paquet linux-headers requis pour la surveillance en temps réel du système de fichiers et de l'activité du réseau est manquant.

Vous pouvez confirmer les en-têtes installés dans le répertoire /usr/src.

## Résolution

Le paquet linux-headers peut être installé avec la commande suivante :

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

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.