Dépannage d'une défaillance du connecteur Linux Secure Endpoint 11

Table des matières

- Introduction
- Informations générales
- Déterminer la prise en charge BTF
- BTF non pris en charge
- Distributions prises en charge par BTF
- Mise à niveau vers un noyau pris en charge BTF
  - Distributions basées sur les RPM
  - Noyau Oracle Linux Unbreakable Enterprise (UEK)
  - SUSE Linux Enterprise et openSUSE Leap
  - Distributions basées sur Debian
- Installer l'en-tête de noyau manquant
  - Distributions basées sur les RPM
    - Vérifier
    - Résolution
  - Noyau Oracle Linux Unbreakable Enterprise (UEK)
    - Vérifier
    - Résolution
  - SUSE Linux Enterprise et openSUSE Leap
    - Vérifier
    - Résolution
  - Distributions basées sur Debian
    - Vérifier
    - Résolution

Introduction

Ce document décrit comment identifier, résoudre et vérifier la panne 11 dans le connecteur Secure Endpoint Linux.

Informations générales

Le connecteur déclenche la panne 11 chaque fois qu'il ne parvient pas à charger le module eBPF nécessaire pour surveiller l'activité et les événements du système.

À partir de la version 1.25 du connecteur Linux, le connecteur donne la priorité à eBPF CO-RE (Compile Once - Run Everywhere) pour surveiller les événements système sur les noyaux qui prennent en charge BTF, sans nécessiter l'installation d'en-têtes de noyau. Cette méthode d'observabilité du système est plus efficace et constitue l'option privilégiée.

Le connecteur revient à la méthode de chargement eBPF héritée qui nécessite l'installation d'en-têtes de noyau lors de l'utilisation de versions de connecteur Linux antérieures à 1.25 ou s'exécutant sur un noyau qui ne prend pas en charge BTF. Ces en-têtes ne sont généralement pas inclus dans les installations de distribution standard et doivent être installés séparément.

La panne 11 est soulevée si le connecteur ne parvient pas à charger le module eBPF en utilisant l'une ou l'autre des approches, ce qui indique que le système est dans un état non protégé. Ce document détaille les étapes nécessaires pour résoudre ce problème.

Déterminer la prise en charge BTF

Le connecteur nécessite que l'une de ces conditions soit vraie afin de charger le module eBPF nécessaire pour surveiller l'activité du système de fichiers et du réseau :
1. Le noyau actuel a `CONFIG_DEBUG_INFO_BTF` activé. (Il s'agit de l'option préférée.)
2. Les en-têtes du noyau de la version en cours d'exécution sont installés sur le système.

Pour vérifier si votre noyau en cours d'exécution a `CONFIG_DEBUG_INFO_BTF` activé, exécutez la commande :

```
cat /boot/config-$(uname -r) | grep CONFIG_DEBUG_INFO_BTF
```

Si vous voyez `CONFIG_DEBUG_INFO_BTF=y` alors votre noyau prend en charge BTF et le connecteur peut surveiller les événements du système de fichiers et du réseau en utilisant eBPF.

BTF non pris en charge

Si vous exécutez le connecteur version 1.25 ou ultérieure, pensez à mettre à niveau le noyau vers une version qui prend en charge BTF. Une liste des distributions pour lesquelles BTF est activé par défaut est disponible plus loin dans ce document.

Si votre noyau actuel ne prend pas en charge BTF, alors le connecteur requiert l'installation des fichiers d'en-tête du noyau. Le défaut 11 est déclenché si le connecteur ne parvient pas à localiser ces fichiers requis. Suivez les étapes décrites dans Installer l'en-tête de noyau manquant pour résoudre ce problème.

Distributions prises en charge par BTF

Ces distributions ont `CONFIG_DEBUG_INFO_BTF` activé par défaut dans la dernière version du noyau :

- Centos/RHEL 8.2 et versions ultérieures
- Ubuntu 20.04 et versions ultérieures
- Oracle Linux 8.5 et versions ultérieures
- Debian 11 et versions ultérieures
- Alma Linux 8.3 et versions ultérieures

- Rocky Linux 8.3 et versions ultérieures
- SUSE Enterprise 15 SP4 / openSUSE Leap 15.4 et versions ultérieures

Mise à niveau vers un noyau pris en charge BTF

Si vous êtes sur une distribution qui prend en charge BTF dans une version ultérieure du noyau, il est préférable que vous mettiez à jour votre noyau afin de résoudre la panne 11.

Avant de procéder à la mise à jour de votre noyau, mettez d'abord à niveau votre connecteur Linux vers la version 1.25.0 ou ultérieure pour vous assurer que votre connecteur prend en charge BTF.

Distributions basées sur les RPM

Cette section s'applique aux :

- Alma Linux
- Amazon Linux
- Linux CentOS
- Noyau compatible Oracle Linux Red Hat (RHCK)
- Red Hat Enterprise Linux
- Rocky Linux

Pour effectuer une mise à niveau vers la dernière version du noyau :

1. Vérifiez si des mises à jour sont disponibles pour le noyau :

   ```
   yum check-update
   ```

   Si vous voyez `kernel.x86_64` dans le résultat, alors il y a une mise à jour du noyau disponible.
2. Mettre à jour le paquet du noyau :

   ```
   sudo yum update kernel
   ```

3. Redémarrez votre système :

   ```
   sudo reboot
   ```

4. Vérifiez que le nouveau noyau prend en charge BTF et que le défaut 11 est effacé par le connecteur.

Noyau Oracle Linux Unbreakable Enterprise (UEK)

Pour effectuer une mise à niveau vers la dernière version du noyau :

1. Vérifiez si des mises à jour sont disponibles pour le noyau :

   ```
   yum check-update
   ```

Si vous voyez `kernel-uek.x86_64` dans le résultat, alors il y a une mise à jour du noyau disponible.

2. Mettre à jour le paquet du noyau :

   ```
   sudo yum update kernel-uek
   ```

3. Redémarrez votre système :

   ```
   sudo reboot
   ```

4. Vérifiez que le nouveau noyau prend en charge BTF et que le défaut 11 est effacé par le connecteur.

SUSE Linux Enterprise et openSUSE Leap

Pour effectuer une mise à niveau vers la dernière version du noyau :

1. Vérifiez la version actuelle du noyau :

   ```
   uname -r
   ```

2. Répertoriez les packages `kernel-default` disponibles :

   ```
   zypper search -s --match-exact kernel-default
   ```

   Le résultat apparaît comme suit :

   ```
   | kernel-default       | package |

    |

     |
   ```

Recherchez une `version` supérieure à la version actuelle de votre noyau, déterminée à l'étape 1.

3. Installez les nouvelles versions de `kernel-default` avec la commande :

   ```
   sudo zypper install kernel-default=
   ```

4. Redémarrez votre système :

   ```
   sudo reboot
   ```

5. Vérifiez que le nouveau noyau prend en charge BTF et que le défaut 11 est effacé par le connecteur.

Distributions basées sur Debian

Pour effectuer une mise à niveau vers la dernière version du noyau :

1. Récupérez les dernières listes de packages :

   ```
   sudo apt update
   ```

2. Installez les derniers packages :

   ```
   sudo apt upgrade
   ```

3. Redémarrez votre système :

   ```
   sudo reboot
   ```

4. Vérifiez que le nouveau noyau prend en charge BTF et que le défaut 11 est effacé par le connecteur.

Installer l'en-tête de noyau manquant

Avant d'installer un en-tête de noyau manquant, essayez de mettre à niveau votre système vers une version prise en charge par BTF. Si cela ne résout pas le problème 11, ou si votre distribution ne prend pas encore en charge BTF dans la dernière version, alors continuez à installer l'en-tête de noyau manquant.

Distributions basées sur les RPM

Cette section s'applique aux :

- Alma Linux
- Amazon Linux
- Linux CentOS
- Noyau compatible Oracle Linux Red Hat (RHCK)
- Red Hat Enterprise Linux
- Rocky Linux

Vérifier

Les distributions basées sur RPM nécessitent qu'un paquet `kernel-devel` soit installé pour le noyau en cours d'exécution. Pour vérifier si un paquet `kernel-devel` est installé pour le noyau en cours d'exécution, exécutez :

```
rpm -qa | grep kernel-devel-$(uname -r)
```

S'il n'y a pas de résultats, alors le paquet `kernel-devel` requis est manquant et doit être installé.

Si le paquet `kernel-`development correct est installé et que le connecteur soulève toujours la défaillance 11, certains des fichiers requis pourraient avoir été falsifiés. Cette commande vérifie si des fichiers ont été modifiés ou sont manquants :

```
rpm --verify --nomtime --noghost kernel-default-devel
```

Si des fichiers sont manquants ou modifiés, alors `le` paquet de développement du `noyau` doit être désinstallé et réinstallé pour s'assurer que les fichiers requis sont disponibles. Cette commande ne fournit aucun résultat si tous les fichiers du package sont intacts et non modifiés.

Résolution

Pour installer le package `kernel-devel` requis, exécutez la commande :

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

Vérifiez à nouveau. Le défaut 11 est effacé par le connecteur après environ une minute.

Noyau Oracle Linux Unbreakable Enterprise (UEK)

Vérifier

Oracle Linux UEK nécessite l'installation d'un package `kernel-uek-devel` pour le noyau en cours d'exécution. Pour vérifier si un paquet `kernel-uek-devel` est installé pour le noyau en cours d'exécution, exécutez :

```
rpm -qa | grep kernel-uek-devel-$(uname -r)
```

S'il n'y a pas de résultats, alors le paquet `kernel-uek-devel` requis est manquant et doit être installé.

Résolution

Pour installer le package `kernel-uek-devel` requis, exécutez la commande :

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

Vérifiez à nouveau. Le défaut 11 est effacé par le connecteur après environ une minute.

SUSE Linux Enterprise et openSUSE Leap

Vérifier

SUSE et openSUSE nécessitent que le package `kernel-default-devel` soit installé pour le noyau en cours d'exécution. Pour vérifier si le paquet `kernel-default-devel` est installé pour le noyau en cours d'exécution, exécutez :

```
zypper search -si kernel-default-devel | grep $(uname -r | sed "s/-default//")
```

S'il n'y a pas de résultats, alors le paquet `kernel-default-devel` requis est manquant et doit être installé.

Résolution

Installer les en-têtes du noyau

1. Pour déterminer si le paquet `kernel-default-devel` correct pour votre version de noyau est disponible pour l'installation, exécutez la commande :

   ```
   zypper search -s kernel-default-devel | grep $(uname -r | sed "s/-default//")
   ```

Le résultat inclut la syntaxe suivante :

```
| kernel-default-devel |

 |

  |

   |
```

Si vous voyez un résultat similaire, prenez note de la `version` spécifiée dans le résultat et passez à l'étape 2. Sinon, ignorez cette section et utilisez plutôt les étapes pour mettre à jour le noyau et installer les en-têtes de noyau correspondants.

2. Installez le package `kernel-default-devel` à l'aide de cette commande, en remplaçant `<version>` par la version disponible identifiée à l'étape précédente :

   ```
   sudo zypper install --oldpackage kernel-default-devel=
   ```

3. Vérifiez que le package `kernel-default-devel` a été installé. Le défaut 11 est effacé par le connecteur après environ une minute.

Mettre à jour le noyau et installer les en-têtes correspondants

Si le paquet `kernel-default-devel` n'est pas disponible, mettez à jour votre noyau vers une version prise en charge et installez les en-têtes de noyau correspondants.

1. Indiquez les paquets `kernel-default` et `kernel-default-devel` avec la commande :

```
zypper search -s --match-exact kernel-default kernel-default-devel
```

Recherchez les versions correspondantes des packages `kernel-default` et `kernel-default-devel`. Exemple :

```
| kernel-default       | package |

 |

  |

    | kernel-default-devel | package |

     |

      |
```

Prenez note de la `nouvelle version` spécifiée dans le résultat.
Remarque: si vous ne trouvez pas de noyau plus récent vers lequel effectuer la mise à niveau, vous devez effectuer la mise à niveau vers une version de distribution plus récente.

2. Installez les nouvelles versions de `kernel-default` et `kernel-default-devel` avec la commande

:

```
sudo zypper install kernel-default=


            kernel-default-devel=
```

3. Redémarrez votre système :

   ```
   sudo reboot
   ```

4. Vérifiez à nouveau. Le défaut 11 est effacé par le connecteur.

Distributions basées sur Debian

Vérifier

Les distributions basées sur Debian nécessitent qu'un paquet `linux-headers` soit installé pour le noyau en cours d'exécution. Pour vérifier si un paquet `linux-headers` est installé pour le noyau en cours d'exécution, exécutez :

```
apt list linux-headers-$(uname -r)
```

S'il n'y a pas de résultats, alors le paquet `linux-headers` requis est manquant et doit être installé.

Résolution

Pour installer le package `linux-headers` requis, exécutez la commande :

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

Vérifiez à nouveau. Le défaut 11 est effacé par le connecteur après environ une minute.

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.