Dépannage de la compatibilité des connecteurs Linux sur RHEL CentOS Oracle Linux

Table des matières

Introduction

Environnement

- Version du connecteur
- Système d'exploitation
- Version du noyau

Problème

- Symptômes

Résolution

- Mise à niveau du connecteur

Autres informations utiles

- Compatibilité avec Linux OS
- Guide de l'utilisateur Linux

Introduction

Ce document décrit une incompatibilité entre les versions 1.12.4 et antérieures du connecteur Cisco Secure Endpoint Linux.

Environnement

Sur ces plates-formes, le connecteur peut sembler fonctionner normalement mais ne détecte pas les événements de changement de nom de fichier et de réseau, Red Hat Enterprise Linux, CentOS et Oracle Linux 7.8. Effectuez une mise à niveau vers la version 1.12.5 ou ultérieure du connecteur pour restaurer la détection complète des événements.

Ce problème s'applique aux versions des connecteurs, des systèmes d'exploitation et du noyau décrites dans les sections suivantes.

Version du connecteur

Les versions de connecteur concernées sont les suivantes :

- 1.12.4 et versions antérieures

Système d'exploitation

Les systèmes d'exploitation concernés sont les suivants :

- Red Hat Enterprise Linux 7.8
- CentOS 7.8
- Oracle Linux 7.8 (RHCK)

Remarque : Oracle Unbreakable Enterprise Kernel (UEK) est pris en charge dans les versions 1.18.0 et ultérieures des connecteurs.

Version du noyau

Les versions du noyau concernées sont :

- 3.10.0-1127.el7.x86_64 ou version ultérieure

Problème

Sur Red Hat Enterprise Linux, CentOS et Oracle Linux 7.8 avec noyau version 3.10.0-1127.el7.x86_64 ou ultérieure, les versions 1.12.4 et antérieures du connecteur Cisco Secure Endpoint Linux ne détectent pas les événements de changement de nom de fichier et de réseau.

Symptômes

Utilisez ces symptômes pour confirmer le problème :

- Dans la console Cisco Secure Endpoint, les événements de changement de nom de fichier et de réseau ne sont pas détectés par le connecteur et n'apparaissent pas dans la trajectoire du périphérique.
- À partir d'une fenêtre de terminal, exécutez la commande sudo cat /var/log/messages | grep "noyau : ampnetworkflow : <info> _msg_send_offset : homologue déconnecté". La

commande renvoie plusieurs résultats, indiquant une défaillance dans le module noyau ampnetworkflow utilisé par le connecteur.

```
sudo cat /var/log/messages | grep "kernel: ampnetworkflow: <info> _msg_send_offset: peer disconnected"
```

Résolution

Mise à niveau du connecteur

Effectuez ces étapes pour confirmer le problème, mettre à niveau le connecteur et confirmer le correctif :

1. Vérifiez la version installée du connecteur sur le point d'extrémité. Si la version du connecteur est 1.12.4 ou antérieure, passez à l'étape suivante.
2. Confirmez la version du noyau en cours d'exécution :

   À partir d’une fenêtre de terminal, exécutez la commande uname -r.

   ```
   uname -r
   ```

   La commande retourne 3.10.0-1127.el7.x86_64 ou une version ultérieure du noyau. Si la commande renvoie cette version ou une version ultérieure, passez à l'étape suivante.

3. Mettez à niveau le connecteur Cisco Secure Endpoint Linux vers la version 1.12.5 ou ultérieure.
4. Après la mise à niveau, vérifiez que Renommer le fichier et Événements réseau sont détectés à nouveau et s'affichent dans Trajectoire du périphérique.
5. Vérifiez que l'erreur ampnetworkflow n'apparaît plus dans le journal système :

   ```
   sudo cat /var/log/messages | grep "kernel: ampnetworkflow: <info> _msg_send_offset: peer disconnec
   ```

Autres informations utiles

Compatibilité avec Linux OS

- Ouvrez la documentation sur la compatibilité du système d'exploitation du connecteur Linux Cisco Secure Endpoint

Guide de l'utilisateur Linux

- Ouvrez le Guide de l'utilisateur du connecteur Cisco Secure Endpoint Linux

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.