Création de modules de noyau de connecteur Linux pour terminal sécurisé Cisco

Table des matières

Introduction

Cet article explique comment identifier quand les modules noyau précompilés requis pour la surveillance du système de fichiers et du réseau du connecteur Cisco Secure Endpoint Linux ne sont pas disponibles pour le noyau du système en cours d'exécution, et la procédure de compilation manuelle des modules noyau pour que la surveillance du système de fichiers et du réseau soit opérationnelle.

Pour les besoins de cet article, un « noyau non supporté » est une version du noyau qui est supportée par le connecteur Linux, mais les modules de noyau précompilés spécifiques requis pour la version du noyau ne sont pas inclus dans le paquet d'installation du connecteur et doivent donc être compilés manuellement. Cela peut être le cas pour une version donnée d'un connecteur Linux s'exécutant sur un système d'exploitation qui utilise une mise à jour de version roulante, telle qu'Amazon Linux 2.

Toutes les distributions Linux et les versions du noyau ne supportent pas les modules du noyau compilés. Cet article vous aidera à identifier quand compiler manuellement les modules du noyau peut être utilisé.

Conditions préalables

Exigences

- Pour les systèmes basés sur RHEL, gcc fourni par la distribution installé ; kernel-devel installé pour le noyau en cours d'exécution.
- Pour les systèmes utilisant un Unbreakable Enterprise Kernel (UEK), gcc fourni par la distribution installé ; kernel-uek-devel installé pour le noyau en cours d'exécution.

Applicabilité

Système d'exploitation

- RHEL/CentOS 7
- Noyau compatible Oracle Linux 7 Red Hat (RHCK)
- Oracle Linux 7 UEK 5 et versions antérieures
- Amazon Linux 2

Versions du noyau

- Le module de noyau de surveillance du réseau peut être compilé pour les versions 2.6 à 4.14 inclusivement du noyau.
- Le module noyau de surveillance du système de fichiers peut être compilé pour les versions 3.10 à 4.14 inclusivement du noyau.

REMARQUES :

- Sur les versions 2.6 jusqu'à la version 3.10 du noyau, le connecteur utilise les redirections (un module de noyau hors de l'arborescence) pour la surveillance du système de fichiers, ce qui n'est pas applicable à la compilation personnalisée.
- Les versions de noyau comprises entre 4.14 et 4.19 ne sont pas compatibles avec le connecteur et ne sont pas applicables à la compilation personnalisée.
- Pour les versions 4.19 et ultérieures du noyau, le connecteur utilise des modules eBPF pour la surveillance du système de fichiers et du réseau. Référez-vous à l'article Linux Kernel-Devel Fault pour plus de détails sur la résolution de cette erreur sur ces versions du noyau.

Versions des connecteurs

- 1.16.0 et versions ultérieures
- 1.18.0 et versions ultérieures pour la création de modules de noyau UEK personnalisés

Diagnostic d'un noyau non pris en charge

Lorsque le connecteur est exécuté sur un ordinateur avec un noyau non pris en charge, les défaillances 8 (échec du démarrage du moniteur de système de fichiers en temps réel) et 9 (échec du démarrage du moniteur de réseau en temps réel) sont déclenchées et le connecteur fonctionne dans un état dégradé sans surveillance du système de fichiers ou du réseau.

Les étapes suivantes peuvent être effectuées à partir d'une fenêtre de terminal afin d'identifier si le connecteur est exécuté sur un noyau non pris en charge :

1. Vérifiez que la défaillance 8 et/ou la défaillance 9 du connecteur sont déclenchées :

```
$ /opt/cisco/amp/bin/ampcli status
[logger] Set minimum reported log level to notice
Trying to connect...
Connected.
Status:        Connected
Mode:        Degraded
Scan:        Ready for scan
Last Scan:    none
Policy:        unsupported kernel example (#7607)
Command-line:    Enabled
Faults:        2 Critical
Fault IDs:    8, 9
        ID 8 - Critical: Realtime filesystem monitor failed to start.
        ID 9 - Critical: Realtime network monitor failed to start.
```

2. Vérifiez que le noyau en cours d'exécution est compris entre 2.6 et 4.14, inclus, et qu'il ne correspond à aucune des versions de module de noyau précompilées.
   La commande suivante affiche la version courante du noyau :

```
$ uname -r
4.14.97-90.72.amzn2.x86_64
```

   Les versions précompilées du module noyau fournies avec le connecteur sont répertoriées à l'aide de la commande suivante :

3.

```
$ ls /opt/cisco/amp/bin/modules/
4.14.186-146.268.amzn2.x86_64  4.14.198-152.320.amzn2.x86_64  4.14.209-160.335.amzn2.x86_64  4.14.
4.14.192-147.314.amzn2.x86_64  4.14.200-155.322.amzn2.x86_64  4.14.209-160.339.amzn2.x86_64  4.14.
4.14.193-149.317.amzn2.x86_64  4.14.203-156.332.amzn2.x86_64  4.14.214-160.339.amzn2.x86_64  4.14.
```

   Dans l'exemple ci-dessus, la version 4.14.97-90.72.amzn2.x86_64 du noyau n'est pas incluse dans la liste des modules disponibles.

Le connecteur Linux est approprié pour compiler des modules de noyau personnalisés si tous les éléments suivants sont vrais :

- Le ou les défauts 8 et/ou 9 sont surélevés sur le connecteur.
- La version actuelle du noyau est comprise entre 2.6 et 4.14, inclus.
- La version actuelle du noyau n'est pas incluse dans la liste des modules de noyau précompilés `/opt/cisco/amp/bin/modules`

Résolution

Si un connecteur Linux est exécuté sur un noyau non pris en charge, la procédure suivante peut être utilisée pour compiler des modules de noyau personnalisés pour le système :

1. Installer les dépendances système requises :

```
$ yum install gcc
```

`gcc` est nécessaire pour compiler les modules du noyau avec des options spécifiques.

   1. Sur les systèmes utilisant un noyau basé sur RHEL, utilisez la commande suivante pour installer le package de noyau requis :

```
$ yum install kernel-devel-$(uname -r)
```

   2. Sur les systèmes utilisant UEK, utilisez la commande suivante pour installer le package de noyau requis :

```
$ yum install kernel-uek-devel-$(uname -r)
```

      Selon votre système, `kernel-devel-$(uname -r) ou kernel-uek-devel-$(uname -r)` est nécessaire pour compiler les modules du noyau pour le noyau en cours d'exécution.

2. Exécutez le script compile_kmods.sh avec les privilèges racine :

```
$ sudo /opt/cisco/amp/bin/compile_kmods.sh
```

Le script compile_kmods.sh tentera de compiler les modules du noyau de surveillance du système de fichiers et du réseau pour la version courante du noyau. Les modules de noyau personnalisés seront créés dans le répertoire `/opt/cisco/amp/extras/modules`. À la fin de l'exécution, le script redémarre automatiquement le connecteur afin que les modules du noyau nouvellement compilés puissent être chargés sur le système.

3. Vérifiez que les erreurs 8 et 9 ont été supprimées :

```
$ /opt/cisco/amp/bin/ampcli status
[logger] Set minimum reported log level to notice
Trying to connect...
Connected.
Status:        Connected
Mode:        Normal
Scan:        Ready for scan
Last Scan:    2021-06-14 05:53 PM
Policy:        unsupported kernel example (#7607)
Command-line:    Enabled
Faults:        None
```

Autres commandes

L'exécutable compile_kmods.sh est disponible dans les versions 1.16.0 et ultérieures du connecteur Secure Endpoint Linux, et il est installé automatiquement sur les distributions de système d'exploitation compatibles. L'exécutable compile_kmods.sh a été amélioré dans le connecteur Secure Endpoint Linux version 1.18.0 et plus récente pour prendre en charge la compilation personnalisée des UEK.

La compilation personnalisée des modules du noyau pour la surveillance du réseau est prise en charge sur les versions du noyau 2.6 à 4.14, tandis que la compilation personnalisée des modules du noyau pour la surveillance du système de fichiers est prise en charge sur les versions du noyau 3.10 à 4.14.

Commandes disponibles

NOTE: l'exécutable compile_kmods.sh doit être exécuté avec les privilèges racine.

- L'option `-h/–help` affiche la liste complète des options disponibles :

```
$ /opt/cisco/amp/bin/compile_kmods.sh --help
Usage: compile_kmods [OPTIONS]

OPTIONS:

    -f, --force           force overwriting compiled kmod
    -h, --help            show help
```

- L'option `-f/–force` peut être utilisée pour forcer un module de noyau personnalisé précédemment compilé pour le noyau en cours d'exécution à être écrasé. Cela devrait être utilisé lorsque le module noyau personnalisé actuel a été construit avec une ancienne version du connecteur et doit être recompilé avec une version mise à jour du connecteur. Le processus de mise à jour du connecteur ne recompile pas les modules du noyau du client dans le cadre de la mise à jour.

Dépannage

Si les défaillances 8 et/ou 9 sont toujours soulevées après que les étapes de résolution sont suivies, alors les étapes suivantes peuvent être effectuées pour examiner plus en détail le problème :

- Recherchez dans le journal système `/var/log/messages` des lignes de journal similaires à celles-ci :
    - Le journal suivant indique que la version actuelle du noyau sur l'ordinateur n'utilise pas les modules du noyau pour la surveillance du système de fichiers et du réseau. Sur les

versions du noyau supérieures ou égales à 4.18, le système de fichiers et le réseau sont surveillés à l'aide de modules eBPF.

```
init: cisco-amp pre-start: AMP kernel modules are not required on this kernel version '5.4.1
```

- Le journal suivant indique qu'aucune version du noyau n'a été trouvée dans le répertoire des modules du noyau précompilés, `/opt/cisco/amp/bin/modules`, qui sont compatibles avec la version courante du noyau :

```
init: cisco-amp pre-start: finding compatible kernel modules in /opt/cisco/amp/bin/modules t
init: cisco-amp pre-start: failed to find kernel versions
init: cisco-amp pre-start: failed to install and load all required kernel modules in /opt/ci
```

- Le journal suivant indique qu'aucune version de noyau n'a été trouvée dans le répertoire des modules de noyau compilés personnalisés, `/opt/cisco/amp/extra/modules`, qui sont compatibles avec la version courante du noyau :

```
init: cisco-amp pre-start: finding compatible kernel modules in /opt/cisco/amp/extra/modules
init: cisco-amp pre-start: failed to find kernel versions
init: cisco-amp pre-start: failed to install and load all required kernel modules in /opt/ci
```

- Vérifiez si les modules du système de fichiers du connecteur Linux Secure Endpoint et du noyau de surveillance du réseau sont chargés :

```
$ lsmod | grep ampfsm
ampfsm                 24576  0
```

```
$ lsmod | grep ampnetworkflow
ampnetworkflow         65536  0
```

- Mettez à niveau le connecteur Secure Endpoint Linux vers une version plus récente, le cas échéant.

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.