Création de modules de noyau de connecteur Linux de point de terminaison sécurisé Cisco

Contenu

Introduction

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

Pour les besoins de cet article, un « noyau non pris en charge » est une version du noyau qui est prise en charge par le connecteur Linux mais les modules 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 de connecteur Linux donnée exécutée sur un système d'exploitation qui utilise une mise à jour de version continue, comme Amazon Linux 2.

Toutes les distributions Linux et les versions du noyau ne prennent pas en charge les modules compilés du noyau. Cet article vous aidera à identifier lorsque la compilation manuelle des modules du noyau peut être utilisée.

Conditions préalables

Conditions requises

- 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 noyau d'entreprise non cassable (UEK), gcc fourni par la distribution est installé ; kernel-uek-devel installé pour le noyau en cours d'exécution.

Applicabilité

Système d'exploitation

- RHEL/CentOS 7
- Noyau compatible Red Hat d'Oracle Linux 7 (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.
- Le module de noyau de surveillance du système de fichiers peut être compilé pour les versions 3.10 à 4.14 inclusivement.

REMARQUES :

- Sur les versions 2.6 du noyau jusqu'à la version 3.10, le connecteur utilise redirfs (un module de noyau hors de l'arbre) pour la surveillance du système de fichiers qui ne s'applique pas à la compilation personnalisée.
- Les versions de noyau entre 4.14 et 4.19 ne sont pas compatibles avec le connecteur et ne sont pas non plus 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. Reportez-vous à l'article Linux Kernel-Devel Fault pour plus de détails sur la résolution de cette erreur sur ces versions du noyau.

Versions du connecteur

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

Diagbruyant Un noyau non pris en charge

Lorsque le connecteur est exécuté sur un ordinateur avec un noyau non pris en charge, la défaillance 8 (échec du démarrage du moniteur du système de fichiers en temps réel) et la défaillance 9 (échec du démarrage du moniteur réseau en temps réel) sont surélevées et le connecteur s'exécute 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 fonctionne sur un noyau non pris en charge :

1. Vérifiez que le connecteur présente la défaillance 8 et/ou la défaillance 9 déclenchée :

   ```
   $ /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, inclusivement, et qu'il ne correspond à aucune des versions précompilées du module de noyau.
   La commande suivante affiche la version actuelle du noyau en cours d'exécution :

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

Les versions de module de noyau précompilées disponibles, 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 4.14.219-161.340.amzn2.x86_64 4.14.225-
169.362.amzn2.x86_64 4.14.192-147.314.amzn2.x86_64 4.14.200-155.322.amzn2.x86_64 4.14.209-
160.339.amzn2.x86_64 4.14.219-164.354.amzn2.x86_64 4.14.231-173.360.amzn2.x86_64 4.14.193-
149.317.amzn2.x86_64 4.14.203-156.332.amzn2.x86_64 4.14.214-160.339.amzn2.x86_64 4.14.225-
168.357.amzn2.x86_64 4.14.231-173.361.amzn2.x86_64
```

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

Le connecteur Linux convient à la compilation de modules de noyau personnalisés si tous les éléments suivants sont vrais :

- Le connecteur présente une ou plusieurs défaillances (8 et/ou 9).
- La version actuelle du noyau est comprise entre 2.6 et 4.14, inclusivement.
- La version actuelle du noyau n'est pas incluse dans la liste des modules précompilés du noyau `/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.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)
   ```

   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-$(uname -r) orkernel-uek-devel-$(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 root :

   ```
   $ 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 de réseau pour la version actuelle du noyau en cours d'exécution. Les modules de noyau personnalisés seront créés sous `/opt/cisco/amp/extras/modules` répertoire. À la fin de l'exécution, le script redémarrera automatiquement le connecteur afin que les modules du noyau nouvellement compilés puissent être chargés sur le système.
3. Confirmez que les erreurs 8 et 9 ont été effacées :

   ```
   $ /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
```

Plus de 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 du système d'exploitation compatibles. L'exécutable compile_kmods.sh a été amélioré dans le connecteur Secure Endpoint Linux version 1.18.0 et ultérieure pour prendre en charge la compilation personnalisée des clés UEK.

Les modules de noyau de compilation personnalisée pour la surveillance du réseau sont pris en charge sur les versions 2.6 à 4.14 du noyau, tandis que les modules de noyau de compilation personnalisée pour la surveillance du système de fichiers sont pris en charge sur les versions 3.10 à 4.14 du noyau.

Commandes disponibles

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

- 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 la suppression d'un module de noyau personnalisé précédemment compilé pour le noyau en cours d'exécution. Ceci doit être utilisé lorsque le module de noyau personnalisé actuel a été construit avec une version plus ancienne 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 client dans le cadre de la mise à jour.

Dépannage

Si la ou les défaillances 8 et/ou 9 sont toujours soulevées après la *Résolution* les étapes sont suivies, puis les étapes suivantes peuvent être effectuées pour approfondir l'enquête :

- Recherchez les lignes de journal dans le journal système `/var/log/messages` qui sont similaires aux suivantes : Le journal suivant indique que la version actuelle du noyau sur l'ordinateur n'utilise pas de modules de noyau pour la surveillance du système de fichiers et du réseau. Sur les versions de 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
'5.4.117-58.216.amzn2.x86_64'; skipping reinstalling kernel modules
```

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

```
init: cisco-amp pre-start: finding compatible kernel modules in /opt/cisco/amp/bin/modules
```

```
to install 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/cisco/amp/bin/modules, continuing without some modules loaded
```

Le journal suivant indique qu'aucune version de noyau n'est trouvée dans le répertoire de modules de noyau compilé personnalisé, `/opt/cisco/amp/extra/modules`, qui sont compatibles avec la version actuelle du noyau :

```
init: cisco-amp pre-start: finding compatible kernel modules in /opt/cisco/amp/extra/modules to install 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/cisco/amp/extra/modules, continuing without some modules loaded
```

- Vérifiez si les modules du système de fichiers du connecteur Secure Endpoint Linux 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.