Creazione di moduli kernel per i connettori Linux di Cisco Secure Endpoint

Sommario

Introduzione

Questo articolo spiega come identificare quando i moduli kernel precompilati necessari per il monitoraggio del file system e della rete del connettore Cisco Secure Endpoint Linux non sono disponibili per il kernel di sistema attualmente in esecuzione e la procedura per compilare manualmente i moduli kernel in modo che il monitoraggio del file system e della rete sia operativo.

Ai fini di questo articolo, un "kernel non supportato" è una versione del kernel supportata dal connettore Linux, ma i moduli kernel precompilati specifici richiesti per la versione del kernel non sono inclusi nel pacchetto di installazione del connettore e devono quindi essere compilati manualmente. Questo può essere il caso di una determinata release del connettore Linux in esecuzione su un sistema operativo che utilizza un aggiornamento in sequenza, come Amazon Linux 2.

Non tutte le distribuzioni Linux e la versione del kernel supportano l'esecuzione di moduli kernel compilati. Questo articolo consente di identificare quando è possibile utilizzare moduli del kernel compilati manualmente.

Prerequisiti

Requisiti

- Per i sistemi basati su RHEL, installazione del GCC fornito dalla distribuzione; kernel-devel installato per il kernel attualmente in esecuzione.
- Per i sistemi che utilizzano un Unbreakable Enterprise Kernel (UEK), è installato il gcc fornito dalla distribuzione; kernel-uek-devel installato per il kernel attualmente in esecuzione.

Applicabilità

Sistema operativo

- RHEL/CentOS 7
- Kernel compatibile con Oracle Linux 7 Red Hat (RHCK)
- Oracle Linux 7 UEK 5 e versioni precedenti
- Amazon Linux 2

Versioni kernel

- Il modulo del kernel di monitoraggio della rete può essere compilato per le versioni del kernel da 2.6 a 4.14 incluse.
- Il modulo del kernel di monitoraggio del file system può essere compilato per le versioni del kernel da 3.10 a 4.14 incluse.

NOTE:

- Nelle versioni kernel da 2.6 a 3.10, il connettore utilizza redirfs (un modulo kernel out-of-tree) per il monitoraggio del file system, che non è applicabile per la compilazione personalizzata.
- Le versioni del kernel comprese tra 4.14 e 4.19 non sono compatibili con il connettore e non sono applicabili per la compilazione personalizzata.
- Per le versioni kernel 4.19 e successive, il connettore utilizza moduli eBPF per il monitoraggio del file system e della rete. Per ulteriori informazioni sulla risoluzione dell'errore in queste versioni del kernel, consultare l'articolo Linux Kernel-Devel Fault.

Versioni connettore

- 1.16.0 e successive
- 1.18.0 e versioni successive per la creazione di moduli kernel UEK personalizzati

Diagnostalgia un kernel non supportato

Quando il connettore è in esecuzione su un computer con un kernel non supportato, verrà generato l'errore 8 (avvio del monitoraggio del file system in tempo reale non riuscito) e l'errore 9 (avvio del monitoraggio della rete in tempo reale non riuscito) e il connettore verrà eseguito in uno stato degradato senza monitoraggio del file system o della rete.

Da una finestra del terminale è possibile eseguire le seguenti operazioni per verificare se il connettore è in esecuzione su un kernel non supportato:

1. Verificare che nel connettore sia stato generato un errore 8 e/o un errore 9:

   ```
   $ /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. Verificare che il kernel in esecuzione corrente sia compreso tra 2.6 e 4.14, incluse, e che non corrisponda ad alcuna delle versioni precompilate del modulo del kernel.
   Il comando seguente visualizza la versione corrente del kernel in esecuzione:

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

Le versioni precompilate disponibili del modulo kernel in pacchetto con il connettore sono elencate utilizzando il comando seguente:

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
```
Nell'esempio sopra riportato, il kernel versione 4.14.97-90.72.amzn2.x86_64 non è incluso nell'elenco dei moduli kernel disponibili.

Il connettore Linux è adatto per la compilazione di moduli kernel personalizzati se si verificano tutte le seguenti condizioni:

- Errore/i 8 e/o 9 del connettore.
- La versione corrente del kernel è compresa tra 2,6 e 4,14 inclusi.
- La versione corrente del kernel non è inclusa nell'elenco dei moduli del kernel precompilati `/opt/cisco/amp/bin/modules`

Risoluzione

Se un connettore Linux è in esecuzione su un kernel non supportato, è possibile utilizzare la seguente procedura per compilare moduli kernel personalizzati per il sistema:

1. Installa dipendenze di sistema necessarie:

   ```
   $ yum install gcc
   ```
   `gcc` è richiesto per compilare i moduli del kernel con opzioni specifiche.Sui sistemi che utilizzano un kernel basato su RHEL, usare il seguente comando per installare il pacchetto del kernel richiesto:

   ```
   $ yum install kernel-devel-$(uname -r)
   ```
   Sui sistemi che utilizzano UEK, usare il seguente comando per installare il pacchetto del kernel richiesto:
   ```
   $ yum install kernel-uek-devel-$(uname -r)
   ```
   A seconda del sistema in uso, per compilare i moduli kernel per il kernel corrente in esecuzione è necessario utilizzare `kernel-devel-$(uname -r) orkernel-uek-devel-$(uname -r)`.
2. Eseguire lo script compile_kmods.sh con i privilegi root:
   ```
   $ sudo /opt/cisco/amp/bin/compile_kmods.sh
   ```
   Lo script compile_kmods.sh tenterà di compilare i moduli kernel di monitoraggio del file system e della rete per la versione corrente del kernel in esecuzione. I moduli kernel personalizzati verranno creati in `/opt/cisco/amp/extras/modules` directory. Al termine dell'esecuzione, lo script riavvierà automaticamente il connettore in modo che i moduli kernel appena compilati possano essere caricati sul sistema.
3. Confermare che gli errori 8 e 9 sono stati eliminati:

   ```
   $ /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
   ```

Altri comandi

L'eseguibile compile_kmods.sh è disponibile nel connettore Secure Endpoint Linux versione 1.16.0 e successive e viene installato automaticamente nelle distribuzioni compatibili del sistema operativo. L'eseguibile compile_kmods.sh è stato migliorato nel connettore Secure Endpoint Linux versione 1.18.0 e successive per supportare la compilazione personalizzata di UEK.

I moduli kernel di compilazione personalizzata per il monitoraggio della rete sono supportati nelle versioni kernel da 2.6 a 4.14, mentre i moduli kernel di compilazione personalizzata per il monitoraggio del file system sono supportati nelle versioni kernel da 3.10 a 4.14.

Comandi disponibili

NOTA: l'eseguibile compile_kmods.sh deve essere eseguito con privilegi di root.

- L'opzione `-h/–help` visualizza l'elenco completo delle opzioni disponibili:

  ```
  $ /opt/cisco/amp/bin/compile_kmods.sh --help Usage: compile_kmods [OPTIONS] OPTIONS: -f, --force force overwriting compiled kmod -h, --help show help
  ```
- L'opzione `-f/–force` può essere usata per forzare la sovrascrittura di un modulo del kernel personalizzato compilato in precedenza per il kernel attualmente in esecuzione. Deve essere utilizzato quando il modulo del kernel personalizzato corrente è stato creato con una versione precedente del connettore e deve essere ricompilato con una versione aggiornata del connettore. Il processo di aggiornamento del connettore non ricompila i moduli kernel del cliente come parte dell'aggiornamento.

Risoluzione dei problemi

Se i guasti 8 e/o 9 continuano a verificarsi dopo la *Risoluzione* per analizzare ulteriormente il problema, effettuare le seguenti operazioni:

- Cercare nel registro di sistema `/var/log/messages` righe simili alle seguenti: Il seguente registro indica che la versione corrente del kernel in esecuzione sul computer non utilizza i moduli kernel per il monitoraggio del file system e della rete. Nelle versioni del kernel maggiori o uguali a 4.18, il file system e la rete vengono monitorati utilizzando i moduli 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
  ```
  I seguenti log indicano che non esistono versioni del kernel nella directory dei moduli del kernel precompilati, `/opt/cisco/amp/bin/modules`, compatibili con la versione corrente del kernel in esecuzione:

  ```
  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
  ```
  I seguenti log indicano che non sono presenti versioni del kernel nella directory dei moduli del kernel compilati personalizzati, `/opt/cisco/amp/extra/modules`, compatibili con la versione corrente del kernel in esecuzione:

```
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
```

- Verificare se i moduli del file system del connettore Linux dell'endpoint sicuro e del kernel di monitoraggio della rete sono caricati:

```
$ lsmod | grep ampfsm ampfsm 24576 0

$ lsmod | grep ampnetworkflow ampnetworkflow 65536 0
```

- Aggiornare il connettore Secure Endpoint Linux a una versione più recente, se disponibile.