Bouwen aan Cisco Secure Endpoint Linux-kabelmodules

Inhoud

Inleiding

Dit artikel legt uit hoe te identificeren wanneer vooraf samengestelde kernelmodules die vereist zijn voor het bestandsysteem van de Cisco Secure Endpoint Linux-connector en netwerkbewaking niet beschikbaar zijn voor de momenteel draaiende systeemkern, en de procedure voor het handmatig compileren van kernelmodules, zodat bestands- en netwerkbewaking operationeel is.

Voor de toepassing van dit artikel is een "niet-ondersteunde kern" een kernelversie die wordt ondersteund door de Linux-connector, maar de specifieke vooraf gecompileerde kernelmodules die vereist zijn voor de kernelversie, zijn niet opgenomen in het aansluitinstallatiepakket en moeten daarom handmatig worden gecompileerd. Dit kan het geval zijn voor een bepaalde Linux-connectiviteitsrelease die actief is op een besturingssysteem dat gebruikmaakt van een Rollend release update, zoals Amazon Linux 2.

Niet alle Linux distributies en kernel versie ondersteunen gecompileerde kernelmodules. Dit artikel zal helpen bij het identificeren wanneer handmatig compilerende kernelmodules kunnen worden gebruikt.

Voorwaarden

Vereisten

- voor op RHEL gebaseerde systemen, de door distributie geboden gcc geïnstalleerd; Kernniveau geïnstalleerd voor momenteel draaiende kern.
- voor systemen die gebruik maken van een niet-breekbare Enterprise Kernel (UEK), de door distributie geboden gcc geïnstalleerd; Kernlaag-laag geïnstalleerd voor momenteel draaiende kern.

Toepasselijkheid

Besturingssysteem

- RHEL/CentOS 7
- Oracle Linux 7 Red Hat-compatibele Kernel (RHCK)
- Oracle Linux 7 UEK 5 en hoger
- Amazon Linux 2

Kernel Versies

- De netwerkmonitormodule kan worden samengesteld voor de Kernversies 2.6 tot en met 4.14.
- De module van het systeem voor systeembewaking kan worden samengesteld voor de kanaalversies 3.10 tot en met 4.14.

OPMERKINGEN:

- Op kernelversies 2.6 tot en met 3.10 gebruikt de connector herfs (een out-of-tree kernel module) voor bestandsbewaking, die niet van toepassing is voor aangepaste compilatie.
- Kernelversies tussen 4.14 en 4.19 zijn niet compatibel met de -aansluiting en zijn ook niet van toepassing voor aangepaste compilatie.
- Voor kleinere versies 4.19 en nieuwer gebruikt de connector eBPF-modules voor bestandssysteem en netwerkbewaking. Raadpleeg het artikel van de Linux Kernel-Devel voor meer informatie over het oplossen van deze fout bij deze kernelversies.

Aansluitversies

- 1.16.0 en nieuwer
- 1.18.0 en nieuwer voor het maken van aangepaste UEK-kernelmodules

diagknipsel Een niet-ondersteunde Kernel

Als de connector op een computer met een niet-ondersteund netwerk wordt ingeschakeld, zal fout 8 (Realtime-bestandsmonitor niet gestart) en fout 9 (Realtime-netwerkmonitor niet gestart) worden verhoogd en zal de connector in gestoord toestand draaien zonder bestandsbewaking of netwerkbewaking.

De volgende stappen kunnen vanuit een terminalvenster worden uitgevoerd om te bepalen of de connector op een niet-ondersteunde kern actief is:

1. Controleer of de connector fout 8 en/of fout 9 heeft, die is opgelopen:

   ```
   $ /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. Controleer of de huidige rackkern, inclusief tussen 2.6 en 4.14, ligt en of deze niet overeenkomt met een van de vooraf gecompileerde versies van de kernelmodule.
   De volgende opdracht geeft de huidige versie van het actieve pit weer:

   ```
   $ uname -r 4.14.97-90.72.amzn2.x86_64
   ```
   De beschikbare vooraf gecompileerde kernel module versies die met de connector zijn

uitgerust, worden met de volgende opdracht gerangschikt:

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
```
In het bovenstaande voorbeeld is kernel versie 4.14.97-90.72.amzn2.x86_64 niet opgenomen in de lijst van beschikbare kernelmodules.

De Linux-connector is geschikt voor het compileren van aangepaste kernelmodules als alle volgende waar zijn:

- De connector heeft een of meer fouten 8 en/of 9.
- De huidige kernelversie ligt tussen 2.6 en 4.14, inclusief.
- De huidige Kernversie is niet opgenomen in de lijst van vooraf gecompileerde Kernmodules `/opt/cisco/amp/bin/modules`

Resolutie

Als een Linux-connector op een niet-ondersteunde kern wordt uitgevoerd, kan de volgende procedure worden gebruikt om aangepaste kernelmodules voor het systeem samen te stellen:

1. Installeer de vereiste systeemafhankelijkheden:

   ```
   $ yum install gcc
   ```
   `gcc` is nodig om de kernelmodules met specifieke opties samen te stellen .Op systemen die een op RHEL gebaseerde kern gebruiken, gebruikt u de volgende opdracht om het vereiste granenpakket te installeren:

   ```
   $ yum install kernel-devel-$(uname -r)
   ```
   Gebruik in systemen die UEK gebruiken de volgende opdracht om het vereiste spoorwegpakket te installeren:
   ```
   $ yum install kernel-uek-devel-$(uname -r)
   ```
   Afhankelijk van uw systeem is `er een kernel-devel-$(oname-r) voor het maken van een` kernel-`devel-`$ (uname-r) vereist om de kerelmodules voor het huidige scherpstel te kunnen samenstellen.
2. Draai het compilile_standaard.sh script met wortelvoorrechten:
   ```
   $ sudo /opt/cisco/amp/bin/compile_kmods.sh
   ```
   Het script compile_compds.sh zal proberen om bestanden en netwerk monitorkernel modules samen te stellen voor de huidige actieve versie van de kern. De aangepaste kernelmodules worden gecreëerd onder `/opt/cisco/amp/extras/modules` folder. Aan het eind van de uitvoering zal het script de connector automatisch opnieuw opstarten zodat de nieuw gecompileerde kernelmodules op het systeem kunnen worden geladen.
3. Controleer of de fouten 8 en 9 zijn gewist:

   ```
   $ /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
   ```

Meer opdrachten

Compile_komds.sh uitvoerbaar is beschikbaar in Secure Endpoint Linux-connector versies 1.16.0 en nieuwer, en het wordt automatisch geïnstalleerd op compatibele OS-distributies. Compile_standaard.sh uitvoerbaar werd verbeterd in Secure Endpoint Linux-connector versie 1.18.0 en nieuwer om de aangepaste compilatie van UEKs te ondersteunen.

Aangepaste compiderende kernelmodules voor netwerkbewaking worden ondersteund door de kernelversies 2.6 tot en met 4.14, terwijl aangepaste compilermodules voor bestandsbewaking worden ondersteund door de Kernversies 3.10 tot en met 4.14.

Beschikbare opdrachten

OPMERKING: compilile_mcds.sh moet uitgevoerd worden met wortelvoorrechten.

- De optie`-h/-help` geeft de volledige lijst met beschikbare opties weer:

```
$ /opt/cisco/amp/bin/compile_kmods.sh --help Usage: compile_kmods [OPTIONS] OPTIONS: -f, --
force force overwriting compiled kmod -h, --help show help
```

- De `F/—force` optie kan worden gebruikt om een eerder gecompileerde aangepaste kernelmodule te forceren zodat het momenteel actieve pnel overschreven kan worden. Dit dient te worden gebruikt wanneer de huidige aangepaste kernelmodule is gebouwd met een oudere versie van de connector en opnieuw moet worden gecompileerd met een aangepaste versie van de connector. In het aansluitupproces worden de modules van de klant niet opnieuw samengesteld als onderdeel van de update.

Probleemoplossing

Indien de fout(en) 8 en/of 9 na de *Resolutie* er worden stappen ondernomen , en de volgende stappen kunnen worden ondernomen om het probleem verder te onderzoeken :

- Zoek loglijnen in het systeemlogboek`/var/log/berichten` die op het volgende lijken: In het volgende logbestand staat dat de huidige versie van de kern op de computer geen kernelmodules gebruikt voor de controle van bestanden en netwerken. Voor kleinere versies groter dan of gelijk aan 4.18 worden het bestandsysteem en het netwerk bewaakt met behulp van eBPF-modules.

```
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
```

  In het volgende logboek staat dat er geen kernelversies zijn gevonden in de vooraf gecompileerde kernel modules folder, `/opt/cisco/amp/bin/modules`, die compatibel zijn met de huidige versie van het besturingssysteem:

```
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
```

  In het volgende logboek staat dat er geen kernelversies zijn gevonden in de aangepaste gecompileerde kernel modules folder, `/opt/cisco/amp/extra/modules`, die compatibel zijn met de

huidige versie van het besturingssysteem:

```
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
```

- Controleer of Secure Endpoint Linux-connector-bestandssysteem en netwerkmonitorkermodules zijn geladen:

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

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

- upgrade van de Secure Endpoint Linux-connector naar een nieuwere versie, indien beschikbaar.