Criando módulos de kernel do conector Linux do Cisco Secure Endpoint

Contents

Introduction

Este artigo explica como identificar quando os módulos de kernel pré-compilados necessários para o sistema de arquivos e monitoramento de rede do conector Cisco Secure Endpoint Linux não estão disponíveis para o kernel do sistema em execução no momento, e o procedimento para compilar manualmente os módulos de kernel para que o sistema de arquivos e o monitoramento de rede estejam operacionais.

Para o objetivo deste artigo, um "kernel não suportado" é uma versão de kernel suportada pelo conector Linux, mas os módulos específicos de kernel pré-compilados necessários para a versão de kernel não estão incluídos no pacote de instalação do conector e, portanto, precisam ser compilados manualmente. Esse pode ser o caso de uma determinada versão de conector Linux sendo executada em um sistema operacional que usa uma atualização de versão de lançamento, como o Amazon Linux 2.

Nem todas as distribuições de Linux e versões de kernel suportam a execução de módulos de kernel compilados. Este artigo ajudará a identificar quando os módulos kernel de compilação manual podem ser usados.

Prerequisites

Requirements

- Para sistemas baseados em RHEL, gcc fornecido pela distribuição instalado; kernel-devel instalado para o kernel em execução no momento.
- Para sistemas que utilizam um Kernel Empresarial Ininterrupto (UEK), instalado gcc fornecido pela distribuição; kernel-uek-devel instalado para o kernel em execução no momento.

Aplicabilidade

Sistema operacional

- RHEL/CentOS 7
- Kernel compatível com Red Hat (RHCK) do Oracle Linux 7
- Oracle Linux 7 UEK 5 e anterior
- Amazon Linux 2

Versões do kernel

- O módulo de kernel de monitoração de rede pode ser compilado para as versões de kernel 2.6 a 4.14 inclusive.
- O módulo de kernel de monitoração do sistema de arquivos pode ser compilado para as versões de kernel 3.10 a 4.14 inclusive.

NOTAS:

- Nas versões 2.6 até 3.10 do kernel, o conector usa o comando redirfs (um módulo de kernel fora de árvore) para monitoração do sistema de arquivos que não se aplica à compilação personalizada.
- As versões de kernel entre 4.14 e 4.19 não são compatíveis com o conector e também não se aplicam à compilação personalizada.
- Para as versões 4.19 e mais recentes do kernel, o conector usa módulos eBPF para monitoração de sistema de arquivos e rede. Consulte o artigo Falha de Kernel-Devel do Linux para obter detalhes sobre como resolver essa falha nessas versões de kernel.

Versões do conector

- 1.16.0 e mais recente
- 1.18.0 e mais recente para criar módulos de kernel UEK personalizados

DIAGbarulho um kernel não suportado

Quando o conector está em execução em um computador com um kernel não suportado, a falha 8 (o monitor de sistema de arquivos em tempo real não foi iniciado) e a falha 9 (o monitor de rede em tempo real não foi iniciado) serão aumentadas e o conector será executado em estado degradado sem monitoração de sistema de arquivos ou de rede.

As seguintes etapas podem ser executadas a partir de uma janela do terminal para identificar se o conector está sendo executado em um kernel não suportado:

1. Verifique se a falha do conector 8 e/ou 9 foi elevada:

```
$ /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. Verifique se o kernel em execução está entre 2.6 e 4.14, inclusive, e se ele não corresponde a nenhuma das versões pré-compiladas do módulo kernel.
   O seguinte comando exibe a versão atual do kernel em execução:

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

As versões disponíveis do módulo de kernel pré-compilado juntamente com o conector estão listadas usando o seguinte comando:

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
```

No exemplo acima, a versão de kernel 4.14.97-90.72.amzn2.x86_64 não está incluída na lista de módulos de kernel disponíveis.

O conector Linux é adequado para a compilação de módulos kernel personalizados se todos os itens a seguir forem verdadeiros:

- A(s) falha(s) 8 e/ou 9 no conector está(ão) elevada(s).
- A versão atual do kernel está entre 2,6 e 4,14, inclusive.
- A versão atual do kernel não está incluída na lista de módulos de kernel pré-compilados `/opt/cisco/amp/bin/modules`

Resolução

Se um conector Linux estiver sendo executado em um kernel não suportado, o procedimento a seguir pode ser usado para compilar módulos de kernel personalizados para o sistema:

1. Instalar dependências de sistema necessárias:

```
$ yum install gcc
```

`o gcc` é necessário para compilar os módulos do kernel com opções específicas.Em sistemas que usam um kernel baseado em RHEL, use o seguinte comando para instalar o pacote de kernel necessário:

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

Em sistemas que usam UEK, use o seguinte comando para instalar o pacote de kernel necessário:

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

Dependendo do seu sistema, `kernel-devel-$(uname -r) orkernel-uek-devel-$(uname -r)` é necessário para compilar os módulos kernel para o kernel em execução.

2. Execute o script de compilação_kmods.sh com privilégios raiz:

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

O script de compilação_kmods.sh tentará compilar os módulos do kernel do sistema de arquivos e da rede para a versão atual do kernel em execução. Os módulos de kernel personalizados serão criados sob o comando `/opt/cisco/amp/extras/modules` diretório. No final da execução, o script reiniciará o conector automaticamente para que os módulos do kernel recém-compilados possam ser carregados no sistema.

3. Confirme se as falhas 8 e 9 foram eliminadas:

```
$ /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
```

Mais comandos

O arquivo executável de compilação_kmods.sh está disponível no conector Secure Endpoint Linux versões 1.16.0 e mais recente e é instalado automaticamente em distribuições de SO compatíveis. O arquivo executável de compilação_kmods.sh foi aprimorado no conector Secure Endpoint Linux versão 1.18.0 e mais recente para suportar a compilação personalizada de UEKs.

Os módulos de kernel de compilação personalizados para monitoração de rede são suportados nas versões de kernel 2.6 a 4.14, enquanto os módulos de kernel de compilação personalizados para monitoração de sistema de arquivos são suportados nas versões de kernel 3.10 a 4.14.

Comandos disponíveis

NOTE: o arquivo executável compilarkmods.sh deve ser executado com privilégios raiz.

- A opção `h/—ajuda` exibe a lista completa das opções disponíveis:

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

- A opção `-f/—force` pode ser usada para forçar a substituição de um módulo de kernel personalizado previamente compilado para o kernel em execução. Isso deve ser usado quando o módulo kernel personalizado atual foi criado com uma versão mais antiga do conector e precisa ser recompilado com uma versão atualizada do conector. O processo de atualização do conector não recompila os módulos do kernel do cliente como parte da atualização.

Troubleshooting

Se a(s) falha(s) 8 e/ou 9 ainda estiver(em) elevada(s) após a *Resolução* as etapas são seguidas e as seguintes etapas podem ser executadas para investigar o problema:

- Procure linhas de log no registro do sistema `/var/log/messages` que sejam semelhantes às seguintes: O registro a seguir afirma que a versão atual do kernel em execução no computador não usa módulos de kernel para monitoração de sistema de arquivos e rede. Em versões de kernel maiores ou iguais a 4.18, o sistema de arquivos e a rede são monitorados usando módulos 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
```

  O registro a seguir indica que não há versões de kernel encontradas no diretório de módulos de kernel pré-compilados, `/opt/cisco/amp/bin/modules`, que são compatíveis com a versão atual do kernel em execução:

```
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
```

  O registro a seguir declara que não há versões de kernel encontradas no diretório de módulos de kernel compilados personalizados, `/opt/cisco/amp/extra/modules`, que são

compatíveis com a versão atual do kernel em execução:

```
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
```

- Verifique se os módulos do kernel do sistema de arquivos do conector Linux Secure Endpoint e do monitoramento de rede estão carregados:

```
$ lsmod | grep ampfsm ampfsm 24576 0

$ lsmod | grep ampnetworkflow ampnetworkflow 65536 0
```

- Atualize o conector Secure Endpoint Linux para uma versão mais nova, se disponível.