Cisco Secure Endpoint Linux Connectorカーネルモジュールの構築

内容

概要

この記事では、Cisco Secure Endpoint Linuxコネクタのファイルシステムとネットワーク監視に必要なプリコンパイル済みカーネルモジュールが、現在実行中のシステムカーネルで使用できない場合の識別方法と、ファイルシステムとネットワーク監視が動作するようにカーネルモジュールを手動でコンパイルする手順について説明します。

この記事の目的のために、"unsupported kernel"はLinuxコネクタでサポートされているカーネルバージョンですが、カーネルバージョンに必要な特定のプリコンパイル済みカーネルモジュールはコネクタインストールパッケージに含まれていないため、手動でコンパイルする必要があります。これは、Amazon Linux 2などのローリングリリースアップデートを使用するオペレーティングシステムで実行されている特定のLinuxコネクタリリースの場合に起こります。

すべてのLinuxディストリビューションとカーネルバージョンが、コンパイルされたカーネルモジュールの実行をサポートしているわけではありません。この記事は、カーネルモジュールを手動でコンパイルする際の識別に役立ちます。

前提条件

要件

- RHELベースのシステムでは、ディストリビューション提供のgccがインストールされています。現在カーネルを実行するためにインストールされたkernel-devel。
- Unbreakable Enterprise Kernel(UEK)を使用するシステムでは、ディストリビューション提供のgccがインストールされています。kernel-uek-develが現在実行されているカーネルにインストールされている。

適用性

オペレーティング システム

- RHEL/CentOS 7
- Oracle Linux 7 Red Hat Compatible Kernel(RHCK)
- Oracle Linux 7 UEK 5以前
- Amazon Linux 2

カーネルバージョン

- ネットワークモニタリングカーネルモジュールは、カーネルバージョン2.6から4.14までコンパイルできます。
- ファイルシステム監視カーネルモジュールは、カーネルバージョン3.10から4.14までコンパイルできます。

- カーネルのバージョン2.6から3.10までは、コネクタはファイルシステムの監視にredirfs（ツリーの外のカーネルモジュール）を使用します。これはカスタムコンパイルには適用できません。
- 4.14から4.19までのカーネルバージョンはコネクタと互換性がなく、カスタムコンパイルにも適用されません。
- カーネルバージョン4.19以降では、このコネクタはファイルシステムとネットワークの監視にeBPFモジュールを使用します。これらのカーネルバージョンでこの障害を解決する方法の詳細は、『Linuxカーネル – レベル障害』を参照してください。

コネクタのバージョン

- 1.16.0以降
- カスタムUEKカーネルモジュールを作成するための1.18.0以降

Diag

コネクタがサポートされていないカーネルのコンピュータで動作している場合、障害8(Realtime filesystem monitor failed to start)と障害9(Realtime network monitor failed to start)が起動し、コネクタはファイルシステムやネットワークを監視せずにdegraded状態で動作します。

コネクタがサポートされていないカーネルで動作しているかどうかを確認するには、ターミナルウィンドウから次の手順を実行します。

1. コネクタに障害8または障害9が発生していることを確認します。

   ```
   $ /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. 現在の実行中のカーネルが2.6から4.14の間であり、コンパイル済みカーネルモジュールのどのバージョンとも一致していないことを確認します。
   次のコマンドは、現在の実行カーネルバージョンを表示します。

   ```
   $ uname -r 4.14.97-90.72.amzn2.x86_64
   ```
   コネクタに同梱されている使用可能なプリコンパイル済みカーネルモジュールバージョンは

、次のコマンドを使用して一覧表示されます。

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
```
上記の例では、カーネルバージョン4.14.97-90.72.amzn2.x86_64は利用可能なカーネルモジュールのリストに含まれていません。

Linuxコネクタは、以下のすべてが正しい場合、カスタムカーネルモジュールのコンパイルに適しています。

- コネクタに障害8または9が発生しています。
- 現在のカーネルのバージョンは2.6 ~ 4.14です。
- 現在のカーネルバージョンは、プリコンパイルされたカーネルモジ `/opt/cisco/amp/bin/modules`

解決方法

Linuxコネクタがサポートされていないカーネルで動作している場合は、システムのカスタムカーネルモジュールをコンパイルするために次の手順を使用できます。

1. 必要なシステム依存関係のインストール：

```
$ yum install gcc
```
`gcc`は、カーネルモジュールを特定のオプションでコンパイルするために必要です。RHELベースのカーネルを使用するシステムでは、次のコマンドを使用して必要なカーネルパッケージをインストールします。

```
$ yum install kernel-devel-$(uname -r)
```
UEKを使用するシステムでは、次のコマンドを使用して、必要なカーネルパッケージをインストールします。
```
$ yum install kernel-uek-devel-$(uname -r)
```
現在の実行中のカーネルのカーネルモジュールをコンパイルするには、システムに応じて `kernel-devel-$(uname -r) orkernel-uek-devel-$(uname -r)` が必要です。

2. root priviledgesでcompile_kmods.shスクリプトを実行します。
```
$ sudo /opt/cisco/amp/bin/compile_kmods.sh
```
compile_kmods.shスクリプトは、現在実行中のカーネルバージョンのファイルシステムとネットワーク監視カーネルモジュールのコンパイルを試みます。カスタムカーネルモジュールは、 `/opt/cisco/amp/extras/modules` ディレクトリにインストールされて工場から出荷されます。実行が終了すると、スクリプトはコネクタを自動的に再起動し、新しくコンパイルされたカーネルモジュールをシステムにロードできるようになります。
3. 障害8と9がクリアされたことを確認します。

```
$ /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
```

より多くのコマンド

compile_kmods.sh実行可能ファイルは、Secure Endpoint Linuxコネクタバージョン1.16.0以降で利用可能で、互換性のあるOSディストリビューションに自動的にインストールされます。compile_kmods.sh実行可能ファイルは、UEKのカスタムコンパイルをサポートするために、Secure Endpoint Linuxコネクタバージョン1.18.0以降で改良されました。

ネットワークモニタリング用のカスタムコンパイルカーネルモジュールはカーネルバージョン2.6 ~ 4.14でサポートされ、ファイルシステム監視用のカスタムコンパイルカーネルモジュールはカーネルバージョン3.10 ~ 4.14でサポートされます。

使用可能なコマンド

注：compile_kmods.sh実行可能ファイルは、root権限で実行する必要があります。

- `-h/–help`オプションは、使用可能なオプションの完全なリストを表示します。

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

- `-f/–force`すると、現在実行中のカーネル用にコンパイル済みのカスタムカーネルモジュールを上書きすることができます。これは、現在のカスタムカーネルモジュールが古いバージョンのコネクタで構築されており、コネクタの最新バージョンで再コンパイルする必要がある場合に使用してください。コネクタの更新プロセスでは、お客様のカーネルモジュールは更新の一部として再コンパイルされません。

トラブルシューティング

障害8および/または9が *解決方法* 次の手順に従って、問題をさらに調査できます。

- システムログ/`var`/`log`/messagesで、次のようなログ行を探してください。 次のログは、コンピュータで現在実行されているカーネルバージョンが、ファイルシステムとネットワークの監視にカーネルモジュールを使用していないことを示しています。カーネルのバージョンが4.18以上の場合、ファイルシステムとネットワークはeBPFモジュールを使用して監視されます。

```
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
```

次のログは、プリコンパイルされたカーネルモジュールディレクトリにカーネルバージョンが見つからないことを示しています。 `/opt/cisco/amp/bin/modules`現在の実行カーネルバージョンと互換性がある。

```
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
```

次のログは、カスタムコンパイルされたカーネルモジュールディレクトリにカーネルバージョンが見つからないことを示しています。 `/opt/cisco/amp/extra/modules`現在の実行カーネルバージョンと互換性がある。

```
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
```

- Secure Endpoint Linuxコネクタファイルシステムとネットワークモニタリングカーネルモジュールがロードされているかどうかを確認します。

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

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

- Secure Endpoint Linuxコネクタが利用可能な場合は、新しいバージョンにアップグレードします。