Linuxカーネルデバイスの障害

内容

概要

Red Hat Enterprise Linux (RHEL) 8とその亜種、Oracle Linux 8 Red Hat Compatible Kernel (RHCK)、Oracle Linux 7と8、Unbreakable Enterprise Kernel (UEK) 6、および4.19以降のシステムカーネルで稼働するAmazon Linux 2では、Cisco Secure Endpoint Linuxコネクタで、kernel-develパッケージまたはOracle Linux UEKのkernel-uek-develパッケージが現在稼働しているカーネルにない場合、ファイル移動の監視やDevice Flow Correlation（ネットワークモニタリング）の有効化ができません。 この場合、コネクタはエラーID 11「Required kernel-devel package is missing」を送出します。DebianとUbuntuでは、linux-headersパッケージが見つからないときにこのエラーが発生する可能性があります。

RHEL 8、Oracle Linux 8 RHCK、Oracle Linux 7および8 UEK 6、Amazon Linux 2カーネル4.19以降では、コネクタでeBPFモジュールを使用してリアルタイムのファイルシステムとネットワークモニタリングを行います。eBPFモジュールは、RHEL 6、RHEL 7、Oracle Linux 7 RHCK、Oracle Linux 7 UEK 5以前、およびAmazon Linux 2カーネル4.14以前で実行する場合に使用されるLinuxカーネルモジュールに代わるものです。 Ubuntu 18.04以降およびDebian 10以降では、eBPFモジュールはネイティブです。

互換性を最大限に高めるために、コネクタが使用するeBPFモジュールは、システムにロードして実行する前に、コネクタによって自動的にコンパイルされます。このコンパイルには、現在実行中のカーネルに対応するカーネル開発ヘッダーファイルがインストールされている必要があります。コネクタは、コネクタが起動するたびにeBPFモジュールのコンパイルとロードを試行します

時々、このエラーは、カーネル開発パッケージがマシンに存在しているにもかかわらず、UEKがインストールされているOracle Linuxで発生する可能性があります。これは、コネクタがエンドポイント上のアクティビティを監視するために使用されるeBPFプローブを受け入れるようにSELinuxを設定できない、インストールプロセス中の障害によって発生します。

適用性

この障害は通常、Secure Endpoint Linuxコネクタを新規インストールした後、またはシステムカーネルを更新した後に発生します。

オペレーティング システム

- RHEL/CentOS/Rocky Linux/AlmaLinux 8
- Oracle Linux 8 RHCK

- Oracle Linux 7および8 UEK 5および6
- Ubuntu 18.04以降
- Debian 10以降
- Amazon Linux 2

コネクタバージョン

- Linux 1.13.0以降

RHEL Linux

kernel-develパッケージは、必要なカーネル開発ヘッダファイルを/usr/src/kernelディレクトリにインストールします。これはカーネルのバージョンに従って構成されています。

原因

リアルタイムのファイルシステムおよびネットワークアクティビティの監視に必要なkernel-develパッケージがありません。

解決方法

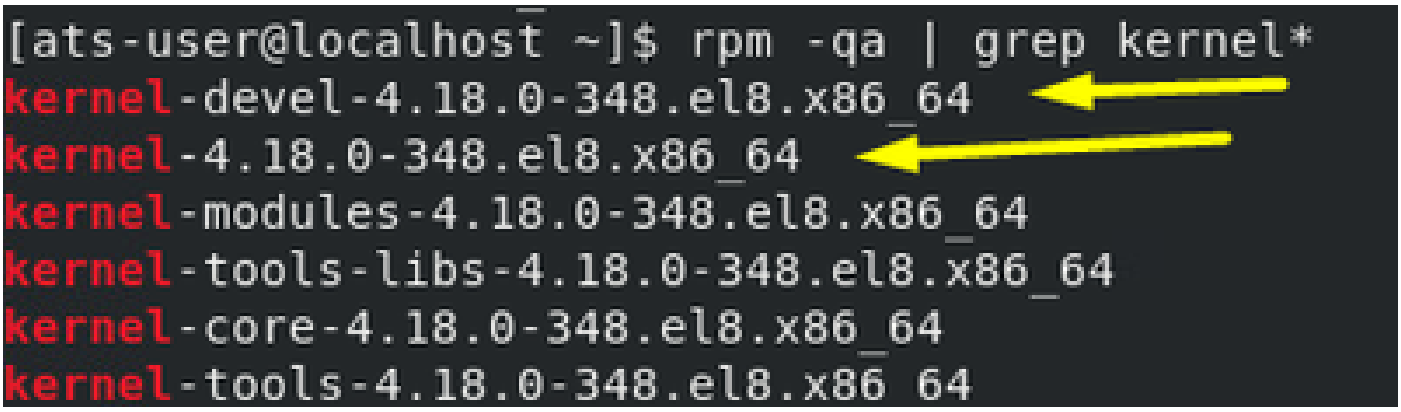
現在実行中のカーネルに一致する'kernel-devel'パッケージをインストールします。

手順

'kernel-devel'パッケージは、現在実行中のカーネルと一致する必要があります。 現在の'kernel-devel'パッケージがインストールされているか、存在しないか、またはその両方を確認するには、次のコマンドを実行します。

```
rpm -qa | grep kernel*
```

以下は、現在動作中のカーネルに対応する'kernel-devel'パッケージを示す出力例です。



現在実行中のカーネルに対応するカーネルデバイスパッケージをインストールするには、次のコマンドを実行します。

```
dnf install -y kernel-devel-$(uname -r)
```

コネクタが復旧し、1分以内に障害がクリアされます。1分以内に障害が解消されない場合は、コネクタを手動で再起動します。再起動後1分以内に障害がクリアされます。

注：上記のコマンドが「No match for argument」エラーで失敗する場合、現在のカーネルバージョンがサポートされなくなっており、OSメンテナがdnfリポジトリからパッケージを削除している可能性があります。この場合、必要なkernel-devel .rpmパッケージをベンダーのOSアーカイブから手動でダウンロードして手動でインストールするか、カーネルをサポートされているバージョンに更新して上記のコマンドを再実行します。

例えば、CentOSを使用して配布でサポートされているバージョンにカーネルを更新できない場合、CentOS用の古いkernel-devel .rpmパッケージをhttp://vault.centos.orgから手動でダウンロードできます。ダウンロードするファイルの名前は、次のbashコマンドの出力によって示されます。

```
echo kernel-devel-$(uname -r).rpm
```

ダウンロードが完了したら、ダウンロードした.rpmファイルが保存されているディレクトリで次のbashコマンドを実行して、kernel-develパッケージをインストールできます。

```
dnf install -y kernel-devel-$(uname -r).rpm
```

Oracle Linux

Oracle Linuxでは、RHCKとUEKという2つの異なるカーネルが使用されています。kernel-develとkernel-uek-develパッケージは、それぞれRHCKとUEKの/usr/src/kernelディレクトリに必要なカーネル開発ヘッダファイルをインストールします。カーネル開発ファイルは、カーネルのバージョンに従って/usr/src/kernelに整理されています。

Oracle Linux RHCK

Oracle Linux RHCKで欠落しているカーネルパッケージを特定し、障害ID 11を解決する手順は、RHEL Linuxの手順と同じです。詳細については、上記のRHEL Linuxのセクションを参照してください。

Oracle Linux UEK

Oracle Linux UEKで見つからないカーネルパッケージを特定し、障害ID 11を解決する手順は、RHEL Linuxと似ていますが、同じではありません。詳細は上記のRHEL Linuxのセクションを参照してください。しかし、"kernel-devel"の全てのインスタンスを"kernel-uek-devel"に置き換えてください。 具体的には、関連するすべてのコマンドについて、`kernel-devel-$(uname -r)`をkernel-uek-devel-$(uname -r)に置き換えます。

注：必要なkernel-uek-devel .rpmパッケージがdnfリポジトリからインストールしようとしたときに見つからない場合は、https://yum.oracle.com/のOracleアーカイブからパッケージを手動でダウンロードしてインストールできます。

Debian/Ubuntu Linux

linux-headersパッケージは、必要なヘッダファイルをカーネルのバージョンに従って整理して/usr/srcディレクトリにインストールします。

原因

リアルタイムのファイルシステムおよびネットワークアクティビティの監視に必要なlinux-headersパッケージが欠落している。

/usr/srcディレクトリにインストールされているヘッダーを確認できます。

解決方法

linux-headersパッケージは、次のコマンドでインストールできます。

```
sudo apt install linux-headers-$(uname -r)
```

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。