SUSE Linux Secure Endpointの障害ID 11のトラブルシューティング

内容

概要

このドキュメントでは、解決するプロセスについて説明します Fault ID 11 / Secure Endpoint 日付： SUSE Linux Enterprise 15 SP2 .

要件

コマンドラインインターフェイス(CLI)は、システムのすべてのユーザに対して使用できますが、使用可能なコマンドはポリシー設定やルート権限によって異なります。これに依存するコマンドについては、この記事の全体を通して説明します。

次の項目に関する知識があることを推奨します。

- Linux Command Line
- Secure Endpoint

使用するコンポーネント

このドキュメントで使用する情報は、次のソフトウェアバージョンに基づくものです。

- Secure Endpoint 1.20
- SUSE Linux Enterprise 15 SP2 カーネルバージョン5.3.18-24.96-default

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

オン SUSE Linux Enterprise 15 Service Pack (SP) 2、カーネルバージョンが5.3.18以上の場合、connectorは eBPF リアルタイムのファイルシステムとネットワーク監視のためのモジュール。「 eBPF モジュー

ルはLinux Kernel モジュールは次の環境で実行される場合に使用されます。 RHEL 6, RHEL 7, Oracle Linux 7 RHCK, Oracle Linux 7 UEK 5 およびそれ以前 Amazon Linux 2 カーネル4.14以前。 を参照 Ubuntu 18.04以降 Debian 10 以降, eBPF モジュールはネイティブです。

適切な互換性を確保するために、コネクタは自動的に eBPF モジュールは、システム上でロードおよび実行される前にコネクタによって使用されます。このコンパイルには、現在のカーネル開発ヘッダファイルに対応する kernel-devel をインストールします。 リアルタイム filesystem ネットワークモニタリングが有効になっている場合、コネクタは eBPF モジュールは、コネクタが起動されるたびに、またはリアルタイムでこれらの機能が有効にされたときに、ポリシー更新の一部として実行されます。

システムが現在のカーネル開発パッケージを失うと、コネクタは障害ID 11: Realtime network and file monitoring is unavailableを生成します。現在実行中のカーネル用のkernel-develパッケージをインストールし、コネクタを再起動します。この障害の問題は、Linuxコネクタがデグレード状態で動作していることです。つまり、障害が解決されるまで期待どおりに動作しません。

トラブルシュート

障害11が発生すると、次のエラーログが表示されます。

- システムログでログ行を探します /var/log/messages これは次のようになります。

init: cisco-amp pre-start: AMP kernel modules are not required on this kernel version '5.3.18-24.96-default'; skipping reinstalling kernel modules

ログには、コンピュータ上の現在のカーネルバージョンがカーネルモジュールを使用していないことが示されています。 filesystem ネットワークモニタリングです4.18以上のカーネルバージョンでは、 filesystem ネットワークは次の方法で監視されます。 eBPF モジュール.

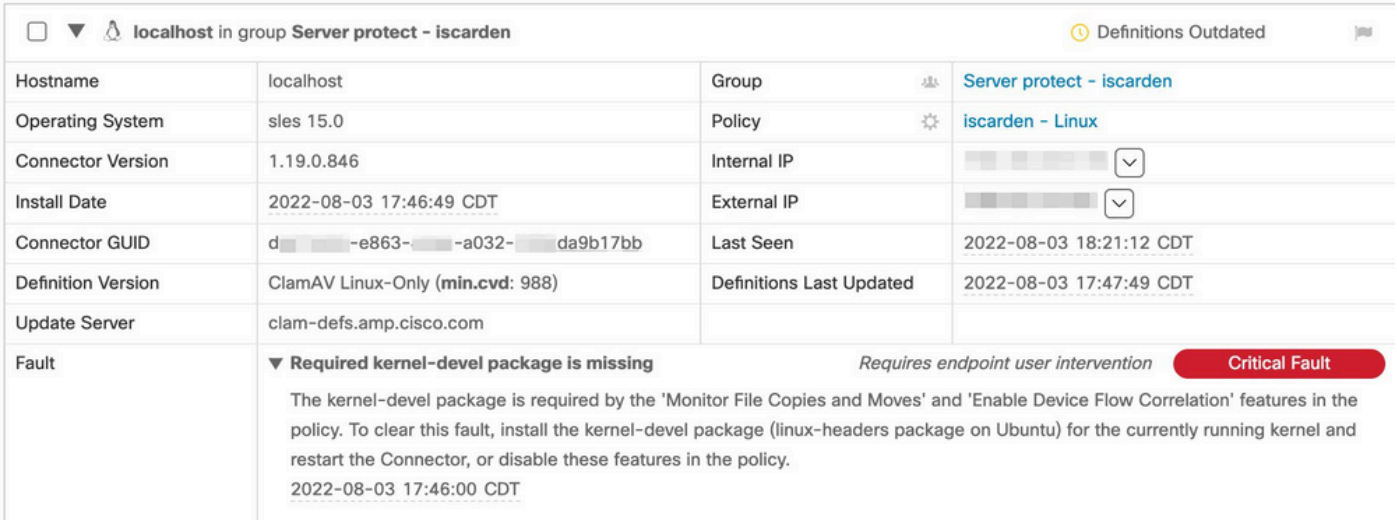
存在しないカーネルヘッダーの識別方法

コネクタがカーネルヘッダーのないコンピュータ上で動作している場合、 Fault ID 11 (Realtime network and file monitoring is unavailable)を使用すると、コネクタが機能低下状態で動作し、 filesystem ネットワークモニタリングです
これらの手順は、コネクタが接続されているかどうかを識別するために、ターミナルウィンドウから実行できます kernel-header が存在するかどうかを確認します。

ステップ 1：影響を受けるデバイスから、コネクタが次の状態であることを確認します。 Fault ID 11：

/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: 2022-08-03 06:31:42 PM Policy: iscarden - Linux (#22192) Command-line: Enabled Orbital: Disabled Faults: 1 Critical Fault IDs: 11 ID 11 - Critical: Realtime network and file monitoring is unavailable. Install the kernel-devel package for the currently running kernel, then, restart the Connector.

Secure Endpointコンソールから、影響を受けるデバイスを見つけ、詳細を展開してFaultセクションを確認します。



ステップ 2：次のコマンドを使用して、現在のカーネルを確認します。

$ uname -r 5.3.18-150200.24.115-default

ステップ 3：カーネルヘッダーがインストールされているかどうかを確認するには、次の手順を実行します。

zypper se -s kernel-default-devel | grep $(uname -r | sed "s/-default//") # zypper se -s kernel-devel | grep $(uname -r | sed "s/-default//")

出力は次のようになります。

```
isaac@localhost:~> zypper se -s kernel-default-devel | grep $(uname -r | sed "s/-default//")
i+ | kernel-default-devel | package | 5.3.18-24.96.1   | x86_64 | SLE-Module-Basesystem15-SP2-Updates
```

i+は、パッケージがインストールされていることを示します。左側の列が v または空白の場合は、パッケージをインストールする必要があります。

「 SUSE computerは、カーネルヘッダーのインストールに適しています（以下の条件をすべて満たす場合）。

- コネクタの障害IDは11です。
- 最小値 kernel バージョンは5.3.18です。
- 「 kernel ヘッダーがインストールされていません。

解決方法

If the SUSE マシンに必要なカーネルヘッダが存在しない場合は、この手続きを使ってマシンに必要なカーネルヘッダをインストールすることができます。

ステップ 1：必要なカーネルヘッダーをインストールします。

sudo zypper install --oldpackage kernel-default-devel=$(uname -r | sed 's/-default//') # sudo zypper install --oldpackage kernel-devel=$(uname -r | sed 's/-default//')

ステップ 2：コネクタを再起動します。

sudo systemctl stop cisco-amp # sudo systemctl start cisco-amp

ステップ 3：障害がクリアされたことを確認します。

/opt/cisco/amp/bin/ampcli # status Trying to connect... Connected. ampcli> status Status: Connected Mode: Normal Scan: Ready for scan Last Scan: 2022-08-05 01:29:47 PM Policy: iscarden - Linux (#22201) Command-line: Enabled Orbital: Disabled Faults: None ampcli > quit

確認

カーネルヘッダーがインストールされているかどうかを確認するには、次のコマンドを実行します。

zypper se -s kernel-default-devel | grep $(uname -r | sed "s/-default//") # zypper se -s kernel-devel | grep $(uname -r | sed "s/-default//")

回避策を実行する前に、次のような出力が表示されました。

```
isaac@localhost:~> zypper se -s kernel-default-devel | grep $(uname -r | sed 's/
-default//') $ zypper se -s kernel-devel | grep $(uname -r | sed 's/-default//')
isaac@localhost:~>
```

回避策を実行した後の出力は次のようになります。

```
isaac@localhost:~> zypper se -s kernel-default-devel | grep $(uname -r | sed "s/-default//")
i+ | kernel-default-devel | package | 5.3.18-24.96.1   | x86_64 | SLE-Module-Basesystem15-SP2-Updates
isaac@localhost:~> zypper se -s kernel-devel | grep $(uname -r | sed "s/-default//")
i | kernel-devel | package | 5.3.18-24.96.1   | noarch | SLE-Module-Basesystem15-SP2-Updates
isaac@localhost:~>
```

関連情報

- セキュアエンドポイントのLinuxコネクタのOS互換性の確認
- Linuxカーネル・デバイスの障害
- Cisco Secure Endpoint Linuxコネクタカーネルモジュールの構築

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。