Fehlerbehebung bei Fehler-ID 11 auf SUSE Linux Secure Endpoint

Inhalt

Einleitung

In diesem Dokument wird der zu behebende Prozess beschrieben. Fault ID 11 Secure Endpoint on SUSE Linux Enterprise 15 SP2 .

Anforderungen

Die Kommandozeile (CLI) steht allen Benutzern eines Systems zur Verfügung, obwohl die Verfügbarkeit einiger Befehle von der Richtlinienkonfiguration und/oder den Root-Berechtigungen abhängt. Die davon abhängigen Befehle sind in diesem Artikel beschrieben.

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Linux Command Line
- Secure Endpoint

Verwendete Komponenten

Die in diesem Dokument verwendeten Informationen basieren auf den folgenden Softwareversionen:

- Secure Endpoint 1.20
- SUSE Linux Enterprise 15 SP2 Kernel-Version 5.3.18-24.96-default

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Hintergrundinformationen

On SUSE Linux Enterprise 15 Service Pack (SP) 2 , mit Kernel-Versionen größer oder gleich 5.3.18,

Connector verwendet eBPF Module zur Echtzeit-Dateisystem- und Netzwerküberwachung. Die Fehlermeldung eBPF Module ersetzt das Linux Kernel Module, die bei der Ausführung auf RHEL 6, RHEL 7, Oracle Linux 7 RHCK, Oracle Linux 7 UEK 5 und früher, und Amazon Linux 2 Kernel 4.14 oder älter. für Ubuntu 18.04 und höher sowie Debian 10 und höher, eBPF -Module nativ sind.

Um die Kompatibilität zu gewährleisten, kompiliert der Connector automatisch die eBPF Module, die vom Steckverbinder vor dem Laden und Ausführen auf dem System verwendet werden. Diese Kompilierung erfordert, dass Kernel-Entwicklungsheader-Dateien, die der aktuellen kernel-devel installiert sind. Wenn Echtzeit filesystem und die Netzwerküberwachung aktiviert ist, kompiliert der Connector das eBPF Module bei jedem Start des Connectors oder bei Aktivierung dieser Funktionen in Echtzeit im Rahmen einer Richtlinienaktualisierung.

Wenn das System das aktuelle Paket kernel-devel verpasst, löst der Connector Fehler-ID 11 aus: Die Echtzeit-Netzwerk- und Dateiüberwachung ist nicht verfügbar. Installieren Sie das Paket kernel-devel für den aktuell laufenden Kernel und starten Sie dann den Connector neu. Das Problem mit diesem Fehler ist, dass der Linux-Connector in einem heruntergestuften Zustand ausgeführt wird, was bedeutet, dass er nicht wie erwartet funktioniert, bis der Fehler behoben ist.

Fehlerbehebung

Wenn Fehler 11 ausgelöst wird, erscheint dieses Fehlerprotokoll:

- Protokollzeilen im Systemprotokoll suchen /var/log/messages die ähnlich sind wie:

```
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
```

Das Protokoll besagt, dass die aktuelle Kernel-Version auf dem Computer keine Kernel-Module für filesystem und Netzwerküberwachung. Bei Kernel-Versionen größer oder gleich 4.18 wird die filesystem und das Netzwerk wird mithilfe von eBPF module.

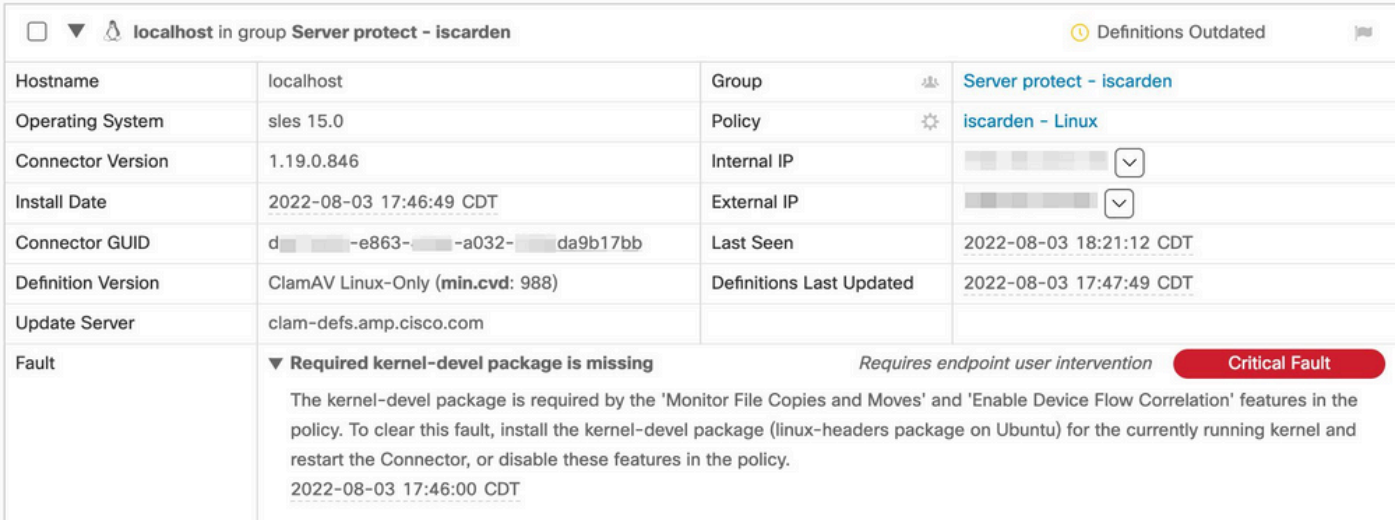
So identifizieren Sie fehlende Kernel-Header

Wenn der Connector auf einem Computer ohne Kernelheader ausgeführt wird, Fault ID 11 (Realtime network and file monitoring is unavailable), läuft der Steckverbinder in einem heruntergestuften Zustand ohne filesystem oder Netzwerküberwachung.
Diese Schritte können von einem Klemmenfenster aus durchgeführt werden, um festzustellen, ob der Steckverbinder kernel-header vorhanden ist oder nicht.

Schritt 1: Überprüfen Sie auf dem betroffenen Gerät, ob der Anschluss 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.
```

Suchen Sie in der Konsole für sichere Endgeräte nach dem betroffenen Gerät, und erweitern Sie die Details, um den Abschnitt Fehler zu überprüfen.



Schritt 2: Überprüfen Sie den aktuellen Kernel mit dem folgenden Befehl:

$ uname -r 5.3.18-150200.24.115-default

Schritt 3: So überprüfen Sie, ob die Kernal-Header installiert sind:

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

Die Ausgabe muss wie folgt aussehen:

```
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
```

Dabei bedeutet i+, dass das Paket installiert ist. Wenn die linke Spalte v oder **leer** ist, muss das Paket installiert werden.

Die Fehlermeldung SUSE Computer ist für die Installation von Kernel-Headern geeignet, wenn alle diese zutreffend sind:

- Der Anschluss hat die Fehler-ID 11.
- Das Minimum kernel Version 5.3.18.
- Die Fehlermeldung kernel Header sind nicht installiert.

Auflösung

Wenn die SUSE Maschine hat nicht die erforderlichen Kernel-Header, dann kann dieses Verfahren verwendet werden, um die erforderlichen Kernel-Header auf der Maschine zu installieren.

Schritt 1: Installieren Sie die erforderlichen Kernel-Header:

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

Schritt 2: Stecker neu starten:

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

Schritt 3: Bestätigen Sie, dass der Fehler gelöscht wurde:

/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

Überprüfung

Um zu überprüfen, ob die Kernel-Header jetzt installiert sind, führen Sie die folgenden Befehle aus:

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

Bevor Sie die Problemumgehung durchgeführt haben, hatten Sie eine Ausgabe wie diese:

```
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:~>
```

Nachdem Sie die Problemumgehung durchgeführt haben, muss die Ausgabe wie folgt aussehen:

```
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:~>
```

Zugehörige Informationen

- Überprüfung der Kompatibilität des sicheren Endpunkt-Linux-Connectors mit dem Betriebssystem
- Linux-Kernel-Devel-Fehler
- Erstellen von Cisco Secure Endpoint Linux Connector Kernel-Modulen

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.