SUSE Linux Secure Endpoint上的故障ID 11故障排除

目錄

簡介

本檔案將說明要解決的程式 Fault ID 第11個，共 Secure Endpoint 於 SUSE Linux Enterprise 15 SP2 .

需求

命令列介面(CLI)對於系統的所有使用者都可用，儘管某些命令的可用性取決於策略配置和/或根許可權。依賴於此的命令將在本文中介紹。

思科建議您瞭解以下主題：

- Linux Command Line
- Secure Endpoint

採用元件

文中使用的資訊是根據以下軟體版本：

- Secure Endpoint 1.20
- SUSE Linux Enterprise 15 SP2 核心版本5.3.18-24.96-default

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

於 SUSE Linux Enterprise 15 Service Pack (SP) 2，核心版本大於或等於5.3.18時，聯結器使用 eBPF 即時檔案系統和網路監控模組。其 eBPF 模組取代Linux Kernel 運行時使用的模組 RHEL 6, RHEL 7, Oracle Linux 7 RHCK, Oracle Linux 7 UEK 5 更早的時候 Amazon Linux 2 核心4.14或更低版本。 對於 Ubuntu 18.04及更高版本以及 Debian 10及更高版本， eBPF 模組是本地的。

為了獲得適當的相容性，聯結器自動編譯 eBPF 聯結器使用的模組，在系統上載入和運行這些模組之

前。此編譯要求核心開發標頭檔案與當前 kernel-devel 已安裝。 當即時 filesystem 啟用網路監控後，聯結器將編譯 eBPF 在每次啟動聯結器時或啟用這些功能時作為策略更新的一部分即時啟動模組。

當系統錯過當前核心級軟體包時，聯結器將引發「Fault ID 11: Realtime network and file monitoring is unavailable（故障ID 11：即時網路和檔案監控不可用）」。為當前運行的核心安裝核心級軟體包，然後重新啟動聯結器。此故障的問題在於Linux聯結器運行在降級狀態，這意味著在故障得到解決之前，聯結器無法按預期工作。

疑難排解

如果發生故障11，則會出現以下錯誤日誌：

- 在系統日誌中查詢日誌行 /var/log/messages 類似以下內容：

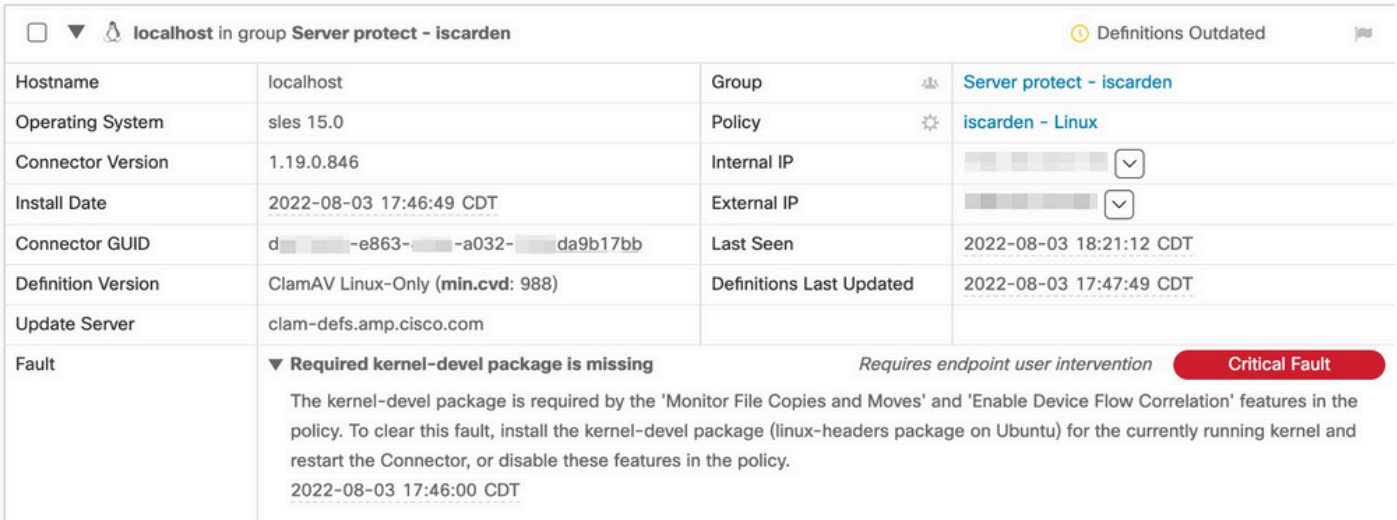
init: cisco-amp pre-start: AMP kernel modules are not required on this kernel version '5.3.18-24.96-default'; skipping reinstalling kernel modules
該日誌指出，電腦上的當前核心版本未將核心模組用於 filesystem 和網路監控。在大於或等於4.18的核心版本上， filesystem 和網路的監控使用 eBPF 模組.

如何識別缺少的核心報頭

在沒有核心標頭的電腦上運行時， Fault ID 11 (Realtime network and file monitoring is unavailable)，聯結器運行在降級狀態，而非 filesystem 或網路監控。
這些步驟可以從終端視窗執行，以便識別聯結器是否被連線 kernel-header 存在與否。

步驟1.在受影響的裝置上，驗證聯結器是否具有 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.
在安全終端控制檯中，找到受影響的裝置並展開詳細資訊以驗證「故障」部分。



步驟2.使用以下命令檢查當前核心：

$ uname -r 5.3.18-150200.24.115-default

步驟3.若要檢查是否已安裝核心標頭：

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

輸出必須如下所示：

```
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
```

其中i+表示軟體包已安裝。如果左邊的列是 v 或**空**，則必須安裝軟體包。

其 SUSE 如果以下所有情況均成立，則電腦適合安裝核心標頭：

- 聯結器的故障ID為11。
- 最小值 kernel 版本為5.3.18。
- 其 kernel 未安裝標頭。

解析

如果 SUSE 電腦沒有所需的核心標頭，則此過程可用於在電腦上安裝所需的核心標頭。

步驟1.安裝必要的核心標頭：

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

步驟2.重新啟動聯結器：

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

步驟3.確認故障已清除：

/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

驗證

若要驗證現在是否已安裝核心標頭，請運行以下命令：

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

執行解決方法之前，您有一個類似以下的輸出：

```
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:~>
```

執行解決方法後，輸出必須類似於以下內容：

```
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:~>
```

相關資訊

- 驗證安全終端Linux聯結器作業系統相容性
- Linux核心級故障
- 構建思科安全終端Linux聯結器核心模組

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。