SUSE Linux安全终端上的故障ID 11故障排除

目录

简介

本文档介绍要解决的流程 Fault ID 第11页 ，共 Secure Endpoint 在 SUSE Linux Enterprise 15 SP2 .

要求

命令行界面(CLI)对于系统的所有用户都可用，尽管某些命令的可用性取决于策略配置和/或根权限。依赖于此的命令将在本文中介绍。

Cisco 建议您了解以下主题：

- Linux Command Line
- Secure Endpoint

使用的组件

本文档中使用的信息基于以下软件版本：

- Secure Endpoint 1.20
- SUSE Linux Enterprise 15 SP2 内核版本5.3.18-24.96-default

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

开启 SUSE Linux Enterprise 15 Service Pack (SP) 2，内核版本大于或等于5.3.18，连接器使用 eBPF 实时文件系统和网络监控模块。此 eBPF 模块取代Linux Kernel 运行时使用的模块 RHEL 6, RHEL 7, Oracle Linux 7 RHCK, Oracle Linux 7 UEK 5 以及更早的时间， Amazon Linux 2 内核4.14或更低版本。 对于 Ubuntu 18.04及更高版本，以及 Debian 10及更高版本， eBPF 模块是本地的。

为获得适当的兼容性，连接器会自动编译 eBPF 连接器使用的模块，在系统上加载和运行这些模块之前。此编译要求内核开发头文件对应于当前的 kernel-devel 已安装。 当实时 filesystem 启用网络监控后，连接器将编译 eBPF 模块在每次启动连接器时或启用这些功能时作为策略更新的一部分实时启动。

当系统错过当前内核级软件包时，连接器将引发“故障ID 11：实时网络和文件监控不可用”(Fault ID 11: Realtime network and file monitoring is unavailable)。为当前运行的内核安装内核级软件包，然后重新启动连接器。此故障的问题在于Linux连接器以降级状态运行，这意味着在解决故障之前，它不会按预期工作。

故障排除

如果引发故障11，则会显示以下错误日志：

- 在系统日志中查找日志行 /var/log/messages 类似于以下内容：

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

日志声明计算机上的当前内核版本不将内核模块用于 filesystem 和网络监控。在大于或等于4.18的内核版本上， filesystem 并使用以下工具监控网络： eBPF 模块.

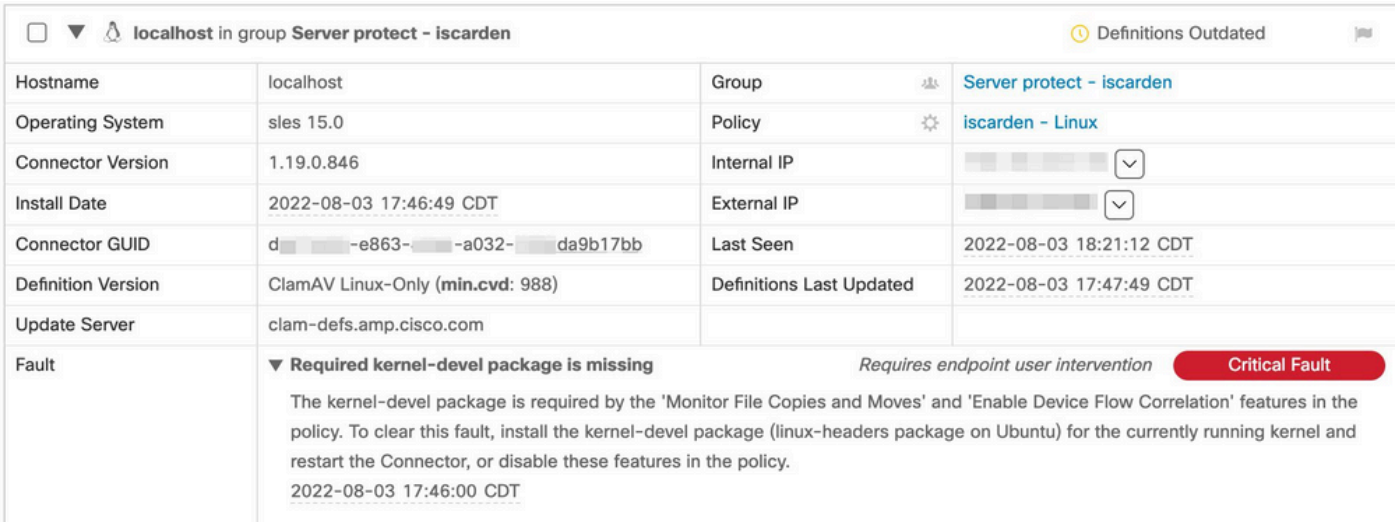
如何识别缺少的内核报头

当连接器在没有内核报头的计算机上运行时， Fault ID 11 (Realtime network and file monitoring is unavailable)，连接器在降级状态下运行，而 filesystem 或网络监控。
这些步骤可以从终端窗口执行，以便识别连接器是否处于连接状态 kernel-header 是否存在。

步骤1:从受影响的设备中，验证连接器是否具有 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.

在安全终端控制台中，找到受影响的设备并展开详细信息以验证Fault部分。



第二步：使用以下命令检查当前内核：

$ uname -r 5.3.18-150200.24.115-default

第三步：要检查内核报头是否已安装，请执行以下操作：

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

输出必须如下所示：

```
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+表示安装了该软件包。如果左侧列为 v 或者**空**，必须安装该软件包。

此 SUSE 如果以下所有情况均属实，则计算机适合安装内核报头：

- 连接器具有故障ID 11。
- 最小值 kernel 版本为5.3.18。
- 此 kernel 未安装信头。

分辨率

如果 SUSE 计算机没有所需的内核报头，则此过程可用于在计算机上安装所需的内核报头。

步骤1:安装必要的内核报头：

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

第二步：重新启动连接器：

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

第三步：确认故障已清除：

/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

验证

要验证现在是否安装了内核报头，请运行以下命令：

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

在执行该解决方法之前，您有一个类似下面的输出：

```
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:~>
```

执行此解决方法后，输出必须类似于以下内容：

```
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:~>
```

相关信息

- 验证安全终端Linux连接器操作系统兼容性
- Linux内核级故障
- 构建思科安全终端Linux连接器内核模块

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。