Resolución de problemas de Fault ID 11 en SUSE Linux Secure Endpoint

Contenido

Introducción

Este documento describe el proceso a resolver Fault ID 11 de Secure Endpoint encendido SUSE Linux Enterprise 15 SP2 .

Requirements

La interfaz de línea de comandos (CLI) está disponible para todos los usuarios de un sistema, aunque la disponibilidad de algunos comandos depende de la configuración de la directiva y/o de los permisos raíz. Los comandos que dependen de esto se divulgan a lo largo de este artículo.

Cisco recomienda que tenga conocimiento sobre estos temas:

- Linux Command Line
- Secure Endpoint

Componentes Utilizados

La información utilizada en el documento se basa en estas versiones de software:

- Secure Endpoint 1.20
- SUSE Linux Enterprise 15 SP2 kernel versión 5.3.18-24.96-default

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Encendido SUSE Linux Enterprise 15 Service Pack (SP) 2 , con versiones del núcleo mayores o iguales a 5.3.18, el conector utiliza eBPF módulos para monitorizar el sistema de archivos en tiempo real y la

red. eBPF reemplaza a Linux Kernel Módulos utilizados cuando se ejecuta en RHEL 6, RHEL 7, Oracle Linux 7 RHCK, Oracle Linux 7 UEK 5 y anteriores, y Amazon Linux 2 kernel 4.14 o anterior. Para Ubuntu 18.04 y posteriores, así como Debian 10 y posteriores, eBPF los módulos son nativos.

Para lograr una compatibilidad adecuada, el conector compila automáticamente el eBPF módulos utilizados por el conector antes de cargarlos y ejecutarlos en el sistema. Esta compilación requiere que los archivos de encabezado de desarrollo del núcleo correspondan a la versión actual kernel-devel están instalados. En tiempo real filesystem y la supervisión de red está habilitada, el conector compila el eBPF módulos cada vez que se inicia el conector o en tiempo real cuando se activan estas funciones, como parte de una actualización de políticas.

Cuando el sistema pierde el paquete kernel-devel actual, el conector genera Fault ID 11: La red en tiempo real y el monitoreo de archivos no están disponibles. Instale el paquete kernel-devel para el núcleo que se está ejecutando actualmente y, a continuación, reinicie el conector. El problema con esta falla es que el conector Linux se ejecuta en un estado degradado, lo que significa que no funciona como se esperaba hasta que se resuelve la falla.

Troubleshoot

Si se genera el error 11, aparece este registro de errores:

- Buscar líneas de registro en el registro del sistema /var/log/messages que son similares a esto:

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

El registro indica que la versión actual del núcleo en el equipo no utiliza módulos del núcleo para filesystem y supervisión de red. En las versiones del núcleo mayores o iguales que 4.18, el filesystem y la red se supervisan mediante el uso de eBPF módulos.

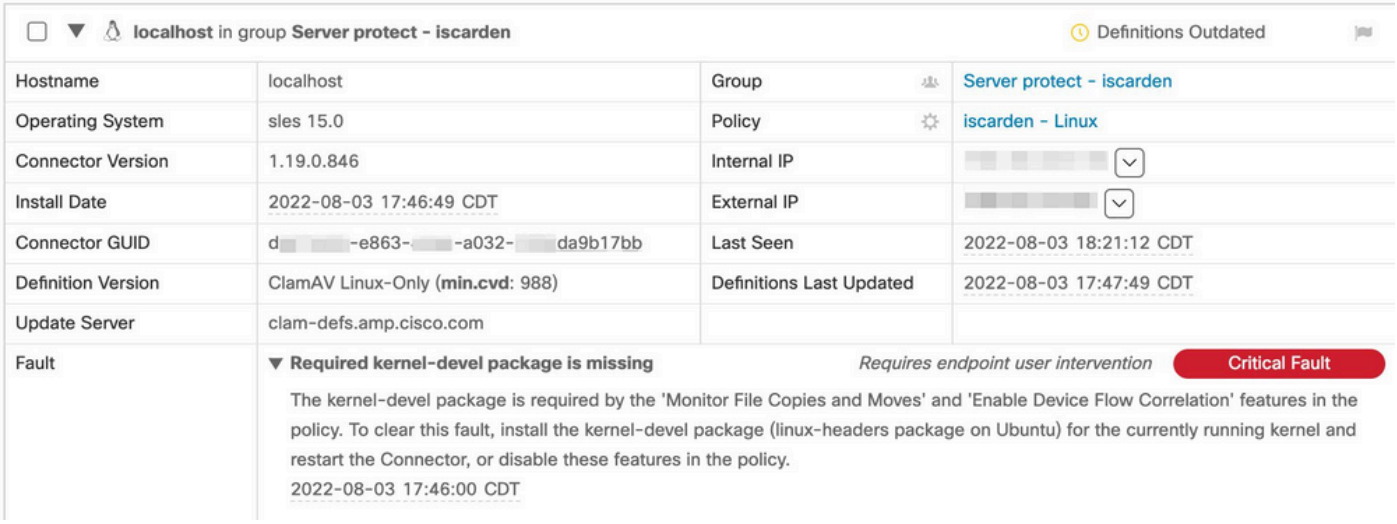
Cómo identificar encabezados de núcleo ausentes

Cuando el conector se ejecuta en un equipo sin encabezados de núcleo, Fault ID 11 (Realtime network and file monitoring is unavailable), el conector se ejecuta en un estado degradado sin filesystem o supervisión de red.
Estos pasos se pueden realizar desde una ventana de terminal para identificar si el conector kernel-header está presente o no.

Paso 1. En el dispositivo afectado, compruebe que el conector tiene 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.

Desde la consola de Secure Endpoint, busque el dispositivo afectado y expanda los detalles para verificar la sección Fault.



Paso 2. Verifique el núcleo actual con este comando:

$ uname -r 5.3.18-150200.24.115-default

Paso 3. Para verificar si los encabezados kernal están instalados o no:

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

El resultado debe ser similar al siguiente:

```
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
```

Donde i+ significa que el paquete está instalado. Si la columna de la izquierda es v o está **vacío**, el paquete debe estar instalado.

SUSE equipo es adecuado para la instalación de encabezados de kernel si todos estos son verdaderos:

- El conector tiene ID de fallo 11.
- El mínimo kernel versión es 5.3.18.
- kernel no están instalados.

Resolución

Si SUSE equipo no tiene los encabezados de kernel requeridos, entonces este procedimiento se puede utilizar para instalar los encabezados de kernel requeridos en el equipo.

Paso 1. Instale los encabezados del núcleo necesarios:

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

Paso 2. Reinicie el conector:

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

Paso 3. Confirme que se ha borrado el fallo:

/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

Verificación

Para verificar si los encabezados del núcleo están instalados, ejecute estos comandos:

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

Antes de realizar la solución alternativa, tenía un resultado similar a este:

```
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:~>
```

Después de realizar la solución alternativa, el resultado debe ser similar a este:

```
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:~>
```

Información Relacionada

- Verifique la compatibilidad del sistema operativo del conector de Linux de terminal seguro
- Falla de Linux Kernel-Devel
- Creación de módulos del núcleo del conector de Linux de Cisco Secure Endpoint

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).