Identificação e solução de problemas de falha 11 no ponto de extremidade seguro do SUSE Linux

Contents

Introduction

Este documento descreve o processo a ser resolvido Fault ID 11 de Secure Endpoint ligado SUSE Linux Enterprise 15 SP2 .

Requirements

A interface de linha de comando (CLI) está disponível para todos os usuários de um sistema, embora a disponibilidade de alguns comandos dependa da configuração da política e/ou das permissões raiz. Os comandos que dependem disso são divulgados em todo este artigo.

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Linux Command Line
- Secure Endpoint

Componentes Utilizados

As informações usadas no documento são baseadas nestas versões de software:

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Ligado SUSE Linux Enterprise 15 Service Pack (SP) 2 , com versões de kernel maiores ou iguais a 5.3.18, o conector usa eBPF módulos para monitoramento de rede e sistema de arquivos em tempo real. O eBPF módulos substitui o Linux Kernel Módulos usados quando executado em RHEL 6, RHEL 7, Oracle

Linux 7 RHCK, Oracle Linux 7 UEK 5 e anteriores, e Amazon Linux 2 kernel 4.14 ou anterior. Para Ubuntu 18.04 e seguintes, bem como Debian 10 e posterior, eBPF os módulos são nativos.

Para obter a compatibilidade adequada, o conector compila automaticamente o eBPF módulos usados pelo conector antes que ele os carregue e execute no sistema. Esta compilação requer que os arquivos de cabeçalho de desenvolvimento do kernel correspondam ao atual kernel-devel estão instalados. Quando em tempo real filesystem e o monitoramento de rede estiver ativado, o conector compilará o eBPF módulos sempre que o conector é iniciado, ou em tempo real quando esses recursos são ativados, como parte de uma atualização de política.

Quando o sistema perde o pacote kernel-devel atual, o conector levanta a ID de falha 11: A rede em tempo real e o monitoramento de arquivos não estão disponíveis. Instale o pacote kernel-devel para o kernel atualmente em execução e reinicie o Conector. O problema com essa falha é que o conector Linux é executado em um estado degradado, o que significa que ele não funciona como esperado até que a falha seja resolvida.

Troubleshoot

Se a falha 11 for gerada, este log de erros será exibido:

- Procurar linhas de log no log do sistema /var/log/messages que são semelhantes a:

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

O log indica que a versão atual do kernel no computador não usa módulos do kernel para filesystem e monitoramento de rede. Nas versões do kernel maiores ou iguais a 4.18, o filesystem e a rede são monitorados com o uso de eBPF módulos.

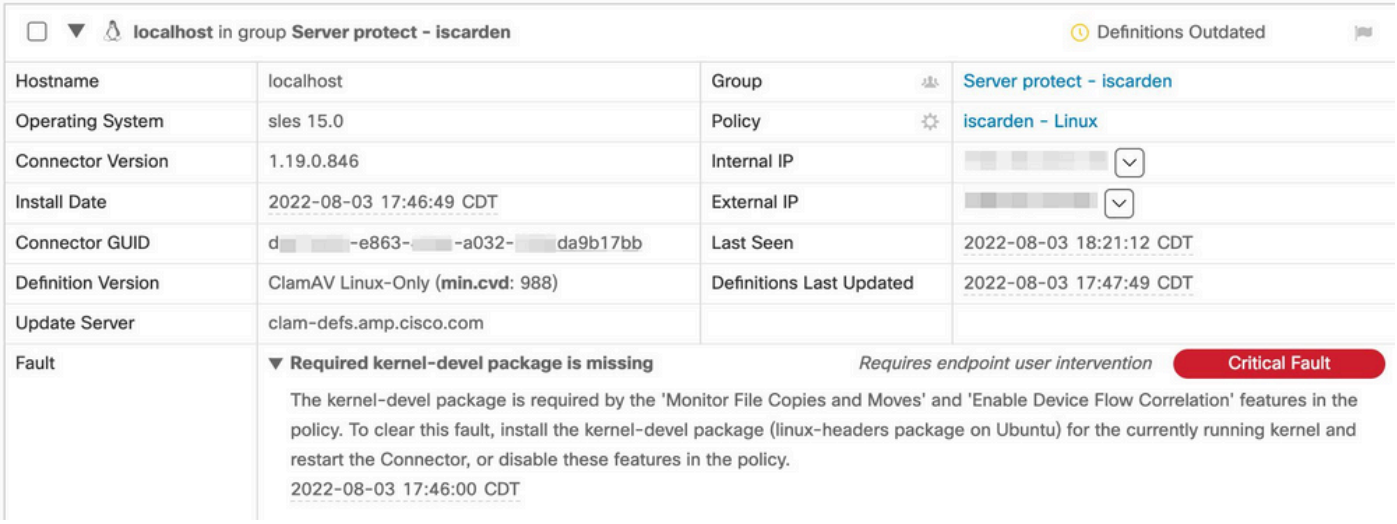
Como identificar cabeçalhos de kernel ausentes

Quando o conector é executado em um computador sem cabeçalhos do kernel, Fault ID 11 (Realtime network and file monitoring is unavailable), o conector é executado em estado degradado sem filesystem ou monitoramento de rede.
Essas etapas podem ser executadas em uma janela de terminal para identificar se o conector kernel-header está presente ou não.

Etapa 1. A partir do dispositivo afetado, verifique se o conector tem 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.

No console do Secure Endpoint, localize o dispositivo afetado e expanda os detalhes para verificar a seção Fault.



Etapa 2. Verifique o kernel atual com este comando:

$ uname -r 5.3.18-150200.24.115-default

Etapa 3. Para verificar se os cabeçalhos do kernal estão instalados ou não:

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

A saída deve ser assim:

```
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
```

Onde i+ significa que o pacote está instalado. Se a coluna da esquerda for v ou estiver **em branco**, o pacote deve ser instalado.

O SUSE o computador é adequado para a instalação de cabeçalhos do kernel se todos estes forem verdadeiros:

- O conector tem o ID de falha 11.
- O mínimo kernel versão é 5.3.18.
- O kernel os cabeçalhos não estão instalados.

Resolução

Se a SUSE a máquina não tem os cabeçalhos do kernel necessários, então este procedimento pode ser usado para instalar os cabeçalhos do kernel necessários na máquina.

Etapa 1. Instale os cabeçalhos do kernel necessários:

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

Etapa 2. Reinicie o conector:

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

Etapa 3. Confirme se a falha foi eliminada:

/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

Verificar

Para verificar se os cabeçalhos do kernel estão instalados agora, execute estes 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 executar a solução, você tinha uma saída semelhante a esta:

```
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:~>
```

Depois de executar a solução, a saída deve ser semelhante a esta:

```
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:~>
```

Informações Relacionadas

- Verificar Compatibilidade do Sistema Operacional do Conector Linux de Ponto de Extremidade Seguro
- Falha no nível de kernel do Linux
- Construindo Módulos Kernel do Conector Linux para Cisco Secure Endpoint

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.