Dépannage de l'ID de panne 11 sur le terminal sécurisé SUSE Linux

Table des matières

Introduction

Ce document décrit le processus de résolution Fault ID 11 sur Secure Endpoint activé SUSE Linux Enterprise 15 SP2 .

Exigences

L'interface de ligne de commande (CLI) est disponible pour tous les utilisateurs d'un système, bien que la disponibilité de certaines commandes dépend de la configuration de la stratégie et/ou des autorisations racine. Les commandes qui en dépendent sont décrites tout au long de cet article.

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Linux Command Line
- Secure Endpoint

Composants utilisés

Les informations utilisées dans le document sont basées sur les versions logicielles suivantes :

- Secure Endpoint 1.20
- SUSE Linux Enterprise 15 SP2 version du noyau 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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

On (activé) SUSE Linux Enterprise 15 Service Pack (SP) 2, avec des versions de noyau supérieures ou égales à 5.3.18, le connecteur utilise eBPF pour la surveillance en temps réel des systèmes de fichiers et du réseau. Les eBPF remplace le module Linux Kernel Modules utilisés lors de son

exécution sur RHEL 6, RHEL 7, Oracle Linux 7 RHCK, Oracle Linux 7 UEK 5 et plus tôt, et Amazon Linux 2 noyau 4.14 ou antérieur. Pour Ubuntu 18.04 et versions ultérieures, ainsi que Debian 10 ans et plus, eBPF sont natifs.

Pour une bonne compatibilité, le connecteur compile automatiquement les eBPF modules utilisés par le connecteur avant son chargement et son exécution sur le système. Cette compilation nécessite que les fichiers d'en-tête de développement du noyau qui correspondent au kernel-devel sont installés. En temps réel filesystem et que la surveillance du réseau est activée, le connecteur compile eBPF modules chaque fois que le connecteur est démarré, ou en temps réel lorsque ces fonctionnalités sont activées, dans le cadre d'une mise à jour de stratégie.

Lorsque le paquet kernel-devel actuel manque au système, le connecteur déclenche l'ID de panne 11 : le réseau en temps réel et la surveillance des fichiers ne sont pas disponibles. Installez le paquet kernel-devel pour le noyau en cours d'exécution, puis redémarrez le connecteur. Le problème avec ce défaut est que le connecteur Linux fonctionne dans un état dégradé, ce qui signifie qu'il ne fonctionne pas comme prévu jusqu'à ce que le défaut soit résolu.

Dépannage

Si le défaut 11 est déclenché, ce journal d'erreurs apparaît :

- Rechercher des lignes de journal dans le journal système /var/log/messages qui sont similaires à ceci :

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

Le journal indique que la version actuelle du noyau sur l'ordinateur n'utilise pas de modules de noyau pour filesystem et la surveillance du réseau. Sur les versions du noyau supérieures ou égales à 4.18, le filesystem et réseau sont surveillés à l'aide de eBPF modules.

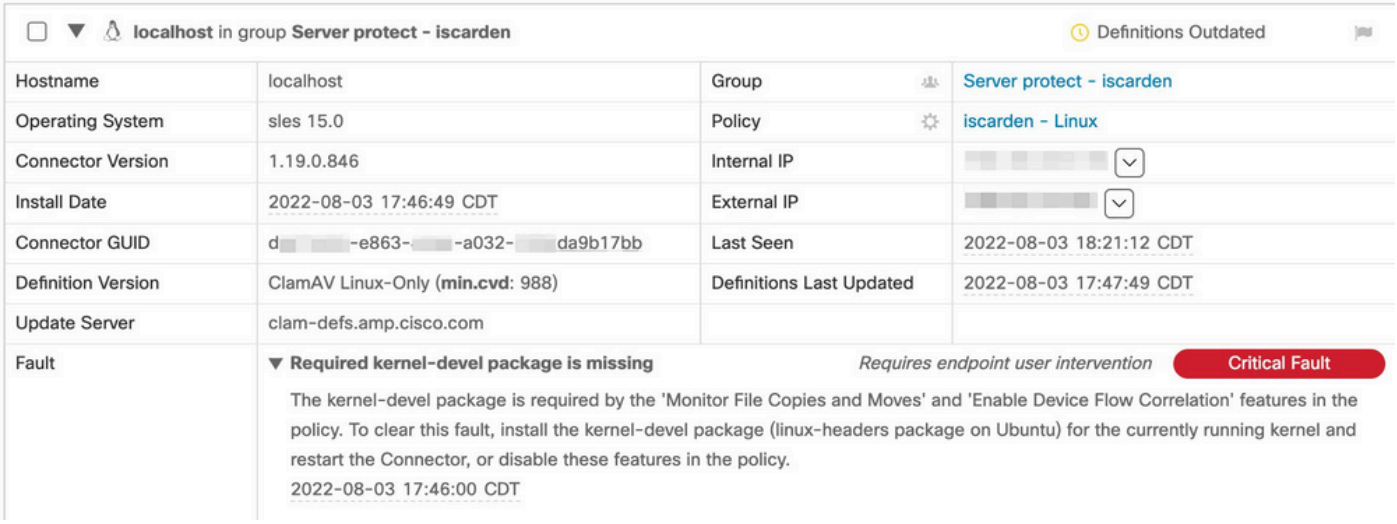
Comment identifier les en-têtes de noyau absents

Lorsque le connecteur fonctionne sur un ordinateur sans en-tête de noyau, Fault ID 11 (Realtime network and file monitoring is unavailable), le connecteur fonctionne dans un état dégradé sans filesystem ou la surveillance du réseau.
Ces étapes peuvent être effectuées à partir d'une fenêtre de borne afin d'identifier si le connecteur kernel-header est présent ou non.

Étape 1. À partir du périphérique concerné, vérifiez que le connecteur a 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.

Àpartir de la console Secure Endpoint, recherchez le périphérique concerné et développez les détails pour vérifier la section Fault.



Étape 2. Vérifiez le noyau actuel avec cette commande :

$ uname -r 5.3.18-150200.24.115-default

Étape 3. Afin de vérifier si les en-têtes du noyau sont installés ou non :

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

Le résultat doit être le suivant :

```
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
```

Où i+ signifie que le package est installé. Si la colonne de gauche est v ou est **vide**, le package doit être installé.

Les SUSE L'ordinateur est approprié pour l'installation des en-têtes de noyau si toutes ces conditions sont vraies :

- Le connecteur a l'ID de panne 11.
- Le minimum kernel version 5.3.18.
- Les kernel les en-têtes ne sont pas installés.

Résolution

Si la SUSE n'a pas les en-têtes de noyau requis, alors cette procédure peut être utilisée pour installer les en-têtes de noyau requis sur la machine.

Étape 1. Installez les en-têtes de noyau nécessaires :

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

Étape 2. Redémarrez le connecteur :

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

Étape 3. Confirmez que la panne est résolue :

/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

Vérifier

Afin de vérifier si les en-têtes du noyau sont maintenant installés, exécutez ces commandes :

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

Avant d'effectuer la solution de contournement, vous obteniez un résultat similaire à celui-ci :

```
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:~>
```

Après avoir effectué la solution de contournement, le résultat doit être similaire à celui-ci :

```
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:~>
```

Informations connexes

- Vérifier la compatibilité du système d'exploitation du connecteur Linux Secure Endpoint
- Défaillance du noyau Linux
- Création de modules de noyau de connecteur Linux pour terminal sécurisé Cisco

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.