Resolver falla de política SELinux del conector Linux

Contenido

Introducción

Este documento describe la falla que se genera cuando la política SELinux en el sistema impide que el conector monitoree la actividad del sistema.

Antecedentes

El conector requiere esta regla en la política Secure Enterprise Linux (SELinux) si SELinux está habilitado y en modo de aplicación:

```
allow unconfined_service_t self:bpf { map_create map_read map_write prog_load prog_run };
```

Esta regla no está presente en la política predeterminada de SELinux en sistemas basados en Red Hat. El conector intenta agregar esta regla a través de la instalación de un módulo de políticas de SELinux llamado `cisco-secure-bpf durante una instalación o actualización`. El fallo se genera si `Cisco-Secure-BPF` no se puede instalar y cargar, o está deshabilitado. Se notifica al usuario un Fault 19 como se describe en la lista de Cisco Secure Endpoint Linux Connector Faults si el conector provoca este fallo.

Aplicabilidad

Este fallo puede ser provocado después de una nueva instalación o actualización del Conector, o después de modificar la política SELinux del sistema.

Sistemas operativos

- Red Hat Enterprise Linux 7
- CentOS 7
- Oracle Linux (RHCK/UEK) 7

Versiones del conector

- Linux 1.2.0 y versiones posteriores

Resolución

Hay dos métodos para resolver este error:

1. Vuelva a instalar o actualice el conector.
2. Modifique manualmente la política de SELinux.

Reinstale o actualice el conector

Un módulo de políticas de SELinux llamado `cisco-secure-bpf` está instalado para proporcionar la modificación de la política de SELinux requerida durante una instalación o actualización del conector. Realice una reinstalación o actualización estándar del conector para este método de resolución.

Modificar manualmente la política de SELinux

Un administrador del sistema debe crear y cargar manualmente un módulo de política SELinux para modificar la política SELinux. Realice estos pasos para cargar la regla de política de SELinux requerida:

1. Guarde esto en un archivo llamado `cisco-secure-bpf.te`

```
module cisco-secure-bpf 1.0;
require {
type unconfined_service_t;
class bpf { map_create map_read map_write prog_load prog_run };
}
#============= unconfined_service_t ==============
allow unconfined_service_t self:bpf { map_create map_read map_write prog_load prog_run };â€‹
```

2. Genere y cargue el módulo con estos comandos.

```
checkmodule -M -m -o "cisco-secure-bpf.mod" "cisco-secure-bpf.te"
semodule_package -o "cisco-secure-bpf.pp" -m "cisco-secure-bpf.mod"
semodule -i "cisco-secure-bpf.pp"
```

3. Reinicie el conector para borrar el error.

Los comandos usados para construir y cargar el módulo de políticas de SELinux requieren el uso del paquete `policies-coreutils-python` y sus dependencias. Ejecute este comando para instalar este paquete.

```
yum install policycoreutils-python
```

Verificar la modificación de la política de SELinux

Ejecute este comando para verificar si el módulo de política `Cisco-secure-bpf` SELinux está instalado.

```
semodule -l | grep cisco-secure-bpf
```

La modificación de la política de SELinux se ha producido si la salida informa "`cisco-secure-bpf 1.0`".

Ejecute este comando para verificar si la regla de política SELinux requerida está presente.

```
sesearch -A | grep "unconfined_t unconfined_t : bpf"
```

El fallo se borra después de reiniciar el conector si la salida informa "`allow unconfined_service_t self:bpf { map_create map_read map_write prog_load prog_run };`".

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).