Resolver falha de política SELinux do conector Linux

Contents

Introdução

Este documento descreve a falha levantada quando a política SELinux no sistema impede que o conector monitore a atividade do sistema.

Informações de Apoio

O conector exige esta regra na política do Secure Enterprise Linux (SELinux) se o SELinux estiver habilitado e no modo de imposição:

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

Esta regra não está presente na política padrão do SELinux em sistemas baseados no Red Hat. O conector tenta adicionar essa regra através da instalação de um módulo de política SELinux chamado `cisco-secure-bpf durante uma instalação ou atualização`. A falha é gerada se `cisco-secure-bpf` falha ao instalar e carregar ou está desabilitado. O usuário é notificado sobre uma Falha 19, conforme descrito na lista de [Falhas do Conector do Cisco Secure Endpoint Linux](#), se essa falha for ocasionada pelo conector.

Aplicabilidade

Essa falha pode ser gerada após uma nova instalação ou atualização do Connector, ou após a modificação da política SELinux do sistema.

Sistemas operacionais

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

Versões do conector

- Linux 1.22.0 e posterior

Resolução

Há dois métodos para resolver essa falha:

1. Reinstalar ou atualizar o conector.
2. Modificar manualmente a política do SELinux.

Reinstalar ou atualizar o conector

Um módulo de política SELinux chamado `cisco-secure-bpf` O está instalado para fornecer a modificação de política do SELinux necessária durante uma instalação ou atualização do conector. Execute uma reinstalação ou atualização padrão do conector para este método de resolução.

Modificar manualmente a política do SELinux

Um administrador do sistema deve criar e carregar manualmente um módulo de política do SELinux para modificar a política do SELinux. Execute estas etapas para carregar a regra de política SELinux necessária:

1. Salve-o em um arquivo chamado `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. Construa e carregue o módulo usando estes 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 o Conector para eliminar a falha.

Os comandos usados para construir e carregar o módulo de política SELinux requerem o uso do pacote `policycoreutils-python` e suas dependências. Execute este comando para instalar este pacote.

```
yum install policycoreutils-python
```

Verificar a modificação da política do SELinux

Execute este comando para verificar se o módulo de política `cisco-secure-bpf` SELinux está instalado.

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

A modificação da política do SELinux ocorreu se a saída relatar "`cisco-secure-bpf 1.0`".

Execute este comando para verificar se a regra de política SELinux necessária está presente.

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

A falha será eliminada após o conector ser reiniciado se a saída informar "`allow unconfined_service_t self:bpf { map_create map_read map_write prog_load prog_run };`".

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.