

# 解决Linux连接器SELinux策略故障

## 目录

[简介](#)

[背景信息](#)

[适用范围](#)

[操作系统](#)

[连接器版本](#)

[分辨率](#)

[安装依赖关系](#)

[重新安装或升级连接器](#)

[手动修改SELinux策略](#)

[验证SELinux策略修改](#)

## 简介

本文档介绍当系统上的SELinux策略阻止连接器监视系统活动时引起的故障。

## 背景信息

如果启用了SELinux并处于实施模式，则连接器要求此规则在Secure Enterprise Linux(SELinux)策略中：

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

此规则在基于Red Hat的系统的默认SELinux策略中不存在。在安装或升级期间，连接器尝试通过安装名为cisco-secure-bpf的SELinux策略模块来添加此规则。如果出现以下情况，则会引发故障cisco-secure-bpf无法安装和加载，或者已禁用。如果连接器引发此故障，则会按照[Cisco Secure Endpoint Linux Connector Faults](#)列表中的说明通知用户发生故障19。

## 适用范围

在重新安装或升级连接器后，或修改系统的SELinux策略后，可能会发生此故障。

## 操作系统

- Red Hat Enterprise Linux 7
- CentOS 7

- Oracle Linux(RHCK/UEK)7

## 连接器版本

- Linux 1.22.0及更高版本

## 分辨率

有两种方法可以解决此故障：

1. 重新安装或升级连接器。
2. 手动修改SELinux策略。

## 安装依赖关系

这两种方法都要求系统上安装“policycoreutils-python”软件包来构建和加载SELinux策略模块。运行此命令可安装此软件包。

```
yum install policycoreutils-python
```

## 重新安装或升级连接器

名为cisco-secure-bpf的SELinux策略模块 在安装或升级连接器期间，将安装以提供所需的SELinux策略修改。按照标准重新安装或升级此解析方法的连接器。

## 手动修改SELinux策略

系统管理员必须手动构建和加载SELinux策略模块才能修改SELinux策略。执行以下步骤以加载所需的SELinux策略规则：

1. 将此文件保存在名为cisco-secure-bpf.te的文件中

```
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 };
```

2. 使用这些命令构建和加载模块。

```
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. 重新启动连接器以清除故障。

## 验证SELinux策略修改

运行此命令以检查是否安装了cisco-secure-bpf SELinux策略模块。

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

如果输出报告“cisco-secure-bpf 1.0”，则发生SELinux策略修改。

运行此命令以检查是否存在所需的SELinux策略规则。

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

如果输出报告“allow unconfined\_service\_t self:bpf { map\_create map\_read map\_write prog\_load prog\_run };”，则故障在连接器重新启动后清除。

## 关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。