# LinuxコネクタSELinuxポリシー障害の解決

## 内容



## 概要

このドキュメントでは、システムのSELinuxポリシーによってコネクタがシステムアクティビティをモニタできなくなったときに発生する障害について説明します。

## 背景説明

SELinuxが有効で強制モードの場合、コネクタは、このルールがSecure Enterprise Linux(SELinux)ポリシーに含まれていることを要求します。

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

このルールは、Red Hatベースのシステムのデフォルトの SELinuxポリシーには存在しません。コネクタは、インストールまたはアップグレード時に`cisco-secure-bpf`という名前のSELinuxポリシーモジュールをインストールすることによってこのルールの追加を試みます。 このエラーは、次の場合に発生します Ciscoセキュア BPF インストールおよびロードに失敗したか、無効になっています。 このエラーがコネクタによって発生すると、Cisco Secure Endpoint Linuxコネクタの障害のリストに記載されているように、ユーザに障害19が通知されます。

## 適用性

このエラーは、コネクタの新規インストールまたはアップグレード後、またはシステムのSELinuxポリシーの変更後に発生する可能性があります。

### オペレーティング システム

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

### コネクタバージョン

- Linux 1.22.0以降

## 解決方法

このエラーを解決するには、次の2つの方法があります。

1. コネクタを再インストールまたはアップグレードします。
2. SELinuxポリシーを手動で変更します。

### 依存関係のインストール

どちらの方法でも、SELinuxポリシーモジュールを構築してロードするために、システムに「policycoreutils-python」パッケージをインストールする必要があります。このパッケージをインストールするには、次のコマンドを実行します。

```
yum install policycoreutils-python
```

### コネクタの再インストールまたはアップグレード

`cisco-secure-bpf`という名前のSELinuxポリシーモジュール は、コネクタのインストールまたはアップグレード時に必要なSELinuxポリシーの変更を行うためにインストールされます。この解決方法に従って、コネクタの標準の再インストールまたはアップグレードを実行します。

### SELinuxポリシーの手動変更

SELinuxポリシーを変更するには、システム管理者がSELinuxポリシーモジュールを手動で構築してロードする必要があります。必要なSELinuxポリシールールをロードするには、次の手順を実行します。

1. これを`cisco-secure-bpf.te`という名前のファイルに保存します

```
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. 次のコマンドを使用して、モジュールを構築してロードします。

```
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. コネクタを再起動して障害をクリアします。

## SELinuxポリシーの変更を確認する

このコマンドを実行して、cisco-secure-bpf SELinuxポリシーモジュールがインストールされているかどうかを確認します。

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

出力に「cisco-secure-bpf 1.0」が表示される場合、SELinuxポリシーの変更が発生していますを参照。

このコマンドを実行して、必要なSELinuxポリシールールが存在するかどうかを確認します。

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

出力に「allow unconfinded_service_t self:bpf { map_create map_read map_write prog_load prog_run };」と表示される場合、コネクタの再起動後に障害がクリアされます。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。