解決Linux聯結器SELinux策略故障

目錄

簡介

本文描述當系統上的SELinux策略阻止聯結器監視系統活動時出現的故障。

背景資訊

如果啟用了SELinux並在實施模式下，則聯結器要求此規則位於Secure Enterprise Linux(SELinux)策略中：

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

基於Red Hat的系統上的預設SELinux策略中不存在此規則。在安裝或升級過程中，聯結器會嘗試通過安裝名為`cisco-secure-bpf`的SELinux策略模組來新增此規則。 如果出現以下情況，則會引發故障`cisco-secure-bpf` 無法安裝和載入，或已被禁用。 如果聯結器引發此故障，則會按照Cisco Secure Endpoint Linux Connector Faults清單中的說明通知使用者發生故障19。

適用性

在重新安裝或升級聯結器之後，或修改系統的SELinux策略之後，可能會引發此故障。

作業系統

- Red Hat Enterprise Linux 7
- CentOS 7

- Oracle Linux(RHCK/UEK)7

聯結器版本

- Linux 1.22.0及更高版本

解析

有兩種方法可以解決此故障：

1. 重新安裝或升級聯結器。
2. 手動修改SELinux策略。

安裝依賴項

這兩種方法都要求系統上安裝「policycoreutils-python」軟體包來構建和載入SELinux策略模組。運行此命令以安裝此程式包。

```
yum install policycoreutils-python
```

重新安裝或升級聯結器

名為cisco-secure-bpf的SELinux策略模組 在安裝或升級聯結器的過程中，將安裝以提供所需的SELinux策略修改。為此解析方法執行聯結器標準重新安裝或升級。

手動修改SELinux策略

系統管理員必須手動構建和載入SELinux策略模組才能修改SELinux策略。執行以下步驟以載入所需的SELinux策略規則：

1. 將此內容儲存在名為cisco-secure-bpf.te的檔案中

```
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. 使用這些命令構建和載入模組。

```
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. 重新啟動聯結器以清除故障。

驗證SELinux策略修改

運行此命令以檢查是否安裝了cisco-secure-bpf SELinux策略模組。

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

如果輸出報告「cisco-secure-bpf 1.0」，則會發生SELinux策略修改.

運行此命令以檢查是否存在所需的SELinux策略規則。

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

如果輸出報告「allow unconded_service_t self:bpf { map_create map_read map_write prog_load prog_run }；」，則聯結器重新啟動後故障會清除。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。