Linux Connector SELinux-Richtlinienfehler beheben

Inhalt

Einleitung

Dieses Dokument beschreibt den Fehler, der ausgelöst wird, wenn die SELinux-Richtlinie auf dem System verhindert, dass der Connector die Systemaktivität überwacht.

Hintergrundinformationen

Der Connector erfordert diese Regel in der Secure Enterprise Linux (SELinux)-Richtlinie, wenn SELinux aktiviert ist, und im Erzwingungsmodus:

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

Diese Regel ist in der SELinux-Standardrichtlinie auf Red Hat-basierten Systemen nicht vorhanden. Der Connector versucht, diese Regel durch die Installation eines SELinux-Richtlinienmoduls mit dem Namen `cisco-secure-bpf während einer Installation oder eines Upgrades`. Der Fehler wird ausgelöst, wenn `cisco-secure-bpf` kann nicht installiert und geladen werden oder ist deaktiviert. Der Benutzer wird über einen Fehler 19, wie in der Liste der Cisco Secure Endpoint Linux Connector-Fehler beschrieben, informiert, wenn dieser Fehler durch den Connector ausgelöst wird.

Geltungsbereich

Dieser Fehler kann nach einer Neuinstallation oder einem Upgrade des Connectors oder nach einer Änderung der SELinux-Richtlinie des Systems ausgelöst werden.

Betriebssysteme

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

Anschlussvarianten

- Linux 1.2.0 und höher

Auflösung

Es gibt zwei Möglichkeiten, diesen Fehler zu beheben:

1. Installieren Sie den Steckverbinder neu, oder aktualisieren Sie ihn.
2. Ändern Sie die SELinux-Richtlinie manuell.

Installieren Sie den Anschluss neu, oder aktualisieren Sie ihn.

Ein SELinux-Richtlinienmodul mit dem Namen `cisco-secure-bpf` wird installiert, um die erforderliche Änderung der SELinux-Richtlinie während einer Installation oder eines Upgrades des Connectors bereitzustellen. Führen Sie für diese Auflösungsmethode eine standardmäßige Neuinstallation oder Aktualisierung des Steckverbinders durch.

Ändern Sie die SELinux-Richtlinie manuell.

Ein Systemadministrator muss manuell ein SELinux-Richtlinienmodul erstellen und laden, um die SELinux-Richtlinie zu ändern. Führen Sie diese Schritte aus, um die erforderliche SELinux-Richtlinienregel zu laden:

1. Speichern Sie das Paket in der Datei `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. Erstellen und laden Sie das Modul mit diesen Befehlen.

```
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. Starten Sie den Connector neu, um den Fehler zu beheben.

Die Befehle, die zum Erstellen und Laden des SELinux-Richtlinienmoduls verwendet werden, erfordern die Verwendung des `policycoreutils-python`-Pakets und seiner Abhängigkeiten. Führen Sie diesen Befehl aus, um dieses Paket zu installieren.

```
yum install policycoreutils-python
```

Überprüfung der Änderung der SELinux-Richtlinie

Führen Sie diesen Befehl aus, um zu überprüfen, ob das Richtlinienmodul `cisco-secure-bpf` SELinux installiert ist.

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

Die Änderung der SELinux-Richtlinie ist erfolgt, wenn die Ausgabe "`cisco-secure-bpf 1.0" meldet.`.

Führen Sie diesen Befehl aus, um zu überprüfen, ob die erforderliche SELinux-Richtlinienregel vorhanden ist.

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

Der Fehler wird nach dem Neustart des Connectors gelöscht, wenn die Ausgabe folgende Meldung ausgibt: "`allow unrestricted_service_t self:bpf { map_create map_read map_write prog_load prog_run };".`

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.