**Diagnose and address routine SELinux policy violations.**

**Introduction**

In **RHEL 7**, each package doesn’t store its own **SELinux** policy. The **SELinux** policy is stored in one and only one package called **selinux-policy-targeted**.

When a policy has been written for a given process and **SELinux** is in **Permissive** or **Enforcing** mode, all action not allowed by the **SELinux** policy will trigger a violation.

The following procedure will give you some details about any **SELinux** policy violation.

**Main Procedure**

Install the **setroubleshoot-server** package:

# yum install -y setroubleshoot-server

Note: In fact, it’s the **policycoreutils-python** package that really contains the **semanage** command. However, I have always found the **setroubleshoot-server** package name, that contains the **policycoreutils-python** package itself, easier to remember!

Display the **SELinux** policy violations:

# sealert -a /var/log/audit/audit.log

In addition, when an **AVC** (**A**ccess **V**ector **C**ache) event occurs, you can grab the associated line displayed in the **/var/log/audit/audit.log** file and send it to the **audit2why** command to get a diagnostic.

For example, let’s assume you’ve got this line in your **/var/log/audit/audit.log** file:

type=AVC msg=audit(**1415714880.156:29**): avc: denied { name\_connect } for pid=1349 \

comm="nginx" dest=8080 scontext=unconfined\_u:system\_r:httpd\_t:s0 \

tcontext=system\_u:object\_r:http\_cache\_port\_t:s0 tclass=tcp\_socket

Execute this command to get a diagnostic:

# **grep 1415714880.156:29 /var/log/audit/audit.log | audit2why**

Was caused by:

One of the following booleans was set incorrectly.

Description:

Allow httpd to act as a relay

Allow access by executing:

# setsebool -P httpd\_can\_network\_relay 1

Description:

Allow HTTPD scripts and modules to connect to the network using TCP.

Allow access by executing:

# setsebool -P httpd\_can\_network\_connect 1

This will make your investigation much easier!