15.8.4 SELinux Troubleshooting Facts

This lesson covers the following topics:

- Analyzing and troubleshooting SELinux context violations
- SELinux Troubleshooting Tools

Analyzing and Troubleshooting SELinux Context Violations

As a network administrator, you will often be required to analyze and troubleshoot SELinux violations. SELinux violations are logged when an SELinux policy rule has been violated. SELinux violations are recorded as AVC (Access Vector Cache) event errors and are stored in the audit.log files (audit.log, audit.log.1, audit.log.2, etc.), These audit log files are saved in the /var/log/audit directory.

To locate these errors, you can search through the log files looking for 'type=ACV'. For example, as a root user or using **sudo**, you could use the **cat** command to display the contents of the log file. To see only ACV errors, you can pipe the result to grep as follows:

```
cat /var/log/audit/audit.log | grep type=AVC
```

Result:

```
type=AVC msg=audit (1543359698.852:262): avc: denied { create } for pid=5136
comm="gdm-session-wor" name="gdm" scontext=system_u:system_r:xdm_t:s0-s0:c0.c1023
tcontext=system_u:object_r:admin_home_t:s0 tclass=dir
```

One method of analyzing these errors is to simply read the error and determine the offending source and target. As an example, from the error above you can determine the following:

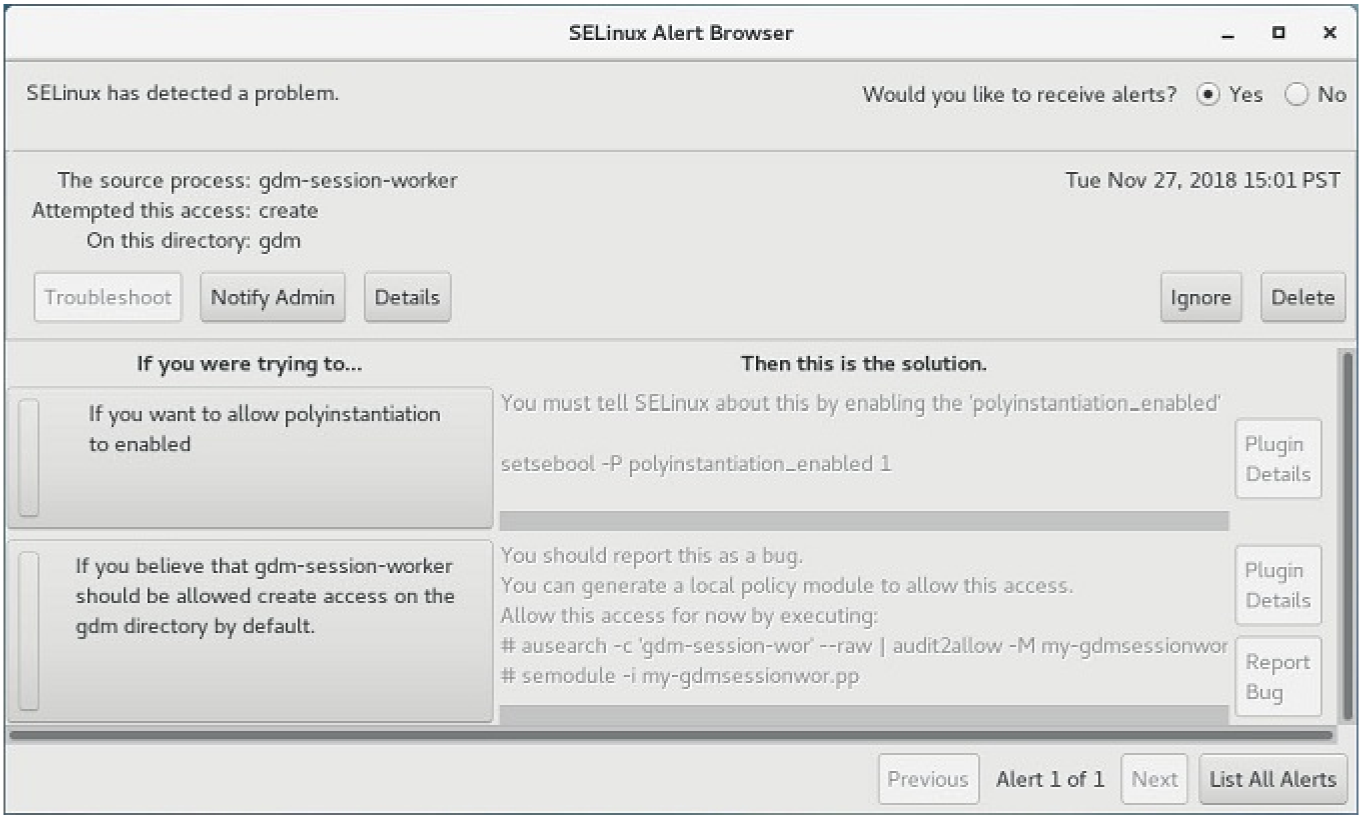
Result	Description
type=AVC	Indicates this is an SELinux error.
avc: denied { create }	A command to create something was denied.
pid=5136	The offending processor id was 5136.
comm="gdm-session-wor"	The command issued was 'gdm-session-wor'. (This is the pam authentication backend for both the login process and the screensaver process.)
name=“gdm”	gmd is the abbreviation for GNOME.
scontext=	The source context for the error was:

	• system_u (a system account user) • system_r (a system account role) • xdm_t (the type, e.g. the display manager)
tcontext=	The target context for the error was: • system_u (user) • object_r (role) • admin_home_t (type) • s0 tclass=dir (level)

SELinux Troubleshooting Tools

To aid in troubleshooting SELinux errors, you can also install additional tools. Perhaps the most common tool is semanage. Semanage is installed as part of the policycoreutils-python package. On Centos 7, this can be installed by running: **yum install -y setroubleshoot-server**

Once installed, you can view SELinux errors by running the semanage command **sealert** (SELinux Alert). Sealert can be run from the command line or from the GUI (if installed) and will aid you in determining the cause of the error and any possible solutions. When run from the GUI, you will see something similar to the following:



SELinux Alert Browser

SELinux has detected a problem.

Would you like to receive alerts? ● Yes ○ No

The source process: gdm-session-worker
Attempted this access: create
On this directory: gdm

Tue Nov 27, 2018 15:01 PST

If you were trying to...	Then this is the solution.
If you want to allow polyinstantiation to enabled	You must tell SELinux about this by enabling the 'polyinstantiation_enabled' setsebool -P polyinstantiation_enabled 1
If you believe that gdm-session-worker should be allowed create access on the gdm directory by default.	You should report this as a bug. You can generate a local policy module to allow this access. Allow this access for now by executing: # ausearch -c 'gdm-session-wor' --raw | audit2allow -M my-gdmsessionwor # semodule -i my-gdmsessionwor.pp

Alert 1 of 1

To run from the command line run: **sealert -a /var/log/audit/audit.log**

Sample output:

```
SELinux is preventing /usr/libexec/gdm-session-worker from create access on the
directory gdm.
***** Plugin catchall_boolean (89.3 confidence) suggests ******************

If you want to allow polyinstantiation to enabled
Then you must tell SELinux about this by enabling the 'polyinstantiation_enabled'
boolean.

Do
setsebool -P polyinstantiation_enabled 1

***** Plugin catchall (11.6 confidence) suggests **************************

If you believe that gdm-session-worker should be allowed create access on the gdm
directory by default.
Then you should report this as a bug.
You can generate a local policy module to allow this access.

Do
allow this access for now by executing:
# ausearch -c 'gdm-session-wor' --raw | audit2allow -M my-gdmsessionwor
# semodule -i my-gdmsessionwor.pp


Additional Information:
Source Context system_u:system_r:xdm_t:s0-s0:c0.c1023
Target Context system_u:object_r:admin_home_t:s0
Target Objects gdm [ dir ]
Source gdm-session-wor
Source Path /usr/libexec/gdm-session-worker
Port <Unknown>
Host <Unknown>
Source RPM Packages gdm-3.26.2.1-5.el7.x86_64
Target RPM Packages
Policy RPM selinux-policy-3.13.1-192.el7.noarch
Selinux Enabled True
Policy Type targeted
Enforcing Mode Enforcing
Host Name Centos
```

Platform Linux Centos 3.10.0-862.el7.x86_64 #1 SMP Fri Apr
20 16:44:24 UTC 2018 x86_64 x86_64
Alert Count 1
First Seen 2018-11-27 15:01:38 PST
Last Seen 2018-11-27 15:01:38 PST
Local ID ddff0dcb-b6bd-442a-a33a-eece5a7c8f7f

Raw Audit Messages

```
type=AVC msg=audit(1543359698.852:262): avc: denied { create } for pid=5136
comm="gdm-session-wor" name="gdm" scontext=system_u:system_r:xdm_t:s0-
s0:c0.c1023 tcontext=system_u:object_r:admin_home_t:s0 tclass=dir

type=SYSCALL msg=audit(1543359698.852:262): arch=x86_64 syscall=mkdir
success=no exit=EACCES a0=5576cee45890 a1=1c0 a2=5576cee458a0 a3=2 items=0
ppid=5104 pid=5136 auid=0 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0
tty=(none) ses=7 comm=gdm-session-wor exe=/usr/libexec/gdm-session-worker
subj=system_u:system_r:xdm_t:s0-s0:c0.c1023 key=(null)
```

Hash: gdm-session-wor,xdm_t,admin_home_t,dir,create