SELinux configuration for Pandora FMS

SELinux configuration for Pandora FMS

Introduction

In Pandora FMS the installation should always be done with Security-Enhanced Linux (SELinux) deactivated. After the installation and due to the need to have it enabled in some environments, we're going to detail the configuration settings in CentOS 7.

CentOS 7

Audit2allow installation

CentOS 7 will soon reach its end of life (EOL). *This documentation is retained for historical purposes.*

To create this type of rules use Audit2allow, which will be in charge of allowing the necessary actions.

Before you start creating the rules for the policies, you may need to install a number of packages to be able to use Audit2allow. enter in the command terminal with root or equivalent rights (prefix the command with sudo):

```
yum install selinux-policy-devel -y
yum install policycoreutils-python -y
```

Location of SELinux directory

CentOS 7 will soon reach its end of life (EOL). *This documentation is retained for historical purposes.*

Errors returned by SELinux could be locate in the route bellow:

- /var/www/html/pandora_console/log/audit.log
- /var/log/messages

IMPORTANT:

In versions prior to 747, the audit log path is: /var/log/audit/audit.log.

If updating from OUM you will need to modify the logrotate file.

In order to check the cleanest way, we highly recomend to remove previous logs and wait until it are generated again with new records.

Stop syslog (This service could be called rsyslog too):

```
# /etc/init.d/syslog stop
```

Remove audit.log and system message log file.

```
# rm /var/www/html/pandora_console/log/audit.log /var/log/messages
```

And start it again:

```
# /etc/init.d/syslog start
```

SELinux configuration

CentOS 7 will soon reach its end of life (EOL). *This documentation is retained for historical purposes.*

To configure SELinux with the desired value, we will modify its configuration file:

```
# This file controls the state of SELinux on the system.
# SELinux= can take one of these three values:
#     enforcing - SELinux security policy is enforced.
#     permissive - SELinux prints warnings instead of enforcing.
#     disabled - No SELinux policy is loaded.
SELinux=enforcing
# SELinuxTYPE= can take one of these two values:
#     targeted - Targeted processes are protected,
#     mls - Multi Level Security protection.
SELinuxTYPE=targeted
```

We will set SELinux to “enforcing” in order to execute in a restrictive way (check audit.log for denied executions by SELinux). The other option is to set SELinux to “permissive”, it won't block executions and it will record errors in the audit.log file.

Locate entries to create policies rules

CentOS 7 will soon reach its end of life (EOL). *This documentation is retained for historical purposes.*

To show the last input logs, execute:

```
# tail -f /var/www/html/pandora_console/log/audit.log /var/log/messages
```

You can notice some errors like:

```
 # type=AVC msg=audit(1431437562.755:437): avc:  denied  { write } for  pid=1835
comm="httpd" name="collections" dev=dm-0 ino=266621
scontext=unconfined_u:system_r:httpd_t:s0
tcontext=system_u:object_r:var_spool_t:s0 tclass=dir
```

To convert these errors in SELinux rules:

```
 # grep collections /var/www/html/pandora_console/log/audit.log | audit2allow -M
pandora
```

After this, 2 new files will be created:

```
 - pandora.pp
 - pandora.te
```

To activate the new rule, we will execute:

```
# sudo semodule -i pandora.pp
```

Repeat the process to add missed rules. After this, SELinux will stop reporting errors.

Needed rules for proper working of Pandora FMS

CentOS 7 will soon reach its end of life (EOL). *This documentation is retained for historical purposes.*

If you want that Pandora FMS execute all services properly, you will have to create some rules for the following operations:

- Create, update and delete collections.
- Send e-mails by programmed tasks (Cronjob).
- Agent remote config.

The other way, SELinux will block any accion associated to this operations.

In order to join all rules in one and use Pandora FMS with SELinux enabled, it will be:

```
 # grep -e data_in -e collections -e var_spool_t -e zip -e md5 -e denied
/var/www/html/pandora_console/log/audit.log| audit2allow -M pandora
```

After that you will have to repeat the step above to enable the rule.

```
# sudo semodule -i pandora.pp
```

Go back to Pandora FMS documentation index