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 its installation, and due to the need to have it activated in some environments, the configuration settings for different GNU/Linux distributions are detailed.

Rocky Linux 8

Audit2allow installation

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

Before starting to create the rules for the policies, you may need to install a number of packages in order to use Audit2allow.

Enter in the command terminal with root key or equivalent rights (prefix the command sudo):

```
dnf install selinux-policy-devel -y
dnf install policycoreutils-python-utils -y
```

Location of the SELinux log directory

The errors returned by SELinux can be found in the following paths:

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

In case of updating Pandora FMS by OUM you should modify the logrotate file corresponding.

To check more clearly what SELinux blocks, it is recommended to delete the previous *logs* and wait for them to be generated again with new records.

syslog must be stopped (this service could also be called rsyslog). Enter in the command terminal

with root key or equivalent rights (prefix the command sudo):

```
systemctl stop syslog
```

The `audit.log` and the *log* system messages file must be deleted:

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

Restart syslog (this service could also be called rsyslog):

```
systemctl start syslog
```

SELinux configuration

To configure SELinux to the desired value, modify its configuration file `/etc/selinux/config`:

```
# 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
```

- If you need SELinux to run in restrictive mode, allowing to execute only what appears within the module rules, you must set it to `enforcing`, thus removing (through the `audit.log`) the executions denied by SELinux.
- If instead you need to print warnings (*warnings*) instead of blocking actions, leave them `permissive`, and then check these *warnings* in the `audit.log` file.

Locate the entries for the creation of policy rules

To display the latest *logs* entries, enter the command terminal with root key or equivalent rights (prefix the command with sudo):

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

You may notice that errors will be displayed:

```
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 into rules that SELinux can interpret, you must execute:

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

This will create two files in the current directory:

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

To activate the new rule, execute:

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

Repeat the process to add the missing rules. After adding all the rules, SELinux will stop reporting errors.

Necessary rules for the correct operation of Pandora FMS

For Pandora FMS to be able to execute all the services correctly, rules should be created for the following features:

- Create, update and delete collections.
- Sending e-mail messages using scheduled tasks (Cronjob).
- Remote agent configuration.
- Monitoring snmptrapd.
- Monitoring NetFlow.

Otherwise, SELinux will block any action associated with these features.

A way to unite all these rules in one, to be able to use Pandora FMS completely, would be:

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

Then you should repeat the step described above to activate the rule. This would cover all possible conflicts between Pandora FMS and SELinux. Enter in the command terminal with root key or equivalent rights (prefix the command sudo):

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

Practical summary

The rules to use SELinux with Pandora FMS are summarized, *taking into account that for each particular case the values and parameters should be changed in a customized way* such as `dev=sdaX` or `pid=XXX`.

The setsebool command is a tool for setting *booleans* for SELinux. The `-P` option indicates to persist the set value across restarts, and the 1 at the end of the instruction indicates true value, thus activating your application. Enter in the command terminal with root key or equivalent rights (prefix the command sudo):

```
setsebool -P httpd_unified 1
setsebool -P httpd_read_user_content 1
setsebool -P httpd_can_network_connect 1
setsebool -P httpd_execmem 1
setsebool -P httpd_can_network_connect_db 1
setsebool -P httpd_can_connect_ldap 1
setsebool -P authlogin_nsswitch_use_ldap 1
setsebool -P nis_enabled 1
setsebool -P httpd_setrlimit 1
```

The chcon command changes the SELinux context of files. The `-t` option indicates a SELinux file type and the `-R` option applies it to a directory and all its contents recursively. Enter in the command terminal with root key or equivalent rights (prefix the command sudo):

```
chcon -R -t httpd_sys_content_rw_t /var/www/html/pandora
chcon -R -t httpd_sys_content_rw_t /var/spool/pandora/
chcon -R -t httpd_sys_content_rw_t /tmp/
```

The following rules are added, always remembering the necessary customization for each case. Enter in the command terminal with root key or equivalent rights (prefix the command sudo):

```
echo 'type=AVC msg=audit(1709637797.944:2074063): avc:  denied  { write } for
pid=176072 comm="php-fpm" name="collections" dev="sda5" ino=142704842
scontext=system_u:system_r:httpd_t:s0 tcontext=system_u:object_r:var_spool_t:s0
tclass=dir permissive=1' | audit2allow -a
echo 'type=AVC msg=audit(1709639101.328:2100929): avc:  denied  { unlink } for
pid=152354 comm="php-fpm" name="gotty_cron_tmp.log" dev="sda5" ino=134725871
scontext=system_u:system_r:httpd_t:s0 tcontext=system_u:object_r:user_home_t:s0
tclass=file permissive=1'  | audit2allow -a
echo 'type=AVC msg=audit(1710850539.491:32359350): avc:  denied  { write } for
pid=3895348 comm="connection" name="tmp" dev="sda5" ino=8398230
scontext=system_u:system_r:mysqld_t:s0
tcontext=system_u:object_r:httpd_sys_rw_content_t:s0 tclass=dir permissive=1' |
audit2allow -a
```

The following command is used to create the rules in a file named `rules_apply.pp`:

```
audit2allow -a -M rules_apply
```

The rules created in the previous step with the semodule command are applied:

```
semodule -i rules_apply.pp
```

Back to Pandora FMS Documentation Index