Configuración de SELinux para Pandora FMS

Configuración de SELinux para Pandora FMS

Introducción

En Pandora FMS la instalación se debe realizar siempre con Security-Enhanced Linux (SELinux) desactivado. Tras su instalación, y ante la necesidad de tenerlo activado en algunos entornos, se detallan los ajustes de configuración para diferentes distribuciones de GNU/Linux.

Rocky Linux 8

Instalación de Audit2allow

Para crear este tipo de reglas se utiliza Audit2allow, el cual será el encargado de permitir las acciones necesarias.

Antes de comenzar con la creación de las reglas para las políticas es posible que se necesite instalar una serie de paquetes para poder utilizar Audit2allow.

Introduzca en la terminal de comandos con clave de root o derechos equivalentes (anteponga el comando sudo):

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

Localización del directorio log de SELinux

Los errores que devuelve SELinux se pueden encontrar en las siguientes rutas:

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

En caso de actualizar Pandora FMS por OUM se deberá modificar el archivo logrotate correspondiente.

Para comprobar de una forma más clara lo que bloquea SELinux, se recomienda borrar los *logs* anteriores y esperar a que se vuelvan a generar con nuevos registros.

Se debe detener syslog (este servicio también podría llamarse rsyslog). Introduzca en la terminal de comandos con clave de root o derechos equivalentes (anteponga el comando sudo):

```
systemctl stop syslog
```

Se debe borrar `audit.log` y el archivo *log* de mensajes del sistema:

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

Iniciar de nuevo syslog (este servicio también podría llamarse rsyslog):

```
systemctl start syslog
```

Configuración de SELinux

Para configurar SELinux con el valor deseado, se modifica su fichero de configuración `/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
```

- Si se necesita que SELinux se ejecute en modo restrictivo, dejando ejecutar solamente lo que aparece dentro de las reglas de los módulos, se debe configurar a `enforcing`, sacando así (mediante el `audit.log`) las ejecuciones denegadas por SELinux.
- Si por el contrario se necesita que imprima las advertencias (*warnings*) en lugar de bloquear las acciones se dejará en `permissive`, y luego comprobar estos *warnings* en el archivo `audit.log`.

Localizar las entradas para la creación de las reglas de las políticas

Para visualizar las últimas entradas de los *logs* introduzca en la terminal de comandos con clave de root o derechos equivalentes (anteponga el comando sudo):

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

Se podrá observar que saldrán errores, por ejemplo:

```
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
```

Para convertir estos errores en reglas que SELinux pueda interpretar se debe ejecutar:

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

Esto creará dos ficheros en el directorio actual:

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

Para activar la nueva regla se debe ejecutar:

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

Se debe repetir el proceso para añadir las reglas que falten. Después de añadir todas las reglas, SELinux dejará de reportar errores.

Reglas necesarias para el correcto funcionamiento de Pandora FMS

Para que Pandora FMS pueda ejecutar todos los servicios correctamente, se deberán crear reglas para las siguientes funcionalidades:

- Crear, actualizar y borrar colecciones.
- Enviar mensajes de correo electrónico mediante las tareas programadas (Cronjob).
- Configuración remota de los agentes.
- Monitorización snmptrapd.
- Monitorización NetFlow.

De otra forma, SELinux bloqueará cualquier acción asociada a estas funcionalidades.

Una forma de unir todas estas reglas en una sola, para poder usar Pandora FMS totalmente, sería:

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

Luego se debe repetir el paso descrito arriba para activar la regla. Con se abarcarían todos los posibles conflictos entre Pandora FMS y SELinux. Introduzca en la terminal de comandos con clave de root o derechos equivalentes (anteponga el comando sudo):

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

Resumen práctico

Se resumen las reglas para utilizar SELinux con Pandora FMS *teniendo muy en cuenta que para cada caso en particular se deberán cambiar los valores y parámetros de manera personalizada* tales como `dev=sdaX` o `pid=XXX`.

El comando setsebool es una herramienta para establecer *booleanos* para SELinux. La opción `-P` indica que persista el valor ajustado a través de reinicios, y el `1` al final de la instrucción indica valor verdadero, activando así su aplicación. Introduzca en la terminal de comandos con clave de root o derechos equivalentes (anteponga el comando 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
```

El comando chcon cambia el contexto SELinux de los ficheros. La opción `-t` indica un tipo de fichero SELinux y la opción `-R` lo aplica a un directorio y todo su contenido de manera recursiva. Introduzca en la terminal de comandos con clave de root o derechos equivalentes (anteponga el comando 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/
```

Se agregan las siguientes reglas, recordando siempre las personalizaciones necesarias para cada caso. Introduzca en la terminal de comandos con clave de root o derechos equivalentes (anteponga el comando 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
```

Se utiliza el siguiente comando para crear las reglas en un fichero llamado `rules_apply.pp`:

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

Se aplican las reglas creadas en el paso anterior con el comando semodule:

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

CentOS 7

Instalación de Audit2allow

CentOS 7 pronto alcanzará su fin de ciclo de vida (EOL). *Esta documentación se conserva por propósitos históricos.*

Para crear este tipo de reglas se utiliza Audit2allow, el cual será el encargado de permitir las acciones necesarias.

Antes de empezar con la creación de las reglas para las políticas es posible que se necesite instalar una serie de paquetes para poder utilizar Audit2allow.

Introduzca en la terminal de comandos con clave de root o derechos equivalentes (anteponga el comando sudo):

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

Localización del directorio log de SELinux

Los errores que devuelve SELinux se pueden encontrar en las siguientes rutas:

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

En versiones anteriores a la 747, el fichero `audit.log` se encuentra en `/var/log/audit/audit.log`.

En caso de actualizar por OUM se deberá modificar el archivo logrotate correspondiente.

Para comprobar de una forma más clara lo que bloquea SELinux, se recomienda borrar los *logs* anteriores y esperar a que se vuelvan a generar con nuevos registros.

Se debe detener syslog (este servicio también podría llamarse rsyslog). Introduzca en la terminal de comandos con clave de root o derechos equivalentes (anteponga el comando sudo):

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

Se debe borrar `audit.log` y el archivo *log* de mensajes del sistema:

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

Iniciar de nuevo syslog (este servicio también podría llamarse rsyslog):

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

Configuración de SELinux

CentOS 7 pronto alcanzará su fin de ciclo de vida (EOL). *Esta documentación se conserva por propósitos históricos*.

Para configurar SELinux con el valor deseado, se modifica su archivo de configuración:

```
# 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
```

- Si se necesita que SELinux se ejecute en modo restrictivo, dejando ejecutar solamente lo que aparece dentro de las reglas de los módulos, se debe configurar a `enforcing`, sacando así (mediante el `audit.log`) las ejecuciones denegadas por SELinux.
- Si por el contrario se necesita que imprima las advertencias (*warnings*) en lugar de bloquear las acciones se dejará en `permissive`, y luego comprobar estos *warnings* en el archivo `audit.log`.

Localizar las entradas para la creación de las reglas de las políticas

CentOS 7 pronto alcanzará su fin de ciclo de vida (EOL). *Esta documentación se*

conserva por propósitos históricos.

Para visualizar las últimas entradas de los *logs* introduzca en la terminal de comandos con clave de root o derechos equivalentes (anteponga el comando sudo):

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

Se podrá observar que saldrán errores, por ejemplo:

```
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
```

Para convertir estos errores en reglas que SELinux pueda interpretar se debe ejecutar:

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

Esto creará dos ficheros en el directorio actual:

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

Para activar la nueva regla se debe ejecutar:

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

Se debe repetir el proceso para añadir las reglas que falten. Después de añadir todas las reglas, SELinux dejará de reportar errores.

Reglas necesarias para el correcto funcionamiento de Pandora FMS

CentOS 7 pronto alcanzará su fin de ciclo de vida (EOL). *Esta documentación se conserva por propósitos históricos*.

Para que Pandora FMS pueda ejecutar todos los servicios correctamente, se deberán crear reglas para las siguientes funcionalidades:

- Crear, actualizar y borrar colecciones.
- Enviar *e-mails* mediante las tareas programadas (Cronjob).
- Configuración remota de los agentes.

De otra forma, SELinux bloqueará cualquier acción asociada a estas funcionalidades.

Una forma de unir todas estas reglas en una sola, para poder usar Pandora FMS totalmente, sería:

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

Luego se debe repetir el paso descrito arriba para activar la regla. Con se abarcarían todos los posibles conflictos entre Pandora FMS y SELinux. Introduzca en la terminal de comandos con clave de root o derechos equivalentes (anteponga el comando sudo):

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

Volver al índice de documentación de Pandora FMS