



Configuración de SELinux para Pandora FMS



<https://pandorafms.com/manual/!775/>

Permanent link:

https://pandorafms.com/manual/!775/es/documentation/pandorafms/technical_annexes/09_selinux_configuration_for_pandora_fms

2018/03/18 21:03



Configuración de SELinux para Pandora FMS

Introducción

En Pandora FMS la instalación se debe realizar siempre con Security-Enhanced Linux (SELinux) desactivado. Tras la instalación y ante la necesidad de tenerlo activado en algunos entornos, vamos a detallar ajustes de configuración en CentOS 7.

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 utilice 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 los podremos 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 deberá modificarse 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.

Detener syslog (este servicio también podría llamarse rsyslog):

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

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:

```
# /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, modificaremos 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 queremos que SELinux se ejecute en modo restrictivo dejando ejecutar solo lo que aparece dentro de las reglas de los módulos, lo configuraremos a “enforcing”, sacándonos mediante el `audit.log` las ejecuciones denegadas por SELinux. Si por el contrario queremos que nos imprima los warnings en lugar de bloquearnos las acciones lo dejaremos en “permissive”, podremos 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, ejecutaremos:

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

Observaremos que nos saldrán errores como 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, ejecutaremos:

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

Esto creará 2 archivos en el directorio actual:

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

Para activar la nueva regla ejecutamos:

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

Repetir el proceso para añadir las reglas que falten. Después de añadir todas las reglas, SELinux parará 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 para poder usar Pandora FMS al 100% 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 repetiríamos el paso descrito arriba para activar la regla. Con esto abarcaríamos todos los posibles conflictos entre Pandora FMS y SELinux.

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

[Volver al Índice de Documentación Pandora FMS](#)