Configuración de Selinux para PandoraFMS

Volver al Índice de Documentación Pandora FMS

Introducción

Desde PandoraFMS siempre hemos recomendado instalar Pandora con Selinux desactivado (incluyéndolo incluso por defecto en nuestra ISO), pero en algunos entornos es imprescindible/aconsejable tenerlo habilitado por cuestiones obvias de seguridad.

En esta guía detallaremos cómo crear de una forma personalizada las políticas para los diferentes módulos dentro de Selinux.

Para crear este tipo de reglas utilizaremos Audit2allow, que será el encargado de permitir las acciones necesarias.

Instalación de Audit2allow

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.

```
# sudo yum install selinux-policy-devel
# sudo yum install policycoreutils-python
```

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

IMPORTANTE:

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 limpia qué es lo que está bloqueando Selinux, recomendamos borrar los logs anteriores y esperar a que se vuelvan a generar con nuevos registros. Para ello:

Paramos syslog (Este servicio también podría llamarse rsyslog):

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

Borramos el audit.log y el archivo log de mensajes del sistema:

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

Iniciamos de nuevo syslog:

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

Configuración de Selinux

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

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 PandoraFMS

Para que PandoraFMS 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 PandoraFMS al 100% seria:

```
# 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 PandoraFMS y Selinux.

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

Volver al Índice de Documentación Pandora FMS