SELinux

Alberto Molina Coballes

IES Gonzalo Nazareno

5 de febrero de 2021

SELinux

- Security-Enhanced Linux (SELinux). Módulos del kérnel que implementan principalmente MAC (*Mandatory Access Control*)
- Además proporciona Role-Based Access Control (RBAC), Type Enforcement (TE) y Multi-Level Security (MLS)
- El kérnel consulta a SELinux si un proceso está autorizado o no
- Desarrollado inicialmente por NSA
- Actualmente desarrollado principalmente por Red Hat
- Habilitado por defecto en RHEL y CentOS, opcional en otras distribuciones

```
sudo getenforce
Enforcing
```

SELinux. Modos

Enforcing Modo por defecto. SELinux aplicado y denegando cualquier proceso no permitido de forma explícita

```
setenforce 1
```

Permissive SELinux habilitado, registrando cualquier proceso no permitido en logs, pero no denegando

```
setenforce 0
```

Disabled SELinux deshabilitado completamente

Es posible pasar un dominio específico a modo permisivo:

Tipos de política

MLS *Multi Level Security* utilizado en entornos complejos

Targeted Solo procesos seleccionados se ejecutan en un dominio confinado, mientras que el resto lo hace en uno no confinado

- Modo por defecto en RHEL
- Los procesos que escuchan peticiones a través de la red suelen estar confinados (servicios)

```
[root@selinux centos]# sestatus
SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:             targeted <-----
Current mode:                   enforcing
Mode from config file:          enforcing
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Memory protection checking:     actual (secure)
Max kernel policy version:      31
```

Contextos

- Se utilizan reglas (políticas) para autorizar o prohibir cada operación
- Lo que puede hacer un proceso depende de los contextos de seguridad
- Cada fichero o proceso tiene asociado un contexto de SELinux
- El contexto se define por la identidad del usuario que lo inicia, el rol, el tipo y el nivel de seguridad

Identidad Usuario de SELinux, múltiples usuarios pueden usar la misma identidad SELinux, sufijo `_u`

Rol Se pueden asociar diferentes roles a cada identidad según sea necesario, sufijo `_r`

Tipo (dominio) Asociado al tipo de proceso, sufijo `_t`. Usado por la mayoría de políticas

Nivel de seguridad Utilizado en entornos complejos

-Z

Las instrucciones relevantes que necesiten información sobre los contextos incluyen el argumento -Z:

```
id -Z
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023

ps Z
LABEL                             PID TTY      STAT   TIME COMMAND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 5253 pts/0 Ss   0:00 -bash
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 5422 pts/0 R+   0:00 ps Z

ls -lZ
total 0
-rw-rw-r--. 1 centos centos unconfined_u:object_r:user_home_t:s0 0 feb  3 10:19 borrame

sudo ls -lZ /root/
total 16
-rw-------. 1 root root system_u:object_r:admin_home_t:s0 5589 ene 13  2020 anaconda-ks.cfg
-rw-------. 1 root root system_u:object_r:admin_home_t:s0 5355 ene 13  2020 original-ks.cfg
```

Aspectos a considerar

Cuando se interactúa con SELinux podemos encontrar diferentes situaciones:

- Utilizar los diferentes procesos dentro de lo permitido para cada dominio. Funcionamiento normal
- Utilizar algún proceso confinado fuera de los límites permitidos
  - Buscamos en Internet: ~~`setenforce 0`~~
  - Pasamos el proceso a modo permisivo:

    ```
    semanage permissive -a httpd_t
    ```

  - Modificamos el proceso y/o el contexto para que funcione correctamente
- Definir o modificar la política para un proceso. Uso más avanzado

Problemas típicos con un proceso confinado

- Ejecutamos un servicio en un puerto no permitido

```
semanage port -l|grep ^http_port
http_port_t                    tcp      80, 81, 443, 488, 8008, 8009, 8443, 9000
```

- Un servicio lee o escribe ficheros de un tipo no definido en la política:

```
ls -Zl /var/www/html/
-rw-r--r--. 1 root root unconfined_u:object_r:samba_share_t:s0       5 Feb  4 15:56 index2.html
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 5 Feb  4 16:03 index.html
```

Modificar un contexto

chcon `chcon -t httpd_sys_content_t index2.html`

restorecon `restorecon index2.html`
Se puede usar recursivamente (`-R`)

semanage Supongamos el caso en el que pongamos DocumentRoot en `/srv/www`. Debemos modificar la política para que permita poner contenido web en ese directorio:

```
semanage fcontext  -a -t httpd_sys_content_t   ‘‘/srv/www(/.*)?’’
```

Además debemos ejecutar `restorecon` sobre el directorio porque las políticas de SELinux se leen solo al iniciar el equipo

Herramientas adicionales

- SELinux registra la actividad relevante en `/var/log/audit/audit.log`
- Cada registro de audit.log tiene un código de registro (`[0-9]10.[0-9]3:[0-9]2`)
- Podemos pasar el código de registro como parámetro a `audit2why` o `audit2allow`:

```
grep 1612454328.715:412 /var/log/audit/audit.log |audit2why
```

- Instalamos el paquete `setools-console`

```
sesearch -A -s httpd_t
...
ls -Zl /usr/sbin/httpd
...
sesearch -A -s httpd_t -t httpd_exec_t
```