Fundamentos de SELinux

Contenidos

1. ¿Qué es *SELinux* ?

- *SELinux* es una implementación de un sistema de control de acceso centralizado, en inglés *Mandatory Access Control (MAC)*.
- El control de acceso se realiza en función de políticas que definen quién tiene acceso (sujetos) y a qué recursos (objetos).
- Es el administrador del sistema quién tiene la potestad de definir como se lleva a cabo este control de acceso y no los propietarios de los recursos.
- En *SELinux*:
  - Sujetos: son los usuarios y sus procesos.
  - Objetos: son los recursos, como los discos, la memoria, los canales de comunicación, los archivos, etc.
  - Cada sujeto u objeto posee un conjunto de atributos de seguridad (contexto o etiqueta SELinux).
  - El control de acceso a los objetos se realiza mediante políticas de seguridad basadas en reglas.

2. Beneficios de SELinux

- Mejora la seguridad del sistema debido a que:
  - Sólo se permite el acceso a un objeto si existe una regla de política de SELinux que lo permita específicamente.
  - Control de acceso detallado basado en aspectos tales como el rol del usuario, el tipo de recurso, el nivel de sensibilidad de los datos o el grado de confidencialidad.
  - La política SELinux se define administrativamente y se aplica a todo el sistema.
  - Mejora de la mitigación de los ataques de escalada de privilegios. Si un proceso se ve comprometido, el atacante sólo tiene acceso a las funciones normales de ese proceso y a los archivos a los que el proceso ha sido configurado para tener acceso.
  - SELinux puede utilizarse para reforzar la confidencialidad e integridad de los datos, así como para proteger los procesos de las entradas no fiables.

3. Qué no es responsabilidad de SELinux

- SELinux no es:
  - Un cortafuegos.
  - Un antivirus.
  - Responsable de las contraseñas del sistema.
- En definitiva, no es una solución para la seguridad del sistema todo en uno

4. Contexto *SELinux*

- *Contexto SELinux (etiqueta SELinux)*
  - Los procesos y recursos poseen un contexto SELinux (etiqueta SELinux). Un contexto se define mediante 5 atributos (**3 obligatorios y 2 opcionales**).

    Usuario:Rol:Tipo:Nivel:Categoria
  - Ejemplo:

    `system_u:system_r:xserver_t:s0-s0:c0.c1023`
  - Las definiciones de los contextos de los archivos se almacenan en los archivos de configuración de las políticas. Cuando el sistema arranca, a cada proceso o archivo se le asigna el contexto que tiene definido en la política que se aplique.
  - Durante la vida de un proceso o recurso su contexto SELinux puede cambiar, o sea, **es dinámico.** Este cambio se puede deber a:
    - Órdenes ejecutadas por el administrador del sistema que cambian los contextos.
    - Transiciones realizadas internamente por propios los procesos.

4. Contexto SELinux

- Contexto SELinux:
  - **Usuario (_u).** Los usuarios *SELinux* no coinciden con los usuarios del sistema anfitrión (`user_u, system_u`, …)
  - **Rol (_r).** El papel que juega un usuario *SELinux* en el sistema (`sysadm_r, user_r, …`)
  - **Tipo (_t).** Todas las entidades controladas por *SELinux* se clasifican en categorías o tipos (`file_t, user_home_t`, …)
  - **Nivel.** Permite controlar el acceso a los datos en función de distintos niveles de sensibilidad (`s0 – s15`).
  - **Categoría.** Permite controlar el acceso a los datos en función de su grado de confidencialidad (`c0, c1, … c1023`).
- Ejemplos:

```
system_u:system_r:xserver_t
system_u:system_r:xserver_t:s0-s0:c0.c1023
system_u:system_r:xserver_t:SystemLow-SystemHigh
```

5. Políticas de seguridad SELinux

- *SELinux* soporta distintos tipos de políticas de seguridad:
  - Para sistemas de propósito general: tipo "*Mandatory*" y su versión simplificada "Targeted". Basada en dominios formados por procesos y recursos que se definen en función del atributo tipo de las etiquetas SELinux.
  - Para sistemas en los que se debe tener en cuenta distintos niveles de sensibilidad de los datos (sistemas gubernamentales, de defensa, …): Sistemas de Seguridad Multinivel (MLS) .
  - Para sistemas en los que se deben tener en cuenta distintas categorías de confidencialidad de los datos: Sistemas de Seguridad Multicategoría (MCS) .

6. Modos de funcionamiento de SELinux

- *Independientemente del tipo de sistema, se recomienda ejecutar siempre SELinux.*
- Modos de ejecución:
  - *Enforcing*.
  - *Permissive*.
  - *Disabled*.
- ¿Cómo saber en qué modo se está ejecutando?
  - Orden `sestatus`
  - Orden `getenforce`
- ¿Cómo configurar el modo de ejecución?
  - Temporalmente: orden `setenforce`
  - Permanentemente: archivo de configuración `/etc/SELinux/config`

7. Usando *SELinux*

- Instalación de la interfaz completa de órdenes para administrar SELinux

```
#  dnf install policycoreutils-Python
```

- Instalación de la interfaz gráfica para utilizar SELinux

```
#  dnf install policycoreutils-gui
```

7. Usando SELinux

- Manejo de contextos:
  - Visualizar información de contexto: opción –Z con los órdenes `id, ls o ps`.

    ```
    # id –Z
    # ls -Z /bin/bash
    # ps –Z
    ```
  - Modificar temporalmente el contexto: orden `chcon`

    ```
    # chcon -t user_home_t /tmp/myfile
    ```
  - Restaurar el contexto original de un archivo (contexto que tiene definido en los ficheros de configuración de la política que se aplica): orden `restorecon`

    ```
    # restorecon /tmp/myfile
    ```
  - Modificar del contexto original de un archivo: orden `semanage`

    ```
    # semanage fcontext -a -t user_home_t /var/cache/myfile
    ```
  - Cambiar el rol y el tipo del intérprete de órdenes que me atiende (sesión): orden `newrole`

    ```
    # newrole -r system_r -t unconfined_t
    ```
  - Establecer el usuario SELinux del intérprete de órdenes que me atiende (sesión): orden `runcon`

    ```
    # runcon -u system_u /bin/bash
    ```

7. Usando SELinux

- **Variables boolenas SELinux**: especifican si un proceso perteneciente a un determinado servicio puede hacer uso de una determinada funcionalidad del sistema. Por ejemplo:
  - `httpd_can_network_connect_db`: especifica si el proceso httpd (servicio Apache) puede conectarse a un servicio de bases de datos remoto.
- Visualizar el estado de las variables booleanas: órdenes `semanage` y `getsebool`

```
# semanage boolean -l
# getsebool -a
# getsebool httpd_can_network_connect_db
```

- Modificar valores: orden `setsebool`

```
# setsebool httpd_can_network_connect_db on
# setsebool -P httpd_can_network_connect_db on
```

8. Configuración de SELinux

- Ficheros de configuración globales `/etc/selinux`

  `/etc/selinux/config`

  `/etc/selinux/semanage.conf`

  `/etc/sestatus.conf`

  `/etc/security/sepermit.conf`

- Ficheros asociados a la política empleada
  - Ficheros básicos de configuración de la política

    `/etc/selinux/<policy_name>`

9. Un ejemplo: el entorno de virtualización KVM y SELinux

- KVM es un entorno de virtualización para sistemas Linux desarrollado por Red Hat.
- En contextos de sistemas de información corporativos, junto con VMware y Citric, se trata de una de las tecnologías de virtualización más utilizadas.
- **Dominio Virt**. Dominio SELinux responsable del control de acceso de los procesos de virtualización y los recursos que utilizan.
  - Definición uniforme de los contextos que dan lugar al dominio.
  - Aplicación uniforme de las reglas.

9. Un ejemplo: el entorno de virtualización KVM y SELinux

- Etiquetas SELinux del dominio v*irt*:

Type/Description	SELinux Context
Virtualized guest processes. MCS1 is a random MCS field. Approximately 500,000 labels are supported.	system_u:system_r:svirt_t:MCS1
Virtualized guest images. Only *svirt_t* processes with the same MCS fields can read/write these images.	system_u:object_r:svirt_image_t:MCS1
Virtualized guest shared read/write content. All *svirt_t* processes can write to the svirt_image_t:s0 files.	system_u:object_r:svirt_image_t:s0
Virtualized guest shared read only content. All svirt_t processes can read these files/devices.	system_u:object_r:svirt_content_t:s0
Virtualized guest images. Default label for when an image exits. No *svirt_t* virtual processes can read files/devices with this label.	system_u:object_r:virt_content_t:s0

9. Un ejemplo: el entorno de virtualización KVM y SELinux

- Variables booleanas SELinux del domino virt:

Entidad	Significado
virt_use_comm	Permite a virt el uso de comunicaciones series y paralelas
virt_use_fusefs	Permite a virt leer archivos fuse
virt_use_nfs	Permite a virt manejar sistemas de archivos NFS
virt_use_samba	Permite a virt manejar archivos CIFS
virt_use_sanlock	Permite a sanlock manejar archivos virt lib
virt_use_sysfs	Permite a virt manejar la configuración de dispositivos PCI
virt_use_xserver	Permite a las máquinas virtuales interactuar con el servidor X
virt_use_usb	Permite a virt utilizar dispositivos USB

10. Bibliografía

Uso de SELinux. Configuración básica y avanzada de Security-Enhanced Linux (SELinux)

https://access.redhat.com/documentation/es-es/red_hat_enterprise_linux/8/html/using_SELinux/index

SELinux Project Wiki.

http://SELinuxproject.org/page/Main_Page