



Sistemas Operativos 2

Unidad 5: Seguridad

Sistema SELinux

René Ornelis
Primer semestre de 2025

Contenido

1	Historia.....	4
2	Antecedentes	4
3	Arquitectura	4
3.1	Security context	5
3.2	Modos de acceso	5
3.2.1	Control de Acceso Discrecional.....	5
3.2.2	Control de Acceso Mandatorio	6
4	Aplicación	7
5	Modos de operación.....	8
6	Ventajas.....	9
7	Desventajas	9
8	Referencias.....	9

Índice de figuras

Figura 1: Contexto de seguridad	5
Figura 2: Seguridad en modelo discrecional.....	6
Figura 3: Control de acceso mandatorio	7
Figura 4: Aislamiento de dos procesos	7

Sistema SELinux

1 Historia

SELinux, o Security-Enhanced Linux, es una extensión del núcleo de Linux que implementa un sistema de control de acceso obligatorio (MAC) dentro del sistema operativo. Fue desarrollado inicialmente por la Agencia de Proyectos de Investigación Avanzada de Defensa (DARPA) y la Agencia de Seguridad Nacional (NSA) de los Estados Unidos. Se lanzó por primera vez en 2000 como una parte del Proyecto NSA Security-Enhanced Linux, y posteriormente fue incluido en la versión 2.6 del kernel de Linux en 2003.

2 Antecedentes

Antes de SELinux, el control de acceso en Linux se basaba en un modelo de control de acceso discrecional (DAC), que otorgaba permisos de acceso a los archivos y recursos a los usuarios en función de su identidad y los permisos establecidos por el propietario del recurso. Sin embargo, este modelo tenía limitaciones en términos de seguridad, ya que confiaba en la autoridad del usuario para gestionar los permisos adecuadamente.

Dado que el modelo DAC no proporcionaba suficiente seguridad para aplicaciones críticas, la NSA y DARPA comenzaron a trabajar en un sistema que permitiera un control de acceso más granular y reforzado. Así nació SELinux, que implementa el modelo MAC, donde las políticas de seguridad son impuestas por un sistema central, en lugar de depender de la discreción del usuario o del propietario del recurso.

Por ejemplo: Apache web server, es un servicio que corre con altos privilegios (usuario *root*) ya que necesita acceso a los puertos 80 y 443 y solo el usuario root puede acceder a los puertos menores de 1024. Si este servicio es vulnerado, entonces el perpetrador se tiene acceso a **todo** el sistema.

La arquitectura de SELinux permite restringir los procesos a un conjunto de recursos (archivos, puertos, etc) que tiene asignado, de forma que, si es vulnerado, el perpetrador no podrá modificar el sistema más allá del servicio comprometido.

Sin embargo, su uso puede generar problemas de compatibilidad con ciertas aplicaciones, ya que los recursos que la aplicación necesita pueden estar bloqueados o depender de servicios que no han sido configurados adecuadamente para funcionar con SELinux. Esto implica que el administrador debe realizar una investigación y configurar las aplicaciones y servicios necesarios, la cual es una tarea compleja. Adicionalmente, los desarrolladores de aplicaciones deben incluir en su instalación la configuración de las políticas necesarias para que su aplicación sea compatible con SELinux.

Aunque es posible, no es recomendable deshabilitar SELinux, ni siquiera en ambientes de desarrollo, ya que estos deben ser lo más parecido posible a los ambientes de producción.

3 Arquitectura

SELinux se implementa como una serie de extensiones del núcleo de Linux que añaden funcionalidades de control de acceso a nivel de núcleo. Utiliza etiquetas de seguridad (security labels) para identificar los sujetos (usuarios, procesos) y los objetos (archivos, directorios,

puertos de red) del sistema. Estas etiquetas son utilizadas por SELinux para aplicar políticas de acceso, que determinan qué acciones están permitidas para cada sujeto en relación con cada objeto.

3.1 Security context

En SELinux, el contexto de seguridad es una parte fundamental del sistema que se utiliza para etiquetar y clasificar los sujetos y objetos del sistema. Estas etiquetas, conocidas como etiquetas de seguridad o contextos de seguridad, son asignadas a procesos, archivos, directorios, puertos de red y otros recursos del sistema.

El contexto de seguridad en SELinux consiste típicamente en tres componentes (ver Figura 1):

1. **Usuario:** Identifica al usuario o rol que inicia el proceso o que posee el objeto.
2. **Rol:** Identifica el rol del usuario, que puede ser administrativo o no administrativo, y ayuda a definir los permisos que el usuario tiene sobre los objetos del sistema.
3. **Tipo de objeto:** Identifica el tipo de objeto al que se aplica el contexto de seguridad, como un archivo, un directorio, un proceso, un socket, etc.

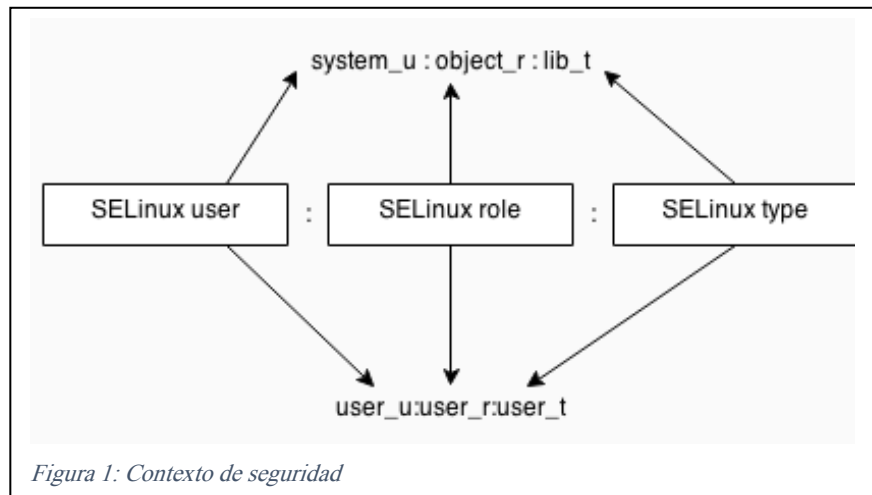


Figura 1: Contexto de seguridad

Estas etiquetas son utilizadas por SELinux para aplicar políticas de seguridad, determinando qué acciones están permitidas o denegadas para un sujeto en relación con un objeto específico. Por ejemplo, si un proceso con un contexto de seguridad particular intenta acceder a un archivo con un contexto de seguridad diferente, SELinux evaluará las políticas definidas para determinar si se permite o deniega el acceso.

La asignación adecuada de contextos de seguridad es esencial para el funcionamiento correcto de SELinux. Si los contextos de seguridad no se aplican correctamente, pueden surgir problemas de acceso a los recursos del sistema y las políticas de SELinux pueden no aplicarse como se espera.

3.2 Modos de acceso

3.2.1 Control de Acceso Discrecional

DAC (por sus siglas en inglés) es un modelo de control de acceso utilizado en sistemas operativos como Linux y Unix. En el DAC, los propietarios de los recursos (archivos, directorios, dispositivos, etc.) tienen el control discrecional sobre quién puede acceder a ellos y

qué tipo de acceso se permite. Es decir, el propietario del recurso tiene el poder de decidir quién puede leer, escribir o ejecutar el recurso.

Bajo el modelo de DAC, cada recurso tiene un conjunto de permisos asociados, que generalmente se dividen en tres categorías:

1. **Lectura (Read):** Permite ver el contenido del recurso.
2. **Escritura (Write):** Permite modificar el contenido del recurso.
3. **Ejecución (Execute):** Permite ejecutar el recurso si es un programa o script.

Estos permisos se asignan a tres categorías de usuarios: el propietario del recurso, el grupo al que pertenece el recurso y todos los demás usuarios. Cada categoría puede tener permisos distintos.

Por ejemplo, observando la Figura 2, si un archivo llamado "script" tiene permisos de lectura y escritura para el propietario, pero solo permisos de lectura para el grupo y para otros usuarios, significa que el propietario puede leer y modificar el archivo, mientras que los miembros del grupo y otros usuarios solo pueden leerlo.

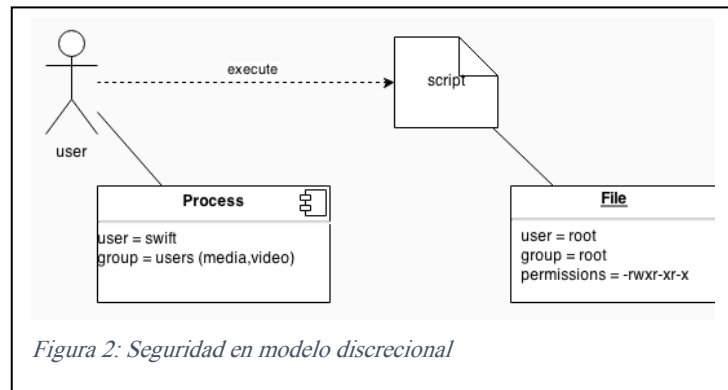


Figura 2: Seguridad en modelo discrecional

El modelo de DAC es relativamente simple y fácil de entender, pero tiene algunas limitaciones en términos de seguridad. Por ejemplo, si un usuario malicioso obtiene acceso a una cuenta con privilegios suficientes para modificar los permisos de un recurso, puede cambiarlos para obtener acceso no autorizado.

Para abordar estas limitaciones y mejorar la seguridad, se han desarrollado modelos de control de acceso más avanzados, como el Control de Acceso Obligatorio (MAC), que proporciona un control más granular y centralizado sobre los accesos a los recursos del sistema.

3.2.2 Control de Acceso Mandatorio

En Linux, el Modo de Acceso Mandatorio (MAC) es un modelo de control de acceso en el cual las políticas de seguridad son aplicadas de manera obligatoria por el sistema operativo, sin depender de la discreción del propietario del recurso o del usuario. A diferencia del Modo de Acceso Discrecional (DAC), donde los propietarios de los recursos pueden decidir quién puede acceder a ellos y qué tipo de acceso se permite, en el MAC las políticas de acceso son determinadas por un sistema central y aplicadas de manera uniforme a todos los usuarios y procesos del sistema.

En el contexto de Linux, SELinux (Security-Enhanced Linux) es una implementación popular de MAC. SELinux utiliza etiquetas de seguridad (security labels) para identificar los sujetos (usuarios, procesos) y los objetos (archivos, directorios, puertos de red) del sistema, y luego aplica políticas de acceso basadas en estas etiquetas.

Las políticas de SELinux definen qué acciones están permitidas para cada sujeto en relación con cada objeto, según criterios como la clasificación de seguridad de los sujetos y

objetos, el contexto de seguridad de la operación solicitada y reglas predefinidas de acceso. Estas políticas se aplican de manera obligatoria y son independientes de los permisos tradicionales de Unix (lectura, escritura, ejecución) asociados con los archivos y directorios.

El MAC proporciona una capa adicional de seguridad al sistema operativo Linux, ayudando a prevenir y mitigar ataques al restringir de manera más granular los accesos a los recursos del sistema. Aunque la configuración de SELinux puede ser compleja y requerir un conocimiento técnico profundo, sus beneficios en términos de seguridad suelen superar sus desafíos de implementación.

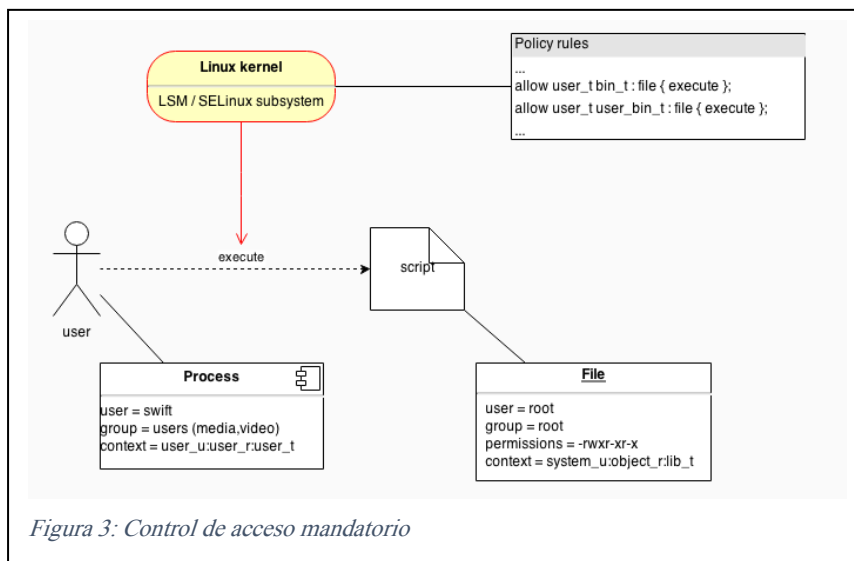


Figura 3: Control de acceso mandatorio

Por ejemplo: si vemos la Figura 3, el usuario *user* y el archivo *script*, además del acceso discrecional, tienen cada uno asociado su propio contexto de seguridad. Cuando el usuario intenta ejecutar el archivo, aunque el acceso discrecional indique que tiene acceso de lectura y ejecución (r-x), en la política de SELinux no hay ninguna regla que permita la ejecución y por lo tanto se deniega.

4 Aplicación

- Cada proceso y archivo está marcado con un contexto de seguridad (*labeling*)
- Los nuevos archivos heredan el contexto de seguridad del directorio contenedor.
- La política le asigna los contextos a los procesos.
- El login y el shell pueden, por política, asignar el contexto de seguridad a procesos que se inicien. Tal como se muestra en la Figura 4, dos servicios importantes como el servidor web Apache y la base de datos MariaDB, que ambos corren con usuario *root*, con la aplicación de políticas de SELinux, ambos procesos pueden ser aislados a los recursos de cada uno, y aunque sean vulnerados, no podrán dañar los archivos del otro proceso.

El proceso de etiquetado, conocido como *labeling*, se refiere a la

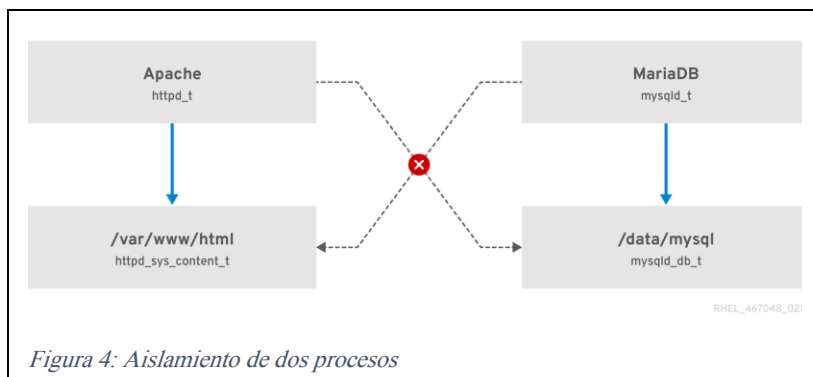


Figura 4: Aislamiento de dos procesos

asignación de etiquetas de seguridad a los diferentes objetos del sistema, como usuarios, archivos, procesos, hardware, entre otros. Durante la instalación del sistema, el sistema asigna automáticamente estas etiquetas, definiendo el dominio y contexto de seguridad de cada objeto según las políticas preestablecidas.

Es importante señalar que estas etiquetas pueden ser modificadas en cualquier momento si es necesario reaplicar las políticas de seguridad, por ejemplo, en caso de un incidente de seguridad.

Sin embargo, es crucial tener precaución, ya que las actualizaciones del sistema pueden sobrescribir las políticas de SELinux y reetiquetar los objetos según la nueva política. Esto puede generar problemas si se han realizado cambios manuales en las etiquetas de archivos o usuarios, ya que durante un upgrade automático —especialmente en servidores de producción— las modificaciones previas pueden perderse. Para evitar esta situación, se recomienda no alterar los archivos de política predeterminados del sistema, ya que estos pueden ser actualizados con nuevas versiones, lo que puede resultar en la pérdida de configuraciones personalizadas. En su lugar, se deben agregar archivos de configuración personalizados, como los archivos **local** o **custom**, los cuales no se verán afectados por las actualizaciones del sistema. De esta manera, se garantiza que los cambios realizados en las políticas de SELinux se mantengan intactos y sean aplicados correctamente.

5 Modos de operación

- **Strict:** SELinux aplica de manera rigurosa todas las políticas de seguridad configuradas en el sistema. Esto implica que cada proceso, archivo, dispositivo y objeto del sistema tiene restricciones detalladas que definen lo que puede o no hacer. Si una acción no está explícitamente permitida por las políticas, se bloquea y se registra como un evento de seguridad. Este modo ofrece el nivel más alto de seguridad, ya que restringe de manera exhaustiva las interacciones y los accesos entre los diferentes componentes del sistema, minimizando las posibilidades de que se realicen actividades no autorizadas. Sin embargo, puede ser más restrictivo y puede generar problemas de compatibilidad si no se ajustan correctamente las políticas para las aplicaciones y procesos específicos. En este modo todo es denegado por omisión, hay que establecer las reglas de lo permitido.
- **Targeted:** Todo se permite, excepto lo marcado por la política. El modo **Targeted** es una configuración intermedia que se utiliza en la mayoría de las distribuciones de Linux que implementan SELinux. En este modo, SELinux aplica las políticas de seguridad de manera más restringida solo a un conjunto específico de procesos y servicios que se consideran más críticos, como servicios de red o procesos privilegiados. El resto de los procesos y objetos en el sistema operan con una política más flexible y permisiva, lo que reduce el impacto en la funcionalidad general del sistema y mejora la compatibilidad con aplicaciones no críticas. Es el modo más utilizado en entornos de producción, ya que proporciona un buen balance entre seguridad y facilidad de uso.
 - contexto *unconfined_t*
- **Permissive:** En este modo, SELinux no aplica las políticas de seguridad de forma activa. En lugar de bloquear acciones no permitidas, simplemente las registra como alertas en los logs del sistema. Esto permite monitorear el comportamiento de SELinux sin que las políticas de seguridad interfieran con las operaciones del sistema. Este modo es útil para la depuración y pruebas de

configuración, ya que permite que los administradores verifiquen el comportamiento de SELinux y ajusten las políticas sin que se produzcan bloqueos o interrupciones. Sin embargo, no ofrece ninguna protección de seguridad activa mientras esté en este modo. Es recomendable usar este modo solo en entornos de prueba o cuando se estén realizando ajustes a las políticas de SELinux antes de activar un modo más restrictivo.

Finalmente, aunque está disponible, deshabilitar SELinux debe ser considerado solo como una opción temporal y en circunstancias específicas, como para la resolución de problemas de compatibilidad. En la mayoría de los casos, es mucho más seguro mantener SELinux habilitado y, si es necesario, ajustar las políticas para que se adapten a los requerimientos del sistema. Esto garantizará un mayor nivel de protección y ayudará a evitar que el sistema sea vulnerable a posibles ataques. Incluso en los ambientes de desarrollo se debe mantener SELinux para que dichos ambientes sean lo más parecido a los ambientes de producción.

6 Ventajas

1. **Refuerzo de la seguridad:** Al implementar un modelo MAC, SELinux ofrece un control más granular sobre los permisos de acceso, lo que reduce la superficie de ataque del sistema.
2. **Políticas de seguridad flexibles:** SELinux permite a los administradores definir políticas de seguridad personalizadas para adaptarse a las necesidades específicas de su entorno.
3. **Protección contra ataques de día cero:** Al limitar los privilegios de los procesos y usuarios, SELinux puede mitigar los efectos de los ataques de día cero al limitar el alcance de las acciones maliciosas.
4. **Auditoría mejorada:** SELinux proporciona herramientas para auditar las acciones del sistema, lo que facilita la detección y respuesta ante actividades sospechosas.

7 Desventajas

1. **Complejidad:** La configuración de SELinux puede ser compleja y requerir un conocimiento técnico profundo. Los administradores pueden enfrentar dificultades al definir y mantener políticas de seguridad adecuadas.
2. **Posible impacto en el rendimiento:** La aplicación de políticas de SELinux puede introducir cierta sobrecarga en el sistema, lo que puede afectar el rendimiento en entornos de alta carga.
3. **Compatibilidad con aplicaciones:** Algunas aplicaciones pueden no ser compatibles de forma nativa con SELinux y pueden requerir ajustes adicionales para funcionar correctamente en entornos SELinux habilitados.

SELinux ofrece una capa adicional de seguridad para sistemas Linux al implementar un modelo MAC. Aunque puede requerir un esfuerzo adicional para configurar y mantener, sus ventajas en términos de seguridad suelen superar sus posibles desventajas.

8 Referencias

https://selinuxproject.org/page/Main_Page

[https://wiki.centos.org/HowTos\(2f\)SELinux.html](https://wiki.centos.org/HowTos(2f)SELinux.html)

https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html/using_selinux/index

https://wiki.gentoo.org/wiki/SELinux/Quick_introduction#SELinux_policy

https://en.wikipedia.org/wiki/Security-Enhanced_Linux

<https://www.redhat.com/en/topics/linux/what-is-selinux>