

SELinux Introduction**Summary**

Investigacion de SELinux Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magnam aliquam quaerat voluptatem. Ut enim aequaleam animo, cum corpore dolemus, fieri tamen permagna accessio potest, si aliquod aeternum et infinitum impendere malum nobis opinemur. Quod idem licet transferre in voluptatem, ut postea variari voluptas distinguere possit, augeri amplificarique non possit. At etiam Athenis, ut e patre audiebam facete et urbane Stoicos irridente, statua est in quo a nobis philosophia defensa et collaudata est, cum id, quod maxime placeat, facere possimus, omnis voluptas assumenda est, omnis dolor repellendus. Temporibus autem quibusdam et.

Keywords: Cibersecurity; Linux; Selinux

Contents

1 Introduccion	2
1.1 Que es Selinux	2
1.2 Caracteristicas de Selinux	2
2 Bases de SELinux	3
2.1 Herramientas de terminal auxiliares	3
2.1.1 Selinux Contexts	3
2.2 Selinux Labels	4
2.2.1 Selinux Roles	6
2.2.2 Selinux sensitivity	7
2.3 Selinux Policies	7
3 Casos especiales	7
3.1 Contenedores	7
4 Escenarios	7
4.1 Escenario 1	7
4.2 Escenario 2	7
5 Referencias	7
5.1 Referencia archivos	7
5.2 Referencia archivos de configuracion	7
5.3 Referencia archivos de errores	7
5.4 Referencias comandos	8
5.4.1 Desactivar acciones silenciosas	8
5.4.2 Retiquetar el sistema de archivos	8
5.4.2.1 Grano Grueso	8
5.4.2.2 Grano Fino	8
5.4.3 Monitorizacion Basica SELinux	9
5.4.4 Obtencion de logs de SELinux	10
5.4.5 Lectura de Label o etiquetas (Etiquetas)	10
5.5 Herramientas complementarias	11
5.5.1 Cockpit	11
5.5.2 Udrca	12
6 Glosario	13
References	13

1 Introduccion

En los sistemas Unix tradicionales, el control de accesos se realiza de forma discrecional Discretionary Access Control (DAC)[1], lo que permite a usuarios y administradores gestionar los permisos sobre archivos y procesos basándose en los identificadores de usuario (UID), de grupo (GID) y otros atributos. Este enfoque flexible puede generar problemas de seguridad, ya que permite a los usuarios manejar los permisos sobre los archivos y recursos que poseen. Por ejemplo, un usuario podría otorgar permisos demasiado amplios a otros usuarios o grupos, lo cual podría permitir el acceso a personas no autorizadas. Adicionalmente podría darse el caso de que se creasen archivos que deberían tener permisos incompatibles debido a quien debe acceder a esos archivos. Para abordar todo esto existe el concepto de Multi-Level Security (MLS)[2]

Security Enhanced Linux (SELinux)[3] se desarrolló para resolver esta problemática mediante la implementación de Mandatory Access Control (MAC)[4], donde las políticas de seguridad son definidas exclusivamente por los administradores del sistema y no pueden ser modificadas ni ignoradas por los usuarios regulares. Además, SELinux sigue una política de “denegación por defecto”, lo que significa que, en ausencia de una regla explícita para una acción, esta será denegada por defecto. Esto contrasta con el modelo DAC, donde un acceso puede ser permitido si no se especifica lo contrario. Cabe recalcar que SELinux no sobrescribe los permisos del DAC si no que los extiende.

1.1 Que es Selinux

SELinux es código que se ejecuta en el espacio de usuario, aprovechando el código de kernel Linux Security Modules (LSM)[5] para proporcionar MAC a través de los recursos del sistema. Los procesos se limitan a dominios, que se pueden considerar como recintos de pruebas. El acceso a objetos del sistema y prestaciones como archivos, colas de mensajes, semáforos, redes, se controla por dominio siguiendo el principio de menor privilegio.

Los directorios y archivos en SELinux se etiquetan con un tipo de dato persistente conocido como Label que es independiente de los UNIX DAC habituales. Esta capa adicional permite un control más estricto sobre el acceso a los objetos: si un intruso obtiene el control de un proceso propiedad de un usuario, el acceso a todos los archivos propiedad de ese usuario no se otorga automáticamente. El tipo de acceso (lectura, escritura, creación) también puede ser controlado por SELinux. Para una descripción más gráfica y simple se puede referenciar a [6].

1.2 Características de Selinux

- El acceso solo está permitido si existe una regla de política SELinux que lo permita específicamente.
- La política de SELinux está definida administrativamente y se aplica en todo el sistema por SELinux.
- Las decisiones de acceso de SELinux se basan en toda la información disponible, como un usuario de SELinux, rol, tipo y, opcionalmente, un nivel de todo el sistema.

- Mejora de la mitigación para ataques de escalada de privilegios. Los procesos se ejecutan en dominios y, por lo tanto, están separados entre sí. Las reglas de política de SELinux definen cómo los procesos acceden a los archivos y otros procesos.
- SELinux se puede utilizar para hacer cumplir la confidencialidad e integridad de los datos, así como para proteger los procesos de entradas no confiables
- SELinux se ejecuta a nivel de kernel
- SELinux como tal se integra a nivel de kernel a través del framework LSM (Linux Security Modules)
- La aplicación de políticas de SELinux es veloz porque todo, ya está definido por archivos de texto o comandos, transpila a Common Intermediate Language (CIL)[7]

2 Bases de SELinux

SELinux tiene tres modos de operación [Disabled, Permissive, Enforcing]

- Disabled
 - SELinux no interactúa con el sistema
- Permissive
 - SELinux no bloquea nada, en cambio solo notifica cuando un evento transgrede una regla
- Enforcing
 - SELinux bloquea todas las acciones que no tengan políticas asociadas

La existencia de estos tres modos se explica en el sentido de que cada uno existe para uno de tres escenarios.

- Disabled: Cuando se quiere desactivar SELinux por completo.
- Permissive: Cuando se quiere permitir el funcionamiento del sistema sin bloquearlo para:
 - Aprender el funcionamiento del sistema y refinar políticas
 - Razones adicionales
- Enforcing: Cuando las políticas están listas para ser desplegadas

2.1 Herramientas de terminal auxiliares

En una instalación básica no vienen todos los paquetes necesarios para administrar el sistema de forma cómoda, por eso se recomienda

```
1 dnf install setools-console setools sepolicy_analysis policycoreutils (bash)
python3-policycoreutils
```

2.1.1 SELinux Contexts

El contexto en SELinux es una etiqueta que se asocia a cada archivo, proceso y recurso del sistema para definir sus permisos y roles de seguridad. Un contexto típico en SELinux se compone de tres elementos principales:

- User (usuario): Define el usuario de seguridad de SELinux.
- Role (rol): Define el rol de seguridad de SELinux.

- Type (Dominio o tipo (dominio)): Define el tipo de seguridad de SELinux, que es el más importante para la política de acceso.
- Sensivity level (Nivel de sensibilidad):

Cada atributo puede identificar porque su etiqueta termina en:

- `_u`: usuario
- `_r`: rol
- `_t`: dominio

De todos estos el mas importante es el tercero, el dominio, porque la mayoria de las politicas trabajan sobre este valor.

Todos los comandos basicos de visualizacion de atributos se pueden ver en Section 5.4.5

Se puede acceder a los valoers de Selinux asociados a un proceso en `/proc/$PID/attr`. Esta carpeta define los atributos asociados a un proceso.

```
[asada fedora] - [~/Documents/git/trabajo/selinux-galifornia] - [Sun Dec 01, 14:57]
[$] <git:(master*)> ps -eZ | grep sshd
system_u:system_r:sshd_t:s0-s0:c0.c1023 82694 ? 00:00:00 sshd
[asada fedora] - [~/Documents/git/trabajo/selinux-galifornia] - [Sun Dec 01, 14:57]
[$] <git:(master*)> ls /proc/82694/attr
current exec fscreate keycreate prev sockcreate
[asada fedora] - [~/Documents/git/trabajo/selinux-galifornia] - [Sun Dec 01, 14:57]
[$] <git:(master*)> cat /proc/82694/attr/*
system_u:system_r:sshd_t:s0-s0:c0.c1023system_u:system_r:init_t:s0%
```

El significado de los archivos es el siguiente:

- El archivo `current` muestra el contexto SELinux actual del proceso.
- El archivo `exec` muestra el contexto SELinux que será asignado por la próxima ejecución de la aplicación realizada a través de esta aplicación. Normalmente está vacío.
- El archivo `fscreate` muestra el contexto SELinux que será asignado al siguiente archivo escrito por la aplicación.
- El archivo `keycreate` muestra el contexto SELinux que será asignado a las claves almacenadas en caché en el kernel por esta aplicación. Normalmente está vacío.
- El archivo `prev` muestra el contexto SELinux previo para este proceso en particular. Este normalmente es el contexto de su aplicación padre.
- El fichero `sockcreate` muestra el contexto SELinux que será asignado al siguiente socket creado por la aplicación. Normalmente está vacío.

2.2 Selinux Labels

En SELinux, todos los objetos y procesos están etiquetados con un Label, este representa el contexto y define detalladamente cómo pueden interactuar entre sí. Finalmente, SELinux también aísla los procesos en dominios, lo que impide que un proceso comprometido, como un servidor web, acceda a recursos fuera de su dominio designado. Por lo tanto, SELinux es capaz de mitigar la escalada de privilegios y reducir los riesgos en el sistema, al restringir las acciones que un atacante podría llevar a cabo, limitando su acceso a recursos y otras operaciones que podrían ser posibles en un sistema Unix estándar con DAC en lugar del MAC de SELinux.

Aquí estan listadas las Etiquetas mas comunes:

Tipo de etiqueta	Ruta	Descripción
unconfined_t	/example	Carpeta sin restricciones de SELinux
user_home_t	/home/user	Carpeta home de usuario
default_t	common	Carpeta por defecto
bin_t	bin	Carpeta de binarios
boot_t	boot	Carpeta de boot
device_t	dev	Carpeta de dispositivos
etc_t	etc	Carpeta de configuración
home_root_t	home	Carpeta raíz de home
lib_t	lib	Carpeta de librerías
lost_found_t	lost+found	Carpeta de archivos eliminados
mnt_t	mnt	Carpeta montada
proc_t	proc	Carpeta de procesos
admin_home_t	root	Carpeta de home del usuario root
var_run_t	run	Carpeta de archivos de ejecución
sysfs_t	sys	Carpeta de información kernel y dispositivos
tmp_t	tmp	Carpeta de archivos temporales
usr_t	usr	Carpeta de archivos de binarios y similares de solo lectura
var_t	var	Carpeta de archivos de datos variables

- Diferencia entre contexto y Label
 - Contexto es el conjunto de politicas asociadas a un nombre (Label)
 - Label es el identificador por el cual el archivo va a ser juzgado a la hora de aplicar politicas

2.2.1 Selinux Roles

La principal forma de control en SELinux son las Etiquetas, pero existe otra que es a través de roles. Por convención, los roles SELinux se definen con un sufijo `_r`. El acceso por roles es la base del user-based access control (UBAC)

En la mayoría de los sistemas SELinux, el administrador puede asignar los siguientes roles SELinux a los usuarios estos son los roles más destacados:

- El rol `user_r` es para usuarios restringidos. A este rol sólo se le permite tener procesos con tipos específicos para aplicaciones de usuario final. Los tipos privilegiados, incluyendo aquellos utilizados para cambiar a otro usuario Linux, no están permitidos para este rol.
- El rol `staff_r` está pensado para operaciones no críticas. Este rol está generalmente restringido a las mismas aplicaciones que el usuario restringido, pero tiene la capacidad de cambiar de rol. Es el rol por defecto de los operadores (para mantener a los usuarios en su rol menos privilegiado el mayor tiempo posible). su rol menos privilegiado el mayor tiempo posible).
- El rol `sysadm_r` está destinado a los administradores del sistema. Este rol es muy privilegiado, permitiendo varias tareas de administración del sistema. Sin embargo, ciertas aplicaciones de usuario final (especialmente si esos tipos se utilizan para software potencialmente vulnerable o no fiable) para mantener el sistema libre de infecciones.
- El rol `secadm_r` está pensado para administradores de seguridad. Este rol permite cambiar la política SELinux y manipular los controles SELinux. Generalmente se utiliza cuando se necesita una separación de funciones entre los administradores del sistema y la gestión de las políticas del sistema.
- El rol `system_r` está pensado para demonios y procesos en segundo plano. Este rol es bastante privilegiado, ya que admite varios tipos de procesos de demonio y de sistema. Sin embargo, los tipos de aplicaciones de usuario final y otros tipos administrativos no están permitidos en este rol.
- El rol `unconfined_r` está pensado para usuarios finales. Este rol permite un número limitado de tipos, pero esos tipos son muy privilegiados ya que permiten ejecutar cualquier aplicación lanzada por un usuario (u otro proceso no confinado) de una manera más o menos no confinada (no restringida por SELinux). (no restringida por las reglas de SELinux). Este rol, como tal, sólo está disponible si el administrador del sistema quiere proteger ciertos procesos (la mayoría demonios) mientras mantiene el resto de las operaciones del sistema casi intactas por SELinux.

SELinux Roles			
<code>auditadm_r</code>	<code>container_user_r</code>	<code>dbadm_r</code>	<code>guest_r</code>
<code>logadm_r</code>	<code>nx_server_r</code>	<code>object_r</code>	<code>secadm_r</code>
<code>staff_r</code>	<code>sysadm_r</code>	<code>system_r</code>	<code>unconfined_r</code>

SELinux Roles			
user_r	webadm_r	xguest_r	

2.2.2 Selinux sensivity

2.3 Selinux Policies

Las politicas se guardan en XML en el directorio /var/lib/setroubleshoot/setroubleshoot.xml

3 Casos especiales

3.1 Contenedores

4 Escenarios

4.1 Escenario 1

4.2 Escenario 2

5 Referencias

5.1 Referencia archivos

5.2 Referencia archivos de configuracion

- /etc/selinux/config
 - Controla la configuracion de SELinux en el sistema.
 - `grep ^SELINUX= /etc/selinux/config => Permissive||Enforcing`
- /sys/fs/selinux/enforce
 - Archivo que indica el estado de selinux
 - `cat /sys/fs/selinux/enforce => 0/1`
- /sys/fs/selinux
 - Directorio con toda la configuracion de selinux
- /etc/default/grub
 - In grub (/etc/default/grub) `GRUB_CMDLINE_LINUX="selinux=0"` to disable

5.3 Referencia archivos de errores

- /var/log/audit/*

5.4 Referencias comandos

5.4.1 Desactivar acciones silenciosas

```
1 # -D desactiva mecanismos "don't audit" (bash)
2 semodule -DB
3 # Para volver a activar sirve con reconstruir las politicas
4 semodule -B
```

5.4.2 Retiquetar el sistema de archivos

5.4.2.1 Grano Grueso

```
1 # al reiniciar el sistema reetiqueta el sistema de archivos si selinux (bash)
  detecta este archivo
2 touch /.autorelabel
```

```
1 # Verifica los contextos de seguridad de los archivos sin realizar (bash)
  cambios.
2 fixfiles check
3
4 # Restaura el contexto de seguridad de los archivos a sus valores
  predeterminados.
5 fixfiles restore
6
7 # Pregunta por la eliminacion de /tmp y reetiqueta todos los archivos del
  sistema de archivos.
8 fixfiles relabel
9
10 # Verifica que todos los archivos tengan el contexto de seguridad correcto.
11 fixfiles verify
12
13 # Reetiqueta todo el sistema
14 fixfiles -F onboot
15
16 # Estos comandos pueden tener como ultimo parametro la carpeta padre o
  archivo a reetiquetar
17 fixfiles check [folder|file]
```

5.4.2.2 Grano Fino

```
1 # Cambia el contexto de seguridad de un archivo o directorio. (bash)
2 chcon
```

```
1 # Verifica el contexto de seguridad de un archivo utilizando las (bash)
  reglas de política de SELinux.
2 matchpathcon
```

```

1 # Restaura el contexto de seguridad predeterminado de un archivo o (bash)
  directorio.
2 restorecon

```

5.4.3 Monitorizacion Basica SELinux

```

1 # Obtiene el estado actual de cumplimiento de politicas de selinux en (bash)
  el sistema
2 getenforce
3 # Ouput: Enforcing|Permissive

```

```

1 # Obtiene el estado basico de Selinux en el sistema (bash)
2 sestatus
3 # Output:
4 # SELinux status:                enabled
5 # SELinuxfs mount:              /sys/fs/selinux
6 # SELinux root directory:       /etc/selinux
7 # Loaded policy name:           targeted
8 # Current mode:                 enforcing
9 # Mode from config file:        enforcing
10 # Policy MLS status:            enabled
11 # Policy deny_unknown status:   allowed
12 # Memory protection checking:   actual (secure)
13 # Max kernel policy version:    33

```

```

1 # Obtiene el estado basico de los componenetes de las politicas de (bash)
  Selinux en el sistema
2 seinfo
3 # Ouput:
4 # Statistics for policy file: /sys/fs/selinux/policy
5 # Policy Version:              33 (MLS enabled)
6 # Target Policy:               selinux
7 # Handle unknown classes:      allow
8 #   Classes:                   134   Permissions:                   460
9 #   Sensitivities:              1   Categories:                   1024
10 #   Types:                     5266  Attributes:                    264
11 #   Users:                     8   Roles:                         15
12 #   Booleans:                  365   Cond. Expr.:                  398
13 #   Allow:                     68070  Neverallow:                    0
14 #   Auditallow:                181   Dontaudit:                    8830
15 #   Type_trans:                284397  Type_change:                   94
16 #   Type_member:               37   Range_trans:                  6164
17 #   Role allow:                40   Role_trans:                   419
18 #   Constraints:              70   Validatetrans:                0
19 #   MLS Constrain:            72   MLS Val. Tran:                0
20 #   Permissives:               9   Polcap:                       6
21 #   Defaults:                 7   Typebounds:                   0
22 #   Allowxperm:                0   Neverallowxperm:              0
23 #   Auditallowxperm:          0   Dontauditxperm:               0
24 #   Ibendportcon:              0   Ibkeycon:                     0

```

25	#	Initial SIDs:	27	Fs_use:	35
26	#	Genfscon:	110	Portcon:	665
27	#	Netifcon:	0	Nodecon:	0

5.4.4 Obtencion de logs de SELinux

SELinux setroubleshootd es el proceso que se encarga de gestionar los errores y recomendaciones al usuario de selinux [8]

```
1 # Obtiene los logs relacionados con intentos de accesos no autorizados (bash)
  de recursos
2 journalctl -e -u setroubleshootd
```

```
1 # Obtiene los logs relacionados con intentos de accesos no autorizados (bash)
  de recursos sis usar comando de systemd
2 cat /var/log/audit/audit.log
```

```
1 # Obtiene los ultimos errores lanzados por selinux (bash)
2 ausearch -m avc
3 # En concreto maneja la salida de proceso de auditoria que es la categoria
  en la que esta SELinux
```

5.4.5 Lectura de Etiquetas

```
1 # Obtiene las etiquetas del usuario (bash)
2 id -Z
3 # Output:
4 # unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

```
1 # Obtiene las etiquetas de los archivos (bash)
2 ls -Z
3 # Output:
4 # unconfined_u:object_r:admin_home_t:s0 disk
  unconfined_u:object_r:admin_home_t:s0 podman
  unconfined_u:object_r:admin_home_t:s0 test-secret.asc
5 # unconfined_u:object_r:admin_home_t:s0 mnt
  unconfined_u:object_r:admin_home_t:s0 test.asc
6 ls -lZ
7 # Output:
8 # total 8
9 # drwxr-xr-x. 3 root root unconfined_u:object_r:admin_home_t:s0 89 Nov 17
  21:38 disk
10 # drwxr-xr-x. 2 root root unconfined_u:object_r:admin_home_t:s0 6 Nov 24
  02:25 mnt
11 # drwxr-xr-x. 3 root root unconfined_u:object_r:admin_home_t:s0 19 Nov 17
  21:40 podman
12 # -rw-r--r--. 1 root root unconfined_u:object_r:admin_home_t:s0 1745 Nov 23
  17:54 test.asc
```

```
13 # -rw-r--r--. 1 root root unconfined_u:object_r:admin_home_t:s0 3779 Nov 23
    17:54 test-secret.asc
```

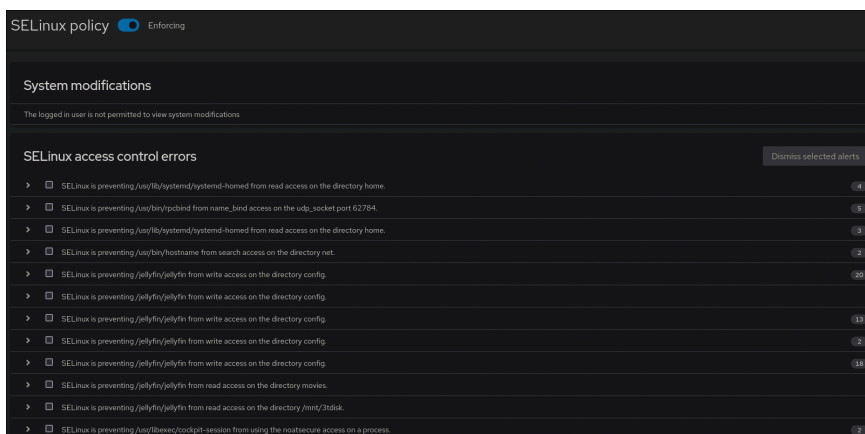
```
14
```

```
1 # Lista los atributos de un proceso (bash)
2 ls /proc/$PID/attr
3 # Output:
4 # current exec fscreate keycreate prev sockcreate
5
6 # Obtiene las etiquetas de procesos
7 ps -Z
8 # Output:
9 # LABEL PID TTY TIME CMD
10 # unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 5937 pts/1 00:00:00
    bash
11 # unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 6099 pts/1 00:00:00
    ps
```

5.5 Herramientas complementarias

5.5.1 Cockpit

Cockpit [9] es una interfaz grafica para servidores, en ella podemos ver diferentes aspectos de un servidor, en este caso las politicas de SELinux que aplica junto a un yaml de ansible para ejecutar esas mismas politicas que han sido modificadas de la base en otros equipos



SELinux policy	
System modifications	
The logged-in user is not permitted to view system modifications.	
SELinux access control errors	
> <input type="checkbox"/> SELinux is preventing /usr/lib/systemd/systemd from read access on the directory home.	(4)
> <input type="checkbox"/> SELinux is preventing /usr/bin/pctsd from name_bind access on the udp_socket port 62784.	(5)
> <input type="checkbox"/> SELinux is preventing /usr/lib/systemd/systemd from read access on the directory home.	(3)
> <input type="checkbox"/> SELinux is preventing /usr/bin/hotswap from search access on the directory net.	(2)
> <input type="checkbox"/> SELinux is preventing /usr/sbin/yafm from write access on the directory config.	(20)
> <input type="checkbox"/> SELinux is preventing /usr/sbin/yafm from write access on the directory config.	(2)
> <input type="checkbox"/> SELinux is preventing /usr/sbin/yafm from write access on the directory config.	(13)
> <input type="checkbox"/> SELinux is preventing /usr/sbin/yafm from write access on the directory config.	(3)
> <input type="checkbox"/> SELinux is preventing /usr/sbin/yafm from write access on the directory config.	(16)
> <input type="checkbox"/> SELinux is preventing /usr/sbin/yafm from read access on the directory mounts.	(2)
> <input type="checkbox"/> SELinux is preventing /usr/sbin/yafm from read access on the directory /mnt/Toshiba.	(2)
> <input type="checkbox"/> SELinux is preventing /usr/libexec/cgcpfd-session from read access on a process.	(2)
> <input type="checkbox"/> SELinux is preventing /usr/libexec/cgcpfd-session from using the rbindfs access on a process.	(2)
> <input type="checkbox"/> SELinux is preventing /usr/libexec/cgcpfd-session from using the sighv access on a process.	(3)
> <input type="checkbox"/> SELinux is preventing /usr/lib/udev/chkconfig from using the rbindfs access on a process.	(3)
> <input type="checkbox"/> SELinux is preventing /usr/lib/udev/chkconfig from using the rbindfs access on a process.	(3)
> <input type="checkbox"/> SELinux is preventing /usr/lib/udev/chkconfig from using the sighv access on a process.	(3)

Cockpit adicionalmente nos muestra de forma sencilla los fallos de acceso y sus formas de permitir ademas de un boton para implementarlas con un solo click

[illegible][illegible]

5.5.2 Udica

6 Glosario

CIL – Common Intermediate Language 3

DAC – Discretionary Access Control 2, 4

LSM – Linux Security Modules: Es un marco que proporciona ganchos dentro del kernel de Linux en varios lugares, incluyendo los puntos de entrada de llamadas al sistema. Cuando estos "hooks" se activan, las implementaciones de seguridad registradas, como SELinux, ejecutan sus funciones automáticamente. 2

Label – Label o etiqueta 1, 2, 4, 5, 10

MAC – Mandatory Access Control 2, 4

MLS – Multi-Level Security: Tambien conocido pero desactualizado MCS o Multilevel Category Security 2

SELinux – Security Enhanced Linux 2, 3, 6, 10, 11

UBAC – user-based access control 6

dominio – Dominio o tipo 4

evento: Accion en el sistema que accede o modifica un recurso o archivo (en linux todo es un archivo) 3

References

- [1] Accessed: Nov. 30, 2024. [Online]. Available: https://en.wikipedia.org/wiki/Discretionary_access_control
- [2] Accessed: Nov. 30, 2024. [Online]. Available: https://en.wikipedia.org/wiki/Multilevel_security
- [3] Accessed: Nov. 30, 2024. [Online]. Available: https://en.wikipedia.org/wiki/Security-Enhanced_Linux
- [4] Accessed: Nov. 30, 2024. [Online]. Available: https://en.wikipedia.org/wiki/Mandatory_access_control
- [5] Accessed: Nov. 30, 2024. [Online]. Available: https://en.wikipedia.org/wiki/Linux_Security_Modules
- [6] [Online]. Available: https://people.redhat.com/duffy/selinux/selinux-coloring-book_A4-Stapled.pdf
- [7] Accessed: Nov. 30, 2024. [Online]. Available: <https://selinuxproject.org/page/PolicyLanguage>
- [8] Accessed: Nov. 30, 2024. [Online]. Available: <https://linux.die.net/man/8/setroubleshootd>

-
- [9] Accessed: Nov. 30, 2024. [Online]. Available: <https://github.com/cockpit-project/cockpit>
 - [10] Accessed: Nov. 30, 2024. [Online]. Available: https://en.wikipedia.org/wiki/Linux_Security_Modules
 - [11] Accessed: Nov. 30, 2024. [Online]. Available: https://en.wikipedia.org/wiki/Linux_Security_Modules
 - [12] Accessed: Nov. 30, 2024. [Online]. Available: <https://documentation.suse.com/sle-micro/6.1/html/Micro-selinux/index.html>
 - [13] Sven Vermeulen, *SELinux System Administration v3*. 2020. [Online]. Available: [https://public.jdstone1.com/books_and_magazines/Computer_Books/Operating_Systems/SELinux%20System%20Administration%20\(3rd%20ed\).pdf](https://public.jdstone1.com/books_and_magazines/Computer_Books/Operating_Systems/SELinux%20System%20Administration%20(3rd%20ed).pdf)
 - [14] Accessed: Nov. 30, 2024. [Online]. Available: https://docs.redhat.com/en/documentation/red_hat_enterprise_linux/9/html/using_selinux/getting-started-with-selinux_using-selinux
 - [15] Accessed: Nov. 30, 2024. [Online]. Available: https://docs.redhat.com/en-us/documentation/red_hat_enterprise_linux/7/pdf/selinux_users_and_administrators_guide/Red_Hat_Enterprise_Linux-7-SELinux_Users_and_Administrators_Guide-en-US.pdf
 - [16] Accessed: Nov. 30, 2024. [Online]. Available: <https://selinuxproject.org/page/FAQ>
 - [17] Accessed: Nov. 30, 2024. [Online]. Available: <https://github.com/SELinuxProject/selinux-notebook/blob/main/src/title.md>
 - [18] Accessed: Nov. 30, 2024. [Online]. Available: https://docs.redhat.com/en/documentation/red_hat_enterprise_linux/6/html/security-enhanced_linux/sect-security-enhanced_linux-fixing_problems-searching_for_and_viewing_denials#sect-Security-Enhanced_Linux-Fixing_Problems-Searching_For_and_Viewing_Denials
 - [19] Accessed: Nov. 30, 2024. [Online]. Available: <https://www.redhat.com/en/blog/selinux-denial2>
 - [20] Accessed: Nov. 30, 2024. [Online]. Available: https://docs.redhat.com/en/documentation/red_hat_enterprise_linux/8/html/using_selinux/troubleshooting-problems-related-to-selinux_using-selinux#identifying-selinux-denials_troubleshooting-problems-related-to-selinux
 - [21] Accessed: Nov. 30, 2024. [Online]. Available: https://docs.redhat.com/en/documentation/red_hat_enterprise_linux/7/html/security_guide/sec-creating_audit_reports#sec-Creating_Audit_Reports
 - [22] Accessed: Nov. 30, 2024. [Online]. Available: https://docs.redhat.com/en/documentation/red_hat_enterprise_linux/7/html/selinux_users_and_administrators_guide/sect-security-enhanced_linux-working_with_selinux-selinux_contexts_labeling_files

- [23] Accessed: Nov. 30, 2024. [Online]. Available: https://docs.redhat.com/en/documentation/red_hat_enterprise_linux/9/html/using_selinux/configuring-selinux-for-applications-and-services-with-non-standard-configurations_using-selinux#configuring-selinux-for-applications-and-services-with-non-standard-configurations_using-selinux
- [24] Accessed: Nov. 30, 2024. [Online]. Available: <https://paritoshbh.me/blog/allow-access-port-selinux-firewall>
- [25] Accessed: Nov. 30, 2024. [Online]. Available: <https://blog.ryanmartin.me/selinux-containers>
- [26] Accessed: Nov. 30, 2024. [Online]. Available: <https://github.com/containers/container-selinux>
- [27] Accessed: Nov. 30, 2024. [Online]. Available: <https://danwalsh.livejournal.com/76016.html>
- [28] Accessed: Nov. 30, 2024. [Online]. Available: <https://danwalsh.livejournal.com/81143.html>
- [29] Accessed: Nov. 30, 2024. [Online]. Available: <https://danwalsh.livejournal.com/77830.html>
- [30] Accessed: Nov. 30, 2024. [Online]. Available: <https://danwalsh.livejournal.com/81756.html>
- [31] Accessed: Nov. 30, 2024. [Online]. Available: <https://access.redhat.com/articles/6999267>
- [32] Accessed: Nov. 30, 2024. [Online]. Available: <https://www.techtarget.com/searchDataCenter/tutorial/How-to-write-an-SELinux-policy>
- [33] Accessed: Nov. 30, 2024. [Online]. Available: <https://www.techtarget.com/searchDataCenter/tutorial/How-to-configure-SELinux-for-applications-and-services>
- [34] Accessed: Nov. 30, 2024. [Online]. Available: <https://github.com/SELinuxProject/selinux/wiki/Tools>
- [35] Accessed: Nov. 30, 2024. [Online]. Available: <https://github.com/containers/udica>
- [36] Accessed: Nov. 30, 2024. [Online]. Available: <https://wiki.gentoo.org/wiki/SELinux/Tutorials>
- [37] Accessed: Nov. 30, 2024. [Online]. Available: <https://wiki.gentoo.org/wiki/SELinux>
- [38] Accessed: Nov. 30, 2024. [Online]. Available: <https://github.com/SELinuxProject/selinux-notebook/blob/main/src/title.md>
- [39] Accessed: Nov. 30, 2024. [Online]. Available: <https://www.man7.org/linux/man-pages/man8/ausearch.8.html>
- [40] Accessed: Nov. 30, 2024. [Online]. Available: <https://prefetch.net/blog/2010/11/02/configuring-a-linux-nfs-server-in-a-selinux-managed-environment/>