Actinver

Security Enhanced Linux (SELinux)

Alex Callejas | Red Hat

Octubre 2025

Jornada de Ciberseguridad Actinver

Actinver

Alex Callejas

Content Architect @ Red Hat

@dark_axl

github.com/AlexCallejas

t.me/FedoraMexico

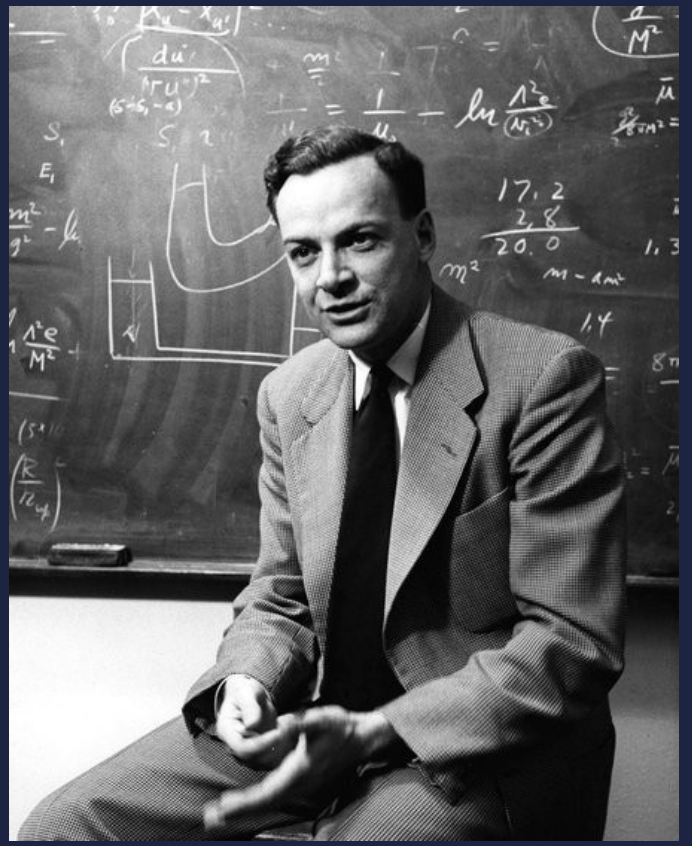
Geek by nature, Linux by choice, Fedora of course!

Jornada de Ciberseguridad Actinver

Actinver

“Si no puedes explicar algo en términos simples, significa que no lo entiendes.”

Richard P. Feynman



Actinver

SELinux

- Es complejo
- No funciona
- Es mejor deshabilitarlo

Actinver

¿Cómo funciona SELinux?

¿Qué es?

SELinux es un sistema de **ETIQUETADO**, lo que significa que cada *proceso, archivo, directorio y objeto* del sistema tiene una **ETIQUETA**. Las **políticas** controlan el **acceso** entre los *procesos etiquetados* y los *objetos etiquetados*. El **kernel** hace cumplir estas reglas.

Conceptos básicos

Los dos conceptos más importantes son: **Labeling** (archivos, procesos, puertos, etc.) y **Type enforcement** (que aísla los procesos entre sí según su tipo).

Formato

El formato de etiquetas es:

`user:role:type:level` (*opcional*)

Actinver

¿Cómo funciona SELinux?

Archivo de configuración	`/etc/selinux/config`
Obtener modo	`# getenforce`
Cambiar modo	`# setenforce`
Status	`# sestatus`
Re-etiquetar sistema	`# touch /.autorelabel ; reboot`

SELINUX IS A LABELING SYSTEM

Actinver

¿Cómo funciona SELinux?

Ejemplo práctico

Apache Web Server

- Binario: **`/usr/sbin/httpd`** → `httpd_exec_t`
- Archivos de configuración: **`/etc/httpd`** → `httpd_config_t`
- Logs: **`/var/log/httpd`** → `httpd_log_t`
- Directorio de contenido: **`/var/www/html`** → `httpd_sys_content_t`
- Unit file: **`/usr/lib/systemd/system/httpd.service`** → `httpd_unit_file_d`
- Proceso: **`/usr/sbin/httpd -DFOREGROUND`** → `httpd_t`
- Puertos: **`80/tcp`**, **`443/tcp`** → `http_port_t` `httpd_t`

Política: Un proceso que se ejecuta en el contexto ***`httpd_t`*** sólo puede interactuar con objetos con la etiqueta ***`httpd_something_t`***.

SELINUX IS A LABELING SYSTEM

Actinver

¿Qué trata de decirme SELinux?

Troubleshooting/Herramientas

1. Etiquetado

Es el error más común.

- Agregar o modificar contexto: **`semanage`**
- Aplicar cambios de contexto a la política: **`restorecon`**
- Comprobar contexto de un archivo: **`matchpathcon`**

2. Necesita saber

Aplicaciones confinadas configuradas de forma *no estándar*.

- Revisar booleanos: **`getsebool -a`**
- Encender/Apagar booleanos: **`setsebool [on|off]`**
- Comprobar contexto de un archivo: **`matchpathcon`**

3. Bugs

Bugs en la aplicación o en la política.

- Rutas inusuales en el código
- Configuraciones
- Redirección del **`stdout`**
- File descriptors
- Memoria ejecutable
- Librerías mal construídas

4. Sistema comprometido

- Si las herramientas nos diferencian contextos
- Si tienes dominios confinados que intentan:
  - Cargar modulos de kernel
  - Apagar el modo *enforcing*
  - Escribir a **`etc_t`**/**`shadow_t`**
  - Modificar reglas de **`iptables`**

Actinver

SELinux en la vida real

```
[root@vmtest01 ~]# cat ~/index.html
Hola Actinver!
[root@vmtest01 ~]# mv ~/index.html /var/www/html/
[root@vmtest01 ~]#
[root@vmtest01 ~]# wget localhost
--2025-10-20 20:49:22--  http://localhost/
Resolving localhost (localhost)... ::1, 127.0.0.1
Connecting to localhost (localhost)|::1|:80... connected.
HTTP request sent, awaiting response... 403 Forbidden
2025-10-20 20:49:22 ERROR 403: Forbidden.

[root@vmtest01 ~]#
```

SELINUX IS A LABELING SYSTEM

Actinver

SELinux en la vida real

```
[root@vmtest01 ~]# tail /var/log/httpd/error_log

[Mon Oct 20 20:49:22.387701 2025] [core:error] [pid 555:tid 139880684480256]
(13)Permission denied: [client ::1:54922] AH00035: access to /index.html denied
(filesystem path '/var/www/html/index.html') because search permissions are missing on
a component of the path

[root@vmtest01 ~]#
```

Actinver

SELinux en la vida real

```
[root@vmtest01 ~]# journalctl -f -t setroubleshoot

-- Logs begin at Mon 2025-10-20 20:49:18 UTC. --

Oct 20 20:49:22 vmtest01.rootzilopochtli.lab setroubleshoot[1539]: failed to retrieve
rpm info for /var/www/html/index.html

Oct 20 20:49:22 vmtest01.rootzilopochtli.lab setroubleshoot[1539]: SELinux is
preventing httpd from getattr access on the file /var/www/html/index.html. For
complete SELinux messages run: sealert -l 4cc11a34-9f9f-49c2-ba0f-0dc9a848ee38

Oct 20 20:49:22 vmtest01.rootzilopochtli.lab setroubleshoot[1539]: failed to retrieve
rpm info for /var/www/html/index.html

Oct 20 20:49:22 vmtest01.rootzilopochtli.lab setroubleshoot[1539]: SELinux is
preventing httpd from getattr access on the file /var/www/html/index.html. For
complete SELinux messages run: sealert -l 4cc11a34-9f9f-49c2-ba0f-0dc9a848ee38

[root@vmtest01 ~]#
```

SELINUX IS A LABELING SYSTEM

Actinver

SELinux en la vida real

```
[root@vmtest01 ~]# ausearch -m avc -ts recent

time->Thu Nov 08 20:49:22 2024

type=AVC msg=audit(1731120562.387:114): avc:  denied  { getattr } for  pid=555
comm="httpd" path="/var/www/html/index.html" dev="vda1" ino=3207
scontext=system_u:system_r:httpd_t:s0 tcontext=unconfined_u:object_r:admin_home_t:s0
tclass=file permissive=0

----

time->Thu Nov 08 20:49:22 2024

type=AVC msg=audit(1731120562.387:115): avc:  denied  { getattr } for  pid=555
comm="httpd" path="/var/www/html/index.html" dev="vda1" ino=3207
scontext=system_u:system_r:httpd_t:s0 tcontext=unconfined_u:object_r:admin_home_t:s0
tclass=file permissive=0

[root@vmtest01 ~]#
```

SELINUX IS A LABELING SYSTEM

Actinver

SELinux en la vida real

```
[root@vmtest01 ~]# ls -Z /var/www/html/index.html
unconfined_u:object_r:admin_home_t:s0 /var/www/html/index.html
[root@vmtest01 ~]#
[root@vmtest01 ~]# restorecon -v /var/www/html/index.html
Relabeled /var/www/html/index.html from unconfined_u:object_r:admin_home_t:s0 to
unconfined_u:object_r:httpd_sys_content_t:s0
[root@vmtest01 ~]#
[root@vmtest01 ~]# ls -Z /var/www/html/index.html
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/index.html
[root@vmtest01 ~]#
```

SELINUX IS A LABELING SYSTEM

Actinver

SELinux en la vida real

```
[root@vmtest01 ~]# wget localhost
--2025-10-20 21:23:15--  http://localhost/
Resolving localhost (localhost)... ::1, 127.0.0.1
Connecting to localhost (localhost)|::1|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 15 [text/html]
Saving to: ‘index.html’

index.html
100%[=====================================================>]          15  --.-KB/s     in 0s

2025-10-20 21:23:15 (2.82 MB/s) - ‘index.html’ saved [15/15]

[root@vmtest01 ~]#
```

SELINUX IS A LABELING SYSTEM

Actinver

¿Qué trata de decirme SELinux?

Troubleshooting: Análisis de los mensajes de negación

- Pre-requisitos:
  - `policycoreutils-python-utils` y `setroubleshoot-server`
- Procedimiento:
  1. Listar denegaciones

     ```
     # sealert -l "*"
     ```

  2. Habilitar auditoría de ruta completa de los objetos accedidos

     ```
     # auditctl -w /etc/shadow -p w -k shadow-write
     ```

  3. Limpiar la caché de setroubleshoot

     ```
     # rm -f /var/lib/setroubleshoot/setroubleshoot.xml
     ```

  4. Reproducir el comportamiento
  5. Repetir paso 1
  6. Deshabilitar auditoría

     ```
     # auditctl -W /etc/shadow -p w -k shadow-write
     ```

Actinver

Empoderando la administración con SELinux

Listando usuarios:

```
# semanage user -l
```

Listando mapeo de usuarios

```
# semanage login -l
```

Usuarios de SELinux

- **`user_u`**
  Usuarios estándar, no administrativos (no **`sudo`** ni **`su`**).
- **`sysadm_u`**
  Usuarios administrativos (**`sudo`** y **`su`**).
- **`staff_u`**
  Estos usuarios pueden utilizar **`sudo`** pero no **`su`**.

Actinver

Empoderando la administración con SELinux

```
[alex@vmtest01 ~]$ id -Z
unconfined_u:unconfined_t:unconfined_t:s0-s0:c0.c1023
[alex@vmtest01 ~]$ sudo -i
[root@vmtest01 ~]#
[root@vmtest01 ~]# getenforce
Enforcing
[root@vmtest01 ~]# semanage login -l

Login Name           SELinux User         MLS/MCS Range        Service

__default__          unconfined_u         s0-s0:c0.c1023       *
root                 unconfined_u         s0-s0:c0.c1023       *
[root@vmtest01 ~]#
```

SELINUX IS A LABELING SYSTEM

Actinver

Empoderando la administración con SELinux

```
[root@vmtest01 ~]# semanage login -m -s user_u -r s0 __default__
[root@vmtest01 ~]# semanage login -l

Login Name           SELinux User         MLS/MCS Range        Service

__default__          user_u               s0                   *
root                 unconfined_u         s0-s0:c0.c1023       *
[root@vmtest01 ~]# exit
logout
[alex@vmtest01 ~]$ exit
logout
```

SELINUX IS A LABELING SYSTEM

Actinver

Empoderando la administración con SELinux

```
[alex@vmtest01 ~]$ id -Z
user_u:user_r:user_t:s0
[alex@vmtest01 ~]$ sudo -i
sudo: PERM_SUDOERS: setresuid(-1, 1, -1): Operation not permitted
sudo: unable to open /etc/sudoers: Operation not permitted
sudo: setresuid() [0, 0, 0] -> [1000, -1, -1]: Operation not permitted
sudo: error initializing audit plugin sudoers_audit
[alex@vmtest01 ~]$ su -
Password: ********
su: Authentication failure
[alex@vmtest01 ~]$ exit
logout
```

SELINUX IS A LABELING SYSTEM

Actinver

Empoderando la administración con SELinux

```
[root@vmtest01 ~]# semanage login -m -s unconfined_u -r s0-s0:c0.c1023 __default__
[root@vmtest01 ~]# semanage login -l

Login Name           SELinux User         MLS/MCS Range        Service

__default__          unconfined_u         s0-s0:c0.c1023       *
root                 unconfined_u         s0-s0:c0.c1023       *
[root@vmtest01 ~]#
```

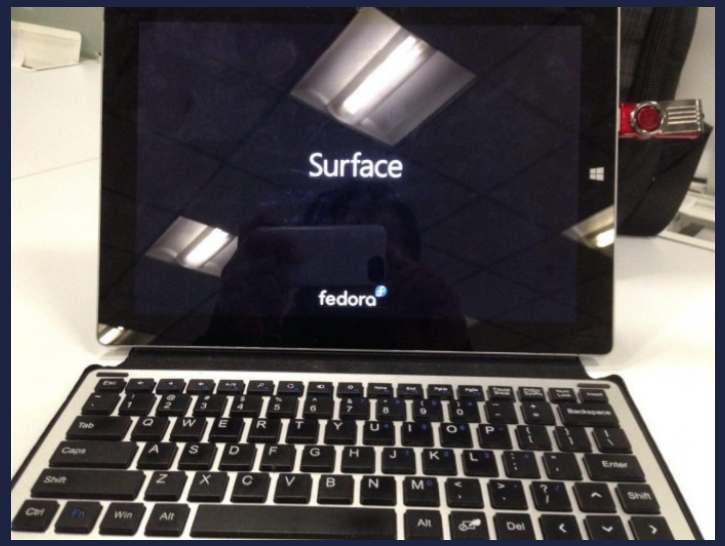
SELINUX IS A LABELING SYSTEM

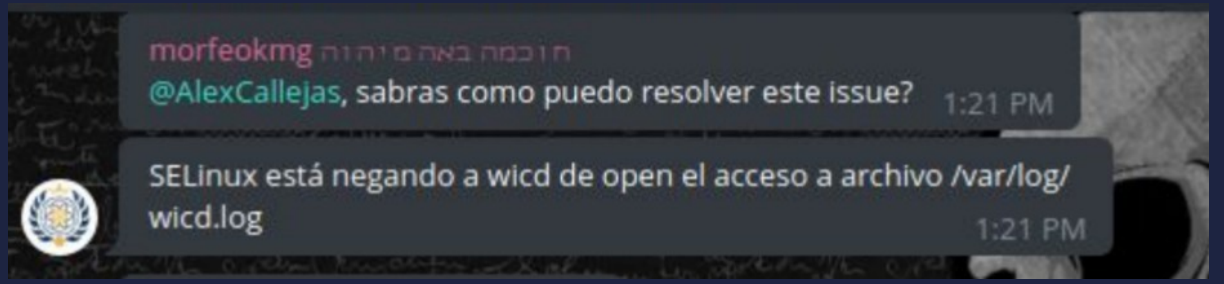
Actinver

SELinux en la vida real

Microsoft Surface con Fedora

- **`wicd`** en lugar de **`NetworkManager`**





SELINUX IS A LABELING SYSTEM

Actinver

SELinux en la vida real

```
[root@vmtest01 ~]# grep denied audit.log | cut -d { -f2 | sort -n | uniq -u
 create } for  pid=2670 comm="wicd" scontext=system_u:system_r:NetworkManager_t:s0
tcontext=system_u:system_r:NetworkManager_t:s0 tclass=appletalk_socket permissive=1
 create } for  pid=2670 comm="wicd" scontext=system_u:system_r:NetworkManager_t:s0
tcontext=system_u:system_r:NetworkManager_t:s0 tclass=ax25_socket permissive=1
 ioctl } for  pid=2670 comm="wicd" path="socket:[52681]" dev="sockfs" ino=52681 ioctlcmd=0x8b01
scontext=system_u:system_r:NetworkManager_t:s0 tcontext=system_u:system_r:NetworkManager_t:s0 tclass=ax25_socket
permissive=1
 ioctl } for  pid=2670 comm="wicd" path="socket:[52684]" dev="sockfs" ino=52684 ioctlcmd=0x8b01
scontext=system_u:system_r:NetworkManager_t:s0 tcontext=system_u:system_r:NetworkManager_t:s0 tclass=appletalk_socke
permissive=1
 setattr } for  pid=2214 comm="wicd" name="dhclient.conf.template" dev="dm-0" ino=437068
scontext=system_u:system_r:NetworkManager_t:s0 tcontext=unconfined_u:object_r:etc_t:s0 tclass=file permissive=0
 setattr } for  pid=2280 comm="wicd" name="dhclient.conf.template" dev="dm-0" ino=437068
scontext=system_u:system_r:NetworkManager_t:s0 tcontext=unconfined_u:object_r:etc_t:s0 tclass=file permissive=0
 setattr } for  pid=2573 comm="wicd" name="dhclient.conf.template" dev="dm-0" ino=437068
scontext=system_u:system_r:NetworkManager_t:s0 tcontext=unconfined_u:object_r:etc_t:s0 tclass=file permissive=0
 setattr } for  pid=2670 comm="wicd" name="dhclient.conf.template" dev="dm-0" ino=437068
scontext=system_u:system_r:NetworkManager_t:s0 tcontext=unconfined_u:object_r:etc_t:s0 tclass=file permissive=1
 setattr } for  pid=859 comm="wicd" name="dhclient.conf.template" dev="dm-0" ino=437068
scontext=system_u:system_r:NetworkManager_t:s0 tcontext=unconfined_u:object_r:etc_t:s0 tclass=file permissive=0
[root@vmtest01 ~]#
```

SELINUX IS A LABELING SYSTEM

Actinver

SELinux en la vida real

```
[root@vmtest01 ~]# ausearch  -c 'wicd' -if audit.log | audit2allow -M my_wicd
******************** IMPORTANT ***********************
To make this policy package active, execute:

semodule -i my_wicd.pp

[root@vmtest01 ~]#
[root@vmtest01 ~]# cat my_wicd.te

module my_wicd 1.0;

require {
        type NetworkManager_t;
        type etc_t;
        class ipx_socket create;
        class ax25_socket { create ioctl };
        class appletalk_socket { create ioctl };
        class file setattr;
}

#============= NetworkManager_t ==============
allow NetworkManager_t etc_t:file setattr;
allow NetworkManager_t self:appletalk_socket { create ioctl };
allow NetworkManager_t self:ax25_socket { create ioctl };
allow NetworkManager_t self:ipx_socket create;
[root@vmtest01 ~]#
```

SELINUX IS A LABELING SYSTEM

Actinver

SELinux en la vida real

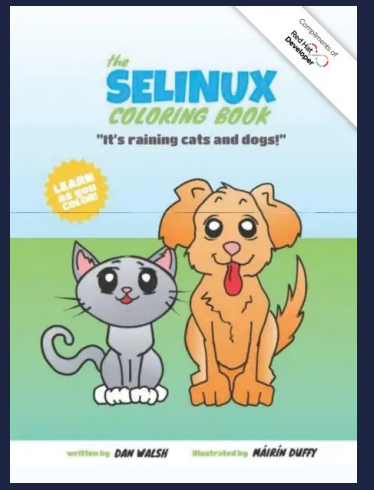
```
[root@vmtest01 ~]# dnf -y install selinux-policy-devel

[root@vmtest01 ~]# vi my_wicd.te

[root@vmtest01 ~]#  make -f /usr/share/selinux/devel/Makefile my_wicd.pp
Compiling targeted my_wicd module
Creating targeted my_wicd.pp policy package
rm tmp/my_wicd.mod tmp/my_wicd.mod.fc
[root@vmtest01 ~]#
```

SELINUX IS A LABELING SYSTEM

Actinver

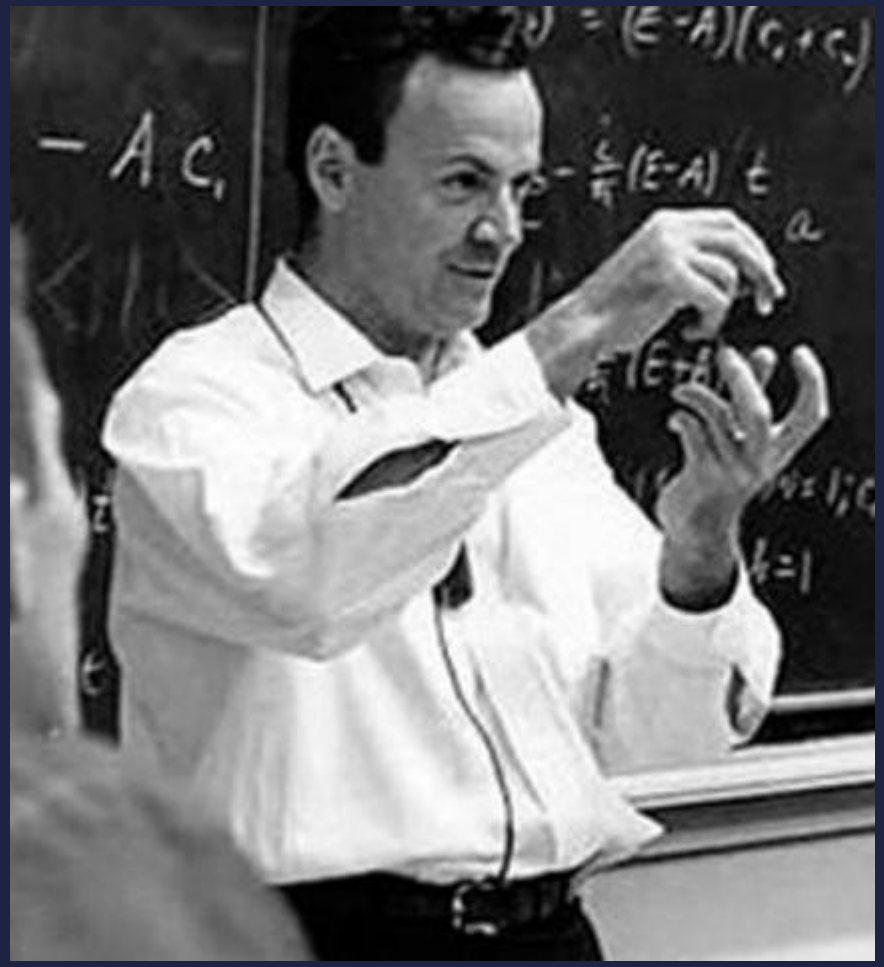
Referencias

- **Using SELinux**
  https://docs.redhat.com/en/documentation/red_hat_enterprise_linux/10/html-single/using_selinux/index
- **Fedora Project SELinux Docs**
  https://fedoraproject.org/wiki/SELinux
- **Dan Walsh’s Blog**
  https://danwalsh.livejournal.com/
- **A SysAdmin's guide to SELinux: 42 answers to the big questions**
  https://opensource.com/article/18/7/sysadmin-guide-selinux
- **A sysadmin's handy cheat sheet for SELinux**
  https://opensource.com/article/18/8/cheat-sheet-selinux



SELINUX IS A LABELING SYSTEM

Jornada de Ciberseguridad Actinver



“No te limites a aprender, ve y haz algo con ello.”

Richard P. Feynman

Actinver

¡Gracias!