

SELinux

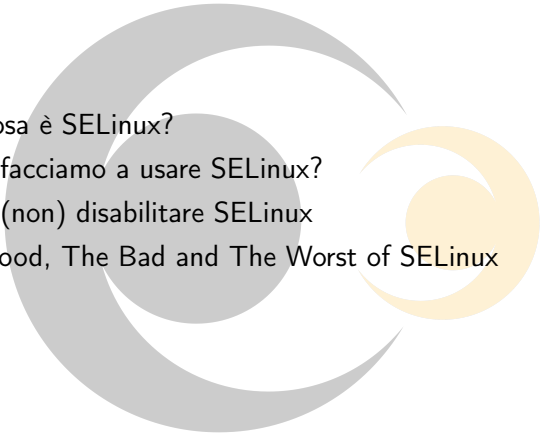
The Good, The Bad and The Worst

Luca Andrea Fusè

EXTRAORDY

- Consulente, RHCA e istruttore in Extraordy
 - TL;DR Faccio cose su Linux, OpenShift, Ansible e co.
- (Ex-)membro del [POuL](#), LUG del PoliMi
- Iscritto ad ILS nella sezione di Milano

Cosa andremo a vedere oggi

- 
- ❶ Che cosa è SELinux?
 - ❷ Come facciamo a usare SELinux?
 - ❸ Come (non) disabilitare SELinux
 - ❹ The Good, The Bad and The Worst of SELinux

Che cosa è SELinux?



Che cosa è SELinux?

- SELinux è un software che implementa un **Mandatory Access Control** (MAC) che viene implementato mediante le *LSM API* del kernel Linux.
- I permessi definiti da SELinux vengono validati dopo i permessi definiti dai software di **Discretionary Access Control** (DAC).

Che cosa è SELinux?

- I file e le risorse del sistema hanno delle “etichette” associate (*SELinux context*), che ne definiscono il tipo di entità e le proprietà di sicurezza.
- Queste etichette permettono al sistema di valutare se l'oggetto di una richiesta sia consentito o meno al soggetto richiedente.

Che cosa è SELinux?

- Il comportamento default è **Deny First**, ossia se non c'è una regola esplicita che lo permette allora l'interazione non viene consentita
- Se un'azione viene negata, questo tentativo di violazione viene loggato nell'**audit log**
- SELinux ha tre stati (enforcing, permissive, disabled) e tre modalità di funzionamento (**targeted**, minimum, mls).

Che cosa è SELinux?

Alcuni termini usati...

DAC

Discretionary Access Control, ossia limitazioni di accesso al contenuto appartenente a soggetti/gruppi. Questi permessi sono trasferibili.

e.g. Permessi classici su Linux

MAC

Mandatory Access Control, ossia il sistema limita la capacità di un soggetto di eseguire operazioni su un oggetto del sistema.

e.g. SELinux (ma anche AppArmor, Smack, TOMOYO)

Che cosa è SELinux?

Alcuni termini usati...

LSM API

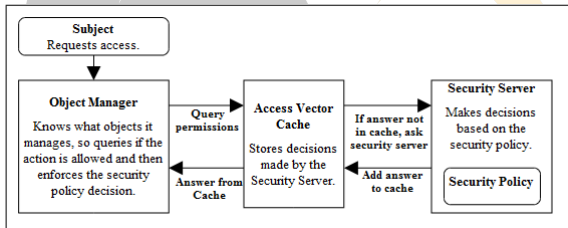
Linux Security Module, framework che fornisce un meccanismo con cui vari sistemi di sicurezza possono essere caricati dal kernel.

Che cosa è SELinux?

TL;DR

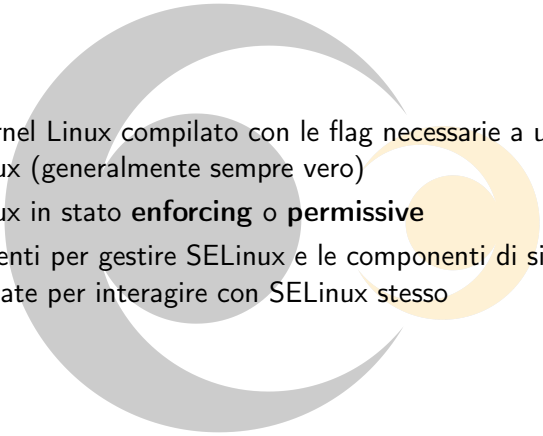
SELinux è il software che risponde alla domanda:

May <subject> do <action> to <object>?

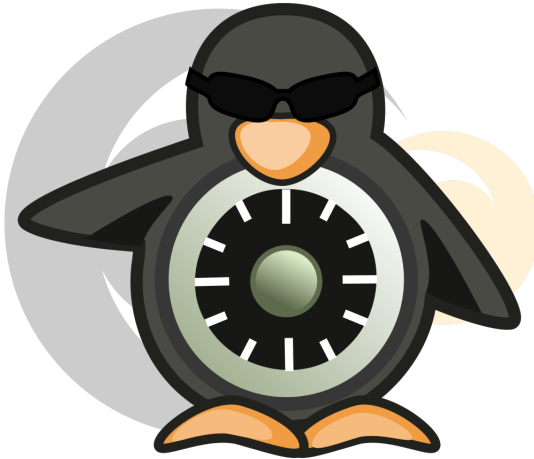


Che cosa è SELinux?

Cosa ci serve per usarlo

- 
- ❶ Un kernel Linux compilato con le flag necessarie a usare SELinux (generalmente sempre vero)
 - ❷ SELinux in stato **enforcing** o **permissive**
 - ❸ Strumenti per gestire SELinux e le componenti di sistema compilate per interagire con SELinux stesso

Come facciamo a usare SELinux?



Come facciamo a usare SELinux?

SELinux è attivo?

```
# getenforce
```

Il comando mi ritornerà se SELinux è in stato **permissive** oppure se è in stato **enforcing**

Come facciamo a usare SELinux?

Switch stato temporaneo

```
# setenforce 0/1
```

Il comando imposterà SELinux (se abilitato) in stato **permissive** o **enforcing**. Lo switch è momentaneo (non sopravvive al reboot).

Come facciamo a usare SELinux?

Switch modalità in modo permanente

```
# vim /etc/selinux/config
```

```
...
```

```
SELINUX=enforcing
```

```
...
```

Editando questo file posso impostare la modalità di esecuzione di SELinux all'avvio del sistema (reboot necessario).

Come facciamo a usare SELinux?

Vedere le label di SELinux di un file

```
# ls -Z myfile
```

```
unconfined_u:object_r:user_home_t:s0 myfile
```

Il comando `ls`, se compilato con le flag per SELinux, ha l'opzione `-Z` per poter mostrare le label assegnati a un file

Come facciamo a usare SELinux?

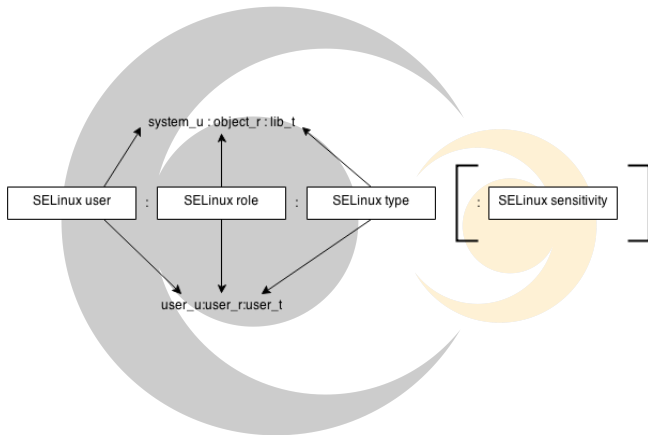
Vedere le label di SELinux di un processo

```
# ps -ZC sshd  
system_u:system_r:sshd_t:s0-s0:c0.c1023 138390 ?  
00:00:00 sshd
```

Il comando `ps`, se compilato con il supporto per SELinux, ha l'opzione `-Z` per poter mostrare le label di un processo.

Come facciamo a usare SELinux?

Cosa significano le label?



Come facciamo a usare SELinux?

Stati di SELinux

Enforcing

Stato di default di SELinux, tutte le operazioni eseguite vengono registrate e - in base alle policy definite - vengono permesse o negate.

Permissive

Stato in cui SELinux registra tutte le operazioni che vengono eseguita, ma non le impedisce.

Disabled

In questa stato SELinux non è abilitato (e di conseguenza non ci piace).

Come facciamo a usare SELinux?

Modalità di SELinux

Targeted

Modalità di funzionamento standard, esegue SELinux facendo solo **type enforcing**.

MLS e MCS

Multi-Level Security e Multi-Category Security: oltre all'uso del type enforcing, ai file vengono assegnate categorie e/o un certo livello di confidenzialità in modo da filtrare maggiormente chi vi può accedere.

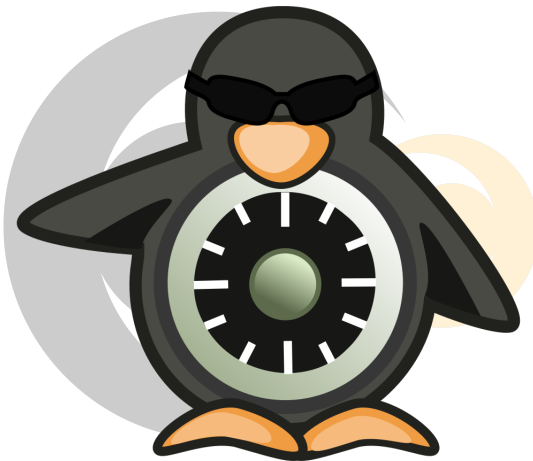
Come facciamo a usare SELinux?

Riabilitare SELinux

```
# sed -i s/^SELINUX\=disabled/SELINUX\=enforcing/  
# touch /.autorelabel
```

Per passare dalla modalità **disabled** alla modalità **enforcing** devo creare il file `.autorelabel`. I file modificati/creati quando SELinux è disabilitato sono privi delle label necessarie.

Come non disabilitare SELinux



Come non disabilitare SELinux

Problemi con SELinux

Tutto molto bello ma...

Quando eseguiamo il nostro applicativo, questo si schianta **male**.
SELinux, per qualche ragione, ne ha bloccato l'esecuzione.
Che facciamo?

Come non disabilitare SELinux

Problemi con SELinux

Abbiamo due soluzioni:

- 1 ~~Piangiamo~~ Disabilitiamo SELinux (**spoiler: no**)
- 2 Andiamo a capire quale policy va a bloccare l'oggetto

Come non disabilitare SELinux

Perché il mio applicativo viene bloccato da SELinux?

Quale azione viene bloccata da SELinux?

```
# ausearch -m AVC -ts today
```

Posto che il demone auditd sia in esecuzione, il comando ci mostra tutti gli errori generati da SELinux.

La ricerca viene fatta in `/var/log/auditd/audit.log`

Come non disabilitare SELinux

Perché il mio applicativo viene bloccato da SELinux?

Quale azione viene bloccata da SELinux?

```
# dnf install -y setroubleshoot-server  
# sealert -l "*" 
```

Ci mostra una spiegazione di quello che è avvenuto ed un possibile fix di sicurezza

Come non disabilitare SELinux

Come risolvere il problema?

Metodo 1

```
# chcon -t selinux_type /example/dir
```

Imposta temporaneamente un particolare contesto sulla directory target. Questo contesto non sopravvive ad un **restorecon**.

Come non disabilitare SELinux

Come risolvere il problema?

Metodo 2

```
# semanage fcontext -a -t selinux_type /dir/(.*)?  
# restorecon -Rv /dir
```

Il comando semanage imposta il contesto di un file o di una sottodirectory al livello del database interno di SELinux. Possiamo fare la stessa cosa anche con le porte.

Restorecon invece si assicura che questi contesti siano applicata correttamente.

Come non disabilitare SELinux

Come risolvere il problema?

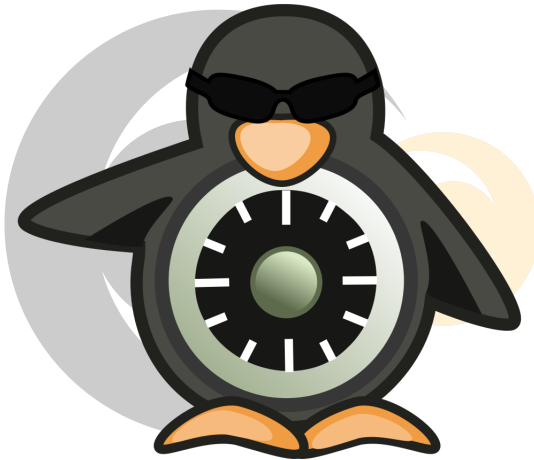
Metodo 3

```
# ausearch -c 'myprocess' --raw | audit2allow -M mypol  
# semodule -X 300 -i mypol.pp
```

Uso gli errori rilevati da auditd per generare una policy andando ad usare il tool audit2allow.



Di cosa non abbiamo parlato?



Di cosa non abbiamo parlato?

Creazione di policy custom

Selinux ci permette di creare delle policy custom con un linguaggio definito, le policy le possiamo importare sui nostri sistemi (mediante pacchetto del nostro sistema Linux o manualmente)

Di cosa non abbiamo parlato?

Gestione dello stato MLS e dello stato MCS

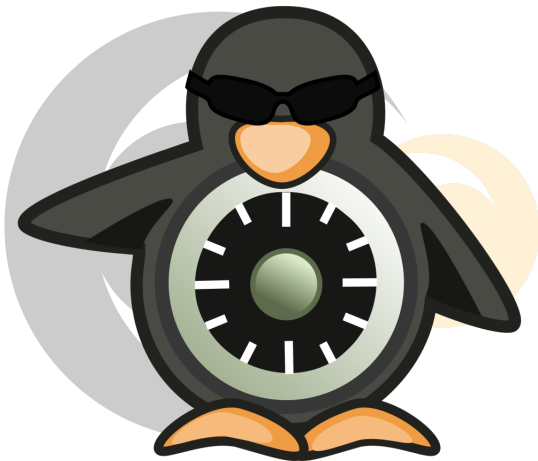
Non abbiamo parlato di come SELinux può gestire differenti stati di riservatezza dei dati, di come gestisce diverse tipologie di utenti (tipologie utenti di SELinux, non solo di sistema).

Di cosa non abbiamo parlato?

SELinux ed i container

SELinux ci permette di gestire i permessi di file e processi del nostro sistema. Ma i container sono processi isolati del nostro sistema. Non abbiamo visto come i container vengono influenzati da SELinux e degli strumenti che ci permettono di generare delle policy in modo comodo ed efficiente (il tool in questione è [Udica](#)).

The Good, The Bad and the Worst of SELinux



The Good, The Bad and the Worst of SELinux

The Good

- SELinux ci permette di aumentare la sicurezza dei nostri sistemi andando a limitare cosa possono fare i processi e gli utenti ben oltre i classici permessi di sistema.
- Ci mette al sicuro anche da eventuali bug di sicurezza non mitigati dall'applicazione (a volte, tutto dipende dal bug in questione)
- Anche se non lo abbiamo visto, ci permette di forzare l'applicazione di confidenzialità dei dati e dei processi

The Good, The Bad and the Worst of SELinux

The Bad

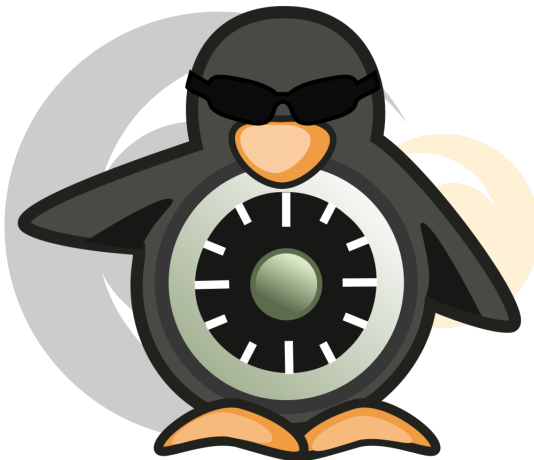
- A volte tutto questo “enforcing” ci rompe le scatole, le applicazioni non partono e non è immediatamente chiaro il motivo
- Se non abbiamo già delle policy configurate, dobbiamo risolvere i problemi riscontrati con configurazioni custom o policy custom
- SELinux non ci protegge da tutto, non è un antivirus e non mitiga tipi di attacchi che non copre

The Good, The Bad and the Worst of SELinux

The Worst: SELinux disabilitato

```
# vim /etc/selinux/config  
...  
SELINUX=disabled  
...
```

Domande?



Chi siamo?

Parliamo di Extraordy

Extraordy

- Ci occupiamo di consulenza sul mondo Linux (e affini), con una spiccata verticalità su Red Hat
- Ci occupiamo di formazione erogando i corsi ufficiali di Red Hat
- Abbiamo il podcast [Geek Talk](#) in cui vengono intervistati diversi ospiti
- Abbiamo il nostro magazine [Cappello Rosso](#)
- Oltre a questo, facciamo cose, beviamo birre, ~~facciamo flame su gli editor~~ abbiamo educate riflessioni sulle preferenze di editor

Chi siamo?

Parliamo di Extraordy

Vi piace quello che facciamo? Volete saperne di più?

- jobs.extraordy.com

- [Gentoo Wiki](#) (da cui anche uno degli schemi utilizzati)
- [SELinux Book](#) (da cui anche uno degli schemi utilizzati)
- [Documentazione di Red Hat su SELinux](#)
- [LSM API](#)
- [SELinux Coloring Book](#) by Red Hat
- [SELinux logo](#) by Máirín Duffy
- [Github di Extraordy](#)



Queste slides sono licenziate sotto [CC-BY-SA 4.0](#)

