

# SELinux

---

## Général

### Interrogations

#### Niveau de protection

```
getenforce
```

#### Paramètres

```
sestatus
```

#### Types associés à un fichier

```
ls -Z
```

#### Contexte de sécurité actif dans un terminal de commande

```
id -Z
```

#### Contexte de sécurité appliqué à un processus

Utiliser l'option -Z de la commande ps

```
ps -axZ
```

## Fichiers

### Fichier de configuration

Voir le contenu du fichier [/etc/selinux/config](#)

```
cat /etc/selinux/config
```

## Fichier de log

Voir le contenu du fichier </var/log/audit/audit.log>

---

[Haut de page](#)

## Activation

### Persistant

Modifier le fichier de configuration </etc/selinux/config> avec le niveau souhaité.

```
SELINUX=disabled      # désactivé
SELINUX=enforcing     # activé
SELINUX=permissive   # pas de blocage mais les infos sont tracées dans le
fichier /var/log/audit/audit.log
```

### Temporaire

Utiliser la commande setenforce. La modification s'applique jusqu'au prochain redémarrage.

```
sudo setenforce 0 # passage en mode permissive
sudo setenforce 1 # passage en mode enforcing
```

### Forcer le ré-étiquetage

Pour forcer le système à ré-étiqueter le système de fichier :

```
sudo touch /.autorelabel
sudo reboot
```

---

## Contexte SELinux

### Étiquettes

Le format des étiquettes est de la forme **user:role:type:level**

## Fichiers

### Interrogation

```
semanage fcontext -l
```

### Modification

Pour définir le contexte après modification du répertoire par défaut des log MySQL :

```
semanage fcontext -a -t mysqld_db_t "/path/to/my/custom/datadir(/.*)"?  
restorecon -Rv /path/to/my/custom/datadir
```

## Ports

### Interrogation

```
semanage port -l
```

### Modification

Pour définir le contexte mysql sur un port différent du port par défaut 3306 (3307 par exemple) :

```
semanage port -a -t mysqld_port_t -p tcp 3307
```

---

## Dépannage

### Recherche problèmes

- Installer le paquet **setroubleshoot**

```
sudo dnf install setroubleshoot # Redhat  
sudo apt install setroubleshoot # Ubuntu
```

- Lancer la commande suivante :

```
sudo sealert -l "*" 
```

---

[Haut de page](#)

## Sources

[Introduction à SELinux  
MySQL et SELinux](#)

---

[Haut de page](#)

From:

<https://wiki.iot-acis.fr/> - **Wiki**

Permanent link:

<https://wiki.iot-acis.fr/doku.php?id=all:bibles:linux:selinux>

Last update: **2024/11/25 11:29**

