

Sécurité sous Linux – Sécurité avancée

Security-Enhanced **Linux** ou **App**lication **Armor** (Ubuntu, Suze)

Modèle de sécurité ajouté au système standard de Linux

Permet de configurer les accès de chaque processus afin de les restreindre au strict nécessaire → Limitation des dégâts en cas de compromission

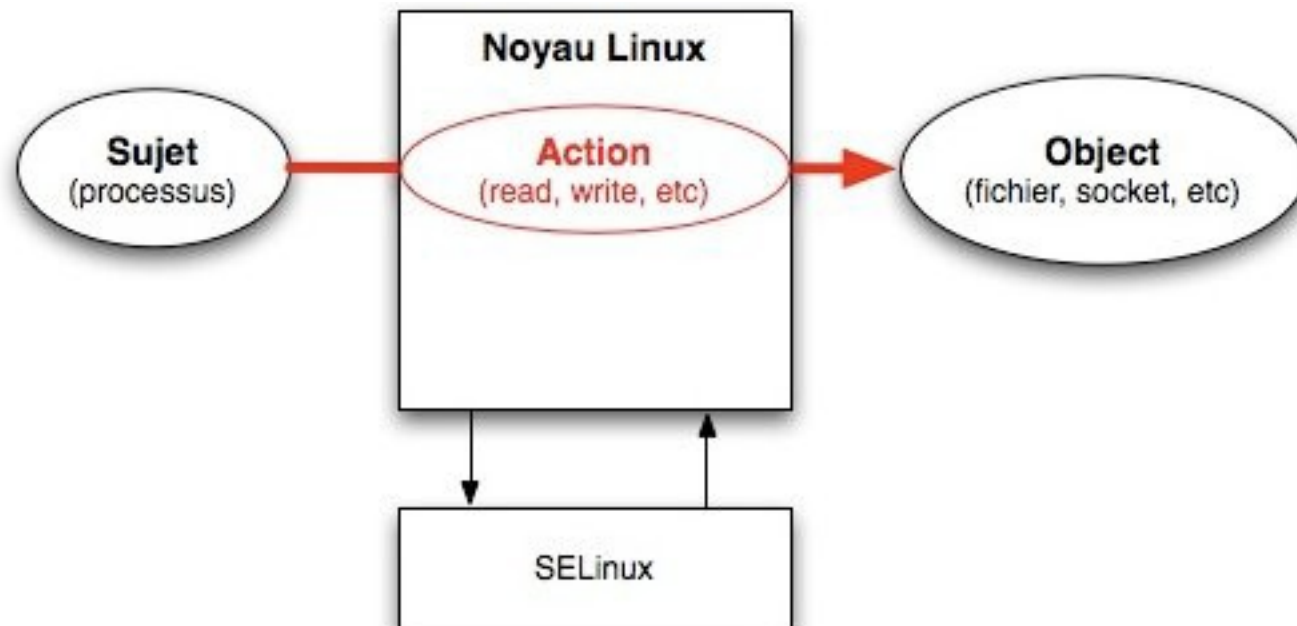
SELinux n'intervient pas si les droits classiques interdisent l'action

Sécurité sous Linux - SELinux

Appel système par un processus



Vérification par le noyau à travers SELinux (qui est intégré au noyau)



Sécurité sous Linux - SELinux

Quand SELinux est activé :

Chaque processus, chaque fichier, chaque socket, ... est associé à 3 informations:

Identité	-->	_u
Rôle	-->	_r
Type	-->	_t

Les droits accordés par SELinux sont liés aux types

Sécurité sous Linux - SELinux

SELinux activé: aucune action autorisée par défaut



Nécessité d'ajouter des règles (allow domain, type, permission)

Ex.:

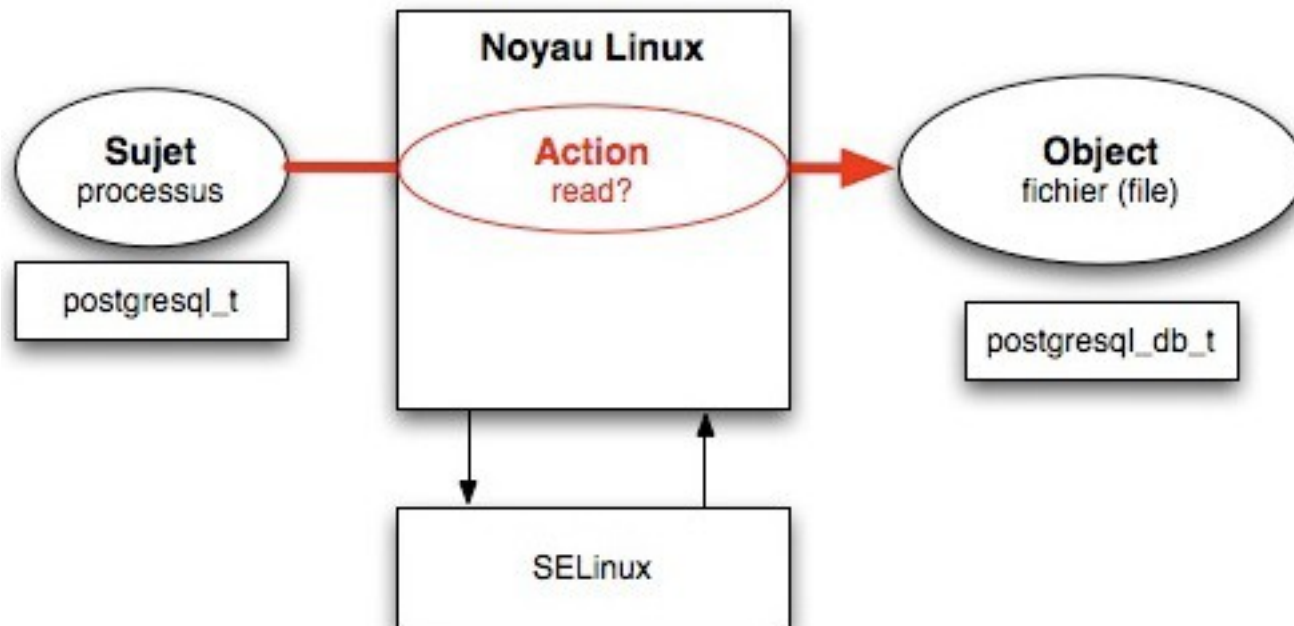
`allow postgresql_t postgresql_db_t : file create_file_perms`

`autorisation type du processus type de ressources : opération autorisée`

(Permet au processus PostgreSQL - SGBD - de lire les fichiers des bases de données PostgreSQL)

Sécurité sous Linux - SELinux

allow postgresql_t postgresql_db_t : file create_file_perms



allow postgresql_t postgresql_db_t:file create_file_perms;

Sécurité sous Linux - SELinux

```
allow firefox_t user_home_t : file { read write };
```

Cette règle autorise le navigateur firefox à lire et écrire dans les fichiers contenus dans le répertoire home de l'utilisateur courant et uniquement là

Remarque 1: les règles sont pré-écrites car apportées par les packages de règles installés (#apt-get install selinux-basics selinux-policy-default)

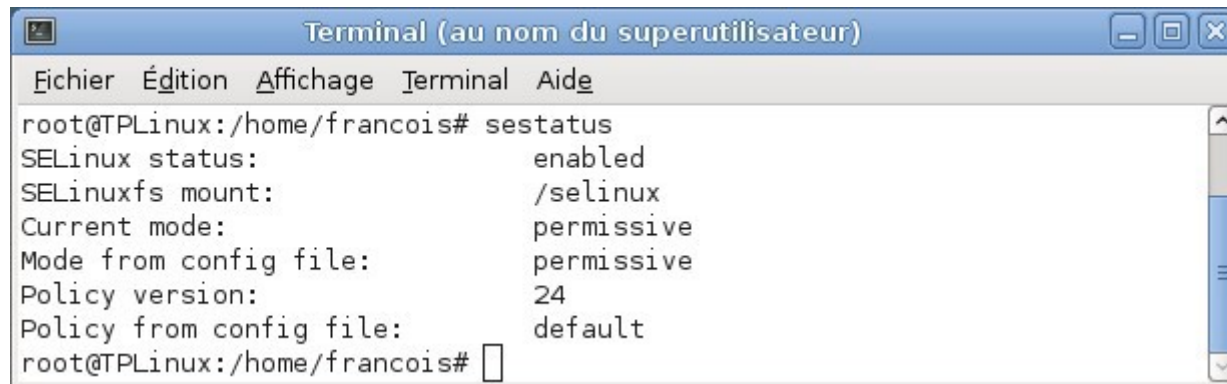
Remarque 2: SELinux n'est pas un pare-feu

Sécurité sous Linux - SELinux

Le pare-feu filtre les flux de données échangés entre une machine et le reste du réseau

SELinux filtre l'accès aux programmes/processus sur la station

#sestatus pour afficher le statut de SELinux

A terminal window titled "Terminal (au nom du superutilisateur)" showing the output of the 'sestatus' command. The window has a menu bar with "Fichier", "Édition", "Affichage", "Terminal", and "Aide". The terminal text shows SELinux is enabled, with the SELinuxfs mounted at /selinux, and the current mode is permissive, matching the mode from the config file. The policy version is 24, and the policy from the config file is default.

```
root@TPLinux:/home/francois# sestatus
SELinux status:                enabled
SELinuxfs mount:              /selinux
Current mode:                  permissive
Mode from config file:         permissive
Policy version:                24
Policy from config file:       default
root@TPLinux:/home/francois#
```

Permissive: SELinux est installé mais ne protège pas

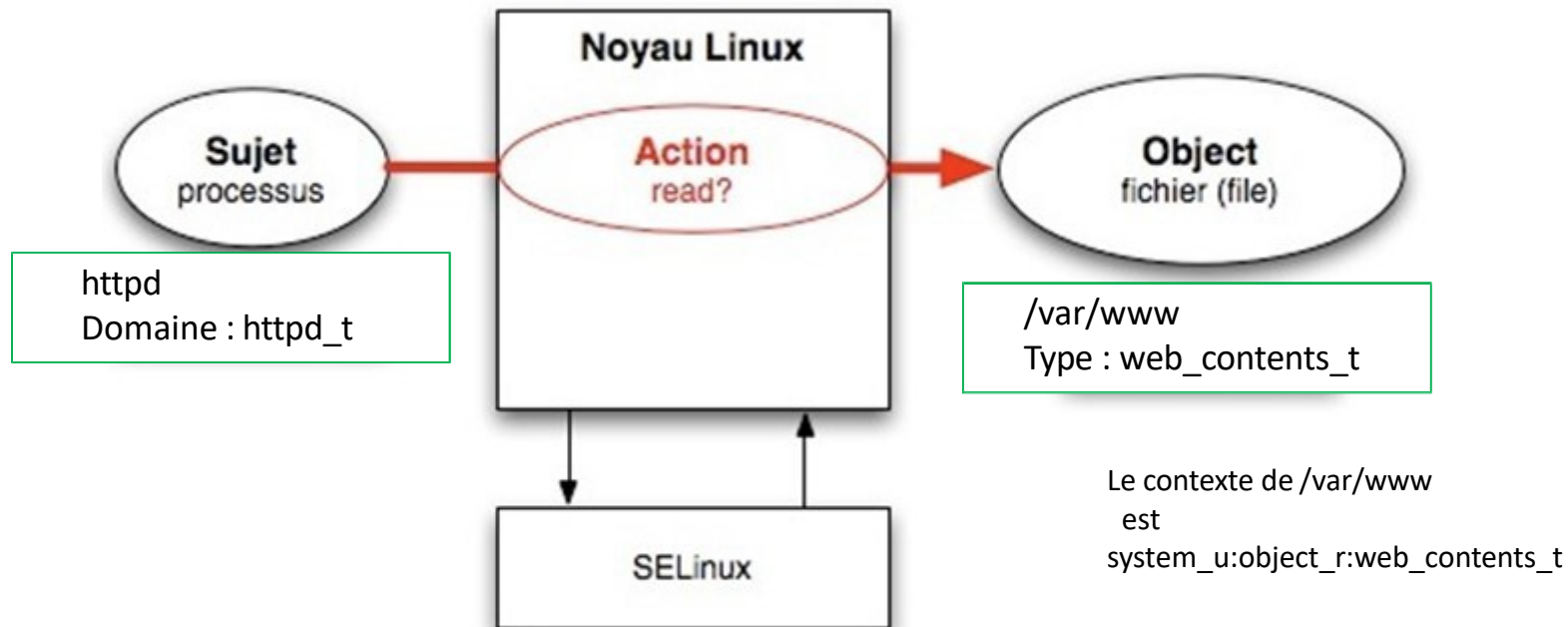
Enforcing: SELinux est installé et les règles s'appliquent

Sécurité sous Linux - SELinux

Exemples de l'utilité de SELinux :

- ❑ Un pirate rentre sur une machine à distance et essaie de lancer un shell
Le processus appelant le shell ("/bin/bash"...) devra être autorisé à lancer un shell par SELinux. Typiquement, on va associer un type shell_exec_t aux programmes de type shell et n'autoriser leur exécution qu'aux processus (grâce à leur type) qui en ont le besoin comme les programmes de login par exemple
- ❑ Un service Apache qui tourne en root sur un serveur SELinux se fait pirater
Le Security Server de SELinux, utilisant les politiques de sécurité qui ont été chargées dans le noyau, interdira au processus Apache agressé d'agir autrement que ce qu'on lui a imposé

Sécurité sous Linux - SELinux



Règle spécifique Apache (package) : **allow** httpd_t web_contents_t file:{ read };

Le domaine Apache ne peut pas accéder à d'autres répertoires (même si root possède le démon)

NB: Domaine = identifiant pour un processus / Type = identifiant pour une ressource

Sécurité sous Linux - SELinux

Par défaut, seul /var/www a le contexte web_contents_t

Problème :

Si certains répertoires de sites sont en dehors de /var/www

→ Apache ne peut les lire

Solution

Changer le contexte du fichier ou du répertoire

Les commandes

chcon

semanage