Security Enhanced Linux

SELinux

Jean-Denis Girard
http://www.SysNux.pf/

CLUSIR Tahiti - 17/10/2014

Plan

- Introduction
- Sécurité classique
- Contrôle d'accès obligatoire
- Principes
- Pratique
- Conclusion

Introduction

- SELinux est l'un des modules de sécurité disponibles pour Linux ; voir aussi Tomoyo, Smack, AppArmor, IMA, Yama.
- Initialement projet de recherche de l'université d'Utah (projet FLASK), puis repris par la NSA, le code a été fourni sous licence GPL en décembre 2000, puis incorporé au noyau Linux en août 2003 (2.6.0-test3).
- Activé sur Red Hat (CentOS, Fedora), disponible pour les autres distributions
- Implémentation d'un architecture de **contrôle d'accès obligatoire** (MAC) forte et flexible, dans l'objectif d'assurer le cloisonnement des données.
- SELInux est composé :
  - de contrôles intégrés au noyau (LSM),
  - d'utilitaires permettant de définir les politiques.

Sécurité classique

- Dans le schéma classique Unix, l'accès à une ressource (lecture `r`, écriture `w`, exécution `x`) est déterminé par l'utilisateur (propriétaire `u`, groupe `g` ou autre `o`).
- Le contrôle d'accès discrétionnaire (**DAC**) permet à l'utilisateur de déterminer les permissions des objets.

```
[jdg@tiare ~]$ touch /tmp/test
[jdg@tiare ~]$ ls -l /tmp/test
-rw-r-----. 1 jdg jdg 0 15 oct.  09:56 /tmp/test
[jdg@tiare ~]$ chmod g+w /tmp/test
[jdg@tiare ~]$ chmod o+r /tmp/test
[jdg@tiare ~]$ ls -l /tmp/test
-rw-rw-r--. 1 jdg jdg 0 15 oct.  09:56 /tmp/test
```

- Modèle insuffisant car un utilisateur (ou un programme compromis) pourrait donner accès à des données confidentielles.

MAC

- Le système d'exploitation contraint les utilisateurs ou programmes dans leurs accès aux ressources.
- Pour SELinux :
  - les **objets** sont des ressources système : fichiers, répertoires, sockets et autres périphériques,
  - les **sujets** sont les process (commandes ou programmes).
- Sujets et objets se voient attribué un contexte de sécurité.
- Le système détermine l'accès à un objet par un sujet selon la politique de sécurité chargée.
- Le **sujet ne peut pas modifier le contexte de sécurité d'un objet**.
- Ainsi un sujet est confiné.

Principes SELinux

- Supporte deux formes de MAC :
  - *Type Enforcement* (**TE**), les process fonctionnent dans certains domaines, et les actions sur les objets sont contrôlées par la politique de sécurité,
  - *Multi-Level Security* (**MLS**) / *Multi-Category Security* (**MCS**) : implémentation du modèle Bell – La Padula, qui apporte différents niveaux d'accès.
- Les utilisateurs Linux sont associés à des personnes ou des serveurs ; SELinux définit des **identités** qui correspondent généralement à des classes d'utilisateurs, par exemple `unconfined_u`, `staff_u`. La classe `system_u` est réservé aux process système.
- En outre, SELinux utilise la notion de **rôle** (**RBAC**) dans son contrôle d'accès TE. Chaque utilisateur est ainsi associé à un ou plusieurs rôles, exemple : `unconfined_r`, gest`_r`, `staff_r`.

- Finalement, SELinux introduit la notion de **type** (ou domaine) :
  - pour un sujet, il définit à quels process l'identité peut accéder,
  - pour un objet, il définit quelles sont les permissions de l'identité sur cet objet.

  Exemples : `user_home_t`, `httpd_t`.
- Ces trois éléments forment le **contexte de sécurité** SELinux, présenté sous forme de chaîne de caractères, par exemple :

  utilisateur : `unconfined_u:unconfined_r:unconfined_t`
  fichier utilisateur : `unconfined_u:object_r:user_home_t`
  process Apache : `system_u:system_r:httpd_t`

  On l'appelle aussi étiquette de sécurité ou simplement étiquette.
- Le contexte de sécurité est complété par le ou les niveaux de sécurité MLS et MCS :

  ```
  unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
  ```

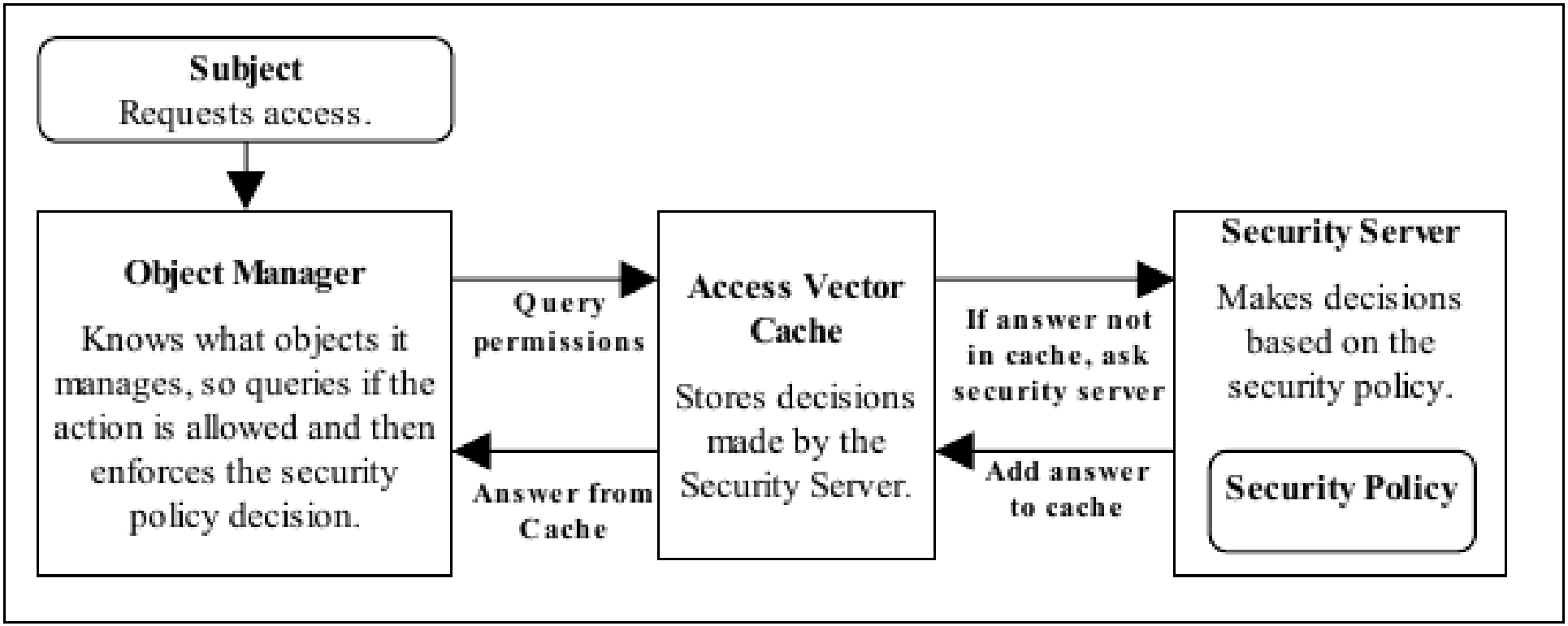
- L'étiquetage est maintenu par le système, soit par héritage, soit par l'application adaptée à SELinux, soit par des utilitaires. Par exemple, la **copie d'un fichier peut provoquer un changement de contexte**, alors qu'il est **conservé lors d'un déplacement**.

  Des transitions de types sont possibles.

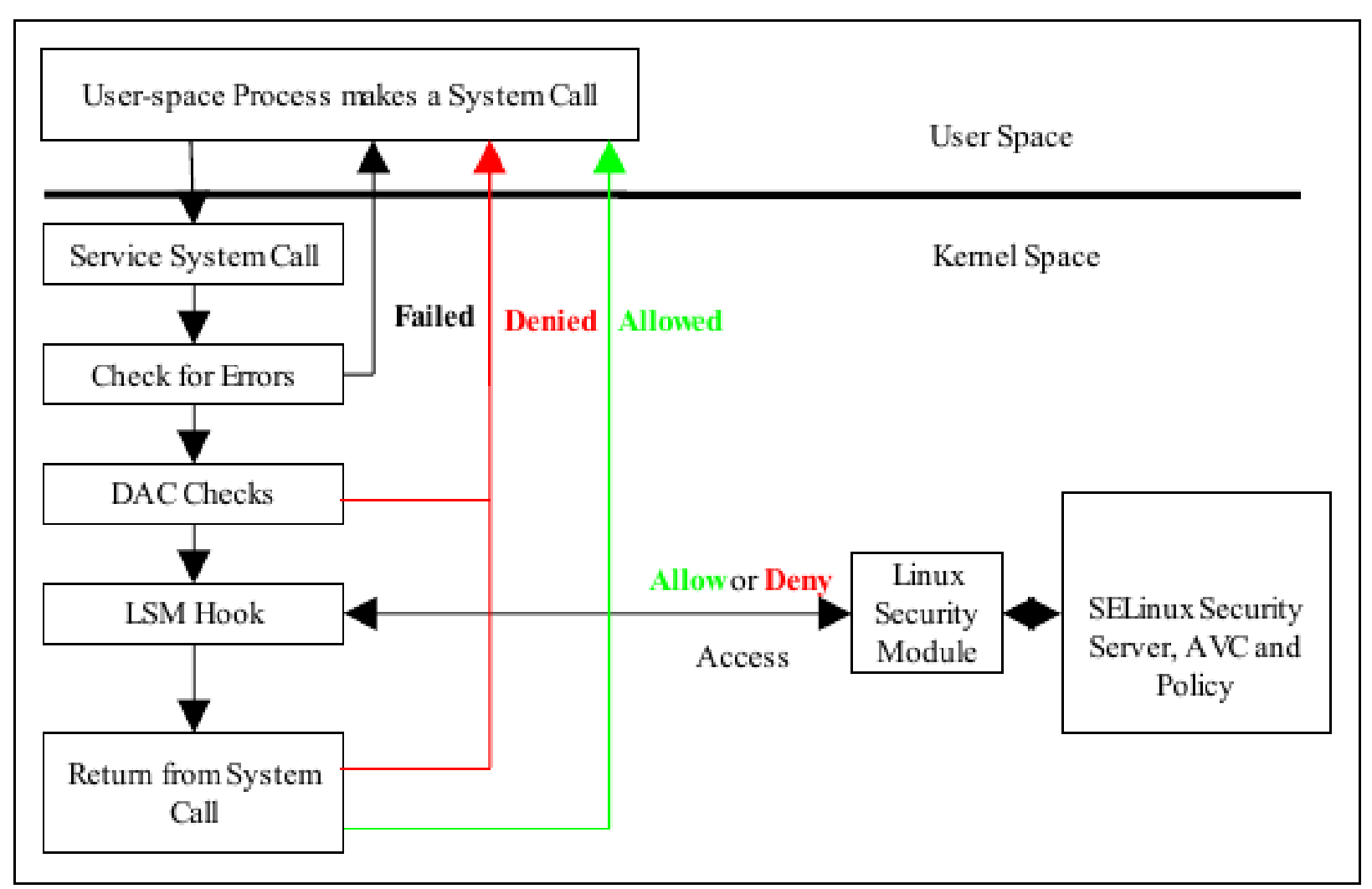
- Plusieurs politiques SELinux sont proposées par les diverses distributions Linux.

  Sur Red Hat, *targeted* est utilisée par défaut : seuls les services sensibles sont visés, les autres actions sont acceptées par défaut.

Différents composants :



- SELinux ne remplace le contrôle d'accès classique.
- Déroulement d'un appel système :



Pratique

- Dans la pratique, l'état SELinux est visible / modifiable via les commandes `sestatus` / `getenforce` / `setenforce`.
- Il existe trois modes de fonctionnement :
  - *disabled* : complètement désactivé,
  - *permissive* : actif, mais ne bloque pas les accès,
  - *enforcing* : actif, bloque les accès.
- Un serveur exposé à Internet **doit fonctionner en mode actif**.
- La configuration est regroupée dans le répertoire `/etc/selinux/`, par exemple `config` permet de définir le mode de fonctionnement de manière permanente.
- `/sys/fs/selinux` est l'interface avec le noyau.

- Différentes commandes classiques (`ls`, `ps`, `id`, ...) se voient dotées d'une nouvelle option **z**, qui affiche les étiquettes SELinux.

```
[jdg@centos7 ~]$ ls -Z
drwxr-xr-x. jdg jdg unconfined_u:object_r:user_home_t:s0
rpmbuild
-rw-r-----. jdg jdg unconfined_u:object_r:user_home_t:s0 test


[jdg@centos7 ~]$ ps axZ | grep http
system_u:system_r:httpd_t:s0  7229 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0  7231 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0  7232 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0  7233 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0  7234 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0  7235 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 \
                              7237 grep --color=auto http
```

- Les refus d’accès sont enregistrés dans le journal d'audit (`/var/log/audit/audit.log`) avec le type `AVC` ou `USER_AVC`.

  Par exemple :

```
[jdg@tiare ~]$ sudo grep -i AVC /var/log/audit/audit.log |
grep denied

type=AVC msg=audit(1413388901.065:18632):

   avc:  denied  { create } for  pid=4290

   comm="kdm" name=".xsession-errors-192.168.10.103:0"

   scontext=system_u:system_r:xdm_t:s0-s0:c0.c1023

   tcontext=system_u:object_r:user_home_t:s0

   tclass=file

   permissive=0
```

- L'administrateur du système aura sans doute à **adapter** SELinux selon ses besoins.
- Le cas le plus simple concerne un ensemble de valeurs booléennes qui autorisent / interdisent les accès :

  `getsebool -a` affiche toutes les valeurs gérées

  `setsebool` permet de modifier une valeur

Exemples :

```
[jdg@centos7 ~]$ getsebool -a | grep httpd_enable_homedirs
httpd_enable_homedirs --> off
[jdg@centos7 ~]$ sudo setsebool httpd_enable_homedirs on
[jdg@centos7 ~]$ getsebool -a | grep httpd_enable_homedirs
httpd_enable_homedirs --> on
```

- Pour des cas plus compliqués, il faut créer des règles SELinux personnalisées.
- les utilitaires `audit2allow`, `audit2why` (RPM `policycoreutils-python`) permettent de créer de nouvelles règles simplement, par exemple :

```
[sysnux@webdev ~]$ sudo grep denied /var/log/audit/audit.log
 . . .
type=AVC msg=audit(1339794159.666:584): avc:  denied  { rmdir }
for  pid=3842 comm="sshd" name="xxx" dev=dm-0 ino=914430
scontext=system_u:system_r:chroot_user_t:s0-s0:c0.c1023
tcontext=system_u:object_r:httpd_sys_content_t:s0 tclass=dir

[sysnux@webdev ~]$ sudo grep '1339794159.666:584'
/var/log/audit/audit.log | grep 'avc:  denied' | audit2allow -M
sftp14

******************** IMPORTANT ***********************

To make this policy package active, execute:

semodule -i sftp14.pp
```

Les règles deviennent **automatiquement permanentes**.

- Parfois l'étiquetage SELinux n'est pas correct ; par exemple lorsque des fichiers sont déplacés, comme une archive copiée d'un serveur vers un autre, ou lorsque SELinux a été désactivé et que des changements ont été effectués sur le système de fichiers.

  La commande `restorecon -R` permet de restaurer les contextes par défaut dans l'arborescence actuelle.

  Si on souhaite rétablir les contextes par défaut pour l'ensemble du système de fichiers, il est conseillé de :

  - Créer un fichier (vide) `.autorelabel` à la racine du système de fichier.
  - Redémarrer le système.
- On peut aussi besoin de changer le contexte d'un objet : commande `chcon`.

- La commande `semanage` permet de lister / modifier certains éléments de la configuration de SELinux.

  Par exemple, liste des utilisateurs / rôles, liste des ports :

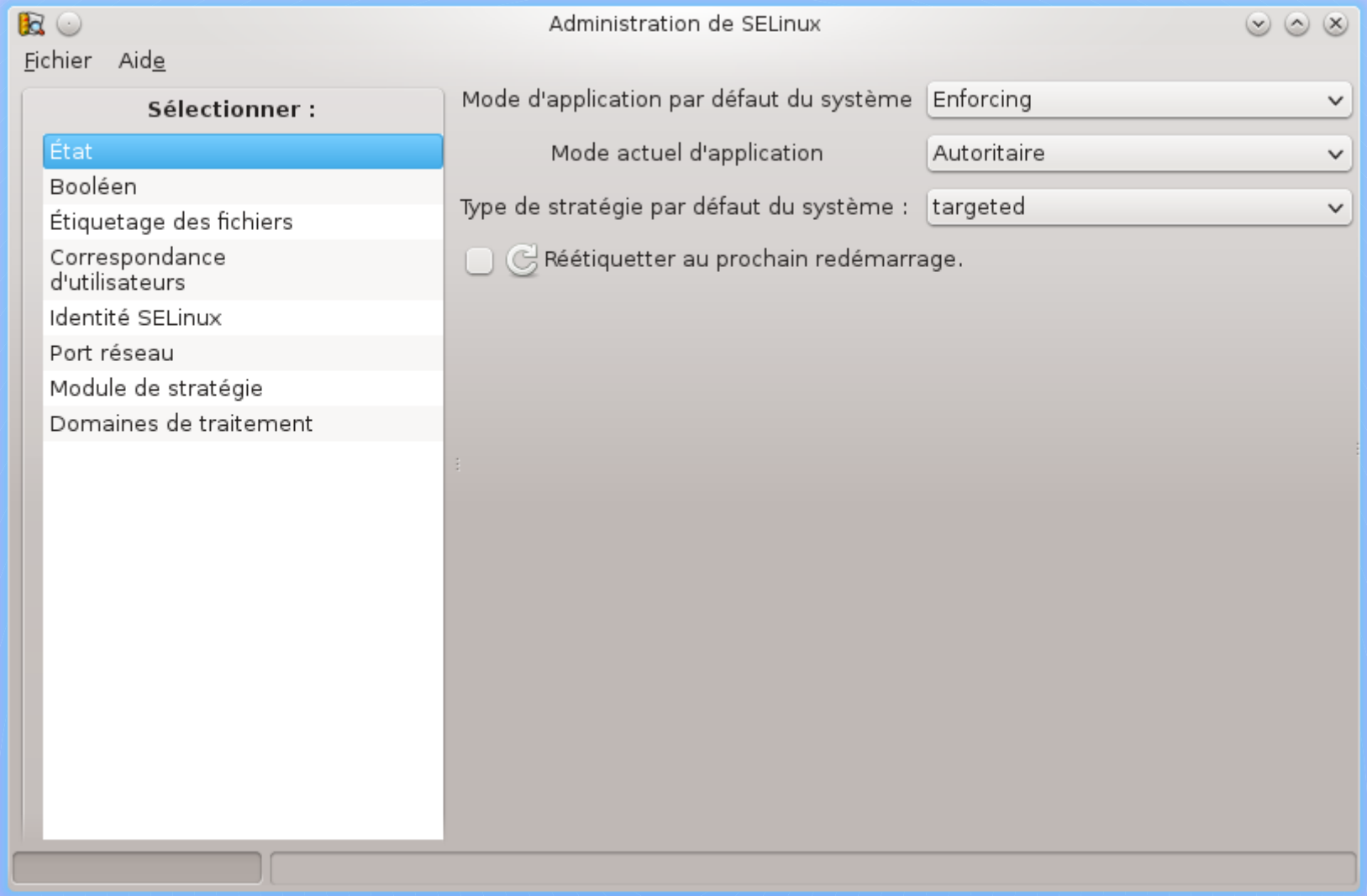
```
[jdg@centos7 ~]$ sudo semanage user -l

Identité SELinux        Rôles SELinux

guest_u                 guest_r
root                    staff_r sysadm_r system_r unconfined_r
staff_u                 staff_r sysadm_r system_r unconfined_r
sysadm_u                sysadm_r
system_u                system_r unconfined_r
unconfined_u            system_r unconfined_r
user_u                  user_r
xguest_u                xguest_r
```

Liste des ports avec `http` dans le type :

```
[jdg@centos7 ~]$ sudo semanage port -l | grep http
http_cache_port_t              tcp    8080, 8118, 8123, 10001-10010
http_cache_port_t              udp    3130
http_port_t                    tcp    80, 81, 443, 488, 8008, 8009,
                                      8443, 9000
pegasus_http_port_t            tcp    5988
pegasus_https_port_t           tcp    5989
```

Utilisée avec les options `--add` et `--modify` , `semanage` permet d'ajouter / modifier ces divers éléments de la politique SELinux.

Pour les machines disposant d'un environnement graphique, le paquet `policycoreutils-gui` fournit une vue graphique :



Conclusion

- SELinux fournit un contrôle d'accès obligatoire combinant *Role Based Access Control*, *Type Enforcement* et, en option *Multi-Level Security* et *Multi-Category Security*.
- SELinux **confine** les utilisateurs ou process aux domaines autorisés par leurs rôles ; il peut ainsi bloquer certaines menaces.
- SELinux **ne remplace pas les mesures de sécurité classiques** (mises à jour, mots de passe sérieux, firewall, ...).
- Références :
  - The SELinux Notebook – The Foundations
  - Red Hat EL 7 – System Administrators Guide + Security Guide
  - Cahier de l'administrateur Debian - Introduction à SELinux
  - Site du projet http://www.selinuxproject.org
  - Dan Walsh's Blog http://danwalsh.livejournal.com