**SE Linux**

|  |  |
| --- | --- |
| **DESC** | |
| Security Enhanced Linux : Mécanisme de contrôle d’accès avancé  Concurrencé par GRSecurity | |
| **FILES** | |
| /etc/selinux/config |  |
| **QUICK START** | |
|  | |

**Généralités :**

* Il est aux fichiers et processus ce que le firewall est au réseau.
* On définit ce qu’un utilisateur ou un processus peut faire : Par exemple un processus ne sera autorisé à interagir qu’avec certains fichiers et processus

**Modes de SE Linux :**

* Enforcing : SE Linux assure la sécurité et logs les accès refusés
* Permissive : SE Linux n’assure pas la sécurité, aucun accès n’est restreint mais on log quand même les accès refusés (permet de tester SE Linux)
* Disabled

**Politique de sécurité de SE Linux :**

* Targeted : Permissions custom précises
* Minimum :
* Mls : multi level security protection. Mode de protection avancé, besoin de package additionnels.

**Changement de mode : activé SE Linux à partir d’un état désactivé :**

* Mettre Permissive dans la conf
* Reboot
* Mettre enforcing dans la conf
* Reboot

Ou

* Set enforce 0|1|2|enforcing|permissive|disabled et pas besoin de reboot