**Set enforcing and permissive modes for SELinux.**

.

**Presentation**

**SELinux** stands for **S**ecurity-**E**nhanced **Linux**. It is a way to improve the server security.

The **/etc/selinux/config** file stores the current configuration:

# more /etc/selinux/config

*# This file controls the state of SELinux on the system.*

*# SELINUX= can take one of these three values:*

*#     enforcing - SELinux security policy is enforced.*

*#     permissive - SELinux prints warnings instead of enforcing.*

*#     disabled - No SELinux policy is loaded.*

*SELINUX=enforcing*

*# SELINUXTYPE= can take one of three two values:*

*#     targeted - Targeted processes are protected,*

*#     minimum - Modification of targeted policy. Only selected processes are protected.*

*#     mls - Multi Level Security protection.*

*SELINUXTYPE=targeted*

**SELinux** can run in three different modes (**enforcing**, **permissive** and **disabled**) well described in the above file.  
Besides the mode, there is a **SELinux** type (**targeted**, **minimum** and **mls**). Except if you work in a military agency, you will never need to change the **targeted** type.

**Configuration**

To get the current **SELinux** status:

# sestatus

To set **enforcing** mode, type:

# setenforce enforcing

To make this change permanent, edit the **/etc/sysconfig/selinux** file (or the **/etc/selinux/config** file) and replace the following value:

SELINUX=**enforcing**

**Alternatively**, to set **permissive** mode, type:

# setenforce permissive

To make this change permanent, edit the **/etc/sysconfig/selinux** file (or the **/etc/selinux/config** file) and replace the following value:

SELINUX=**permissive**

To make the reboot mandatory to change the configuration (**-P** can be added but **with caution**), type:

# setsebool **secure\_mode\_policyload** on