**SELinux- Security Enhanced Linux**

* It is an advanced access control mechanism that implements MAC (Mandatory Access Control).
* In traditional access control scheme, DAC (Discretionary [you get what you choose] Access Control) was used.

**Need of SELinux:**

* In DAC, user can set the permissions (rwx) of the files without any restrictions. So according to permissions set, user owner, group owner and others can access the files/directory. Even user owner change the user of file as well. DAC leaves too much access control in the hands of end users. In such cases, system administrator can’t restrict certain users from accessing some certain processes.
* With MAC, system administrator restricts users to access certain processes only. For an example, System admin allows users to run some scripts, to view some log files but restricts to use sudo or su commands, to restrict scripts to be run from their home directory.
* With MAC, even a user opens files/directories to world access, it doesn’t mean everyone can access files/directory. MAC constrains access what users can do. For an example, users can see files/directories and those are visible for everyone. But system admin constrains users to read those files/directories.

**SELinux Modes:**

1. Enforcing : SELinux is operating
2. Permissive : SELinux is active but only displaying warnings
3. Disabled : SELinux is turned off entirely
4. Enforcing:

* SELinux enforce (make something happen forcefully) its policy (set of rules) on the system.
* Any unauthorized access attempt by users/processes are denied.
* Access denials are also written to relevant log files.

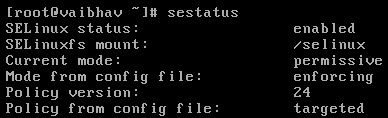
1. Permissive:

* SELinux doesn’t apply its policy.
* No access is denied.
* Policy violation is still written to relevant log files.

1. Disabled:

* SELinux is entirely turned off. No policy is applied and no enhanced security is running.
* To see mode of SELinux.

Command: sestatus OR getenforce





* To change SELinux mode either enforcing or permissive temporary,

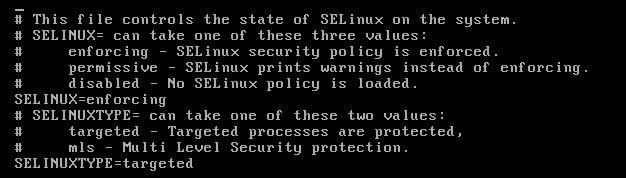
Command: setenforce 1: for setting enforcing mode

Command: setenforce 0: for setting permissive mode

Note: We can’t use setenforce command when SELinux in disabled mode.

* To change SELinux modes(any) permanently,

Command: vi /etc/selinux/config OR vi /etc/sysconfig/selinux



* Change the value of SELINUX.
* To reflect changes made, restart of system is must. Without restarting the system, SELinux will not change permanently.
* To restart the system,

Command: reboot

* Setting the status to permissive first is necessary because every file in the system needs to have its context labelled before SELinux can be enforced