

## MANAGING SELINUX (BASICS OF SELINUX)


### Basic SELinux Security Concepts:

- ➔ SELinux is a security enhancement to Linux that allows users and administrators more control over which users and applications can access which resources, such as files. Standard Linux access controls, such as file modes (-rwxr-xr-x) are modifiable by the user and applications that the user runs, whereas SELinux access controls are determined by a policy loaded on the system and not changeable by careless users or misbehaving applications.

### Important SELinux configuration Files:

- ➔ `/etc/selinux/config` is the main configuration file of SELinux.
- ➔ `/etc/sysconfig/selinux` contains a symbolic link to the actual configuration file, `/etc/selinux/config`.

**Note:** If you want to turn on or off the SELinux security you need to make changes in the main configuration file i.e. `/etc/selinux/config` file.

 root@master-server:~

```
[root@master-server ~]# cat /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 these two values:
#     targeted - Targeted processes are protected,
#     mls - Multi Level Security protection.
SELINUXTYPE=targeted

[root@master-server ~]#
```

### Modes of SELinux:

- Enforcing, Permissive and Disabled

#### Enforcing:

Enable and enforce the SELinux security policy on the system, denying access and logging actions

- **Permissive**

Permissive mode is similar to Debugging Mode. In Permissive Mode, SELinux policies and rules are applied to subjects and objects, but actions ( for example, Access Control denials) are not affected. The biggest advantage of Permissive Mode is that log files and error messages are generated based on the SELinux policy implemented.

- **Disabled:**

SELinux is turned off and no warn and log messages will be generated and stored.

To check the SELinux Mode:

#getenforce

```
root@master-server:~  
[root@master-server ~]# getenforce  
Enforcing  
[root@master-server ~]#
```

#sestatus

```
root@master-server:~  
[root@master-server ~]# sestatus  
SELinux status:                enabled  
SELinuxfs mount:              /selinux  
Current mode:                  enforcing  
Mode from config file:         enforcing  
Policy version:                24  
Policy from config file:       targeted  
[root@master-server ~]#
```

Display the SELinux context of a file or directory.:

# ls -Z selinux

```
[root@master-server ~]# touch selinux  
[root@master-server ~]# ls -Z selinux  
-rw-r--r--. root root unconfined_u:object_r:admin_home_t:s0 selinux  
[root@master-server ~]#
```

To display the context of a directory the syntax is

# ls -ldZ selinuxx

root@master-server:~

```
[root@master-server ~]# ls -ldZ selinuxx
drwxr-xr-x. root root unconfined_u:object_r:admin_home_t:s0 selinuxx
[root@master-server ~]#
```

### Changing the Modes of SELinux:

- ➔ To change the mode of SELinux the syntax is
- ➔ #setenforce <options>
- ➔ Options used are 0 or 1 (Where 0 means Permissive and 1 means Enforcing)
- ➔ To change the SELinux Mode to permissive
- ➔ #setenforce 0
- ➔ • Verify it by getenforce or sestatus command.

#getenforce

root@master-server:~

```
[root@master-server ~]# getenforce
Enforcing
[root@master-server ~]#
```

# setenforce 0

# getenforce

# sestatus

root@master-server:~

```
[root@master-server ~]# getenforce
Enforcing
[root@master-server ~]# setenforce 0
[root@master-server ~]# getenforce
Permissive
[root@master-server ~]# sestatus
SELinux status:                enabled
SELinuxfs mount:                /selinux
Current mode:                    permissive
Mode from config file:          enforcing
Policy version:                  24
Policy from config file:         targeted
[root@master-server ~]# ^C
[root@master-server ~]#
```

Note: To change the SELinux Mode back to Enforcing mode

#setenforce 1

Verify the change

```
root@master-server:~  
[root@master-server ~]# getenforce  
Permissive  
[root@master-server ~]# setenforce 1  
[root@master-server ~]# getenforce  
Enforcing  
[root@master-server ~]# sestatus  
SELinux status:                enabled  
SELinuxfs mount:              /selinux  
Current mode:                  enforcing  
Mode from config file:         enforcing  
Policy version:                24  
Policy from config file:       targeted  
[root@master-server ~]#
```

Disabling and Enabling the SELinux Security:


- ➔ To disable the SELinux protection or to change it to disabled Mode
- ➔ Edit the /etc/selinux/config file and change SELINUX=disabled
- ➔ Whenever changing the mode of SELinux from Enforcing/Permissive to Disabled or Disabled to Permissive/Enforcing, you need to restart the system so that the changes can take effect.
- ➔ First check the current status of SELinux and the configuration file.
- ➔ #getenforce ; #cat /etc/selinux/config

```
[root@master-server ~]# getenforce
Enforcing
[root@master-server ~]# cat /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 these two values:
#     targeted - Targeted processes are protected,
#     mls - Multi Level Security protection.
SELINUXTYPE=targeted

[root@master-server ~]#
```

- ➔ Now, edit the configuration file, restart the computer and check the status
- ➔ #vim /etc/selinux/config
- ➔ #init 6 (to reboot the system)

 root@master-server:~

```
# 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=disabled
# SELINUXTYPE= can take one of these two values:
#     targeted - Targeted processes are protected,
#     mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

#### Note:

To Enable it back the procedure is exactly same as above, instead of SELINUX=disabled change it to SELINUX=enforcing or permissive. Don't forget to restart the system, unless the system is rebooted the changes will not take effect.