4 Effective Methods to Disable SELinux Temporarily or Permanently

On some of the Linux distribution SELinux is enabled by default, which may cause some unwanted issues, if you don’t understand how SELinux works and the fundamental details on how to configure it. I strongly recommend that you understand SELinux and implement it on your environment. But, until you understand the implementation details of SELinux you may want to disable it to avoid some unnecessary issues.

To **disable SELinux** you can use any one of the 4 different methods mentioned in this article.

The SELinux will enforce security policies including the mandatory access controls defined by the US Department of Defence using the Linux Security Module (LSM) defined in the Linux Kernel. Every files and process in the system will be tagged with specific labels that will be used by the SELinux. You can use ls -Z and view those labels as shown below.

```
# ls -Z /etc/ -rw-r--r--  root root  system_u:object_r:etc_t:s0
a2ps.cfg  -rw-r--r--  root root  system_u:object_r:adjtime_t:s0   adjt
ime  -rw-r--r--  root root  system_u:object_r:etc_aliases_t:s0 aliases
  drwxr-x---  root root  system_u:object_r:auditd_etc_t:s0 audit  drwx
r-xr-x  root root  system_u:object_r:etc_runtime_t:s0 blkid  drwxr-xr-
x  root root  system_u:object_r:bluetooth_conf_t:s0 bluetooth  drwx---
---  root root  system_u:object_r:system_cron_spool_t:s0 cron.d  -rw-
rw-r--  root disk  system_u:object_r:amanda_dumpdates_t:s0 dumpdates
```

Method 1: Disable SELinux Temporarily

To disable SELinux temporarily you have to modify the /selinux/enforce file as shown below. Please note that this setting will be gone after the reboot of the system.

```
# cat /selinux/enforce  1    #
echo 0 > /selinux/enforce    # cat /selinux/enforce  0
```

You can also use setenforce command as shown below to disable SELinux. Possible parameters to setenforce commands are: Enforcing , Permissive, 1 (enable) or 0 (disable).

```
# setenforce 0
```

Method 2: Disable SELinux Permanently

To disable the SELinux permanently, modify the /etc/selinux/config and set the SELINUX=disabled as shown below. One you make any changes to the /etc/selinux/config, reboot the server for the changes to be considered.

```
# cat /etc/selinux/config
  SELINUX=disabled  SELINUXTYPE=targeted  SETLOCALDEFS=0
```

Following are the possible values for the **SELINUX** variable in the **/etc/selinux/config** file

- **enforcing** – The Security Policy is always Encoforced
- **permissive -** This just simulates the enforcing policy by only printing warning messages and not really enforcing the SELinux. This is good to first see how SELinux works and later figure out what policies should be enforced.
- **disabled -** Completely disable SELinux

Following are the possible values for **SELINUXTYPE** variable in the **/etc/selinux/config** file.

This indicates the type of policies that can be used for the SELinux.

- **targeted** - This policy will protected only specific targeted network daemons.
- **strict -** This is for maximum SELinux protection.

Method 3: Disable SELinux from the Grub Boot Loader

If you can’t locate /etc/selinux/config file on your system, you can pass disable SELinux by passing it as parameter to the Grub Boot Loader as shown below.

```
# cat /boot/grub/grub.conf
  default=0  timeout=5  splashimage=(hd0,0)/boot/grub/splash.xpm.gz  h
iddenmenu  title Enterprise Linux Enterprise Linux Server (2.6.18-92.e
l5PAE)  root (hd0,0)  kernel /boot/vmlinuz-2.6.18-92.el5PAE ro root=LA
BEL=/ rhgb quiet selinux=0
  initrd /boot/initrd-2.6.18-92.el5PAE.img  title Enterprise Linux Ent
erprise Linux Server (2.6.18-92.el5)  root (hd0,0)  kernel /boot/vmlin
uz-2.6.18-92.el5 ro root=L
ABEL=/ rhgb quiet selinux=0  initrd /boot/initrd-2.6.18-92.el5.img
```

Method 4: Disable Only a Specific Service in SELinux – HTTP/Apache

If you are not interested in disability the whole SELinux, you can also disable SELinux only for a specific service. For example, do disable SELinux for HTTP/Apache service, modify the **httpd_disable_trans** variable in the **/etc/selinux/targeted/booleans** file.

Set the httpd_disable_trans variable to 1 as shown below.

```
# grep httpd /etc/selinux/targeted/booleans  httpd_builtin_scripting=1
```

```
  httpd_disable_trans=1
httpd_enable_cgi=1  httpd_enable_homedirs=1  httpd_ssi_exec=1  httpd_t
ty_comm=0  httpd_unified=1
```

Set SELinux boolean value using setsebool command as shown below. Make sure to restart the HTTP service after this change.

```
# setsebool httpd_disable_trans 1 # service httpd restart
```