Managing SELINUX

Advance permission check

```
[root@localhost ~]# ls -lZ
total 9
drwxr-xrwx. 3 root root system_u:object_r:unlabeled_t:s0      1024 Feb  9 03:58 acl
-rw-------. 1 root root system_u:object_r:admin_home_t:s0     1387 Jan 20 06:45 anaconda-ks.cfg
-rw-r--r--. 1 root root system_u:object_r:admin_home_t:s0     1542 Jan 20 06:48 initial-setup-ks.cfg
drwxr-xr-x. 2 root root unconfined_u:object_r:admin_home_t:s0   21 Feb  9 03:56 sudocopy
drwxrwxr-x+ 2 root root unconfined_u:object_r:admin_home_t:s0    6 Feb  8 21:40 vivek
[root@localhost ~]#
```

Important SELinux configuration Files

1. **/etc/selinux/config** is the main configuration file of **SELinux.**

```
[root@localhost ~]# vi /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 three values:
#     targeted - Targeted processes are protected,
#     minimum - Modification of targeted policy. Only selected processes are protected.
#     mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

2. **/etc/sysconfig/selinux** contains a symbolic link to the actual configuration file

```
[root@localhost ~]# vi /etc/sysconfig/selinux

# 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 three values:
#     targeted - Targeted processes are protected,
#     minimum - Modification of targeted policy. Only selected processes are protected.
#     mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

check the SELinux Mode

```
[root@localhost ~]# getenforce
Enforcing
[root@localhost ~]#
[root@localhost ~]# sestatus
SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:             targeted
Current mode:                   enforcing
Mode from config file:          enforcing
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Memory protection checking:     actual (secure)
Max kernel policy version:      31
```

Managing SELINUX

Changing the Modes of SELinux

```
[root@localhost ~]# setenforce 0
[root@localhost ~]# getenforce
Permissive
[root@localhost ~]# setenforce 1
[root@localhost ~]# getenforce
Enforcing
[root@localhost ~]#
```

Permanent change modes of SELINUX

```
[root@localhost ~]# vi /etc/sysconfig/selinux
```

```
# 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 three values:
#     targeted - Targeted processes are protected,
#     minimum - Modification of targeted policy. Only selected processes are protected.
#     mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

CHANGE SELINUX MODE

```
# 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 three values:
#     targeted - Targeted processes are protected,
#     minimum - Modification of targeted policy. Only selected processes are protected.
#     mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

COMPLUSARY REBOOT THE SYSTEM AFTER CHANGE MODE

```
[root@localhost ~]# reboot
```

```
[root@localhost ~]# sestatus
SELinux status:                disabled
[root@localhost ~]#
```

CHANGE MODE

```
# 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 three values:
#     targeted - Targeted processes are protected,
#     minimum - Modification of targeted policy. Only selected processes are protected.
#     mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

Managing SELINUX

change the context of a file or directory the syntax

```
[root@localhost ~]# chcon -t var_t acl
[root@localhost ~]# ls -ldZ acl
drwxr-xrwx. 3 root root system_u:object_r:var_t:s0 1024 Feb  9 03:58 acl
[root@localhost ~]#
```

Restoring back the modified SELinux context to its default value

```
[root@localhost ~]# ls -ldZ acl
drwxr-xrwx. 3 root root system_u:object_r:admin_home_t:s0 1024 Feb  9 03:58 acl
[root@localhost ~]#
[root@localhost ~]# chcon -t var_t acl
[root@localhost ~]# ls -ldZ acl
drwxr-xrwx. 3 root root system_u:object_r:var_t:s0 1024 Feb  9 03:58 acl
[root@localhost ~]#
[root@localhost ~]# restorecon acl
[root@localhost ~]#
[root@localhost ~]# ls -ldZ acl
drwxr-xrwx. 3 root root system_u:object_r:admin_home_t:s0 1024 Feb  9 03:58 acl
[root@localhost ~]#
```

How to Set Boolean

```
[root@localhost ~]# getsebool -a |grep ftp
ftpd_anon_write --> off
ftpd_connect_all_unreserved --> off
ftpd_connect_db --> off
ftpd_full_access --> off
ftpd_use_cifs --> off
ftpd_use_fusefs --> off
ftpd_use_nfs --> off
ftpd_use_passive_mode --> off
httpd_can_connect_ftp --> off
httpd_enable_ftp_server --> off
tftp_anon_write --> off
tftp_home_dir --> off
[root@localhost ~]# setsebool -P ftpd_connect_db on
[root@localhost ~]# getsebool -a |grep ftp
ftpd_anon_write --> off
ftpd_connect_all_unreserved --> off
ftpd_connect_db --> on
ftpd_full_access --> off
ftpd_use_cifs --> off
ftpd_use_fusefs --> off
ftpd_use_nfs --> off
ftpd_use_passive_mode --> off
httpd_can_connect_ftp --> off
httpd_enable_ftp_server --> off
tftp_anon_write --> off
tftp_home_dir --> off
[root@localhost ~]#
```