1.SELinux mode

2 type of modes

a. getenforce ----- o/p will be enforcing -------- to see you are in which mode

b. setenforce <mode>------ to set the mode

check the file /etc/sysconfig/SELinux

c. modes
-enforcing
-permissive ----/var/log/audit.audit.log
-disable ------ not good

d. policy – 1. Targated ------ targated processes are protected

2. Minimal ------ only specified processes are protected

3. Mls ------- multilevel security (not needed for basic security)

---------- Context

ls -Z

1.user

2. role

3. type

Every directory has specific context type to see that use

ls -z

Every process also has specific context

ps -zaux

If processes shows unconfined means SELinux doesnot care about them

Specially the processes that are providing services on your machine

e.g SSH process

ssshd_t ---they have type and called as source

usually

which source type has access to which target type

e.g yum install -y httpd

/var/www is root of web server

cd /var/www

ls -z -------check context labels

$semanage fcontext -l ----- to see all levels used by the server

Yum whatprovides */sepolicy

Yum install <package name> ------- to generate manual pages

To see help

sepolicy –help

To apply context level

semanage