1- check the current SELINUX MODE

```
[root@www ~]# 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:          error (Success)
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Memory protection checking:     actual (secure)
Max kernel policy version:      33
```

Its status is enabled and the current mode is enforcing

2- change the selinux mode temporarily

You can do so by setenforcing whichever mode you want

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

3- To permanently edit you can do so in /etc/selinux/config

```
[root@www ~]# man selinux
[root@www ~]# vim /etc/se
security/       selinux/        services        sesta
[root@www ~]# vim /etc/se
security/       selinux/        services        sesta
[root@www ~]# vim /etc/selinux/config
```

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


~
```

Enabling the selinux type to permissive

4- to view the SELINUX context of files

System_u is the user

Object_r is the role which is given to files by default but roles are different for system processes are given by system_r and for kernel level processes is given by kernel_r

Type is given by admin_home_t because its a given type defined by SELINUX of admin_home

And the security level enables access on reads and writes between processes and given files for the given user for example a user having s0-s100 can for example write to all the 99 security files

```
total 192
-rw-------. 1 root root system_u:object_r:admin_home_t:s0   919 Dec 20 13:37 anaconda-ks.cfg
-rw-r--r--. 1 root root system_u:object_r:admin_home_t:s0 22592 Jan 18 13:35 get-docker.sh
-rw-r--r--. 1 root root system_u:object_r:admin_home_t:s0 70152 May 10  2022 libcgroup-0.41-19.el8.x86_64.rpm
-rw-r--r--. 1 root root system_u:object_r:admin_home_t:s0 93664 May 10  2022 libcgroup-tools-0.41-19.el8.x86_64.r
drwxr-xr-x. 2 root root system_u:object_r:admin_home_t:s0     6 Jan 18 14:50 static
```

5- List current booleans

```
[root@www ~]# getsebool -a
abrt_anon_write --> off
abrt_handle_event --> off
abrt_upload_watch_anon_write --> on
antivirus_can_scan_system --> off
antivirus_use_jit --> off
auditadm_exec_content --> on
authlogin_nsswitch_use_ldap --> off
authlogin_radius --> off
authlogin_yubikey --> off
awstats_purge_apache_log_files --> off
boinc_execmem --> on
cdrecord_read_content --> off
cluster_can_network_connect --> off
cluster_manage_all_files --> off
cluster_use_execmem --> off
cobbler_anon_write --> off
cobbler_can_network_connect --> off
cobbler_use_cifs --> off
cobbler_use_nfs --> off
collectd_tcp_network_connect --> off
colord_use_nfs --> off
condor_tcp_network_connect --> off
conman_can_network --> off
conman_use_nfs --> off
container_connect_any --> off
container_manage_cgroup --> off
container_read_certs --> off
container_use_cephfs --> off
container_use_devices --> off
```

6- allow apache_httpd to send mails

```
[root@www ~]# getsebool -a | grep mail
gitosis_can_sendmail --> off
httpd_can_sendmail --> off
logging_syslogd_can_sendmail --> off
logwatch_can_network_connect_mail --> off
mailman_use_fusefs --> off
postfix_local_write_mail_spool --> on
[root@www ~]# setsebool -P httpd_can_sendmail on
[root@www ~]#
```

7- setting httpd can network connect to on

```
[root@www ~]# getsebool -a | grep httpd
httpd_anon_write --> off
httpd_builtin_scripting --> on
httpd_can_check_spam --> off
httpd_can_connect_ftp --> off
httpd_can_connect_ldap --> off
httpd_can_connect_mythtv --> off
httpd_can_connect_zabbix --> off
httpd_can_manage_courier_spool --> off
httpd_can_network_connect --> off
httpd_can_network_connect_cobbler --> off
httpd_can_network_connect_db --> off
httpd_can_network_memcache --> off
httpd_can_network_relay --> off
httpd_can_sendmail --> on
httpd_dbus_avahi --> off
httpd_dbus_sssd --> off
httpd_dontaudit_search_dirs --> off
httpd_enable_cgi --> on
httpd_enable_ftp_server --> off
httpd_enable_homedirs --> off
httpd_execmem --> off
httpd_graceful_shutdown --> off
httpd_manage_ipa --> off
httpd_mod_auth_ntlm_winbind --> off
httpd_mod_auth_pam --> off
httpd_read_user_content --> off
httpd_run_ipa --> off
httpd_run_preupgrade --> off
httpd_run_stickshift --> off
httpd_serve_cobbler_files --> off
httpd_setrlimit --> off
httpd_ssi_exec --> off
httpd_sys_script_anon_write --> off
httpd_tmp_exec --> off
httpd_tty_comm --> off
httpd_unified --> off
httpd_use_cifs --> off
httpd_use_fusefs --> off
httpd_use_gpg --> off
httpd_use_nfs --> off
httpd_use_opencryptoki --> off
httpd_use_openstack --> off
httpd_use_sasl --> off
httpd_verify_dns --> off
[root@www ~]# setsebool -P httpd_can_network_connect on
[root@www ~]#
```

8/9- modify selinux contexts of a file

```
[root@www /]# ll -dZ web
drwxr-xr-x. 2 root root unconfined_u:object_r:default_t:s0 6 Jan 29 16:20 web
[root@www /]# semanage fcontext -a -t  httpd_sys_content_t /web
[root@www /]# res
rescan-scsi-bus.sh  reset               resize2fs           resizecons          resizepart          restorecc
[root@www /]# res
rescan-scsi-bus.sh  reset               resize2fs           resizecons          resizepart          restorecc
[root@www /]# restorecon
afs/   bin/   boot/  dev/   etc/   home/  lib/   lib64/ media/ mnt/   opt/   proc/  root/  run/   sbin/  srv/
[root@www /]# restorecon
afs/   bin/   boot/  dev/   etc/   home/  lib/   lib64/ media/ mnt/   opt/   proc/  root/  run/   sbin/  srv/
[root@www /]# restorecon --help
restorecon: invalid option -- '-'
usage:  restorecon [-iIDFmnprRv0xT] [-e excludedir] pathname...
usage:  restorecon [-iIDFmnprRv0xT] [-e excludedir] -f filename
[root@www /]# man restorecon
[root@www /]# restorecon -vR /web
Relabeled /web from unconfined_u:object_r:default_t:s0 to unconfined_u:object_r:httpd_sys_content_t:s0
[root@www /]#
```

10- difference between cp and mv

Cp and mv without preserving context or -a would use the directory's security context using -a preserves the context and mv preserves the context as well but to be sure you could use -Z option with the commands

11- running apache on linux with selinux enforcing

```
[root@www /]# getenforce
Enforcing
[root@www /]#
```

```
[root@www /]# semanage port -l | grep http
http_cache_port_t              tcp      8080, 8118, 8123, 10001-10010
http_cache_port_t              udp      3130
http_port_t                    tcp      80, 81, 443, 488, 8008, 8009, 8443, 9000
pegasus_http_port_t            tcp      5988
pegasus_https_port_t           tcp      5989
[root@www /]# semanage port -l | grep ssh
```

```
[vomato@www /]$ wget http://localhost:80
--2025-01-29 16:49:13--  http://localhost/
Resolving localhost (localhost)... ::1, 127.0.0.1
Connecting to localhost (localhost)|::1|:80... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://www.za3bola.com [following]
--2025-01-29 16:49:13--  https://www.za3bola.com/
Resolving www.za3bola.com (www.za3bola.com)... 192.168.159.130
Connecting to www.za3bola.com (www.za3bola.com)|192.168.159.130|:443... connected.
ERROR: The certificate of ‘www.za3bola.com’ is not trusted.
ERROR: The certificate of ‘www.za3bola.com’ doesn't have a known issuer.
```

12- editing the default port for sshd and adding the port 2222 for selinux

```
[root@www log]# semanage port -l | grep ssh
ssh_port_t                     tcp      2222, 22
[root@www log]#
```

```
Include /etc/ssh/sshd_config.d/*.conf

# If you want to change the port on a SELinux system, you have to tell
# SELinux about this change.
# semanage port -a -t ssh_port_t -p tcp #PORTNUMBER
#
Port 2222
```

13- send a critical message and check /var/log/messages

```
load_policy     localeconv      localtime_r     lockfile        log10l          log2f
loadunimap      localectl       locate          loff_t          log1p           log2l
local           localedef       lock            log             log1pf          logb
[root@www ~]# man logger
[root@www ~]# logger -p news.crit "hello"
[root@www ~]# man logger
```

```
Jan 29 19:04:44 www root[4335]: hello
Jan 29 19:05:30 www root[4355]: hello
```

14-send with priority info

```
[root@www ~]# logger "info message" -p news.info
```

```
Jan 29 19:08:29 www root[4359]: info message
```

15-*.crit and mail.crit

The difference between *.crit and mail.crit means that the logging of all services will be done on a priority of critical and higher and mail.crit logs the mail facility with critical logs or higher priorities to the specified location

16- log customer messages and adding a rule and testing log

```
[root@www ~]# logger "customer log" -p local0.info
[root@www ~]#
```

```
# Log the customer messages
local0.*                                                /var/log/cursomters
# Log cron stuff
```

```
boot.log-20250129         cursomters
[root@www ~]# vim /var/log/
anaconda/                 btmp
audit/                    btmp-20250101
boot.log                  chrony/
boot.log-20250123         cron
boot.log-20250124         cron-20241229
boot.log-20250125         cron-20250118
boot.log-20250126         cron-20250119
boot.log-20250127         cron-20250126
boot.log-20250128         cups/
boot.log-20250129         cursomters
[root@www ~]# vim /var/log/c
chrony/        cron           cron-20241229  cron-202
[root@www ~]# vim /var/log/c
chrony/        cron           cron-20241229  cron-202
[root@www ~]# vim /var/log/cursomters
[root@www ~]#
```

```
tomato@Tomato: ~/CS/devops/ITIextra/docker/tocker
Jan 29 21:41:23 www root[4827]: customer log
Jan 29 21:42:01 www root[4866]: customer log
~
~
~
~
~
~
~
~
```

17- to add all kernel logs to the system you can do so by adding the kern.* /var/log/kern

```
kern.*                                                  /var/log/kern
```

18- add the mail.crit line with the specified file

```
mail.crit                                               /var/log/critical-mail
```

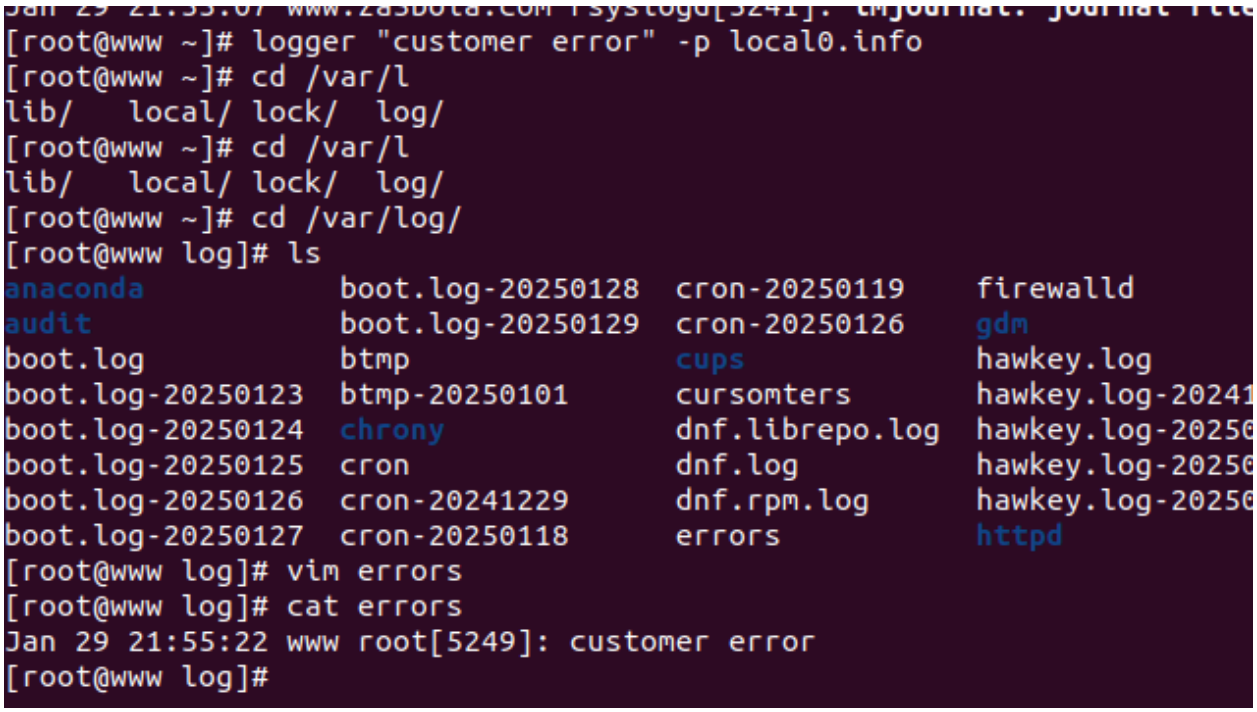
19- log cron to test cron for all cron except info or debug logs

```
cron.!=info;cron.!=debug                                /var/log/testcron
```

20-log messages containing the keyword error to /var/log/errors

```
:msg, contains,"error"                                  /var/log/errors
# Log anything (except mail) of level info or higher.
```

Testing the log using logger


[root@www ~]# logger "customer error" -p local0.info
[root@www ~]# cd /var/l
lib/ local/ lock/ log/
[root@www ~]# cd /var/l
lib/ local/ lock/ log/
[root@www ~]# cd /var/log/
[root@www log]# ls
anaconda boot.log-20250128 cron-20250119 firewalld
audit boot.log-20250129 cron-20250126 gdm
boot.log btmp cups hawkey.log
boot.log-20250123 btmp-20250101 cursomters hawkey.log-20241
boot.log-20250124 chrony dnf.librepo.log hawkey.log-20250
boot.log-20250125 cron dnf.log hawkey.log-20250
boot.log-20250126 cron-20241229 dnf.rpm.log hawkey.log-20250
boot.log-20250127 cron-20250118 errors httpd
[root@www log]# vim errors
[root@www log]# cat errors
Jan 29 21:55:22 www root[5249]: customer error
[root@www log]#