Chapter 11 - Analyzing And Storing Logs

/etc/rsyslog.conf -> file contains configurations for the system logs
/etc/logrotate.conf -> configuration for saving the log files

/var/log -> file that contains the services logs

/var/log/messages -> contains the syslog messages ex: messages or exceptions for auth. and jobs processing messages
/var/log/secure -> related to security and auth. events
/var/log/cron -> logs related to mail server
/var/log/boot.log -> related to system startup

systemd-journald
rsyslog > read the logs and write them in /var/log

Syslog Priority, 0 is the highest

0->emerg
1->alert
2->crit
3->err
4->warning
5->notice
6->info
7->debug

to manually write a log message:

logger -p local7.notice "this is manually log entry"
-p : the priority of the message

to view a log file

tail -f file

Command	Description
journalctl -n 5	print the last 5 logs
journalctl -f	
journalctl -p err	print the error logs

Command	Description
journalctl -p crit	print the critical logs
journalctl -b	print the boot logs
journalctl --since yesterday	

to make the logs permanent in the file:

create dir that have the same name of the temp dir
mkdir /var/log/journal

then:

chown -R root:system-journal /var/log/journal

then:

vi /etc/system/journald.conf
and change Storage = auto -> Storage = persistent

then:

systemctl restart systemd-journald

Timezone configuration:

timedatectl list-timezones
timedatectl set-timezone Africa/Cairo
timedatectl set-time 9:00:00