ANALYZE AND STORE LOGS	
SYSTEM LOGGING	Processes and the operating system kernel record a log of events that happen. These logs are used to audit the system and troubleshoot problems. The systemd-journald and rsyslog services handle the syslog messages in Red Hat Enterprise Linux 8 and 9
System Log files	**/var/log/messages** Most syslog messages are logged here. Exceptions include messages about authentication and email processing, scheduled job execution, and purely debugging-related messages. **/var/log/secure** Syslog messages about security and authentication events. **/var/log/maillog** Syslog messages about the mail server. **/var/log/cron** Syslog messages about scheduled job execution **/var/log/boot.log** Non-syslog console messages about system startup

Overview Syslog Priorities

CODE	PRIORITY	SEVERITY
0	emerg	System is unusable
1	alert	Action must be taken immediately
2	crit	Critical condition
3	err	Non-critical error condition
4	warning	Warning condition
5	notice	Normal but significant event
6	info	Informational event
7	debug	Debugging-level message

DESCRIPTION	COMMANDS / OPTIONS
Rotates log files to prevent them from taking too much space in the /var/log directory	**To install logroted** sudo apt-get install logrotate **main configuration file** : /etc/logrotate.conf logroted[options] [configuration file] -d debug -f force -m mail -s state --status <config file>
The last 10 lines of the file specified and continues to output new lines in the file as they get written	tail -f /path/to/file
Sends messages to the rsyslog service	**logger [options] msg** -p Specifies a priority -t Adds a tag to the message -i Logs the PID with each message -s Writes the message to stderr as well as the system log -f Logs the contents of a file -u Writes to a socket instead of the system log -n Sends messages to a remote syslog server -d UDP instead of a stream for remote logging -P Specifies a port for remote logging -w Waits for confirmation from the remote server

DESCRIPTION	COMMANDS / OPTIONS
To retrieve log messages from the journal	**journalctl [options] [unit]** **-n(n**) Limiting the number of log entries -p Filtering logs by priority level -o Customizing output format **--list-boots** Listing system boots **-f** outputs the last 10 lines of the system journal **-u** show messages for a specifed systemd unit **--since** To limit the output to a specific time range **Example:** journalctl --since "1 Hour ago" **-b** To limit the output to a specific system boot
System journal config file location	/etc/systemd/journald.conf
An overview of the current time-related system settings	**timedatectl[options]** list-timezones set-timezone xxxx set-time 0000 set-ntp false /ture
chronyd service keeps on track the usually inaccurate local RTC	chronyd — daemon that can be started at boot time chronyc — command-line interface for chrony **Install chronyd in RHEL Server** yum install chrony **Check status of service** systemctl status chronyd **To Check Chrony Synchronization** chronyc tracking **To check information about chrony's sources** chronyc sources