Chapter – 9 ANALYZING AND STORING LOGS

Objectives:

- Interpret events in relevant syslog files to troubleshoot problems or review system status.
- Find and interpret entries in the system journal to troubleshoot problems or review system status.
- Configure the system journal to preserve the record of events when a server is rebooted.
- Maintain accurate time synchronization using NTP and configure the time zone to ensure correct time stamps for events recorded by the system journal and logs.

REVIEWING SYSLOG FILES

ANALYZING AND MONITORING SYSLOG ENTRY

Log messages start with the oldest message on top and the newest message at the end of the log file. The rsyslog service uses a standard format while recording entries in log files.
Location of log files: /var/log

REVIEWING SYSTEM JOURNAL ENTRIES

FINDING EVENTS

The systemd-journald service stores logging data in a structured called the journal. This data includes extra information about the log event.

To retrieve log messages from the journal, use the **journalctl** command.

Adding Manual Log:
logger -p facility “message”
i.e. logger -p authpriv.alert "Logging test authpriv.alert"
Location to store .conf file: /etc/rsyslog.d/
Note: You can find facility of log in file /etc/rsyslog.conf
[Priority: emerg(System is unusable), alert(Action must be taken immediately), crit(Critical condition), err(Non-critical error condition), warning(Warning condition), notice(Normal but significant event), info(Informational event), debug(Debugging-level message)]s

MAINTAINING ACCURATE TIME

SETTING LOCAL CLOCKS AND TIME ZONES

- Correct synchronized system time is critical for log file analysis across multiple systems. The *Network Time Protocol* (*NTP*) is a standard way for machines to provide and obtain correct time information on the Internet.
- The timedatectl command shows an overview of the current time-related system settings, including current time, time zone, and NTP synchronization settings of the system.