Red Hat
Enterprise
Linux 9

RHCSA-SA1 LAB-Book

Chapter 11 - Analyzing and Storing 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.

Many systems record logs of events in text files which are kept in the /var/log directory.

These logs can be inspected using normal text utilities such as less and tail.

A standard logging system based on the Syslog protocol is built into Red Hat Enterprise Linux.

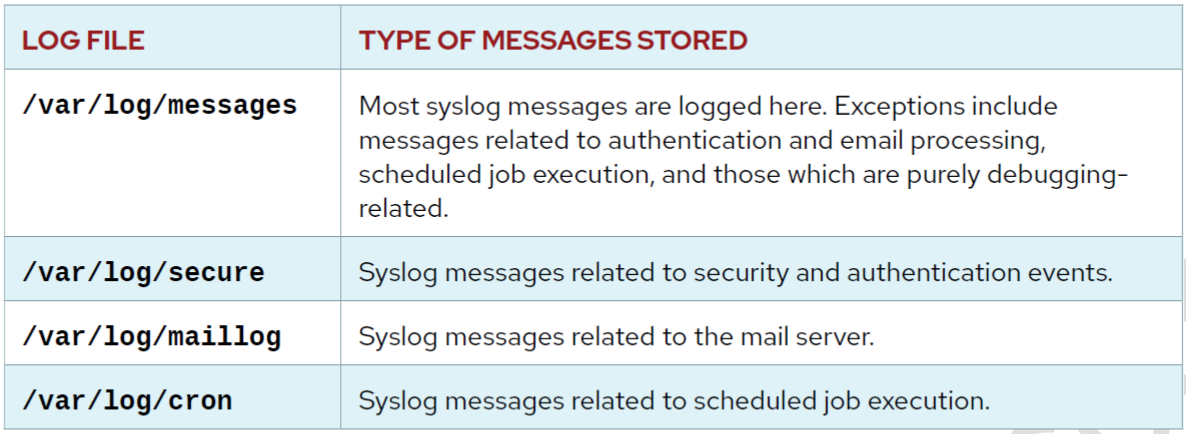
Many programs use this system to record events and organize them into log files.

The **systemd-journald** and **rsyslog** services handle the syslog messages in Red Hat Enterprise Linux 8. It collects event messages from many sources including the kernel, output from the early stages of the boot process, standard output and standard error from daemons as they start up and run, and syslog events.

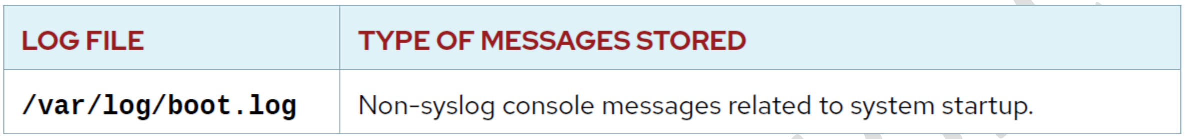
The rsyslog service sorts and writes syslog messages to the log files that do persist across reboots in /var/log.

The rsyslog service sorts the log messages to specific log files based on the type of program that sent each message, or facility, and the priority of each syslog message.

In addition to syslog message files, the /var/log directory contains log files from other services on the system.

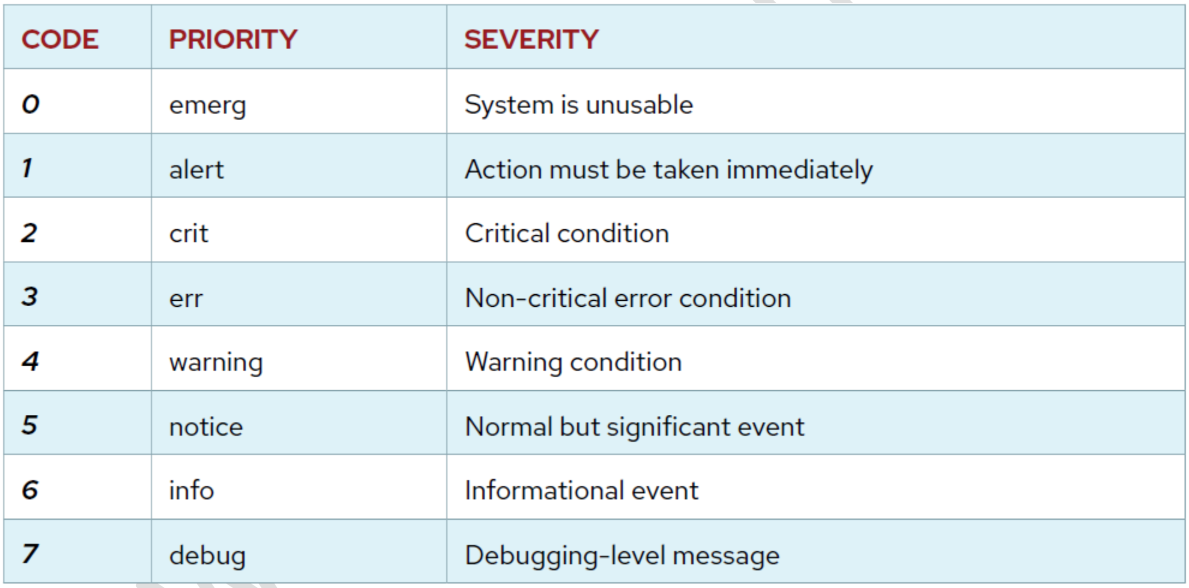


LOG FILE	TYPE OF MESSAGES STORED
/var/log/messages	Most syslog messages are logged here. Exceptions include messages related to authentication and email processing, scheduled job execution, and those which are purely debugging-related.
/var/log/secure	Syslog messages related to security and authentication events.
/var/log/maillog	Syslog messages related to the mail server.
/var/log/cron	Syslog messages related to scheduled job execution.



LOG FILE	TYPE OF MESSAGES STORED
/var/log/boot.log	Non-syslog console messages related to system startup.

Logging Events to the System:



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

Log File Rotation:

The logrotate tool rotates log files to keep them from taking up too much space in the file system containing the /var/log directory.

When a log file is rotated, it is renamed with an extension indicating the date it was rotated. For example, the old /var/log/messages file may become /var/log/messages-20190130 if it is rotated on 2019-01-30.

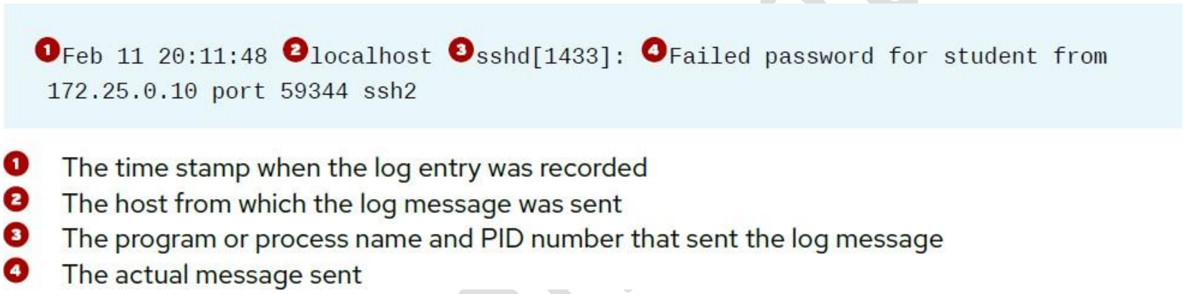
Once the old log file is rotated, a new log file is created and the service that writes to it is notified.

After a certain number of rotations, typically after four weeks, the oldest log file is discarded to free disk space.

A scheduled job runs the logrotate program daily to see if any logs need to be rotated.

Most log files are rotated weekly, but logrotate rotates some faster, or slower, or when they reach a certain size.

Example: the anatomy of a log message in the /var/log/secure log file



```
❶Feb 11 20:11:48 ❷localhost ❸sshd[1433]: ❹Failed password for student from
 172.25.0.10 port 59344 ssh2
```

❶ The time stamp when the log entry was recorded
❷ The host from which the log message was sent
❸ The program or process name and PID number that sent the log message
❹ The actual message sent

Practical based on above:

1) To monitor for failed login attempts, run the tail command in one terminal and then in another terminal, run the ssh command as the root user while a user tries to log in to the system.

➔tail -f /var/log/secure

Finding Events:

The systemd-journald service stores logging data in a structured, indexed binary file called the journal.

This data includes extra information about the log event.

Practical based on above:

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

➔Command: journalctl

2)To display specific log entries using journalctl.

➔Command journalctl -n 5

3)To display the last 10 lines of the system journal and continues to output new journal entries as they get written to the journal.

➔Command: journalctl -f

4) To display the entries as per priority level using either name or number (code) use the below command.

Priority Levels: debug, info, notice, warning, err, crit, alert, and emerg.

➔Command: journalctl -p err

5) List all journal entries from today's records.

➔Command: journalctl - - since today

6) List all journal entries ranging from 2019-02-10 20:30:00 to 2019-02-13 12:00:00

➔Command: journalctl - - since “2019-02-10 20:30:00 “ - - until “2019-02-13 12:00:00”

7) Display all entries in the last hour, you can use the below command.

➔Command: journalctl - - since “-1 hour”

8) To visible content of the journal, there are fields attached to the log entries that can only be seen when verbose output is turned on.

➔Command: journalctl -o verbose

9) To display the journal entries related to sshd. service systemd unit from a process with PID 1182.

➔Command: journalctl _SYSTEMD_UNIT=sshd.service _ PID=1182

Setting Local Clocks and Time Zones:

1. To overview of the current time-related system settings, including current time, time zone, and NTP Synchronization settings of the system.

➔Command: timedatectl

2. A database of time zones is available and can be listed using below command.

➔Command: timedatectl list-timezones

3. To update the current time zone use the below command.

➔ Command: timedatectl set-timezone America/Phoenix

4. To set the system current time use the below command.

➔ Command: timedatectl set-time 9:00:00

5. To enables or disables NTP synchronization for automatic time adjustment. The option requires either a true or false argument to turn it on or off.

➔ Command: timedatectl set-ntp true

6. After configuring the above details / pointing chronyd to the local time source, "classroom.example.com", you should restart the service.

➔Command: systemctl restart chronyd

7. After setting up NTP synchronization, you should verify that the local system is seamlessly using the NTP server to synchronize the system clock using the chrony sources command. For more verbose output with additional explanations about the output, use the chronyc sources -v command.

➔ Command: chronyc sources -v

END