CHAPTER-11 ANALYZE AND STORE LOGS

Describe System Log Architecture

System Logging

The operating system kernel and other processes record a log of events that happen when the system is running. These logs are used to audit the system and to troubleshoot problems. You can use text utilities such as the **less and tail** commands to inspect these logs.

Red Hat Enterprise Linux uses a standard logging system that is based on the **Syslog protocol** to log the system messages. Many programs use the logging system to record events and to organize them into log files. The **systemd-journald** and **rsyslog services** handle **the syslog messages** in Red Hat Enterprise Linux 9.

The systemd-journald service is at the heart of the operating system **event logging architecture**. The systemd-journald service collects event messages from many sources:

- System kernel
- Output from the early stages of the boot process
- Standard output and standard error from daemons
- Syslog events

The systemd-journald service restructures the logs into a standard format and writes them into a structured**, indexed system journal**. By default, this journal is stored on a file system that does not persist across reboots.

The rsyslog service reads syslog messages that the systemd-journald service receives from the journal as they arrive. The rsyslog service then processes the syslog events, and records them to its log files or forwards them to other services according to its own configuration.

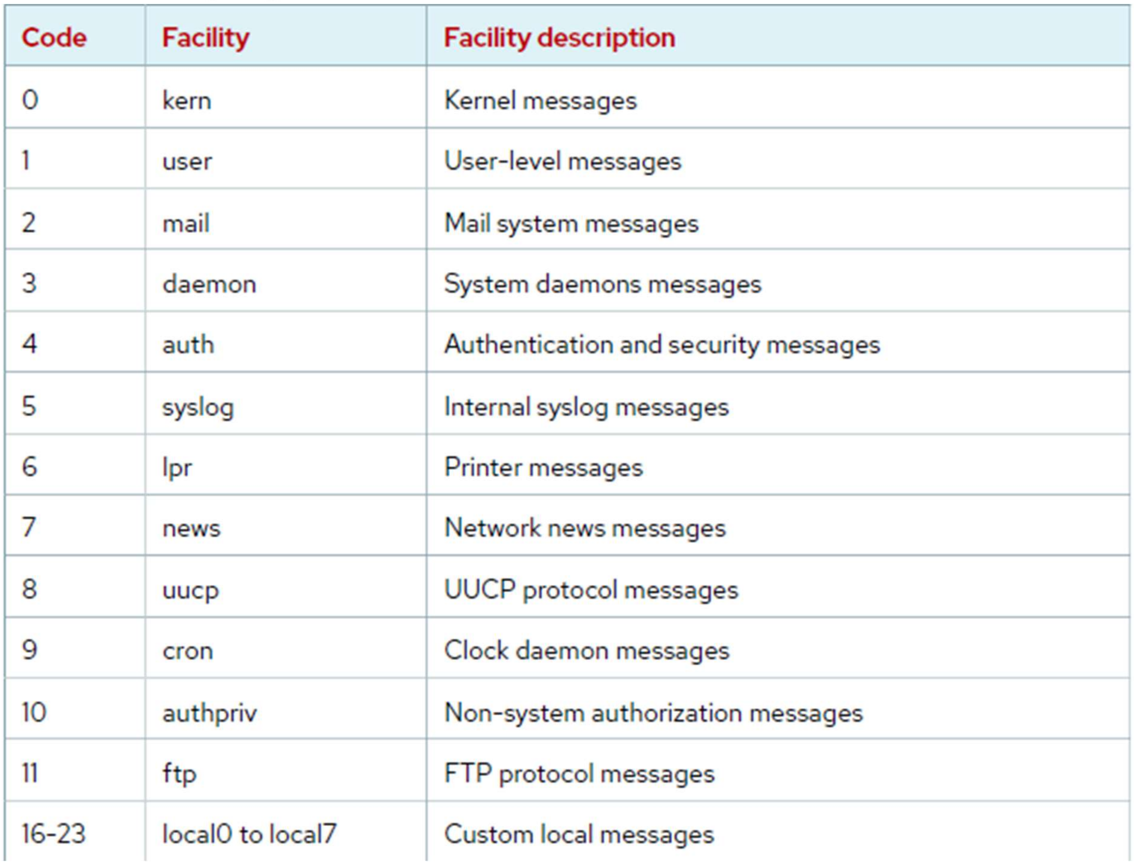
The rsyslog service sorts and writes syslog messages to the log files that do persist across reboots in the **/var/log directory**. The service also sorts the log messages to specific log files according to the type of program that sent each message and the priority of each syslog message.
To syslog message files, the /var/log directory contains log files from other services on the system. The following table lists some useful files in the /var/log directory.

LOG FILE	TYPE OF STORED MESSAGES
/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.

Review Syslog Files

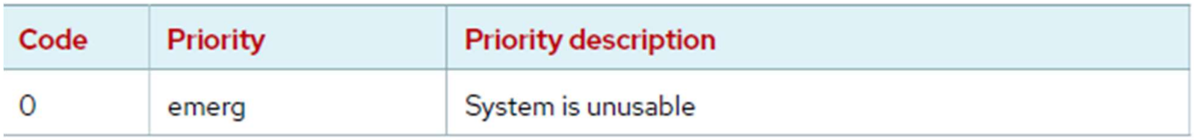
Log Events to the System

Overview of Syslog Facilities

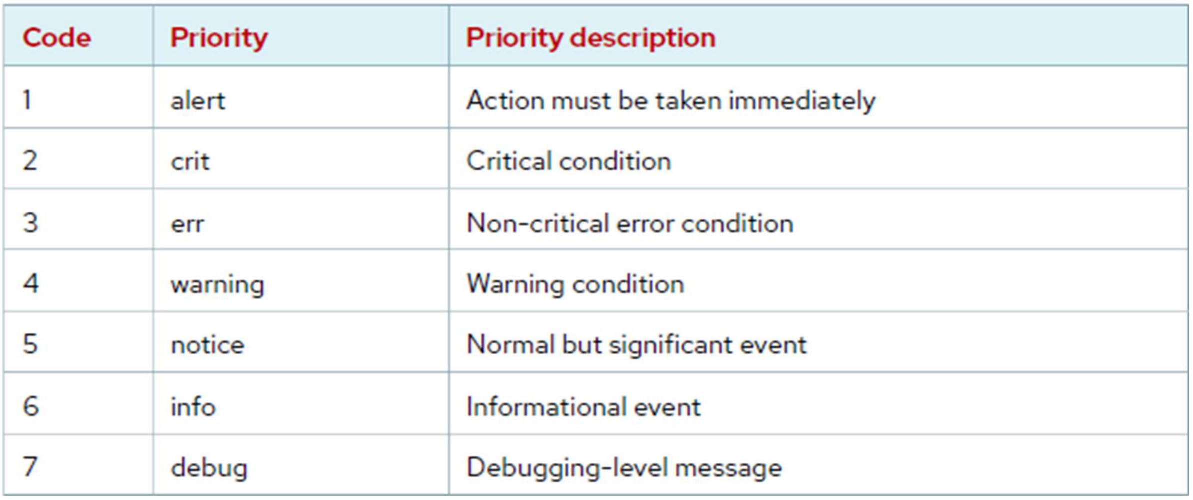


Code	Facility	Facility description
0	kern	Kernel messages
1	user	User-level messages
2	mail	Mail system messages
3	daemon	System daemons messages
4	auth	Authentication and security messages
5	syslog	Internal syslog messages
6	lpr	Printer messages
7	news	Network news messages
8	uucp	UUCP protocol messages
9	cron	Clock daemon messages
10	authpriv	Non-system authorization messages
11	ftp	FTP protocol messages
16-23	local0 to local7	Custom local messages

Overview of Syslog Priorities



Code	Priority	Priority description
0	emerg	System is unusable



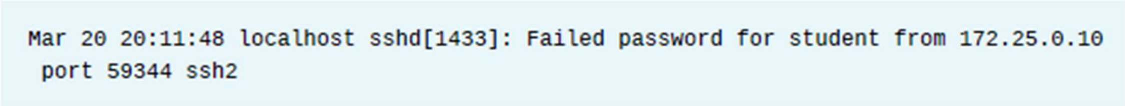
Code	Priority	Priority description
1	alert	Action must be taken immediately
2	crit	Critical condition
3	err	Non-critical error condition
4	warning	Warning condition
5	notice	Normal but significant event
6	info	Informational event
7	debug	Debugging-level message

The rsyslog service uses the facility and priority of log messages to determine how to handle them. Rules configure this facility and priority in the /etc/rsyslog.conf file and in any file in the /etc/rsyslog.d directory with the .conf extension. Software packages can easily add rules by installing an appropriate file in the /etc/rsyslog.d directory.

DESCRIPTION	COMMANDS / OPTIONS
Rotates log files to prevent them from taking too much space in the /var/log directory	**Syntax:** logrotade [options][directory_name] **-p** parent directory **Example:** [user@host ~]$ mkdir -p /Dir1/Dir2 ↵ **-v** Enables verbose mode **-m** Sets file modes or permissions **Example:** [user@host ~]$ mkdir -m a=rwx [directories] ↵

Analyse a Syslog Entry

Log messages start with the oldest message at the start and the newest message at the end of the log file. The rsyslog service uses a standard format for recording entries in log files.



```
Mar 20 20:11:48 localhost sshd[1433]: Failed password for student from 172.25.0.10
 port 59344 ssh2
```

- Mar 20 20:11:48 : Records the time stamp of the log entry.
- localhost : The host that sends the log message.
- sshd[1433] : The program or process name and PID number that sent the log message.
- Failed password for … : The message that was sent.

DESCRIPTION	**COMMANDS / OPTIONS**
Monitor Log Events	Monitoring log files for events is helpful to reproduce issues. **The tail -f /path/to/file** command outputs the last ten lines of the specified file and continues to output newly written lines in the file. **Example:** [user@host ~]$ tail -f /var/log/secure ↵
Send Syslog Messages Manually	**Syntax:** 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

Review System Journal Entries

Find Events on the System Journal

The systemd-journald service stores logging data in a structured, indexed binary file called journal. This data includes extra information about the log event. For example, for syslog events this information includes the priority of the original message and the facility, which is a value that the syslog service assigns to track the process that originated a message.

DESCRIPTION	**COMMANDS / OPTIONS**
To retrieve log messages from the journal, use the journalctl command • The journalctl command highlights important log messages; messages at notice or warning priority are in bold text, while messages at the error priority or higher are in red text.	**Syntax:** 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

Preserve the System Journal

System Journal Storage

By default, Red Hat Enterprise Linux 9 stores the system journal in the /run/log directory, and the system clears the system journal after a reboot. You can change the configuration settings of the systemd-journald service in the **/etc/systemd/journald.conf** file so that the journals persist across a reboot.

The Storage parameter in the **/etc/systemd/journald.conf** file defines whether to store system journals in a volatile manner or persistently across a reboot. Set this parameter to persistent, volatile, auto, or none as follows:

- **Persistent:** Stores journals in the /var/log/journal directory, which persists across reboots. If the /var/log/journal directory does not exist, then the systemd-journald service creates it.
- **Volatile:** Stores journals in the volatile /run/log/journal directory. As the /run file system is temporary and exists only in the runtime memory, the data in it, including system journals, does not persist across a reboot.
- **Auto:** If the /var/log/journal directory exists, then the systemd-journald service uses persistent storage; otherwise it uses volatile storage. This action is the default if you do not set the Storage parameter.
- **None:** Do not use any storage. The system drops all logs, but you can still forward the logs.

The systemd-journald process logs the current limits on the size of the journal when it starts. The following command output shows the journal entries that reflect the current size limits:

```
[user@host ~]$ journalctl | grep -E 'Runtime Journal|System Journal'
```

Configure Persistent System Journals

DESCRIPTION	COMMANDS / OPTIONS
To configure the systemd-journald service to preserve system journals persistently across a reboot	**Example: Create the /var/log/journal directory** **[root@host ~]#** mkdir /var/log/journal Set the Storage parameter to the persistent value in the **/etc/systemd/ journald.conf** file. Run your chosen text editor as the superuser to edit the **/etc/ systemd/journald.conf** file. **Example: Restart the systemd-journald service to apply the configuration changes.**

	[root@host ~]# systemctl restart systemd-journald **Example: To limit the output to a specific system boot, use the journalctl command –b option.** **[root@host ~]#** journalctl -b 1 ↵ **Example: You can list the system boot events that the journalctl command recognizes by using the --list-boots option.** **[root@host ~]#** journalctl --list-boots ↵

Maintain Accurate Time

Administer Local Clocks and Time Zones

System time synchronization is critical for log file analysis across multiple systems. Also, some services might require time syncronization to work properly. The Network Time Protocol is a standard way for machines to provide and obtain correct time information over the Internet.

The **timedatectl** command shows an overview of the current time-related system settings, including the current time, time zone, and NTP synchronization settings of the system.

The **chronyd service** keeps on track the usually inaccurate local Real-Time Clock (RTC) by synchronizing it to the configured NTP servers. If no network connectivity is available, then the chronyd service calculates the RTC clock drift, and records it in the file that the driftfile value specifies in the **/etc/chrony.conf** configuration file.

DESCRIPTION	**COMMANDS / OPTIONS**
The timedatectl command	**Syntax:** journalctl [options] [unit] list-timezones set-timezone xxxx set-time 0000 set-ntp false /ture
Configure and Monitor the chronyd Service	**chronyd** — daemon that can be started at boot time **chronyc** — command-line interface for chrony **Install chronyd in RHEL Server** **Syntax:** yum install chrony **Check status of service** **Syntax:** systemctl status chronyd **To Check Chrony Synchronization** **Syntax:** chronyc tracking **To check information about chrony's sources** **Syntax:** chronyc sources