# RedHat Certified System Administrator (RHEL 9)

SUMMARY

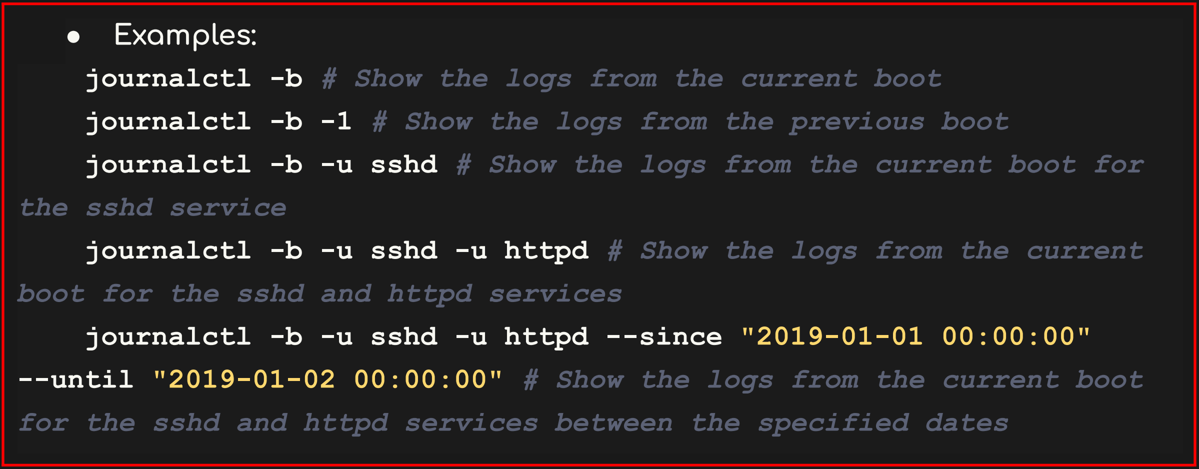
## System Logging

Services Can Log using three different methods:

- systemd-journald: The systemd-journald daemon collects and stores logging data.
- rsyslog: The rsyslog daemon is a traditional logging service that can be used to collect and store logging data.
- Directly to a file: Some services (for example httpd) can log directly to a file.

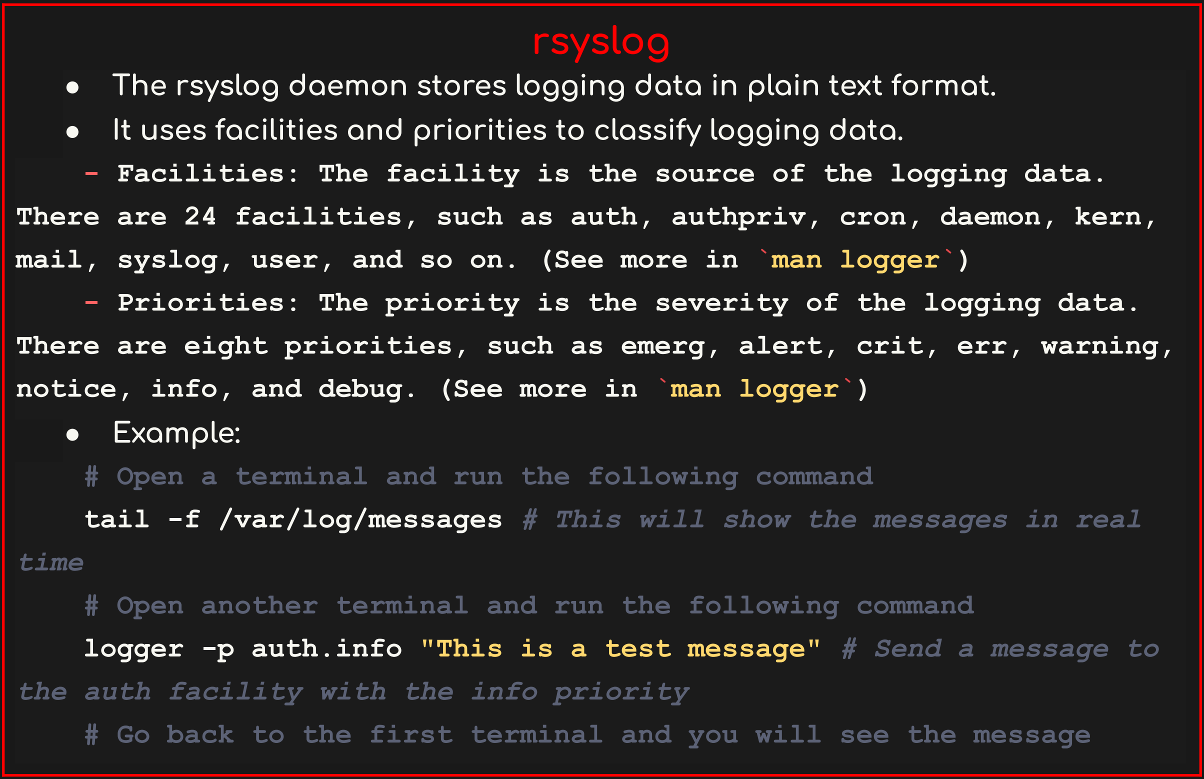
## systemd-journad

- The systemd-journald is a system service that collects and stores logging data.
  - Check its status with `systemctl status systemd-journald`
- The systemd-journald daemon collects and stores logging data starting from the boot process.
- The systemd-journald daemon stores logging data in binary format.
- By default, the systemd-journald daemon is not persistent across reboots (it store the logs in /run/log/journal)
  - To make it persistent, you have two options:
    1. Create a directory /var/log/journal.
    2. Change the configuration file /etc/systemd/journald.conf, and set the Storage option to persistent. (check the man page for more options `man journald.conf`)
- The utility journalctl can be used to query the systemd-journald daemon.
  - The utility journalctl can be used to query and filter the logging data collected by the systemd-journald daemon.



- Examples:

```
    journalctl -b # Show the logs from the current boot
    journalctl -b -1 # Show the logs from the previous boot
    journalctl -b -u sshd # Show the logs from the current boot for the sshd service
    journalctl -b -u sshd -u httpd # Show the logs from the current boot for the sshd and httpd services
    journalctl -b -u sshd -u httpd --since "2019-01-01 00:00:00" --until "2019-01-02 00:00:00" # Show the logs from the current boot for the sshd and httpd services between the specified dates
```



## rsyslog

- The rsyslog daemon stores logging data in plain text format.
- It uses facilities and priorities to classify logging data.

```
    - Facilities: The facility is the source of the logging data. There are 24 facilities, such as auth, authpriv, cron, daemon, kern, mail, syslog, user, and so on. (See more in `man logger`)
    - Priorities: The priority is the severity of the logging data. There are eight priorities, such as emerg, alert, crit, err, warning, notice, info, and debug. (See more in `man logger`)
```

- Example:

```
    # Open a terminal and run the following command
    tail -f /var/log/messages # This will show the messages in real time
    # Open another terminal and run the following command
    logger -p auth.info "This is a test message" # Send a message to the auth facility with the info priority
    # Go back to the first terminal and you will see the message
```