Lab 1: Exploring Rocky log locations

Objectives

- Identify key log files and directories.
- Understand the difference between journald and traditional logs.

Tasks

1. Log in to a Rocky Linux VM as a non-root user with sudo.
2. Explore traditional logs:
    - List files in `/var/log` and note sizes and ownership.
    - Inspect:
        - `/var/log/messages` (or `/var/log/syslog` if present)
        - `/var/log/secure`
        - `/var/log/dnf.log`
        - `/var/log/cron`
        - `/var/log/audit/audit.log` (if auditd is installed)[1][2]
3. Use basic tools to inspect logs:
    - `tail`, `less`, `grep`, `zgrep` (for rotated logs).
    - Find all sudo attempts in `/var/log/secure`.
4. Compare this with what `journalctl` shows:
    - `journalctl -xe`
    - `journalctl -b`
    - `journalctl -k`[3][4]
5. Short written questions:
    - Which logs are only visible in the journal and not as plaintext?
    - Which logs are only in files under `/var/log`?

Lab 2: Configuring persistent journald logging

By default, journald may store logs only in `/run/log/journal` (volatile). Configure persistent logging.[2][4][1]

Objectives

- Enable persistent storage for the journal.
- Verify logs survive reboots.

Tasks

1. Check current journald storage:
    - `journalctl --disk-usage`
    - `ls -ld /run/log/journal /var/log/journal`
2. Enable persistence:
    - Create directory: `sudo mkdir -p /var/log/journal`[5][4]
    - Ensure proper ownership/permissions via tmpfiles:
        - `sudo systemd-tmpfiles --create --prefix /var/log/journal`[4]
    - Edit `/etc/systemd/journald.conf`:
        - Set `Storage=persistent` (uncomment if needed).[6][1][2]
3. Apply changes:
    - `sudo systemctl restart systemd-journald` (or `systemctl daemon-reexec` after editing config).[7][6]
4. Verification:
    - Reboot the VM.
    - Run `journalctl -b -1` and confirm you can see logs from the previous boot.[3][4]
    - Confirm journal files exist under `/var/log/journal` and note their sizes.[1][2]
5. Question:
    - Explain the difference between `Storage=auto`, `volatile`, and `persistent` in `journald.conf`.[2][1]

Lab 3: Querying and filtering with journalctl

Focus on log analysis and filtering using `journalctl`.[7][4][3]

Objectives

- Use `journalctl` filters effectively.
- Correlate issues by service, unit, and priority.

Tasks

1. Basic usage:
    - View last 50 lines: `journalctl -n 50`
    - Follow logs: `journalctl -f`
2. Time-based filtering:
    - Show logs from the last 10 minutes.
    - Show logs since a specific date/time (e.g. `--since "2026-01-21 13:00:00"`).[4][7]
3. Service/unit filtering:
    - Show logs for `sshd` only: `journalctl -u sshd`
    - Show logs for a systemd unit you install/enable in another lab (e.g., `nginx.service` or a custom unit).[7]
4. Priority-based filtering:
    - Show only errors and above: `journalctl -p err -b`[8][3][4]
    - Count how many `err` or higher messages occurred on the current boot.
5. Export and rotation operations:
    - Show total disk usage: `journalctl --disk-usage`[1][2][4]
    - Reduce size with `journalctl --vacuum-size=100M` in a lab-only VM and observe impact.[2][4][1]
6. Question:
    - When would you prefer `journalctl -u <service>` over grepping `/var/log/messages`?

Lab 4: Integrating journald and rsyslog

Have students see how journald and rsyslog work together and configure a custom log stream.[8][3][1]

Objectives

- Understand journald → syslog (rsyslog) forwarding.
- Create a custom rsyslog rule and verify it using journald.

Tasks

1. Confirm services:
   - `systemctl status systemd-journald`
   - `systemctl status rsyslog` (install if missing: `sudo dnf install rsyslog -y`).[3][1]
2. Inspect `/etc/systemd/journald.conf`:
   - Ensure `ForwardToSyslog=yes` so rsyslog gets journal messages.[1][3]
3. Inspect `/etc/rsyslog.conf` and `/etc/rsyslog.d/`:
   - Identify modules being loaded (e.g. `imjournal`).
   - Find the rule that writes to `/var/log/messages`.[1]
4. Create a custom rsyslog rule:
   - In `/etc/rsyslog.d/app-debug.conf`, add something like:
     - All `local0.*` → `/var/log/app-debug.log`
   - Restart rsyslog: `sudo systemctl restart rsyslog`.[8][1]
5. Generate logs:
   - Use `logger -p local0.info "Test info from lab"` and `logger -p local0.err "Test error from lab"`.
   - Verify:
     - Entries appear in `/var/log/app-debug.log`.
     - Same messages visible via `journalctl -t logger` or filtered by priority.[4][3]
6. Question:
   - Describe how a log line from `logger` ends up both in the journal and in `/var/log/app-debug.log`.

Lab 5: Remote logging (optional extension)

If you have multiple Rocky VMs, add a small remote logging scenario.[9][8]

Objectives

- Configure rsyslog to send logs to a remote syslog receiver.
- Confirm that journald logs are relayed off-box.

Tasks

1. On the "log server":
    - Enable rsyslog to listen on UDP 514 and/or TCP 514 (e.g. add `module(load="imudp")` and `input(type="imudp" port="514")`).[8]
    - Add a rule to write remote logs to `/var/log/remote.log`.
    - Restart rsyslog and confirm port listening with `ss -lunpt | grep 514`.
2. On the "client":
    - Ensure journald forwards to syslog (`ForwardToSyslog=yes`).[3]
    - Configure rsyslog to forward all messages to the server:
        - `*.* @@logserver.example.com:514` (TCP) in `/etc/rsyslog.d/remote.conf`.[9][8]
    - Restart rsyslog.
3. Testing:
    - On client: `logger -p auth.notice "Remote auth test from $(hostname)"`.
    - On server: Tail `/var/log/remote.log` and confirm the message appears.[8]
4. Question:
    - Why is journald alone not enough for remote log forwarding in typical RHEL/Rocky setups?

Additional information…..

1. https://docs.rockylinux.org/9/books/admin_guide/17-log/
2. https://docs.rockylinux.org/8/books/admin_guide/17-log/
3. https://www.redhat.com/en/blog/rsyslog-systemd-journald-linux-logs
4. https://www.digitalocean.com/community/tutorials/how-to-use-journalctl-to-view-and-manipulate-systemd-logs
5. https://access.redhat.com/solutions/696893
6. https://support.cpanel.net/hc/en-us/articles/360053094893-How-to-enable-persistent-logging-for-the-systemd-journal-journalctl
7. https://reintech.io/blog/enabling-using-journald-system-logging-rocky-linux
8. https://www.loggly.com/ultimate-guide/centralizing-with-syslog/
9. https://docs.redhat.com/en/documentation/red_hat_enterprise_linux/9/html/security_hardening/assembly_configuring-a-remote-logging-solution_security-hardening
10. https://docs.rockylinux.org/10/books/admin_guide/17-log/
11. https://www.reddit.com/r/linuxadmin/comments/1liggsa/managing_systemd_logs_on_linux_with_journalctl/
12. https://wiki.almalinux.org/series/system/SystemSeriesA09.html
13. https://www.youtube.com/watch?v=Tjwko6UsJ60
14. https://www.youtube.com/watch?v=sY3gZQueuSA
15. https://docs.eclecticiq.com/ic/3.2.3/install-configure-upgrade/rocky/reference/config-and-log-files/