□□ Log Management Referenc

Category: All About Ubuntu
Last Updated: May 14th, 2025

□□ Default Log File Locations

Most Linux systems (especially Debian/Ubuntu) store logs in these locations:

Path	Purpose
`/var/log/`	Main system log directory
`/var/log/syslog`	General system messages
`/var/log/auth.log`	Authentication (sudo, SSH, etc.)
`/var/log/kern.log`	Kernel messages
`/var/log/dmesg`	Boot-time hardware logs
`/var/log/ufw.log`	UFW firewall logs
`/var/log/fail2ban.log`	Fail2Ban logs
`/var/log/apache2/`	Apache logs
`/var/log/mysql/`	MySQL logs
`/var/log/journal/`	`systemd` journal logs (binary format)

> □□ **Best Practice:** Custom scripts should log to `/var/log/your-script-name.log` for consistency and ease of monitoring.

□□ How to Locate Log Files

1. **Explore the `/var/log` directory**

```
ls -lah /var/log
```

---

2. **Search for `.log` files**

- Search entire system:

```
sudo find / -type f -iname '*.log' 2>/dev/null
```

- Search recent `.log` files (modified in last day):

```
sudo find / -type f -iname '*.log' -mtime -1 2>/dev/null
```

---

3. **Use `locate` for fast results**

```
sudo updatedb
locate '*.log'
```

---

4. **Search config files for log paths**

```
grep -R --include='*.conf' -n '\.log' /etc
```

---

5. **Live view or tail logs**

- Tail latest lines:

```
tail -n 50 /var/log/syslog
```

- Live follow:

```
tail -f /var/log/fail2ban.log
```

□□ Log Rotation wit`logrotate`

To prevent log files from growing indefinitely, configure rotation using files in:

```
/etc/logrotate.d/
```

□ Example: Correct Logrotate Format

File: `/etc/logrotate.d/fail2ban-ip-lookup`

```
/var/log/fail2ban-ip-lookup.log {
    su root root
    daily
    rotate 7
    compress
    missingok
    notifempty
    create 644 root root
}
```

- `su root root` ensures correct user/group even when run via cron.
- `daily` rotates logs each day.
- `rotate 7` keeps 7 old copies.
- `compress` gzips old logs.
- `notifempty` skips rotation if the file is empty.
- `create 644 root root` sets the new log file's permissions and ownership.

□□ Test & Force Rotation

- **Dry run** of logrotate:

```
sudo logrotate -d /etc/logrotate.conf
```

- **Force rotate** a specific config:

```
sudo logrotate -f /etc/logrotate.d/fail2ban-ip-lookup
```

□□ Clear Log File Without Deleting

Preserve file permissions:

```
sudo truncate -s 0 /var/log/your-log-file.log
```

□□ Optional: Email Alerts on Log Events

Example for alerting on high abuse score:

```
grep "Abuse Score: 100" /var/log/fail2ban-ip-lookup.log | mail -s "□□ High Abuse Score Alert" you@example.com
```

Revision #1
Created 14 May 2025 21:44:56 by Nate Nash
Updated 4 June 2025 23:32:00 by Nate Nash