Presented by Group 22

Log Management and Rotation with Logrotate

Linux Operating System and Applications

9 August, 2025

Team Members

Nguyen Van Hoa

22127118

Nguyen Ngoc Bao Khang

22127179

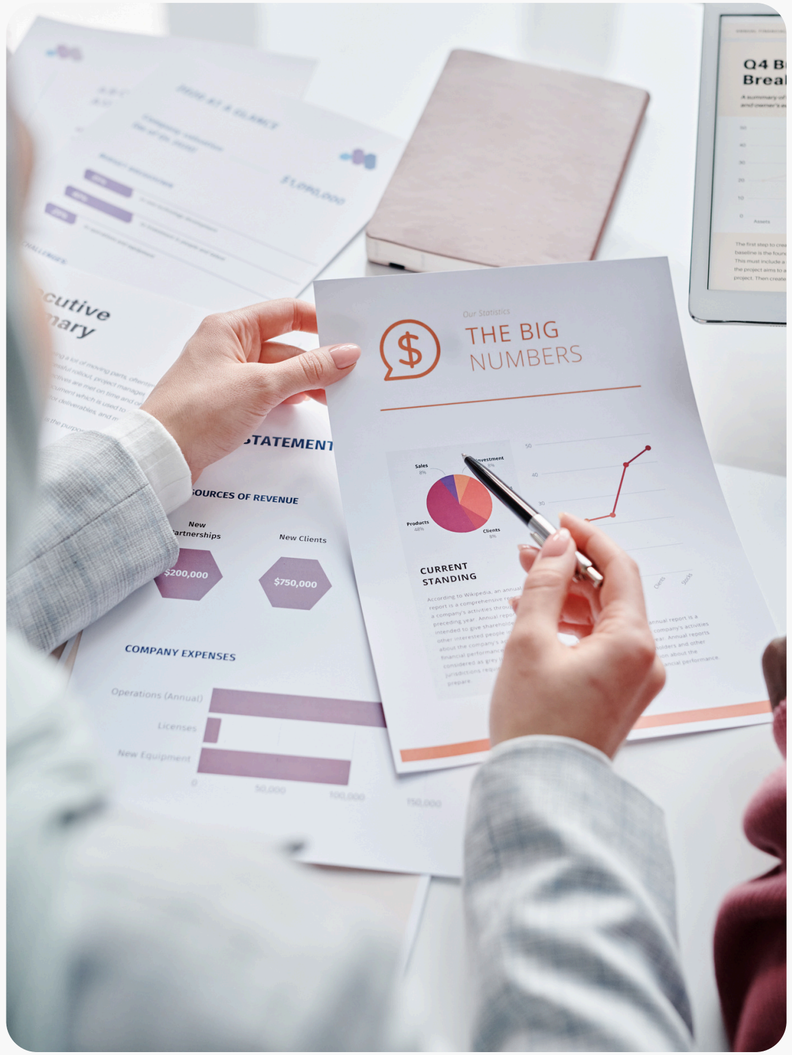
Why Log Management Matters

Essential information
Logs are essential for troubleshooting, auditing, and monitoring

Log Management
Important to archive, compress, or delete them regularly

Storage problems
Without management, logs can consume disk space

Introduction to syslogd/rsyslogd



Collects and stores system logs

Categorized by:

- Facility (e.g., auth, cron, daemon)
- Level (e.g., debug, info, warn, err)
- Action (e.g., store, forward)

Config file: /etc/rsyslog.conf

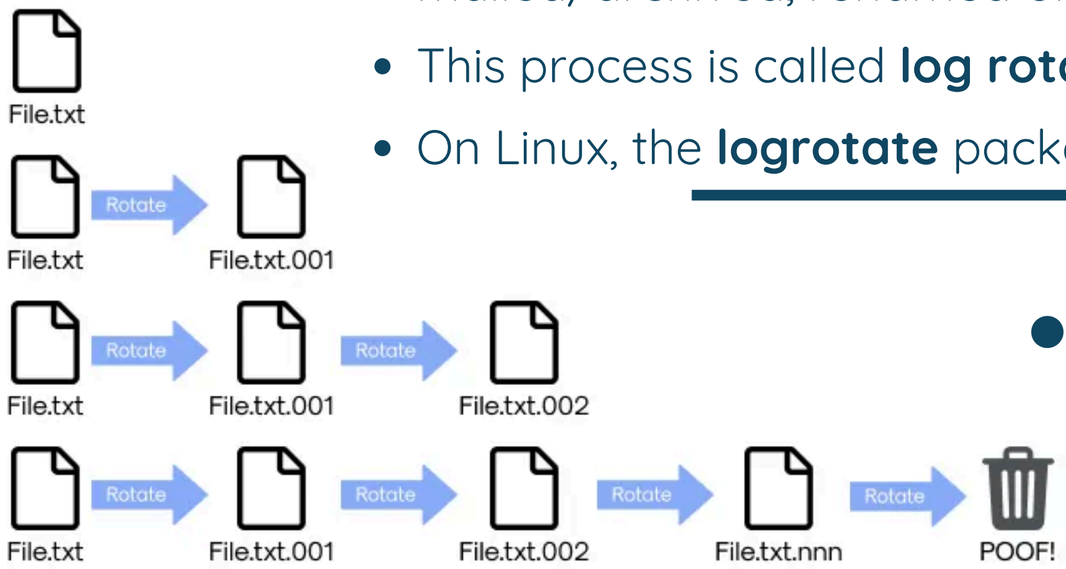
Common log location: /var/log

Common log files:

- /var/log/messages: General system messages
- /var/log/auth.log or /secure: Authentication events
- /var/log/syslog: System activity
- /var/log/nginx/: Web server logs

What is log rotation?

- Over time, the system can pile up a huge amount of log files, which can chew up a lot of disk space.
- To prevent this, old and/or large log files can be compressed, mailed/archived, renamed or removed.
- This process is called **log rotation**.
- On Linux, the **logrotate** package offers utilities for log rotation.



logrotate *package installation*

Debian/Ubuntu	`apt install logrotate`
Arch	`pacman -S logrotate`
Red Hat/Fedora	`dnf install logrotate`
Gentoo	`emerge --ask app-admin/logrotate`
SUSE	`zypper install logrotate`

Configuration

/etc/logrotate.conf

This is the primary configuration file for logrotate which sets default (global) parameters.

/etc/logrotate.d

- syslog-ng
- pacman
- nginx

This is the directory where additional application-specific configuration files are included.

```
# sample logrotate configuration file
compress
/var/log/messages {
    rotate 5
    weekly
    postrotate
        /usr/bin/killall -HUP syslogd
    endscript
}
"/var/log/httpd/access.log" /var/log/httpd/error.log {
    rotate 5
    mail recipient@example.org
    size 100k
    sharedscripts
    postrotate
        /usr/bin/killall -HUP httpd
    endscript
}
/var/log/news/* {
    monthly
    rotate 2
    olddir /var/log/news/old
    missingok
    sharedscripts
    postrotate
        kill -HUP $(cat /var/run/inn.pid)
    endscript
    nocompress
}
~/log/*.log {}
# source: https://man.archlinux.org/man/logrotate.conf.5
```

Configuration

/etc/logrotate.conf

This is the primary configuration file for logrotate which sets default (global) parameters.

/etc/logrotate.d

- syslog-ng
- pacman
- nginx

This is the (default) directory where additional application-specific configuration files are included.

```
# logrotate configuration file for pacman
/var/log/pacman.log {
    monthly
    rotate 3
    compress
    notifempty
    missingok
}
```

Configuration

Retention & Rotation Policy

 # Rotation

rotate <count>
olddir <directory>
noolddir
su <user group>

 # Compression

compress
nocompress
compresscmd
uncompresscmd
compressext
compressoptions
delaycompress
nodelaycompress

 # File Selection

missingok
nomissingok
ifempty
noifempty
minage <count>
maxage <count>
tabooext [+] <list>
taboopat [+] <list>

 # Frequency

hourly
daily
weekly [weekday]
monthly
yearly
size <size>

 # Files & Folders

create [mode] <owner> <group>
nocreate
createolddir [mode] [owner [group]]
nocreateolddir
copy
nocopy
copytruncate
renamecopy
norenamecopy
shred
noshred
shredcycles <count>
allowhardlink
noallowhardlink

 # Mail

mail <address>
nomail
mailfirst
maillast
mailcmd

 # Filenames

extension <ext>
addextension <ext>
start <count>
dateext
nodateext
dateformat <format_string>
dateyesterday
datehourago

 # Scripts

sharedscripts
nosharedscripts
firstaction
lastaction
prerotate
postrotate
preremove

 # Additional config files

include <file/directory>

source: https://man.archlinux.org/man/logrotate.conf.5

Configuration

Configuration file

```
#    # look what this config file does, guys
#compress with gzip    compress
#rotate two files    "/var/log/httpd/access.log" /var/log/httpd/error.log {
#rotate 5 times before removal or mailing        rotate 5
#mail instead of simply removing        mail recipient@example.org
#rotate when file size exceed 100 KB        size 100k
#make the line below run once for 2 files        sharedscripts
#run script after every rotation        postrotate
#            /usr/bin/killall -HUP httpd
#        endscript
#    }
#all files there, Ctrl C and V here    include /etc/logrotate.d
#    # source: https://man.archlinux.org/man/logrotate.conf.5
```

More rules:

local definitions override global ones, and later definitions override earlier ones.

logrotate *status*

Did you know?

logrotate also has its own log!

by default, at
/var/lib/logrotate.status

```
"/var/log/mysql/query.log" 2016-3-20-5:0:0
"/var/log/samba/samba-smbd.log" 2016-3-21-5:0:0
"/var/log/httpd/access_log" 2016-3-20-5:0:0
...

# source: https://wiki.archlinux.org/title/Logrotate
```

Or put it elsewhere if you don't like it here. For instance:

```
sudo logrotate -s ~/.config/fastfetch/logrotate.state /etc/logrotate.conf
```

logrotate *on command line*

```
$ logrotate                          or
                    --force     -f   # force, manual rotation
                    --debug     -d   # debug mode, no change to state file or log file
                 --state file   -s   # use alternate state file
             --skip-state-lock       # do not lock the state file
          --wait-for-state-lock      # wait for state file unlock (can meet DEADLOCK!!!)
                  --verbose     -v   # verbose mode, display messages during rotation
                  --log file    -l   # log verbose output
                --mail command  -m   # Tells logrotate which command to use when mailing logs
 config_file config_file2 ...        # and custom rotation config (please avoid overlapping!)

                    --usage          # print a short usage message
                     --help    -?   # print help message
                  --version          # print version info
```

logrotate *on command line*

Manual rotation

- **force rotation:**

```
logrotate -f /etc/logrotate.conf
```

- **rotation in debug mode:**

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

- **view the files:**

```
ls -l /var/log/*.gz
```

Best Practices

Date/timestamp renaming

- This makes the log files more easy to read
- Use the dateext directive

Centralized log files/servers

- Reduce pressure on local servers' storage space.
- Keep logs from being tampered or accessed; compare with host's logs to troubleshoot

...simply keeping the logs

- Keep them fully intact and safe from tampering, you may not know when you need them

Suggested by https://sematext.com/glossary/log-rotation#log-rotation-best-practices

Demonstration

Conclusion

Logrotate allows automatic rotation, compression, removal and mailing of log files, offering a great utility to simplify the administration of log files on a system which can generate a lot of log files.

Thank you for your attention.