Log Rotation:
The unsung hero

Ell Marquez • ell.marquez@rackspace.com

Logs .... Logs .... Logs

What?

- Os Level
  - Rsyslog /etc/syslog.d -
  - /var/log
- Application Logs
  - Nginx, httpd ...
  - /var/log/httpd

Why?

- Logs allow us to Track usage or Troubleshoot however we run into several issues:
  - Log Size
  - Disk Space

How?
Read the man page!

Logrotate

- Rotates , compresses and mails system logs /etc/cron.daily/logrotate
    - Gentoo (logrotate.cron)

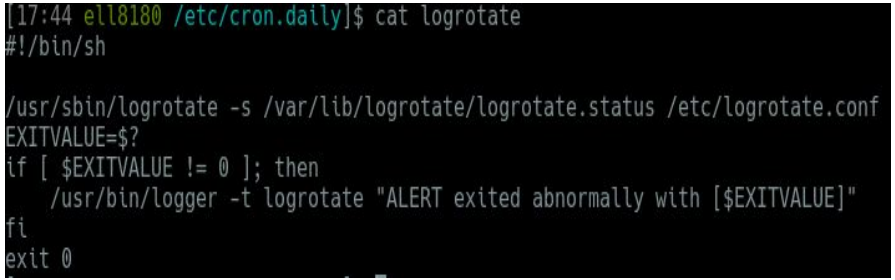
Important Details:

- Logrotate runs as a daily cron job
- Behavior is defined by listing the log file/files followed by a set of commands.
    - Later configuration files may override the options given in earlier files.

How Logrotate Works?

Cron.daily

- Cron schedules a command or script to run automatically.
- A **cron job** is the scheduled task itself
    - Great for repetitive tasks
-



Logrotate .conf

- Read to determine where to find the log files that need to be rotated, how often to rotate and how many archive logs to keep.
- Rotate?
    - Creates a new file and archives the old. .

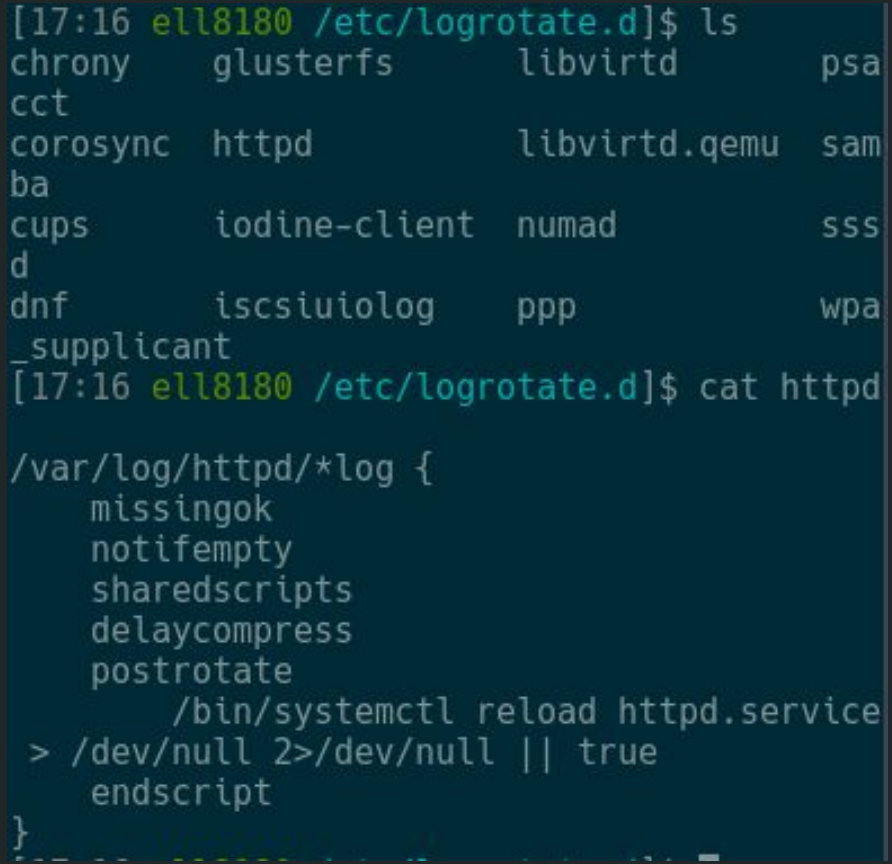
```
6:28 ell8180 /etc]$ cat logrotate.conf
see "man logrotate" for details
rotate log files weekly
ekly

keep 4 weeks worth of backlogs
tate 4

create new (empty) log files after rotating old ones
eate

use date as a suffix of the rotated file
teext

uncomment this if you want your log files compressed
ompress

RPM packages drop log rotation information into this directory
clude /etc/logrotate.d

no packages own wtmp and btmp -- we'll rotate them here
ar/log/wtmp {
  monthly
  create 0664 root utmp
  minsize 1M
  rotate 1


ar/log/btmp {
  missingok
  monthly
  create 0600 root utmp
  rotate 1


system-specific logs may be also be configured here.
```

logrotate.conf

- Read the man page!
- rotation - daily, weekly, monthly , yearly
- create- mode owner group
- dateext - adding a daily extension like YYYYMMDD instead of simply adding a number
- compress - Old versions of log files are compressed with gzip by default
- Note: include /etc/logrotate.d

Logrotate.d

- Applications installed through your package manager will also create a config file in /etc/logrotate.d
  - Sharedscripts - Normally, prerotate and postrotate scripts are run for each log which is rotated and the absolute path to the log file is passed as first argument to the script.



Configuration Commands

Where?

- Most application files will contain just one block of instructions to follow
    - Blocks are enclosed in curly brackets
- Some applications will include multiple files or add a file block to logrotate.conf

How?

```
/var/log/httpd/*log /etc/httpd/logs/*log {
    missingok
    notifempty
    sharedscripts
    delaycompress
    postrotate
        /bin/systemctl reload httpd.service >
/dev/null 2>/dev/null || true
    endscript
}
```

Let's talk troubleshooting!

Testing Logrotate

Verbose

“-v”, tells logrotate to say what it’s doing while it’s doing it.

Debug

The debug flag, “-d”, tells logrotate to go through the motions of rotating logs but not actually rotate them.

Force

The force flag, “-f”, forces logrotate to rotate all logs when it runs, whether or not they would normally need to be rotated at that time.

*** if logrotate is set to add a date to the name of an archived log, not even using the force flag will get logrotate to make a new archive in the same day (since the name it would use for the archive is already taken). You may need to rename the most recent archive.

How does logrotate remember?

```
[17:44 ell8180 /etc/cron.daily]$ cat logrotate
#!/bin/sh

/usr/sbin/logrotate -s /var/lib/logrotate/logrotate.status /etc/logrotate.conf
EXITVALUE=$?
if [ $EXITVALUE != 0 ]; then
    /usr/bin/logger -t logrotate "ALERT exited abnormally with [$EXITVALUE]"
fi
exit 0
```

```
[18:49 ell8180 ~]$ cat /var/lib/logrotate/logrotate.status
ogrotate state -- version 2

"/var/log/dnf.librepo.log" 2017-4-24-8:13:1
"/var/log/cups/page_log" 2016-8-14-20:0:0
"/var/log/iodine-client.log" 2016-8-14-20:0:0
"/var/log/cups/bjnp_log" 2016-8-15-12:0:0
"/var/log/dnf.rpm.log" 2017-4-24-8:13:1
"/var/log/dnf.plugin.log" 2016-8-14-20:0:0
"/var/log/hawkey.log" 2017-4-24-8:13:1
"/var/log/sssd/*.log" 2016-8-14-20:0:0
```

Troubleshooting

[root@unknown-splunk log]# logrotate -f /etc/logrotate.conf
error: syslog:1 glob failed for #/var/log/audit/audit.log*: No such file or directory
error: found error in file syslog, skipping

[root@734552-Splunk log]# logrotate -dv /etc/logrotate.conf
reading config file /etc/logrotate.conf
including /etc/logrotate.d
reading config file mcelog
reading config info for /var/log/mcelog
reading config info for /var/log/cron
/var/log/maillog
/var/log/messages
/var/log/secure
/var/log/spooler
#/var/log/audit/audit.log*

error: syslog:1 glob failed for #/var/log/audit/audit.log*: No such file or directory
error: found error in file syslog, skipping
removing last 1 log configs
reading config file up2date

```
[root@734552-Splunk logrotate.d]# cat syslog
/var/log/cron
/var/log/maillog
/var/log/messages
/var/log/secure
/var/log/spooler
#/var/log/audit/audit.log*
{
    sharedscripts
    size 1M
    compress
    postrotate
        /bin/kill -HUP `cat /var/run/syslogd.pid 2> /dev/null` 2> /dev/null || true
    endscript
}
```