

logrotate

- log proliferation containment

David Morgan

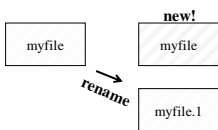
© David Morgan 2005

Logrotate function

- “rotates, compresses, and mails system logs”
- Operates on any file(s) you specify
- Operated on each, periodically
- Copies/renames it & makes a fresh empty
 - copies/renames previous backups first

© David Morgan 2005

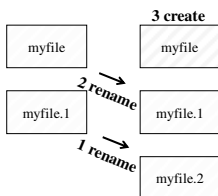
Logrotate function, January



- renames "myfile" to "myfile.1"
- creates new, empty "myfile"

© David Morgan 2005

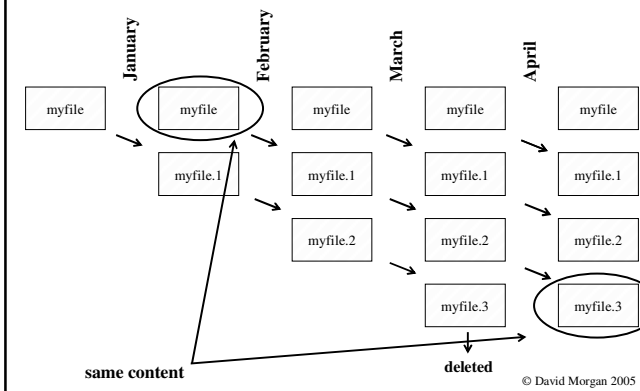
Logrotate function, February



- renames "myfile.1" to "myfile.2"
- renames "myfile" to "myfile.1"
- creates new, empty "myfile"

© David Morgan 2005

Logrotate function, count



pseudocode equivalent

<code>rm file.3</code>	delete the oldest
<code>mv file.2 file.3</code>	2nd archive becomes 3rd, by renaming
<code>mv file.1 file.2</code>	1st becomes 2nd
<code>mv file file.1</code>	current log becomes 1st archive
<code>touch file</code>	new log created, empty with normal name

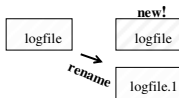
logrotate configuration file

General	Example
<pre># global directives <directive> <directive></pre>	<pre>weekly rotate 2 compress</pre>
<pre># file-specific treatments <filename 1> { <directive> <directive> }</pre>	<pre></var/log/messages> { nocompress }</pre>
<pre><filename 2> { <directive> <directive> }</pre>	<pre></var/log/samba/*.log> { monthly }</pre>

© David Morgan 2005

A little file confusion

ROTATION



before



after



© David Morgan 2005

The problem

- new archive *is* the old log, despite new name
- daemon faithfully continues writing to this file
 - writes to the archive
 - *not* the new log!
- must tell daemon(s) to switch files

© David Morgan 2005

The reason

- standard filesystem operations
- files are only *opened* by name
- but read, written, closed by handle/inode
- name change is superficial after a file is opened

typical file usage

first and last mention

```
declare variable fhandle
fhandle = fopen(name of file)
fread( fhandle, <where to put what you read> )
...
fwrite( fhandle, <the stuff you want written> )
fclose( fhandle )
```

© David Morgan 2005

The fix

- close/open the archive/log files
- daemon is in control of that
 - kill the daemon and restart it
 - signal the daemon to reprocess its config file(s)

e.g., `kill -HUP $(cat /var/run/syslogd.pid)`

or

`killall -e -HUP syslogd`

© David Morgan 2005

Add to pseudocode

`rm file.4`

`mv file.2 file.3`

`mv file.1 file.2`

`mv file file.1`

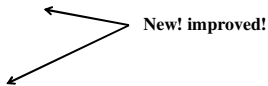
`touch file`

`killall -e -HUP <name of daemon>` ← **New! improved!**

© David Morgan 2005

Use 'postrotate/endscript'

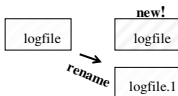
```
weekly
rotate 2
compress
</var/log/messages> {
    nocompress
    postrotate
        /sbin/killall -HUP syslogd
    endscript
}
</var/log/samba/*.log> {
    monthly
    postrotate
        /sbin/killall -HUP smbd
    endscript
}
```



© David Morgan 2005

File confusion dispelled

ROTATION



before



after



OK now!

© David Morgan 2005

logrotate - please note

- uses no configuration file by default
 - specify explicitly on command line
- is not recurring
 - partner with cron for that
- can rotate per size threshold instead of interval

© David Morgan 2005

logrotate - Fedora 4 defaults

- config file(s)
 - */etc/logrotate.conf* specified explicitly on command line (in */etc/cron.daily/logrotate*)
 - and “includes” 27 more config files from */etc/logrotate.d*
- recurrence
 - *runs* daily (per cron)
 - *rotates* weekly (unless otherwise by exception)
 - keeps 4 weeks’ worth

© David Morgan 2005