

# swatch (**s**imple **w**atchdog) keeping vigil over files

David Morgan

© David Morgan 2005

## rpm failed dependencies

[www.rpmfind.net](http://www.rpmfind.net) - needed perl-file-tail and perl-mail-sendmail

```
[root@EMACH1 ~]# rpm -Uvh perl-File-Tail-0.98-4.noarch.rpm
warning: perl-File-Tail-0.98-4.noarch.rpm: Header V3 DSA signature: NOKEY, key ID 1ac70ce6
Preparing... ##### [100%]
 1:perl-File-Tail ##### [100%]
[root@EMACH1 ~]# rpm -Uvh perl-Mail-Sendmail-0.79-7.noarch.rpm
warning: perl-Mail-Sendmail-0.79-7.noarch.rpm: Header V3 DSA signature: NOKEY, key ID
1ac70ce6
Preparing... ##### [100%]
 1:perl-Mail-Sendmail ##### [100%]
[root@EMACH1 ~]# rpm -Uvh swatch-3.1.1-3.fc4.noarch.rpm
warning: swatch-3.1.1-3.fc4.noarch.rpm: Header V3 DSA signature: NOKEY, key ID 1ac70ce6
Preparing... ##### [100%]
 1:swatch ##### [100%]
```

© David Morgan 2005

## swatch operation

- watches a file (e.g., a log)
- notices designated content
- reacts to its presence
- uses pattern-action specification to do so
  - pattern detection = trigger
  - action = resultant response

© David Morgan 2005

## target file definition

- command line's -t or -f option
  - swatch -f <filename>
- default: /var/log/messages

© David Morgan 2005

## target content definition: where?

- in a configuration file
- command line's -c option  
swatch -c <filename>
- default: ~/.swatchrc

© David Morgan 2005

## target content definition: how?

- watchfor <regular expression>  
watchfor /hello/                    find lines containing hello  
  
watchfor /sun|moon/                find lines containing sun or moon
- ignore <regular expression>  
ignore /goodbye/                    find lines containing hello

© David Morgan 2005

## reaction to target content

- watchfor

keyword(s) for reaction(s)

- ignore

define “no reaction!”

pattern/trigger

watchfor /hello/

<reaction keyword>

<reaction keyword>

} action/response

·  
·

© David Morgan 2005

## main action keywords

- echo

- mail

- exec

- pipe

matching message (contains “hello”) printed  
in red on terminal that launched swatch

matching message sent in email  
titled “hello visible” to you@isp.com  
(provided local mail transport agent running)

watchfor /hello/

echo=red

mail addresses=you\@isp.com,subject="hello visible"

(tell perl @ is literal)

© David Morgan 2005

# precedence

## swatch -f testfile

testfile :

text

hello goodbye

more text

matches both  
watchfor's target  
and  
ignore's target

~/swatchrc :

1. watchfor /hello/  
echo=red  
ignore /goodbye/

or

2. ignore /goodbye/  
watchfor /hello/  
echo=red

echoes "hello goodbye"?

**does**

**doesn't**

© David Morgan 2005

# examine vs tail

- batch mode (-t) examine whole file once and exit
- monitor mode (-f) continually examine incremental content whenever added

© David Morgan 2005

## swatching multiple files

- individual swatch instances, per file
  - swatch -c .swatchrc.messages -f /var/log/messages
  - swatch -c .swatchrc.secure -f /var/log/secure
- watching multiple machines
  - implicit if local machine used as a loghost  
(ie, other machines' log messages directed to local message file)

© David Morgan 2005

## restart after rotate

- must make swatch switch focus from old to new log file (renaming not sufficient - holds file by inode not name once opened)
- swatch does it
  - command line -r <time> option
  - set time to follow logrotation occasions
- logrotate can do it
  - postrotate script that runs/restarts swatch  
([Linux System Security](#) p 506)

© David Morgan 2005