Swatch
"simple log file monitoring"

Ivan Bütler – 23. Sept. 2009

Log File Monitoring

I am lazy – and therefore I do not check my log files daily. Even if the logs would disclose configuration errors, major or critical problems or even hacking attacks, the manual step of digging into the logs is somehow too exhausting. That's why most of the computers and servers I know are not monitored well. Sure – some of you have central logging facilities and a working monitoring team watching your logs day and night. But the rest of the world resides in the dark.

Alternatively, I decided to use "swatch", a program that is available since 10 years or more. Swatch is a simple perl program tailing logs and searching for patterns. Once the pattern matches, a notification can be executed, either by just belling, console text message, pager, sms or e-mail messages. In my case, I like to be informed with e-mails. This little tutorial shows how simple a swatch monitoring system could be setup and I encourage you to do the same with swatch or other similar tools on your internet facing servers.

Swatch Installation on CentOS

Swatch is in the standard CentOS repository; so I install it.

```
yum install swatch

================================================================================================================================
Package                      Version
================================================================================================================================
Installing:
 swatch                      3.1.1-1.el5.rf                                rpmforge                              45 k
Installing for dependencies:
 perl-Bit-Vector             6.4-2.2.2.1                                   base                                 182 k
 perl-Carp-Clan              5.3-1.2.1                                     base                                  22 k
 perl-Date-Calc              5.4-1.2.2.1                                   base                                 271 k
 perl-Date-Manip             5.54-2.el5.rf                                 rpmforge                             210 k
 perl-File-Tail              0.99.3-1.2.el5.rf                             rpmforge                              21 k
 perl-Mail-Sendmail          0.79-1.2.el5.rf                               rpmforge                              23 k
 perl-TimeDate               1:1.16-5.el5                                  base                                  32 k

Transaction Summary
================================================================================================================================
Install      8 Package(s)
Update       0 Package(s)
Remove       0 Package(s)

Total download size: 805 k
Is this ok [y/N]: y
```

List of files belonging to Swatch

See the list of files belonging to swatch – it's is very small. See the examples in the examples folder.

```
[root@tycoon ~]# rpm -ql swatch
/usr/bin/swatch
/usr/lib/perl5/vendor_perl/5.8.8/Swatch
/usr/lib/perl5/vendor_perl/5.8.8/Swatch/Actions.pm
/usr/lib/perl5/vendor_perl/5.8.8/Swatch/Throttle.pm
/usr/lib/perl5/vendor_perl/5.8.8/auto/Swatch
/usr/lib/perl5/vendor_perl/5.8.8/auto/Swatch/Actions
/usr/lib/perl5/vendor_perl/5.8.8/auto/Swatch/Actions/autosplit.ix
/usr/share/doc/swatch-3.1.1
/usr/share/doc/swatch-3.1.1/CHANGES
/usr/share/doc/swatch-3.1.1/COPYING
/usr/share/doc/swatch-3.1.1/COPYRIGHT
/usr/share/doc/swatch-3.1.1/KNOWN_BUGS
/usr/share/doc/swatch-3.1.1/README
/usr/share/doc/swatch-3.1.1/examples
/usr/share/doc/swatch-3.1.1/examples/SendMail.pm
/usr/share/doc/swatch-3.1.1/examples/swatchrc.monitor
/usr/share/doc/swatch-3.1.1/examples/swatchrc.personal
/usr/share/doc/swatch-3.1.1/tools
/usr/share/doc/swatch-3.1.1/tools/reswatch
/usr/share/doc/swatch-3.1.1/tools/swatch_oldrc2newrc
/usr/share/man/man1/swatch.1.gz
/usr/share/man/man3/Swatch::Actions.3pm.gz
/usr/share/man/man3/Swatch::Throttle.3pm.gz
```

"Hello World" Swatch Configuration Example

I have used this sample configuration file as a starting point. For the sake of this tutorial, I am watching for the "panic" string.

```
[root@croft swatch]# cat /etc/swatch/swatch.messages.conf
#
# Swatch configuration file for constant monitoring
#

# Bad login attempts
watchfor   /INVALID|REPEATED|INCOMPLETE/
        mail = ivan.buetler@csnc.ch

# System crashes and halts
watchfor   /(panic|halt)/
        echo
        mail = ivan.buetler@csnc.ch

# System reboots
watchfor   /SunOS Release/
        mail = ivan.buetler@csnc.ch

# watch for error
watchfor /error/
         mail = ivan.buetler@csnc.ch

# watch for reboot
watch for /reboot/
        mail = ivan.buetler@csnc.ch
```

Testing your Swatch Example

Test your swatch configuration with "**echo panic >> /var/log/messages**". The configuration matches the string "panic" and prints it on your swatch shell, additionally an e-mail is sent to ivan.buetler@csnc.ch

Start Swatch

```
swatch --config-file=/etc/swatch/swatch.messages.conf --tail-file=/var/log/messages

*** swatch version 3.1.1 (pid:16305) started at Wed Sep 23 11:32:26 CEST 2009
```

Echo "panic" into /var/log/messages

```
echo "this is a test: panic is just a string" >> /var/log/messages
```

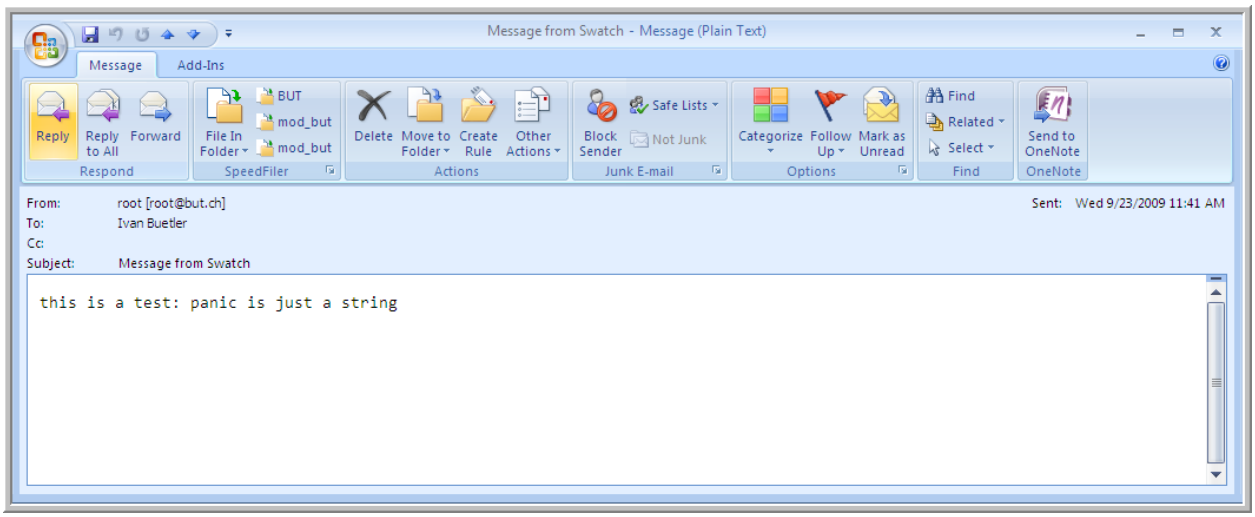
See the pattern match on the screen

```
swatch --config-file=/etc/swatch/swatch.messages.conf --tail-file=/var/log/messages

*** swatch version 3.1.1 (pid:16305) started at Wed Sep 23 11:32:26 CEST 2009

this is a test: panic is just a string
```

If your server is configured with e-mail, an e-mail should be sent to the configured e-mail address. In my case to ivan.buetler@csnc.ch



Run Swatch in Daemon Mode

If everything works as expected, remove the "echo" command from your swatch configuration and use swatch in daemon mode.

```
swatch --config-file=/etc/swatch/swatch.messages.conf \
--tail-file=/var/log/messages  --daemon
```

Needless to say you can start swatch automatically after a reboot and make sure swatch runs with a low privileged user that has read access to your log files.

Thank You for reading this tutorial

Ivan Bütler, E1
Compass Security AG

ivan.buetler@csnc.ch

References & Links

- Swatch Info: http://sial.org/howto/logging/swatch/
- Syslog-NG Watch: http://sial.org/howto/logging/sec.pl/
- Linux Journal Swatch Article: http://www.linuxjournal.com/article/4776