Installation swatch

Simple watch daemon

19th of October 2000

Document name:	Installation swatch-V1.0.pdf
Version:	V 1.0
Author:	Ivan Buetler, Compass Security AG
	ivan.buetler@csnc.ch
	http://www.csnc.ch/
References:	README swatch
Date of delivery:	19th of October 2000
Document state:	PUBLIC

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

CONTENT

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

Date: Okt 19, 2000

1 Installation

1.1 Introduction

swatch (simple watch daemon) is a very good tool to monitor log files in general. As far as you recognize unused log-entires, you have the half mile in being informed about malicous events. Swatch bases on perl.

1.2 Version control

Version	Author	Description	Filename
1.0	Ivan Buetler ivan.buetler@csnc.ch	Initial version saved on http://www.csnc.ch/download/	Installation-swatch-V1.0.pdf

[Ivan] If you feel like having something you would like to see in this document, pls. Let me know. I will leave the version control chapter in the future. So everybody can see who did what on this document.

1.3 Download source

Download swatch from:

ftp.stanford.edu/general/security-tools/swatch

1.4 Software requirements

Swatch needs

- perl
- perl module Date-Calc
- perl module Tail
- perl module Time-HiRes

If perl and these perl modules are not installed, swatch will not run. On the otherside, the distribution does not need to be compiled 8-).

1.5 Copy the source to /opt/download

Compass recommends to copy or move all sources to the /opt/download directory. After the sucessfull compilation and installation, the sources goes to /opt/installed directory. If the Solaris

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

Administrator wants to check weither a package is already installed or not, he can use the traditional pkginfo (Solaris packages) and the list of /opt/installed to check versions of installed packages.

1.6 Unpack the source

gzip -d swatch.tar.gz
tar –xvf swatch.tar

This will untar the sources into /opt/download/swatch directory

1.7 Installation of swatch

- perl Makefile.PL
- make
- make test
- make install

1.8 Swatch configuration

Swatch bases on a configuration file, which needs to be adapted for your needs. Within the config-files, you can define patterns recognized by swatch.

Example:

```
#
# Personal Swatch configuration file
#
# Alert me of bad login attempts and find out who is on that system
#================================================================
watchfor = /INVALID|REPEATED|INCOMPLETE/
        echo=inverse
        mail=root

# Important program errors
#================================================================
watchfor = /LOGIN/
        echo=inverse
        mail=root
watchfor = /passwd/
        echo=bold
        mail=root
watchfor = /ruserok/
        echo=bold
        mail=root

# Ignore this stuff
#================================================================
ignore = /nntp/,/xntp|ntpd/,/faxspooler/,/XSTATS/,/NSTATS/,/AXFR/

# Report unusual tftp info
#================================================================
ignore = /tftpd.*(ncd|kfps|normal exit)/
watchfor = /tftpd/
```

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

```
        echo
        mail=root

# Kernel problems
#====================================================================
watchfor = /(panic|halt|SunOS Release)/
        echo=bold
        mail=root
watchfor = /file system full/
        echo=bold
        mail=root
ignore = /vmunix.*(at|on)/
watchfor = /vmunix/
        echo
        mail=root

watchfor = /fingerd.*(root|[Tt]ip|guest)/
        echo
        mail=root

watchfor = /su:/
        echo=bold
        mail=root

#====================================================================
#watchfor = /.*/
#       echo
#       mail=root

# Ivan Watch Rules
#====================================================================
watchfor = /(Connection from)/
        mail=root
watchfor = /bad username/
        mail=root
watchfor = /REFUSED/
        mail=root
watchfor = /unapproved AXFR/
        mail=root
watchfor = /fatal/
        mail=root
watchfor = /(sshd2[170])/
        mail=root
watchfor = /(coming from)/
        mail=root
watchfor = /REPEATED LOGIN FAILURES/
        mail=root
```

In the example above, the e-mail to root is the action after a pattern matches. You can also define other actions or having self-written scripts behind specific actions. Read the manual for further and advanced swatch usage.

1.9 Clean-up Installation

Compass recommends to tar the already running distribution and move it to /opt/installed directory.

cd /opt/download/swatch
tar –cvpf swatch-compiled.tar *
mv ./swatch-compiled.tar /opt/installed

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

2 Appendix

2.1 README

corro:swatch-3.0b2# more README

Thank you for your interest in swatch: the Simple WATCHdog.

Swatch was originally written to actively monitor messages as
they are written to a log file via the UNIX syslog utility. For
a simple demonstration type "perl swatch --examine=FILENAME" with
FILENAME being the file that you would like to see the contents of.
All this example will do is demonstrate the different text modes
that are available with to the echo action.

Read the INSTALL file for installation instructions.

This is a beta release of version 3.0, so please use it with caution.
The code is still slightly ahead of the documentation.

IF YOU ENCOUNTER A BUG...

Please send mail to eta@engr.ucsb.edu about it, but first make
sure that it is not mentioned in the KNOWN_BUGS file and that you are
using the latest release.

You my want to try the latest snapshot which is named swatch.<DATE>.tar and
will be updated very frequently. This will be located in the NEW directory
at the FTP site.

MAJOR CHANGES

The configuration file now has a completely different format. You can still
use your old configuration files if you use the "--old-style-config" switch
if you insist.

I have re-written most a lot of the code to take advantage of features
and modules that were made available with perl 5.

It now requires perl 5 and the following modules: Time::HiRes, Date::Calc, and
File::Tail.

It now uses the File::Tail module instead of the unix tail(1) command to
actively monitor a file.

I have added the seven colors that color xterminals recognize to the echo
action.

The manual is now embedded into the script in POD format.

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

I have eliminated the use of swatch specific perl libraries.

SUGGESTIONS?

Please mail them to Todd.Atkins@Alumni.Stanford.ORG

2.2 INSTALL

corro:swatch-3.0b2# cat INSTALL
To install, simply issue the following commands:

```
perl Makefile.PL
make
make test
make install
make realclean
```

Swatch installs just like a CPAN module. If you are not familiar with this process then you may want to read about it by issuing the command:

```
man ExtUtils::MakeMaker
```

Use the "perldoc" command if your "man" cannot find the document.

2.3 Directory listing

The following directory listing shows you all sources to successfully compile swatch and have it up and running (perl is installed)

```
drwxr-xr-x   6 root     other        512 Sep  5 23:21 .
drwxr-xr-x   9 root     other        512 Sep 13 20:59 ..
drwxr-xr-x   6 root     root        1024 Sep  5 23:12 Date-Calc-4.3
-rw-------   1 root     root      481280 Jan 24  2000 Date-Calc-4.3.tar
drwxrwxrwx   3 root     root         512 Sep  5 23:13 Tail-0.60
-rw-------   1 root     root       19968 Jan 24  2000 Tail-0.60.tar
drwxr-xr-x   4 root     root         512 Sep  5 23:13 Time-HiRes-01.20
-rw-------   1 root     root       40960 Jan 24  2000 Time-HiRes-01.20.tar
drwxr-xr-x   4 root     root         512 Jun 25  1999 swatch-3.0b2
-rw-------   1 root     root       71680 Jan 24  2000 swatch-3_0b2.tar
-rw-r--r--   1 root     root      133120 Sep  5 22:38 swatch-all-includes.tar
-rw-r--r--   1 root     other       2155 Sep  5 23:16 swatch.rc
```

the file „swatch-all-includes.tar“ stores all required files.

2.4 PERL installation

Please install perl with the ordinary pkgadd command.

```
cd /opt/download/pkg; pkgadd –d ./perl-5.005_03-sol26-sparc-local
```

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch