

How to Install Swatch

- OVERVIEW2**
- INSTALL SWATCH.....2**
- CUSTOMIZE SWATCH WITH VDOPS MODS3**
 - DROP ROOT PRIVILEGES3
 - REAP CHILDREN4
 - DELIVER MAIL IMMEDIATELY4
 - CORRECT MAN PAGE.....5
- CREATE THE CONFIG FILE.....6**
- CREATE THE INIT.D SCRIPT6**
- INSTALL SUPPORTING CODE.....7**
- TEST8**
 - LOAD SWATCH.....8
 - VERIFY THAT SWATCH IS WORKING8
- MAINTAIN.....9**
 - CRON JOBS9
- WEB PAGE.....9**
 - VIRTUAL HOST9
 - WEB DIRECTORY10
 - RESTART APACHE10
 - TEST10

OVERVIEW

This document describes how to install Swatch on loghost.

Review the documentation at <http://swatch.widgets.com> for an overview of how swatch works.

INSTALL SWATCH

```
jurbanite> sudo su tocops
[...]
jurbanite> cd /opt/vdops/src/centos-5
jurbanite> tar xvfz /opt/vdops/archive/swatch-3.2.2.tar.gz
[...]
jurbanite> cd swatch-3.2.2
jurbanite> sudo su netops
jurbanite> perl Makefile.PL
Writing Makefile for swatch
jurbanite>
```

If 'perl Makefile.PL' complains about missing Perl modules, install them.

```
jurbanite> cpan
CPAN: File::HomeDir loaded ok (v0.69)

cpan shell -- CPAN exploration and modules installation (v1.9205)
ReadLine support enabled

cpan[1]> install Date::Calc Date::Parse File::Tail Time::HiRes
[...]
cpan[2]> quit
jurbanite>
jurbanite> make
cp swatch blib/script/swatch
/opt/vdops/bin/perl "-MExtUtils::MY" -e "MY->fixin(shift)" blib/script/swatch
Manifesting blib/man1/swatch.1
Manifesting blib/man3/Swatch::Threshold.3
Manifesting blib/man3/Swatch::Throttle.3
Manifesting blib/man3/Swatch::Actions.3
jurbanite> make test
PERL_DL_NONLAZY=1 /opt/vdops/bin/perl "-MExtUtils::Command::MM" "-e" "test_harness(0, 'blib/lib', 'blib/arch')" t/*.t
t/01cpan_modules.....ok
All tests successful.
Files=1, Tests=1, 0 wallclock secs ( 0.01 usr 0.01 sys + 0.06 cusr 0.01 csys = 0.09 CPU)
Result: PASS
jurbanite> make install
Writing /opt/vdops/lib/perl5/site_perl/5.8.8/i686-linux-thread-multi/auto/swatch/.packlist
Appending installation info to /opt/vdops/lib/perl5/5.8.8/i686-linux-thread-multi/perllocal.pod
jurbanite>
```

At this point, the 'swatch' Perl script is still sitting in ./swatch-3.2.2; now, you manually copy it into position:

```
jurbanite> cp swatch /opt/vdops/script/swatch
jurbanite> chmod 555 /opt/vdops/script/swatch
```

Also, copy 'silence-swatch' from an existing installation to /opt/vdops/script

```
cp ~/silence-swatch /opt/vdops/script
chmod 755 /opt/vdops/script/silence-swatch
chown tocops:netops /opt/vdops/script/silence-swatch
```

CUSTOMIZE SWATCH WITH VDOPS MODS

Drop Root Privileges

Make the first few pages look as follows. This change tells swatch to check to see if it is running as 'root' and if so to drop privileges to those of 'tocops'. In theory, no one should be loading swatch as root ... but this change fixes that problem, just in case someone forgets.

```
#!/opt/vdops/bin/perl

eval 'exec /opt/vdops/bin/perl -S $0 ${1+"$@"}'
    if 0; # not running under some shell
#####
# I hacked this section in --sk 4-28-2006
#####
use Sys::Syslog;

# Change UID
change_uid('tocops');

#####
# Change owner uid if necessary
#####
sub change_uid {
    my $owner = shift;
    my $name;
    my $gid;
    my $uid;

    # Find UID of owner
    $uid = getpwnam($owner);

    # Change UID if necessary
    if ($uid == $UID) {
        # Do nothing;
    }
    else {
        log_it("Changing uid from $UID to $uid");
        ($UID, $EUID) = ($uid, $uid);
        unless ($uid == $UID) {
            log_it("Failed to change uid");
            die "$PROGRAM_NAME must run as $owner, bailing";
        }
        chdir;
    }

    return 1;
}
}
```

```
#####
# Send messages to syslog
#####
sub log_it {
    my $msg = shift;
    my $username = getpwuid ($<);
    my $ident = "$0 by $username";
    my $facility = "local5";
    my $level = "info";

    # Do the work
    openlog ($ident, '', $facility);
    syslog ($level, $msg);
    closelog ();

    return 1;
}

#####
# End of SK hack
#####
```

Reap Children

And then, around line 130, make the following change. This tells swatch to kill off any children it produces, after a decent interval -- prevents the accumulation of zombies. Not strictly necessary, as the zombies generally aren't malicious. But it keeps the process table from filling up with junk.

Change

```
$SIG{'CHLD'} = 'IGNORE';
```

To

```
$SIG{'CHLD'} = 'DEFAULT';
```

Deliver Mail Immediately

Normally, when one employs the 'mail' verb in swatch emit e-mail, swatch dumps the resulting message into sendmail's queue, for delivery whenever sendmail gets around to it. We want swatch to send the message immediately.

```
cd /opt/vdops/lib/perl5/site_perl/5.8.8/Swatch
cp Actions.pm Actions.pm.ori
```

Edit Actions.pm. Around line 143, change the '-odq' to '-odb', i.e. change the 'q' to an 'b'. [This tells sendmail to deliver the mail immediately, rather than dumping it into a queue for later delivery.]

Change

```
if (! $args{'MAILER'} ) {
    foreach my $mailer (qw(/usr/lib/sendmail /usr/sbin/sendmail)) {
        $args{'MAILER'} = $mailer if ( -x $mailer );
    }
    if ($args{'MAILER'} ne '') {
        $args{'MAILER'} .= ' -oi -t -odq';
    }
}
```

To

```
if (! $args{'MAILER'} ) {
    foreach my $mailer (qw(/usr/lib/sendmail /usr/sbin/sendmail)) {
        $args{'MAILER'} = $mailer if ( -x $mailer );
    }
    if ($args{'MAILER'} ne '') {
        $args{'MAILER'} .= ' -oi -t -odb';
    }
}
```

Correct man page

Replace

Perform action(s) on each match for up to B<count> matches during the time interval specified by B<seconds>

with

Perform action(s) after each B<count> number of matches during the time interval specified by B<seconds>

Find the following section and remove the “=begin text” and “=end text” lines.

```
=head1 CONFIGURATION EXAMPLE
```

```
=begin text
```

```
perlcode my $fsf_regex = '\d{2}:\d{2}:\d{2}\s+(.* file system full)';
```

```
watchfor /$fsf_regex/
```

```
    threshold track_by=$1,type=limit,count=1,seconds=60
```

```
    echo
```

```
bell
```

```
=end text
```

CREATE THE CONFIG FILE

Grab a copy of the existing swatch.conf from its home and place it in the tocops home directory.

```
jurbanite> mkdir /opt/vdops/etc/swatch/backup
jurbanite> chown tocops:vdops /opt/vdops/etc/swatch
jurbanite> mkdir /opt/vdops/etc/swatch/
jurbanite> chmod 775 /opt/vdops/etc/swatch
jurbanite> cp ~/swatch.conf /opt/vdops/etc/swatch
```

CREATE THE INIT.D SCRIPT

Put this file into /etc/init.d and give ownership to 'tocops'.

```
jurbanite# cp /somewhere/swatch.init.script /etc/init.d/swatch
jurbanite# chown tocops:vdops /etc/init.d/swatch
jurbanite# chmod 755 /etc/init.d/swatch
jurbanite# chkconfig --add swatch
```

Here is 'swatch.init.script'.

```
#!/bin/bash
#
# swatch          Starts swatchd/klogd.
#
#
# chkconfig: 2345 12 88
# description: $prog is an network monitoring program
### BEGIN INIT INFO
# Provides: $swatch
### END INIT INFO

# Source function library.
. /etc/init.d/functions

# Check for missing binaries (stale symlinks should not happen)
SWATCH_BIN=/opt/vdops/script/swatch
test -x $SWATCH_BIN || exit 5

# Check for existence of needed config file
SWATCH_CONFIG=/opt/vdops/etc/swatch/swatch.conf
test -r $SWATCH_CONFIG || exit 6

# Watch syslog
FILE=/loghost/log/syslog

# Miscellaneous parameters
PARAM>--awk-field-syntax

RETVAL=0
prog="swatch"

start() {
    echo $"Starting $prog"
    $SWATCH_BIN -c $SWATCH_CONFIG -t $FILE --tail-args -F $PARAM &
    RETVAL=$?
}
```

```

        echo
        return $RETVAL
    }
    stop() {
        echo $"Shutting down $prog"
        killproc $prog
        RETVAL=$?
        echo
        return $RETVAL
    }
    rhstatus() {
        status swatch
    }
    restart() {
        stop
        start
    }
    reload() {
        echo $"$prog does not need reloading"
        echo
    }
    case "$1" in
        start)
            start
            ;;
        stop)
            stop
            ;;
        status)
            rhstatus
            ;;
        restart)
            restart
            ;;
        reload)
            reload
            ;;
        condrestart)
            ;;
        *)
            echo $"Usage: $0 {start|stop|status|restart|condrestart}"
            exit 1
    esac
    exit $?

```

INSTALL SUPPORTING CODE

We employ swatch to send us e-mail and page us when it detects something amiss. Swatch can perform these functions natively. However, in order to acquire additional control over the notification process, those of us who add stanzas to swatch.conf tend to employ the 'page_em' and 'mail_em' scripts as front-ends to pages and e-mails. Copy these scripts to /home/tocops/bin

```

jurbanite> pwd
/home/tocops/bin
jurbanite> ls
mail_em page_em ping-swatch pong-swatch toclogd zero-logs
jurbanite>

```

These scripts rely on the 'Netops Toolkit', a collection of Perl modules, specifically the NetopsData.pm, Swatch.pm, and Utilities.pm modules.

```
jurbanite> pwd
/opt/vdops/lib/perl5/site_perl/FHCRC/Netops
jurbanite> ls
APCTools.pm      IFTools.pm      NetopsTools.pm  SwatchOps.pm
CiscoTools.pm   MRTGTools.pm   PingTools.pm    Utilities.pm
HostTools.pm    NetopsData.pm  SNMPTools.pm
jurbanite>
```

They also rely on numerous Perl modules. 'cpan' is your friend; use it to install each module, until a 'perl -c /home/tocops/bin/page_em' results in an 'ok' message. Remember to run 'cpan' as the user 'netops', not as yourself or as any other user.

```
jurbanite> pwd
/home/tocops/bin
jurbanite> perl -c page_em
page_em syntax OK
jurbanite>
```

TEST

Load swatch

```
jurbanite> sudo su tocops
[...]
jurbanite> /etc/init.d/swatch start
Starting swatch

jurbanite>
*** swatch version 3.2.2 (pid:23292) started at Mon Feb 18 16:32:11 PST 2008
```

If swatch.conf contains syntax errors, this will show up here.

Verify that swatch is working

```
jurbanite> /home/tocops/bin/ping-swatch -s yes
Starting /home/tocops/bin/ping-swatch v1.5.2
Swatch is alive
Ending /home/tocops/bin/ping-swatch v1.5.2
jurbanite>
```

Verify that 'silence-swatch' works.

MAINTAIN

Cron Jobs

Create the following crontab as user 'tocops'

```
jurbanite> crontab -e
```

```
# Minute Hour    Day/mo  Month   Day/wk  Command
25,55   *        *       *       *       $HOME/bin/ping-swatch -s yes > /dev/null 2&1
1       0        *       *       *       $HOME/bin/zero-logs
0       */2     *       *       *       $HOME/bin/build-past-log-html
```

The ping-swatch program exercises swatch by logging a test message to syslog, which swatch should pick-up using the following section in swatch.conf

```
#####
# Spawn pong-swatch if ping-swatch sends us a ping
#####
watchfor=/Pinging swatch: are you there/
exec=/home/tocops/bin/pong-swatch
```

If pong-swatch doesn't run, ping-swatch detects this ... and tries stopping and restarting swatch and then repeating the test. If pong-swatch still hasn't responded, then ping-swatch pages 'duty' (unless it is running interactively, in which case it just whines to you.)

WEB PAGE

Virtual Host

```
[skendric@jurbanite html]$ sudo su netops
```

Create the virtual host

```
[skendric@jurbanite html]$ vi /etc/httpd/conf.d/vdops.conf
```

And add these lines

```
# Swatch

<VirtualHost 10.1.2.3:80>
    DocumentRoot "/var/www/html/swatch/"
    ServerName swatch.widgets.com
    ServerAlias swatch
    ServerAdmin operators@widgets.com
    <Directory /var/www/html/swatch/>
        Options FollowSymLinks Includes Indexes
        AllowOverride None
        Order deny,allow
        Deny from all
        Allow from 10.2.0.0/16
        Allow from 10.204.0.0/16
        Allow from 10.205.0.0/16
```

```
</Directory>
</VirtualHost>
```

Web Directory

Create the web directory:

```
[jurbanite swatch]$ mkdir /var/www/html/swatch
```

Copy index.html and swatch.txt to the new directory and make a symbolic link for swatch.conf

```
[skendric@jurbanite swatch]$ ln -s /opt/vdops/etc/swatch/swatch.conf
swatch.conf
```

```
[skendric@jurbanite swatch]$ pwd
/var/www/html/swatch
[skendric@jurbanite swatch]$ ls
total 68
drwxr-xr-x 2 netops vdops 4096 Nov  7 11:34 ./
drwxr-xr-x 6 root   root 4096 Sep 26 08:19 ../
-rw-r--r-- 1 netops vdops 10126 Nov  7 11:34 index.html
-rw-r--r-- 1 netops vdops 10594 Nov  7 11:17 index.html.bak
lrwxrwxrwx 1 netops vdops   33 Nov  7 11:21 swatch.conf ->
/opt/vdops/etc/swatch/swatch.conf
-rw-r--r-- 1 netops vdops 11299 Nov  7 11:19 swatch.txt
[skendric@jurbanite swatch]$
```

Restart apache

```
[skendric@jurbanite html]$ sudo /etc/init.d/httpd graceful
```

Test

Point a web browser to your site (i.e. <http://swatch.widgets.com>) and verify that all links are working.