

Configuring SWATCH

On AUTH1

1. Create the configuration file for swatch:

- Edit /usr/local/etc/swatch.conf -- use TAB and not SPACE for the lines below "watchfor"!

```
$ sudo vi /usr/local/etc/swatch.conf
```

```
- - - - - cut below - - - - -
```

```
watchfor /client ([0-9A-F.:]+)\D\d+ \((\S+)\): zone transfer '(.*)\IN' denied/  
mail=sysadm,subject=Zone AXFR denied for $3 from $1  
threshold type=limit,count=1,seconds=600
```

```
- - - - - cut above - - - - -
```

2. Enable the mail server

- Add to /etc/rc.conf

```
postfix_enable="YES"
```

- Then run the following commands

```
$ sudo newaliases
```

```
$ sudo service postfix start
```

3. Try sending mail to yourself

- Now send yourself an email:

```
$ echo hello | mail sysadm@auth1.grpX.dns.nsrc.org
```

... don't forget to replace X above with the number of your group.

- See if the mail has arrived:

```
$ mutt -f /var/mail/sysadm
```

(answer Yes if you are asked to create the folder for the mail)

4. Start swatch:

- This must be done as root, remember to use sudo:

```
$ sudo -s
```

```
# swatch -c /usr/local/etc/swatch.conf --tail-file=/etc/namedb/log/  
general --daemon
```

```
# exit
```

```
$ ps auxww | grep swatch
```

- You should see a line like the following:

```
root 58811 0.0 0.0 11500 2124 5 RJ 11:41AM 0:00.02 /usr/local/bin/  
perl /usr/local/bin/swatch -c /usr/local/etc/swatch.conf --tail-file=/etc/namedb/  
log/general --daemon
```

7. Ask another group to perform a zone transfer of your zone:

From their machine:

```
# dig @auth1.grpX.dns.nsrc.org YOURTLD axfr                (where X is  
YOUR group)
```

Q: do they get a copy of your zone ?

Q: do you get an email about it ?

8. Check that mails are coming in:

```
# mutt -f /var/mail/sysadm
```

Note the information contained in the message.