Syslog/SWATCH exercises
AfNOG 11, Kigali

Syslog-ng and swatch already installed on the workshop machines, otherwise install with:

apt-get install syslog-ng swatch

Choose your router:

PC1-10: 196.200.218.249
PC11-20: 196.200.218.250
PC21-28: 196.200.218.251
PC29-36: 196.200.218.252
PC37-44: 196.200.218.253

1. Make Syslog-NG on your machine listen to packets from the router. Edit /etc/syslog-ng/syslog-ng.conf. Find the lines:
   ```
   # (this is equivalent to the "-r" syslogd flag)
   # udp();
   ```
   and change it to:
   ```
   # (this is equivalent to the "-r" syslogd flag)
   udp();
   ```
2. Add a rule to filter everything in facility local5, and create one file per router per hour. Edit the same file, and copy+paste the following at the bottom of the file:
   ```
   filter f_routers
   {
     facility(local5);
   };
   log
   {
     source(s_all);
     filter(f_routers);
     destination(routers);
   };
   destination routers {     file("/var/log/network/$YEAR/
   $MONTH/$DAY/$HOST-$YEAR-$MONTH-$DAY-$HOUR.log"
     owner(root)
     group(root)
     perm(0644)
     dir_perm(0755)
     create_dirs(yes)
   ```

```
  template("$YEAR $DATE $HOST $MSG\n"));
};
```

3. Create the directory /var/log/network/
   `sudo mkdir /var/log/network/`
4. Restart syslog-ng:
   `sudo /etc/init.d/syslog-ng restart`
5. We already preconfigured the routers to forward all logs to you via the NOC machine - so you don't need to do anything.

   "At home" you would have to change your router config similar like this:

```
RTRX(config)# logging XXX.XXX.XXX.XXX     (your servers IP)
RTRX(config)# logging facility local5
RTRX(config)# logging userinfo
```

6. Change to the rancid user ('sudo bash' then 'su -s /bin/bash rancid') and use clogin to change something on your router config ('enable','conf t', ..., end, write)
7. On your PC check /var/log/network/2010/05/31/ - logs should start appearing
8. If not log in to the router again, enter config mode and exit, this should generate logs

SWATCH:

1. Edit the SWATCH config file `/etc/swatch.conf`, put in the following:

```
watchfor /PRIV_AUTH_PASS/
  mail=net@noc.mgmt.ws.afnog.org,subject=Enable mode entered
  threshold type=limit,count=1,seconds=3600
watchfor /CONFIG_I/
  mail=net@noc.mgmt.ws.afnog.org,subject=Router config
  threshold type=limit,count=1,seconds=3600
watchfor /LINK-3-UPDOWN/
  mail=net@noc.mgmt.ws.afnog.org,subject=Link state change
  threshold type=limit,count=1,seconds=3600
```

   Please make sure the mail and threshold lines are indented by tabs and not spaces

2. Add a statement to /etc/syslog-ng/syslog-ng.conf to export all router messages to a common file (not very pretty, but it works):

```
destination everything {
  file("/var/log/everything"
  template("$DATE <$FACILITY.$PRIORITY> $HOST $MSG\n")
  template_escape(no)  );
```

```
};
log {
 source(s_all);
 destination(everything);
};
```

3. Restart syslog-ng:
   ```
   sudo /etc/init.d/syslog-ng restart
   ```
4. Start swatch as root:
   ```
   swatch -c /etc/swatch.conf -t /var/log/everything
   ```
5. Login to your router, enter and exit config mode, disable and enable
6. Check that mails are coming in to the RT-mailgate on the NOC machine