

Log management – exercises – GhNog,Cape Coast

Part I

1. Stop the existing syslog daemon:

```
# /etc/rc.d/syslogd stop
```

2. Install syslog-ng:

```
# pkg_add -r ftp://41.218.234.1/packages/All/syslog-ng2-2.0.9_2.tbz  
  
# N.B: Alternatively, you can install using ports as below  
# portinstall -PP syslog-ng
```

You should see this when the package finished installing – read the instructions and perform steps 2 & 3 from the list below:

syslog-ng is now installed! To replace FreeBSD's standard syslogd (/usr/sbin/syslogd), complete these steps:

1. Create a configuration file named /usr/local/etc/syslog-ng/syslog-ng.conf (a sample named syslog-ng.conf.sample has been included)
2. Configure syslog-ng to start automatically by adding the following to /etc/rc.conf:

```
syslog_ng_enable="YES"
```

3. Prevent the standard FreeBSD syslogd from starting automatically by adding a line to the end of your /etc/rc.conf file that reads:

```
syslogd_enable="NO"
```

4. Shut down the standard FreeBSD syslogd:

```
# kill `cat /var/run/syslog.pid`
```

5. Start syslog-ng:

```
/usr/local/etc/rc.d/syslog-ng.sh start
```

3. Create /usr/local/etc/syslog-ng/syslog-ng.conf:

```
# cd /usr/local/etc/syslog-ng  
# cp syslog-ng.conf.sample syslog-ng.conf  
# chmod 644 syslog-ng.conf
```

Edit the newly created file (syslog-ng.conf) and add this at the **end** of the file:

```
log { source(src); filter(f_local7); destination(local7); };  
destination local7 { file("/var/log/local7.log"); };
```

4. Start syslog-ng:

```
# /usr/local/etc/rc.d/syslog-ng start
```

... check that the daemon has started:

```
# ps ax | grep syslog-ng
```

... you should see something like:

```
6054 ?? Is  0:00.00 /usr/local/sbin/syslog-ng -p /var/run/syslog.pid
```

5. Test the syslog service

```
# logger -p local7.info 'this is a test'
```

... control that a file `/var/log/local7.log` now exists:

```
# ls -l /var/log/local7.log
```

... control that you see the test message.

```
# tail /var/log/local7.log
```

6. Ask someone else in the room to send a syslog message to your host, using the '-h' option of the logger command. The **other** person should type this on **their** PC – so for example if you are PC123, and you ask PC125 to send you a message, they will type this:

```
# logger -h pcX.ghe0.dns.gh -p local7.info 'message from pc125'
```

... check that the message appears in **your** `/var/log/local7.log`

Part II

1. Edit `/usr/local/etc/syslog-ng/syslog-ng.conf`, and **change** the line at the bottom:

```
destination local7 { file("/var/log/local7.log"); };
```

to

```
destination local7 {  
  file("/var/log/local7/$YEAR/$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"));  
};
```

2. Create the directory `/var/log/local7/`

```
# mkdir /var/log/local7
```

3. Restart syslog-ng

```
# /usr/local/etc/rc.d/syslog-ng restart
```

4. Repeat steps 5 & 6 from Part I (send a message using logger + get another person to send a message from another machine)

5. See if messages are starting to appear under

```
/var/log/local7/2009/07/XX/...
```