Network Management & Monitoring

Using syslog-ng

Notes:

* Commands preceded with "$" imply that you should execute the command as a general user - not as root.
* Commands preceded with "#" imply that you should be working as root.
* Commands with more specific command lines (e.g. "RTR-GW>" or "mysql>") imply that you are executing commands on remote equipment, or within another program.

Exercises

Please find your classmates that are using the same router as you. Get in to a group and do the following exercise together. That is, pick one person who will log in to your group's router, but all of you should assist with the actual configuration.

1. Configure your virtual routers to send syslog messages to your server:

The routers are able to send syslog messages to multiple destinations, so that 1 router can send messages to 4 or even 5 destinations.
For this exercise, we shall configure the router to send messages to extX,
Your group's PC.

You will SSH to your group's router and do the following:

```
$ ssh cisco@10.10.0.X
rtrX> enable
rtrX# config terminal
```

Enter the command "logging 10.10.0.X0" directing the router to send logs to your PC, extX

```
rtrX# logging 10.10.0.X0

rtrX(config)# logging facility local0
rtrX(config)# logging userinfo
rtrX(config)# exit
rtrX# write memory
```

Now run 'show logging' to see the summary of the logging configuration.

```
rtrX# show logging
```

Logout from the router (exit)

```
rtrX# exit
```

That's it. The router should now be sending UDP SYSLOG packets to your PC on port 514.
To verify this log in on your PC and do the following:

```
          $ sudo -s
          # apt-get install tcpdump               (don't worry if it's already
installed)
          # tcpdump -e -s0 -ni eth0 port 514
```

Then have one person in your group log back in on the router and do the following:

```
          $ ssh cisco@10.10.0.X
          rtrX.ws.nsrc.org> enable
          rtrX.ws.nsrc.org# config terminal
          rtrX.ws.nsrc.org(config)# exit
          rtrX.ws.nsrc.org> exit
```

You should see some output on your PC's screen from TCPDUMP. It should look something like:

```
02:20:24.942289 ca:02:0d:b3:00:08 > 52:54:4a:5e:68:77, ethertype IPv4 (0x0800),
length 144: 10.10.0.6.63515 > 10.10.0.250.514: SYSLOG local0.notice, length: 102
02:20:24.944376 ca:02:0d:b3:00:08 > c4:2c:03:0b:3d:3a, ethertype IPv4 (0x0800),
length 144: 10.10.0.6.53407 > 10.10.0.241.514: SYSLOG local0.notice, length: 102
```

Now you can configure the logging software on your PC to receive this information and log it to a new set of files:

2. Install syslog-ng

These exercises are done as root. If you are not root on your machine then become root by typing:

```
          $ sudo -s

          # apt-get install syslog-ng
```

2. Edit /etc/syslog-ng/syslog-ng.conf

Find the lines:

```
source s_src {
       system();
       internal();
};
```

and change them to:

```
source s_src {
       system();
       internal();
       udp();
};
```

Save the file and exit.

Now, create a config section for our network logs:

```
          # cd /etc/syslog-ng/conf.d/

          # editor 10-network.conf
```

In this file, copy and paste the following:

```
          filter f_routers { facility(local0); };

          log {
                              source(s_src);
                              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"));
          };
```

Save the file and exit.

3. Create the directory /var/log/network/

```
          # mkdir /var/log/network/
```

4. Restart syslog-ng:

```
          # service syslog-ng restart
```

5. Test syslog

To be sure there are some logging messages log back in to the router, and run some "config" commands, then logout. e.g.

```
          # ssh cisco@10.10.0.X
          rtrX> enable
          rtrX# config terminal
          rtrX(config)# exit
          rtrX> exit
```

Be sure you log out of the router. If too many people log in without logging out then others cannot gain access to the router.

6. On your PC, See if messages are starting to appear under
   /var/log/network/2014/.../

```
          $ cd /var/log/network
          $ ls
          $ cd 2014
          $ ls
          ... this will show you the directory for the month
          ... cd into this directory
          $ ls
          ... repeat for the next level (the day of the month)
          $ ls
```

Troubleshooting

If no files are appearing under the /var/log/network directory, then another command to try while logged into the router, in config mode, is to shutdown / no shutdown a Loopback interface, for example:

```
          $ ssh cisco@rtrX

          rtrX> enable
          rtrX# conf t
          rtrX(config)# interface Loopback 999
          rtrX(config-if)# shutdown
```

wait a few seconds

```
          rtrX(config-if)# no shutdown
```

Then exit, and save the config ("write mem"):

```
          rtrX(config-if)# exit
          rtrX(config)# exit
          rtrX# write memory
          rtr1# exit
```

Check the logs under `/var/log/network`

```
          # cd /var/log/network
          # ls
```

...follow the directory trail

Still no logs?

Try the following command to send a test log message locally:

```
          # logger -p local0.info "Hello World\!"
```

If a file has not been created yet under `/var/log/network`, then check your configuration for typos. Don't forget to restart the syslog-ng service each time you change the configuration.

What other commands can you think of that you can run on the router (BE CAREFUL!) that will trigger syslog messages? You could try logging in on the router and typing an incorrect password for "enable".

Be sure that you do an "ls" command in your logging directory to see if a new log file has been created at some point.