Network Management & Monitoring

Log management, part I : Using rsyslog

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

The routers are able to send syslog messages to multiple destinations, so that 1 router can send messages to 4 or even 5 destinations. We therefore need to configure the router to send messages to each of the PCs in the group.

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

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

```
$ ssh cisco@10.10.X.254
rtrX.ws.nsrc.org> enable
rtrX.ws.nsrc.org# config terminal

rtrX.ws.nsrc.org(config)# logging 10.10.X.Y

... where X.Y is the IP of your PC (group + number).

rtrX.ws.nsrc.org(config)# logging facility local5
rtrX.ws.nsrc.org(config)# logging userinfo
rtrX.ws.nsrc.org(config)# exit
rtrX# write memory
```

Now run "show logging" to see the summary of the log configuration.

The other participants in your group will be doing the same thing, so you should not be surprised if you see other destinations as well in the output of "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 bash
# 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.X.254
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 local5.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 local5.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. Configure rsyslog

Edit file /etc/rsyslog.conf and find and un-comment the following lines:

```
#$ModLoad imudp
#$UDPServerRun 514
```

(remove #)

Then comment-out the following change:

```
        $PrivDropToUser syslog
        $PrivDropToGroup syslog
```

(add #)

Then save the file and exit.

Now, create a file named "/etc/rsyslog.d/99-routerlogs.conf, with the following lines:

```
        $template RouterLogs,"/var/log/network/%$YEAR%/%$MONTH%/%$DAY%/%HOSTNAME%-%$HOUR%.log"
        local5.*                -?RouterLogs
```

Save and exit, then:

```
        # mkdir /var/log/network
        # chown syslog /var/log/network
```

4. Restart rsyslog

```
        # service rsyslog restart
```

6. On your PC, See if messages are starting to appear under

```
        /var/log/network/2011/.../
```

7. If not, try to login back into the router, and run some "config" commands,
   then logout. I.E.

```
        # ssh cisco@10.10.X.254
        rtrX.ws.nsrc.org> enable
        rtrX.ws.nsrc.org# config terminal
        rtrX.ws.nsrc.org(config)# exit
        rtrX.ws.nsrc.org> exit
```

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

Other commands to try while you are logged into the router, in config mode:

- shutdown / no shutdown the Loopback interfaces, for example:

```
        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")
```

Check the logs under /var/log/network

Still no logs?

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

```
# logger -p local5.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 rsyslog 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 ?

What about access lists ?

Others ?