Log Management Part 1: Using rsyslog

Network Monitoring & Management

Contents

1 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. "rtrX>" or "mysql>") imply that you are executing commands on remote equipment, or within another program.

2 Exercise

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.

2.1 Configure sending of syslog messages from your group's router

Configure your virtual router to send syslog messages to every server in your group.

Everyone in your group should log into your group's router and do the following (assuming you are already logging in on your virtual machine):

```
$ ssh cisco@rtrX
rtrX> enable
rtrX# config terminal

rtrX(config)# logging 10.10.X.Y

... where X.Y is the IP of your PC (group + number, example pc2 = 10.10.1.2).

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

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

```
rtrX# show logging
```

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" - Press SPACE to page through the output

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 as user sysadm (if you have not already done so) and do the following:

```
$ sudo -s
# apt-get install tcpdump               (if already installed dont worry)
# tcpdump -s0 -nv -i eth0 udp port 514
```

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

```
$ ssh cisco@rtrX
rtrX> enable
rtrX# config terminal
rtrX(config)# exit
rtrX> exit
```

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

```
11:20:24.942289 10.10.1.254.63515 > 10.10.1.1.514: SYSLOG local0.notice, length: 110
11:20:24.944376 10.10.1.254.53407 > 10.10.1.1.514: SYSLOG local0.notice, length: 102
```

When you have seen this, hit Ctrl-C to exit tcpdump.

Aside: to learn more about tcpdump type "man tcpdump" at the command line

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

2.2 Configure rsyslog

Be sure you are logged in to your virtual machine and that you are the root user.

Edit the file /etc/rsyslog.conf:

```
# editor /etc/rsyslog.conf
```

. . . and find and un-comment the following lines (that is, remove the initial '#' only)

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

```
change to:
```

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

Then change this line:

```
$PrivDropToGroup syslog

change to:

$PrivDropToGroup adm
```

Then save the file and exit.

Now, create a file named "/etc/rsyslog.d/30-routerlogs.conf"

```
# editor /etc/rsyslog.d/30-routerlogs.conf
```

... and add the following lines (carefully COPY and PASTE):

```
$template   RouterLogs,"/var/log/network/%$YEAR%/%$MONTH%/%$DAY%/%HOSTNAME%-%$HOUR%.log"
local0.*    -?RouterLogs
& ~
```

PLEASE double check (verify) that what you have pasted is the SAME as what is above. In particular, make sure that you are using TAB and not SPACE between "template" and "RouterLogs", and also between "local0.*" and "-?RouterLogs".

If the above is not pasted correctly, it will NOT work.

Save and exit, then do:

```
# mkdir /var/log/network
# chown syslog:adm /var/log/network
# chmod g+w /var/log/network
```

Restart rsyslog:

```
# service rsyslog restart
```

2.3 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@rtrX
rtrX> enable
rtrX# config terminal
rtrX(config)# exit
rtrX> 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.

On your PC, See if messages are starting to appear under `/var/log/network/<year>/<month>/<day>/`

```
$ cd /var/log/network
$ ls
$ cd 2013
$ 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
```

Then use 'tail' to look at the log file(s) in this directory. The names are dynamic based on the sender and the host, so use the file that you see. It may be something like this:

```
$ ls
rtr8-16.log
$ tail rtr8-16.log
... logging messages are shown ...
```

2.4 Troubleshooting rsyslog

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 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? 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.