

Log management: Using syslog-ng

Introduction

Goals

- Learn how to use syslog-ng to manage logs.

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.

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.

Configure your virtual routers to send syslog messages to your DB 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. We therefore need to configure the router to send messages to each of the PCs in the group.

Configure routers below to send logs to db.campusY.ws.nsrc.org (100.28.Y.130)

- bdr1.campusY.ws.nsrc.org
- core1.campusY.ws.nsrc.org
- dist1-b1.campusY.ws.nsrc.org
- dist1-b2.campusY.ws.nsrc.org

You will SSH to your group’s routers and do the following:

```
$ ssh nmmlab@bdr1.campusY.ws.nsrc.org
bdr1.campusY> enable
bdr1.campusY# config terminal
```

Repeat the next command “logging 100.68.Y.130” for each routers in your campus group.

```
logging 100.68.6.130 logging facility local0 logging userinfo
```

```
bdr1.campusY(config)# logging 100.68.Y.130
bdr1.campusY(config)# logging facility local0
bdr1.campusY(config)# logging userinfo
bdr1.campusY(config)# exit
bdr1.campusY# write memory
```

Now run ‘show logging’ to see the summary of the logging configuration.

```
bdr1.campusY# show logging
```

Logout from the router (exit)

```
bdr1.campusY# exit
```

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

Connect to the server vtp-cndo using the class password. Like this:

```
ssh ubuntu@vtp-cndo.ws.nsrc.org
```

Once connected do:

```
$ lxc exec db-campusY /bin/bash
```

Once access into db-campusY, run the following command.

```
# apt-get install tcpdump          (don't worry if it's already installed)
# tcpdump -s0 -nv -i eth0 port 514
```

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

```
$ ssh nmmlab@bdr1.campusY.ws.nsrc.org
bdr1.campusY> enable
bdr1.campusY# config terminal
(config)# exit
bdr1.campusY> exit
```

You should see some output on your DB Server’s screen from TCPDUMP. It should look something like:

```
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
14:05:02.620767 IP (tos 0x0, ttl 254, id 43, offset 0, flags [none], proto UDP (17), length
    100.68.6.1.62222 > 100.68.6.130.514: [udp sum ok] SYSLOG, length: 187
    Facility local0 (16), Severity notice (5)
```

```
Msg: 466: Feb 22 14:05:01.545: %SSH-5-SSH2_USERAUTH: User 'nmmlab' authentication fo
```

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

Install syslog-ng

SSH into your DB Server

```
$ ssh sysadm@db.campusY.ws.nsrc.org
```

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 syslog-ng-core
```

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

```
# nano /etc/syslog-ng/syslog-ng.conf
```

Find the lines:

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

Add “udp();” and it will look like below:

```
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/
# nano 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.

Create the directory `/var/log/network/`

```
# mkdir -p /var/log/network/
```

Restart syslog-ng:

```
# systemctl restart syslog-ng
```

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 nmmlab@bdr1.campusY.ws.nsrc.org
bdr1.campusY> enable
bdr1.campusY# config terminal
bdr1.campusY(config)# exit
bdr1.campusY> 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.

On your DB Server, See if messages are starting to appear under `/var/log/network/2017/...`

```

# cd /var/log/network
# ls
2017

```

```
# cd 2017
# ls
02 03
```

... above will show you the directory for the month

```
# cd 02
# ls
22 23
```

... above will show you the day of the month

```
# cd 23
# ls
100.68.6.1-2017-02-22-14.log
```

... above will show you the router's

You can view the resulting log file by using a pager program such as less, more, cat, etc...

You will see the logging is capture like below;

```
# less 100.68.6.1-2017-02-22-14.log
```

```
2017 Feb 22 14:11:04 100.68.6.1 %SYS-5-CONFIG_I: Configured from console by nmmlab on vty0
2017 Feb 22 14:11:05 100.68.6.1 %SSH-5-SSH2_CLOSE: SSH2 Session from 100.64.0.241 (tty = 0)
2017 Feb 22 14:12:24 100.68.6.1 %SSH-5-SSH2_SESSION: SSH2 Session request from 100.68.2.135
2017 Feb 22 14:12:24 100.68.6.1 %SSH-5-SSH2_CLOSE: SSH2 Session from 100.68.2.135 (tty = 0)
```

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 nmmlab@bdr1.campusY.ws.nsrc.org
```

```
bdr1.campusY> enable
bdr1.campusY# conf t
bdr1.campusY(config)# interface Loopback 999
bdr1.campusY(config-if)# shutdown
```

wait a few seconds

```
bdr1.campusY(config-if)# no shutdown
```

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

```
bdr1.campusY(config-if)# exit
bdr1.campusY(config)# exit
bdr1.campusY# write memory
bdr1.campusY# 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.