Configuring rsyslog

Network Monitoring & Management

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.

Exercise

You are going to work with your classmates to aggregate all the logs from your campus devices onto your srv1 VM, so you can view them centrally.

Configure your routers to send syslog messages to your shared server (srv1):

Configure each of the network devices below to send logs to srv1.campusY.ws.nsrc.org (100.68.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 can divide up this work between yourselves. Login to each of these devices and do the following:

```
$ ssh nmmlab@bdr1.campusY.ws.nsrc.org   # for example
bdr1.campusY> enable
bdr1.campusY# config terminal
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 network devices should now be sending UDP SYSLOG packets to your shared server (srv1) on port 514. To verify this log in on your shared server:

```
$ ssh sysadm@srv1.campusY.ws.nsrc.org
```

and do the following:

```
sudo -s
# apt install tcpdump        (don't worry if it's already
installed)
# tcpdump -s0 -nv -i ens3 port 514
```

Then have one person in your group log back in on one of the network devices to make it generate some logs:

```
$ 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 shared server's (srv1) screen from TCPDUMP. It should look something like:

```
tcpdump: listening on ens3, 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 215)
    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 for SSH2 Session from 100.64.1.123
(tty = 2) using crypto cipher 'aes128-cbc', hmac 'hmac-sha1'
Succeeded
```

Now you can configure the logging software on your shared server (srv1) to receive this information and log it to a new set of files.

Configure rsyslog

One person needs to SSH into your shared server (srv1)

```
$ ssh sysadm@srv1.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
#
```

Edit the file /etc/rsyslog.conf:

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

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

```
#module(load="imudp")
#input(type="imudp" port="514")
```

change to:

```
module(load="imudp")
input(type="imudp" port="514")
```

and underneath those lines add:

```
module(load="pmciscoios")
$RulesetParser rsyslog.ciscoios
$RulesetParser rsyslog.rfc5424
$RulesetParser rsyslog.rfc3164
```

(this replaces the ruleset parser chain (https://www.rsyslog.com/doc/v8-stable/configuration/ruleset/rsconf1_rulesetparser.html) to allow rsyslog to parse messages in Cisco IOS's proprietary format)

Aside: you may find some systems have a slightly different config:

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

That’s fine - you can uncomment those instead.

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(name="RouterLogs" type="list") {
  constant(value="/var/log/network/")
  property(name="$year")
  constant(value="/")
  property(name="$month")
  constant(value="/")
  property(name="$day")
  constant(value="/")
  property(name="hostname" securepath="replace")
  constant(value="-")
  property(name="$hour")
  constant(value=".log")
}

local0.*  action(type="omfile" dynafile="RouterLogs")
& stop
```

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

Save and exit, then do the following to create the log directory:

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

Restart rsyslog:

```
# systemctl restart rsyslog
```

Check for any errors:

```
# journalctl -eu rsyslog
```

If there are errors in your configuration files, rsyslog won’t be able to start. Correct them before continuing.

Test syslog

To be sure there are some logging messages log back in to any of your campus devices, and run some “config” commands, then logout. e.g.

```
$ ssh nmmlab@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 host, See if messages are starting to appear under `/var/log/network/<year>/<month>/<day>/`

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

Then use ‘tail’ to look at the log file(s) in this directory. The names are dynamic based on the sent hostname and the hour of the time, so use the file that you see. It may be something like this:

```
$ ls
gi0-1.bdr1.campus1.ws.nsrc.org-16.log

$ tail gi0-1.bdr1.campus1.ws.nsrc.org-16.log
... logging messages are shown ...
```

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 nmmlab@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.

Optional: upgrading to latest rsyslog

This section is for reference only.

The version of rsyslog in Ubuntu 22.04+ is fine for production use.

If you are running an older version of Ubuntu, or if you need the very latest rsyslog features, you can replace the Ubuntu version of rsyslog with the one from the Adiscon stable PPA, which is updated frequently:

```
add-apt-repository ppa:adiscon/v8-stable
apt-get install rsyslog
```

However, installing this package may remove the file `/usr/lib/tmpfiles.d/00rsyslog.conf`. If you find it doesn't exist, then recreate it with the following contents:

```
# Override systemd's default tmpfiles.d/var.conf to make
/var/log writable by
# the syslog group, so that rsyslog can run as user.
# See tmpfiles.d(5) for details.

# Type Path    Mode UID  GID  Age Argument
z /var/log 0775 root syslog -
z /var/log/auth.log 0640 syslog adm -
z /var/log/mail.err 0640 syslog adm -
z /var/log/mail.log 0640 syslog adm -
z /var/log/kern.log 0640 syslog adm -
z /var/log/syslog 0640 syslog adm -
d /var/spool/rsyslog 0700 syslog adm -
```

If you don't do this, then on bootup the permissions on the `/var/log` directory will be set incorrectly, and rsyslog won't be able to create files (https://lists.archive.carbon60.com/rsyslog/users/24511).

To check, reboot then use `ls -ld /var/log` to check permissions on the directory:

```
$ ls -ld /var/log
drwxr-xr-x 1 root syslog .....
^^^^^^^^^^ WRONG

drwxrwxr-x 1 root syslog .....
^^^^^^^^^^ RIGHT
```