

Central Logging

One thing that can make your life easier, in case something unexpected happens, is to have logs. I have decided to use my `control01` node as a central logging server using `rsyslog`.

On logging server

Create folder where we store the logs:

```
# as root
mkdir /var/log/central
```

`Rsyslog` will use TCP/UDP port 514, but you need to enable it. Edit `/etc/rsyslog.conf`, and make sure these lines look like this (uncommented):

```
# provides UDP syslog reception
module(load="imudp")
input(type="imudp" port="514")

# provides TCP syslog reception
module(load="imtcp")
input(type="imtcp" port="514")
```

Next create config to tell `rsyslog` to put all logs in previously created folder, create `/etc/rsyslog.d/central.conf`

```
$template RemoteLogs, "/var/log/central/%HOSTNAME%.log"
*,* ?RemoteLogs
```

This will put all logs under `/var/log/central/<hostname>.log`

Last thing, and this is kind of optional, we need to tell `logrotate` about this, and have it rotate the logs, so you don't end up with 100+MB text files.

Create file `/etc/logrotate.d/central`

```
/var/log/central/*.log
{
    rotate 4
    weekly
    missingok
    notifempty
    compress
    delaycompress
    sharedscripts
    postrotate
        invoke-rs.d rsyslog rotate >/dev/null 2>&1 || true
    endscript
}
```

- **rotate** - How many rotated copies to keep before removing the oldest one.
- **weekly** - Rotate log every 7 days.
- **missingok** - If the log file is missing, go on to the next one without issuing an error message.
- **notifempty** - Do not rotate the log if it is empty.
- **compress** - Gzip the logs.
- **delaycompress** - Postpone compression of the previous log file to the next rotation cycle.
- **sharedscripts** - Because we are going to use wildcard, we need this argument, telling `logrotate` this setting is for multiple logs.
- **postrotate** - What to do after rotation is finished, in this case invoke `rsyslog rotate`.

Some more info about options: <https://linux.die.net/man/8/logrotate>

Restart `rsyslog`

```
systemctl restart rsyslog
```


That's it for a server, no need to restart `logrotate`, that will be run via `cron`.

On logging clients

Now we set up nodes to send their logs to our server. Our server is called `control01`, and all nodes have this entry in their `/etc/hosts` file. We have did this here: [OS setting](#)

```
192.168.0.101 control01 control01.local
```

All you need to do is make sure you put following line `*,* @@control01.local:514` (of course with your hostname or the IP of your logging server) at the start of `/etc/rsyslog.conf`.

 **Warning**

Do not do this on `control01` (your logging server), that one is already logging to local files no need to also send the logs to localhost and possibly get logging loop (Thanks Vincent for pointing this out.)

For me, including the comments, the top of that file looks like this:

```
# /etc/rsyslog.conf configuration file for rsyslog
#
# For more information install rsyslog-doc and see
# /usr/share/doc/rsyslog-doc/html/configuration/index.html
#
# Default logging rules can be found in /etc/rsyslog.d/50-default.conf
*,* @@control01.local:514

#####
#### MODULES ####
#####

-
-
-
```

Nothing else, just restart `rsyslog`

```
systemctl restart rsyslog
```


Next, check the folder on the logging server. New logs should start appearing there in a seconds.

```
ubuntu@control01:/var/log/central$ ls
control01.log control02.log control03.log cube01.log cube02.log cube03.log cube04.log cube05.log cube06.log
ubuntu@control01:/var/log/central$
```

Inav

Just a nifty little program to watch your logs in real time, with filters and so on.

```
sudo apt install lnav
lnav /var/log/central/*.log
```

 Liked it ? Buy me a drink :)

Comments

What do you think?

5 Responses

👍

😄

😍

😮

😡

😞

Upvote

Funny

Love

Surprised

Angry

Sad

11 Comments

<https://rpi4cluster.com>

Disqus' Privacy Policy

Login

Favorite

Tweet

Share

Sort by Best

Join the discussion...

LOG IN WITH

OR SIGN UP WITH DISQUS ?

Taz Elikhaila • 2 months ago • edited

use this to validate the conf file if you're stuck

```
rsyslogd -N1 -f /etc/rsyslog.conf
```

1 ^ | v • Reply • Share ›

DRUSE DRU • 10 months ago

Can't manage to see logs in central folder at control01... I created hosts file in all nodes and edited files as described here but central folder is empty. How could I debug this?

Thanks again

^ | v • Reply • Share ›

viadoportes Mod → **DRUSE DRU** • 10 months ago

Hmm there is little that can't work here. Try telnet control01.local 514 from some other node than control01 if it can connect to the syslog server.

^ | v • Reply • Share ›

DRUSE DRU → **viadoportes** • 10 months ago

it connects:

```
ubuntu@cuba01:~$ telnet control01.local 514
Trying 192.168.86.21...
Connected to control01.
Escape character is '^['

This is control01 /etc/rsyslog.conf

# /etc/rsyslog.conf configuration file for rsyslog
#
# For more information install rsyslog-doc and see
# /usr/share/doc/rsyslog-doc/html/configuration/index.html
#
# Default logging rules can be found in /etc/rsyslog.d/50-default.conf

#####
see more
```

^ | v • Reply • Share ›

viadoportes Mod → **DRUSE DRU** • 10 months ago

Hmm only difference I can see from mine is that I have IP in the rsyslog.conf on nodes. Look here: <https://pastebin.com/7ZqHfn4D> just for fun try to create empty file with the node name where it should be... maybe there is some permissions issue or something.

^ | v • Reply • Share ›

DRUSE DRU → **viadoportes** • 10 months ago

Tried replacing name with ip with no success... how could i do that test?

^ | v • Reply • Share ›

viadoportes Mod → **DRUSE DRU** • 10 months ago

This is super strange, it should just work, Its very old function of rsyslog baring network issue there should be nothing preventing it. Make sure you have rsyslog installed and running. Also check with `journalctl -u rsyslog` on both node and server if its complains about something.

^ | v • Reply • Share ›

Nikolas Bousios (Rambou) • a year ago

Saying that

^ | and all nodes have this entry in their /etc/hosts file:

it's not true. At what step have we edited the /etc/hosts files of every node? Did ansible did this automatically somehow?

^ | v • Reply • Share ›

viadoportes Mod → **Nikolas Bousios (Rambou)** • a year ago

Sorry, I will add link to the point when it was done. In here: <https://rpi4cluster.com/k3s...>

^ | v • Reply • Share ›

Vincent • a year ago

Just think it might worth adding for rsyslog newbs like that the line

```
*,* @control01.local:514
```

should not be added to the central host as shit will hit the fan and you'll fall in a logloop (I think) Also, apparently the '~' in the template is deprecated and should be replaced by 'stop' and because we are extracting everything (".") the '%~' or '% stop' will generate a warning as there is nothing else to process anyway, so you can remove it!

^ | v • Reply • Share ›