======================== Syslog_Configuration ==========================

→ rsyslog is responsible for log processing in RHEL. rsyslog is abbreviation of 'Rocket Fast System for Log processing'. rsyslog offers high-performance, great security features and modular design. It can accept input from wide variety of sources, transform it and output the result to diverse destinations.

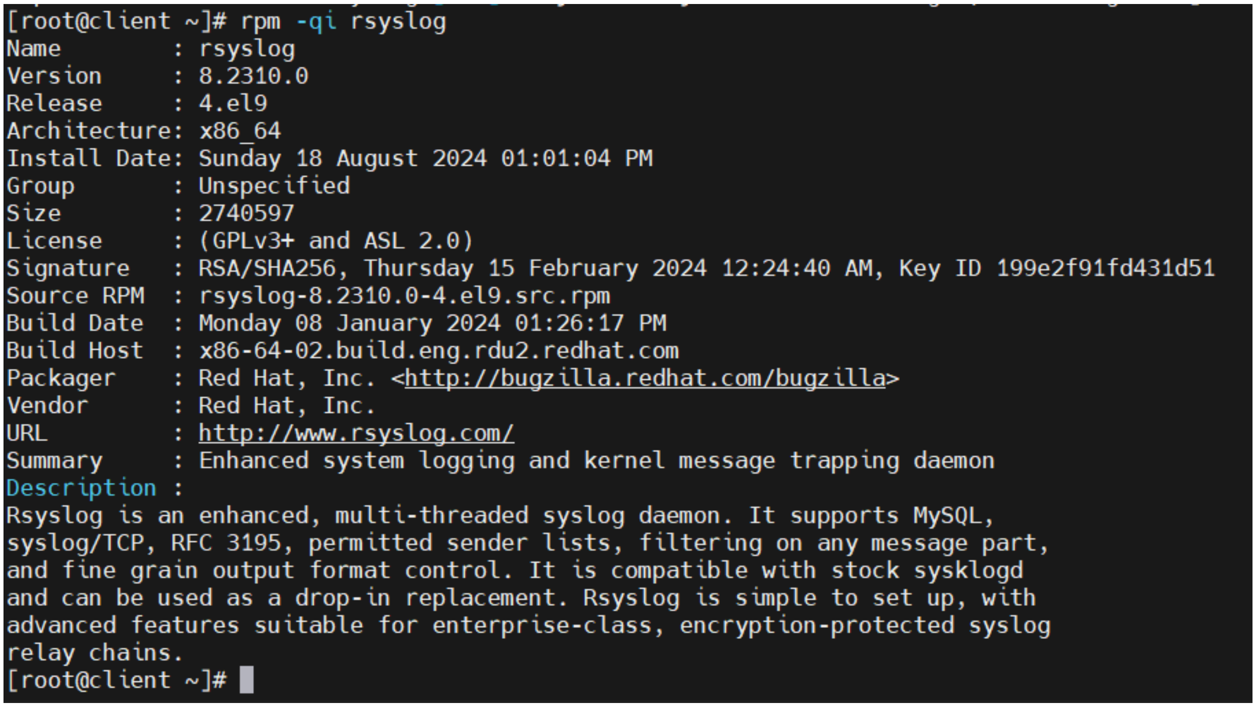
In this article, we will configure a central logging server using rsyslog on RHEL and then we will configure RHEL clients to submit their local logs to this rsyslog based central logging server.

→ rsyslog is by default installed on most of the Linux distros including RHEL/CentOS. Connect to rsyslog server and check status of rsyslog.service, start it if it is not running. (Install the package from repository if there is no such service present)

On Server :-

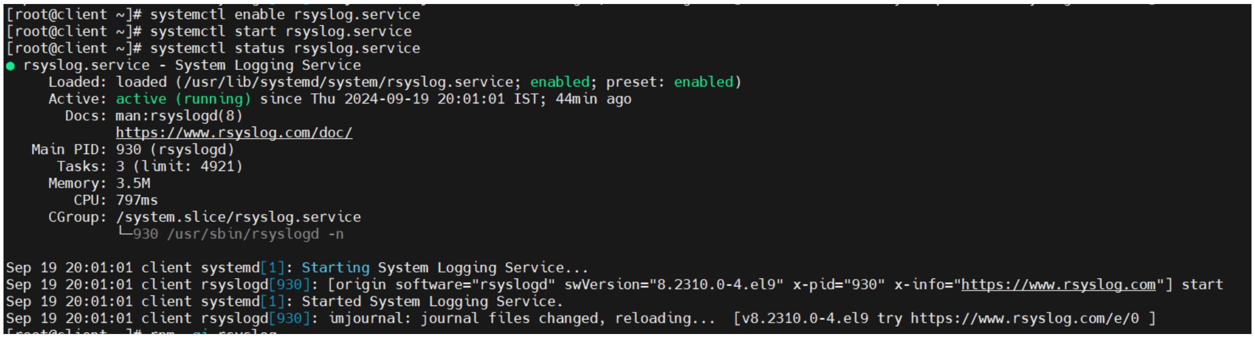
—----------------

# rpm -qi rsyslog



```
[root@client ~]# rpm -qi rsyslog
Name        : rsyslog
Version     : 8.2310.0
Release     : 4.el9
Architecture: x86_64
Install Date: Sunday 18 August 2024 01:01:04 PM
Group       : Unspecified
Size        : 2740597
License     : (GPLv3+ and ASL 2.0)
Signature   : RSA/SHA256, Thursday 15 February 2024 12:24:40 AM, Key ID 199e2f91fd431d51
Source RPM  : rsyslog-8.2310.0-4.el9.src.rpm
Build Date  : Monday 08 January 2024 01:26:17 PM
Build Host  : x86-64-02.build.eng.rdu2.redhat.com
Packager    : Red Hat, Inc. <http://bugzilla.redhat.com/bugzilla>
Vendor      : Red Hat, Inc.
URL         : http://www.rsyslog.com/
Summary     : Enhanced system logging and kernel message trapping daemon
Description :
Rsyslog is an enhanced, multi-threaded syslog daemon. It supports MySQL,
syslog/TCP, RFC 3195, permitted sender lists, filtering on any message part,
and fine grain output format control. It is compatible with stock sysklogd
and can be used as a drop-in replacement. Rsyslog is simple to set up, with
advanced features suitable for enterprise-class, encryption-protected syslog
relay chains.
[root@client ~]#
```

# systemctl start rsyslog.service
# systemctl enable rsyslog.service
# systemctl status rsyslog.service

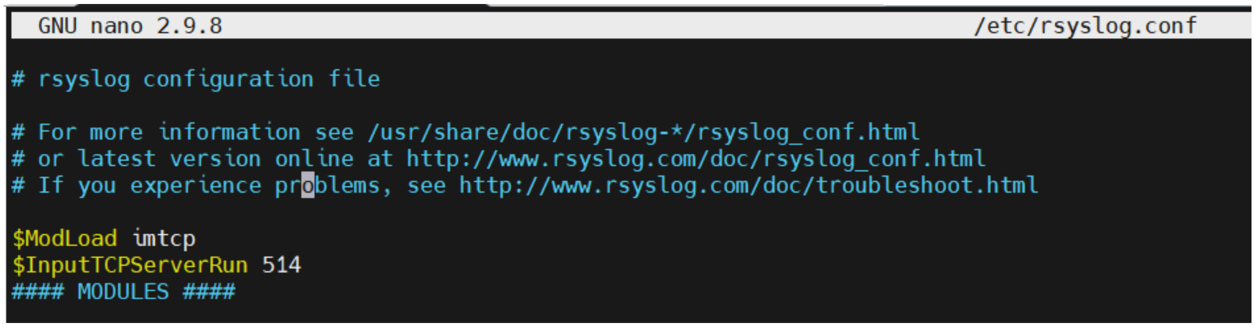


```
[root@client ~]# systemctl enable rsyslog.service
[root@client ~]# systemctl start rsyslog.service
[root@client ~]# systemctl status rsyslog.service
● rsyslog.service - System Logging Service
     Loaded: loaded (/usr/lib/systemd/system/rsyslog.service; enabled; preset: enabled)
     Active: active (running) since Thu 2024-09-19 20:01:01 IST; 44min ago
       Docs: man:rsyslogd(8)
             https://www.rsyslog.com/doc/
   Main PID: 930 (rsyslogd)
      Tasks: 3 (limit: 4921)
     Memory: 3.5M
        CPU: 797ms
     CGroup: /system.slice/rsyslog.service
             └─930 /usr/sbin/rsyslogd -n

Sep 19 20:01:01 client systemd[1]: Starting System Logging Service...
Sep 19 20:01:01 client rsyslogd[930]: [origin software="rsyslogd" swVersion="8.2310.0-4.el9" x-pid="930" x-info="https://www.rsyslog.com"] start
Sep 19 20:01:01 client systemd[1]: Started System Logging Service.
Sep 19 20:01:01 client rsyslogd[930]: imjournal: journal files changed, reloading...  [v8.2310.0-4.el9 try https://www.rsyslog.com/e/0 ]
```

→ Edit this file and add this two line and save the file

# nano /etc/rsyslog.conf

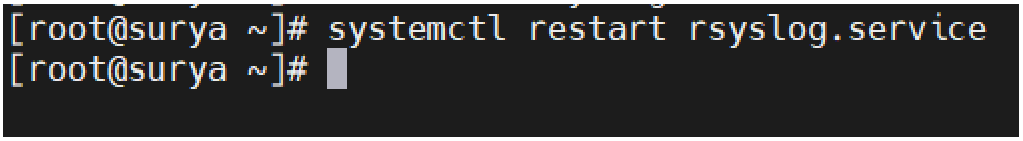
```
        $ModLoad imtcp
        $InputTCPServerRun 514
```



```
  GNU nano 2.9.8                                            /etc/rsyslog.conf

# rsyslog configuration file

# For more information see /usr/share/doc/rsyslog-*/rsyslog_conf.html
# or latest version online at http://www.rsyslog.com/doc/rsyslog_conf.html
# If you experience problems, see http://www.rsyslog.com/doc/troubleshoot.html

$ModLoad imtcp
$InputTCPServerRun 514
#### MODULES ####
```

→ Now restart the rsyslog.service.

# systemctl restart rsyslog.service



```
[root@surya ~]# systemctl restart rsyslog.service
[root@surya ~]# 
```

→ Allow rsyslog service port in Linux firewall and reload the firewall.

# firewall-cmd --permanent --add-port=514/tcp

# firewall-cmd --reload

=> Now syslog server is successfully configured

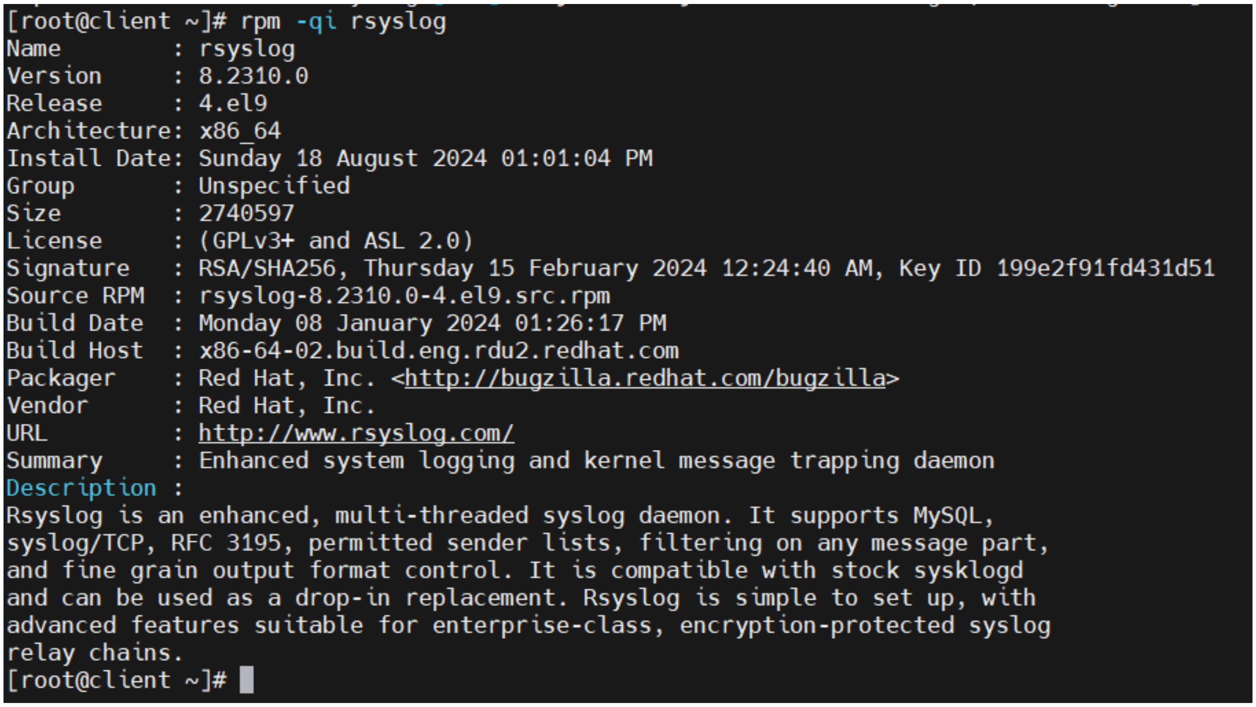
—---

On Client:-

—-----------

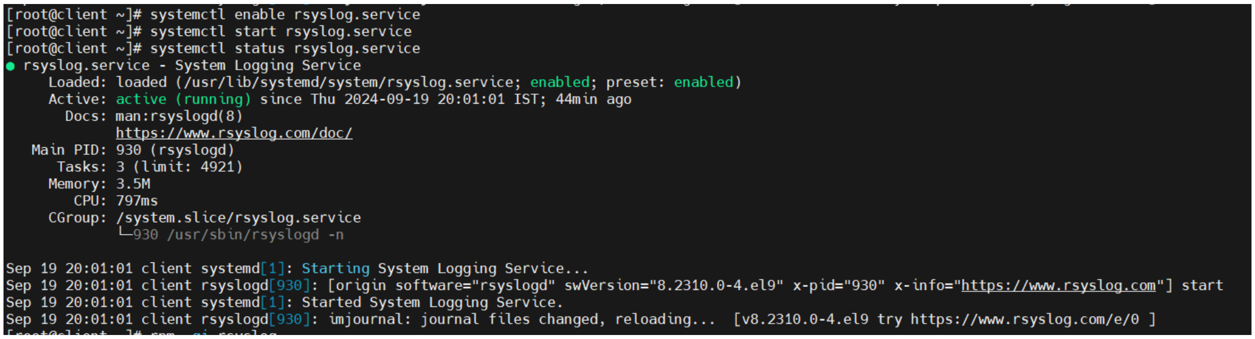
→ Connect to rsyslogclient.nehraclasses and check status of rsyslog.service, start & enable it if not running.

# rpm -qi rsyslog



```
[root@client ~]# rpm -qi rsyslog
Name        : rsyslog
Version     : 8.2310.0
Release     : 4.el9
Architecture: x86_64
Install Date: Sunday 18 August 2024 01:01:04 PM
Group       : Unspecified
Size        : 2740597
License     : (GPLv3+ and ASL 2.0)
Signature   : RSA/SHA256, Thursday 15 February 2024 12:24:40 AM, Key ID 199e2f91fd431d51
Source RPM  : rsyslog-8.2310.0-4.el9.src.rpm
Build Date  : Monday 08 January 2024 01:26:17 PM
Build Host  : x86-64-02.build.eng.rdu2.redhat.com
Packager    : Red Hat, Inc. <http://bugzilla.redhat.com/bugzilla>
Vendor      : Red Hat, Inc.
URL         : http://www.rsyslog.com/
Summary     : Enhanced system logging and kernel message trapping daemon
Description :
Rsyslog is an enhanced, multi-threaded syslog daemon. It supports MySQL,
syslog/TCP, RFC 3195, permitted sender lists, filtering on any message part,
and fine grain output format control. It is compatible with stock sysklogd
and can be used as a drop-in replacement. Rsyslog is simple to set up, with
advanced features suitable for enterprise-class, encryption-protected syslog
relay chains.
[root@client ~]#
```

# systemctl start rsyslog.service
# systemctl enable rsyslog.service
# systemctl start rsyslog.service

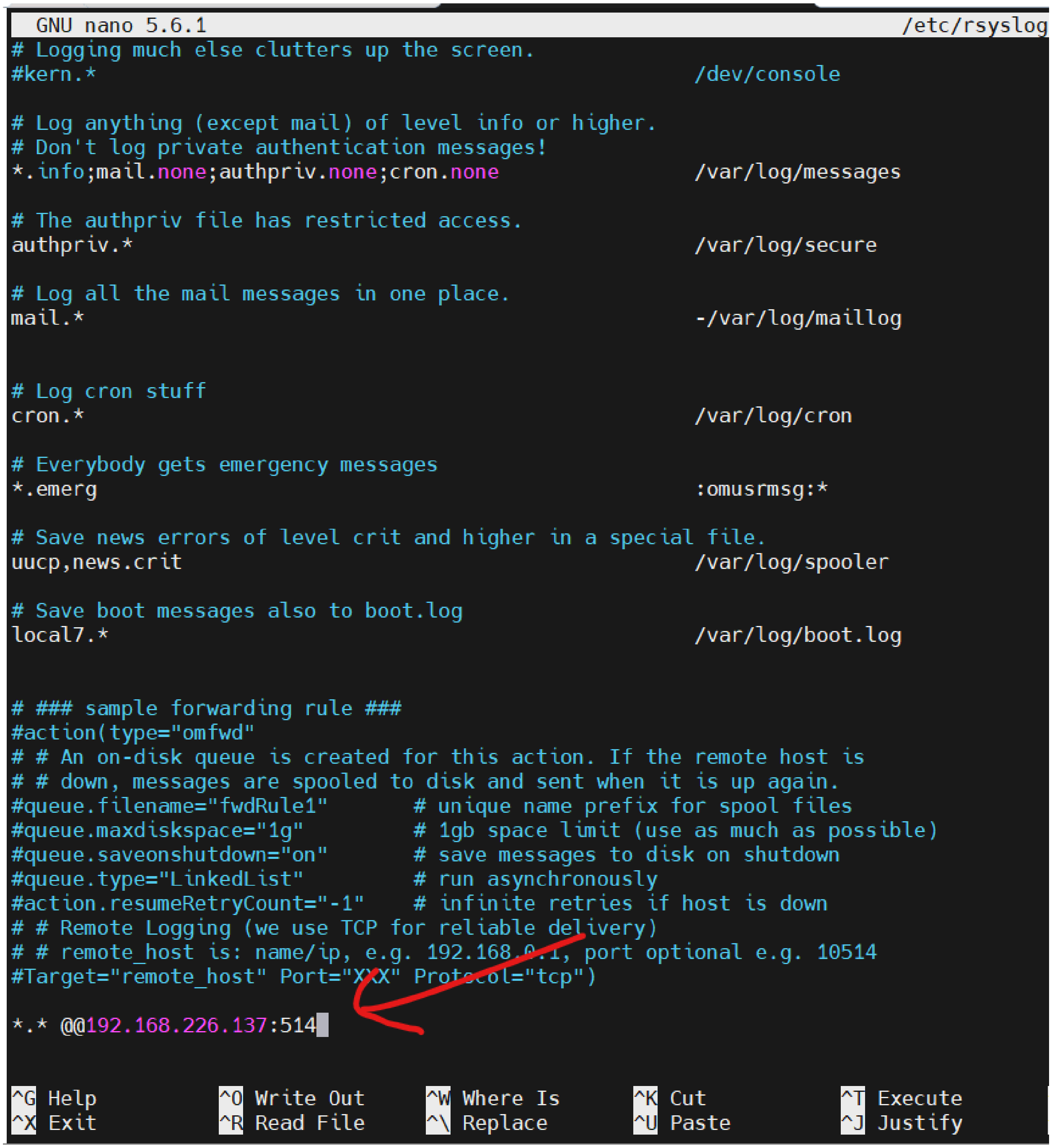


```
[root@client ~]# systemctl enable rsyslog.service
[root@client ~]# systemctl start rsyslog.service
[root@client ~]# systemctl status rsyslog.service
● rsyslog.service - System Logging Service
     Loaded: loaded (/usr/lib/systemd/system/rsyslog.service; enabled; preset: enabled)
     Active: active (running) since Thu 2024-09-19 20:01:01 IST; 44min ago
       Docs: man:rsyslogd(8)
             https://www.rsyslog.com/doc/
   Main PID: 930 (rsyslogd)
      Tasks: 3 (limit: 4921)
     Memory: 3.5M
        CPU: 797ms
     CGroup: /system.slice/rsyslog.service
             └─930 /usr/sbin/rsyslogd -n

Sep 19 20:01:01 client systemd[1]: Starting System Logging Service...
Sep 19 20:01:01 client rsyslogd[930]: [origin software="rsyslogd" swVersion="8.2310.0-4.el9" x-pid="930" x-info="https://www.rsyslog.com"] start
Sep 19 20:01:01 client systemd[1]: Started System Logging Service.
Sep 19 20:01:01 client rsyslogd[930]: imjournal: journal files changed, reloading...  [v8.2310.0-4.el9 try https://www.rsyslog.com/e/0 ]
```

→ Now configure rsyslog client to transmit its log to our rsyslog server by adding the following directives in /etc/rsyslog.conf

# nano /etc/rsyslog.conf

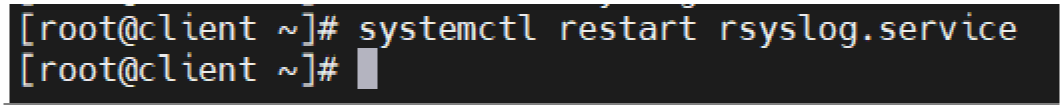
```
*.* @@192.168.226.137:514
```



```
  GNU nano 5.6.1                                                        /etc/rsyslog
# Logging much else clutters up the screen.
#kern.*                                                 /dev/console

# Log anything (except mail) of level info or higher.
# Don't log private authentication messages!
*.info;mail.none;authpriv.none;cron.none                /var/log/messages

# The authpriv file has restricted access.
authpriv.*                                              /var/log/secure

# Log all the mail messages in one place.
mail.*                                                  -/var/log/maillog


# Log cron stuff
cron.*                                                  /var/log/cron

# Everybody gets emergency messages
*.emerg                                                 :omusrmsg:*

# Save news errors of level crit and higher in a special file.
uucp,news.crit                                          /var/log/spooler

# Save boot messages also to boot.log
local7.*                                                /var/log/boot.log


# ### sample forwarding rule ###
#action(type="omfwd"
# # An on-disk queue is created for this action. If the remote host is
# # down, messages are spooled to disk and sent when it is up again.
#queue.filename="fwdRule1"       # unique name prefix for spool files
#queue.maxdiskspace="1g"         # 1gb space limit (use as much as possible)
#queue.saveonshutdown="on"       # save messages to disk on shutdown
#queue.type="LinkedList"         # run asynchronously
#action.resumeRetryCount="-1"    # infinite retries if host is down
# # Remote Logging (we use TCP for reliable delivery)
# # remote_host is: name/ip, e.g. 192.168.0.1, port optional e.g. 10514
#Target="remote_host" Port="XXX" Protocol="tcp")

*.* @@192.168.226.137:514


^G Help         ^O Write Out    ^W Where Is     ^K Cut          ^T Execute
^X Exit         ^R Read File    ^\ Replace      ^U Paste        ^J Justify
```

→ Restart the rsyslog.service to apply changes.

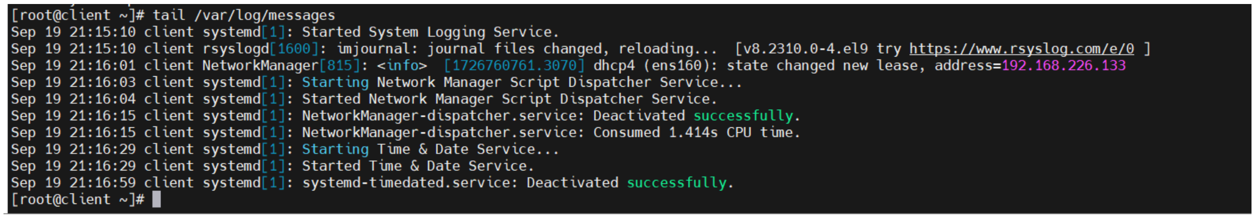
# systemctl restart rsyslog.service



```
[root@client ~]# systemctl restart rsyslog.service
[root@client ~]#
```

→Our rsyslog client has been configured,Now connect to our rsyslog server and check /var/log/messages

# tail /var/log/messages



```
[root@client ~]# tail /var/log/messages
Sep 19 21:15:10 client systemd[1]: Started System Logging Service.
Sep 19 21:15:10 client rsyslogd[1600]: imjournal: journal files changed, reloading...  [v8.2310.0-4.el9 try https://www.rsyslog.com/e/0 ]
Sep 19 21:16:01 client NetworkManager[815]: <info>  [1726760761.3070] dhcp4 (ens160): state changed new lease, address=192.168.226.133
Sep 19 21:16:03 client systemd[1]: Starting Network Manager Script Dispatcher Service...
Sep 19 21:16:04 client systemd[1]: Started Network Manager Script Dispatcher Service.
Sep 19 21:16:15 client systemd[1]: NetworkManager-dispatcher.service: Deactivated successfully.
Sep 19 21:16:15 client systemd[1]: NetworkManager-dispatcher.service: Consumed 1.414s CPU time.
Sep 19 21:16:29 client systemd[1]: Starting Time & Date Service...
Sep 19 21:16:29 client systemd[1]: Started Time & Date Service.
Sep 19 21:16:59 client systemd[1]: systemd-timedated.service: Deactivated successfully.
[root@client ~]# 
```

We can see that client is forwarding its logs to server.

THANK YOU

Suryadev Chaudhay