

# Log Management

## Centralized Log:

Add this script in server Machine:

```
[root@server ~]# vim /etc/rsyslog.conf
```

Uncomment line number 37 and 38, add line 40 & 41 write script

```
root@server:~ — vim /etc/rsyslog.conf
5 # If you experience problems, see http://www.rsyslog.com/doc/troubleshoot.html
6
7 ### GLOBAL DIRECTIVES ###
8
9 # Where to place auxiliary files
10 global(workDirectory="/var/lib/rsyslog")
11
12 # Use default timestamp format
13 module(load="builtin:omfile" Template="RSYSLOG_TraditionalFileFormat")
14
15 ### MODULES ###
16
17 module(load="imuxsock" # provides support for local system logging (e.g. via logger command)
18       SysSock.Use="off") # Turn off message reception via local log socket;
19       # local messages are retrieved through imjournal now.
20 module(load="imjournal" # provides access to the systemd journal
21       UsePid="system" # PID number is retrieved as the ID of the process the journal entry originates from
22       FileCreateMode="0644" # Set the access permissions for the state file
23       StateFile="imjournal.state") # File to store the position in the journal
24 #module(load="imklog") # reads kernel messages (the same are read from journald)
25 #module(load="immark") # provides --MARK-- message capability
26
27 # Include all config files in /etc/rsyslog.d/
28 include(file="/etc/rsyslog.d/*.conf" mode="optional")
29
30 # Provides UDP syslog reception
31 # for parameters see http://www.rsyslog.com/doc/imudp.html
32 #module(load="imudp") # needs to be done just once
33 #input(type="imudp" port="514")
34
35 # Provides TCP syslog reception
36 # for parameters see http://www.rsyslog.com/doc/imtcp.html
37 module(load="imtcp") # needs to be done just once
38 input(type="imtcp" port="514")
39 $template tmplAuth, "var/log/client/%HOSTNAME%/%PROGRAMNAME%.log"
40 *. * ?tmplAuth
41 ### RULES ###
42
43 # Log all kernel messages to the console.
44 # Logging much else clutters up the screen.
45 #kern.* /dev/console
-- INSERT --
40,14 9%
```

You can see client directory

```
[root@server ~]# cd /var/log
[root@server log]# ls
anaconda boot.log-20250727 cron-20250724 gdm mail messages-20250724 secure
audit boot.log-20250804 cron-20250727 hawkey.log maillog messages-20250727 secure
boot.log btmp cron-20250804 hawkey.log-20250706 maillog-20250717 messages-20250804 secure
boot.log-20250706 btmp-20250804 cups hawkey.log-20250717 maillog-20250724 private secure
boot.log-20250708 chrany dnf.librepo.log hawkey.log-20250724 maillog-20250727 qemu-ga speed
boot.log-20250710 client dnf.log hawkey.log-20250804 maillog-20250804 README spool
boot.log-20250717 cron dnf.rpm.log httpd messages samba spool
boot.log-20250724 cron-20250717 firewall lastlog messages-20250717 secure spool
[root@server log]#
```

Add port 514

```
[root@server ~]# systemctl restart rsyslog.service
[root@server ~]# firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpv6-client http ssh
  ports: 2021/tcp
  protocols:
  forward: yes
  masquerade: yes
  forward-ports:
    port=22:proto=tcp:toport=2021:toaddr=
  source-ports:
  icmp-blocks:
  rich rules:
[root@server ~]# firewall-cmd --add-port=514/tcp --permanent
success
[root@server ~]# firewall-cmd --reload
success
[root@server ~]# firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpv6-client http ssh
  ports: 2021/tcp 514/tcp
  protocols:
  forward: yes
  masquerade: yes
  forward-ports:
    port=22:proto=tcp:toport=2021:toaddr=
  source-ports:
  icmp-blocks:
  rich rules:
[root@server ~]#
```

## Client Machine:

```
[root@client ~]# vim /etc/rsyslog.conf
```

Add below text at line no. 82

```
root@client:~ — vim /etc/rsyslog.conf

42 # Log all kernel messages to the console.
43 # Logging much else clutters up the screen.
44 #kern.*                                          /dev/console
45
46 # Log anything (except mail) of level info or higher.
47 # Don't log private authentication messages!
48 *.info;mail.none;authpriv.none;cron.none      /var/log/messages
49
50 # The authpriv file has restricted access.
51 authpriv.*                                      /var/log/secure
52
53 # Log all the mail messages in one place.
54 mail.*                                          -/var/log/maillog
55
56
57 # Log cron stuff
58 cron.*                                          /var/log/cron
59
60 # Everybody gets emergency messages
61 *.emerg                                         :omusrmsg:*
62
63 # Save news errors of level crit and higher in a special file.
64 uucp,news.crit                                  /var/log/spooler
65
66 # Save boot messages also to boot.log
67 local7.*                                       /var/log/boot.log
68
69
70 # ### sample forwarding rule ###
71 #action(type="omfwd"
72 # # An on-disk queue is created for this action. If the remote host is
73 # # down, messages are spooled to disk and sent when it is up again.
74 #queue.filename="fwdRule1"                    # unique name prefix for spool files
75 #queue.maxdiskspace="1g"                      # 1gb space limit (use as much as possible)
76 #queue.saveonshutdown="on"                   # save messages to disk on shutdown
77 #queue.type="LinkedList"                     # run asynchronously
78 #action.resumeRetryCount="-1"                 # infinite retries if host is down
79 # # Remote Logging (we use TCP for reliable delivery)
80 # # remote_host is: name/ip, e.g. 192.168.0.1, port optional e.g. 10514
81 #Target="remote_host" Port="XXX" Protocol="tcp")
82 *.* @192.168.0.3:514
:wq:
```

**Server Machine:** you can see client machine log here

```
[root@server ~]# cd /var/log/client
[root@server client]# ls
client server
[root@server client]# cd client
[root@server client]# ls
accounts-daemon      cupsd                gnome-keyring-secrets.desktop  kdumpctl              rtkit-daemon
alsactl              dbus-broker          gnome-keyring-ssh.desktop      kernel                 run-parts
at-spi2-registrd     dbus-broker-lau      gnome-session                  lvm                    spice-vdagent
at-spi-bus-launcher  dbus-broker-launch   gnome-session-binary           mcelog                 sshd
auditd               dnf                  gnome-shell                    ModemManager           sssd_kcm
augenrules           dracut-cmdline        gnome-software                 NetworkManager          systemd
avahi-daemon         dracut-initqueue     goa-daemon                     org.gnome.Shell.desktop systemd-coredump
bootctl              fwupd                goa-identity-se                PackageKit              systemd-fsck
chronyd              gdm-launch-environment] gsd-color                      packagekitd             systemd-hibernate
colord               gdm-password         gsd-media-keys                 polkitd                 systemd-journald
crond                gdm-wayland-session  gsd-sharing                    realmd                   systemd-logind
CROND               geoclue              gsd-usb-protect                rsyslogd                systemd-modules-1
[root@server client]#
```

## Log Rotation:

### Configuration Files-

```
[root@server ~]# vim /etc/logrotate.d
```

```
root@server:~ — vim /etc/logrotate.d
=====
# Netrw Directory Listing                                (netrw v170)
# /etc/logrotate.d
#   Sorted by      name
#   Sort sequence: [/]/$, \<core\%(\\.d\\+\\)=|>, \.h$, \.c$, \.cpp$, \-|=|+$, *, \.o$, \.obj$, \.info$, \.swp$, \.bak$, \~$
#   Quick Help: <F1>:help  ~:go up dir  D:delete  R:rename  s:sort-by  x:special
# =====
./
./
bootlog
btmpt
chrony
dnf
firewalld
httpd
iscsiuilog
kvm_stat
psacct
rsyslog
sakshi
samba
sssd
wpa_supplicant
wtmpt

I

"/etc/logrotate.d" is a directory                                     8.1      All
```

```
[root@server ~]# vim /etc/logrotate.conf
```

```
root@server:~ — vim /etc/logrotate.conf
see "man logrotate" for details

# global options do not affect preceding include directives

# rotate log files weekly
weekly

# keep 4 weeks worth of backlogs
rotate 4

# create new (empty) log files after rotating old ones
create

# use date as a suffix of the rotated file
dateext

# uncomment this if you want your log files compressed
#compress

# packages drop log rotation information into this directory
include /etc/logrotate.d

# system-specific logs may be also be configured here.

"/etc/logrotate.conf" 221 — 406B
```

## Create directory to create automatic log

```
[root@server ~]# vim /etc/logrotate.d/sakshi
```

[illegible]

Created log file

```
[root@server ~]# mkdir /root/sakshi
[root@server ~]# cd /root/sakshi
[root@server sakshi]# ls
[root@server sakshi]# cd
[root@server ~]# echo "hello Sakshi, this sample log" > /root/sakshi/file.log
[root@server ~]# cd /root/sakshi
[root@server sakshi]# ls
file.log
[root@server sakshi]# cat file.log
hello Sakshi, this sample log
[root@server sakshi]#
```

## Compress log file

```
[root@server ~]# logrotate -f /etc/logrotate.conf
error: destination /var/log/btmp-20250812 already exists, skipping rotation
error: destination /var/log/firewalld-20250812 already exists, skipping rotation
error: destination /var/log/httpd/error_log-20250812 already exists, skipping rotation
error: destination /var/log/cron-20250812 already exists, skipping rotation
error: destination /var/log/maillog-20250812 already exists, skipping rotation
error: destination /var/log/messages-20250812 already exists, skipping rotation
error: destination /var/log/secure-20250812 already exists, skipping rotation
error: destination /var/log/spooler-20250812 already exists, skipping rotation
error: destination /root/sakshi/file.log-20250812.gz already exists, skipping rotation
error: stat of /root/sakshi/*.log failed: Not a directory
error: destination /var/log/wtmp-20250812 already exists, skipping rotation
[root@server ~]# cd /root/sakshi
[root@server sakshi]# ls
file.log  file.log-20250812.gz
[root@server sakshi]#
```

Unzip log file so that you can use

```
[root@server sakshi]# gunzip file.log-20250812.gz
[root@server sakshi]# ls
file.log  file.log-20250812
[root@server sakshi]#
```