Managing Logs

Most of the system logs under Linux can be found in **/var/log**.

<note important> It is a good idea to put **/var/log** on a separate partition when installing Linux such that verbose logging does not crash the system by consuming too much disk space. </note>

The /var/log/messages file

This file contains the majority of system messages:

```
[root@centos ~]# tail -n 15 /var/log/messages
Dec  4 17:56:26 centos NetworkManager[1313]: <info>   nameserver '10.0.2.3'
Dec  4 17:56:26 centos NetworkManager[1313]: <info>   domain name 'hotspot.s-bit.nl'
Dec  4 17:56:26 centos NetworkManager[1313]: <info> Activation (eth0) Stage 5 of 5 (IP Configure Commit)
scheduled...
Dec  4 17:56:26 centos NetworkManager[1313]: <info> Activation (eth0) Stage 4 of 5 (IP4 Configure Get) complete.
Dec  4 17:56:26 centos NetworkManager[1313]: <info> Activation (eth0) Stage 5 of 5 (IP Configure Commit)
started...
Dec  4 17:56:26 centos dhclient[2530]: bound to 10.0.2.15 -- renewal in 36247 seconds.
Dec  4 17:56:27 centos NetworkManager[1313]: <info> (eth0): device state change: 7 -> 8 (reason 0)
Dec  4 17:56:28 centos NetworkManager[1313]: <info> Policy set 'System eth0' (eth0) as default for IPv4 routing
and DNS.
Dec  4 17:56:28 centos NetworkManager[1313]: <info> Activation (eth0) successful, device activated.
Dec  4 17:56:28 centos NetworkManager[1313]: <info> Activation (eth0) Stage 5 of 5 (IP Configure Commit)
complete.
Dec  4 17:56:28 centos ntpd[1652]: Listening on interface #5 eth0, 10.0.2.15#123 Enabled
Dec  4 18:01:03 centos ntpd[1652]: synchronized to 193.104.37.238, stratum 2
Dec  4 18:01:03 centos ntpd[1652]: time reset +1.120416 s
Dec  4 18:01:03 centos ntpd[1652]: kernel time sync status change 2001
```

```
Dec  4 18:07:25 centos ntpd[1652]: synchronized to 193.104.37.238, stratum 2
```

The /bin/dmesg Command

This command shows the boot sequence messages:

```
[root@centos ~]# dmesg | more
Initializing cgroup subsys cpuset
Initializing cgroup subsys cpu
Linux version 2.6.32-358.23.2.el6.i686 (mockbuild@c6b9.bsys.dev.centos.org) (gcc
 version 4.4.7 20120313 (Red Hat 4.4.7-3) (GCC) ) #1 SMP Wed Oct 16 17:21:31 UTC
 2013
KERNEL supported cpus:
  Intel GenuineIntel
  AMD AuthenticAMD
  NSC Geode by NSC
  Cyrix CyrixInstead
  Centaur CentaurHauls
  Transmeta GenuineTMx86
  Transmeta TransmetaCPU
  UMC UMC UMC UMC
BIOS-provided physical RAM map:
 BIOS-e820: 0000000000000000 - 000000000009fc00 (usable)
 BIOS-e820: 000000000009fc00 - 00000000000a0000 (reserved)
 BIOS-e820: 00000000000f0000 - 0000000000100000 (reserved)
 BIOS-e820: 0000000000100000 - 000000006f8f0000 (usable)
 BIOS-e820: 000000006f8f0000 - 000000006f900000 (ACPI data)
 BIOS-e820: 00000000fffc0000 - 0000000100000000 (reserved)
DMI 2.5 present.
SMBIOS version 2.5 @ 0xFFF60
--More--
```

The /var/log/audit/audit.log file

This file contains **events** from the audit system. Events are:

- system calls,
- file access information,
- messages from SELinux.

Firstly start the auditd daemon:

```
[root@centos ~]# service auditd status
auditd is stopped
[root@centos ~]# service auditd start
Starting auditd:                                           [  OK  ]
```

Now view the audit.log file:

```
[root@centos ~]# tail -n 15 /var/log/audit/audit.log
type=DAEMON_START msg=audit(1386184942.561:5633): auditd start, ver=2.2 format=raw
kernel=2.6.32-358.23.2.el6.i686 auid=500 pid=4068 subj=unconfined_u:system_r:auditd_t:s0 res=success
type=CONFIG_CHANGE msg=audit(1386184942.797:20): audit_backlog_limit=320 old=64 auid=500 ses=2
subj=unconfined_u:system_r:auditctl_t:s0 res=1
type=USER_ACCT msg=audit(1386184981.155:21): user pid=4079 uid=0 auid=4294967295 ses=4294967295
subj=system_u:system_r:crond_t:s0-s0:c0.c1023 msg='op=PAM:accounting acct="trainee" exe="/usr/sbin/crond"
hostname=? addr=? terminal=cron res=success'
type=CRED_ACQ msg=audit(1386184981.156:22): user pid=4079 uid=0 auid=4294967295 ses=4294967295
subj=system_u:system_r:crond_t:s0-s0:c0.c1023 msg='op=PAM:setcred acct="trainee" exe="/usr/sbin/crond" hostname=?
addr=? terminal=cron res=success'
type=LOGIN msg=audit(1386184981.158:23): pid=4079 uid=0 subj=system_u:system_r:crond_t:s0-s0:c0.c1023 old
auid=4294967295 new auid=500 old ses=4294967295 new ses=170
type=USER_START msg=audit(1386184981.162:24): user pid=4079 uid=0 auid=500 ses=170
subj=system_u:system_r:crond_t:s0-s0:c0.c1023 msg='op=PAM:session_open acct="trainee" exe="/usr/sbin/crond"
hostname=? addr=? terminal=cron res=success'
```

```
type=CRED_DISP msg=audit(1386184981.230:25): user pid=4079 uid=500 auid=500 ses=170
subj=system_u:system_r:crond_t:s0-s0:c0.c1023 msg='op=PAM:setcred acct="trainee" exe="/usr/sbin/crond" hostname=?
addr=? terminal=cron res=success'
type=USER_END msg=audit(1386184981.233:26): user pid=4079 uid=500 auid=500 ses=170
subj=system_u:system_r:crond_t:s0-s0:c0.c1023 msg='op=PAM:session_close acct="trainee" exe="/usr/sbin/crond"
hostname=? addr=? terminal=cron res=success'
type=USER_ACCT msg=audit(1386185041.317:27): user pid=4086 uid=0 auid=4294967295 ses=4294967295
subj=system_u:system_r:crond_t:s0-s0:c0.c1023 msg='op=PAM:accounting acct="trainee" exe="/usr/sbin/crond"
hostname=? addr=? terminal=cron res=success'
type=CRED_ACQ msg=audit(1386185041.318:28): user pid=4086 uid=0 auid=4294967295 ses=4294967295
subj=system_u:system_r:crond_t:s0-s0:c0.c1023 msg='op=PAM:setcred acct="trainee" exe="/usr/sbin/crond" hostname=?
addr=? terminal=cron res=success'
type=LOGIN msg=audit(1386185041.320:29): pid=4086 uid=0 subj=system_u:system_r:crond_t:s0-s0:c0.c1023 old
auid=4294967295 new auid=500 old ses=4294967295 new ses=171
type=USER_START msg=audit(1386185041.325:30): user pid=4086 uid=0 auid=500 ses=171
subj=system_u:system_r:crond_t:s0-s0:c0.c1023 msg='op=PAM:session_open acct="trainee" exe="/usr/sbin/crond"
hostname=? addr=? terminal=cron res=success'
type=CRED_DISP msg=audit(1386185041.392:31): user pid=4086 uid=500 auid=500 ses=171
subj=system_u:system_r:crond_t:s0-s0:c0.c1023 msg='op=PAM:setcred acct="trainee" exe="/usr/sbin/crond" hostname=?
addr=? terminal=cron res=success'
type=USER_END msg=audit(1386185041.397:32): user pid=4086 uid=500 auid=500 ses=171
subj=system_u:system_r:crond_t:s0-s0:c0.c1023 msg='op=PAM:session_close acct="trainee" exe="/usr/sbin/crond"
hostname=? addr=? terminal=cron res=success'
```

Managing Audit Events

Managing Audit events uses three binaries:

auditd

auditd is the audit system's daemon. When started it writes events to the log file. It is configured by the **/etc/audit/auditd.conf** file:

```
[root@centos ~]# cat /etc/audit/auditd.conf
#
# This file controls the configuration of the audit daemon
#

log_file = /var/log/audit/audit.log
log_format = RAW
log_group = root
priority_boost = 4
flush = INCREMENTAL
freq = 20
num_logs = 5
disp_qos = lossy
dispatcher = /sbin/audispd
name_format = NONE
##name = mydomain
max_log_file = 6
max_log_file_action = ROTATE
space_left = 75
space_left_action = SYSLOG
action_mail_acct = root
admin_space_left = 50
admin_space_left_action = SUSPEND
disk_full_action = SUSPEND
disk_error_action = SUSPEND
##tcp_listen_port =
tcp_listen_queue = 5
tcp_max_per_addr = 1
##tcp_client_ports = 1024-65535
tcp_client_max_idle = 0
enable_krb5 = no
krb5_principal = auditd
##krb5_key_file = /etc/audit/audit.key
```

auditctl

This binary is used to configure the audit system. At boot time, auditctl reads and applies the rules specified in the **/etc/audit/audit.rules** file:

```
[root@centos ~]# cat /etc/audit/audit.rules
# This file contains the auditctl rules that are loaded
# whenever the audit daemon is started via the initscripts.
# The rules are simply the parameters that would be passed
# to auditctl.

# First rule - delete all
-D

# Increase the buffers to survive stress events.
# Make this bigger for busy systems
-b 320

# Feel free to add below this line. See auditctl man page
```

Command Line Switches

The command line switches for the auditctl command are :

```
[root@centos ~]# auditctl --help
usage: auditctl [options]
    -a <l,a>            Append rule to end of <l>ist with <a>ction
    -A <l,a>            Add rule at beginning of <l>ist with <a>ction
    -b <backlog>        Set max number of outstanding audit buffers
                        allowed Default=64
    -c                  Continue through errors in rules
    -C f=f              Compare collected fields if available:
                        Field name, operator(=,!=), field name
```

```
    -d <l,a>            Delete rule from <l>ist with <a>ction
                        l=task,exit,user,exclude
                        a=never,always
    -D                  Delete all rules and watches
    -e [0..2]           Set enabled flag
    -f [0..2]           Set failure flag
                        0=silent 1=printk 2=panic
    -F f=v              Build rule: field name, operator(=,!=,<,>,<=,
                        >=,&,&=) value
    -h                  Help
    -i                  Ignore errors when reading rules from file
    -k <key>            Set filter key on audit rule
    -l                  List rules
    -m text             Send a user-space message
    -p [r|w|x|a]        Set permissions filter on watch
                        r=read, w=write, x=execute, a=attribute
    -q <mount,subtree>  make subtree part of mount point's dir watches
    -r <rate>           Set limit in messages/sec (0=none)
    -R <file>           read rules from file
    -s                  Report status
    -S syscall          Build rule: syscall name or number
    -t                  Trim directory watches
    -v                  Version
    -w <path>           Insert watch at <path>
    -W <path>           Remove watch at <path>
```

audispd

This binary is responsable for distributing audit events to third party applications. audispd is controlled by the auditd daemon. In order to tell audispd how they want to receive events, applications place a file in the **/etc/audisp/plugins.d** directory:

```
[root@centos ~]# ls /etc/audisp/plugins.d/
```

```
af_unix.conf  syslog.conf
```

The format of these files is as follows :

```
[root@centos ~]# cat /etc/audisp/plugins.d/syslog.conf
# This file controls the configuration of the syslog plugin.
# It simply takes events and writes them to syslog. The
# arguments provided can be the default priority that you
# want the events written with. And optionally, you can give
# a second argument indicating the facility that you want events
# logged to. Valid options are LOG_LOCAL0 through 7.

active = no
direction = out
path = builtin_syslog
type = builtin
args = LOG_INFO
format = string
```

Viewing Audit Events

Two binaries are supplied to view audit events: **aureport** and **ausearch**:

The aureport Command

```
[root@centos ~]# aureport

Summary Report
======================
Range of time in logs: 12/04/2013 20:22:22.561 - 12/04/2013 22:12:01.832
Selected time for report: 12/04/2013 20:22:22 - 12/04/2013 22:12:01.832
```

```
Number of changes in configuration: 1
Number of changes to accounts, groups, or roles: 0
Number of logins: 0
Number of failed logins: 0
Number of authentications: 4
Number of failed authentications: 0
Number of users: 3
Number of terminals: 3
Number of host names: 1
Number of executables: 3
Number of files: 0
Number of AVC's: 0
Number of MAC events: 0
Number of failed syscalls: 0
Number of anomaly events: 0
Number of responses to anomaly events: 0
Number of crypto events: 0
Number of keys: 0
Number of process IDs: 129
Number of events: 746
```

Command Line Switches

The command line switches for the aureport command are :

```
[root@centos ~]# aureport --help
usage: aureport [options]
    -a,--avc            Avc report
    -au,--auth            Authentication report
    -c,--config            Config change report
    -cr,--crypto            Crypto report
    -e,--event            Event report
    -f,--file            File name report
```

```
    --failed            only failed events in report
    -h,--host            Remote Host name report
    --help                help
    -i,--interpret            Interpretive mode
    -if,--input <Input File name>    use this file as input
    --input-logs            Use the logs even if stdin is a pipe
    -l,--login            Login report
    -k,--key            Key report
    -m,--mods            Modification to accounts report
    -ma,--mac            Mandatory Access Control (MAC) report
    --node <node name>        Only events from a specific node
    -n,--anomaly            aNomaly report
    -p,--pid            Pid report
    -r,--response            Response to anomaly report
    -s,--syscall            Syscall report
    --success            only success events in report
    --summary            sorted totals for main object in report
    -t,--log            Log time range report
    -te,--end [end date] [end time]    ending date & time for reports
    -tm,--terminal            TerMinal name report
    -ts,--start [start date] [start time]    starting data & time for reports
    --tty                Report about tty keystrokes
    -u,--user            User name report
    -v,--version            Version
    -x,--executable            eXecutable name report
    If no report is given, the summary report will be displayed
```

The ausearch Command

This command can be used to search for all events related to a specific user:

```
[root@centos ~]# ausearch -ui 500 | more
----
```

```
time->Wed Dec  4 20:23:01 2013
type=CRED_DISP msg=audit(1386184981.230:25): user pid=4079 uid=500 auid=500 ses=
170 subj=system_u:system_r:crond_t:s0-s0:c0.c1023 msg='op=PAM:setcred acct="trai
nee" exe="/usr/sbin/crond" hostname=? addr=? terminal=cron res=success'
----
time->Wed Dec  4 20:23:01 2013
type=USER_END msg=audit(1386184981.233:26): user pid=4079 uid=500 auid=500 ses=1
70 subj=system_u:system_r:crond_t:s0-s0:c0.c1023 msg='op=PAM:session_close acct=
"trainee" exe="/usr/sbin/crond" hostname=? addr=? terminal=cron res=success'
----
time->Wed Dec  4 20:24:01 2013
type=CRED_DISP msg=audit(1386185041.392:31): user pid=4086 uid=500 auid=500 ses=
171 subj=system_u:system_r:crond_t:s0-s0:c0.c1023 msg='op=PAM:setcred acct="trai
nee" exe="/usr/sbin/crond" hostname=? addr=? terminal=cron res=success'
----
time->Wed Dec  4 20:24:01 2013
type=USER_END msg=audit(1386185041.397:32): user pid=4086 uid=500 auid=500 ses=1
71 subj=system_u:system_r:crond_t:s0-s0:c0.c1023 msg='op=PAM:session_close acct=
"trainee" exe="/usr/sbin/crond" hostname=? addr=? terminal=cron res=success'
----
time->Wed Dec  4 20:25:01 2013
type=CRED_DISP msg=audit(1386185101.537:37): user pid=4095 uid=500 auid=500 ses=
--More--
```

Command Line Switches

The command line switches for the ausearch command are :

```
[root@centos ~]# ausearch --help
usage: ausearch [options]
    -a,--event <Audit event id>    search based on audit event id
    -c,--comm  <Comm name>        search based on command line name
    -e,--exit  <Exit code or errno>    search based on syscall exit code
```

```
    -f,--file  <File name>        search based on file name
    -ga,--gid-all <all Group id>    search based on All group ids
    -ge,--gid-effective <effective Group id>  search based on Effective
                    group id
    -gi,--gid <Group Id>        search based on group id
    -h,--help            help
    -hn,--host <Host Name>        search based on remote host name
    -i,--interpret            Interpret results to be human readable
    -if,--input <Input File name>    use this file instead of current logs
    --input-logs            Use the logs even if stdin is a pipe
    --just-one            Emit just one event
    -k,--key  <key string>        search based on key field
    -l, --line-buffered        Flush output on every line
    -m,--message  <Message type>    search based on message type
    -n,--node  <Node name>        search based on machine's name
    -o,--object  <SE Linux Object context> search based on context of object
    -p,--pid  <Process id>        search based on process id
    -pp,--ppid <Parent Process id>    search based on parent process id
    -r,--raw            output is completely unformatted
    -sc,--syscall <SysCall name>    search based on syscall name or number
    -se,--context <SE Linux context> search based on either subject or
                     object
    --session <login session id>    search based on login session id
    -su,--subject <SE Linux context> search based on context of the Subject
    -sv,--success <Success Value>    search based on syscall or event
                    success value
    -te,--end [end date] [end time]    ending date & time for search
    -ts,--start [start date] [start time]    starting data & time for search
    -tm,--terminal <TerMinal>    search based on terminal
    -ua,--uid-all <all User id>    search based on All user id's
    -ue,--uid-effective <effective User id>  search based on Effective
                    user id
    -ui,--uid <User Id>        search based on user id
    -ul,--loginuid <login id>    search based on the User's Login id
```

```
    -uu,--uuid <guest UUID>        search for events related to the virtual
                    machine with the given UUID.
    -v,--version             version
    -vm,--vm-name <guest name>    search for events related to the virtual
                    machine with the name.
    -w,--word              string matches are whole word
    -x,--executable  <executable name>  search based on excutable name
```

<note important> For more information on the audit system, please see the **auditd**, **auditctl**, **audispd**, **aureport** and **ausearch** manuals. </note>

Applications

Certain applications manage their own log files directly, for example:

- cups,
- httpd,
- samba,
- ...

```
[root@centos ~]# ls -l /var/log
total 2328
-rw-------. 1 root root   2368 Oct 25 09:41 anaconda.ifcfg.log
-rw-------. 1 root root  20136 Oct 25 09:41 anaconda.log
-rw-------. 1 root root  26479 Oct 25 09:41 anaconda.program.log
-rw-------. 1 root root 129927 Oct 25 09:41 anaconda.storage.log
-rw-------. 1 root root  40453 Oct 25 09:41 anaconda.syslog
-rw-------. 1 root root  57009 Oct 25 09:41 anaconda.xlog
-rw-------. 1 root root  94561 Oct 25 09:41 anaconda.yum.log
drwxr-x---. 2 root root   4096 Dec  4 20:22 audit
-rw-r--r--. 1 root root   2359 Dec  5 09:25 boot.log
-rw-------. 1 root utmp      0 Dec  3 15:40 btmp
-rw-------. 1 root utmp      0 Nov  4 14:03 btmp-20131203
```

```
drwxr-xr-x. 2 root root   4096 Oct 25 09:47 ConsoleKit
-rw-------. 1 root root  64188 Dec  5 09:45 cron
-rw-------. 1 root root 140524 Nov  4 14:03 cron-20131104
-rw-------. 1 root root  30483 Dec  3 15:40 cron-20131203
drwxr-xr-x. 2 lp   sys    4096 Aug 17 12:19 cups
-rw-r--r--. 1 root root  22097 Dec  5 09:24 dmesg
-rw-r--r--. 1 root root  22097 Dec  4 17:52 dmesg.old
-rw-r--r--. 1 root root 343566 Oct 25 10:36 dracut.log
drwxrwx--T. 2 root gdm    4096 Dec  5 09:25 gdm
-rw-r--r--. 1 root root 147168 Oct 28 18:24 lastlog
-rw-------. 1 root root   3052 Dec  5 09:25 maillog
-rw-------. 1 root root   3005 Nov  3 17:02 maillog-20131104
-rw-------. 1 root root    956 Dec  3 14:47 maillog-20131203
-rw-------. 1 root root 178920 Dec  5 09:36 messages
-rw-------. 1 root root 482087 Nov  4 14:00 messages-20131104
-rw-------. 1 root root  85315 Dec  3 15:18 messages-20131203
drwxr-xr-x. 2 ntp  ntp    4096 Feb 22  2013 ntpstats
-rw-r--r--. 1 root root     87 Dec  5 09:25 pm-powersave.log
drwx------. 2 root root   4096 Aug 23  2010 ppp
drwxr-xr-x. 2 root root   4096 Oct 25 18:07 prelink
drwxr-xr-x. 2 root root   4096 Dec  5 09:24 sa
drwx------. 3 root root   4096 Sep 10 11:40 samba
-rw-------. 1 root root   8744 Dec  5 09:39 secure
-rw-------. 1 root root  21027 Nov  4 13:55 secure-20131104
-rw-------. 1 root root   1926 Dec  3 14:48 secure-20131203
-rw-------. 1 root root   4247 Dec  5 09:25 spice-vdagent.log
-rw-------. 1 root root      0 Dec  3 15:40 spooler
-rw-------. 1 root root      0 Oct 25 09:36 spooler-20131104
-rw-------. 1 root root      0 Nov  4 14:03 spooler-20131203
drwxr-x---. 2 root root   4096 Sep 19 11:08 sssd
-rw-------. 1 root root      0 Oct 25 09:34 tallylog
-rw-r--r--. 1 root root 159862 Oct 25 10:45 vboxadd-install.log
-rw-r--r--. 1 root root     73 Oct 25 10:45 vboxadd-install-x11.log
-rw-rw-r--. 1 root root    142 Oct 25 10:45 VBoxGuestAdditions.log
```

```
-rw-rw-r--. 1 root root    141 Oct 25 10:45 VBoxGuestAdditions-uninstall.log
-rw-r--r--. 1 root root      0 Oct 25 09:44 wpa_supplicant.log
-rw-rw-r--. 1 root utmp  87552 Dec  5 09:38 wtmp
-rw-r--r--. 1 root root  41304 Dec  5 09:38 Xorg.0.log
-rw-r--r--. 1 root root  50764 Dec  4 22:12 Xorg.0.log.old
-rw-r--r--. 1 root root  57535 Oct 25 09:46 Xorg.9.log
-rw-------. 1 root root  11877 Nov  8 14:54 yum.log
```

rsyslog

rsyslog, centralises system logs by using the **rsyslog** daemon.

rsyslog is an improved version of syslogd and adds additional functionality:

- the use of the TCP protocol,
- high availability,
- MySQL and PostgreSQL backends.

The messages sent to rsyslog are tagged with a **Facility** and a **Priority**. Together they are refered to as a **Selector**.

rsyslog decides what to do when it receives messages in accordance with its configuration file. rsyslog can:

- ignore the information,
- send the information to another machine (for example, **@machine2**),
- write the information to a file on disk (for example, **/var/log/messages**),
- send the information to a specific user (for example **root**),
- send the information to all connected users,
- send the information to another application via a tube.

The rsyslog daemon is configured by the **/etc/sysconfig/rsyslog** file:

```
[root@centos ~]# cat /etc/sysconfig/rsyslog
# Options for rsyslogd
```

```
# Syslogd options are deprecated since rsyslog v3.
# If you want to use them, switch to compatibility mode 2 by "-c 2"
# See rsyslogd(8) for more details
SYSLOGD_OPTIONS="-c 5"
```

The **SYSLOGD_OPTIONS** directive specifies the compatibility mode with older versions of syslogd:

Directive	**Version**
SYSLOGD_OPTIONS=“-c 5”	Native mode - no compatibility
SYSLOGD_OPTIONS=“-c 2”	rsyslog V2 - compatibility mode
SYSLOGD_OPTIONS=“-c 0”	syslogd mode

Priorities

Priorities indicate to rsyslog the importance of the message:

Level	**Priority**	**Description**
0	emerg/panic	Unusable system
1	alert	Immediate action required
2	crit	Critical condition
3	err/error	Errors found
4	warning/warn	Warnings present
5	notice	Normal condition - important message
6	info	Normal condition - normal message
7	debug	Normal condition - debug message

Facilities

Facilities indicate to rsyslog where the message originated:

Facility	**Origin**
auth/auth-priv	Security/Authentification sub-system

Facility	Origin
cron	cron or at
daemon	Daemons
kern	Kernel
lpr	Printing sub-system
mail	Mail sub-system
news	News sub-system
syslog	Internal rsyslog
user	Users
uucp	UUCP sub-system
local0 - local7	Applications

/etc/rsyslog.conf

rsyslog is configured by editing the **/etc/rsyslog.conf** file:

```
[root@centos ~]# cat /etc/rsyslog.conf
# rsyslog v5 configuration file

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

#### MODULES ####

$ModLoad imuxsock # provides support for local system logging (e.g. via logger command)
$ModLoad imklog   # provides kernel logging support (previously done by rklogd)
#$ModLoad immark  # provides --MARK-- message capability

# Provides UDP syslog reception
#$ModLoad imudp
#$UDPServerRun 514
```

```
# Provides TCP syslog reception
#$ModLoad imtcp
#$InputTCPServerRun 514


#### GLOBAL DIRECTIVES ####

# Use default timestamp format
$ActionFileDefaultTemplate RSYSLOG_TraditionalFileFormat

# File syncing capability is disabled by default. This feature is usually not required,
# not useful and an extreme performance hit
#$ActionFileEnableSync on

# Include all config files in /etc/rsyslog.d/
$IncludeConfig /etc/rsyslog.d/*.conf


#### RULES ####

# Log all kernel messages to the console.
# 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                                                 *

# 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


# ### begin forwarding rule ###
# The statement between the begin ... end define a SINGLE forwarding
# rule. They belong together, do NOT split them. If you create multiple
# forwarding rules, duplicate the whole block!
# Remote Logging (we use TCP for reliable delivery)
#
# 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.
#$WorkDirectory /var/lib/rsyslog # where to place spool files
#$ActionQueueFileName fwdRule1 # unique name prefix for spool files
#$ActionQueueMaxDiskSpace 1g   # 1gb space limit (use as much as possible)
#$ActionQueueSaveOnShutdown on # save messages to disk on shutdown
#$ActionQueueType LinkedList   # run asynchronously
#$ActionResumeRetryCount -1    # infinite retries if host is down
# remote host is: name/ip:port, e.g. 192.168.0.1:514, port optional
#*.* @@remote-host:514
# ### end of the forwarding rule ###

# A template to for higher precision timestamps + severity logging
$template SpiceTmpl,"%TIMESTAMP%.%TIMESTAMP:::date-subseconds% %syslogtag% %syslogseverity-text%:%msg:::sp-if-
no-1st-sp%%msg:::drop-last-lf%\n"
```

```
:programname, startswith, "spice-vdagent" /var/log/spice-vdagent.log;SpiceTmpl
```

This file is divided into three distinct sections:

- **MODULES**,
  - Contains directives that load modules that offer additional functionality to rsyslog,
- **GLOBAL DIRECTIVES**,
  - Contains the directives that configure the global aspects of rsyslog,
- **RULES**,
  - Contains the directives that tell rsyslog what do do with each selector. The rules compatible with syslogd use the same format as before such as **mail.* -/var/log/maillog** whereas rsyslog rules all start with a **$** character.

<note important> An **Action** preceded by a minus sign takes place asynchronously. Synchronous actions produce more pertinent logs but slow down the system. </note>

Modules

Since version three of rsyslog the data received, known as **inputs**, is managed by modules. Examples of modules are:

Module	**Function**
$ModLoad imuxsock.so	Activates local message logging such as those received from the **logger** command (See below)
$ModLoad imklog.so	Activates **Kernel** message logging
$ModLoad imudp.so	Activates the **UDP** protocol
$ModLoad imtcp.so	Activates the **TCP** protocol

In the **/etc/rsyslog.conf** file the **$ModLoad imuxsock.so** and **$ModLoad imklog.so** modules are active:

```
...
$ModLoad imuxsock # provides support for local system logging (e.g. via logger command)
$ModLoad imklog   # provides kernel logging support (previously done by rklogd)
#$ModLoad immark  # provides --MARK-- message capability

# Provides UDP syslog reception
```

```
#$ModLoad imudp
#$UDPServerRun 514

# Provides TCP syslog reception
#$ModLoad imtcp
#$InputTCPServerRun 514
...
```

In order to receive rsyslog messages from other machines via UDP and TCP, the inactive modules concerned have to be activated. This is acheived by editing the **/etc/rsyslog.conf** file as follows and then restarting the rsyslog service:

```
...
$ModLoad imuxsock # provides support for local system logging (e.g. via logger command)
$ModLoad imklog   # provides kernel logging support (previously done by rklogd)
#$ModLoad immark  # provides --MARK-- message capability

# Provides UDP syslog reception
$ModLoad imudp
$UDPServerRun 514

# Provides TCP syslog reception
$ModLoad imtcp
$InputTCPServerRun 514
...
```

```
[root@centos ~]# service rsyslog restart
Shutting down system logger:                               [  OK  ]
Starting system logger:                                    [  OK  ]
```

<note important> By doing this, **Listeners** are created on port UDP/514 and on port TCP/514. Port 514 is the standard port for rsyslog Listeners. The system administrator can, if required, change this value - for example: **$InputTCPServerRun 1514**. </note>

To do the exact opposite of what has just been configured and send all of the rsyslog messages to a remote-host, the lines in the in the sub-section called **begin forwarding rule** of the **/etc/rsyslog.conf** file neeed to be uncommented:

```
...
# ### begin forwarding rule ###
# The statement between the begin ... end define a SINGLE forwarding
# rule. They belong together, do NOT split them. If you create multiple
# forwarding rules, duplicate the whole block!
# Remote Logging (we use TCP for reliable delivery)
#
# 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.
$WorkDirectory /var/lib/rsyslog # where to place spool files
$ActionQueueFileName fwdRule1 # unique name prefix for spool files
$ActionQueueMaxDiskSpace 1g   # 1gb space limit (use as much as possible)
$ActionQueueSaveOnShutdown on # save messages to disk on shutdown
$ActionQueueType LinkedList   # run asynchronously
$ActionResumeRetryCount -1    # infinite retries if host is down
 remote host is: name/ip:port, e.g. 192.168.0.1:514, port optional
*.* @@remote-host:514
# ### end of the forwarding rule ###
...
```

<note important> Messages are sent to the remote-host using the TCP protocol. For that reason the remote-host must be configured to accept TCP connexions. Finally the ***.*** **@@remote-host:514** directive must be modified so it includes the remote-host's IP address. </note>

Global Directives

Directives in this section configure rsyslog itself. For example, the following directive makes rsyslog log to file using the traditional date and time formats compatible with syslogd as opposed to the newer and more precise rsyslog format:

```
$ActionFileDefaultTemplate RSYSLOG_TraditionalFileFormat
```

Rules

Each rule is of the following format:

```
Selector[; ...]  [-] Action
```

There are three types of Selector:

Facility.Priority

Messages of an equal or higher priority than that which is stipulated will be logged.

Facility!Priority

Messages of a lower priority than that which is stipulated will be logged.

Facility=Priority

Messages of a priority equal to that which is stipulated will be logged.

Using the * Wildcard

A Facility or Priority can also be a *. In this case, all of the values of the Facility or Priority are concerned by the rule. For example: **cron.***.

n Facilities with Identical Priorities

Several Facilities can have the same Priority. In this case the Facilities are seperated by commas. For example: **uucp,news.crit**.

n Selectors with Identical Actions

An Action can apply to several Selectors. In this case the Selectors are seperated by semi-colons. For example: ***.info;mail.none;authpriv.none;cron.none**.

/usr/bin/logger

The **/usr/bin/logger** command is used to write user defined messages to rsyslog.

The command uses the following syntax:

```
logger -p Facility.Priority message
```

Enter the following command line into a terminal:

```
[root@centos ~]# logger -p user.info Linux is great
```

Now use **tail** to view the end of the */var/log/messages **file: <code> [root@centos ~]# tail /var/log/messages Dec 7 11:52:07 centos NetworkManager[1319]: <warn> (eth0): DHCPv4 request timed out. Dec 7 11:52:07 centos NetworkManager[1319]: <info> (eth0): canceled DHCP transaction, DHCP client pid 2660 Dec 7 11:52:07 centos NetworkManager[1319]: <info> Activation (eth0) Stage 4 of 5 (IP4 Configure Timeout) scheduled… Dec 7 11:52:07 centos NetworkManager[1319]: <info> Activation (eth0) Stage 4 of 5 (IP4 Configure Timeout) started… Dec 7 11:52:07 centos NetworkManager[1319]: <info> (eth0): device state change: 7 → 9 (reason 5) Dec 7 11:52:07 centos NetworkManager[1319]: <warn> Activation (eth0) failed. Dec 7 11:52:07 centos NetworkManager[1319]: <info> Activation (eth0) Stage 4 of 5 (IP4 Configure Timeout) complete. Dec 7 11:52:07 centos NetworkManager[1319]: <info> (eth0): device state change: 9 → 3 (reason 0) Dec 7 11:52:07 centos NetworkManager[1319]: <info> (eth0): deactivating device (reason: 0). Dec 7 12:14:15 centos trainee: Linux is great </code> <note important> Note that in the above file, the message comes from** trainee **even though trainee was root when the command was executed. </note> ==== Command Line Switches==== The command line switches for the logger command are: <code> [root@centos ~]# logger –help logger: invalid option – '-' usage: logger [-is] [-f file] [-p pri] [-t tag] [-u socket] [message …] </code> =====/usr/sbin/logrotate===== Log files can grow quickly in size. The** /usr/sbin/logrotate

command is used to rotate log files in accordance with the configuration in the /etc/logrotate.conf **file: <code> [root@centos ~]# cat /etc/logrotate.conf # see “man logrotate” for details # 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 # RPM packages drop log rotation information into this directory include /etc/logrotate.d # no packages own wtmp and btmp – we'll rotate them here /var/log/wtmp { monthly create 0664 root utmp minsize 1M rotate 1 } /var/log/btmp { missingok monthly create 0600 root utmp rotate 1 } # system-specific logs may be also be configured here. </code> In the first part of this file can be found the directives to be applied to all log files except** wtmp **and** btmp**:** * weekly **- rotate logs weekly,** * rotate 4 **- keep 4 weeks worth of backlogs,** * create **- create new (empty) log files after rotating old ones,** * dateext **- use date as a suffix of the rotated file,** * include /etc/logrotate.d **- RPM packages drop log rotation information into this directory so that the configuration is appended to the** /etc/logrotate.conf **file. Uncomment the** compress** directive and save the file:

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

Command Line Switches

The command line switches for the logrotate command are:

```
[root@centos ~]# logrotate --help
Usage: logrotate [OPTION...] <configfile>
  -d, --debug               Don't do anything, just test (implies -v)
  -f, --force               Force file rotation
  -m, --mail=command        Command to send mail (instead of `/bin/mail')
  -s, --state=statefile     Path of state file
  -v, --verbose             Display messages during rotation

Help options:
  -?, --help                Show this help message
  --usage                   Display brief usage message
```

~~DISCUSSION:off~~