HugeServer Knowledgebase

Working with Logs on Linux

on April 28, 2017 (https://www.hugeserver.com/kb/linux-log-centos-debian-ubuntu/) by Amir

Leave a comment (https://www.hugeserver.com/kb/linux-log-centos-debian-ubuntu/#respond)

Introduction

If you spend a lot of time in Linux environment, it is essential that you know where the log files are located, log files duty is to help you troubleshoot an issue. When your systems are running smoothly, take some time to learn and understand the content of various log files, which will help you when there is a crisis and you have to look through the log files to identify the issue. there are plenty of logs to be found: logs for the system, logs for the kernel, for package managers, for the boot process, Apache, MySQL, etc. Most log files can be found in one convenient location “/var/log”. These are all system and service logs, those which you will lean on heavily when there is an issue with your operating system or one of the major services. Fortunately, there are many ways that you can view your system logs, all quite simply executed from the command line.

We are assuming that you have root permission, otherwise, you may start commands with “sudo”.

Log files location

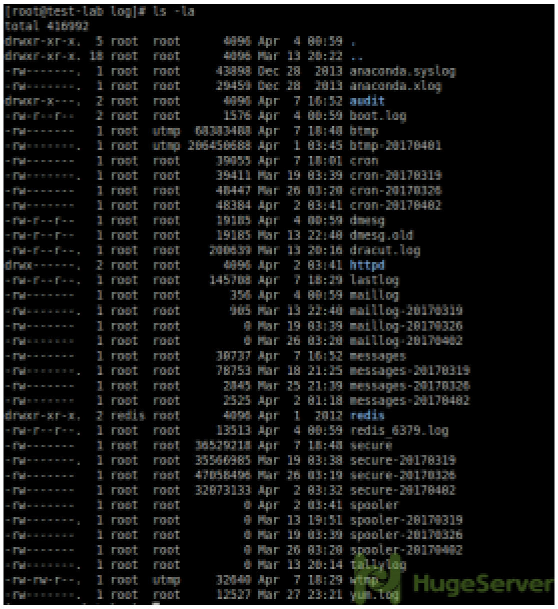
Almost all log files are located in “/var/log/” directory and it’s sub-directories by default, you can use the following command to enter the “log” directory:

```
# cd /var/log
```

Now you can see what is in your log directory, using:

```
# ls -la
```

The output should be something like the picture below:



```
[root@test-lab log]# ls -la
total 416992
drwxr-xr-x.  5 root  root       4096 Apr  4 00:59 .
drwxr-xr-x. 18 root  root       4096 Mar 13 20:22 ..
-rw-------.  1 root  root      43898 Dec 28  2013 anaconda.syslog
-rw-------.  1 root  root      29459 Dec 28  2013 anaconda.xlog
drwxr-x---.  2 root  root       4096 Apr  7 16:52 audit
-rw-r--r--   2 root  root       1576 Apr  4 00:59 boot.log
-rw-------   1 root  utmp   68383488 Apr  7 18:48 btmp
-rw-------.  1 root  utmp  206450688 Apr  1 03:45 btmp-20170401
-rw-------   1 root  root      39055 Apr  7 18:01 cron
-rw-------.  1 root  root      39411 Mar 19 03:39 cron-20170319
-rw-------   1 root  root      40447 Mar 26 03:20 cron-20170326
-rw-------   1 root  root      48384 Apr  2 03:41 cron-20170402
-rw-r--r--   1 root  root      19185 Apr  4 00:59 dmesg
-rw-r--r--   1 root  root      19185 Mar 13 22:40 dmesg.old
-rw-r--r--.  1 root  root     200639 Mar 13 20:16 dracut.log
drwx------.  2 root  root       4096 Apr  2 03:41 httpd
-rw-r--r--.  1 root  root     145708 Apr  7 18:29 lastlog
-rw-------   1 root  root        356 Apr  4 00:59 maillog
-rw-------.  1 root  root        905 Mar 13 22:40 maillog-20170319
-rw-------   1 root  root          0 Mar 19 03:39 maillog-20170326
-rw-------   1 root  root          0 Mar 26 03:20 maillog-20170402
-rw-------   1 root  root      30737 Apr  7 16:52 messages
-rw-------.  1 root  root      78753 Mar 18 21:25 messages-20170319
-rw-------   1 root  root       2845 Mar 25 21:39 messages-20170326
-rw-------   1 root  root       2525 Apr  2 01:18 messages-20170402
drwxr-xr-x.  2 redis root       4096 Apr  1  2012 redis
-rw-r--r--.  1 root  root      13513 Apr  4 00:59 redis_6379.log
-rw-------   1 root  root   36529218 Apr  7 18:48 secure
-rw-------.  1 root  root   35566985 Mar 19 03:38 secure-20170319
-rw-------   1 root  root   47058496 Mar 26 03:19 secure-20170326
-rw-------   1 root  root   32073133 Apr  2 03:32 secure-20170402
-rw-------   1 root  root          0 Apr  2 03:41 spooler
-rw-------.  1 root  root          0 Mar 13 19:51 spooler-20170319
-rw-------   1 root  root          0 Mar 19 03:39 spooler-20170326
-rw-------   1 root  root          0 Mar 26 03:20 spooler-20170402
-rw-------.  1 root  root          0 Mar 13 20:14 tallylog
-rw-rw-r--.  1 root  utmp      32640 Apr  7 18:29 wtmp
-rw-------.  1 root  root      12527 Mar 27 23:21 yum.log
```

For example, you can see “httpd” directory, it’s pretty specific that you can find your “Apache” log file in that directory.

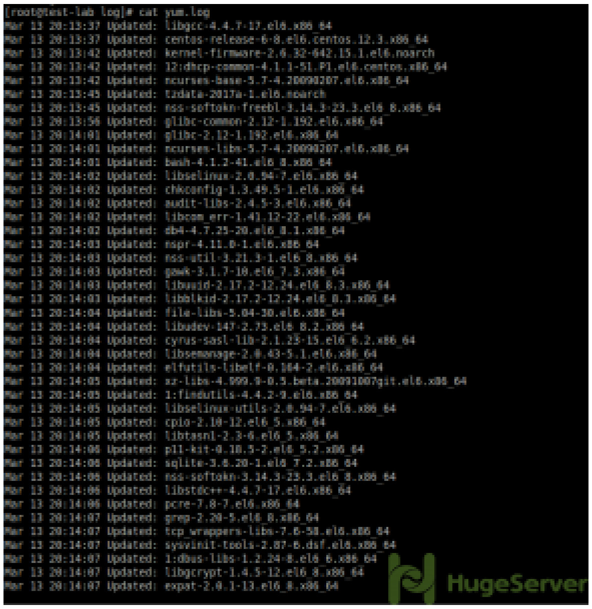
Reading Log files

There are many commands for reading log files and each one of them has a different purpose.

“cat” Command

You can easily “cat” a log file to simply open it. it’s the easiest way to open a log file but it’s not very handy, Let’s see an example of the output(we are going to cat the “yum.log” as an example)

```
# cat yum.log
```



```
[root@test-lab log]# cat yum.log
Mar 13 20:13:37 Updated: libgcc-4.4.7-17.el6.x86_64
Mar 13 20:13:37 Updated: centos-release-6-8.el6.centos.12.3.x86_64
Mar 13 20:13:42 Updated: kernel-firmware-2.6.32-642.15.1.el6.noarch
Mar 13 20:13:42 Updated: 12:dhcp-common-4.1.1-51.P1.el6.centos.x86_64
Mar 13 20:13:42 Updated: ncurses-base-5.7-4.20090207.el6.x86_64
Mar 13 20:13:45 Updated: tzdata-2017a-1.el6.noarch
Mar 13 20:13:45 Updated: nss-softokn-freebl-3.14.3-23.3.el6_8.x86_64
Mar 13 20:13:56 Updated: glibc-common-2.12-1.192.el6.x86_64
Mar 13 20:14:01 Updated: glibc-2.12-1.192.el6.x86_64
Mar 13 20:14:01 Updated: ncurses-libs-5.7-4.20090207.el6.x86_64
Mar 13 20:14:01 Updated: bash-4.1.2-41.el6_8.x86_64
Mar 13 20:14:02 Updated: libselinux-2.0.94-7.el6.x86_64
Mar 13 20:14:02 Updated: chkconfig-1.3.49.5-1.el6.x86_64
Mar 13 20:14:02 Updated: audit-libs-2.4.5-3.el6.x86_64
Mar 13 20:14:02 Updated: libcom_err-1.41.12-22.el6.x86_64
Mar 13 20:14:02 Updated: db4-4.7.25-20.el6_8.1.x86_64
Mar 13 20:14:03 Updated: nspr-4.11.0-1.el6.x86_64
Mar 13 20:14:03 Updated: nss-util-3.21.3-1.el6_8.x86_64
Mar 13 20:14:03 Updated: gawk-3.1.7-10.el6_7.3.x86_64
Mar 13 20:14:03 Updated: libuuid-2.17.2-12.24.el6_8.3.x86_64
Mar 13 20:14:03 Updated: libblkid-2.17.2-12.24.el6_8.3.x86_64
Mar 13 20:14:04 Updated: file-libs-5.04-30.el6.x86_64
Mar 13 20:14:04 Updated: libudev-147-2.73.el6_8.2.x86_64
Mar 13 20:14:04 Updated: cyrus-sasl-lib-2.1.23-15.el6_6.2.x86_64
Mar 13 20:14:04 Updated: libsemanage-2.0.43-5.1.el6.x86_64
Mar 13 20:14:04 Updated: elfutils-libelf-0.164-2.el6.x86_64
Mar 13 20:14:05 Updated: xz-libs-4.999.9-0.5.beta.20091007git.el6.x86_64
Mar 13 20:14:05 Updated: 1:findutils-4.4.2-9.el6.x86_64
Mar 13 20:14:05 Updated: libselinux-utils-2.0.94-7.el6.x86_64
Mar 13 20:14:05 Updated: cpio-2.10-12.el6_5.x86_64
Mar 13 20:14:05 Updated: libtasn1-2.3-6.el6_5.x86_64
Mar 13 20:14:06 Updated: p11-kit-0.18.5-2.el6_5.2.x86_64
Mar 13 20:14:06 Updated: sqlite-3.6.20-1.el6_7.2.x86_64
Mar 13 20:14:06 Updated: nss-softokn-3.14.3-23.3.el6_8.x86_64
Mar 13 20:14:06 Updated: libstdc++-4.4.7-17.el6.x86_64
Mar 13 20:14:06 Updated: pcre-7.8-7.el6.x86_64
Mar 13 20:14:07 Updated: grep-2.20-5.el6_8.x86_64
Mar 13 20:14:07 Updated: tcp_wrappers-libs-7.6-58.el6.x86_64
Mar 13 20:14:07 Updated: sysvinit-tools-2.87-6.dsf.el6.x86_64
Mar 13 20:14:07 Updated: 1:dbus-libs-1.2.24-8.el6_6.x86_64
Mar 13 20:14:07 Updated: libgcrypt-1.4.5-12.el6_8.x86_64
Mar 13 20:14:07 Updated: expat-2.0.1-13.el6_8.x86_64
```

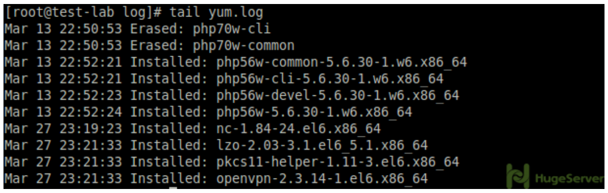
With the cat command, you can see all the log file statically.

“tail” Command

The handiest command that you can use to see your log file is the “tail” command.

If you use the “tail” command with no flags it will show you the last 10 lines of your log file:

```
# tail yum.log
```



```
[root@test-lab log]# tail yum.log
Mar 13 22:50:53 Erased: php70w-cli
Mar 13 22:50:53 Erased: php70w-common
Mar 13 22:52:21 Installed: php56w-common-5.6.30-1.w6.x86_64
Mar 13 22:52:21 Installed: php56w-cli-5.6.30-1.w6.x86_64
Mar 13 22:52:23 Installed: php56w-devel-5.6.30-1.w6.x86_64
Mar 13 22:52:24 Installed: php56w-5.6.30-1.w6.x86_64
Mar 27 23:19:23 Installed: nc-1.84-24.el6.x86_64
Mar 27 23:21:33 Installed: lzo-2.03-3.1.el6_5.1.x86_64
Mar 27 23:21:33 Installed: pkcs11-helper-1.11-3.el6.x86_64
Mar 27 23:21:33 Installed: openvpn-2.3.14-1.el6.x86_64
```

You can see “tail” flags with the command below:

```
# tail --help
```

The basic format of “tail” command:

```
# tail [FLAG] [FILENAME]
```

If you want to see the last 100 line of your log file you can execute:

```
# tail -n 100 yourlog.log
```

The most important flag is the “-f” flag, it will allow you to see your log file live which means the output appended data as the file grows.

```
# tail -f yourlog.log
```

“more” and “less” Command

You can use the “more” command to see your log file page by page and navigate to forward by hitting space:

```
# more yourlog.log
```

“less” is much the same as more command except:

1. You can navigate the file up/down line by line with arrow keys.

2. You can search for string using “/keyword“.
3. And it uses the “vi” editors commands and shortkeys.

```
# less yourlog.log
```

“head” Command

“head” command will show the first 10 lines of your file:

```
# head yourlog.log
```

Combining grep command with other commands

You can add “grep” command if you are seeking for some specific content in your log files such as an IP or a special error:

```
# cat yourlog.log | grep IP
```

```
# tail -f yourlog.log | grep errorname
```

If you are searching for a specific word in your log file meanwhile you want to see the whole content you may use grep like below:

```
# grep --color [PATTERN] yourlog.log
```

“sort” Command

You can sort the output of your log file with the “sort” command, this command can sort your data by many things:

Using the command below will sort your file alphabetically:

```
# sort yourlog.log
```

If you add “-r” flag it will sort your data alphabetically but in reverse order:

```
# sort -r yourlog.log
```

“-n” flag will sort your data from lowest number to highest (if your data contains numbers for each item):

```
# sort -n prices.log
```

You can always use the following command to see all of sort flags:

```
# sort --help
```

“awk” Command

The awk command is a powerful method for processing or analyzing text files, in particular, data files that are organized by lines (rows) and columns.

The basic “awk” format is:

```
awk 'pattern {action}' input-file
```

This means: take each line of the input file if the line contains the pattern apply the action to the line and print the resulting line.
If the pattern is omitted, the action is applied to all lines.

For example:

```
# awk '{ print $5 }' yourlog.log
```

This statement takes the element of the 5th column of each line and prints it as a line in your shell.

```
# awk '/30/ { print $3 }' yourlog.log
```

The string between the two slashes (‘/’) is the diameter. In this case, it is just the string “30”. This means if a line contains the string “30”, the system prints out the element in the 3rd column of that line.
The “awk” command can do very complicated things if you want to learn more about “awk” you can read the user manual with the command below:

```
# man awk
```

“uniq” Command

Uniq command is helpful to remove or detect duplicate entries in a file. This section explains few most frequently used uniq command line options that you might find helpful.

The basic “uniq” format is:

```
# uniq [-options]
```

when uniq command is run without any option, it removes duplicate lines and displays unique lines.

```
# uniq yourlog.log
```

The “-c” flag is to count the occurrence of lines in the file.

```
# uniq -c yourlog.log
```

This flag will print only unique lines in the file.

```
# uniq -u yourlog.log
```

Useful combo commands

As you might know, you can combine the commands that you saw in the previous sections and make very useful and handy commands. here we are going to point to some of them:

```
# cat yourlog.log |awk -F" " '{print $5}'
```

This command will show you the 5th column that separated with (” “).

```
# cat /var/log/yourlog.log | awk -F" " '{print $1}' | uniq -c | sort -n
```

This command will show you the first column that separated with and sort them from lowest to highest with the value of occurrence.

Common Linux log files and usage

```
/var/log/messages : General message and system related stuff
```

```
/var/log/auth.log : Authentication logs
```

```
/var/log/kern.log : Kernel logs
```

```
  /var/log/maillog : Mail server logs
```

```
  /var/log/httpd/ : Apache access and error logs directory
```

```
  /var/log/boot.log : System boot log
```

```
  /var/log/mysqld.log : MySQL database server log files
```

```
  /var/log/utmp   OR   /var/log/wtmp : Login records
```

Going Further

Until now we are just got to know how to read log files, but after the reading section there is a more important thing about log files and it’s how to organize them. if you don’t use an organization solution, you will be facing a lot of problems after a while. In this section, we are going to point to two of the most effective and popular ways to organize your log files.

Log rotation

Logrotate is a tool that can remove, compress and rotate your log files regularly. Logrotare is able to rotate your log files as they grow too large or even you can configure it to do it daily, monthly etc. By default Logrotate invoked daily as a cron job.

Syslog Server

A Syslog server represents a central log monitoring point on a network, to which all kinds of devices including Linux or Windows servers, routers, switches or any other hosts can send their logs over a network. By setting up a Syslog server, you can filter and consolidate logs from different hosts and devices into a single location, so that you can view and archive important log messages more easily.

On most Linux distributions, rsyslog is the standard Syslog daemon that comes pre-installed. Configured in a client/server architecture, rsyslog can play both roles, as a Syslog server rsyslog can gather logs from other devices, and as a Syslog client, rsyslog can transmit its internal logs to a remote Syslog server.

Was this tutorial helpful?

○ ○

Similar Posts

How to monitor Services with Monit on CentOS 7 (https://www.hugeserver.com/kb/how-monitor-services-monit-centos7/)
How to install Apache CouchDB on CentOS 7 (https://www.hugeserver.com/kb/install-apache-couchdb-centos-7/)
How to install Apache CouchDB on Ubuntu 16.04 (https://www.hugeserver.com/kb/how-install-apache-couchdb-ubuntu-16/)
How to install CodeIgniter with Apache, PHP 7.1, and MariaDB 10.2 on Ubuntu 16.04 (https://www.hugeserver.com/kb/how-install-codeigniter-apache-php7-mariadb10-ubuntu16/)
How to install Moodle on Ubuntu 16.04 (https://www.hugeserver.com/kb/how-install-moodle-ubuntu-16/)

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment

Name *

Email *

Website

Post Comment

Services

Dedicated Server (/dedicated-servers/)

Colocation (/colocation/)

Hybrid Server (/hybrid-servers/)

Virtual Server (/virtual-servers/)

FAQ (/about/faq/)

Solutions

Virtualization (/solutions/virtualization/)

Hardware Solutions (/solutions/hardware/)

Software Solutions (/solutions/software/)

Administration (/solutions/administration/)

Company

About HugeServer (/about/)

ION Platform (/about/ion/)

Datacenters (/datacenters/)

Network (/about/network/)

Contact us (/about/contact-us/)

(https:/(/twpis:e/htowm/fHaugeS/ekvedgo/ohgueg.coemr)e(hy/2534297)

E-mail (mailto:sales@hugeserver.com) **Live Chat** **1.888.842.8570**

Privacy (/legal/privacy/) AUP (/legal/aup/) TOS (/legal/tos/) DMCA (/legal/dmca/)