Standard view on logs

Before systemd, we used to work with plain text logs only. Well, it is some generalisation, but in fact, all system logs of Linux were stored as plain text. Some of them still are.

Let's navigate to default log directory and take a look.

cd /var/log

ls -al

As mentioned, /var/log is the default location in all Linux systems for logs. Let's discuss some theory here. The best practice is to have /var/log as separate filesystem, not just directory. What it means? Filesystem is a layer, or structured collection of data in partition on disk drive. Partitions separate these layers. And this is what is enough for now :)

I used this time, to keep you busy reading, while system is preparing the needed log structure :)

So, we listed the directory. We see different files, so let me explain what is what.

|  |  |
| --- | --- |
| **Log name** | **Purpose** |
| syslog | The main system log. Contains all important information about the system and applications. Generally, if something is not writting its own logs, it will be here, in syslog. |
| auth.log | Contains information about authorizations. All user login attempts (with information if successful or not), logout, password changes, remote logins and use of sudo. |
| dmesg | is a kernel ring buffer, not the log (as we understand the logs). It allows us to interact with kernel and get information by querying bootup messages. It doesn't mean, that dmesg contains the booting data, but everything what is going on during the system's work. |
| kern.log | Stores Kernel messages |
| boot.log | Contains system' starting sequence (not kernel boot). Another words, information about started services, applications, disks configurations and so on. |
| lastlog | file to be used with lastlog utility. Contains information abount last logins |
| faillog | similar to lastlog, use this file with faillog utility. Logs fails, like login failures |
| wtmp.log | Contains login infomration. However, it doesn't show information similar to lastlog, but used by other utilities, like who. |
| dpkg.log | Contains data about packages management - install, remove, update, etc. |

These are system logs. Another type of logs are applications logs. Generally, these logs are stored in their directories inside /var/log, like Nginx logs, for example. Let's see it.

ls -al /var/log/nginx

Here we have nginx directory with its logs.

Watch the logs

How to check what is inside the logs? Except binary logs (like lastlog), all logs are text files. Therefore, it is very easy to read them.

cat /var/log/dpkg.log  
tail /var/log/syslog

We have two examples above. All text operations, like cat, less, more, head, tail, grep, etc, work here!

Let's take a look for our Nginx logs.

cat /var/log/nginx/access.log

We can do some requests, using the web browser. Simply click the link

[Open web browser](https://242a7bbe-ffcf-4ac9-986a-968b2fda7cc5-10-244-6-245-80.spch.r.killercoda.com/)

And repeat cat /var/log/nginx/access.log

Hmm... Yes, we see more logs, but it is... unhandy to check, if we want to observe continuously what is logged in the file.

Luckily, tail has very nice argument. With -f we are able to keep the stream open and see all new messages on the screen. If we want to quit, press CTRL c.

tail -f /var/log/nginx/access.log

Pushing messages to log

We are able to "inject" messages to the log files. one of the possibility is to use logger command. This example will simply add the line to the syslog file.

tail /var/log/syslog  
logger "This is a test message"  
tail /var/log/syslog

## ansible.cfg

First, please execute the following command.

ansible --version