

Introduction to Linux System Logging (with rsyslogd)

Andre M. Maier
Elektronikschule Tettnang

`andre.maier@elektronikschule.de`

This work is licensed under a [Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License](https://creativecommons.org/licenses/by-nc-nd/4.0/).



Why is logging important?

- Debugging
- System Security
- Quality Management

Warning!

Experienced hackers are interested in gaining access to system logs, so all logfiles are subject to protection!

What information does a logfile contain?

Diagram illustrating the structure of a log entry with labels and arrows pointing to the corresponding fields in the first line of the log output:

- Date and Time
- Hostname
- Source
- Rel. Timestamp (/proc/uptime)
- Message

```
Jul  2 20:05:02 turing kernel: [ 4606.325527] usb 3-2: new high-speed USB device
number 7 using xhci_hcd
Jul  2 20:05:02 turing kernel: [ 4606.341992] usb 3-2: New USB device found,
idVendor=04f9, idProduct=003f
Jul  2 20:05:02 turing kernel: [ 4606.341997] usb 3-2: New USB device strings:
Mfr=1, Product=2, SerialNumber=3
Jul  2 20:05:02 turing kernel: [ 4606.342000] usb 3-2: Product: HL-2130 series
Jul  2 20:05:02 turing kernel: [ 4606.342002] usb 3-2: Manufacturer: Brother
Jul  2 20:05:02 turing kernel: [ 4606.342004] usb 3-2: SerialNumber: H1N601257
Jul  2 20:05:02 turing mtp-probe: checking bus 3, device 7:
"/sys/devices/pci0000:00/0000:00:14.0/usb3/3-2"
Jul  2 20:05:02 turing mtp-probe: bus: 3, device: 7 was not an MTP device
Jul  2 20:05:02 turing kernel: [ 4606.381675] usb_lpm 3-2:1.0: usb_lpm: USB
Bidirectional printer dev 7 if 0 alt 0 proto 2 vid 0x04F9 pid 0x003F
Jul  2 20:05:02 turing kernel: [ 4606.381698] usbcore: registered new interface
driver usb_lpm
```

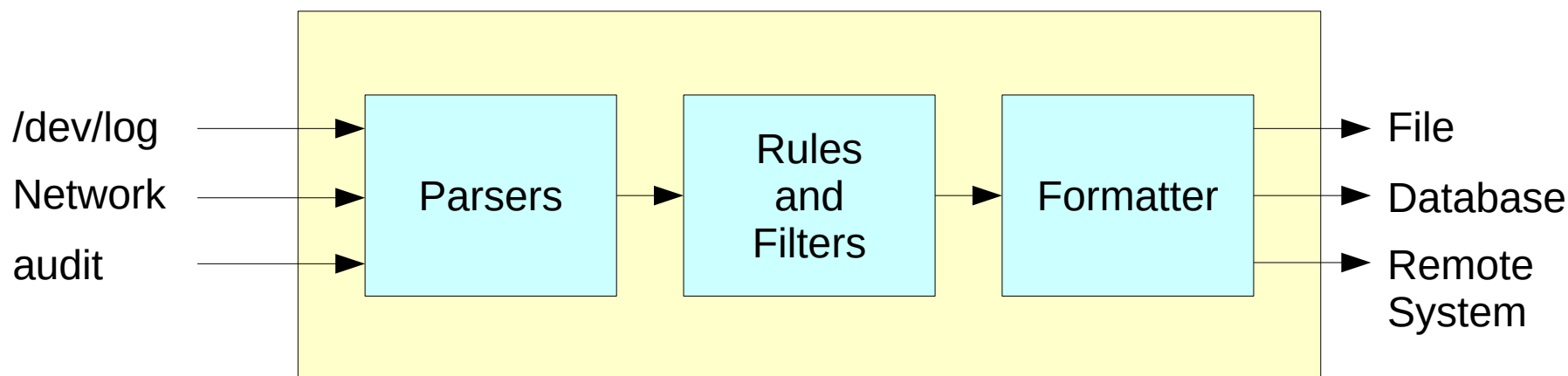
Logfiles

- `/var/log`
 - contains all kinds of logfiles
 - should be located on a separate partition
- Logfile names may vary between distributions.
- Example (Ubuntu):

<code>auth.log</code>	System authentication (e.g. <code>sudo</code> , <code>login</code> , ...)
<code>boot.log</code>	Booting process
<code>dmesg</code>	Kernel ringbuffer
<code>dpkg.log</code>	Package management
<code>kern.log</code>	Kernel messages
<code>syslog</code>	Global system messages (including information from other logfiles)

(r)syslogd

- is the daemon responsible for logging
- offers a large number of features



Configuring (r)syslogd

- Configuration files
 - /etc/rsyslog.conf
 - files in /etc/rsyslog.d
- Example (excerpt):

kern.*	/var/log/kern.log
kern.crit	@192.168.178.24
kern.crit	/dev/console
kern.info	/var/log/kernelinfo.log



Facility



Priority



Action

Facilities, Priorities, and Actions

- Facilities
 - auth, authpriv, cron, daemon, kern, lpr, mail, mark, news, security, syslog, user, uucp, local0 ... local7
 - Asterisk (*) refers to all facilities
- Priorities
 - debug, info, notice, warning, err, crit, alert, emerg
 - error, warn, and panic are deprecated
 - Asterisk (*) refers to all priorities
- Actions
 - Most commonly, the action is a filename in /var/log
 - Asterisk (*) means all logged-in users

Generating Logs from bash

- logger command

Example: `logger "Hi there!"`

NAME

`logger` – a shell command interface to the `syslog(3)` system log module

SYNOPSIS

```
logger [-dhisV] [-f file] [-n server] [-P port] [-p pri]
        [-t tag] [-u socket] [message]
```

DESCRIPTION

`logger` makes entries in the system log. It provides a shell command interface to the `syslog(3)` system log module.

Generating Logs in C

- Example:

```
#include <syslog.h>
```

```
int main( int argc, char** argv )  
{
```

```
    setlogmask( LOG_UPTO( LOG_NOTICE ) );
```

```
    openlog( "demoprogram", LOG_CONS | LOG_PID |  
            LOG_NDELAY, LOG_LOCAL1 );
```

```
    syslog( LOG_NOTICE, "Program started by user %d",  
            getuid() );
```

```
    syslog( LOG_INFO, "Hi there!" );
```

```
    closelog();
```

```
    return 0;
```

```
}
```

logrotate

- is a tool designed to simplify the administration of log files
- allows to rotate, compress, mail, ... logfiles
- is usually run automatically (cronjob) on a daily basis
- Configuration files
 - /etc/logrotate.conf
 - files in /etc/logrotate.d