

WIZ - EXHIBIT 1117
Wiz, Inc. v. Orca Security Ltd.



≡ Menu

- [Home](#)
- [Free eBook](#)
- [Start Here](#)
- [Contact](#)
- [About](#)

20 Linux Log Files that are Located under /var/log Directory

by Ramesh Natarajan on August 1, 2011

Like 4

If you spend lot of time in Linux environment, it is essential that you know where the log files are located, and what is contained in each and every log file.

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.

/etc/rsyslog.conf controls what goes inside some of the log files. For example, following is the entry in rsyslog.conf for /var/log/messages.

```
$ grep "/var/log/messages" /etc/rsyslog.conf
*.info;mail.none;authpriv.none;cron.none                /var/log/messages
```

In the above output,

- *.info indicates that all logs with type INFO will be logged.
- mail.none,authpriv.none,cron.none indicates that those error messages should not be logged into the /var/log/messages file.
- You can also specify *.none, which indicates that none of the log messages will be logged.

The following are the 20 different log files that are located under /var/log/ directory. Some of these log files are distribution specific. For example, you'll see dpkg.log on Debian based systems (for example, on Ubuntu).

1. **/var/log/messages** – Contains global system messages, including the messages that are logged during system startup. There are several things that are logged in /var/log/messages including mail, cron, daemon, kern, auth, etc.
2. **/var/log/dmesg** – Contains kernel ring buffer information. When the system boots up, it prints number of messages on the screen that displays information about the hardware devices that the kernel detects during boot process. These messages are available in kernel ring buffer and whenever the new message comes the old message gets overwritten. You can also view the content of this file using the [dmesg command](#).

3. **/var/log/auth.log** – Contains system authorization information, including user logins and authentication mechanisms that were used.
4. **/var/log/boot.log** – Contains information that are logged when the system boots
5. **/var/log/daemon.log** – Contains information logged by the various background daemons that runs on the system
6. **/var/log/dpkg.log** – Contains information that are logged when a package is installed or removed using [dpkg command](#)
7. **/var/log/kern.log** – Contains information logged by the kernel. Helpful for you to troubleshoot a custom-built kernel.
8. **/var/log/lastlog** – Displays the recent login information for all the users. This is not an ascii file. You should use lastlog command to view the content of this file.
9. **/var/log/maillog** **/var/log/mail.log** – Contains the log information from the mail server that is running on the system. For example, sendmail logs information about all the sent items to this file
10. **/var/log/user.log** – Contains information about all user level logs
11. **/var/log/Xorg.x.log** – Log messages from the X
12. **/var/log/alternatives.log** – Information by the update-alternatives are logged into this log file. On Ubuntu, update-alternatives maintains symbolic links determining default commands.
13. **/var/log/btmp** – This file contains information about failed login attempts. Use the last command to view the btmp file. For example, “last -f /var/log/btmp | more”
14. **/var/log/cups** – All printer and printing related log messages
15. **/var/log/anaconda.log** – When you install Linux, all installation related messages are stored in this log file
16. **/var/log/yum.log** – Contains information that are logged when a package is installed using yum
17. **/var/log/cron** – Whenever [cron daemon](#) (or [anacron](#)) starts a cron job, it logs the information about the cron job in this file
18. **/var/log/secure** – Contains information related to authentication and authorization privileges. For example, sshd logs all the messages here, including unsuccessful login.
19. **/var/log/wtmp** or **/var/log/utmp** – Contains login records. Using wtmp you can find out who is logged into the system. who command uses this file to display the information.
20. **/var/log/faillog** – Contains user failed login attempts. Use faillog command to display the content of this file.

Apart from the above log files, /var/log directory may also contain the following sub-directories depending on the application that is running on your system.

- **/var/log/httpd/** (or) **/var/log/apache2** – Contains the apache web server access_log and error_log
- **/var/log/lighttpd/** – Contains light HTTPD access_log and error_log
- **/var/log/conman/** – Log files for ConMan client. conman connects remote consoles that are managed by conman daemon.
- **/var/log/mail/** – This subdirectory contains additional logs from your mail server. For example, sendmail stores the collected mail statistics in /var/log/mail/statistics file
- **/var/log/prelink/** – prelink program modifies shared libraries and linked binaries to speed up the startup process. /var/log/prelink/prelink.log contains the information about the .so file that was modified by the prelink.
- **/var/log/audit/** – Contains logs information stored by the Linux audit daemon (auditd).
- **/var/log/setroubleshoot/** – SELinux uses setroubleshootd (SE Trouble Shoot Daemon) to notify about issues in the security context of files, and logs those information in this log file.
- **/var/log/samba/** – Contains log information stored by samba, which is used to connect Windows to Linux.
- **/var/log/sa/** – Contains the daily sar files that are collected by the [sysstat package](#).
- **/var/log/sss/** – Use by system security services daemon that manage access to remote directories and authentication mechanisms.

Instead of manually trying to archive the log files, by cleaning it up after x number of days, or by deleting the logs after it reaches certain size, you can do this automatically using [logrotate](#) as we discussed earlier.

To view the log files use any one of the following methods. But, please don't do 'cat | more'.

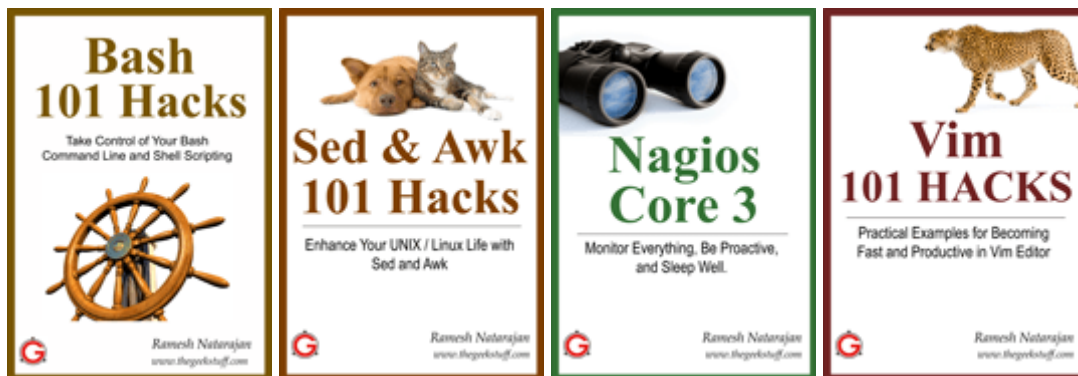
- **vi** – If you are comfortable with the [vi commands](#), use vi editor for quick log file browsing.
- **tail** – If you want to view the content of the log files real time, as the application is writing to it, use “tail -f”. You can also view [multiple log files at the same time](#) (using “tail -f”).
- **grep** – If you know exactly what you are looking for in a log file, you can quickly use grep command to grep a pattern. The [15 practical grep examples](#) will take out all your excuses of not using grep.
- **less** – Less command is very powerful to browse log files. Use these [10 less command tips](#) to master the less command.

Like 4

> [Add your comment](#)

If you enjoyed this article, you might also like..

1. [50 Linux Sysadmin Tutorials](#)
 2. [50 Most Frequently Used Linux Commands \(With Examples\)](#)
 3. [Top 25 Best Linux Performance Monitoring and Debugging Tools](#)
 4. [Mommy, I found it! – 15 Practical Linux Find Command Examples](#)
 5. [Linux 101 Hacks 2nd Edition eBook](#) **Free**
- [Awk Introduction – 7 Awk Print Examples](#)
 - [Advanced Sed Substitution Examples](#)
 - [8 Essential Vim Editor Navigation Fundamentals](#)
 - [25 Most Frequently Used Linux IPTables Rules Examples](#)
 - [Turbocharge PuTTY with 12 Powerful Add-Ons](#)



{ 20 comments... [add one](#) }

- Manojkumar August 1, 2011, 3:27 am

Hi.,
Thanks for great information

[Link](#)

- [krushna](#) August 1, 2011, 3:29 am

Thanks ,Really helpful.

[Link](#)

- Naveen August 1, 2011, 8:36 am

very informative

[Link](#)

- TK Nallappan August 2, 2011, 6:06 am

Hi Ramesh,

Wow!! what an awesome articles about log files under /var/log. I really enjoyed it.

Thanks for your knowledge sharing.

“Log files are god for us(sys admins) to find out the suspicious”

[Link](#)

- Kamal Kishore August 3, 2011, 12:22 pm

NICE....

[Link](#)

- Pooya August 4, 2011, 12:21 pm

hi all.

i think you'd better to specify your linux distro because in some distros such as ubuntu 10.10 it should be /etc/rsyslog.d/50-default.conf instead of /etc/rsyslog.conf .

by the way using " grep "/var/log/messages" /etc/rsyslog" doesn't seem efficient. because it only extracts words in the line that includes "var/log/messages" , i mean these words are not accumulated in only one line necessarily and may be one plus line.

[Link](#)

- hotpotatoe August 11, 2011, 12:48 pm

Thanks, always making good articles 😊

[Link](#)

- Stuart August 11, 2011, 1:28 pm

Thanks, very useful.

[Link](#)

- [Albert](#) April 18, 2012, 11:53 pm

Hi Ramesh,

Is it okay for us to create a custom directory under /var/log for specific regular backup operation?

[Link](#)

- dilipkumar yadav May 21, 2012, 10:59 pm

this is very helpful web site thanks for that

[Link](#)

- gp July 24, 2012, 5:57 am

hi
var/log/boot.log file is not present in suse 11 sp2
how can we find an alternative

[Link](#)

- Ethical February 7, 2013, 6:52 am

Do you know how to delete USB Log

[Link](#)

- archit May 24, 2013, 4:05 am

is there any way to analyse log without going to file , it is very tedious , will aurport or ausearch work or they work only with log generated by auditd ?

[Link](#)

- fernando April 4, 2014, 9:57 pm

Hello, why not let me watch / var / log / auth.log, / var / log / kern.log, / var / log / boot.log, I aparace “Permission denied”, as I can or I can have access permission, if I am in my PCs own user root?, Thanks.

[Link](#)

- Sharath September 20, 2015, 7:10 am

Why is that you suggest not to use “more” command to view the log files? Any particular reason?

[Link](#)

- Satish September 30, 2015, 7:50 pm

Hello Ramesh,

Thanks for the help. But why shouldn't I use cat command to view log files. Any particular reason?

[Link](#)

- arun kumar December 27, 2015, 10:08 am

Hi Ramesh,

can we have log enabled for multipathd service.
or its not choice to have ?

Regs
Arun kumar.R

[Link](#)

- sean January 7, 2016, 6:13 am

Any idea what /var/log/rgc is related to?

[Link](#)

- harikrishna February 12, 2016, 12:40 pm

Ur website is very useful. I have been watching from 2 years. Here you have given info about all logs. Can you explain the details of log file lines. I need to understand if I want to analyze some part of log. But I really donno how to understand.

[Link](#)

- Fred February 1, 2017, 12:04 pm

The dmesg comment is wrong, the /var/log/dmesg file does not contain the current RAM copy of the ring buffer which is displayed by the dmesg command. If you compare the two, they may be different.

/var/log/dmesg contains the *previous* boot cycle's printk output, not the contents of the current RAM ring buffer of messages which is displayed using the dmesg command.

It looks like when the system is shut down controlled, the contents of the current RAM ring buffer gets flushed to the /var/log/dmesg file, so the file, when you boot up again, contains the previous boot cycle's messages, not the current one.

[Link](#)

Leave a Comment

Name

Email

Website

Comment

☐ Notify me of followup comments via e-mail

Next post: [15 Linux Bash History Expansion Examples You Should Know](#)

Previous post: [Dell BIOS: Enable VT, 64-bit, and Execute Disable for VMWare](#)
[RSS](#) | [Email](#) | [Twitter](#) | [Facebook](#) | [Google+](#)

EBOOKS

- **Free** [Linux 101 Hacks 2nd Edition eBook](#) - Practical Examples to Build a Strong Foundation in Linux
- [Bash 101 Hacks eBook](#) - Take Control of Your Bash Command Line and Shell Scripting
- [Sed and Awk 101 Hacks eBook](#) - Enhance Your UNIX / Linux Life with Sed and Awk
- [Vim 101 Hacks eBook](#) - Practical Examples for Becoming Fast and Productive in Vim Editor
- [Nagios Core 3 eBook](#) - Monitor Everything, Be Proactive, and Sleep Well

404 Not Found

nginx

POPULAR POSTS

- [15 Essential Accessories for Your Nikon or Canon DSLR Camera](#)
- [12 Amazing and Essential Linux Books To Enrich Your Brain and Library](#)
- [50 UNIX / Linux Sysadmin Tutorials](#)
- [50 Most Frequently Used UNIX / Linux Commands \(With Examples\)](#)
- [How To Be Productive and Get Things Done Using GTD](#)
- [30 Things To Do When you are Bored and have a Computer](#)
- [Linux Directory Structure \(File System Structure\) Explained with Examples](#)
- [Linux Crontab: 15 Awesome Cron Job Examples](#)
- [Get a Grip on the Grep! – 15 Practical Grep Command Examples](#)
- [Unix LS Command: 15 Practical Examples](#)
- [15 Examples To Master Linux Command Line History](#)
- [Top 10 Open Source Bug Tracking System](#)
- [Vi and Vim Macro Tutorial: How To Record and Play](#)
- [Mommy, I found it! -- 15 Practical Linux Find Command Examples](#)
- [15 Awesome Gmail Tips and Tricks](#)
- [15 Awesome Google Search Tips and Tricks](#)
- [RAID 0, RAID 1, RAID 5, RAID 10 Explained with Diagrams](#)
- [Can You Top This? 15 Practical Linux Top Command Examples](#)
- [Top 5 Best System Monitoring Tools](#)
- [Top 5 Best Linux OS Distributions](#)
- [How To Monitor Remote Linux Host using Nagios 3.0](#)
- [Awk Introduction Tutorial – 7 Awk Print Examples](#)
- [How to Backup Linux? 15 rsync Command Examples](#)
- [The Ultimate Wget Download Guide With 15 Awesome Examples](#)
- [Top 5 Best Linux Text Editors](#)
- [Packet Analyzer: 15 TCPDUMP Command Examples](#)
- [The Ultimate Bash Array Tutorial with 15 Examples](#)
- [3 Steps to Perform SSH Login Without Password Using ssh-keygen & ssh-copy-id](#)
- [Unix Sed Tutorial: Advanced Sed Substitution Examples](#)
- [UNIX / Linux: 10 Netstat Command Examples](#)
- [The Ultimate Guide for Creating Strong Passwords](#)
- [6 Steps to Secure Your Home Wireless Network](#)
- [Turbocharge PuTTY with 12 Powerful Add-Ons](#)

CATEGORIES

- [Linux Tutorials](#)
- [Vim Editor](#)
- [Sed Scripting](#)
- [Awk Scripting](#)
- [Bash Shell Scripting](#)

- [Nagios Monitoring](#)
- [OpenSSH](#)
- [IPTables Firewall](#)
- [Apache Web Server](#)
- [MySQL Database](#)
- [Perl Programming](#)
- [Google Tutorials](#)
- [Ubuntu Tutorials](#)
- [PostgreSQL DB](#)
- [Hello World Examples](#)
- [C Programming](#)
- [C++ Programming](#)
- [DELL Server Tutorials](#)
- [Oracle Database](#)
- [VMware Tutorials](#)

About The Geek Stuff



My name is **Ramesh Natarajan**. I will be posting instruction guides, how-to, troubleshooting tips and tricks on Linux, database, hardware, security and web. My focus is to write articles that will either teach you or help you resolve a problem. Read more about [Ramesh Natarajan](#) and the blog.

Contact Us

Email Me : Use this [Contact Form](#) to get in touch me with your comments, questions or suggestions about this site. You can also simply drop me a line to say hello!.

[Follow us on Google+](#)

[Follow us on Twitter](#)

[Become a fan on Facebook](#)

Support Us

Support this blog by purchasing one of my ebooks.

[Bash 101 Hacks eBook](#)

[Sed and Awk 101 Hacks eBook](#)

[Vim 101 Hacks eBook](#)

[Nagios Core 3 eBook](#)

Copyright © 2008–2018 Ramesh Natarajan. All rights reserved | [Terms of Service](#)