

1.111.3

Configure and use system log files to meet administrative and security needs

Weight 3

Linux Professional Institute Certification — 102

Nick Urbanik <nicku@nicku.org>

This document Licensed under GPL—see section 6

2005 November

Outline

Context

Objectives

Configuring Syslog

- syslog facility

- syslog levels

- syslog actions

- `syslog.conf` example

Rotating Log Files with

`logrotate`

- Configuring `logrotate`

Examining Log Files

- Log Messages

- How to search for
particular events

License Of This Document

1.111.3

Configure and use
system log files to
meet administrative
and security needs
Weight 3

Nick Urbanik

Context

Objectives

Configuring Syslog

Rotating Log Files with
`logrotate`

Examining Log Files

License Of This
Document

Topic 111 Administrative Tasks [21]

Where we are up to

1.111.3
Configure and use
system log files to
meet administrative
and security needs
Weight 3

Nick Urbanik

Context

Objectives

Configuring Syslog

Rotating Log Files with
logrotate

Examining Log Files

License Of This
Document

- 1.111.1 Manage users and group accounts and related system files [4]
- 1.111.2 Tune the user environment and system environment variables [3]
- 1.111.3 **Configure and use system log files to meet administrative and security needs [3]**
- 1.111.4 Automate system administration tasks by scheduling jobs to run in the future [4]
- 1.111.5 Maintain an effective data backup strategy [3]
- 1.111.6 Maintain system time [4]

Description of Objective

1.111.3 Configure and use system log files to meet administrative and security needs [3]

Candidate should be able to configure system logs. This objective includes managing the type and level of information logged, manually scanning log files for notable activity, monitoring log files, arranging for automatic rotation and archiving of logs and tracking down problems noted in logs.

1.111.3

Configure and use system log files to meet administrative and security needs
Weight 3

Nick Urbanik

Context

Objectives

Configuring Syslog

Rotating Log Files with
logrotate

Examining Log Files

License Of This
Document

Key files, terms, and utilities include:

1.111.3 Configure and use system log files to meet administrative and security needs [3]

`/etc/syslog.conf` — configuration file for
 `syslogd`
`/var/log/*` — where the log files are found
`logrotate` — the program that “rotates” log files
`tail -f` — the best way to watch log files as
 things happen

1.111.3

Configure and use
system log files to
meet administrative
and security needs
Weight 3

Nick Urbanik

Context

Objectives

Configuring Syslog

Rotating Log Files with
`logrotate`

Examining Log Files

License Of This
Document

/etc/syslog.conf

- ▶ Each line in `/etc/syslog.conf` contains comments that start with a '#' or rules of the form: `<facility>.<level><action>`

1.111.3

Configure and use
system log files to
meet administrative
and security needs
Weight 3

Nick Urbanik

Context

Objectives

Configuring Syslog

syslog facility

syslog levels

syslog actions

syslog.conf example

Rotating Log Files with
logrotate

Examining Log Files

License Of This
Document

syslog facility

shows where the log message comes from:

`authpriv` — security/authorization messages (private)

`cron` — clock daemon (cron and at)

`daemon` — system daemons without separate facility value

`ftp` — ftp daemon

`kern` — kernel messages

`local0...local7` — reserved for local use

`lpr` — line printer subsystem

`mail` — mail subsystem

`news` — USENET news subsystem

`syslog` — messages generated internally by `syslogd`

`user` — generic user-level message

`uucp` — UUCP subsystem

See \$ **man 3 syslog** ↵

1.111.3

Configure and use
system log files to
meet administrative
and security needs
Weight 3

Nick Urbanik

Context

Objectives

Configuring Syslog

syslog facility

syslog levels

syslog actions

syslog.conf example

Rotating Log Files with
logrotate

Examining Log Files

License Of This
Document

security threshold beyond which messages are logged

in decreasing importance:

`emerg` — system is unusable

`alert` — action must be taken immediately

`crit` — critical conditions

`err` — error conditions

`warning` — warning conditions

`notice` — normal, but significant, condition

`info` — informational message

`debug` — debug-level message

1.111.3

Configure and use
system log files to
meet administrative
and security needs
Weight 3

Nick Urbanik

Context

Objectives

Configuring Syslog

syslog facility

syslog levels

syslog actions

syslog.conf example

Rotating Log Files with
logrotate

Examining Log Files

License Of This
Document

syslog actions

1.111.3
Configure and use
system log files to
meet administrative
and security needs
Weight 3

Nick Urbanik

Context

Objectives

Configuring Syslog

syslog facility

syslog levels

syslog actions

syslog.conf example

Rotating Log Files with
logrotate

Examining Log Files

License Of This
Document

Can be:

- ▶ filename (with full pathname), or
- ▶ a hostname preceded with '@', or
- ▶ a comma-separated list of users, or
- ▶ an asterisk '*' meaning all logged in users

syslog.conf example

```
# 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;news.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
```

1.111.3

Configure and use
system log files to
meet administrative
and security needs
Weight 3

Nick Urbanik

Context

Objectives

Configuring Syslog

syslog facility

syslog levels

syslog actions

syslog.conf example

Rotating Log Files with
logrotate

Examining Log Files

License Of This
Document

syslog.conf example — 2

```
# Save boot messages also to boot.log
local7.*                                /var/log/boot.log

# Note: the rawhide openldap /etc/init.d/ldap script starts slapd with
# the -l daemon option, which was confusing.
# I added the option -l local5 to the (newly created)
# /etc/sysconfig/ldap
local5.*                                -/var/log/slapd

# local4.*                              /var/log/squid

# Now I've set log-facility local1; in dhcpd.conf
local1.*                                /var/log/dhcp-log

#
# INN
#
news.=crit                              /var/log/news/news.crit
news.=err                                /var/log/news/news.err
news.notice                             /var/log/news/news.notice

daemon,kern.*                           /var/log/debug
```

1.111.3

Configure and use
system log files to
meet administrative
and security needs
Weight 3

Nick Urbanik

[Context](#)

[Objectives](#)

[Configuring Syslog](#)

[syslog facility](#)

[syslog levels](#)

[syslog actions](#)

[syslog.conf example](#)

[Rotating Log Files with
logrotate](#)

[Examining Log Files](#)

[License Of This
Document](#)

Rotating Log Files with `logrotate`

1.111.3
Configure and use
system log files to
meet administrative
and security needs
Weight 3

Nick Urbanik

Context

Objectives

Configuring Syslog

Rotating Log Files with
`logrotate`

Configuring `logrotate`

Examining Log Files

License Of This
Document

- ▶ Log files grow rapidly
- ▶ Can grow to extreme sizes without rotation
- ▶ log rotation renames files and redirects logging to the new file: `messages` → `messages.1` → `messages.2` → `messages.3` → `messages.4` → **delete**
- ▶ Run `logrotate` from `cron`

logrotate configuration

- ▶ Main configuration file is `/etc/logrotate.conf`
- ▶ ... but most configuration belongs to the software packages, which put a file into directory `/etc/logrotate.d/`

```
$ cat /etc/logrotate.d/ldap ↵
```

```
# Nick 17 Aug 2003: copied from my /etc/logrotate.conf on ictlab:
/var/log/slaped
    weekly
    create 0664 ldap ldap
    rotate 20
    #postrotate
    #    /etc/rc.d/init.d/ldap condrestart
    #endscript
    notifempty
```

```
$ cat /etc/logrotate.d/syslog ↵
```

```
/var/log/messages /var/log/secure /var/log/maillog
/var/log/spooler /var/log/boot.log /var/log/cron
/var/log/debug
    sharedscripts
    weekly
    rotate 60
    postrotate
        /bin/kill -HUP `cat /var/run/syslogd.pid
        2> /dev/null` 2> /dev/null || true
    endscript
```

1.111.3

Configure and use
system log files to
meet administrative
and security needs
Weight 3

Nick Urbanik

Context

Objectives

Configuring Syslog

Rotating Log Files with
logrotate

Configuring logrotate

Examining Log Files

License Of This
Document

Examining Log Files

1.111.3
Configure and use
system log files to
meet administrative
and security needs
Weight 3

Nick Urbanik

Context

Objectives

Configuring Syslog

Rotating Log Files with
`logrotate`

Examining Log Files

Log Messages

How to search for particular
events

License Of This
Document

- ▶ Many log files are readable by none but root:
- ▶ Simplest: `$ sudo tail -f /var/log/messages` ↩
- ▶ `$ sudo less /var/log/messages` ↩
 - ▶ within `less`, press `F`
- ▶ Using either method, new additions to the log file are shown

Log Messages

Each syslog message contains these fields:

date and time — in local time on my machine

hostname — of the machine that generated the message

program or user — that generated the message, e.g., `kernel`,
`named`, `postfix`, `dhcpcd`, ...

message text

1.111.3

Configure and use
system log files to
meet administrative
and security needs
Weight 3

Nick Urbanik

Context

Objectives

Configuring Syslog

Rotating Log Files with
`logrotate`

Examining Log Files

Log Messages

How to search for particular
events

License Of This
Document

Searching for particular events

1.111.3
Configure and use
system log files to
meet administrative
and security needs
Weight 3

Nick Urbanik

Context

Objectives

Configuring Syslog

Rotating Log Files with
`logrotate`

Examining Log Files

Log Messages

How to search for particular
events

License Of This
Document

- Can `grep` for messages relating to a particular program:

```
$ sudo grep dhcpd /var/log/messages ↵
Nov 14 06:30:13 nicku dhcpd: DHCPDISCOVER from 00:04:e2:2e:c3:d6
via eth0
Nov 14 06:30:13 nicku dhcpd: DHCPOFFER on 192.168.0.8
to 00:04:e2:2e:c3:d6 via eth0
```


Topics Covered

Context

Objectives

Configuring Syslog

- syslog facility

- syslog levels

- syslog actions

- `syslog.conf` example

Rotating Log Files with `logrotate`

- Configuring `logrotate`

Examining Log Files

- Log Messages

- How to search for particular events

License Of This Document

1.111.3

Configure and use
system log files to
meet administrative
and security needs
Weight 3

Nick Urbanik

Context

Objectives

Configuring Syslog

Rotating Log Files with
`logrotate`

Examining Log Files

Log Messages

How to search for particular
events

License Of This
Document

License Of This Document

1.111.3
Configure and use
system log files to
meet administrative
and security needs
Weight 3

Nick Urbanik

Context

Objectives

Configuring Syslog

Rotating Log Files with
logrotate

Examining Log Files

License Of This
Document

Copyright © 2005 Nick Urbanik <nicku@nicku.org>

You can redistribute modified or unmodified copies of this document provided that this copyright notice and this permission notice are preserved on all copies under the terms of the GNU General Public License as published by the Free Software Foundation—either version 2 of the License or (at your option) any later version.