System Logging

What You Will Learn

- The syslog standard
- Facilities and severities
- Syslog servers
- Logging rules
- Where logs are stored
- How to generate your own log messages
- Rotating log files

The Syslog Standard

- Aids in the processing of messages.
- Allows logging to be centrally controlled.
- Uses facilities and severities to categorize messages.

Number	Keyword	Description
0	kern	kernel messages
1	user	user-level messages
2	mail	mail system
3	daemon	system daemons
4	auth	security/authorization messages
5	syslog	messages generated by syslogd
6	lpr	line printer subsystem
7	news	network news subsystem
8	uucp	UUCP subsystem
9	clock	daemon
10	authpriv	security/authorization messages

Number	Keyword	Description
11	ftp	FTP daemon
12	-	NTP subsystem
13	-	log audit
14	-	log alert
15	cron	clock daemon
16	local0	local use 0 (local0)
16	local1	local use 0 (local1)
16	local2	local use 0 (local2)
16	local3	local use 0 (local3)
...		
23	local7	local use 7 (local7)

Code	Severity	Keyword	Description
0	Emergency	emerg (panic)	System is unusable
1	Alert	alert	Action must be taken immediately
2	Critical	crit	Critical conditions
3	Error	err (error)	Error conditions
4	Warning	warning (warn)	Warning conditions
5	Notice	notice	Normal but significant condition
6	Info	info	Informational messages
7	Debug	debug	Debug-level messages

Syslog Servers

- Process syslog messages based on rules.
- syslogd
- rsyslog
- syslog-ng

rsyslog

/etc/rsyslog.conf:

```
$IncludeConfig /etc/rsyslog.d/*.conf
```

Logging Rules

- Selector field
  - **FACILITY.SEVERITY**
  - **mail.***
  - **mail**
  - **FACILITY.none**
  - **FACILITY_1.SEVERITY; FACILITY_2.SEVERITY**
- Action field
  - Determines how a message is processed

Example Logging Rule

```
mail.*          /var/log/mail.log
```

Caching vs Non-caching

- Caching is used if the path starts with a hyphen
  - `mail.info -/var/log/mail.info`
- You may lose some messages during a system crash if you are using caching mode.
- Using caching mode can improve I/O performance.

Example Logging Rules

```
mail.info       -/var/log/mail.info
mail.warn       -/var/log/mail.warn
mail.err        /var/log/mail.err
```

Example Logging Rules

```
auth,authpriv.*                  /var/log/auth.log
*.*;auth.none,authpriv.none  -/var/log/syslog
```

Example Logging Rules

```
*.info;mail.none;authpriv.none;cron.none /var/log/messages
```

logger

```
logger [options] message
```

Options:

```
-p FACILITY.SEVERITY
-t TAG
```

logger

```
$ logger -p mail.info -t mailtest "Test."
$ sudo tail -1 /var/log/mail.log
Apr  4 14:33:16 linuxsvr mailtest: Test.
```

logrotate

```
/etc/logrotate.conf:

include /etc/logrotate.d
```

Example logrotate.conf

```
weekly
rotate 4
create
compressed
include /etc/logrotate.d
```

```
/var/log/debug
/var/log/messages
{
        rotate 4
        weekly
        missingok
        notifempty
        compress
        sharedscripts
        postrotate
                reload rsyslog >/dev/null 2>&1 || true
        endscript
}
```

Test the logrotate configuration

```
# logrotate -fv /etc/logrotate.conf
```

Summary

- The syslog standard
- Facilities and severities
- Syslog servers
- Logging rules
- How to generate your own log messages
- Using logrotate