Logging

A Study in Pain Avoidance

Patrick Haller

April 2007

We are probably not into that kind of logging...

I'm a lumberjack and I'm ok,
I sleep all night
and I work all day.

We are probably not into that kind of logging...

I'm a lumberjack and I'm ok,
I sleep all night
and I work all day.


775A
BARKO


PRENTICE 210C
LAWTEY
FIRE RESCUE

Logging...

32 => 5?

Logging…

$$\log_2 32 = 5$$

Man or Machine?

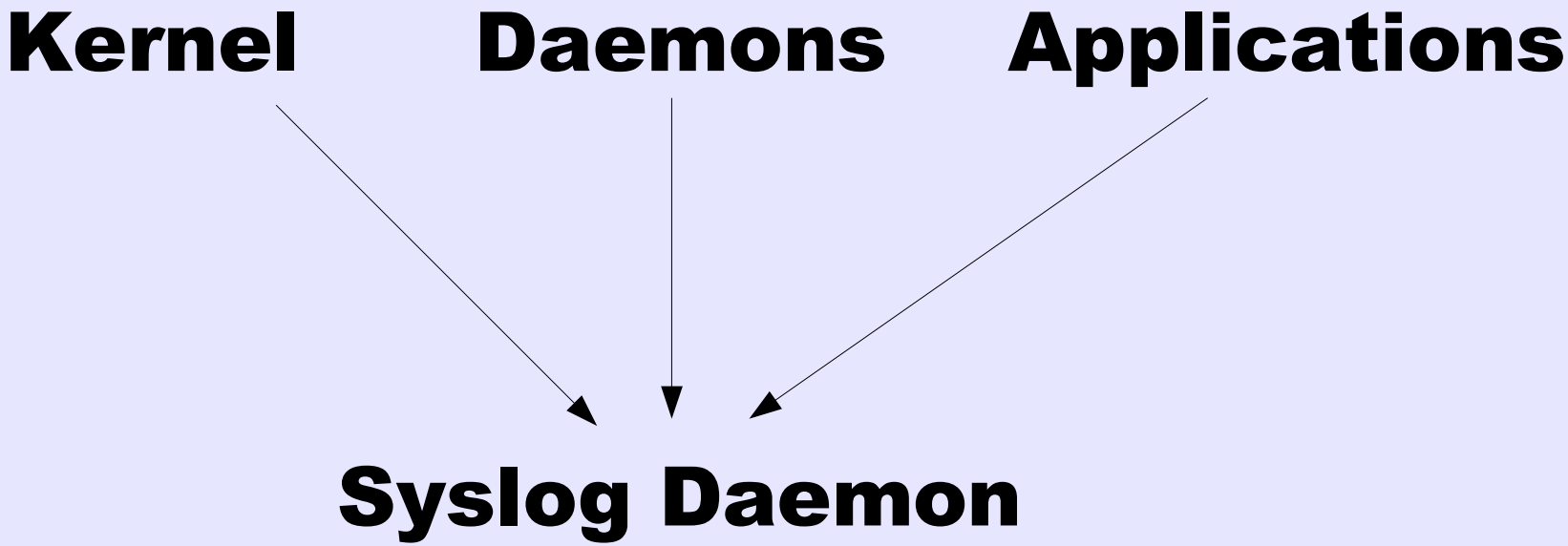
Logging...

How do you know they're working ok?

Logging…

Syslog

Syslog Messages



Syslog Message: Log Levels

```
EMERG     "<0>"  system is unusable
ALERT     "<1>"  action must be taken immediately
CRIT      "<2>"  critical conditions
ERR       "<3>"  error conditions
WARNING   "<4>"  warning conditions
NOTICE    "<5>"  normal but significant condition
INFO      "<6>"  informational
DEBUG     "<7>"  debug-level messages
```

Syslog Message: Facilities

AUTHPRIV	security/authorization messages
CRON	clock daemon (cron and at)
DAEMON	system daemons without separate facility
FTP	ftp daemon
KERN	kernel messages
LPR	line printer subsystem
MAIL	mail subsystem
NEWS	USENET news subsystem
SYSLOG	messages generated internally by syslogd
USER	generic user-level messages
UUCP	UUCP subsystem
LOCAL0-7	reserved for local use

Syslog Daemons

syslog-ng
rsyslogd
syslogd
sdsc-syslogd

Syslog Daemons

syslog-ng
rsyslogd
syslogd
sdsc-syslogd

Syslog Daemons

Where do you want logs to go?

- MySQL
- Flat files
- Some program
- Some other server


WHITEY'S AUTO BOD
533 McBRIDE AVE
286-5557

Syslog-ng limiting damage

```
destination messages {
 file("/var/log/$WEEKDAY/messages"
  template(
   "$HOUR:$MIN:$SEC $TZ $HOST [$LEVEL] $MSG\n"
  )
  template_escape(no)
  create_dirs(yes)
  overwrite_if_older(86500)
 );
};
```

Syslog-ng limiting damage

```
destination messages {
 file("/var/log/$WEEKDAY/messages"
  template(
   "$HOUR:$MIN:$SEC $TZ $HOST [$LEVEL] $MSG\n"
  )
  template_escape(no)
  create_dirs(yes)
  overwrite_if_older(86500)
 );
};
```

Unexamined Logs means failure

Logging…

10 print “FAILURE”
20 goto 10

Syslog Analysis

swatch
logcheck
sec
graphs

Syslog Analysis

swatch

logcheck

sec

graphs

Syslog Reduction

Expected lines get ignored

```
perlcode my $re_pid = qr/ \[ \d{1,6} \] /x;
perlcode my $re_prefix =
  "^$re_timestamp GMT $re_hostname $re_facpri";

perlcode my $re = /$re_prefix (cron|crontab)$re_pid:/
ignore /$re \((phaller|root)\) (CMD|RELOAD|BEGIN|REPLACE|END)/
```

Syslog Analysis

Run swatch from cron daily
Read the extracts
Investigate issues
Update /etc/swatch.conf

Syslog Analysis Niceties

Summarize event counts

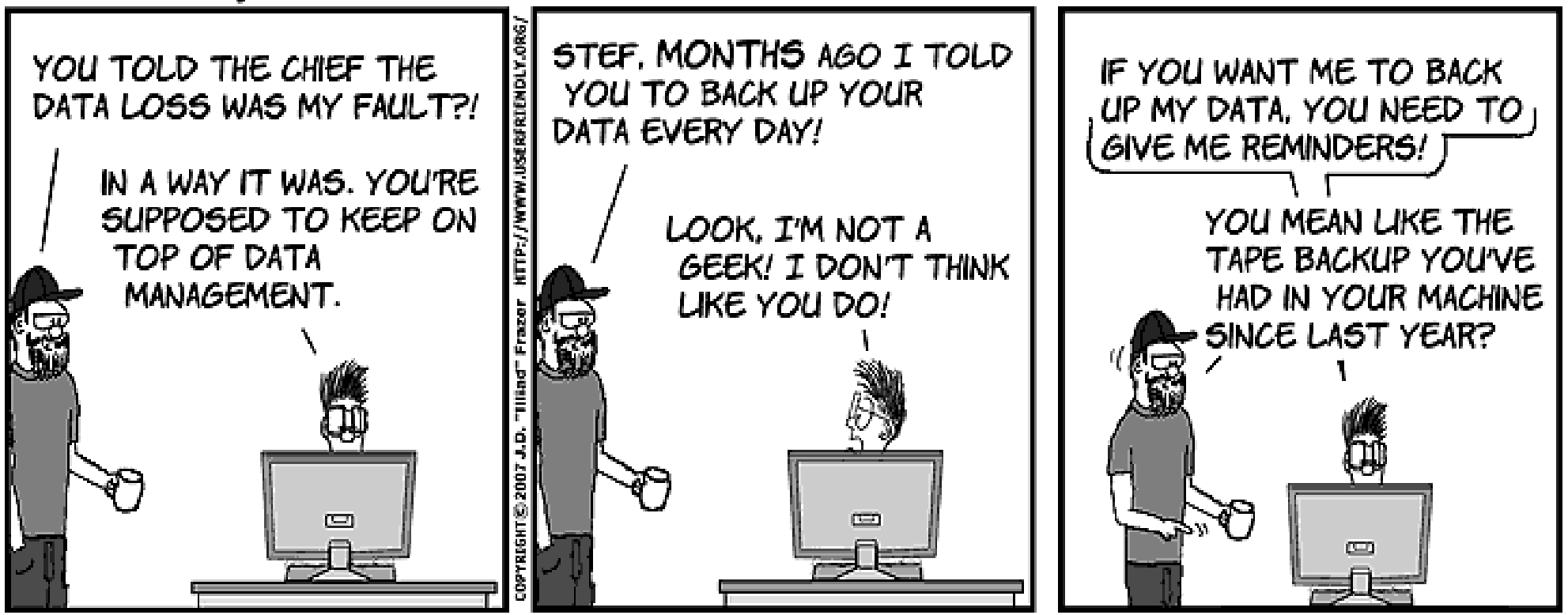
Store in a database

Use perl or PHP to graph

Review periodically

0 10 * * * echo check graphs

USER FRIENDLY by J.D. "Illiad" Frazer



Syslog Analysis Niceties

Summarize event counts

Store in a database

Use perl/python/ruby/whatever

Check for Threshold breaches

***/5 * * * * compliance.py**

Fix or Maintain?