Linux logging
and
logfiles monitoring with
swatch

Sebastian Büttrich, wire.less.dk

edit: November 2009, Pacnog6

Agenda

- Linux logging
- The most important logs
- Swatch and other log watchers

Linux Logging

- two daemons that control logging:

  klogd (sysklogd) and syslogd.
- klogd deals with kernel messages.
- syslogd deals with other system messages, such as applications.
- You can configure the behavior of both by editing the files /etc/syslog.conf and /etc/sysconfig/syslog

Linux
Logging directory

- default directory for most logs is

  /var/log

- logrotating (now default in Ubuntu) is essential, else you will strangulate your own resources (= have beautiful backlog, but run out of space)
- Backup important logfiles to external place by using rsync or scp

Linux

Essential log files

- /var/log/messages: General system and kernel messages
- /var/log/auth.log: Authenication logs
- /var/log/kern.log: Kernel logs
- /var/log/cron.log: Crond logs (cron job)
- /var/log/maillog: Mail server logs
- /var/log/httpd/ or /var/log/apache: Apache access and error logs directory, typically: access.log, error.log
- /var/log/boot.log : System boot log
- /var/log/secure: Authentication log
- /var/log/utmp or /var/log/wtmp : Login records file
- /var/log/dkpg.log: package management

+ individual applications' logfiles (may also be kept in applications directories, outside /var/log)

Linux

Logging directory

- **Most important tools for looking at logfiles:**

  ```
  # less
  # more
  # tail
  # grep
  ```

  archiving tools (tar, gunzip, etc)
  rsync, scp for backing up

- **If you prefer graphical tools, *webmin* is handy for looking at logfiles**

Log monitoring

Swatch & logwatch & others

- Having extensive logfiles is great, however uou also need to make sense of them
- Not realistic to manually keep track of things
- Use log watching utilities to give you automated warnings, alerts, etc, and to act upon suspicious activity

Log monitoring

DenyHosts / Fail2Ban

- DenyHosts is a Python based security tool for SSH servers. It is intended to prevent brute force attacks on SSH servers by monitoring invalid login attempts in the authentication log and blocking the originating IP addresses.
- Fail2Ban's main function is to block selected IP addresses that may belong to hosts that are trying to breach the system's security. It determines the hosts to be blocked by monitoring log files (e.g. /var/log/pwdfail, /var/log/auth.log, etc) and bans any host IP that makes too many login attempts or performs any other unwanted action within a time

Log monitoring
Swatch

- swatch is a perl utility that can monitor just about any type of log.
- It uses regular expressions to look for patterns that you define, and act upon matches.
- Standard actions include output to standard out, sounds, emails -
  but you can trigger any command you wish to – making this extremely powerful.

Log monitoring

Swatch

- **Swatch expects config file at**
  /etc/swatchrc

- **Swatch syntax: see**
  #man swatch
- **Simple example for a swatch config entry:**

  ```
  watchfor        /ALERT:/
  echo bold red
  exec echo "$_ swatch just spit out a alert warning" | mail -s
  swatch-alert  sebastian@less.dk
  ```
- You can use throttle and threshhold (=timeouts) to prevent all too many alerts

That was it ...

Thank you!

sebastian@less.dk
http://wire.less.dk

Sebastian Büttrich, wire.less.dk

edit: November 2009