APPLE DEVICE ADMINISTRATORS MEETING

Trinity Term
Tuesday, 27th June 2017
Hosted by IT Services, University of Oxford

AGENDA

- 12:30 - 12:35 - Introduction
- 12:35 - 12:50 - Unified Logging and the log command in macOS Sierra
  Ben Goodstein, Senior Systems Administrator, IT Services
- 12:50 - 13:05 - Hi, High Sierra! What we know about Apple's next macOS
  Chris Beard, Systems Administrator, IT Services
- 13:05 - 13:30 - Q & A, Discussions

UNIFIED LOGGING

& the `log` command in macOS Sierra

Ben Goodstein
Senior Systems Administrator, IT Services
@fuzzylogiq - Twitter/Github/Slack

TRADITIONAL LOGGING

just kidding

log (n.2)

"record of observations, readings, etc.," originally "record of a ship's progress," 1842, sailor's shortening of *log-book* (1670s), the daily record of a ship's speed, progress, etc., which is from ***log*** (n.1) "piece of wood." The book so called because it recorded the speed measurements made by means of a weighted chip of a tree log on the end of a reeled *log line* (typically 150 to 200 fathoms).

or am I? logs really were originally records of what happened to a bit of wood

log (n.2)

"record of observations, readings, etc.," originally "record of a ship's progress," 1842, sailor's shortening of *log-book* (1670s), the daily record of a ship's speed, progress, etc., which is from ***log*** (n.1) "piece of wood." The book so called because it recorded the speed measurements made by means of a weighted chip of a tree log on the end of a reeled *log line* (typically 150 to 200 fathoms).

log (n.2)

"record of observations, readings, etc.," originally "record of a ship's progress." 1842. sailor's shortening of *log-book* (1670s), the daily record of a ship's speed, progress, etc., which is from ***log*** (n.1) "piece of wood."

The book so called because it recorded the speed measurements made by means of a weighted chip of a tree log on the end of a reeled *log line* (typically 150 to 200 fathoms).

TRADITIONAL LOGGING

TRADITIONAL LOGGING

- File redirection of command output
- syslog API
- Stored on disk
- grep/less
- Apple System Logging (ASL)

ASL replaced syslog/syslogd - to some people's chagrin in 2007 with Leopard - Database model

TRADITIONAL LOGGING – DRAWBACKS

- Disk intensive - SSD
- Imprecise timings
- Multiple logs spread throughout system
- Need to enable more verbose logs e.g. debug level
- Privacy concerns - user data in logs

Lots of different approaches to this - one is jornald, part of systemd on Linux systems

UNIFIED LOGGING

UNIFIED LOGGING

- Single API for all logging from apps compiled for iOS 10+ and macOS 10.12+
- Available on all Apple OS (iOS, macOS, tvOS, watchOS)
- Everything logging all the time, Kernel and Userspace
- High performance
- Compressed, binary log files `/var/db/diagnostics` - no `grep/less`
- In-memory buffers - less is saved to disk
- Accurate to the microsecond
- Private
- `.logarchive` output format but no programmatical API 😞

THE NEW `log` COMMAND

THE NEW `log` COMMAND

- Because real sysadmins don't use Console.app
- Command-line interface to the logging API
- `log show` - for replaying logs in the terminal (`cat/grep`)
- `log stream` - for displaying logs in real time (`tail/grep`)
- `log collect` - for collecting logs into .logarchive for distribution
- `log config` - for configuring the logging API
- `log erase` - for...erasing logs!

log show

```
log show --predicate 'eventMessage contains "aaargh!"' \
         --style syslog \
         --info \
         --last 20m

log show --predicate 'subsystem == "com.apple.coreaudio"' \
         --style json \
         --debug \
         --start "2017-06-26 06:00:00" \
         --end "2017-06-26 06:04:59"
```

talk about different styles

log stream

```
log stream --predicate 'eventMessage contains "aaaarrrggghhh!!' \
           --level default \
           --process 21455

log stream --predicate 'subsystem == "com.apple.coreaudio"' \
           --style json \
           --level debug \
           --timeout 30m
```

talk about how levels are cumulative

log collect

```
log collect --output last3m.logarchive \
            --last 3m

log collect --output . \
            --start "2017-06-26 00:00:00 \
            --end "2017-06-26 00:00:05

log collect --output whatever.logarchive \
            --size 100m
```

if you give a directory it creates a file called system_logs.logarchive

log config

```
log config --subsystem "com.apple.Finder" \
           --mode persist:off

log config --process 14900 \
           --mode level:off

log config --reset \
           --process 14900
```

this can also be done with configuration profiles

log erase (eek!)

```
log erase

log erase --ttl

log erase --all
```

DEMO

FURTHER READING

- Official Apple documentation:
  https://developer.apple.com/documentation/os/logging
- WWDC 2016 session on Unified Logging and Activity Tracing
  https://developer.apple.com/videos/play/wwdc2016/721/
- Apple predicate format syntax (for `log show` and `log stream`):
  https://developer.apple.com/library/content/documentation/Cocoa/Conceptual/Predicates/Articles/pSyntax.html
- Using the logs in Sierra: some practical tips
  https://eclecticlight.co/2016/10/01/using-the-logs-in-sierra-some-practical-tips/
- Overview of the log command (requires Lynda sign-in):
  https://www.lynda.com/Mac-OS-tutorials/Overview-log-command/534419/575401-4.html

THANK YOU

Ben Goodstein
Senior Systems Administrator, IT Services
@fuzzylogiq - Twitter/Github/Slack

I am one with the Force; The Force is with me.