dataJAR

Beyond Device Management

Richard Mallion

Systems Engineer @ dataJAR Ltd

Email: richard@datajar.co.uk
Twitter: @richardmallion
MacAdmins Slack: @red5

Unified Logging

- Overview
- Log Levels
- Subsystems and Categories
- Console App
- Log Command
- Predicates

Traditional Logs

Unified Logging

- Introduced at WWDC 2016
- Centralised logging
- Standardised logging format
- Maximise information collected
- Small footprint
- Compression of log messages
- Defer lot of the work until observation
- Manage log message life cycle
- Privacy by design

Supported Platforms

macOS 10.12+

iOS 10+

tvOS 10+

watchOS 3+

New File Format

.tracev3 files

Compressed binary format

/var/db/diagnostics

/var/db/diagnostics/persist

Approx 52 files are maintained

Each approx 10.5MB

/var/db/uuidtext

Must Use Apple Tools

Console.app

log command line tool

Xcode

OSLog framework

How Does it Work?

Log Levels for
Each Message

Each message has a log level

Log Levels for
Each Message

Three basic levels

- Default (Notice) - Essential for troubleshooting
- Info - Helpful but not essential for troubleshooting
- Debug - Useful during debugging

Log Levels for
Each Message

Two special levels

- Error - Errors seen during the execution of your code
- Fault - Faults and bugs in your code

Subsystems and Categories

Each log message is associated with a

- subsystem

- category

Subsystems

Subsystems identify an app or part of an app

Uses reverse-DNS Notation

com.example.myapp

Categories

Categories identify a particular component or module in a given subsystem

Which can be used to filter logs

Network, start-up, authentication….

Subsystems and Categories

Subsystem	*Category*
uk.co.datajar.projectx	*Network*
uk.co.datajar.projecty	*login*, *password*

Basic Log Level characteristics

Each log level can have two characteristics

Can be set for system, subsystem or category

Basic Log Level characteristics

Is it Enabled?

Stored in disk or memory

Default behaviour - characteristics

Message Level	*Enabled*	*Destination*
Default (Notice)	*Always*	*Disk*
Info	*Yes*	*Memory*
Debug	*No*	*N/A*
Error	*Always*	*Disk*
Fault	*Always*	*Disk*

Default behaviour - characteristics

You can check the current log level of a subsystem

```
sudo log config --status --subsystem uk.co.datajar.myapp
```

```
Mode for 'uk.co.datajar.myapp'  INFO PERSIST_DEFAULT
```

Default behaviour - characteristics

You can enable debug logging for a subsystem

sudo log config --mode "level:debug" --subsystem uk.co.datajar.myapp

Creates a plist in /Library/Preferences/Logging/Subsystems

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
        <key>DEFAULT-OPTIONS</key>
        <dict>
                <key>Level</key>
                <dict>
                        <key>Enable</key>
                        <string>debug</string>
                </dict>
        </dict>
</dict>
</plist>
```

Default behaviour - characteristics

You can enable persistence debug logging for a subsystem

sudo log config --mode "level:debug, persist:debug" --subsystem uk.co.datajar.myapp

Creates a plist in /Library/Preferences/Logging/Subsystems

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
        <key>DEFAULT-OPTIONS</key>
        <dict>
                <key>Level</key>
                <dict>
                        <key>Enable</key>
                        <string>debug</string>
                        <key>Persist</key>
                        <string>debug</string>
                </dict>
        </dict>
</dict>
</plist>
```

Default behaviour - characteristics

Apple have a set of overrides for their various subsystems.

/System/Library/Preferences/Logging/Subsystems

Default behaviour - characteristics

com.apple.su.plist

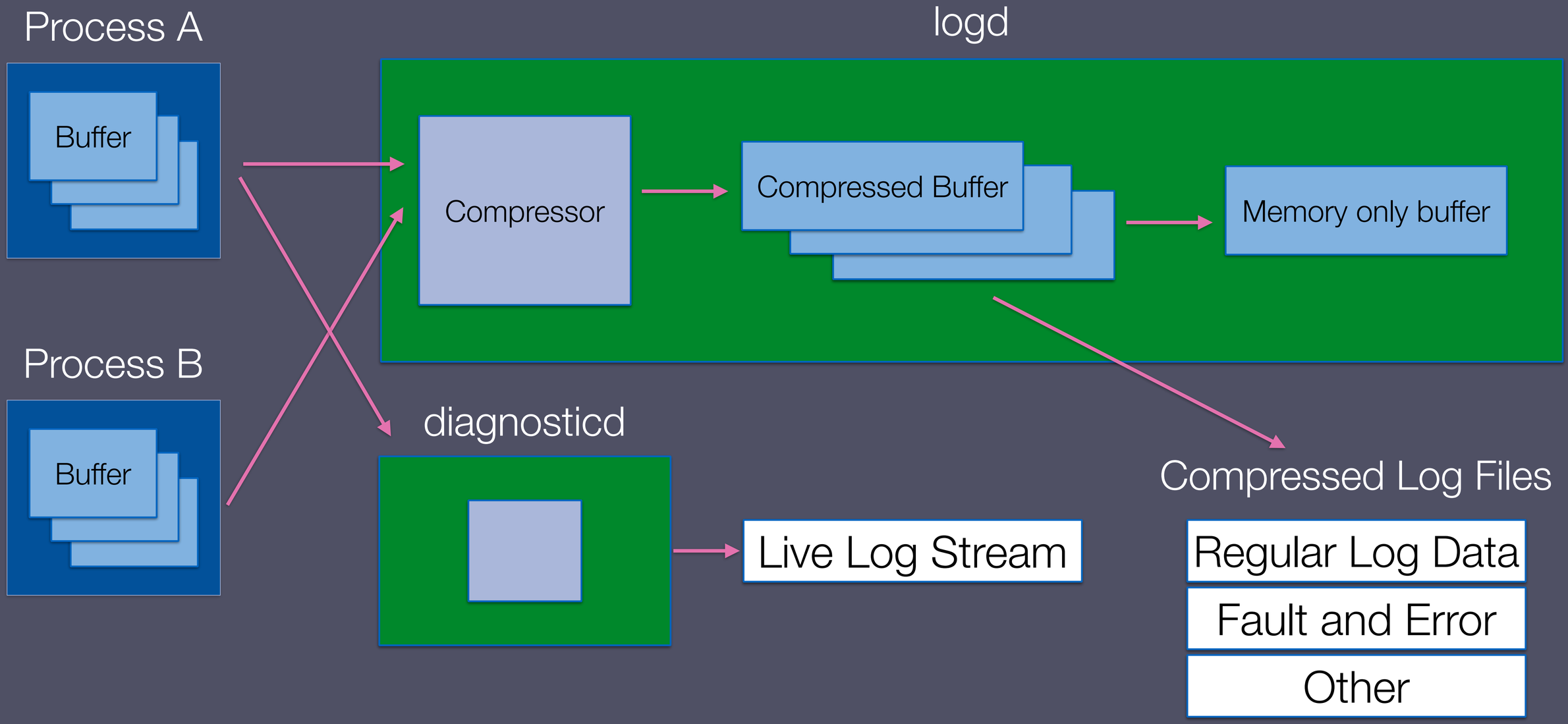
```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
    <dict>
        <key>SU</key>
        <key>DEFAULT-OPTIONS</key>
         <dict>
            <key>Level</key>
            <dict>
                <key>Enable</key>
                <string>Info</string>
                <key>Persist</key>
                <string>Info</string>
            </dict>
            <key>TTL</key>
            <dict>
                <key>Default</key>
                <integer>30</integer>
                <key>Notice</key>
                <integer>30</integer>
                <key>Info</key>
                <integer>30</integer>
                <key>Debug</key>
                <integer>30</integer>
            </dict>
        </dict>
    </dict>
</plist>
```

Default behaviour - characteristics

You can also override the logging level with a plist / configuration profile.

/Library/Preferences/Logging/Subsystems

https://developer.apple.com/documentation/os/logging/customizing_logging_behavior_while_debugging


Process A
Buffer
Process B
Buffer
logd
Compressor
Compressed Buffer
Memory only buffer
diagnosticd
Live Log Stream
Compressed Log Files
Regular Log Data
Fault and Error
Other

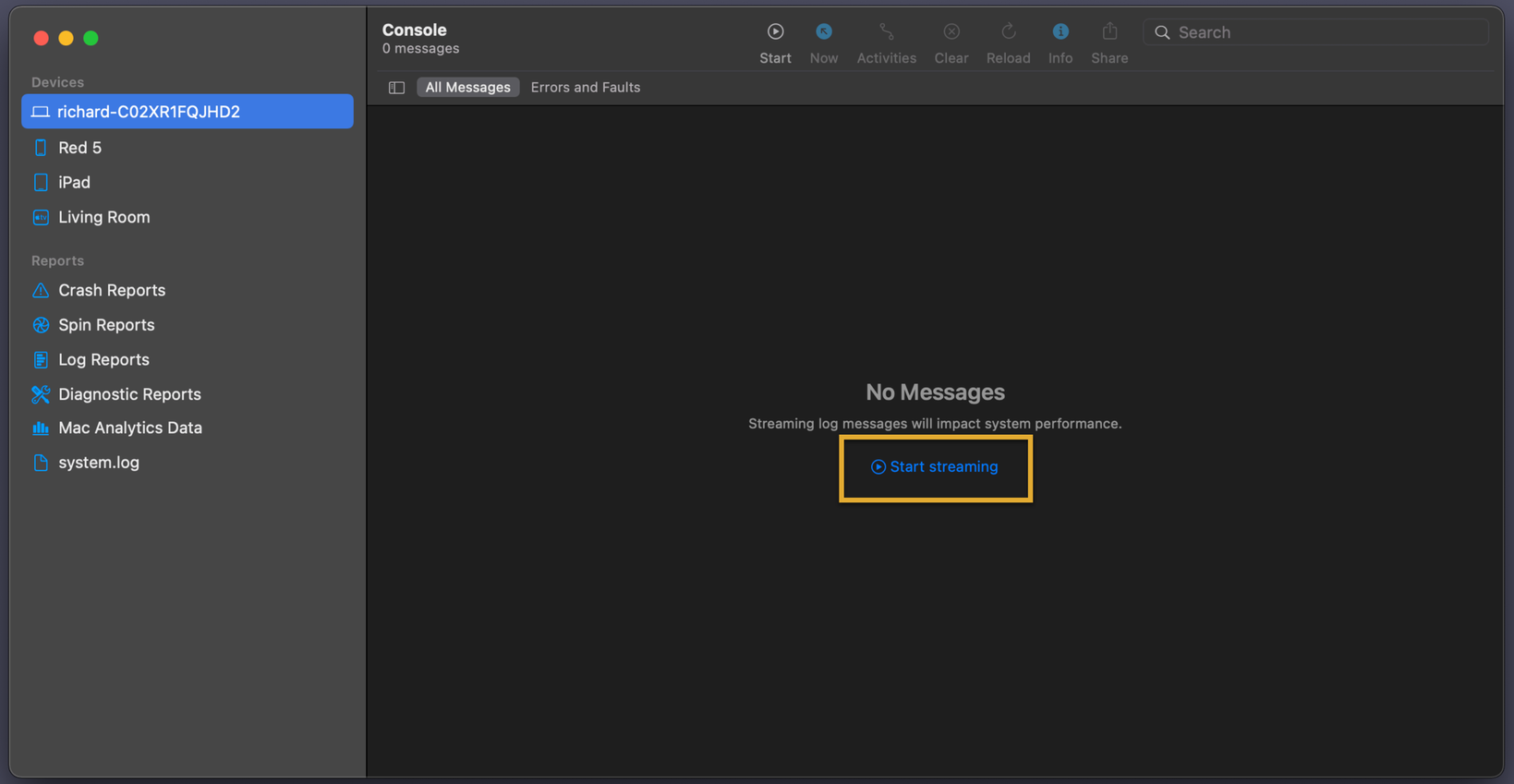
Accessing the logs

Console.app

log command line tool

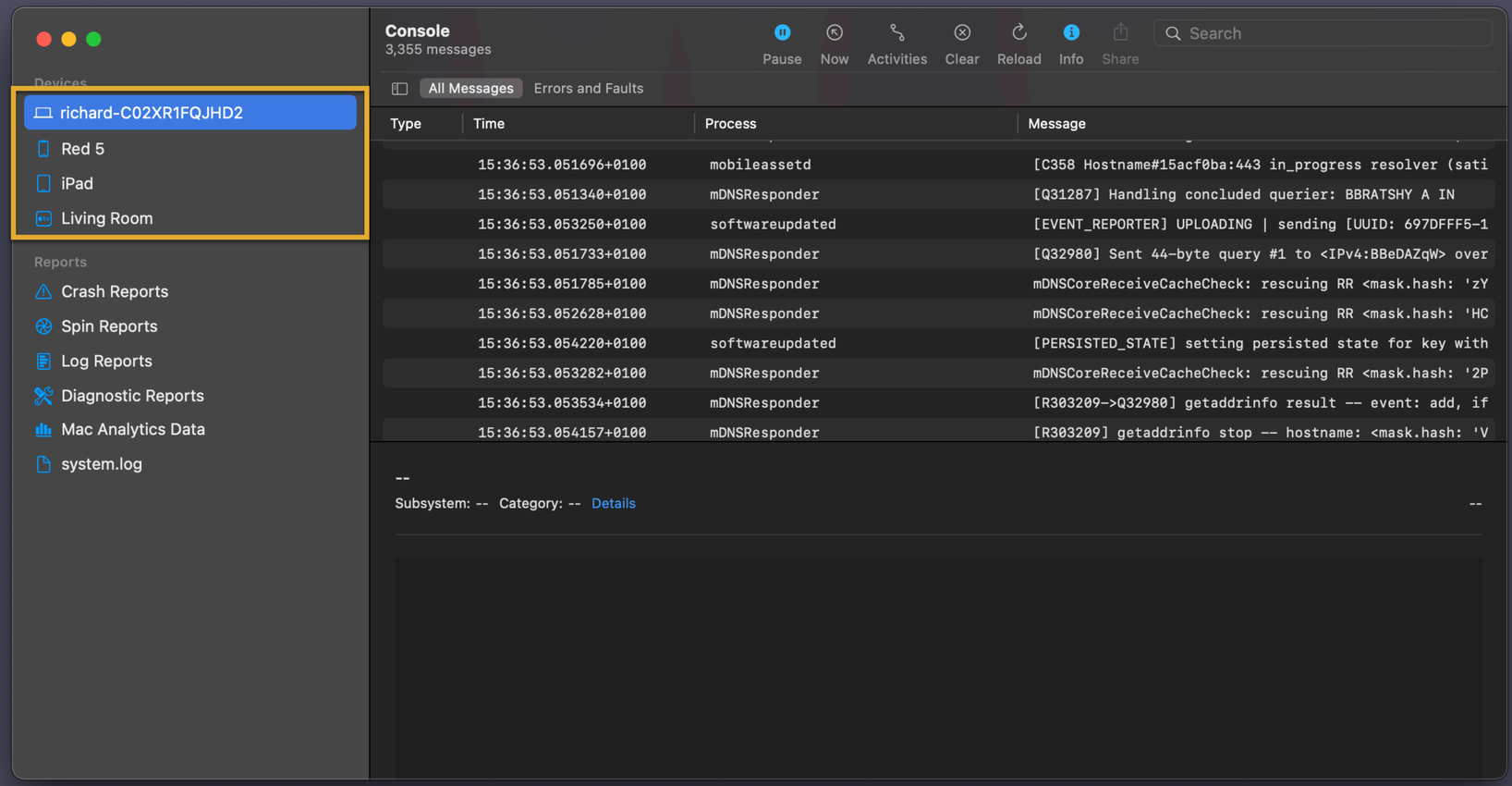

WARNIN
AY 7:36

Console.app


Console
0 messages
Start
Now
Activities
Clear
Reload
Info
Share
Search
All Messages
Errors and Faults
Devices
richard-C02XR1FQJHD2
Red 5
iPad
Living Room
Reports
Crash Reports
Spin Reports
Log Reports
Diagnostic Reports
Mac Analytics Data
system.log
No Messages
Streaming log messages will impact system performance.
Start streaming

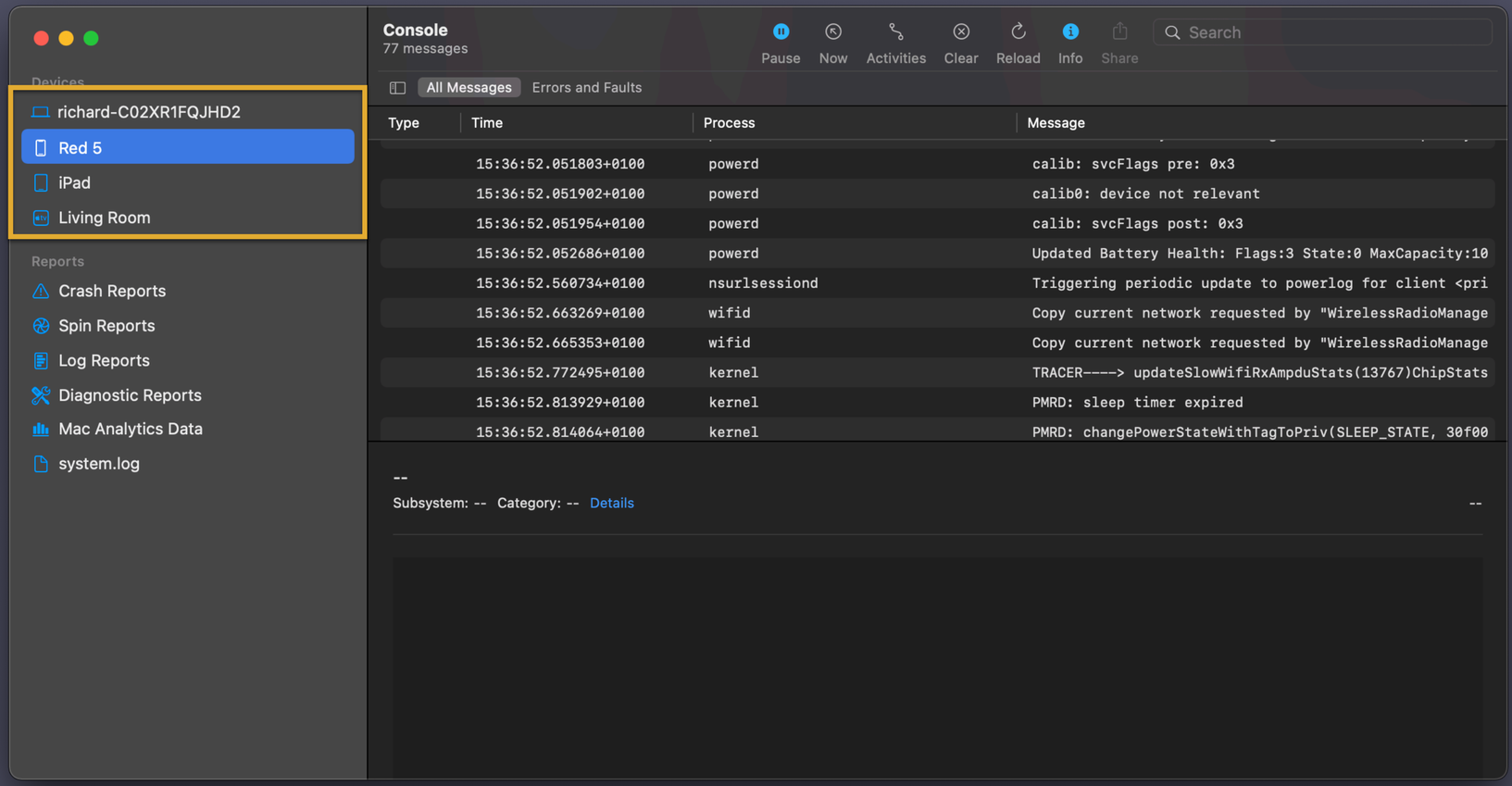

WARNIN
AY 7:36

Console.app


Console
3,355 messages
Pause
Now
Activities
Clear
Reload
Info
Share
Search
All Messages
Errors and Faults
Devices
richard-C02XR1FQJHD2
Red 5
iPad
Living Room
Reports
Crash Reports
Spin Reports
Log Reports
Diagnostic Reports
Mac Analytics Data
system.log
Type
Time
Process
Message
15:36:53.051696+0100 mobileassetd [C358 Hostname#15acf0ba:443 in_progress resolver (sati
15:36:53.051340+0100 mDNSResponder [Q31287] Handling concluded querier: BBRATSHY A IN
15:36:53.053250+0100 softwareupdated [EVENT_REPORTER] UPLOADING | sending [UUID: 697DFFF5-1
15:36:53.051733+0100 mDNSResponder [Q32980] Sent 44-byte query #1 to <IPv4:BBeDAZqW> over
15:36:53.051785+0100 mDNSResponder mDNSCoreReceiveCacheCheck: rescuing RR <mask.hash: 'zY
15:36:53.052628+0100 mDNSResponder mDNSCoreReceiveCacheCheck: rescuing RR <mask.hash: 'HC
15:36:53.054220+0100 softwareupdated [PERSISTED_STATE] setting persisted state for key with
15:36:53.053282+0100 mDNSResponder mDNSCoreReceiveCacheCheck: rescuing RR <mask.hash: '2P
15:36:53.053534+0100 mDNSResponder [R303209->Q32980] getaddrinfo result -- event: add, if
15:36:53.054157+0100 mDNSResponder [R303209] getaddrinfo stop -- hostname: <mask.hash: 'V
--
Subsystem: -- Category: -- Details
--

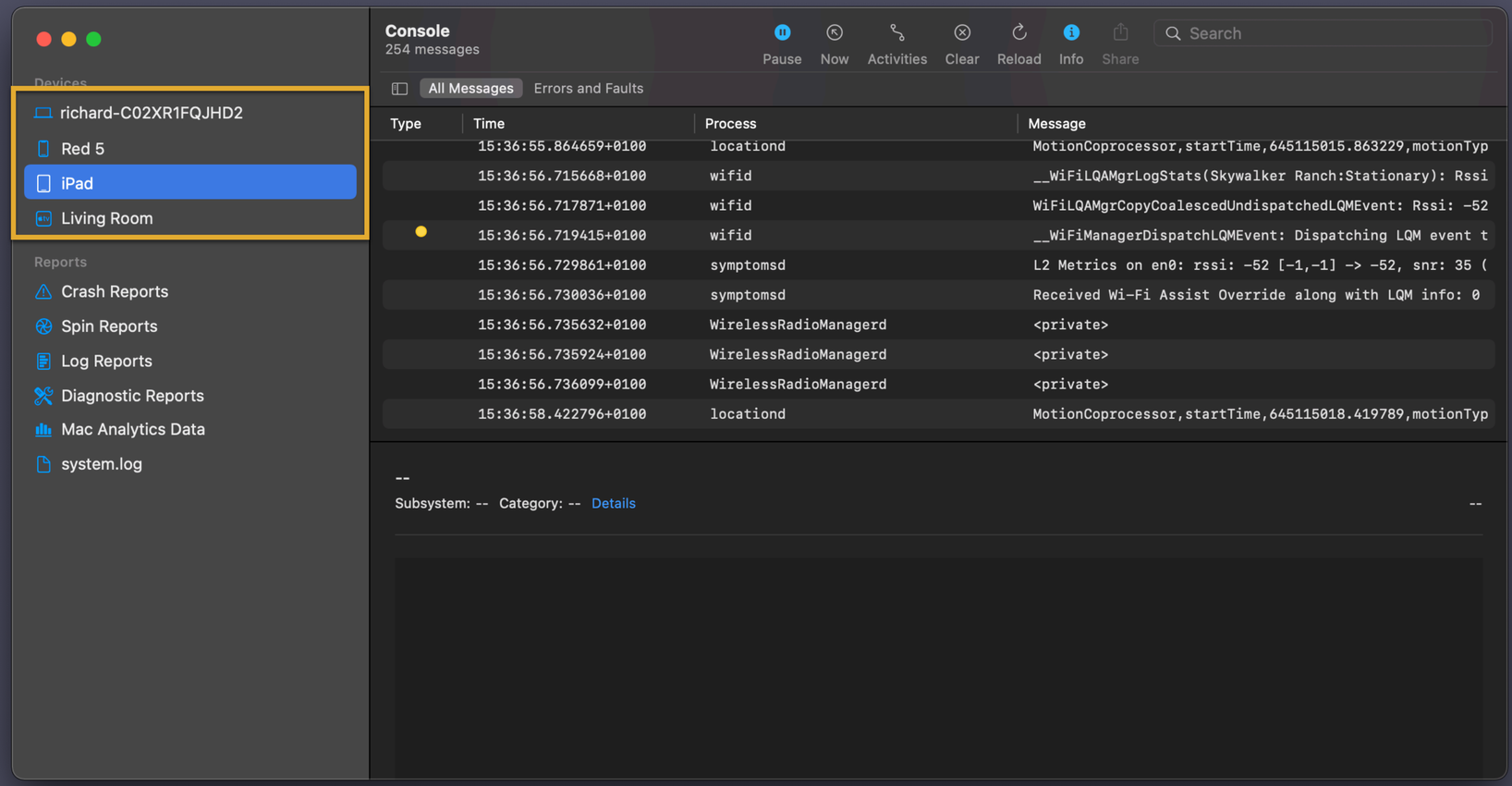

WARNIN
AY 7:36

Console.app


Console
77 messages
Pause
Now
Activities
Clear
Reload
Info
Share
Search
All Messages
Errors and Faults
Devices
richard-C02XR1FQJHD2
Red 5
iPad
Living Room
Reports
Crash Reports
Spin Reports
Log Reports
Diagnostic Reports
Mac Analytics Data
system.log
Type
Time
Process
Message
15:36:52.051803+0100 powerd calib: svcFlags pre: 0x3
15:36:52.051902+0100 powerd calib0: device not relevant
15:36:52.051954+0100 powerd calib: svcFlags post: 0x3
15:36:52.052686+0100 powerd Updated Battery Health: Flags:3 State:0 MaxCapacity:10
15:36:52.560734+0100 nsurlsessiond Triggering periodic update to powerlog for client <pri
15:36:52.663269+0100 wifid Copy current network requested by "WirelessRadioManage
15:36:52.665353+0100 wifid Copy current network requested by "WirelessRadioManage
15:36:52.772495+0100 kernel TRACER----> updateSlowWifiRxAmpduStats(13767)ChipStats
15:36:52.813929+0100 kernel PMRD: sleep timer expired
15:36:52.814064+0100 kernel PMRD: changePowerStateWithTagToPriv(SLEEP_STATE, 30f00
--
Subsystem: -- Category: -- Details
--

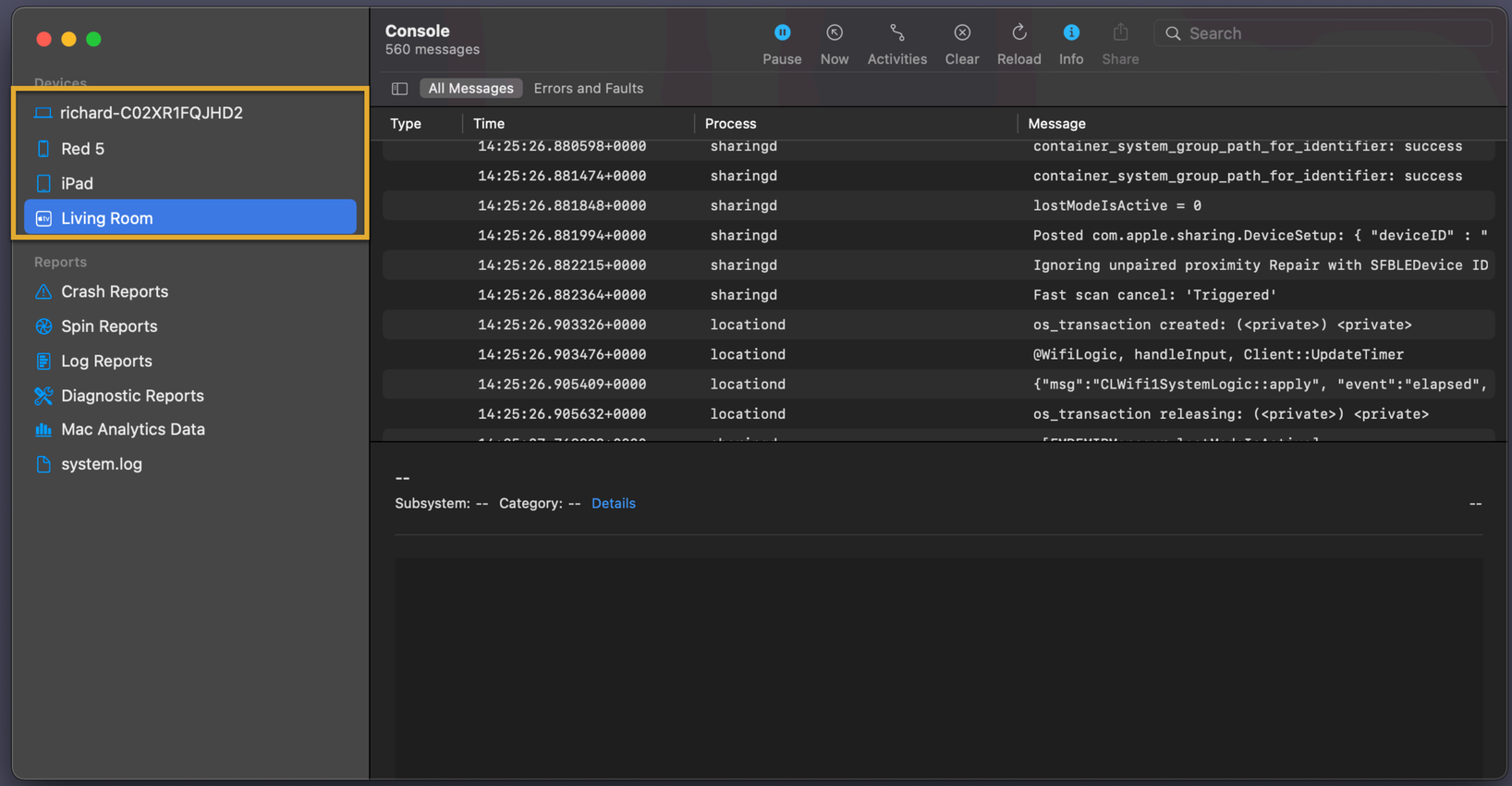

WARNIN
AY 7:36

Console.app


Console
254 messages
Pause
Now
Activities
Clear
Reload
Info
Share
Search
All Messages
Errors and Faults
Devices
richard-C02XR1FQJHD2
Red 5
iPad
Living Room
Reports
Crash Reports
Spin Reports
Log Reports
Diagnostic Reports
Mac Analytics Data
system.log
Type
Time
Process
Message
15:36:55.864659+0100 locationd MotionCoprocessor,startTime,645115015.863229,motionTyp
15:36:56.715668+0100 wifid __WiFiLQAMgrLogStats(Skywalker Ranch:Stationary): Rssi
15:36:56.717871+0100 wifid WiFiLQAMgrCopyCoalescedUndispatchedLQMEvent: Rssi: -52
15:36:56.719415+0100 wifid __WiFiManagerDispatchLQMEvent: Dispatching LQM event t
15:36:56.729861+0100 symptomsd L2 Metrics on en0: rssi: -52 [-1,-1] -> -52, snr: 35 (
15:36:56.730036+0100 symptomsd Received Wi-Fi Assist Override along with LQM info: 0
15:36:56.735632+0100 WirelessRadioManagerd <private>
15:36:56.735924+0100 WirelessRadioManagerd <private>
15:36:56.736099+0100 WirelessRadioManagerd <private>
15:36:58.422796+0100 locationd MotionCoprocessor,startTime,645115018.419789,motionTyp
--
Subsystem: -- Category: -- Details
--


WARNIN
AY 7:36

Console.app


Console
560 messages
Pause
Now
Activities
Clear
Reload
Info
Share
Search
All Messages
Errors and Faults
Devices
richard-C02XR1FQJHD2
Red 5
iPad
Living Room
Reports
Crash Reports
Spin Reports
Log Reports
Diagnostic Reports
Mac Analytics Data
system.log
Type
Time
Process
Message
14:25:26.880598+0000 sharingd container_system_group_path_for_identifier: success
14:25:26.881474+0000 sharingd container_system_group_path_for_identifier: success
14:25:26.881848+0000 sharingd lostModeIsActive = 0
14:25:26.881994+0000 sharingd Posted com.apple.sharing.DeviceSetup: { "deviceID" : "
14:25:26.882215+0000 sharingd Ignoring unpaired proximity Repair with SFBLEDevice ID
14:25:26.882364+0000 sharingd Fast scan cancel: 'Triggered'
14:25:26.903326+0000 locationd os_transaction created: (<private>) <private>
14:25:26.903476+0000 locationd @WifiLogic, handleInput, Client::UpdateTimer
14:25:26.905409+0000 locationd {"msg":"CLWifi1SystemLogic::apply", "event":"elapsed",
14:25:26.905632+0000 locationd os_transaction releasing: (<private>) <private>
--
Subsystem: -- Category: -- Details
--

Console.app

Log Level Colours

Default

Info

Debug

Error

Fault

Console.app

Demo

log

log

```
richard — -bash — 107×28
macbook:~ richard$ log
usage:
    log <command>

global options:
    -?, --help
    -q, --quiet
    -v, --verbose

commands:
    collect         gather system logs into a log archive
    config          view/change logging system settings
    erase           delete system logging data
    show            view/search system logs
    stream          watch live system logs
    stats           show system logging statistics

further help:
    log help <command>
    log help predicates
macbook:~ richard$
```

log stream – Live logs

log

```
richard — log stream — 155×36
macbook:~ richard$ log stream
Timestamp                       Thread     Type        Activity             PID    TTL
2021-06-11 16:00:55.320874+0100 0xd3ae7c   Default     0x0                  148    0    revisiond: (ChunkingLibrary) [com.apple.chunkinglibrary:default] ty
peHint:png typeRequested:kCKProfileTypeFixed typeUsed:kCKProfileTypeFixed sectionCount:1 default:F resolvedType:(null) serverConfig:(null)
2021-06-11 16:00:55.461385+0100 0xd3ae7c   Default     0x0                  148    0    revisiond: (ChunkingLibrary) [com.apple.chunkinglibrary:default] ty
peHint:jpg typeRequested:kCKProfileTypeFixed typeUsed:kCKProfileTypeFixed sectionCount:1 default:F resolvedType:(null) serverConfig:(null)
2021-06-11 16:00:55.511616+0100 0xd3ae7c   Default     0x0                  148    0    revisiond: (ChunkingLibrary) [com.apple.chunkinglibrary:default] ty
peHint:jpg typeRequested:kCKProfileTypeFixed typeUsed:kCKProfileTypeFixed sectionCount:1 default:F resolvedType:(null) serverConfig:(null)
2021-06-11 16:00:55.561030+0100 0xd3ae7c   Default     0x0                  148    0    revisiond: (ChunkingLibrary) [com.apple.chunkinglibrary:default] ty
peHint:jpg typeRequested:kCKProfileTypeFixed typeUsed:kCKProfileTypeFixed sectionCount:1 default:F resolvedType:(null) serverConfig:(null)
2021-06-11 16:00:55.611822+0100 0xd3ae7c   Default     0x0                  148    0    revisiond: (ChunkingLibrary) [com.apple.chunkinglibrary:default] ty
peHint:jpg typeRequested:kCKProfileTypeFixed typeUsed:kCKProfileTypeFixed sectionCount:1 default:F resolvedType:(null) serverConfig:(null)
2021-06-11 16:00:55.660972+0100 0xd3ae7c   Default     0x0                  148    0    revisiond: (ChunkingLibrary) [com.apple.chunkinglibrary:default] ty
peHint:jpg typeRequested:kCKProfileTypeFixed typeUsed:kCKProfileTypeFixed sectionCount:1 default:F resolvedType:(null) serverConfig:(null)
2021-06-11 16:00:55.711295+0100 0xd3ae7c   Default     0x0                  148    0    revisiond: (ChunkingLibrary) [com.apple.chunkinglibrary:default] ty
peHint:jpg typeRequested:kCKProfileTypeFixed typeUsed:kCKProfileTypeFixed sectionCount:1 default:F resolvedType:(null) serverConfig:(null)
2021-06-11 16:00:55.761926+0100 0xd3ae7c   Default     0x0                  148    0    revisiond: (ChunkingLibrary) [com.apple.chunkinglibrary:default] ty
peHint:png typeRequested:kCKProfileTypeFixed typeUsed:kCKProfileTypeFixed sectionCount:1 default:F resolvedType:(null) serverConfig:(null)
2021-06-11 16:00:55.814388+0100 0xd3ae7c   Default     0x0                  148    0    revisiond: (ChunkingLibrary) [com.apple.chunkinglibrary:default] ty
peHint:png typeRequested:kCKProfileTypeFixed typeUsed:kCKProfileTypeFixed sectionCount:1 default:F resolvedType:(null) serverConfig:(null)
2021-06-11 16:00:55.862062+0100 0xd3ae7c   Default     0x0                  148    0    revisiond: (ChunkingLibrary) [com.apple.chunkinglibrary:default] ty
peHint:png typeRequested:kCKProfileTypeFixed typeUsed:kCKProfileTypeFixed sectionCount:1 default:F resolvedType:(null) serverConfig:(null)
2021-06-11 16:00:55.911922+0100 0xd3ae7c   Default     0x0                  148    0    revisiond: (ChunkingLibrary) [com.apple.chunkinglibrary:default] ty
peHint:jpg typeRequested:kCKProfileTypeFixed typeUsed:kCKProfileTypeFixed sectionCount:1 default:F resolvedType:(null) serverConfig:(null)
2021-06-11 16:00:55.962468+0100 0xd3ae7c   Default     0x0                  148    0    revisiond: (ChunkingLibrary) [com.apple.chunkinglibrary:default] ty
peHint:jpg typeRequested:kCKProfileTypeFixed typeUsed:kCKProfileTypeFixed sectionCount:1 default:F resolvedType:(null) serverConfig:(null)
2021-06-11 16:00:56.012184+0100 0xd3ae7c   Default     0x0                  148    0    revisiond: (ChunkingLibrary) [com.apple.chunkinglibrary:default] ty
peHint:png typeRequested:kCKProfileTypeFixed typeUsed:kCKProfileTypeFixed sectionCount:1 default:F resolvedType:(null) serverConfig:(null)
2021-06-11 16:00:56.062063+0100 0xd3ae7c   Default     0x0                  148    0    revisiond: (ChunkingLibrary) [com.apple.chunkinglibrary:default] ty
peHint:jpeg typeRequested:kCKProfileTypeFixed typeUsed:kCKProfileTypeFixed sectionCount:1 default:F resolvedType:(null) serverConfig:(null)
2021-06-11 16:00:56.122339+0100 0xd3b2ee   Activity    0x23d7a3d            68660  0    GoogleSoftwareUpdateDaemon: (Security) SecTrustEvaluateIfNecessary
2021-06-11 16:00:56.122359+0100 0xd3b134   Activity    0x23d7a3f            68660  0    GoogleSoftwareUpdateDaemon: (Security) SecTrustEvaluateIfNecessary
2021-06-11 16:00:56.122382+0100 0xd3b2f0   Activity    0x23d7a50            68660  0    GoogleSoftwareUpdateDaemon: (Security) SecTrustEvaluateIfNecessary
2021-06-11 16:00:56.122388+0100 0xd3b2f1   Activity    0x23d7a3e            68660  0    GoogleSoftwareUpdateDaemon: (Security) SecTrustEvaluateIfNecessary
2021-06-11 16:00:56.122508+0100 0xd3b2ef   Activity    0x23d7a51            68660  0    GoogleSoftwareUpdateDaemon: (Security) SecTrustEvaluateIfNecessary
2021-06-11 16:00:56.122725+0100 0xd3b2ec   Activity    0x23d7a52            68660  0    GoogleSoftwareUpdateDaemon: (Security) SecTrustEvaluateIfNecessary
```

log show – Historical logs

log

```
richard — -bash — 152×34
macbook:~ richard$ log show
Skipping info and debug messages, pass --info and/or --debug to include.
Timestamp                       Thread     Type        Activity            PID    TTL
2021-05-24 11:21:02.856136+0100 0x0        Timesync    0x0                 0      0    === log class: TTL more than 14 days begins
2021-05-24 21:37:55.092132+0000 0x0        Timesync    0x0                 0      0    === system boot: DABA53C8-718B-4452-BBB4-64430EF67C18
2021-05-24 21:38:11.452295+0000 0x334      Default     0x0                 76     3    bluetoothd: [com.apple.bluetooth:bluetoothd] DaemonSetupPCIeTran
sportHostController BTI showed up
2021-05-24 21:38:11.473626+0000 0x333      Fault       0xa0                75     14   recoveryosd: (RecoveryOS) <private>
2021-05-24 21:38:11.487138+0000 0x334      Error       0x0                 76     3    bluetoothd: [com.apple.bluetooth:bluetoothd] DaemonSetupPCIeTran
sportHostController unable to find io service
2021-05-24 21:38:11.491617+0000 0x333      Fault       0xa1                75     14   recoveryosd: (RecoveryOS) <private>
2021-05-24 21:38:11.529955+0000 0x334      Error       0x0                 76     3    bluetoothd: (IOBluetooth) [com.apple.bluetooth:bluetoothd] No Bl
uetooth preference file
2021-05-24 21:38:11.546368+0000 0x334      Fault       0xb1                76     14   bluetoothd: (CoreFoundation) [com.apple.defaults:User Defaults]
Couldn't write values for keys (
    DeviceCache
) in CFPrefsPlistSource<0x7ffb85c05960> (Domain: com.apple.Bluetooth, User: kCFPreferencesAnyUser, ByHost: Yes, Container: (null), Contents Need Refresh
: No): setting preferences outside an application's container requires user-preference-write or file-write-data sandbox access
2021-05-24 21:38:11.547831+0000 0x334      Fault       0xb2                76     14   bluetoothd: (CoreFoundation) [com.apple.defaults:User Defaults]
Couldn't write values for keys (
    PersistentPortsServices
) in CFPrefsPlistSource<0x7ffb85c05960> (Domain: com.apple.Bluetooth, User: kCFPreferencesAnyUser, ByHost: Yes, Container: (null), Contents Need Refresh
: No): setting preferences outside an application's container requires user-preference-write or file-write-data sandbox access
2021-05-24 21:38:11.548651+0000 0x334      Fault       0xb3                76     14   bluetoothd: (CoreFoundation) [com.apple.defaults:User Defaults]
Couldn't write values for keys (
    PersistentPorts
) in CFPrefsPlistSource<0x7ffb85c05960> (Domain: com.apple.Bluetooth, User: kCFPreferencesAnyUser, ByHost: Yes, Container: (null), Contents Need Refresh
: No): setting preferences outside an application's container requires user-preference-write or file-write-data sandbox access
2021-05-24 21:38:11.567106+0000 0x334      Fault       0xb4                76     14   bluetoothd: (CoreFoundation) [com.apple.defaults:User Defaults]
Couldn't write values for keys (
    BluetoothVersionNumber
) in CFPrefsPlistSource<0x7ffb85c05960> (Domain: com.apple.Bluetooth, User: kCFPreferencesAnyUser, ByHost: Yes, Container: (null), Contents Need Refresh
: No): setting preferences outside an application's container requires user-preference-write or file-write-data sandbox access
2021-05-24 21:38:11.762006+0000 0x334      Fault       0xb5                76     14   bluetoothd: (CoreFoundation) [com.apple.defaults:User Defaults]
```

log

By default info and debug messages are skipped

log show --info

log show --debug

Log

Filtering

log

Date and Time constraints

log

Show events relative to the end of the logs

log show --last 1

log show --last 1m

log show --last 1h

log show --last 1d

log show --last boot

log

Show events from a start date

Format YYYY-MM-DD HH:MM:SS

```
log show --start '2021-06-23 11:30:00'
```

log

Show events to an end date

Format YYYY-MM-DD HH:MM:SS

```
log show --end '2021-06-23 11:30:00'
```

log

Combine start and end dates

```
log show --start '2021-06-23 11:30:00' --end
'2021-06-23 11:31:00'
```

log

Predicate based filtering

We can use predicates to filter on subsystems, categories and other data

Predicate - subsystem

log show

Predicate - subsystem

log show `--predicate`

Predicate - subsystem

```
log show --predicate '                                    '
```

Predicate - subsystem

```
log show --predicate '                                    '
```

Predicate - subsystem

```
log show --predicate 'subsystem == "                                    "'
```

Predicate - subsystem

```
log show --predicate 'subsystem == "uk.co.datajar.psumaclogger"'
```

Predicate - category

```
log show --predicate '                    '
```

Predicate - category

```
log show --predicate 'category == "          "'
```

Predicate - category

```
log show --predicate 'category == "network"'
```

Predicate - subsystem and category

```
log show --predicate '
                     '
```

Predicate - subsystem and category

```
log show --predicate 'subsystem == "uk.co.datajar.psumaclogger"
                      '
```

Predicate - subsystem and category

```
log show --predicate 'subsystem == "uk.co.datajar.psumaclogger" and
                      '
```

Predicate - subsystem and category

```
log show --predicate 'subsystem == "uk.co.datajar.psumaclogger" and
category == "network"'
```

Predicate - subsystem and category with time constraint

```
log show --predicate 'subsystem == "uk.co.datajar.psumaclogger" and
category == "network"' --last 5m
```

Predicate - subsystem and category with time constraint

```
log show --predicate 'subsystem == "uk.co.datajar.psumaclogger" and category == "network"' --start '2021-06-23 11:30:00' --end '2021-06-23 11:31:00'
```

Predicate - eventMessage

```
log show --predicate '                                    '
```

Predicate - message

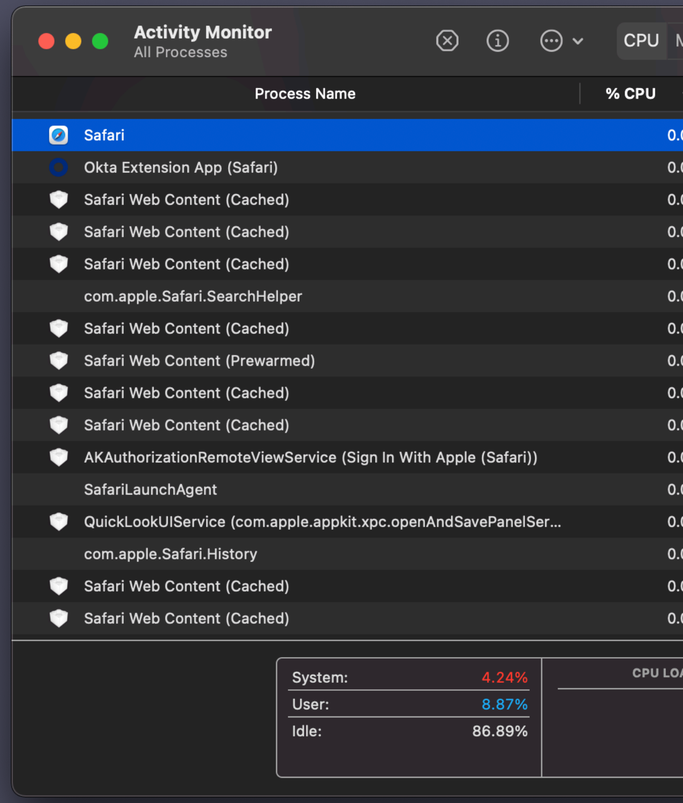
```
log show --predicate 'eventMessage contains "foobar"'
```

Predicate - subsystem, category and message

```
log show --predicate 'subsystem == "uk.co.datajar.psumaclogger" and
category == "network" and eventMessage contains "foobar"'
```

Predicate - process (the process that originated the event)

```
log show --predicate 'process == "Safari"'
```



Predicate - processImagePath (The full path of the process that originated the event)

```
log show --predicate 'process == "sudo"'
//Results

log show --predicate 'processImagePath == "sudo"'
//No Results

log show --predicate 'processImagePath contains "sudo"'
//Results

log show --predicate 'processImagePath == "/usr/bin/sudo"'
//Results
```

Predicate - sender (The name of the library, framework, kernel extension that originated the event)

Predicate - senderImagePath (The full path of the library, framework, kernel extension that originated the event)

Predicate - or

```
log show --predicate 'process == "Safari" or process == "Mail"'
```

Predicate - Grouping your logic

```
log show --predicate 'process == "su" or process == "sudo" and
eventMessage contains "tty"'
```

Predicate - Grouping your logic

```
log show --predicate 'process == "su" or process == "sudo" and
eventMessage contains "tty"'
```

Predicate - Grouping your logic

```
log show --predicate 'process == "su" or process == "sudo" and eventMessage contains "tty"'
```

Predicate - Grouping your logic

```
log show --predicate '(process == "su" or process == "sudo") and
eventMessage contains "tty"'
```

Predicate - case issues

```
log show --predicate 'process == "SaFaRi"'
```

Predicate - case insensitive

```
log show --predicate 'process ==[c] "SaFaRi"'
```

Predicate - case insensitive

```
log show --predicate 'process contains[c] "SaFaRi"'
```

Predicate - beginswith

```
log show --predicate 'process beginswith[c] "SaF"'
```

Predicate - endswith

```
log show --predicate 'process endswith[c] "Ari"'
```

Other Comparisons

Operator	Description
= ==	Equal
!= <>	Not equal
>= =>	Greater than or equal
<= =<	Less than or equal
>	Greater than
<	Less than
AND &&	Logical AND
OR ||	Logical OR
NOT !	Logic NOT

Other Comparisons

Operator	Description
BEGINSWITH	The left-hand expression begins with the right-hand expression
CONTAINS	The left-hand expression contains the right-hand expression
ENDSWITH	The left-hand expression ends with the right-hand expression
LIKE	The left hand expression equals the right-hand expression: ? and * are allowed as wildcard characters
MATCHES	The left hand expression equals the right hand expression using a regex-style comparison

log

Predicate - Documentation

https://developer.apple.com/library/mac/documentation/Cocoa/Conceptual/Predicates/Articles/pSyntax.html

Predicate - messageType

default (0) , info (1) , debug (2) , error (16) , fault (17)

```
log show --predicate 'messageType == "info"'
```

Log Archives

log

Can export yours logs to a .logarchive

Can specify last or start predicates

```
sudo log collect --last 5m --output ~/Desktop
```

log

Log Archives

Can open in Console App

Can also use

```
log show ~/Desktop/mylogs.logarchive
```

Collecting from other paired devices

`--device-name`

`--device-udid`

sudo log collect `--device-name iPad --last 5m --output ~/Desktop`

Predicate - Log Styles

```
--style default, compact, json, ndjson, syslog
```

Privacy

Privacy

We don’t want personal data leaking

Data that is dynamic is considered private

Collections of data (Arrays) are considered private

```
PSUMAC Logger: [uk.co.datajar.psumaclogger:password] Password is <private>
```

log

Privacy

For macOS 10.12 - 10.14, redaction can be disabled

```
sudo log config --mode 'private_data:on'
```

```
sudo log config --mode 'private_data:off'
```

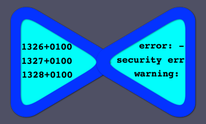
log

Privacy

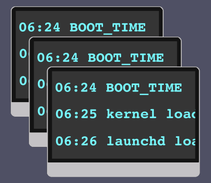
For macOS 10.15.3+ a configuration profile can be used

https://georgegarside.com/blog/macos/sierra-console-private/

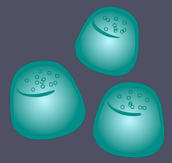
The Eclectic Light Company



Ulbow: Easy to use Log Browser



Consolation: Log Browser



Mints: Log toolbox

Blowhole : Log from command line

https://eclecticlight.co

https://github.com/dataJAR/psumac2021

Unified Logging