# Apple's Unified Logging for Sysadmins

MacSysAdmin 2017
Tim Sutton
Sauce Labs

to get some more staff for the channel that can help keep order as well as provide free osx server support to any that may enter. The goal of the channel is to provide a single spot where various osx administrators can talk about things such as Client Management, Image Deployment using DeployStudio/NetInstall/etc, Security, etc. For those who are interested, the channel info is as follows:

IRC Server - irc.freenode.net
IRC Channel - ##osx-server

My nick on freenode is blood, feel free to msg me at anytime for help with DeployStudio. Thank you.

2010-06-03 02:38:36                                                                                          #2

We now have 3 DeployStudio admins and 7 osx admins. Looking for osx/ds users to come join us in ##osx-server on irc.freenode.net

2010-06-05 20:33:25                                                                                          #3

We are now up to 4 DS admins and 12 osx admins. Head to irc.freenode.net  in ##osx-server if you want free live support for DeployStudio/OSX Server. You can grab any irc client you wish (mirc, xchat etc) to connect.

# MacSysAdmin 2010 (!)

# syslog

- syslog -w

  - -w waits for syslog information

- sudo syslog -c 0 -d

  - log everything: Emergency to Debug

- syslog -c 0

  - check filter mask

# Penn State MacAdmins 2012



**Ed Marczak: Logs, Damn Logs, and Statistics**

# log Command Line Tool

Same functionality as Console from the command line

Stream live log messages

```
$ log stream
$ log stream --predicate 'eventMessage contains "my message"'
```

Display a log file or archive

```
$ log show system_logs.logarchive
```

Enable debug for your subsystem on macOS

```
$ log config --mode "level:debug" --subsystem com.mycorp.myapp
```

```
→ syslog -w

NOTE:  Most system logs have moved to a new logging
system. See log(1) for more information.
```

# Curiosity

I told Tycho I would give a talk about Apple Unified Logging at MacSysAdmin

# Frustration

# Penn State MacAdmins 2017



PEELING BACK THE BARK

> @CHILCOTE

macops.ca/logging
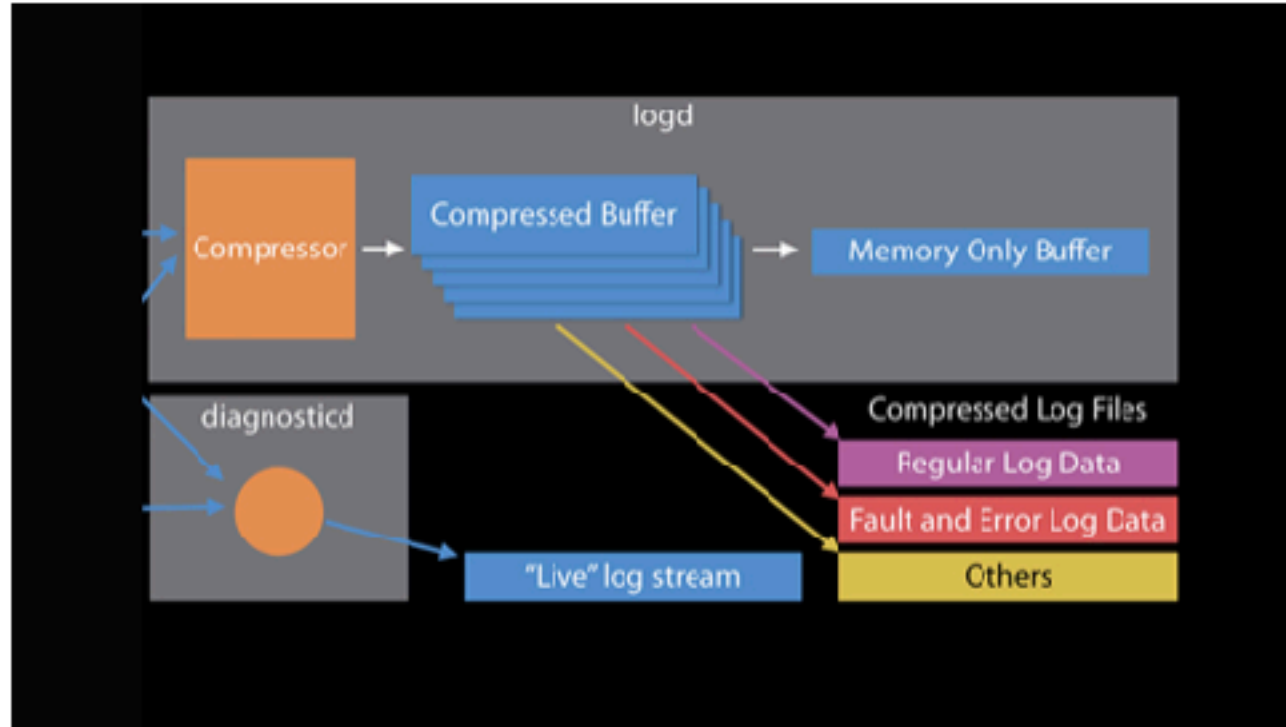
**Unified Logging and Activity Tracing**

Session 721 · iOS, macOS

The new Unified Logging and Tracing System for iOS and macOS uses Activity Tracing for performance, consolidates kernel and user-space logging, and has many other improvements. Learn how Logging and Tracing can help you debug and troubleshoot issues with your apps.

(https://developer.apple.com/videos/play/wwdc2016/721)

# Efficiency

- Logging now to a database, no plaintext - only `log` and Console can read these

- Persistence of log data varies depending on importance

- Message formatting happens at display / review time, not during writing

# Log message types, and scopes

- "Standard" types

  - Default

  - Info

  - Debug

- "Special" types

  - Error

  - Fault

- Events can belong to a subsystem, and categories within

# Privacy

```
{
  "category" : "Registration",
  "processImageUUID" : "E60289AD-3395-3F98-84AD-A6CDDF651631",
  "processUniqueID" : 334,
  "threadID" : 2895,
  "timestamp" : "2017-10-01 13:09:35.139280-0400",
  "traceID" : 28876680072396804,
  "messageType" : "Default",
  "senderProgramCounter" : 960056,
  "processID" : 334,
  "machTimestamp" : 31131983679,
  "timezoneName" : "",
  "subsystem" : "com.apple.IDS",
  "eventMessage" : "  ** Found signed in iCloud account: <private>",
  "senderImageUUID" : "E60289AD-3395-3F98-84AD-A6CDDF651631",
  "processImagePath" : "\/System\/Library\/PrivateFrameworks\/IDS.framework\/identityservicesd.app\/Contents\/MacOS\/iden
  "senderImagePath" : "\/System\/Library\/PrivateFrameworks\/IDS.framework\/identityservicesd.app\/Contents\/MacOS\/ident
}
```

# show vs. stream

Console.app 1.0

# Configuration

- `sudo log config --mode 'level:debug' --subsystem com.apple.WebDriver`

- logging configuration profile property list files

  - (Apple's words, not mine)

# Logging Preferences

```
→ ls /System/Library/Preferences/Logging/Subsystems

com.apple.Accessibility.plist          com.apple.TCC.plist                 com.apple.icloudpreferences.plist    com.apple.persona.plist
com.apple.AppKit.plist                 com.apple.TimeMachine.plist         com.apple.internetAccounts.plist     com.apple.pf.plist
com.apple.AppleIR.plist                com.apple.accounts.plist            com.apple.libsqlite3.plist           com.apple.photoanalysisd.graph.p
com.apple.AssetCache.plist             com.apple.amp.MediaServices.plist   com.apple.locationd.Core.plist       com.apple.photoanalysisd.job.pl
com.apple.AssetCacheServices.plist     com.apple.authkit.plist             com.apple.locationd.Legacy.plist     com.apple.photoanalysisd.plist
com.apple.BezelServices.plist          com.apple.avfaudio.plist            com.apple.locationd.Motion.plist     com.apple.pluginkit.plist
com.apple.DesktopServices.plist        com.apple.awd.awdd.plist            com.apple.locationd.Position.plist   Desk.apple.sandbox.reporting.pli
com.apple.ExchangeWebServices.plist    com.apple.awd.framework.plist       com.apple.locationd.Utility.plist    Exch.apple.sbd.plist
com.apple.Finder.plist                 com.apple.bluetooth.plist           com.apple.mDNSResponder.plist        Find.apple.securityd.plist
com.apple.HTTPServer.plist             com.apple.calendar.plist            com.apple.mac.install.plist          HTTP.apple.sharing.plist
com.apple.IPConfiguration.plist        com.apple.captive.plist             com.apple.mail.plist                 IPCo.apple.siri.plist
com.apple.ManagedClient.plist          com.apple.catalyst.plist            com.apple.mediaremote.plist          com.apple.social.plist
com.apple.NetworkSharing.plist         com.apple.cdp.plist                 com.apple.multipeerconnectivity.plist com.apple.socialpushagent.plist
com.apple.ProtectedCloudStorage.plist  com.apple.clouddocs.plist           com.apple.network.plist              Prot.apple.symptomsd.plist
com.apple.Safari.plist                 com.apple.coreanimation.plist       com.apple.networkextension.plist     com.apple.syncdefaults.plist
com.apple.SafariShared.plist           com.apple.coreaudio.plist           com.apple.networkserviceproxy.plist  com.apple.useractivity.plist
com.apple.SkyLight.plist               com.apple.coredata.plist            com.apple.nlcd.plist
com.apple.StandaloneHIDFudPlugins.plist com.apple.duetactivityscheduler.plist com.apple.notes.plist
com.apple.SystemConfiguration.plist    com.apple.eapol.plist               com.apple.passkit.plist


→ ls /System/Library/Preferences/Logging/Resources
com.apple.WebDriver.plist


→ ls /Library/Preferences/Logging/Subsystems

com.apple.WebDriver.plist              com.sentinelone.sentineld-helper.plist  com.sentinelone.sentineld.plist
com.sentinelone.sentineld-guard.plist  com.sentinelone.sentineld-updater.plist com.sentinelone.sentinelctl.plist
```

You can also override the logging behavior of a specific subsystem by creating and installing a logging configuration profile property list file in the `/Library/Preferences/Logging/Subsystems/` directory. Name the file using an identifier string, in reverse DNS notation, representing the subsystem. For example, `com.your_company.your_subsystem_name.plist`. Next, add one or more settings dictionaries to the top level of the file. A `DEFAULT-OPTIONS` settings dictionary defines global behavior settings for the entire subsystem. Category settings dictionaries define behavior for specific categories of messages within the subsystem. See Listing 8.

Listing 8 Top level structure of a logging profile

```
<dict>
    <key>DEFAULT-OPTIONS</key>
    <dict>
        <!-- GLOBAL SUBSYSTEM OR PROCESS SETTINGS -->
    </dict>
    <key>CategoryName</key>
    <dict>
        <!-- CATEGORY SETTINGS -->
    </dict>
</dict>
```

Each settings dictionary within a logging profile contains a `Level` subdictionary, which contains the following setting keys:

| Key | Description |
| --- | --- |
| Enable | Enables a specific log level. |

https://developer.apple.com/documentation/os/logging?language=objc

Instantly share code, notes, and snippets.

Create a gist now

zwaldowski / **Extra Logging for My Great App.mobileconfig**

★ Star  39     Fork  7

Last active 25 days ago

<> Code    ⟲ Revisions 6    ★ Stars 39    ⑂ Forks 7

Embed ▾    `<script src="https://gi`    ⧉    ⬇    Download ZIP

Apple Configuration Profile for Logging in iOS 10 and macOS Sierra

<> **Extra Logging for My Great App.mobileconfig**    Raw
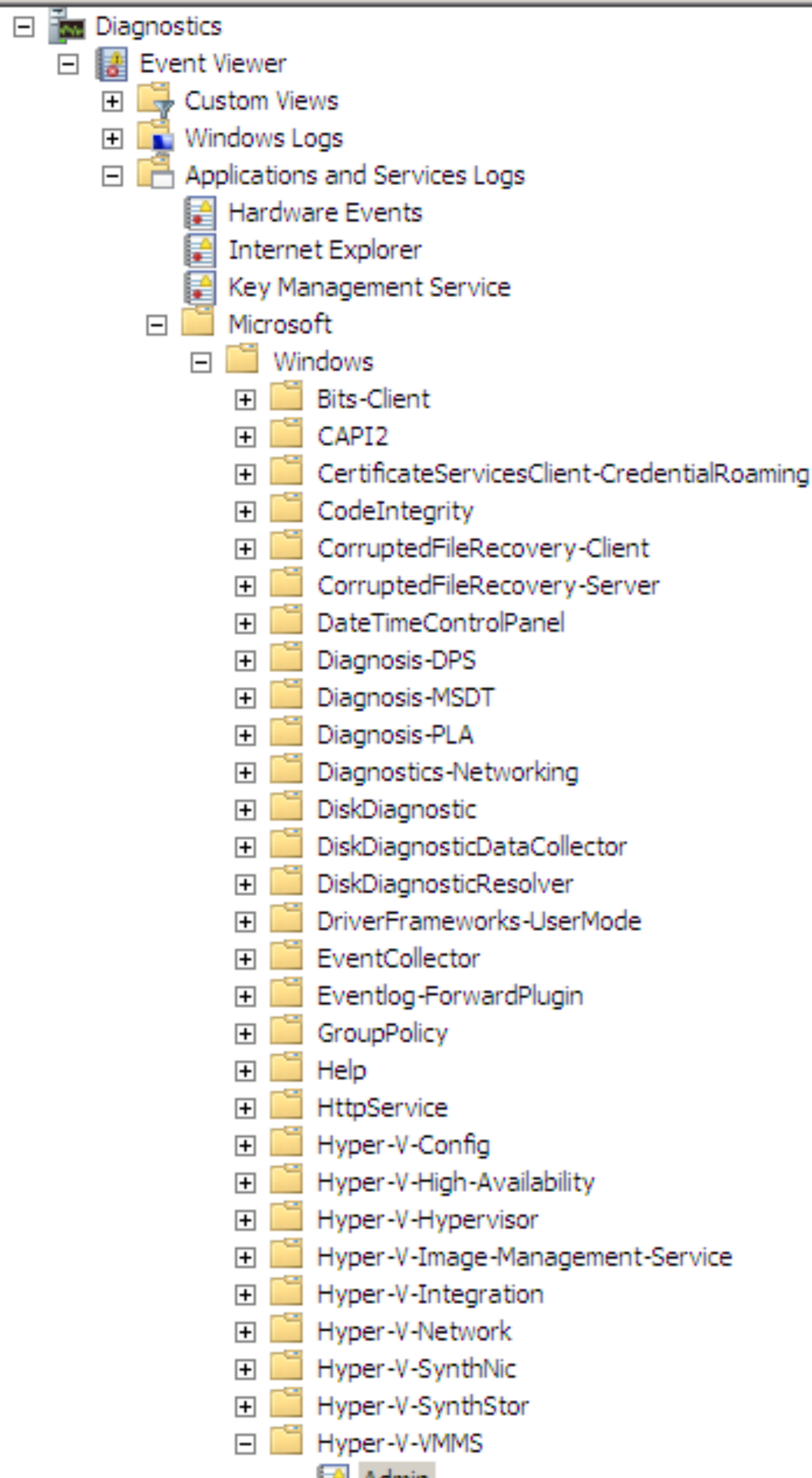
```
 1  <?xml version="1.0" encoding="UTF-8"?>
 2  <!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
 3  <plist version="1.0">
 4  <!-- iOS 10, macOS Sierra, and friends bring a new logging subsystem that's
 5  supposed to scale from the kernel, up to frameworks, and up to apps. It defaults
 6  to a more regimented, privacy-focused approach that large apps and complex
 7  systems need.
 8
 9  It, along with Activity Tracing introduced in iOS 8 and macOS Yosemite and the
10  Console app in macOS Sierra, hope to help you graduate from caveman debugging to
11  quickly identify issues across time, events, user input, and even process
12  boundaries.
13
14  This configuration profile template allows you to change logging behaviors
15  for your app, your frameworks, third party code, and even Apple code without
16  access to the source. The idea is to leave all your logging code in your app —
17  even when shipping — and change the information level at runtime.
18
19  Read more about this:
20   - https://developer.apple.com/reference/os/1891852-logging
21   - https://developer.apple.com/videos/play/wwdc2016/721/
22
23  You can modify and install this payload by double-clicking it in macOS, or on
24  an iOS-based device using Apple Configurator. You can also use Apple
25  Configurator to sign and send this profile to others.
26
27  This, too, is all documented:
28  - https://developer.apple.com/library/ios/documentation/NetworkingInternet/Conceptual/iPhoneOTAConfiguration/Introduction/Intro
29  - https://developer.apple.com/library/ios/featuredarticles/iPhoneConfigurationProfileRef/Introduction/Introduction.html
30  - http://nshipster.com/configuration-profiles/
31
32  And, always remember: assume positive intent. -->
33  <dict>
34      <!-- Change this UUID using `uuidgen`. -->
35      <key>PayloadUUID</key>
36      <st
37      <!-
38      <key
39      <integer>1</integer>
40      <!-- Change this identifier and other info based on your credentials. -->
```

```
 76          <key>com.great-company.my-great-app</key>
 77          <dict>
 78              <key>DEFAULT-OPTIONS</key>
 79              <dict>
 80                  <key>Level</key>
 81                  <dict>
 82                      <!-- The lowest-level log that's enabled.
 83                      All log messages sent through NSLog are at
 84                      the Default level.
 85
 86                      Accepted values:
 87                       - Inherit: The default. Categories inherit
 88                         subsystem behavior, subsystems inherit the
 89                         system (OS) behavior.
 90                       - Default: Only default-level messages.
 91                       - Info: Default-level and info-level messages.
 92                       - Debug: All messages. -->
 93                      <key>Enable</key>
 94                      <string>Debug</string>
 95                      <!-- The lowest-level log that's written to
 96                      disk.
 97
 98                      Accepted values:
 99                       - Inherit: The default. Categories inherit
100                         subsystem behavior, subsystems inherit the
101                         system (OS) behavior.
102                       - Default: Only default-level messages.
103                       - Info: Default-level and info-level messages.
104                       - Debug: All messages. -->
105                      <key>Persist</key>
106                      <string>Debug</string>
107                  </dict>
108                  <!-- Changes how `%@` et. al. are formatted into
109                  the log.
110
111                  To ensure the privacy of users, it is recommended
112                  that log messages consist strictly of static strings
113                  and numbers.
114
115                  Accepted values:
116                   - Inherit. The default. Categories inherit
117                     subsystem behavior, subsystems inherit the
118                     system (OS) behavior.
119                   - Public: Dynamic strings and complex dynamic
120                     objects are collected for the log.
121                   - Private: Static strings and numbers are collected
122                     for the log. -->
123                  <key>Default-Privacy-Setting</key>
124                  <string>Public</string>
125                  <!-- Changes how long non-critical messages stay
126                  in the log, in days (I think).
127
128                  Keys for this dictionary are the non-critical
129                  log levels: Default, Debug, and Info. -->
133                  <integer>14</integer>
134              </dict>
```

https://gist.github.com/zwaldowski/f9c82dfe1595506a36bd71f55cbb7538

/usr/bin/log

# Windows: APIs vs. Files

Diagnostics
- Event Viewer
  - Custom Views
  - Windows Logs
  - Applications and Services Logs
    - Hardware Events
    - Internet Explorer
    - Key Management Service
    - Microsoft
      - Windows
        - Bits-Client
        - CAPI2
        - CertificateServicesClient-CredentialRoaming
        - CodeIntegrity
        - CorruptedFileRecovery-Client
        - CorruptedFileRecovery-Server
        - DateTimeControlPanel
        - Diagnosis-DPS
        - Diagnosis-MSDT
        - Diagnosis-PLA
        - Diagnostics-Networking
        - DiskDiagnostic
        - DiskDiagnosticDataCollector
        - DiskDiagnosticResolver
        - DriverFrameworks-UserMode
        - EventCollector
        - Eventlog-ForwardPlugin
        - GroupPolicy
        - Help
        - HttpService
        - Hyper-V-Config
        - Hyper-V-High-Availability
        - Hyper-V-Hypervisor
        - Hyper-V-Image-Management-Service
        - Hyper-V-Integration
        - Hyper-V-Network
        - Hyper-V-SynthNic
        - Hyper-V-SynthStor
        - Hyper-V-VMMS
          - Admin

**Admin    118 Events**

Filtered:Log: Microsoft-Windows-Hyper-V-VMMS-Admin; Levels: Warning,

| Level | Date and Time | Source | Event ID | Task C... |
|---|---|---|---|---|
| Information | 1/25/2009 7:28:19 PM | Hyper-... | 19020 | None |
| Information | 1/25/2009 7:28:19 PM | Hyper-... | 19020 | None |
| Information | 1/25/2009 7:28:19 PM | Hyper-... | 14094 | None |
| Information | 1/25/2009 7:28:00 PM | Hyper-... | 19040 | None |
| Information | 1/25/2009 7:28:00 PM | Hyper-... | 19040 | None |
| Information | 1/25/2009 7:28:00 PM | Hyper-... | 14092 | None |
| Information | 1/25/2009 7:27:58 PM | Hyper-... | 19020 | None |
| Information | 1/25/2009 7:27:58 PM | Hyper-... | 19020 | None |
| Information | 1/25/2009 7:27:58 PM | Hyper-... | 14094 | None |
| Information | 1/25/2009 7:27:53 PM | Hyper-... | 19040 | None |
| Information | 1/25/2009 7:27:53 PM | Hyper-... | 19040 | None |
| Information | 1/25/2009 7:27:53 PM | Hyper-... | 14092 | None |
| Information | 1/25/2009 7:26:51 PM | Hyper-... | 19020 | None |
| Information | 1/25/2009 7:26:51 PM | Hyper-... | 19020 | None |
| Information | 1/25/2009 7:26:50 PM | Hyper-... | 14094 | None |
| Information | 1/25/2009 7:26:43 PM | Hyper-... | 19040 | None |

**Event 19020, Hyper-V-VMMS**

General | Details

The WMI provider 'VmmsWmiEventProvider' has started.

| | | | |
|---|---|---|---|
| Log Name: | Microsoft-Windows-Hyper-V-VMMS/Admin | | |
| Source: | Hyper-V-VMMS | Logged: | 1/25/20 |
| Event ID: | 19020 | Task Category: | None |
| Level: | Information | Keywords: | |
| User: | SYSTEM | Computer: | benarn |
| OpCode: | Info | | |

More Information:    Event Log Online Help

**Actions**

**Admin**
- Open Saved Log...
- Create Custom View...
- Import Custom View...
- Clear Log...
- Filter Current Log...
- Clear Filter
- Properties
- Disable Log
- Find...
- Save Filtered Log File...
- Attach a Task To this ...
- Save Filter to Custom...
- View
- Refresh
- Help

**Event 19020, Hyper-V-V...**
- Event Properties
- Attach Task To This E...
- Copy
- Save Selected Events...
- Refresh
- Help
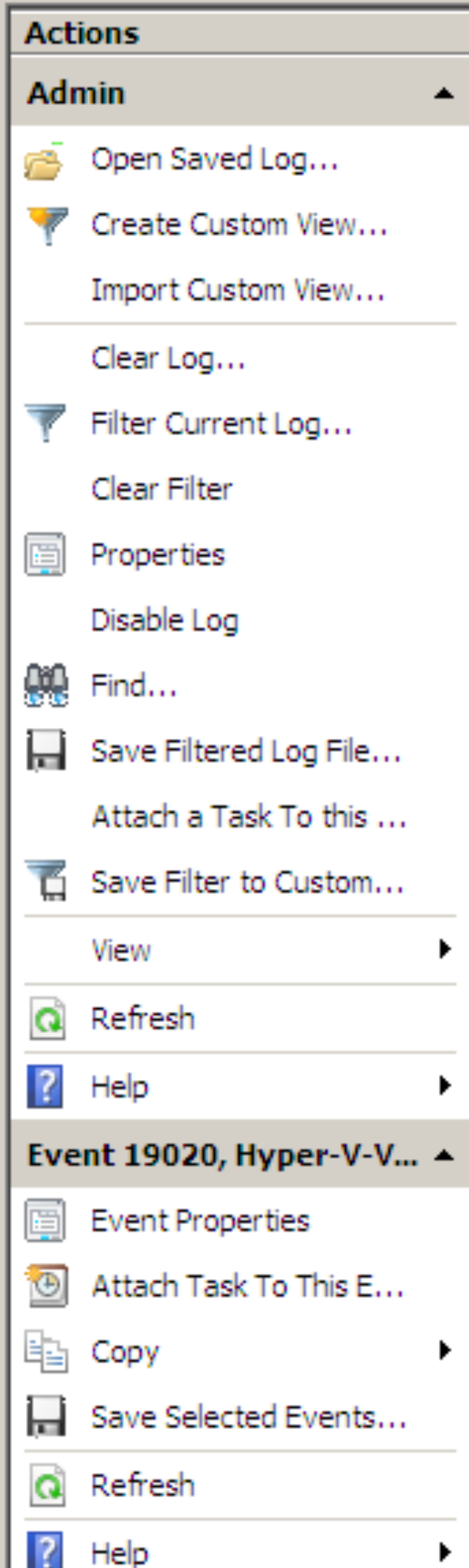
# Tips

# process/senderImagePath

- `--predicate processImagePath` and `senderImagePath` really are full paths, even though `log` and console show only the process *name* in typical output
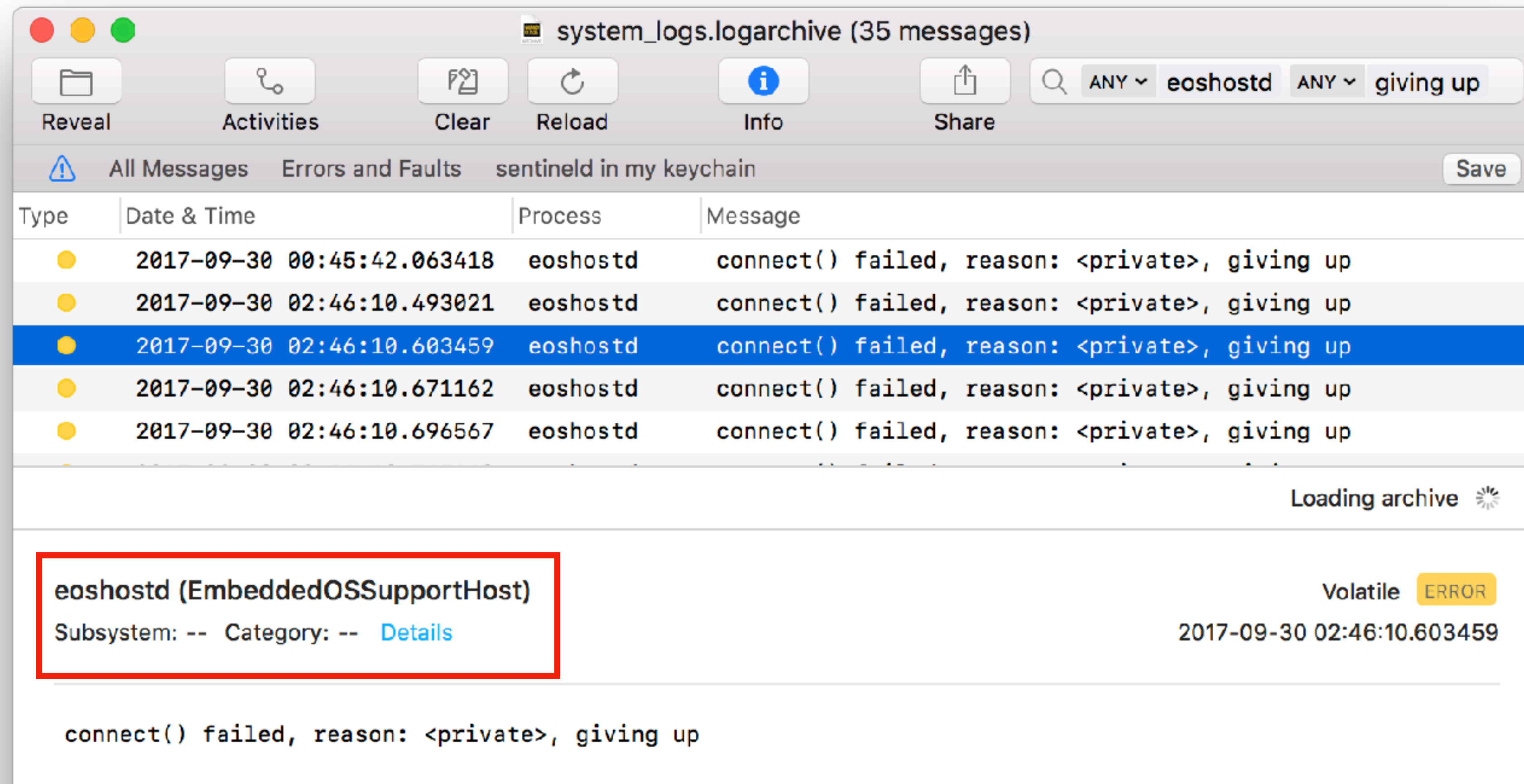
# process/senderImagePath

```
2017-09-30 02:46:10.603459-0400 0x840  Error   0x0   43   eoshostd: (EmbeddedOSSupportHost) connect() failed, reason: <private>, giving up
```

--style syslog

```
2017-09-30 02:46:10.603459-0400   localhost eoshostd[243]: (EmbeddedOSSupportHost) connect() failed, reason: <private>, giving up
```

--style json

```
{
    "processImageUUID" : "469A00D6-3C4F-33EE-95F1-EDE17BCCB531",
    "processUniqueID" : 243,
    "threadID" : 2112,
    "timestamp" : "2017-09-30 02:46:10.603459-0400",
    "traceID" : 1260856231845957636,
    "messageType" : "Error",
    "senderProgramCounter" : 293550405,
    "processID" : 243,
    "machTimestamp" : 159540275634612,
    "timezoneName" : "",
    "eventMessage" : "connect() failed, reason: <private>, giving up",
    "senderImageUUID" : "16538049-0951-3460-ABCD-8F6C06D631D6",
    "processImagePath" : "\/usr\/libexec\/eoshostd",
    "senderImagePath" : "\/System\/Library\/PrivateFrameworks\/EmbeddedOSSupportHost.framework\/Versions\/A\/EmbeddedOSSupport
}
```

| | | | |
|---|---|---|---|
| | 17:17:55.754017 | Dock | applying: <private> |
| | 17:17:55.754002 | Finder | applying: <private> |
| | 17:17:55.754030 | Finder | applying: <private> |
| ○ | 17:17:55.775395 | Mail | subsystem: com.apple.accountsui, category: InternetAccounts, enable_level: 0, persist_level: 0, default_ttl: 0, i |
| | | | 0, enable_oversize: 0, privacy_setting: 0 |
| ○ | 17:17:55.775786 | Mail | <private> |
| | 17:17:55.790184 | opendi… | Client: <private>, UID: 501, EUID: 501, GID: 20, EGID: 20 |
| | 17:17:55.790257 | opendi… | <private> completed, delivered 1 result |
| | 17:17:55.795080 | opendi… | Client: <private>, UID: 501, EUID: 501, GID: 20, EGID: 20 |
| | 17:17:55.795189 | opendi… | <private> completed, delivered 1 result |
| ○ | 17:17:55.814168 | Contac… | bundleid: com.apple.AddressBook, enable_level: 0, persist_level: 0, propagate_with_activity: 0 |
| | 17:17:55.814334 | Contac… | Created DB, header sequence number = 2468 |
| | 17:17:55.815994 | Contac… | Created DB, header sequence number = 2468 |
| ○ | 17:17:55.819282 | Contac… | subsystem: com.apple.launchservices, category: default, enable_level: 0, persist_level: 0, default_ttl: 0, info_t |
| | 17:17:55.835992 | mds | directQueryFetchResultsReply 126981 1795162176 0 |
| | 17:17:55.837648 | mds | directQueryFetchResultsReply 126982 1795162176 0 |
| | 17:17:55.837901 | mds | directQueryFetchResultsReply 126978 1795162176 0 |
| | 17:17:55.838553 | mds | directQueryFetchResultsReply 126984 1795162144 0 |
| | 17:17:55.839183 | mds | directQueryFetchResultsReply 126979 1795162144 0 |
| | 17:17:55.839855 | mds | directQueryFetchResultsReply 126980 1795162112 0 |
| | 17:17:55.862154 | accoun… | <NSXPCConnection: 0x7fa359e135b0> connection from pid 281 (com.apple.Addres) received |
| | 17:17:55.862522 | accoun… | (ACDServer.m:320) -[ACDServer listener:shouldAcceptNewConnection:] <NSXPCConnection: 0x7fa359e135b0> connection f |
| | 17:17:55.935147 | opendi… | Client: <private>, UID: 0, EUID: 0, GID: 0, EGID: 0 |
| | 17:17:55.935298 | opendi… | <private> completed, delivered 1 result |
| ○ | 17:17:55.961918 | Contac… | subsystem: com.apple.CFPasteboard, category: general, enable_level: 0, persist_level: 0, default_ttl: 0, info_ttl |
| ○ | 17:17:55.961942 | Contac… | subsystem: com.apple.CFPasteboard, category: entry, enable_level: 0, persist_level: 0, default_ttl: 0, info_ttl: |

/System/Library/CoreServices/Finder.app/Contents/MacOS/Finder (/System/Library/Frameworks/CoreServices.framework/Versions/A/Frameworks/SharedFileLis

Subsystem: com.apple.sharedfilelist   Category: default   Hide
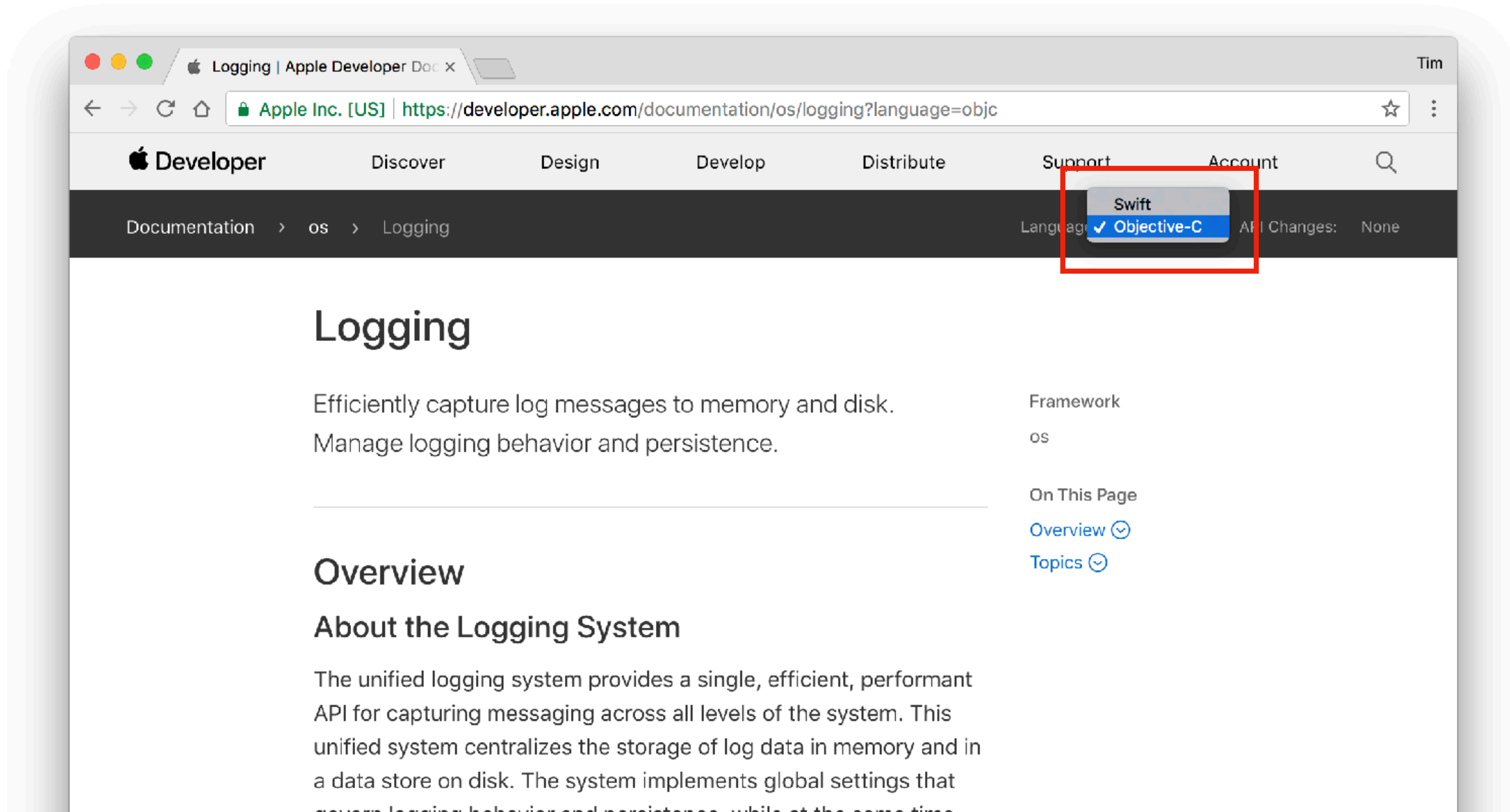
Activity ID: 0   Thread ID: 0x1cb3   PID: 264

applying: <private>

# Metadata naming in Console.app, `log`

| Console.app | 'log' command |
|---|---|
| Message | --predicate 'eventMessage contains "fail"' |
| Process (both path and name) | --predicate 'processImagePath == "/usr/sbin/cfprefsd"' |
| Library (both path and name) | --predicate 'senderImagePath CONTAINS[cd] "cloud"' |
| Type (log level) | --predicate 'messageType == info' |
| Subsystem | --predicate 'subsystem == "com.apple.securityd"' |
| Category | --predicate 'category == "User Defaults Daemon"' |
| PID | --process |

# `log` and predicates

- Quoting really matters for --predicate option!

  - 'eventMessage contains "fail"'

  - 'messageType == info', 'eventType == logEvent'

- Operator capitalization doesn't matter:

  - 'processImagePath CONTAINS[cd] "cfprefs"'

- See Apple's Predicate Programming Guide (or Munki documentation..)

  - https://developer.apple.com/documentation/foundation/nspredicate

  - https://github.com/munki/munki/wiki/Conditional-Items

# Apple Developer Docs

# `log config`

```
→ sudo log config
System mode = INFO STREAM_LIVE


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


→ sudo log config
System mode = INFO STREAM_LIVE PRIVATE_DATA


→ sudo log config --reset


→ sudo log config
System mode = INFO
```

# `log config`

```
→ sudo log config --status --subsystem com.apple.notes
Mode for 'com.apple.notes'  DEBUG PERSIST_DEBUG

→ /usr/libexec/PlistBuddy -c 'Print' \
  /System/Library/Preferences/Logging/Subsystems/com.apple.notes.plist
Dict {
    DEFAULT-OPTIONS = Dict {
        Default-Privacy-Setting = Public
        Enable-Oversize-Messages = true
        Level = Dict {
            Persist = Debug
            Enable = Debug
        }
        TTL = Dict {
            Error = 30
        }
    }
}
```

# `log stats` (new in High Sierra)

**stats**          Shows a breakdown of the events contained within a log datastore or archive. The following options can be supplied to all modes of **log stats:**

    **--archive** <u>archive</u>          Display statistics for events stored in the given archive. The archive must be a valid log archive bundle with the suffix **.logarchive.**

    **--sort** <u>events</u> | <u>bytes</u>          Sort tabulated data output by number of events, or number of bytes.

    **--count** <u>count</u> | <u>all</u>          Limit tabulated data to the given number of lines, or **all** displays all entries in tables.

    **--style** <u>human</u> | <u>json</u>          Control the format style of the requested output mode.

In addition, one of the following output modes can be supplied:

    **--overview**          Displays statistics for the entire archive.

    **--per-book**          Displays statistics per log book, the subsections of a log archive.

    **--per-file**          Displays statistics per file in the archive.

    **--sender** <u>sender</u>          Displays statistics for a given sender image name.

    **--process** <u>process</u>          Displays statistics for a given originating process.

    **--predicate** <u>predicate</u>          Displays statistics for all events matching the given predicate.

# `log stats` (new in High Sierra)

```
→ log stats --predicate 'subsystem == "com.apple.notes"'
== predicate ===============================================================
size:              1,847 bytes (uncompressed)
start:             Sat Sep  9 16:14:05 2017
end:               Sat Sep  9 16:14:08 2017

events:            [          total          log        trace      signpost ]
                   [             26           26            0             0 ]

activity:          [         create transition       action ]
                   [              0            0            0 ]

log messages:      [        default         info        debug        error         fault ]
                   [              0            0           26            0             0 ]

processes:
          [        events (%total),  decomp. bytes (%total),                             image UUID, image ]
          [             20 ( 76.9%),          1,567 ( 84.8%), 65768508-7764-396D-9DC6-C3393641B613, com.apple.Notes.SpotlightIndexEx
          [              6 ( 23.1%),            280 ( 15.2%), A77F5314-1B8B-35B5-8376-62677A2DAC6F, com.apple.Notes.datastore ]

senders:
          [        events (%total),  decomp. bytes (%total),                             image UUID, image ]
          [             17 ( 65.4%),          1,519 ( 82.2%), D2373F71-3179-3516-9234-DCA97ABD4FD7, NotesShared ]
          [              6 ( 23.1%),            280 ( 15.2%), A77F5314-1B8B-35B5-8376-62677A2DAC6F, com.apple.Notes.datastore ]
          [              2 (  7.7%),             32 (  1.7%), 65768508-7764-396D-9DC6-C3393641B613, com.apple.Notes.SpotlightIndexEx
          [              1 (  3.8%),             16 (  0.9%), 4FB06CCB-58C3-3860-BC6C-455E0B36E1FD, Notes ]

categories:
          [        events (%total),  decomp. bytes (%total), category ]
          [             15 ( 57.7%),          1,251 ( 67.7%), Indexer ]
          [              8 ( 30.8%),            572 ( 31.0%),  ]
```
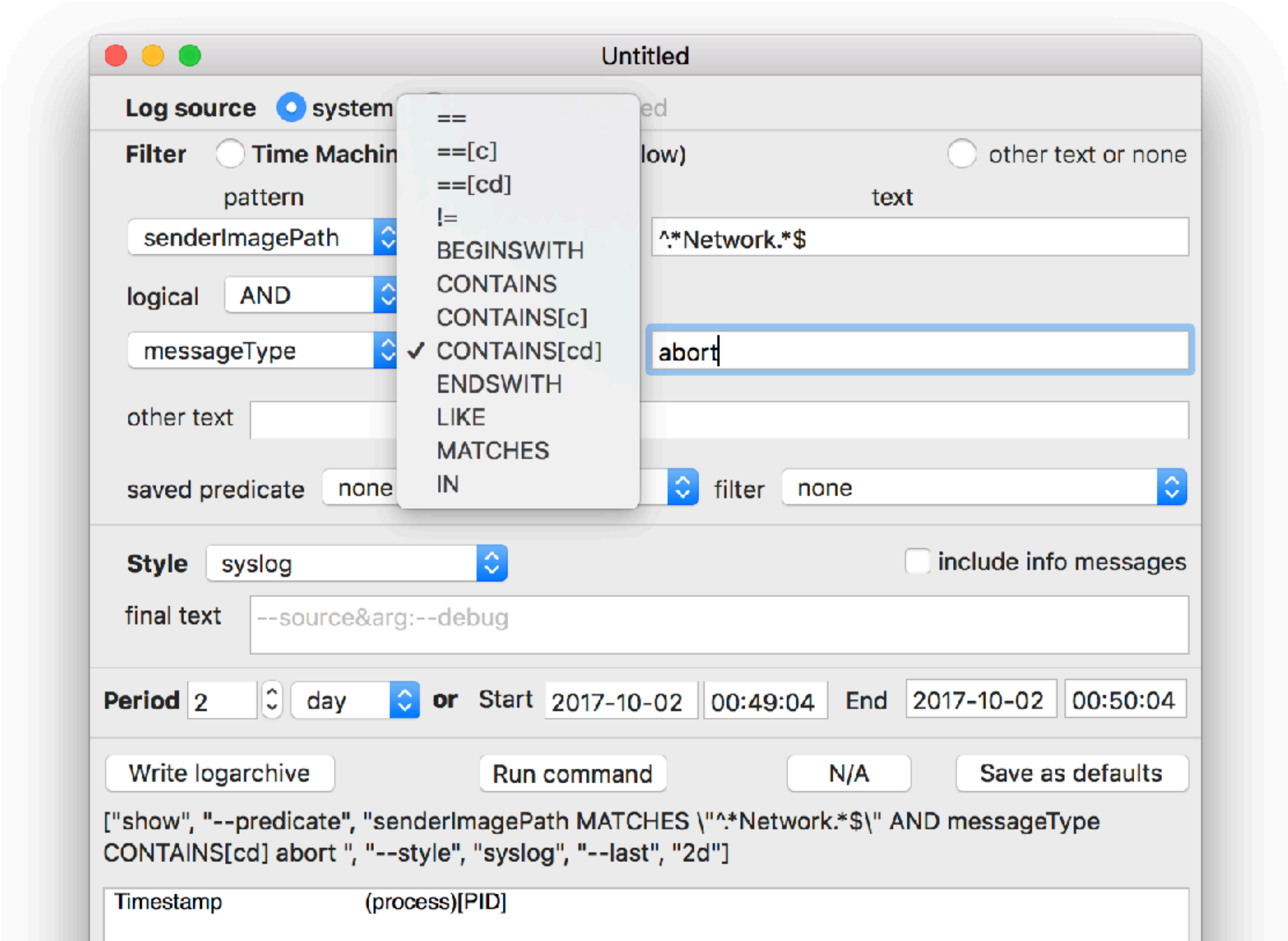
# eclecticlight.co/category/macs (Howard Oakley)

## Consolation

# Other uncertainties

# "Offline" logs?

**show**          Shows contents of the system log datastore, archive <mark>or a specific tracev3 file</mark>.  If a file or archive is not specified, the system datastore will be shown.  If it is from a future system version that log cannot understand, it exists with EX_DATAERR (65) and an error message.  The output contains only default level messages unless --info and/or --debug are specified.

```
→  ~ find /var/db/diagnostics -name '*.tracev3' | wc -l
143
```

# eclecticlight.co/category/macs (Howard Oakley)

## MakeLogarchive
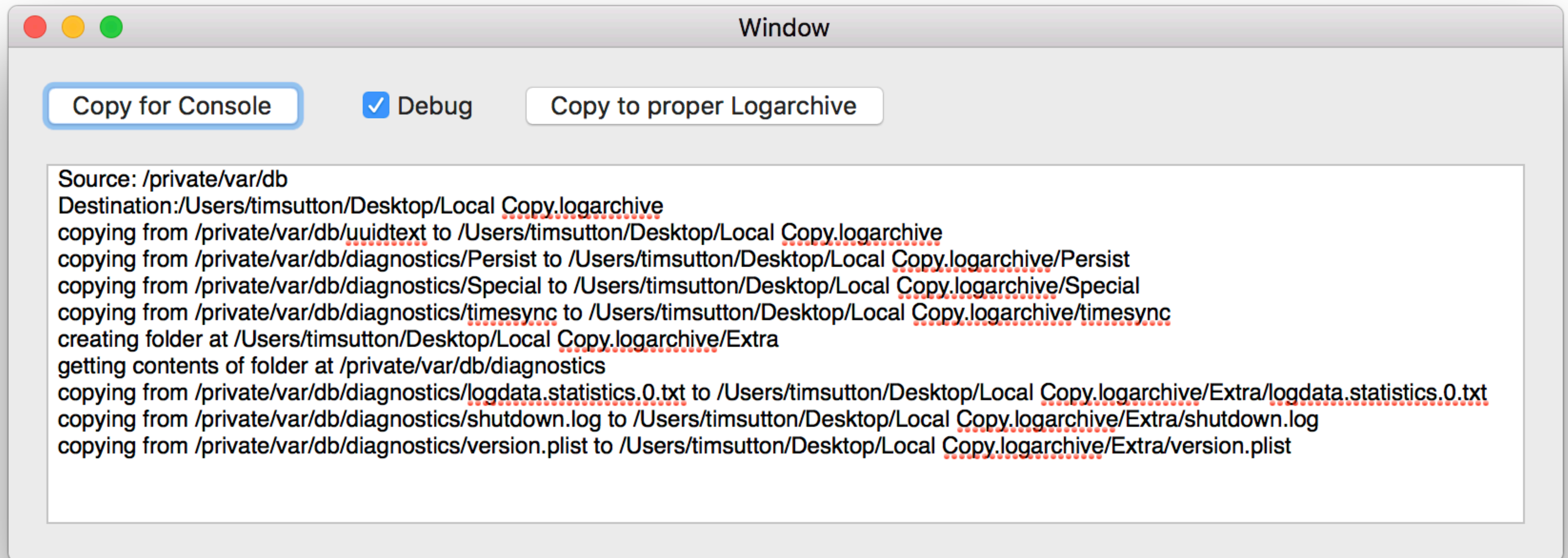
# No public API for reading logs

(ConsoleKit and LoggingSupport private frameworks)

Name (Install Name)
▼ /Applications/Utilities/Console.app/Contents/MacOS/Console
  ▼ /System/Library/PrivateFrameworks/ConsoleKit.framework/Versions/A/ConsoleKit
    ▶ /System/Library/Frameworks/QuartzCore.framework/Versions/A/QuartzCore
    ▼ /System/Library/PrivateFrameworks/LoggingSupport.framework/Versions/A/LoggingSupport

Name (Install Name)
▼ /usr/bin/log
  ▶ /System/Library/PrivateFrameworks/MobileKeyBag.framework/Versions/A/MobileKeyBag
  ▼ /System/Library/PrivateFrameworks/LoggingSupport.framework/Versions/A/LoggingSupport

# Updates for apps to use 10.12 SDK

# /var/log, /Library/Logs, etc.

syslog

# Thank you!

macops.ca/logging