OS X LOGS

DO WE STILL HAVE TO CARE

WHOAMI

Nic Scott

Senior Apple Admin - Kenyon College

bash, python, ruby, automation, forensics

breakfast sandwiches, walking slightly faster than the average person, sarcasm

Slack: @nic.scott

Github: https://github.com/nlscott

Email: scottnl@kenyon.edu

Blog: https://redlinetech.wordpress.com

WHERE WE ARE GOING

- Do We Care?
- How I Ended Up In The Logs
- Some Basics
- Machine Logs
- Centralized Logs
- Now What?
- Resources

DO WE HAVE TO CARE?

NO

- Maybe it’s not required?
- Maybe you resolve problems before you need to check the logs?
- Maybe the solution is always a "reload"

YES

- It is required? (Health Care, Finance, Government)
- Maybe you provide support for a product or service
- Maybe you build something
- Maybe you have to generate reports
- You’re just someone that enjoys lines of monotonous gibberish

LOGS ARE IMPORTANT

- They provide admins a detailed way to troubleshoot issues
- They can help build reports
- They provide the foundation of auditing
- Logs are a narrative, they help tell a story

HOW I ENDED UP IN THE LOGS: I'VE GOT PROBLEMS

- Machines taking 3 - 4 minutes to log in
- Some Students with login issues (denying logins, taking to long, etc)
- Print jobs getting stuck in the local queue, not reaching the print server
- MDM profiles not updating on machines
- Munki/Puppet errors
- Who upgraded a machine to El Capitan

LETS TALK ABOUT LOGS

LOG

an official record of events during the voyage of a ship or aircraft. "a ship's log”

APPLE SYSTEM LOGS & SYSLOG

APPLE SYSTEM LOGS (ASL)

- Apple System Log is a daemon that manages and stores log information
- The Daemon is executed at boot: /System/Library/LaunchDaemon/com.apple.syslogd.plist
- ASL logs are stored in /var/log/asl, also outputs to /var/log/system.log
- ‘aslmanager’ is the tool that manages and rotates logs generated by ASL
- ASL logs are binary, must view with syslog or console

GENERAL SYSTEM LOGS

- System logs are stored in /var/log
- General location for applications, processes to write log files
- There may be multiple files of the same type of log, ending with .gz. These are the compressed logs that have been rotated out

SYSLOG -- APPLE SYSTEM LOG UTILITY

syslog is a command-line utility for a variety of tasks relating to the Apple System Log (ASL). It provides mechanisms for sending and viewing log messages, copying log messages to ASL format data store files, and for controlling the flow of log messages from client processes.

SYSLOG -- APPLE SYSTEM LOG UTILITY

- used to view logs
- converts binary logs into plain text

#to see last 5 lines of system log
$ syslog -w 5

Apr 23 11:12:39 Fahrenheit sandboxd[134] ([34935]) <Notice>: com.apple.Addres(34935) deny network-outbound /private/var/run/mDNSResponder

Apr 23 11:12:43 Fahrenheit com.apple.xpc.launchd[1] (com.apple.quicklook[34936]) <Warning>: Endpoint has been activated through legacy launch(3) APIs. Please switch to XPC or bootstrap_check_in(): com.apple.quicklook

Apr 23 11:12:45 Fahrenheit WindowServer[269] <Error>: _CGXRemoveWindowFromWindowMovementGroup: window 0x834 is not attached to window 0x879

--- last message repeated 1 time ---

Apr 23 11:12:46 Fahrenheit login[34938] <Notice>: USER_PROCESS: 34938 ttys000

SYSLOG -- APPLE SYSTEM LOG UTILITY

#to read a specific file
sudo /usr/bin/syslog -f /private/var/log/asl/2015.11.20.G80.asl

#to see all sudo usage
sudo /usr/bin/syslog -k Sender sudo

#to see all critical messages
sudo /usr/bin/syslog -k Level Nle 2

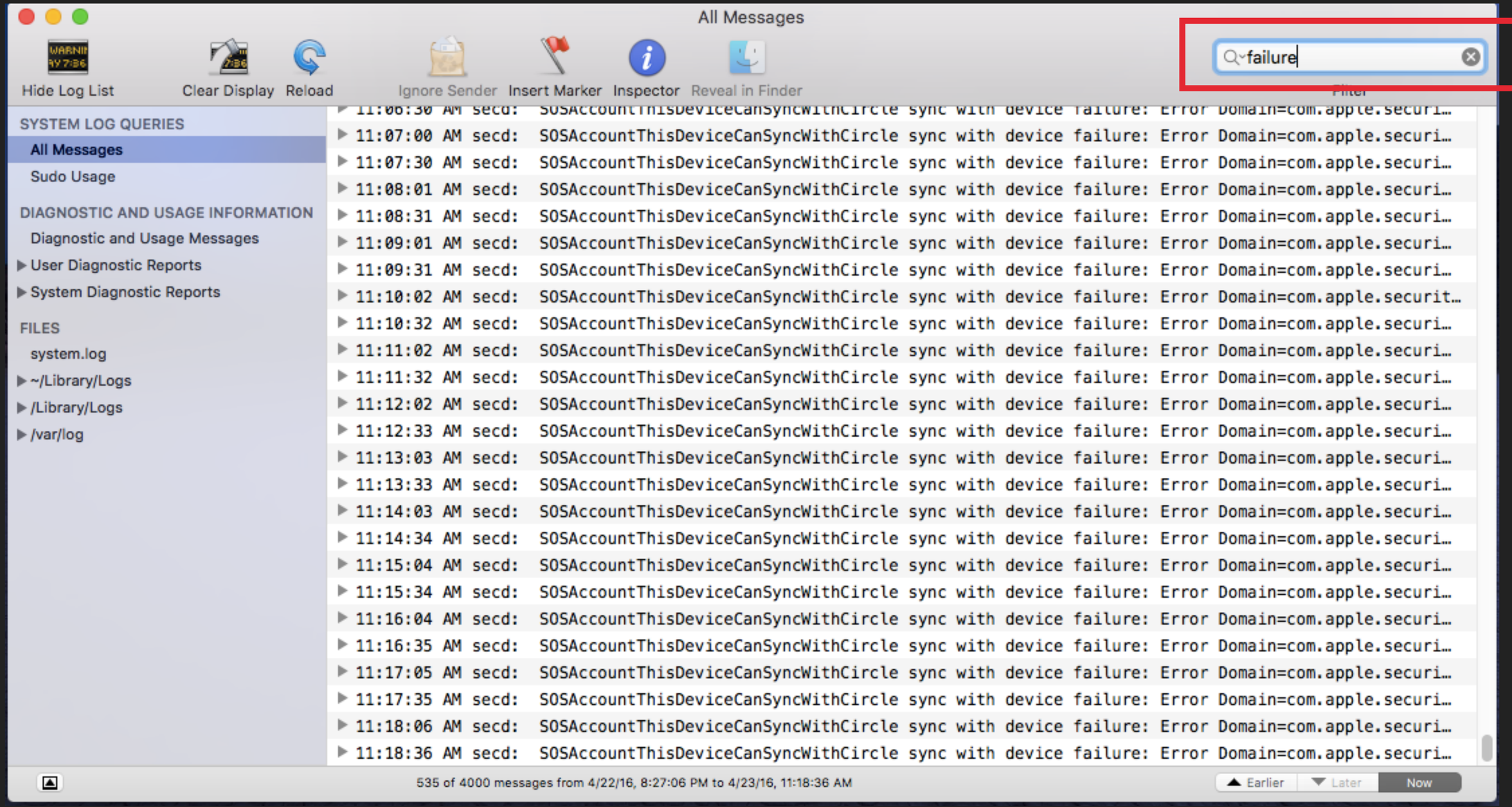
SEVERITY LOGGING LEVEL

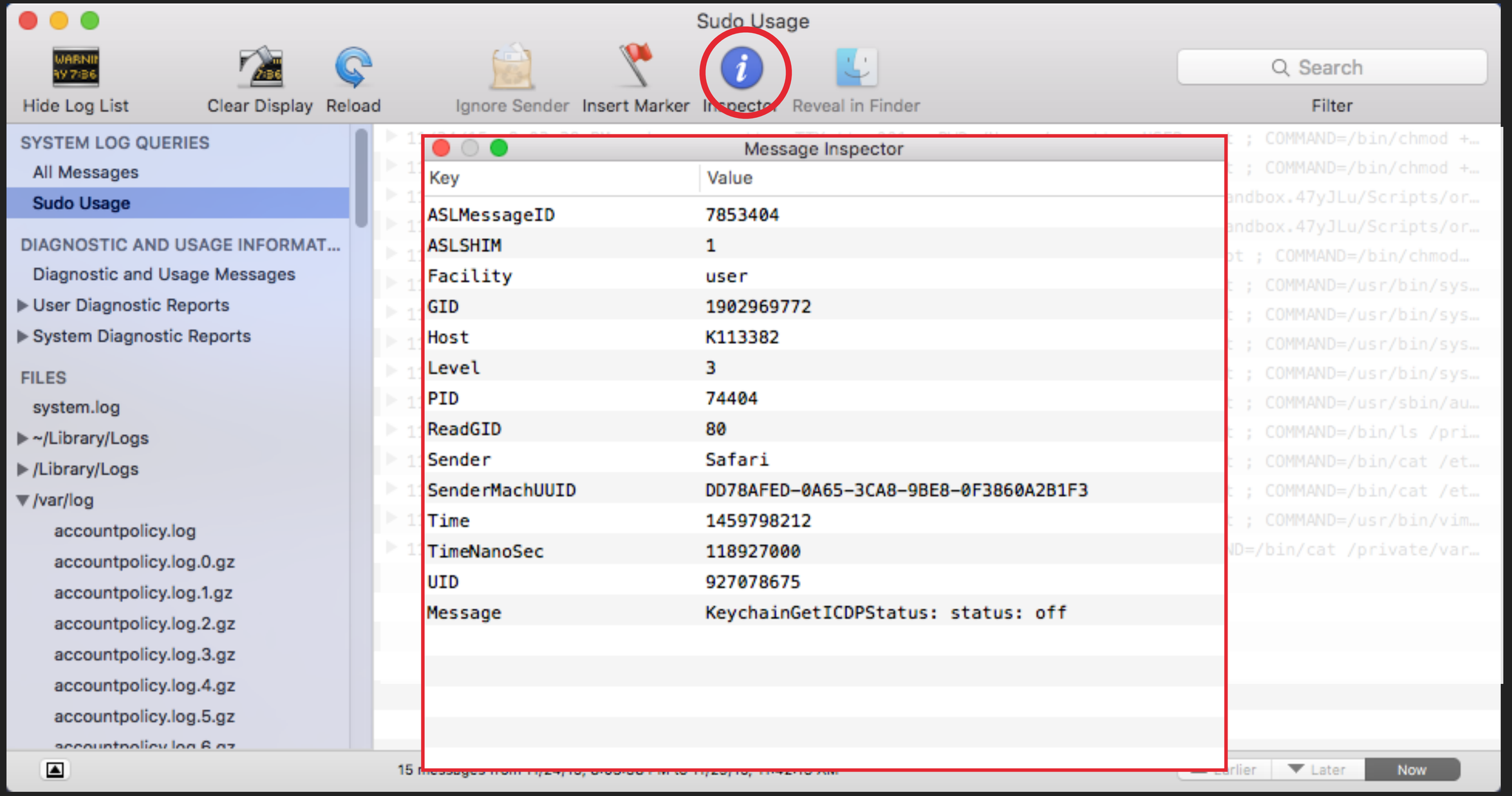
0	Emergency	system is unusable
1	Alert	action must be taken immediately
2	Critical	critical conditions
3	Error	error conditions
4	Warning	warning conditions
5	Notice	normal but significant condition
6	Informational	informational messages
7	Debug	debug-level messages

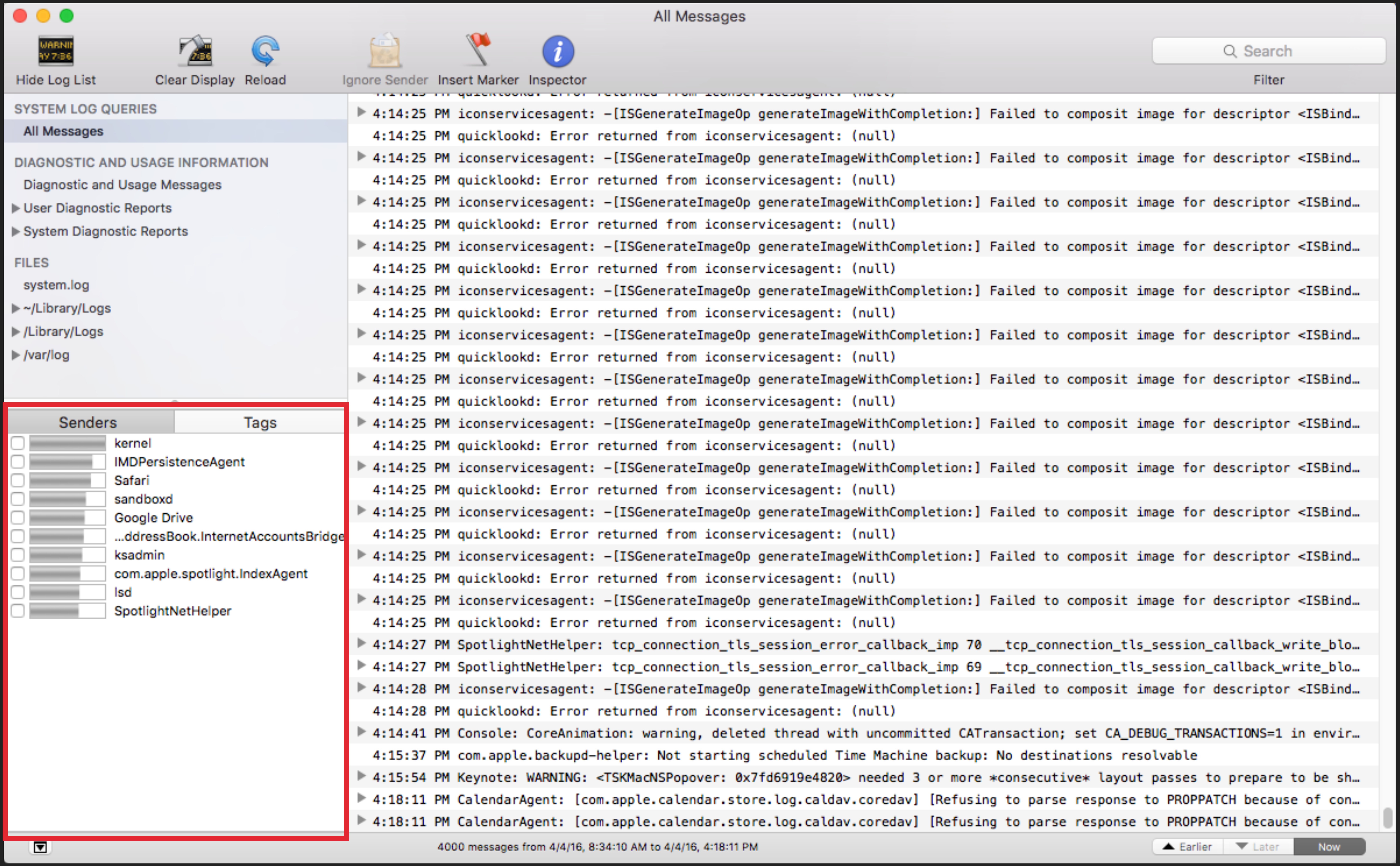
CONSOLE.APP

CONSOLE.APP

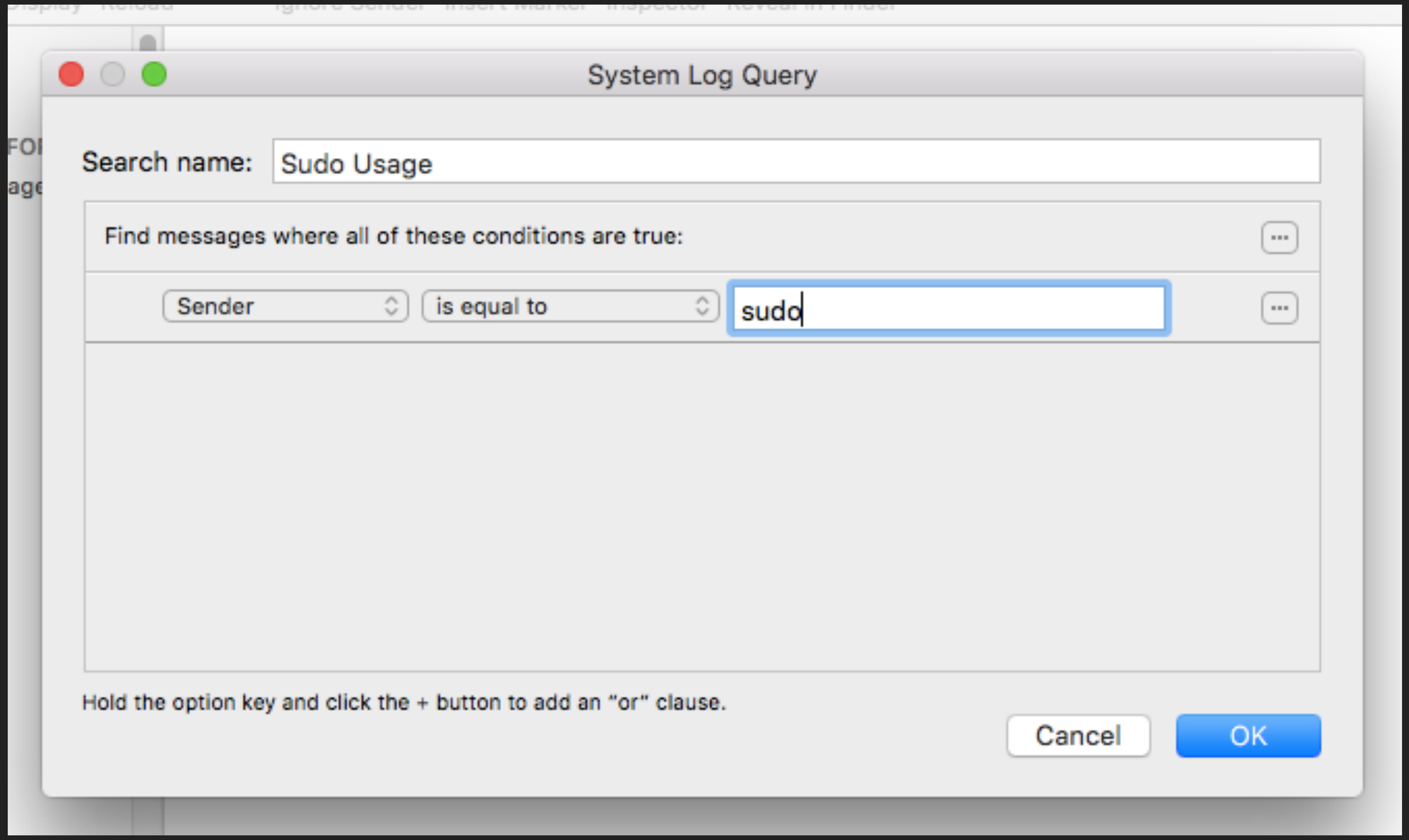
- Use Console to view logs: /Applications/Utilities/Console.app
- search/filter logs
- view info with the “Inspector” or “command + i”
- reveal logs in finder
- save logs to file
- Create custom query

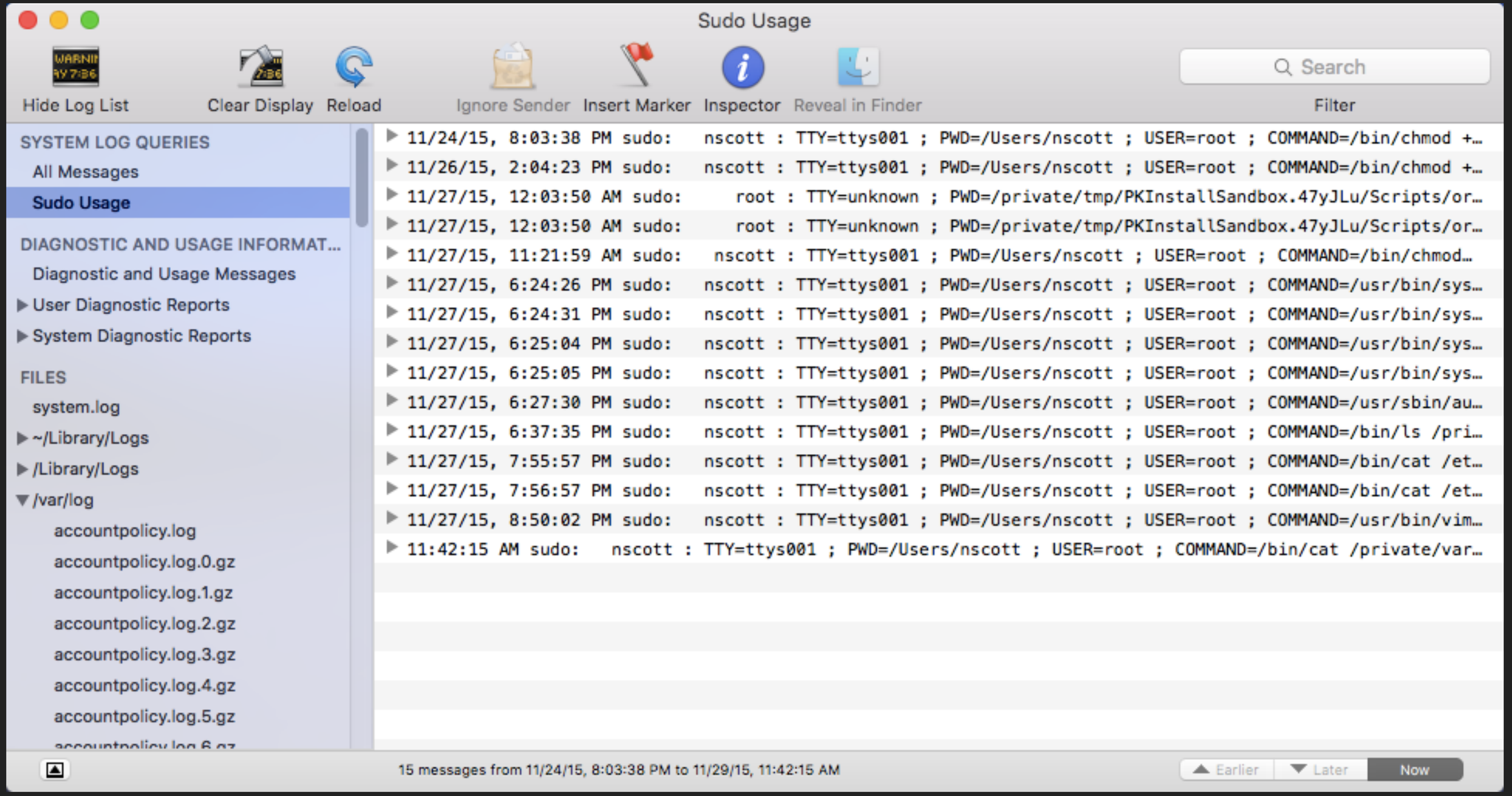

All Messages
Hide Log List
Clear Display
Reload
Ignore Sender
Insert Marker
Inspector
Reveal in Finder
failure
Filter
SYSTEM LOG QUERIES
All Messages
Sudo Usage
DIAGNOSTIC AND USAGE INFORMATION
Diagnostic and Usage Messages
User Diagnostic Reports
System Diagnostic Reports
FILES
system.log
~/Library/Logs
/Library/Logs
/var/log
11:07:00 AM secd: SOSAccountThisDeviceCanSyncWithCircle sync with device failure: Error Domain=com.apple.securi…
11:07:30 AM secd: SOSAccountThisDeviceCanSyncWithCircle sync with device failure: Error Domain=com.apple.securi…
11:08:01 AM secd: SOSAccountThisDeviceCanSyncWithCircle sync with device failure: Error Domain=com.apple.securi…
11:08:31 AM secd: SOSAccountThisDeviceCanSyncWithCircle sync with device failure: Error Domain=com.apple.securi…
11:09:01 AM secd: SOSAccountThisDeviceCanSyncWithCircle sync with device failure: Error Domain=com.apple.securi…
11:09:31 AM secd: SOSAccountThisDeviceCanSyncWithCircle sync with device failure: Error Domain=com.apple.securi…
11:10:02 AM secd: SOSAccountThisDeviceCanSyncWithCircle sync with device failure: Error Domain=com.apple.securit…
11:10:32 AM secd: SOSAccountThisDeviceCanSyncWithCircle sync with device failure: Error Domain=com.apple.securi…
11:11:02 AM secd: SOSAccountThisDeviceCanSyncWithCircle sync with device failure: Error Domain=com.apple.securi…
11:11:32 AM secd: SOSAccountThisDeviceCanSyncWithCircle sync with device failure: Error Domain=com.apple.securi…
11:12:02 AM secd: SOSAccountThisDeviceCanSyncWithCircle sync with device failure: Error Domain=com.apple.securi…
11:12:33 AM secd: SOSAccountThisDeviceCanSyncWithCircle sync with device failure: Error Domain=com.apple.securi…
11:13:03 AM secd: SOSAccountThisDeviceCanSyncWithCircle sync with device failure: Error Domain=com.apple.securi…
11:13:33 AM secd: SOSAccountThisDeviceCanSyncWithCircle sync with device failure: Error Domain=com.apple.securi…
11:14:03 AM secd: SOSAccountThisDeviceCanSyncWithCircle sync with device failure: Error Domain=com.apple.securi…
11:14:34 AM secd: SOSAccountThisDeviceCanSyncWithCircle sync with device failure: Error Domain=com.apple.securi…
11:15:04 AM secd: SOSAccountThisDeviceCanSyncWithCircle sync with device failure: Error Domain=com.apple.securi…
11:15:34 AM secd: SOSAccountThisDeviceCanSyncWithCircle sync with device failure: Error Domain=com.apple.securi…
11:16:04 AM secd: SOSAccountThisDeviceCanSyncWithCircle sync with device failure: Error Domain=com.apple.securi…
11:16:35 AM secd: SOSAccountThisDeviceCanSyncWithCircle sync with device failure: Error Domain=com.apple.securi…
11:17:05 AM secd: SOSAccountThisDeviceCanSyncWithCircle sync with device failure: Error Domain=com.apple.securi…
11:17:35 AM secd: SOSAccountThisDeviceCanSyncWithCircle sync with device failure: Error Domain=com.apple.securi…
11:18:06 AM secd: SOSAccountThisDeviceCanSyncWithCircle sync with device failure: Error Domain=com.apple.securi…
11:18:36 AM secd: SOSAccountThisDeviceCanSyncWithCircle sync with device failure: Error Domain=com.apple.securi…
535 of 4000 messages from 4/22/16, 8:27:06 PM to 4/23/16, 11:18:36 AM
Earlier
Later
Now


Sudo Usage
Hide Log List
Clear Display
Reload
Ignore Sender
Insert Marker
Inspector
Reveal in Finder
Search
Filter
SYSTEM LOG QUERIES
All Messages
Sudo Usage
DIAGNOSTIC AND USAGE INFORMAT...
Diagnostic and Usage Messages
User Diagnostic Reports
System Diagnostic Reports
FILES
system.log
~/Library/Logs
/Library/Logs
/var/log
accountpolicy.log
accountpolicy.log.0.gz
accountpolicy.log.1.gz
accountpolicy.log.2.gz
accountpolicy.log.3.gz
accountpolicy.log.4.gz
accountpolicy.log.5.gz
Message Inspector
Key
Value
ASLMessageID 7853404
ASLSHIM 1
Facility user
GID 1902969772
Host K113382
Level 3
PID 74404
ReadGID 80
Sender Safari
SenderMachUUID DD78AFED-0A65-3CA8-9BE8-0F3860A2B1F3
Time 1459798212
TimeNanoSec 118927000
UID 927078675
Message KeychainGetICDPStatus: status: off
Later
Now

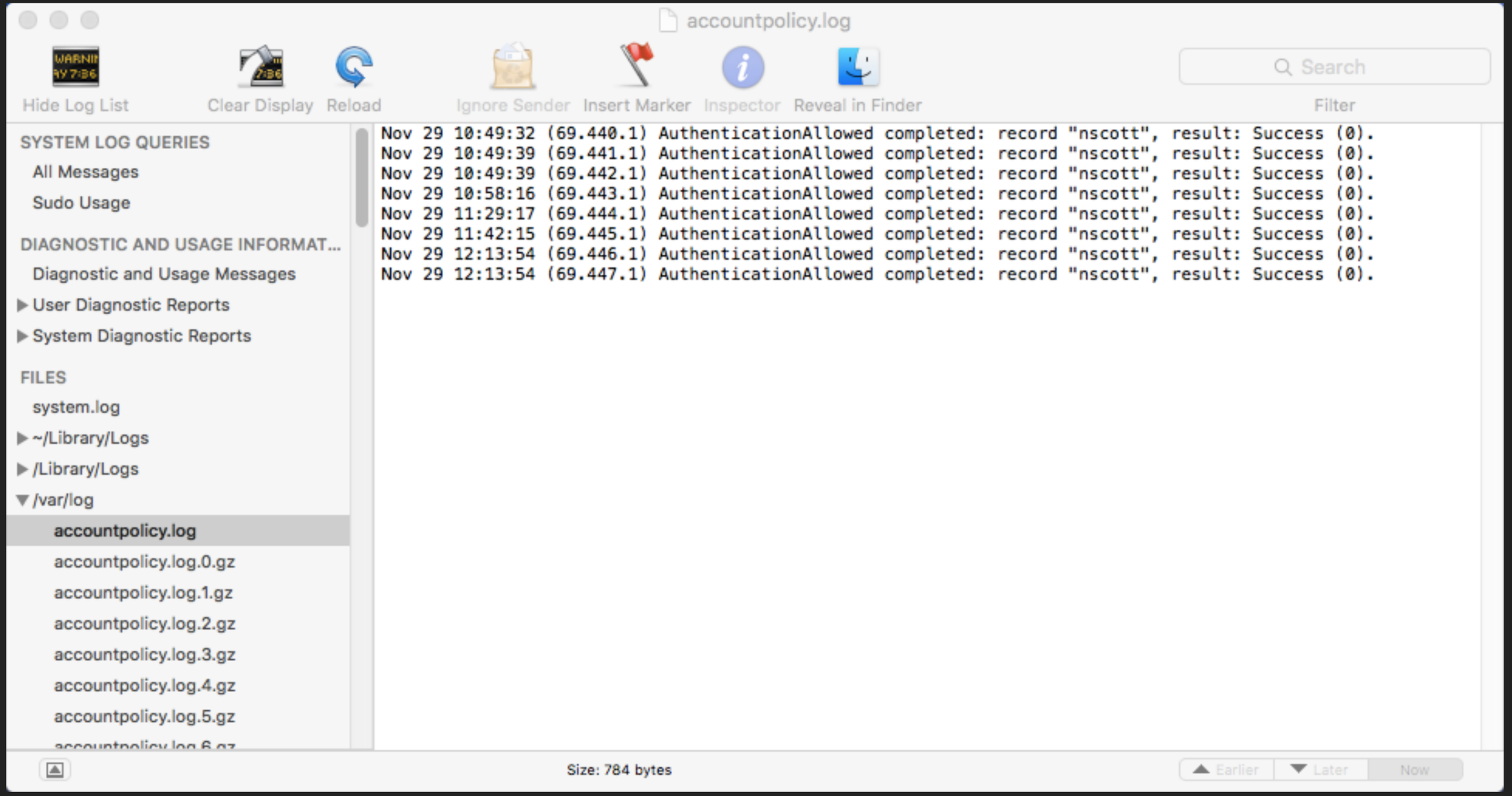

All Messages
Hide Log List
Clear Display
Reload
Ignore Sender
Insert Marker
Inspector
Search
Filter
SYSTEM LOG QUERIES
All Messages
DIAGNOSTIC AND USAGE INFORMATION
Diagnostic and Usage Messages
User Diagnostic Reports
System Diagnostic Reports
FILES
system.log
~/Library/Logs
/Library/Logs
/var/log
Senders
Tags
kernel
IMDPersistenceAgent
Safari
sandboxd
Google Drive
...ddressBook.InternetAccountsBridge
ksadmin
com.apple.spotlight.IndexAgent
lsd
SpotlightNetHelper
4:14:25 PM iconservicesagent: -[ISGenerateImageOp generateImageWithCompletion:] Failed to composit image for descriptor <ISBind...
4:14:25 PM quicklookd: Error returned from iconservicesagent: (null)
4:14:27 PM SpotlightNetHelper: tcp_connection_tls_session_error_callback_imp 70 __tcp_connection_tls_session_callback_write_blo...
4:14:27 PM SpotlightNetHelper: tcp_connection_tls_session_error_callback_imp 69 __tcp_connection_tls_session_callback_write_blo...
4:14:28 PM iconservicesagent: -[ISGenerateImageOp generateImageWithCompletion:] Failed to composit image for descriptor <ISBind...
4:14:28 PM quicklookd: Error returned from iconservicesagent: (null)
4:14:41 PM Console: CoreAnimation: warning, deleted thread with uncommitted CATransaction; set CA_DEBUG_TRANSACTIONS=1 in envir...
4:15:37 PM com.apple.backupd-helper: Not starting scheduled Time Machine backup: No destinations resolvable
4:15:54 PM Keynote: WARNING: <TSKMacNSPopover: 0x7fd6919e4820> needed 3 or more *consecutive* layout passes to prepare to be sh...
4:18:11 PM CalendarAgent: [com.apple.calendar.store.log.caldav.coredav] [Refusing to parse response to PROPPATCH because of con...
4:18:11 PM CalendarAgent: [com.apple.calendar.store.log.caldav.coredav] [Refusing to parse response to PROPPATCH because of con...
4000 messages from 4/4/16, 8:34:10 AM to 4/4/16, 4:18:11 PM
Earlier
Later
Now

- Console.app> File > New System Log Query

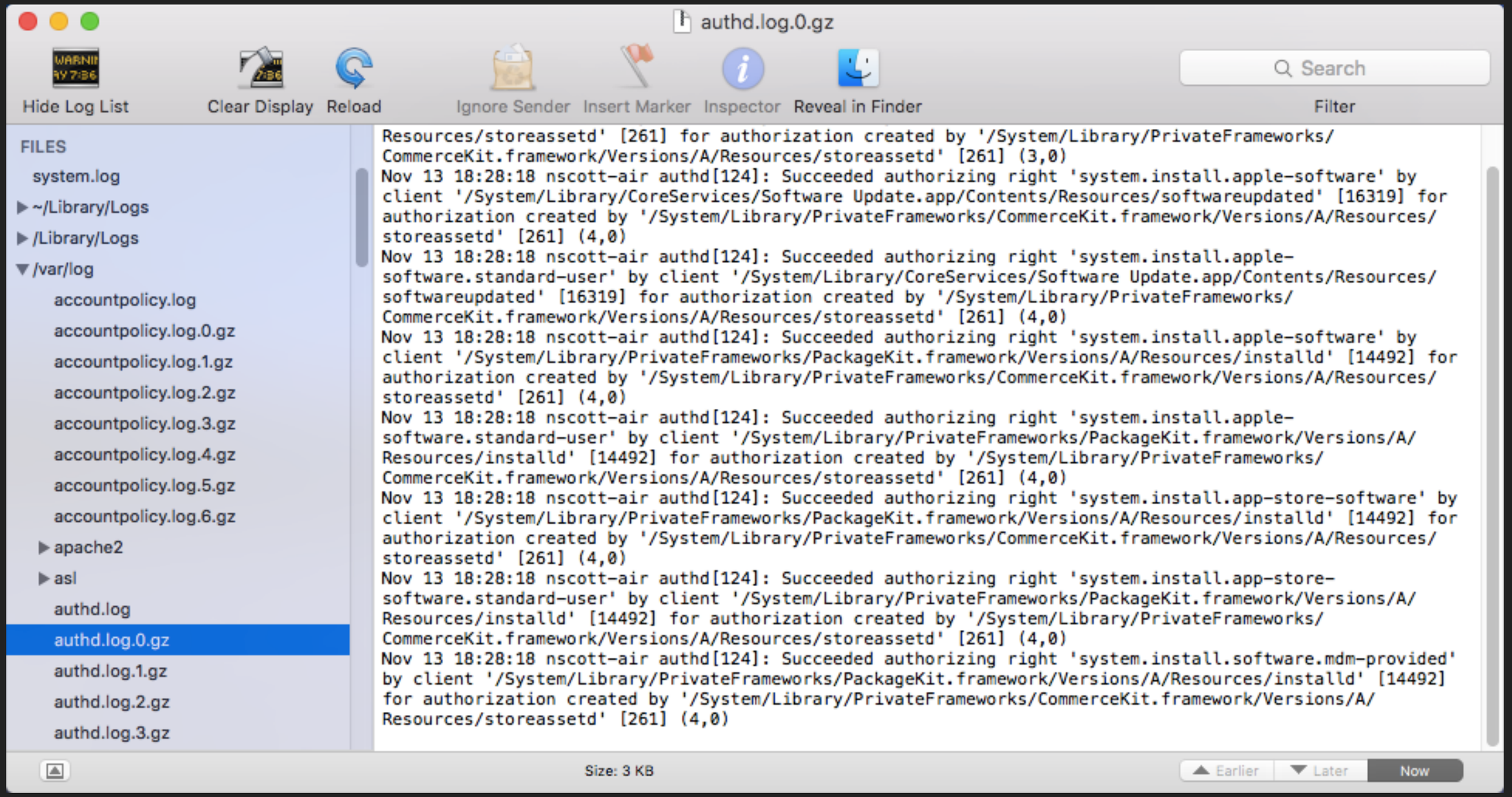



Sudo Usage
Hide Log List
Clear Display
Reload
Ignore Sender
Insert Marker
Inspector
Reveal in Finder
Search
Filter
SYSTEM LOG QUERIES
All Messages
Sudo Usage
DIAGNOSTIC AND USAGE INFORMAT…
Diagnostic and Usage Messages
User Diagnostic Reports
System Diagnostic Reports
FILES
system.log
~/Library/Logs
/Library/Logs
/var/log
accountpolicy.log
accountpolicy.log.0.gz
accountpolicy.log.1.gz
accountpolicy.log.2.gz
accountpolicy.log.3.gz
accountpolicy.log.4.gz
accountpolicy.log.5.gz
11/24/15, 8:03:38 PM sudo: nscott : TTY=ttys001 ; PWD=/Users/nscott ; USER=root ; COMMAND=/bin/chmod +…
11/26/15, 2:04:23 PM sudo: nscott : TTY=ttys001 ; PWD=/Users/nscott ; USER=root ; COMMAND=/bin/chmod +…
11/27/15, 12:03:50 AM sudo: root : TTY=unknown ; PWD=/private/tmp/PKInstallSandbox.47yJLu/Scripts/or…
11/27/15, 12:03:50 AM sudo: root : TTY=unknown ; PWD=/private/tmp/PKInstallSandbox.47yJLu/Scripts/or…
11/27/15, 11:21:59 AM sudo: nscott : TTY=ttys001 ; PWD=/Users/nscott ; USER=root ; COMMAND=/bin/chmod…
11/27/15, 6:24:26 PM sudo: nscott : TTY=ttys001 ; PWD=/Users/nscott ; USER=root ; COMMAND=/usr/bin/sys…
11/27/15, 6:24:31 PM sudo: nscott : TTY=ttys001 ; PWD=/Users/nscott ; USER=root ; COMMAND=/usr/bin/sys…
11/27/15, 6:25:04 PM sudo: nscott : TTY=ttys001 ; PWD=/Users/nscott ; USER=root ; COMMAND=/usr/bin/sys…
11/27/15, 6:25:05 PM sudo: nscott : TTY=ttys001 ; PWD=/Users/nscott ; USER=root ; COMMAND=/usr/bin/sys…
11/27/15, 6:27:30 PM sudo: nscott : TTY=ttys001 ; PWD=/Users/nscott ; USER=root ; COMMAND=/usr/sbin/au…
11/27/15, 6:37:35 PM sudo: nscott : TTY=ttys001 ; PWD=/Users/nscott ; USER=root ; COMMAND=/bin/ls /pri…
11/27/15, 7:55:57 PM sudo: nscott : TTY=ttys001 ; PWD=/Users/nscott ; USER=root ; COMMAND=/bin/cat /et…
11/27/15, 7:56:57 PM sudo: nscott : TTY=ttys001 ; PWD=/Users/nscott ; USER=root ; COMMAND=/bin/cat /et…
11/27/15, 8:50:02 PM sudo: nscott : TTY=ttys001 ; PWD=/Users/nscott ; USER=root ; COMMAND=/usr/bin/vim…
11:42:15 AM sudo: nscott : TTY=ttys001 ; PWD=/Users/nscott ; USER=root ; COMMAND=/bin/cat /private/var…
15 messages from 11/24/15, 8:03:38 PM to 11/29/15, 11:42:15 AM
Earlier
Later
Now

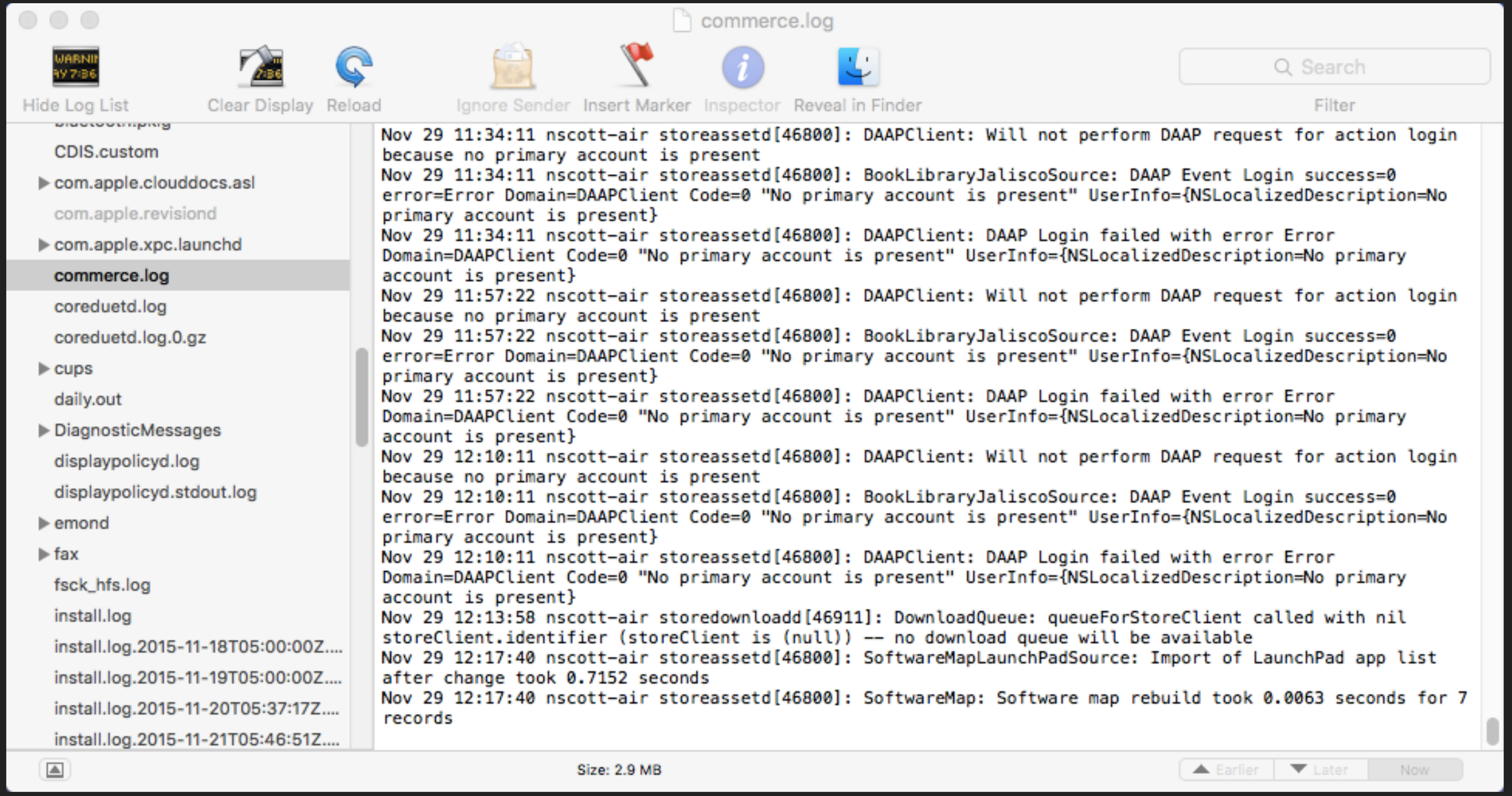
accountpolicy: contains information about authentication events



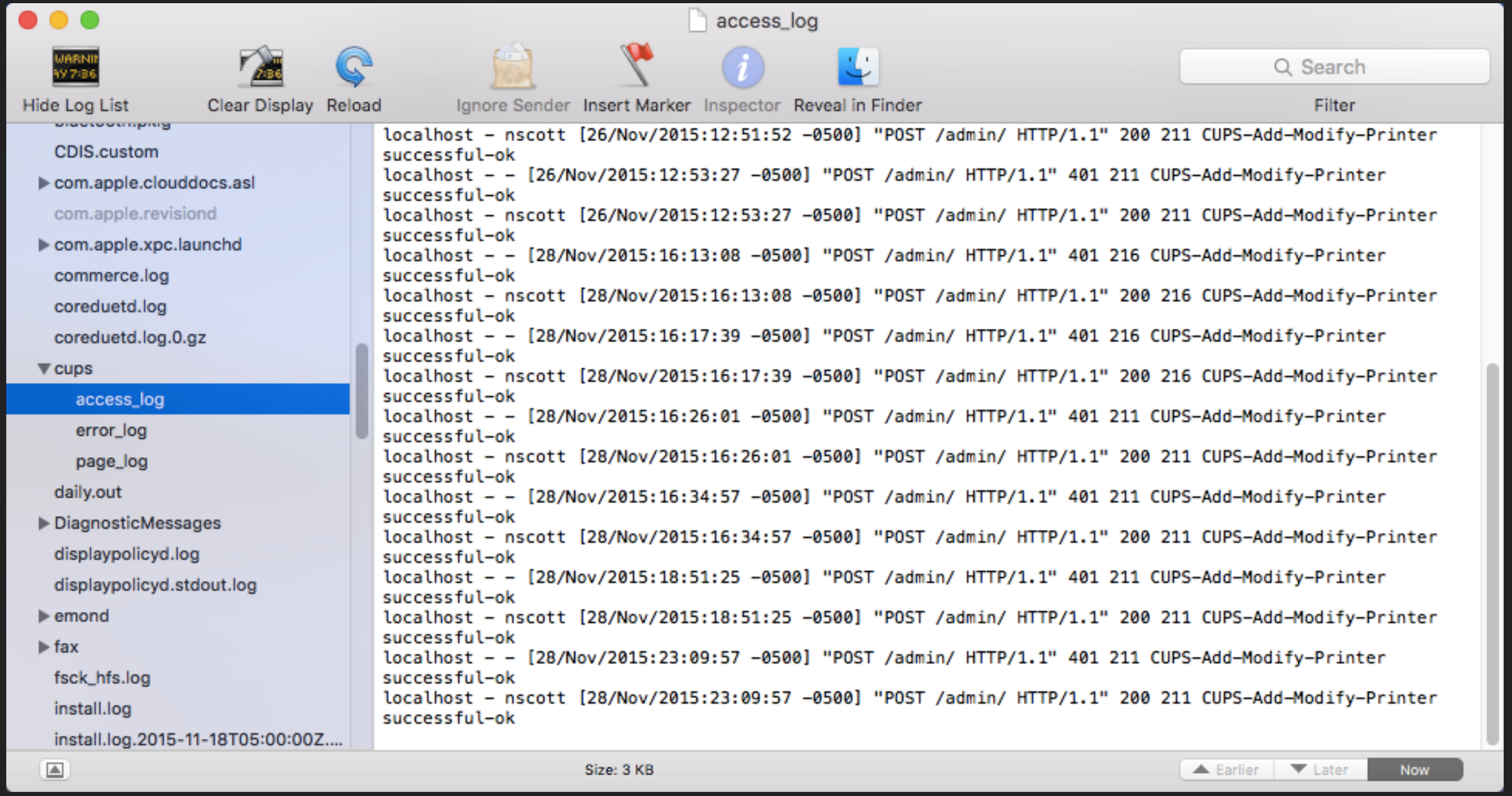
authd: contains information about authentication events



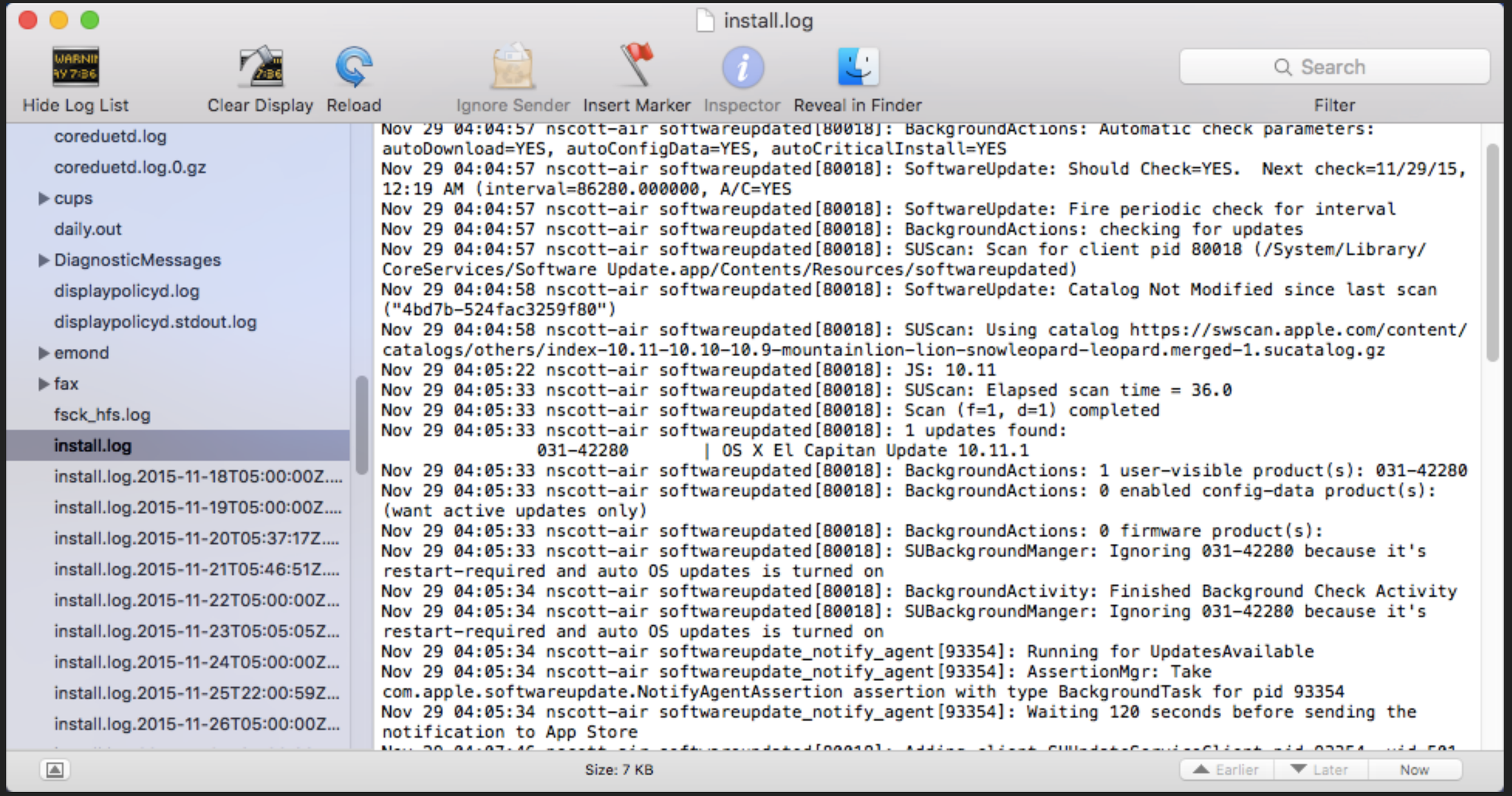
commerce: contains information about software updates and App Store activity



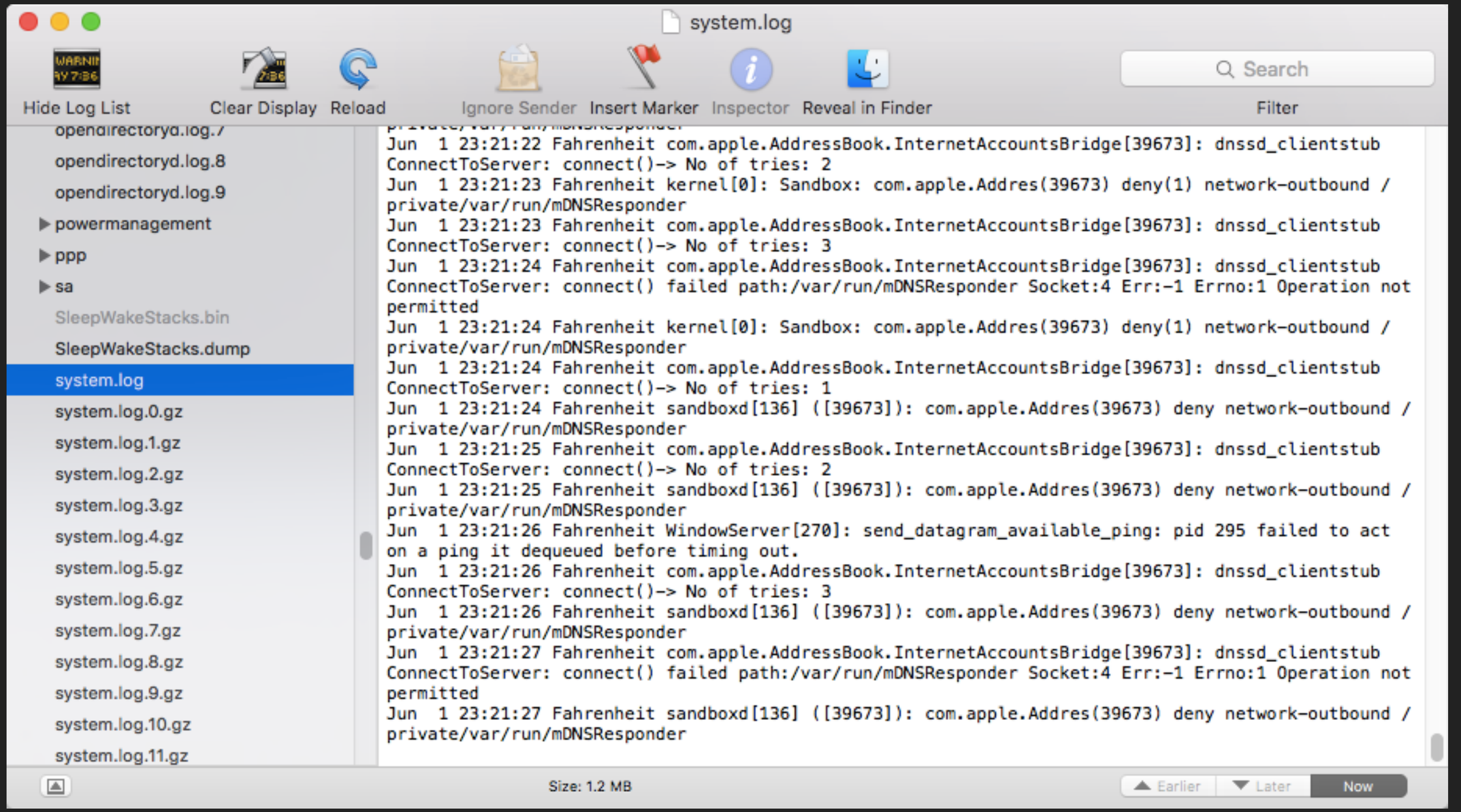
cups: contains information about printing events



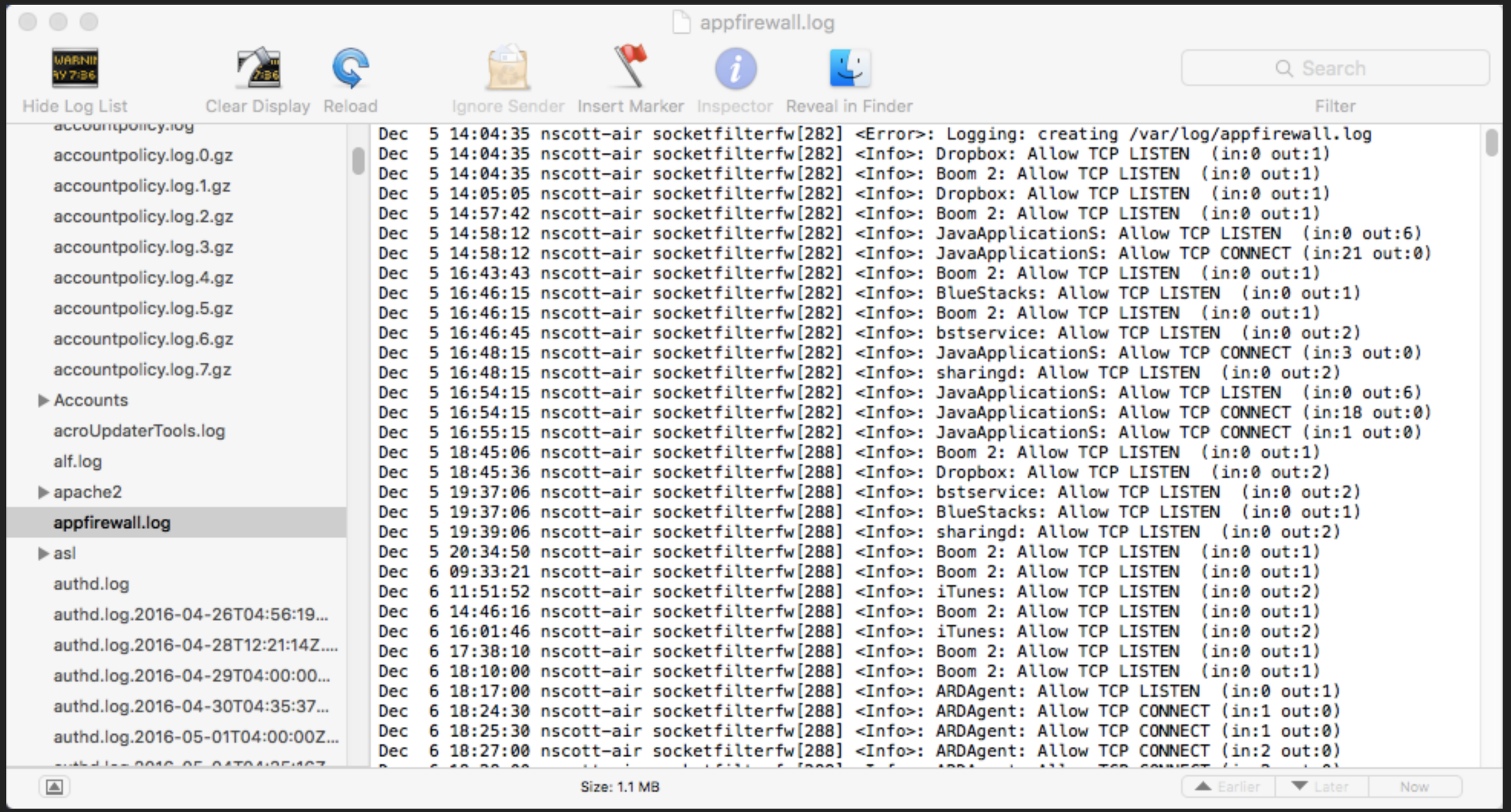
installs: contains information about software installs



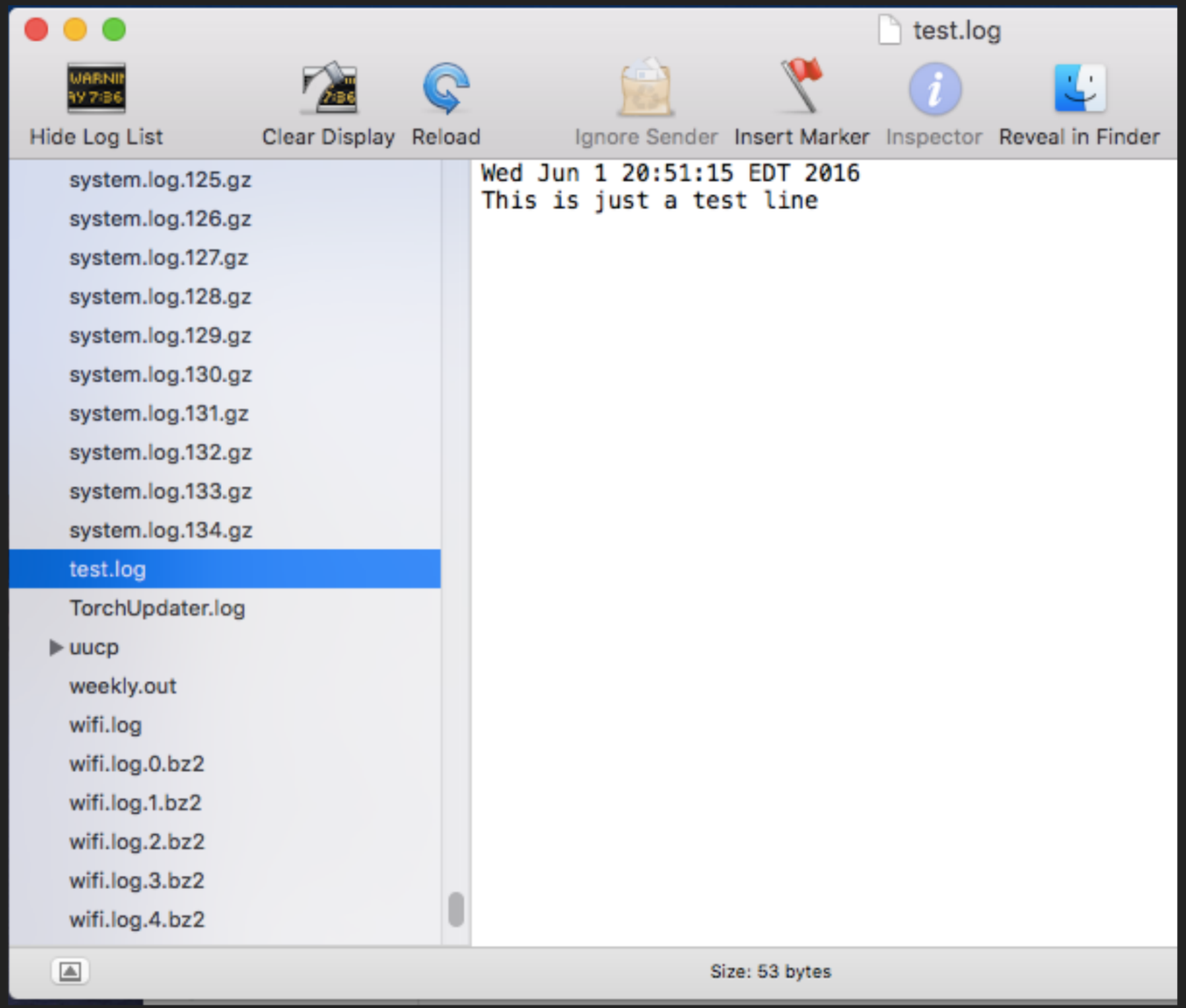
system: contains general information about the computer

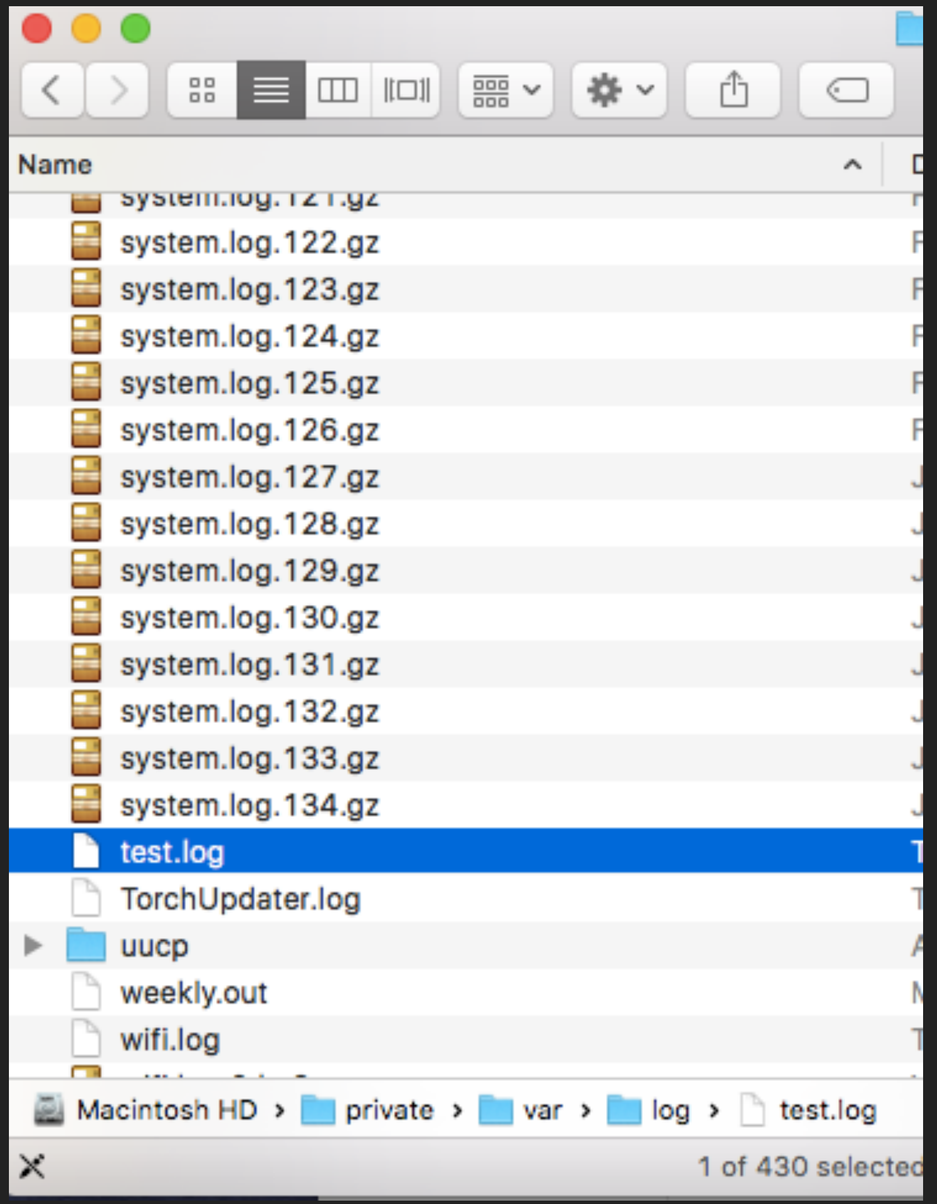


appfirewall: contains informations about application level activity



custom logs: create a text file in /var/logs and read it in console





AUDIT LOGS

AUDIT LOGS

Basic Security Module (BSM) created by SUN, Apple delegated the BSM implementation to McAfee Research, and was then released under the BSD license. The current version is maintained by the Trusted BSD Project, and is known as OpenBSM

AUDIT LOGS

- Audit logs live in /var/audit
- logs are named startime.stoptime
- current log ends with .not_terminated
- logs are saved in binary
- logs can be read with praudit
- filter logs by type with auditreduce
- audit config files in /etc/security

AUDIT - /ETC/SECURITY

audit_class: maps events to readable names

(ap:application)

audit_control: policy and retention

audit_events: maps events to readable names (AUE_auth_user:user authentication:aa)

audit_user: enable/disable auditing per user

(nscott:lo:ad, login/logout & administrative)

audit_warn: a shell script that executes on warnings

AUDIT - LOGS THINGS LIKE

- logins
- log outs
- authentications
- mounts
- reboots
- password changes
- ssh
- chmod or chown

PRAUDIT

praudit -- print the contents of audit trail files

```
#print all current activity
sudo /usr/sbin/praudit -s /var/audit/current
```

AUDIT - EXAMPLE

```
header,140,11,user authentication,0,Sat Apr 23 09:58:04 2016, + 462 msec
subject,nscott,nscott,staff,root,staff,95,100007,96,0.0.0.0
text,Verify password for record type Users 'nscott' node '/Local/Default'
return,failure: Unknown error: 255,5000
trailer,140
header,140,11,user authentication,0,Sat Apr 23 09:58:07 2016, + 892 msec
subject,nscott,nscott,staff,root,staff,95,100007,96,0.0.0.0
text,Verify password for record type Users 'nscott' node '/Local/Default'
return,success,0
trailer,140
```

AUDIT REDUCE

auditreduce -- select records from audit trail files

#show all activity from root
sudo /usr/sbin/auditreduce -e root /var/audit/current | praudit | tail

#show user authentication activity
sudo /usr/sbin/auditreduce -m AUE_auth_user, /var/audit/current | praudit

#show logins
sudo /usr/sbin/auditreduce -m AUE_lw_login, /var/audit/current | praudit

#show logouts
sudo /usr/sbin/auditreduce -m AUE_logout /var/audit/current | praudit

CONFIGURATION FILES

CONFIGURATION

Most logs have a configuration file, including retention policies

System log files:
/etc/syslog.conf

Apple System Logs:
/etc/asl.conf

Audit Logs:
/etc/security/audit_control

/ETC/SYSLOG.CONF

```
# Note that flat file logs are now configured in /etc/asl.conf

install.*                       @127.0.0.1:32376
```

/ETC/ASL.CONF

```
# configuration file for syslogd and aslmanager
##
# aslmanager logs
> /var/log/asl/Logs/aslmanager external style=lcl-b re
# authpriv messages are root/admin readable
? [= Facility authpriv] access 0 80
# remoteauth critical, alert, and emergency messages are root/admin readable
? [= Facility remoteauth] [<= Level critical] access 0 80
# broadcast emergency messages
? [= Level emergency] broadcast
# save kernel [PID 0] and launchd [PID 1] messages
? [<= PID 1] store
# ignore "internal" facility
? [= Facility internal] ignore
# save everything from emergency to notice
? [<= Level notice] store
# Rules for /var/log/system.log
> system.log mode=0640 format=bsd rotate=seq compress file_max=5M all_max=50M ttl=90
? [= Sender kernel] file system.log
? [<= Level notice] file system.log
? [= Facility auth] [<= Level info] file system.log
? [= Facility authpriv] [<= Level info] file system.log
# Facility com.apple.alf.logging gets saved in appfirewall.log
? [= Facility com.apple.alf.logging] file appfirewall.log file_max=5M all_max=50M
```

Rules for /var/log/system.log

> system.log mode=0640 format=bsd rotate=seq compress file_max=5M all_max=50M ttl=90

mode=permissions, set in octal value

format= sets the format for log files, can use xml, asl if you want binary

rotate=sets the naming scheme and compression

file_max= the size of an active log file, before it gets rotated

all_max= total size of all log files before the asl manager starts deleting the oldest

ttl=sets the number of days that rotated logs are kept

/etc/security/audit_control

```
# $P4: //depot/projects/trustedbsd/openbsm/etc/audit_control#8 $
dir:/var/audit #location of logs
flags:lo,aa,ad #aduit flags, tells system what events to record, check /etc/security/audit_class
minfree:5 #%of free space the system needs to continue logging
naflags:lo,aa #flags for events that can’t be tied to a user
policy:cnt,argv #tells audit how to act … cnt, allows the system to run even if events are not being logged.
filesz:2M # size of log files
expire-after:10M #sets when logs are removed, can be set to file size or time length
superuser-set-sflags-mask:has_authenticated,has_console_access
superuser-clear-sflags-mask:has_authenticated,has_console_access
member-set-sflags-mask:
member-clear-sflags-mask:has_authenticated
```

MACHINE LOGS

LOG LOCATIONS

System Log files main folder: /var/log/

Apple System Log: /var/log/asl/*

Audit Log: /var/audit/*

User Logs: ~/Library/Logs

Application Logs: /Library/Logs

WHAT TO LOOK FOR

- Success/successfully
- Failed/Failure
- error
- critical
- created
- deleted
- incorrect
- racoon (vpn activity)
- blued (bluetooth activity)
- enableroot/dsenableroot
- screensharingd
- launchctl
- AppleID
- "network changes"
- "mounted volumes"
- "privilege escalation"
- "account creation"

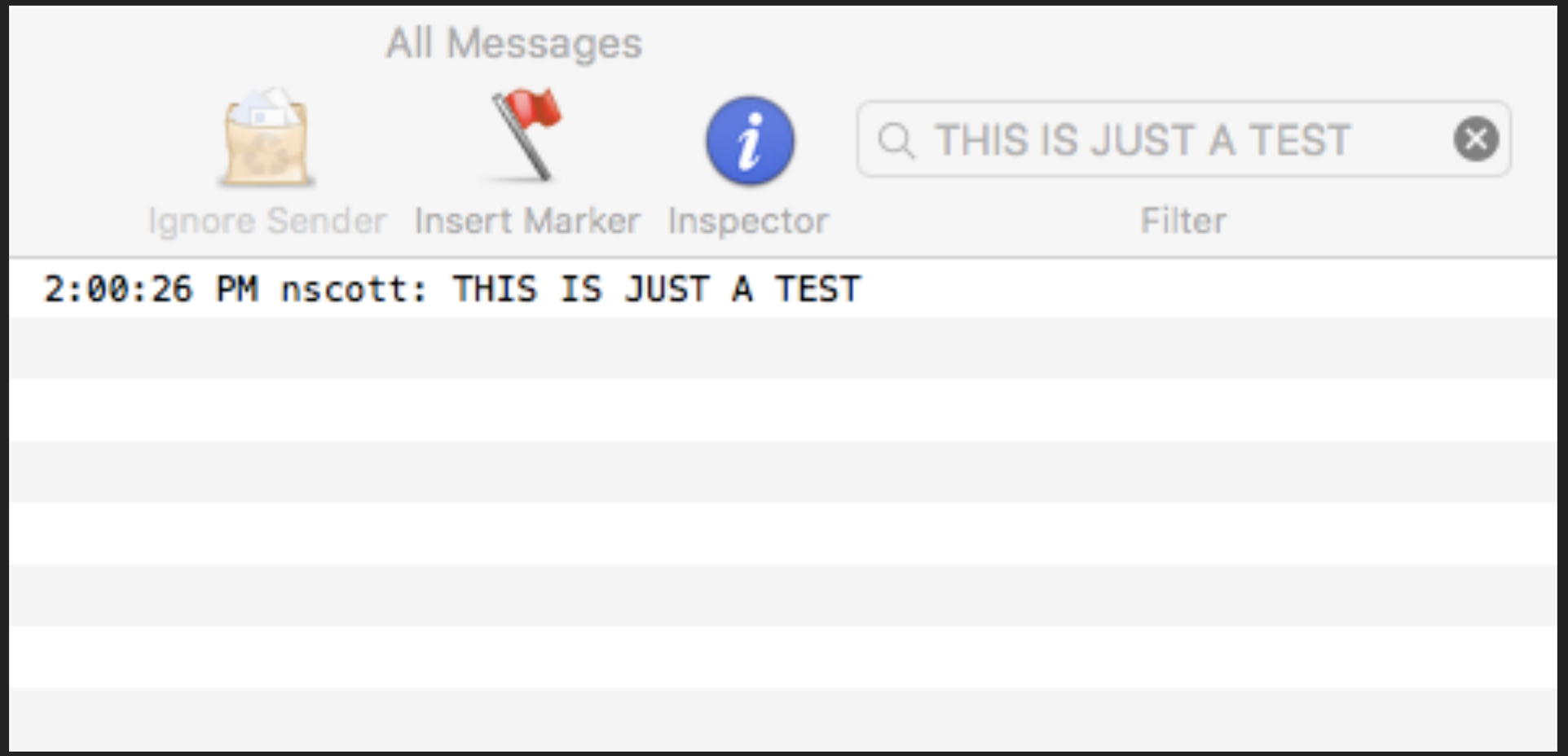
- Kerberos
- "account deletion"
- backupd
- "installed" (install.log)
- boot, reboot, shutdown*
- sudo/su
- root

*shutdown cause = 0 battery removal/powerplug, 3 = hard shutdown, 5 normal shutdown/reboot, -128 unknown, -60 unknown

LOGGER

-- make entries in the system log

```
$ logger "THIS IS JUST A TEST"
$
```



```
#Turn Firewall on

logger "Turning Firewall On"

sudo defaults write /Library/Preferences/com.apple.alf globalstate -int 1
```

LOGGING WITH REDIRECTION

-- standard input and output

Redirect Standard Output:

```
#direct output to a file, this will over write the file
ls -l > log_file.txt

#direct output to a file and append file
ls -l >> log_file.txt
```

Redirect Standard Error:

```
command 2> log_errors.txt
```

Redirect Both Output & Errors:

```
command &> log_file.txt
```

Redirect Both Output & Errors:

```
command &> /dev/null
```

CUSTOM LOGGING WITH REDIRECTION

-- standard input and output

```
#!/bin/bash

#SET UP LOGGING
#— — — — — — — — — — — — — — — — — — — — — — — — —
logpath=/Library/AdminLogs
logfile=$logpath/admin_logs.txt
mkdir $logpath
touch $logfile

#START SCRIPT
#----------------------------------
echo -e  "\nConfiguring System Preferences" >> $logfile
date >> $logfile
```

```
#FIREWALL
#----------------------------------------
echo -e "\nConfiguring Firewall" >> $logfile
date >> $logfile

#Turn Firewall on
logger "Turning Firewall On"
defaults write /Library/Preferences/com.apple.alf globalstate -int 1
```

CUSTOM LOGGING WITH EXEC

exec command: redirects all output to file for the current shell process

```
#!/bin/bash

current_user=$(whoami)
logfile="/Users/$current_user/Desktop/logfile_test.txt"

exec &> $logfile

ls -l
```

CUSTOM LOGGING WITH TEE

tee command: copies standard input to standard output, making a copy

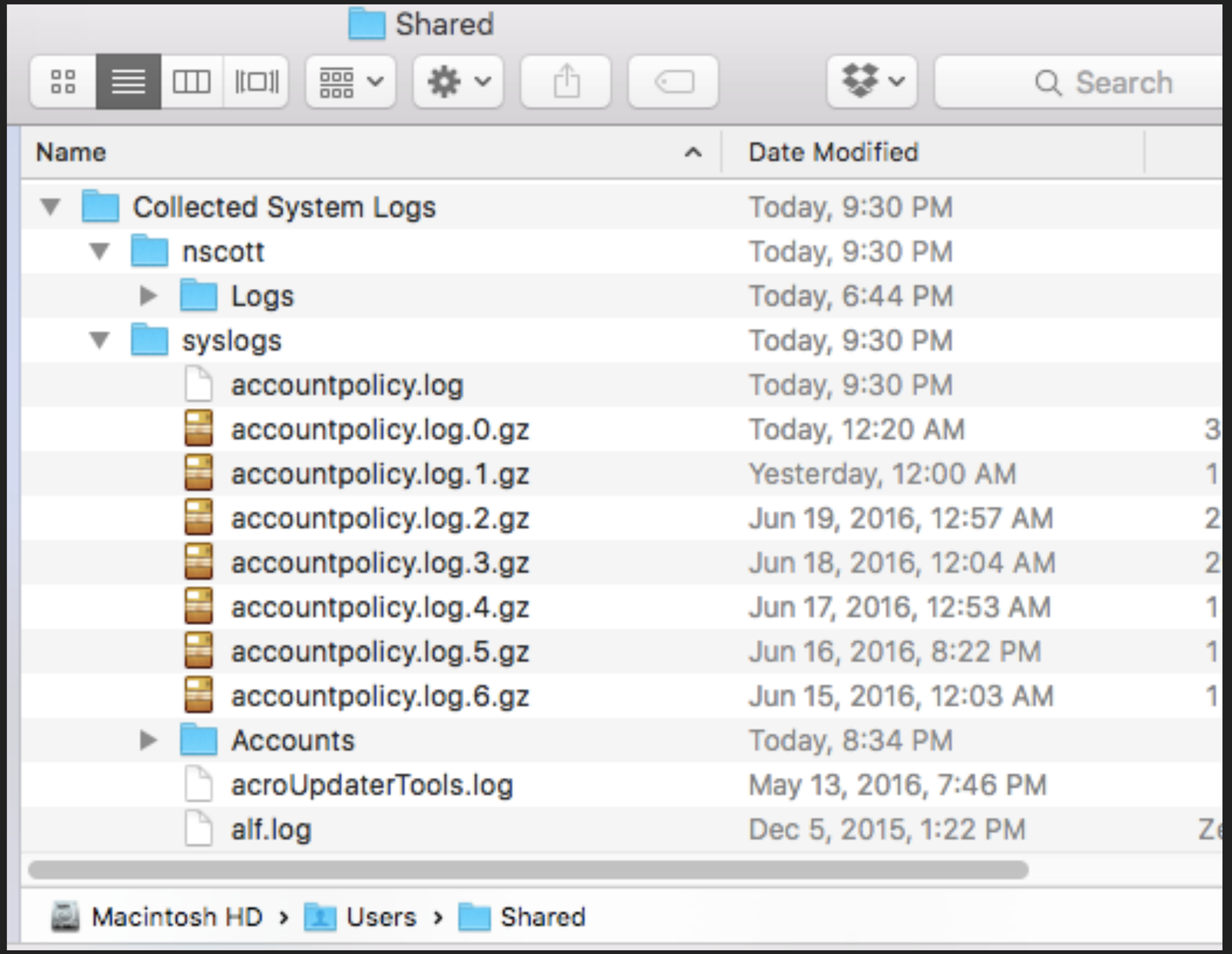
```
#!/bin/bash

current_user=$(whoami)
logfile="/Users/$current_user/Desktop/logfile_test.txt"

ls -l | tee $logfile
```

COLLECTING LOGS

SYSTEM & USER LOGS

collect_syslogs&users.sh

```
#!/bin/bash
#tested on 10.11

#   this script colelcts sytem logs to "/Users/Shared/Syslogs/System Logs", and user logs to individual folders.
#   run this script with sudo

## varibles
collectionfolder="/Users/Shared/Collected System Logs"
system_logs="/var/log/*"
list_of_users=$(ls /Users)

#check to make sure script is run with sudo
[ "$UID" -eq 0 ] || exec sudo bash "$0" "$@"

## make collection log directory
mkdir "$collectionfolder"
mkdir "$collectionfolder/syslogs"

## copy system logs
cp -R -p $system_logs "$collectionfolder/syslogs"

## create folder and copy logs per user
for x in $list_of_users;
do
    if [[ $x != "Shared" && $x != ".localized" ]];then
        #echo $x
        mkdir "$collectionfolder/$x"
        cp -R -p "/Users/$x/Library/Logs" "$collectionfolder/$x"
    fi
done

#change permissions so you can read/write logs. If you need to retain permissions for forensics, delete or comment out this line.
chmod -R 777 "$collectionfolder"
```


Shared
Search
Name
Date Modified
Collected System Logs
Today, 9:30 PM
nscott
Today, 9:30 PM
Logs
Today, 6:44 PM
syslogs
Today, 9:30 PM
accountpolicy.log
Today, 9:30 PM
accountpolicy.log.0.gz
Today, 12:20 AM
accountpolicy.log.1.gz
Yesterday, 12:00 AM
accountpolicy.log.2.gz
Jun 19, 2016, 12:57 AM
accountpolicy.log.3.gz
Jun 18, 2016, 12:04 AM
accountpolicy.log.4.gz
Jun 17, 2016, 12:53 AM
accountpolicy.log.5.gz
Jun 16, 2016, 8:22 PM
accountpolicy.log.6.gz
Jun 15, 2016, 12:03 AM
Accounts
Today, 8:34 PM
acroUpdaterTools.log
May 13, 2016, 7:46 PM
alf.log
Dec 5, 2015, 1:22 PM
Macintosh HD › Users › Shared

SYSDIAGNOSE

-- gathers system-wide diagnostic information helpful in investigating system performance

What sysdiagnose Collects:

- A spindump of the system
- Several seconds of fs_usage output
- Several seconds of top output
- Data about kernel zones
- Status of loaded kernel extensions
- Resident memory usage of user processes
- All system logs, kernel logs, opendirectory log, windowserver log
- power management logs
- A System Profiler report
- All spin and crash reports
- Disk usage information
- I/O Kit registry information
- Network status

#reports all data

```
sudo /usr/bin/sysdiagnose -f ~/Desktop/
```

#reports log data only

```
sudo /usr/bin/sysdiagnose -d —f ~/Desktop/
```

Accessibility
Mail
Safari
SystemConfiguration
acdiagnose-501.txt
airport_info.txt
apsd-status.txt
bc_stats.txt
bootstamps.txt
brctl
com.apple.windowserver.plist
crashes_and_spins
darwinup.txt
dig-results.txt
disks.txt
diskutil.txt
error_log.txt
find-system-migration-history.txt
fsck_hfs_user.log
fsck_hfs_var.log
gpt.txt
hdiutil-pmap.txt
ifconfig.txt
ioreg
ipconfig.txt
kextstat.txt
launchctl-dumpstate.txt
launchctl-list-0.txt
launchctl-list-501.txt
launchctl-print-gui-501.txt
launchctl-print-system.txt
launchctl-print-user-501.txt
locale-501.txt
logs
lsappinfo.txt
lskq.txt
lsregister.txt
microstackshots
microstackshots_lastday.txt
microstackshots_lasthour.txt
microstackshots_lastminute.txt
mount.txt
netstat
network-info
nfsstat.txt
odutil.txt
pluginkit-501.txt
pmset_everything.txt
reachability-info.txt
resolv.conf
scutil.txt
sysctl.txt
sysdiagnose.log
system_profiler.spx
talagent-501.txt
var_run_resolv.conf
zprint.txt

COLLECTING LOGS WITH OSXAUDITOR

-- free Mac OS X computer forensics tool

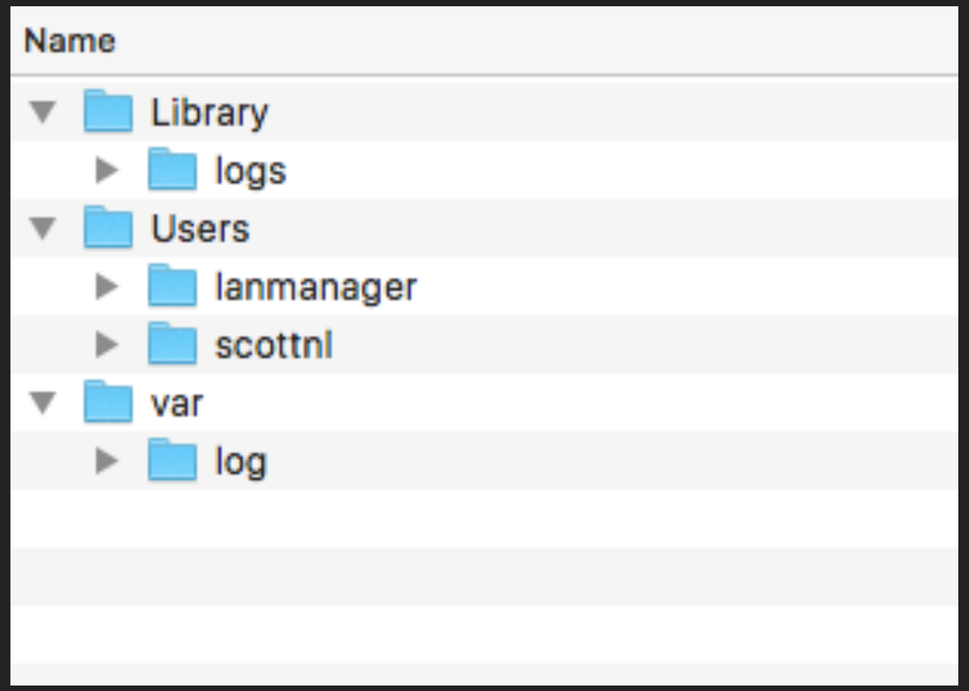
https://github.com/jipegit/OSXAuditor

It can aggregate all logs from the following directories into a zipball:

/var/log
/Library/logs
the user's ~/Library/logs

#usage example
sudo “path to osxauditor.py " -a -z “destination for zip file”

OSXAuditor_report_(computername)_20160224-192334.zip



CENTRALIZED LOGS

BENEFITS

- All your logs are in one location, making it easy to search

- Allows quicker access to information

- Allows for retention of logs, even if the client is off line or the logs have been deleted from the local machine

ELK

-- Elasticsearch, Logstash, Kibana

- Plenty of other options for centralized logging. This isn’t to say ELK is the only way to do this

- Whats more important is the ideas, not what tool you use

VISUALIZATION

-- Discover, Visualize, Dashboards

kibana

Discover | Visualize | Dashboard | Settings | Last 4 hours

*

logstash-*

107,189 hits

Selected Fields

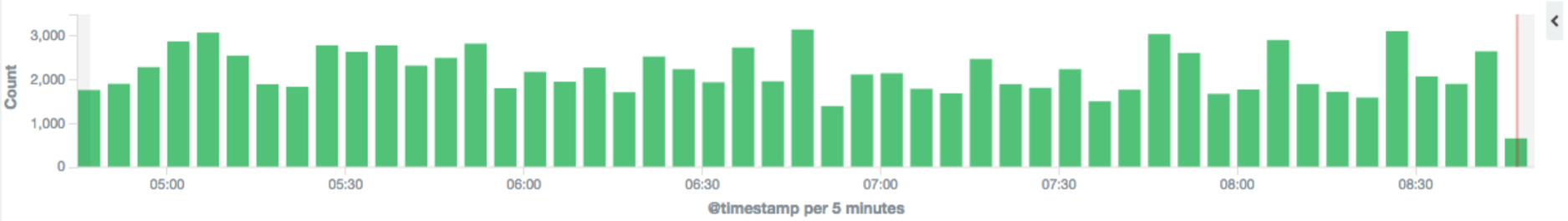
? _source

Available Fields

Popular

- t syslog_hostname
- t syslog_message
- t syslog_program
- @timestamp
- t @version
- t _id
- t _index
- # _score
- t _type
- t host
- t message
- received_at
- t received_from
- t syslog_facility
- # syslog_facility_code
- t syslog_pid
- t syslog_severity
- # syslog_severity_code
- t syslog_timestamp
- t type

June 13th 2016, 04:47:01.614 - June 13th 2016, 08:47:01.614 — by 5 minutes



Time	_source
June 13th 2016, 08:46:58.000	**message:** <27>Jun 13 08:46:58 sma206-13.local puppet-agent[27270]: Could not run: Could not create PID file: /var/lib/puppet/run/agent.pid **@version:** 1 **@timestamp:** June 13th 2016, 08:46:58.000 **type:** syslog **host:** 138.28.104.24 **syslog_timestamp:** Jun 13 08:46:58 **syslog_hostname:** sma206-13.local **syslog_program:** puppet-agent **syslog_pid:** 27270 **syslog_message:** Could not run: Could not create PID file: /var/lib/puppet/run/agent.pid **received_at:** June 13th 2016, 08:48:19.950 **received_from:** 138.28.104.24 **syslog_severity_code:** 5 **syslog_facility_code:** 1 **syslog_facility:** user-level **syslog_severity:** notice **_id:** AVVJzjxMt4s8YfaV2kMJ
June 13th 2016, 08:46:58.000	**message:** <27>Jun 13 08:46:58 olin213-02.local puppet-agent[351]: Could not request certificate: Operation timed out - connect(2) **@version:** 1 **@timestamp:** June 13th 2016, 08:46:58.000 **type:** syslog **host:** 138.28.20.189 **syslog_timestamp:** Jun 13 08:46:58 **syslog_hostname:** olin213-02.local **syslog_program:** puppet-agent **syslog_pid:** 351 **syslog_message:** Could not request certificate: Operation timed out - connect(2) **received_at:** June 13th 2016, 08:48:20.083 **received_from:** 138.28.20.189 **syslog_severity_code:** 5 **syslog_facility_code:** 1 **syslog_facility:** user-level **syslog_severity:** notice **_id:** AVVJzjxMt4s8YfaV2kMM **_type:** syslog **_index:** l
June 13th 2016, 08:46:57.000	**message:** <29>Jun 13 08:46:57 sma206-11.local ruby[3275]: **@version:** 1 **@timestamp:** June 13th 2016, 08:46:57.000 **type:** syslog **host:** 138.28.104.22 **syslog_timestamp:** Jun 13 08:46:57 **syslog_hostname:** sma206-11.local **syslog_program:** ruby **syslog_pid:** 3275 **syslog_message:** **received_at:** June 13th 2016, 08:48:18.700 **received_from:** 138.28.104.22 **syslog_severity_code:** 5 **syslog_facility_code:** 1 **syslog_facility:** user-level **syslog_severity:** notice **_id:** AVVJzjVpt4s8YfaV2kMH **_type:** syslog **_index:** l ogstash-2016.06.13 **score:**
June 13th 2016, 08:46:56.000	**message:** <29>Jun 13 08:46:56 sma206-13.local ruby[27270]: **@version:** 1 **@timestamp:** June 13th 2016, 08:46:56.000 **type:** syslog **host:** 138.28.104.24 **syslog_timestamp:** Jun 13 08:46:56 **syslog_hostname:** sma206-13.local **syslog_program:** ruby **syslog_pid:** 27270 **syslog_message:** **received_at:** June 13th 2016, 08:48:18.160 **received_from:** 138.28.104.24 **syslog_severity_code:** 5

kibana

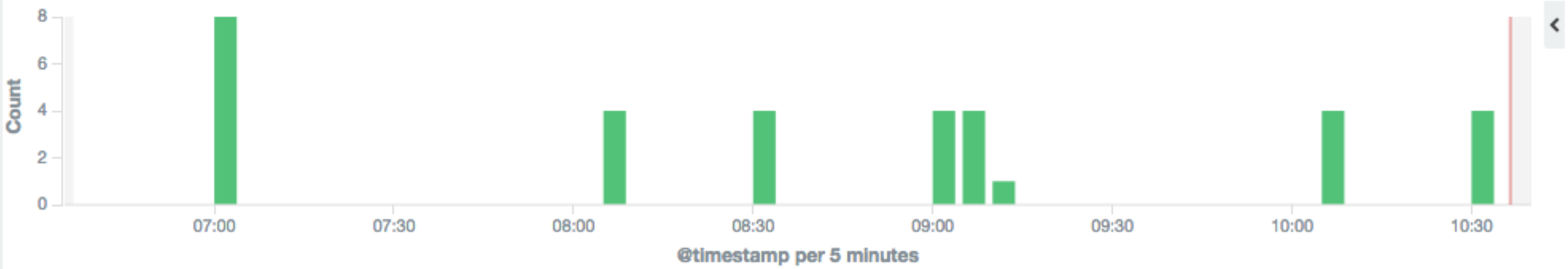
Discover | Visualize | Dashboard | Settings | Last 4 hours

sleep

logstash-*

33 hits

May 20th 2016, 06:36:26.906 - May 20th 2016, 10:36:26.906 — by 5 minutes



Selected Fields

? _source

Available Fields

Popular

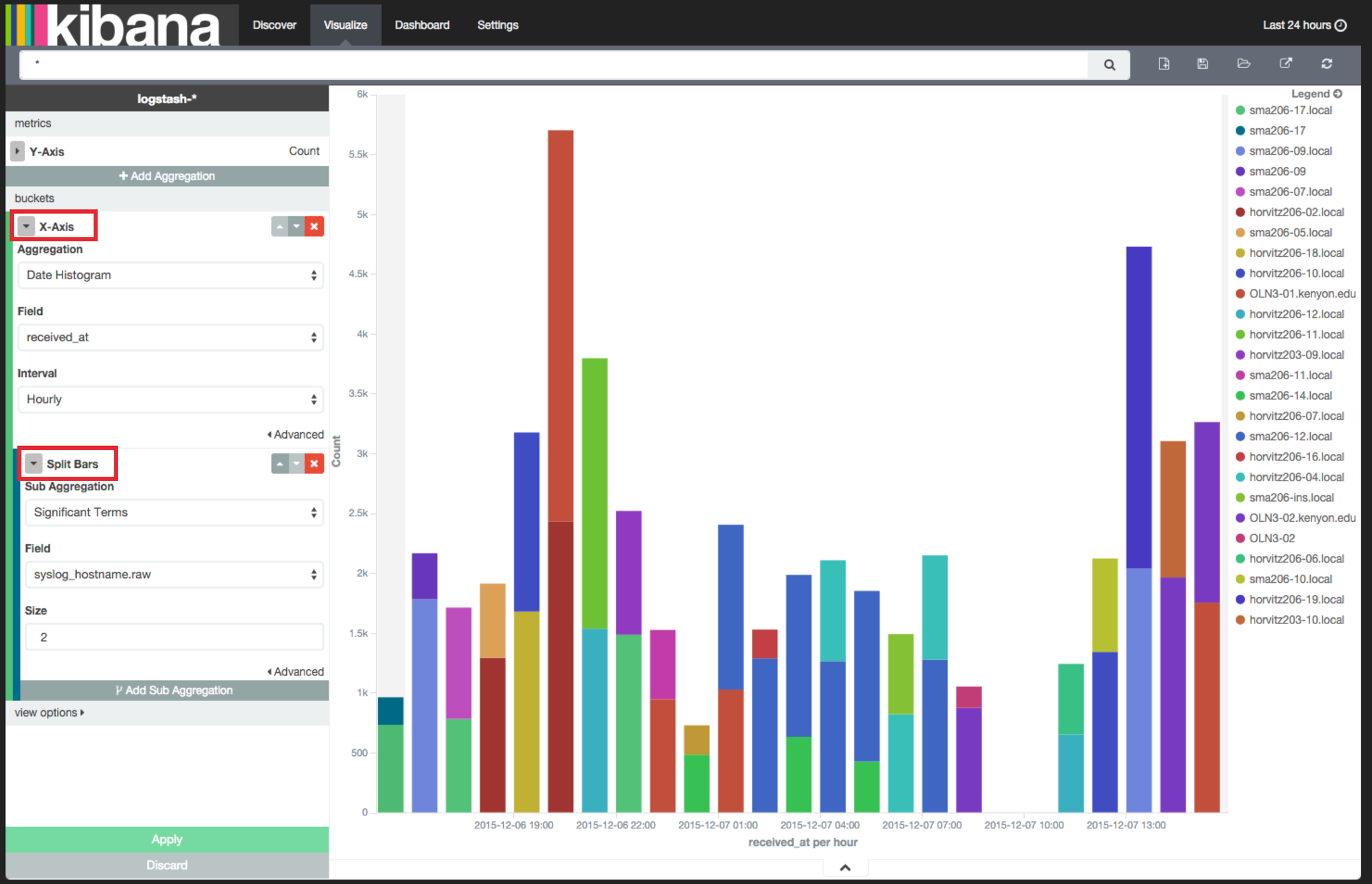
t syslog_hostname
t syslog_message
t syslog_program
@timestamp
t @version
t _id
t _index
_score
t _type
t host
t message
received_at
t received_from
t syslog_facility
syslog_facility_code
t syslog_pid
t syslog_severity

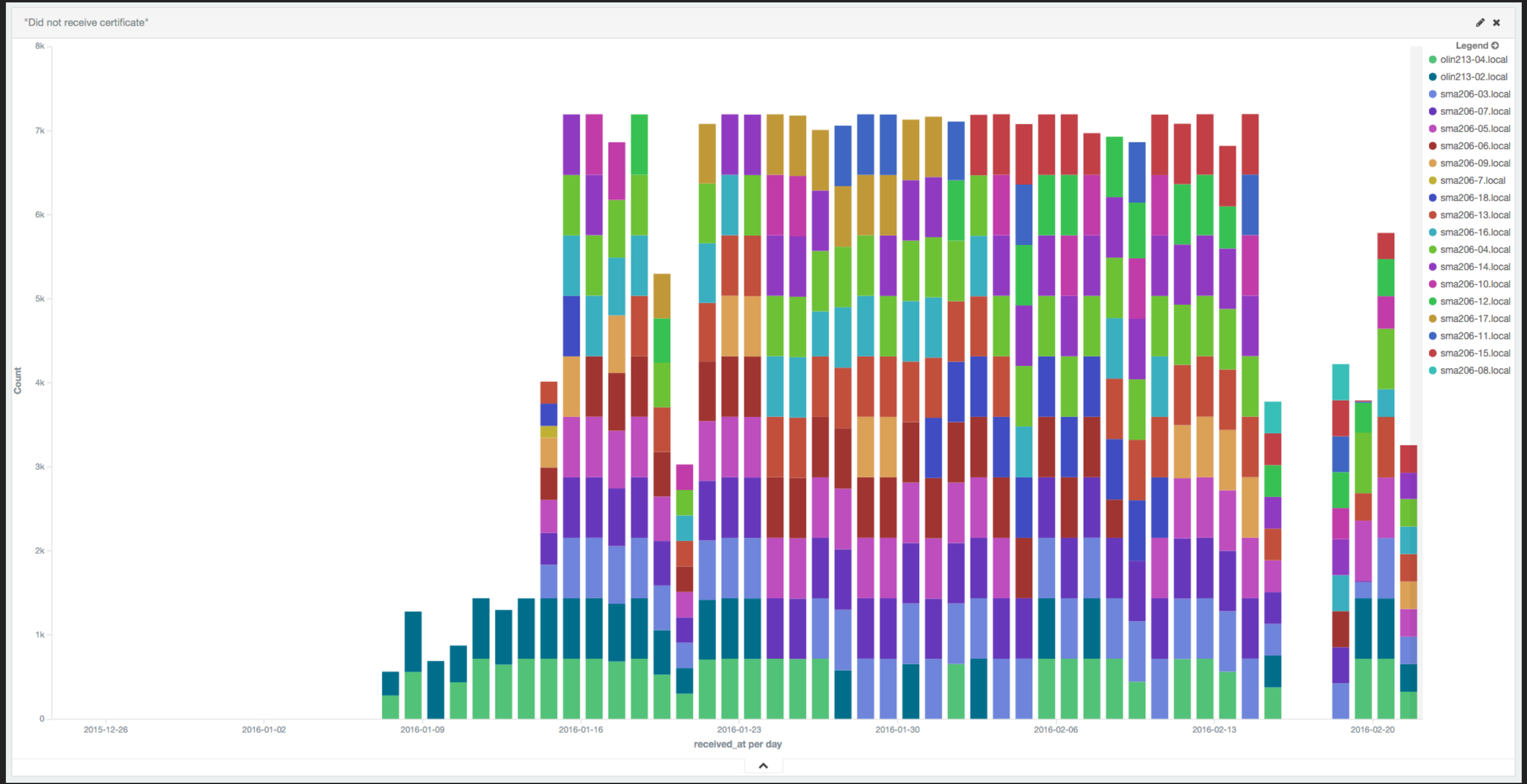
Time	_source
May 20th 2016, 10:33:19.000	**message:** <5>May 20 10:33:19 sma206-09 kernel[0]: ARPT: 708491.581530: AirPort_Brcm43xx::powerChange: System Sleep **syslog_message:** ARPT: 708491.581530: AirPort_Brcm43xx::powerChange: System Sleep **@version:** 1 **@timestamp:** May 20th 2016, 10:33:19.000 **type:** syslog **host:** 138.28.104.20 **syslog_timestamp:** May 20 10:33:19 **syslog_hostname:** sma206-09 **syslog_program:** kernel[0] **received_at:** May 20th 2016, 10:34:09.645 **received_from:** 138.28.104.20 **syslog_severity_code:** 5
May 20th 2016, 10:33:18.000	**message:** <31>May 20 10:33:18 sma206-09.local ntpd[503]: sleep noticed **syslog_message:** sleep noticed **@version:** 1 **@timestamp:** May 20th 2016, 10:33:18.000 **type:** syslog **host:** 138.28.104.20 **syslog_timestamp:** May 20 10:33:18 **syslog_hostname:** sma206-09.local **syslog_program:** ntpd **syslog_pid:** 503 **received_at:** May 20th 2016, 10:34:08.918 **received_from:** 138.28.104.20 **syslog_severity_code:** 5 **syslog_facility_code:** 1 **syslog_facility:** user-level **syslog_severity:** noti
May 20th 2016, 10:33:17.000	**message:** <31>May 20 10:33:17 sma206-09.local configd[202]: SCNC Controller: pm_ConnectionHandler going to sleep, delay = 0. **syslog_message:** SCNC Controller: pm_ConnectionHandler going to sleep, delay

Create a new visualization

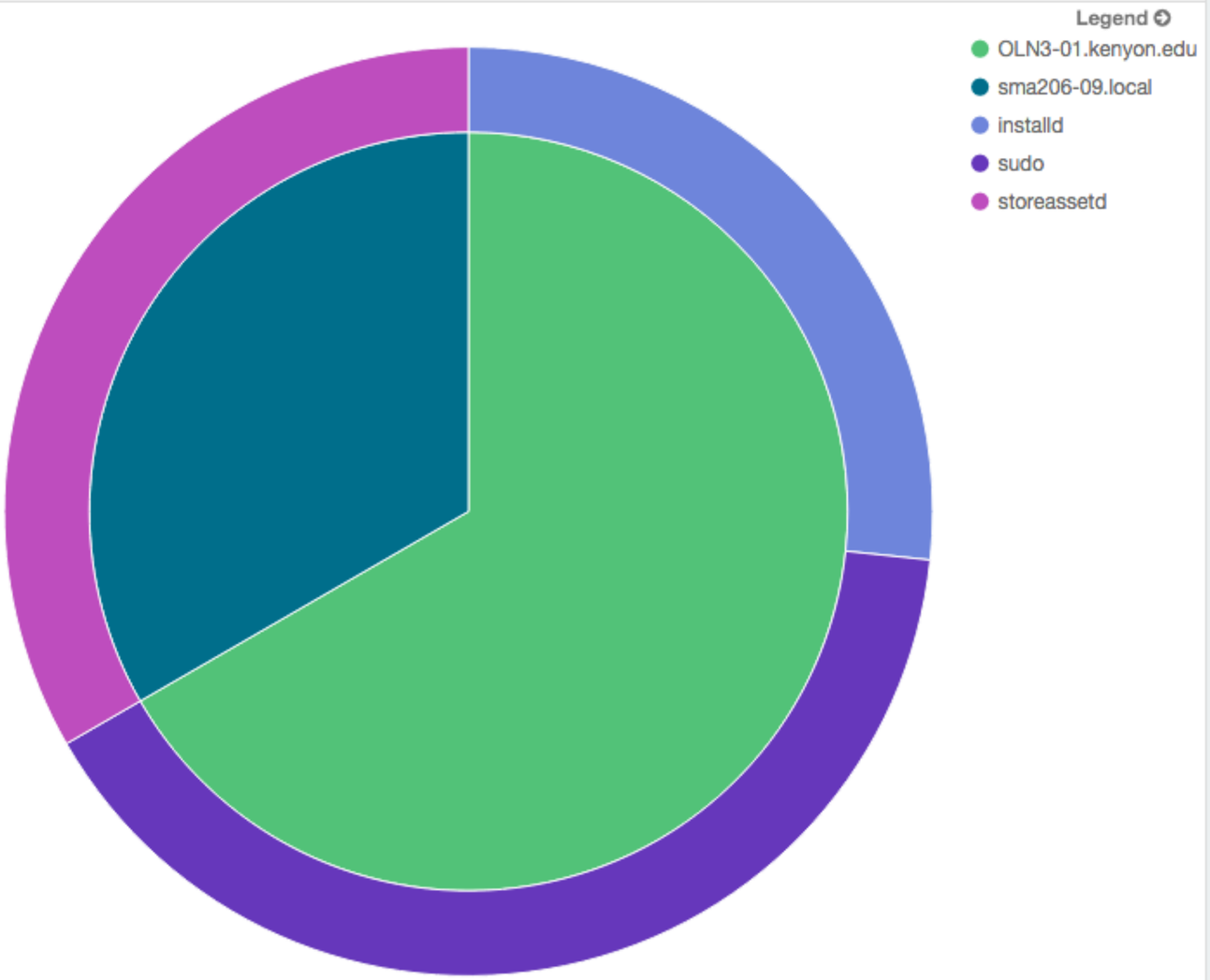
Step 1

Area chart	Great for stacked timelines in which the total of all series is more important than comparing any two or more series. Less useful for assessing the relative change of unrelated data points as changes in a series lower down the stack will have a difficult to gauge effect on the series above it.
Data table	The data table provides a detailed breakdown, in tabular format, of the results of a composed aggregation. Tip, a data table is available from many other charts by clicking grey bar at the bottom of the chart.
Line chart	Often the best chart for high density time series. Great for comparing one series to another. Be careful with sparse sets as the connection between points can be misleading.
Markdown widget	Useful for displaying explanations or instructions for dashboards.
Metric	One big number for all of your one big number needs. Perfect for showing a count of hits, or the exact average a numeric field.
Pie chart	Pie charts are ideal for displaying the parts of some whole. For example, sales percentages by department.Pro Tip: Pie charts are best used sparingly, and with no more than 7 slices per pie.
Tile map	Your source for geographic maps. Requires an elasticsearch geo_point field. More specifically, a field that is mapped as type:geo_point with latitude and longitude coordinates.
Vertical bar chart	The goto chart for oh-so-many needs. Great for time and non-time data. Stacked or grouped, exact numbers or percentages. If you are not sure which chart your need, you could do worse than to start here.


kibana
Discover
Visualize
Dashboard
Settings
Last 24 hours
*
logstash-*
metrics
Y-Axis
Count
+ Add Aggregation
buckets
X-Axis
Aggregation
Date Histogram
Field
received_at
Interval
Hourly
Advanced
Split Bars
Sub Aggregation
Significant Terms
Field
syslog_hostname.raw
Size
2
Advanced
Add Sub Aggregation
view options
Apply
Discard
Count
6k
5.5k
5k
4.5k
4k
3.5k
3k
2.5k
2k
1.5k
1k
500
0
2015-12-06 19:00
2015-12-06 22:00
2015-12-07 01:00
2015-12-07 04:00
2015-12-07 07:00
2015-12-07 10:00
2015-12-07 13:00
received_at per hour
Legend
sma206-17.local
sma206-17
sma206-09.local
sma206-09
sma206-07.local
horvitz206-02.local
sma206-05.local
horvitz206-18.local
horvitz206-10.local
OLN3-01.kenyon.edu
horvitz206-12.local
horvitz206-11.local
horvitz203-09.local
sma206-11.local
sma206-14.local
horvitz206-07.local
sma206-12.local
horvitz206-16.local
horvitz206-04.local
sma206-ins.local
OLN3-02.kenyon.edu
OLN3-02
horvitz206-06.local
sma206-10.local
horvitz206-19.local
horvitz203-10.local


"Did not receive certificate"
Legend
olin213-04.local
olin213-02.local
sma206-03.local
sma206-07.local
sma206-05.local
sma206-06.local
sma206-09.local
sma206-7.local
sma206-18.local
sma206-13.local
sma206-16.local
sma206-04.local
sma206-14.local
sma206-10.local
sma206-12.local
sma206-17.local
sma206-11.local
sma206-15.local
sma206-08.local
Count
8k
7k
6k
5k
4k
3k
2k
1k
0
2015-12-26
2016-01-02
2016-01-09
2016-01-16
2016-01-23
2016-01-30
2016-02-06
2016-02-13
2016-02-20
received_at per day

Software Installs



Machines That Have Downloaded El Capitan

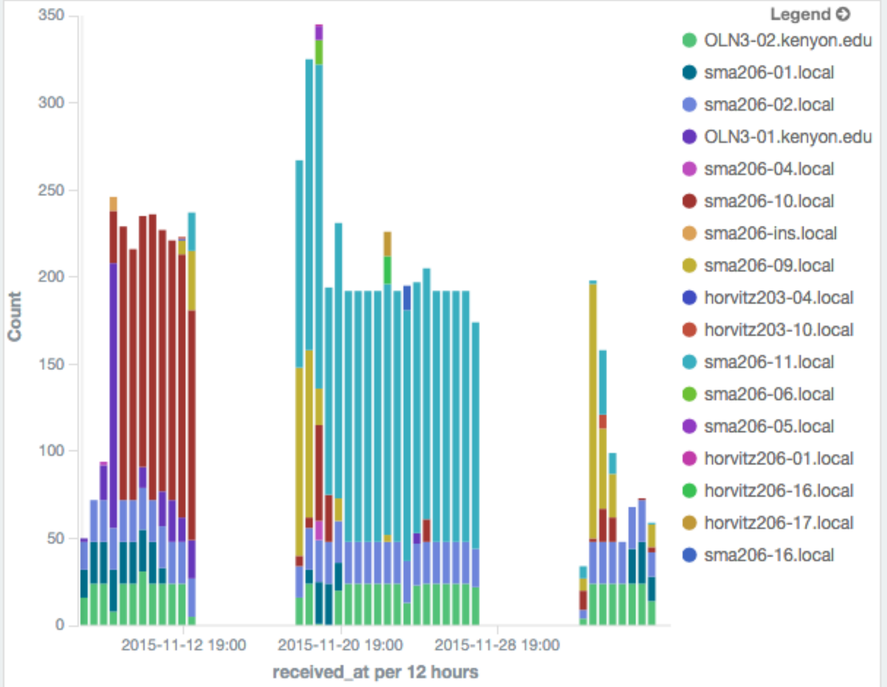
2

Unique count of syslog_hostname.raw

kibana | Discover | Visualize | Dashboard | Settings | Last 30 days

sudo usage | *

SUDO Usage



Sudo Usage Top Commands

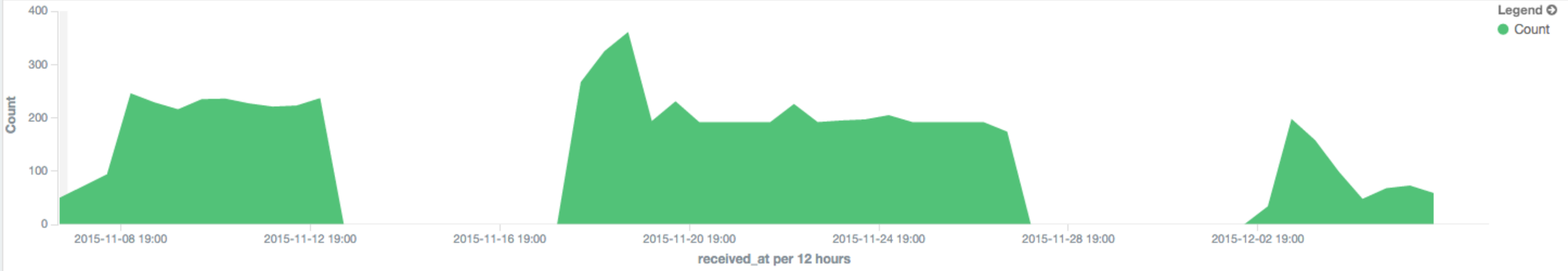
Top 10 unusual terms in syslog_message.raw	Count
root : TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/bin/cat /var/log/commerce.log	2416
root : TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/usr/bin/defaults read /Library/Preferences/com.apple.loginwindow autoLoginUser	1296
weingoldh : no tty present and no askpass program specified ; TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/bin/cat /var/log/commerce.log	53
hnl : no tty present and no askpass program specified ; TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/bin/cat /var/log/commerce.log	38
colmenaresa : no tty present and no askpass program specified ; TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/bin/cat /var/log/commerce.log	23
harperka : no tty present and no askpass program specified ; TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/bin/cat /var/log/commerce.log	20
rasot : no tty present and no askpass program specified ; TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/bin/cat	20

Sudo Usage Top Machines

Top 10 unusual terms in syslog_hostname.raw	Count
sma206-11.local	2645
sma206-10.local	1368
sma206-02.local	827
OLN3-02.kenyon.edu	741
sma206-09.local	478
sma206-01.local	310
OLN3-01.kenyon.edu	269
horvitz206-16.local	17
sma206-06.local	14
horvitz206-17.local	15

Export: Raw Formatted

Sudo Usage Activity



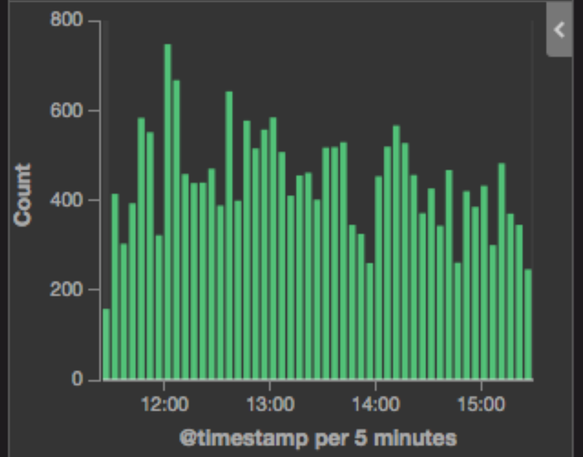
kibana

Discover | Visualize | Dashboard | Settings

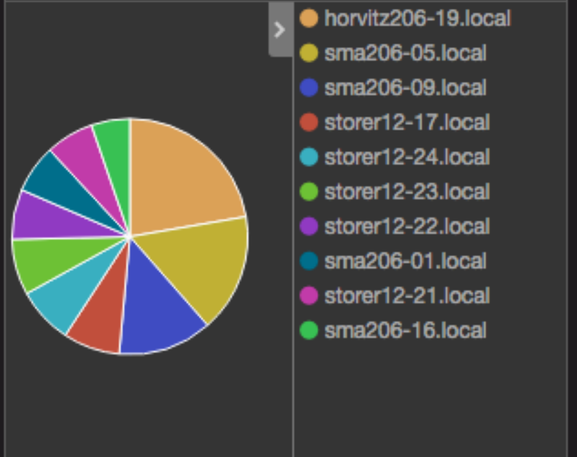
Last 4 hours

Errors *

error - total amount



error - client percentage



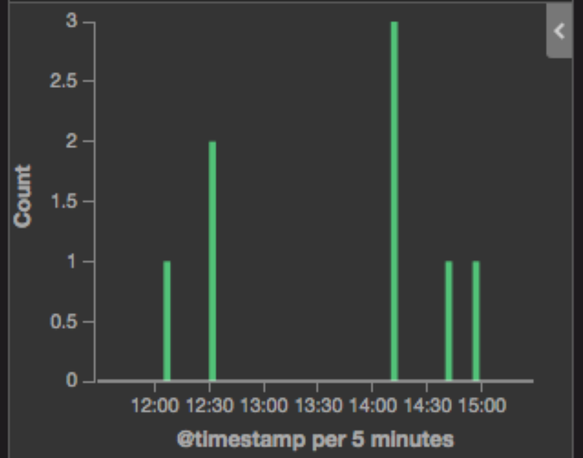
error - top clients

syslog_hostname.raw: Descending	Count
horvitz206-19.local	1,765
sma206-05.local	1,287
sma206-09.local	1,022
storer12-17.local	616
storer12-24.local	613

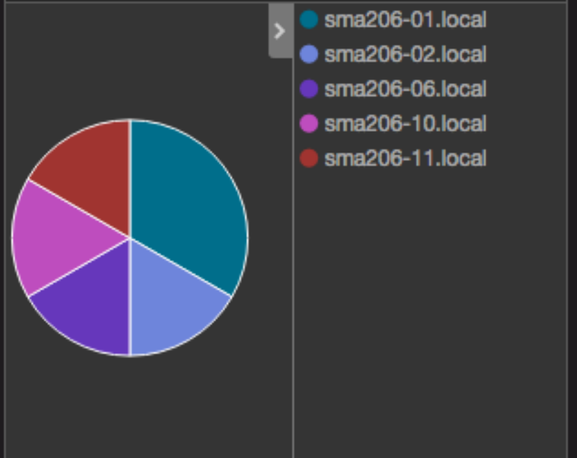
error - top programs

syslog_program.raw: Descending	Count
mdworker	6,604
Final Cut Pro	1,796
mdmclient	1,175
nsurlstoraged	1,139
loginwindow	702

critical - total amount



critical - client percentage

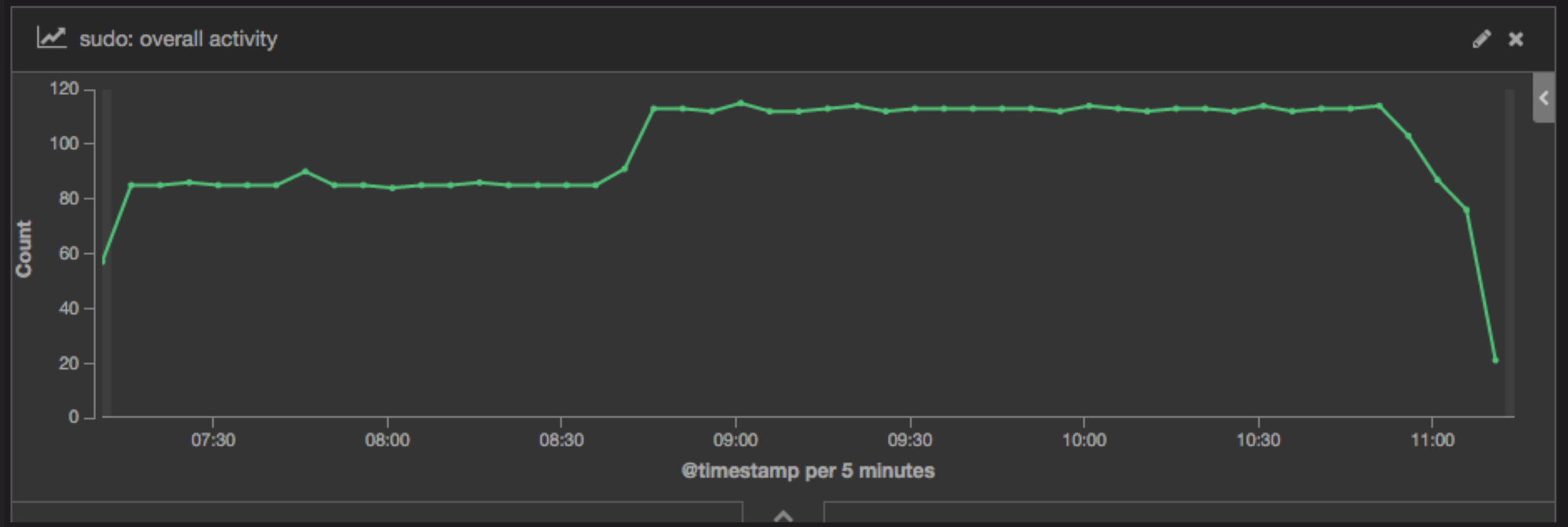


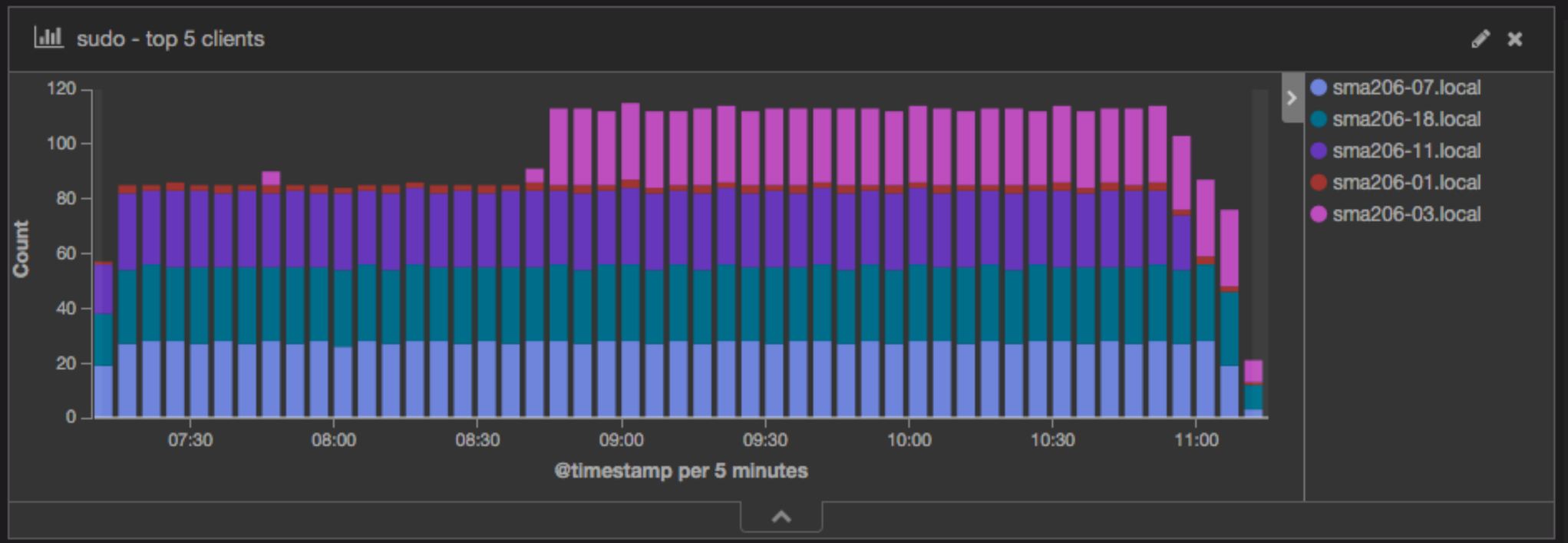
critical - top clients

syslog_hostname.raw: Descending	Count
sma206-01.local	2
sma206-02.local	1
sma206-06.local	1
sma206-10.local	1
sma206-11.local	1

critical - top programs

syslog_program.raw: Descending	Count
coreaudiod	8


sudo: overall activity
120
100
80
60
40
20
0
Count
07:30
08:00
08:30
09:00
09:30
10:00
10:30
11:00
@timestamp per 5 minutes


sudo - top 5 clients
120
100
80
60
40
20
0
Count
07:30
08:00
08:30
09:00
09:30
10:00
10:30
11:00
@timestamp per 5 minutes
sma206-07.local
sma206-18.local
sma206-11.local
sma206-01.local
sma206-03.local

Sudo - unusual commands

syslog_message.raw: Descending	Count
You have not agreed to the Xcode license agreements, please run 'xcodebuild -license' (for user-level acceptance) or 'sudo xcodebuild -license' (for system-wide acceptance) from within a Terminal window to review and agree to the Xcode license agreements.	4,814
lanmanager : TTY=ttys000 ; PWD=/Users/lanmanager ; USER=root ; COMMAND=/usr/bin/xcodebuild -license	2

Sudo - unusual commands

syslog_message.raw: Descending	Count
You have not agreed to the Xcode license agreements, please run 'xcodebuild -license' (for user-level acceptance) or 'sudo xcodebuild -license' (for system-wide acceptance) from within a Terminal window to review and agree to the Xcode license agreements.	172
mdworker(40529) deny mach-lookup com.apple.nsurlstorage-cache (import fstype:hfs fsflag:480D000 flags:240000005E diag:0 isXCode:0 uti:public.html plugin:/Library/Spotlight/RichText.mdimporter - find suspect file using: sudo mdutil -t 29486876)	2
mdworker(56615) deny mach-lookup com.apple.nsurlstorage-cache (import fstype:hfs fsflag:480D000 flags:240000005E diag:0 isXCode:0 uti:public.html plugin:/Library/Spotlight/RichText.mdimporter - find suspect file using: sudo mdutil -t 39938711)	2
root : TTY=unknown ; PWD=/ ; USER=[redacted] ; COMMAND=/bin/bash -c unset SUDO_COMMAND ; /bin/launchctl list	1
root : TTY=unknown ; PWD=/ ; USER=[redacted] ; COMMAND=/bin/bash -c unset SUDO_COMMAND ; /bin/launchctl load -S Aqua "/Library/LaunchAgents/com.google.keystone.agent.plist"	1

EXAMPLES

- "sending status (OS X El Capitan)”
- “appleID="
- "Premiere" AND “crash"
- syslog_program: “AccountPolicyHelper” (exclude local accounts)
- munki*
- "puppet" AND "Could not retrieve catalog from remote server”
- "System Version 10.11” (filter by unique hostname)
- "starting download"

ENROLL CLIENTS

EDIT /ETC/SYSLOG.CONF

```
# Note that flat file logs are now configured in /etc/asl.conf

install.*                       @127.0.0.1:32376
*.*     @xxx.xxx.xxx.xxx
```

ENROLL CLIENTS WITH BASH SCRIPT

```
#!/bin/bash
#this scripts forwards local machines logs to logstash server

#add logserver to local machines
echo -e "\n*.*       @xxx.xxx.xxx.xxx” >> /etc/syslog.conf

#unload syslog
sudo launchctl unload /System/Library/LaunchDaemons/com.apple.syslogd.plist

Sleep 2

#load syslog
sudo launchctl load /System/Library/LaunchDaemons/com.apple.syslogd.plist
```

NOW WHAT?

- USE LOGS TO BE INFORMED ABOUT YOUR FLEET
- USE LOGS TO MAKE BETTER DECISIONS
- USE LOGS TO HELP ALERT, REPORT, & AUDIT

EXAMPLES & IDEAS

- DeployStudio scripts
- Custom scripts (run with ARD on remote machines)
- ELK, Splunk, Loggly
- Munki, Casper, Puppet, Chef, Meraki, … on and on
- Launch daemons (watchpath, Periodically)

RESOURCES & LINKS

https://redlinetech.wordpress.com

Github
https://github.com/nlscott

Apple Developer, Logging Errors and Warnings
https://developer.apple.com/library/mac/documentation/MacOSX/Conceptual/BPSystemStartup/Chapters/LoggingErrorsAndWarnings.html#//apple_ref/doc/uid/10000172i-SW8-SW1

OpenBSM auditing on Mac OS X
https://derflounder.wordpress.com/2012/01/30/openbsm-auditing-on-mac-os-x/

Apple: Mac OS X Server: The System Log
https://support.apple.com/kb/TA26117?locale=en_US

Mac OS X and iOS Internals: To the Apples core by Jonathan Levin (book)

ASL & Open BSM (page 45-56)
https://www.ma.rhul.ac.uk/static/techrep/2015/RHUL-MA-2015-8.pdf

CIA Apple OS X 10.11 Benchmark (page 50-57)
https://benchmarks.cisecurity.org/downloads/show-single/?file=osx1011.100

Logs, Damn Logs and Statistics, Ed Marczak, MacAdmins 2012
https://www.youtube.com/watch?v=dnMnpLsYmxA&list=PL812EF75E41B85E68&index=13

Design and Implementation of theTrustedBSD Mac Framework
http://www.trustedbsd.org/trustedbsd-discex3.pdf

Mac OS X Server: The System Log
https://support.apple.com/kb/TA26117?locale=en_US

AUDIT_CONTROL
http://www.freebsd.org/cgi/man.cgi?apropos=0&sektion=5&query=audit_control&manpath=FreeBSD+7.0-current&format=html

OSXAuditor
https://github.com/jipegit/OSXAuditor

When Mac's Get Hacked
https://digital-forensics.sans.org/summit-archives/2012/when-macs-get-hacked.pdf

Bash Redirection
http://www.catonmat.net/blog/bash-one-liners-explained-part-three/

Enterprise Mac Security: El Capitan, Chapter 5, Reviewing logs and monitoring
https://www.amazon.com/Enterprise-Mac-Security-OS/dp/148421711X?ie=UTF8&*Version*=1&*entries*=0

How To Install Elasticsearch, Logstash, and Kibana (ELK Stack) on Ubuntu 14.04
https://www.digitalocean.com/community/tutorials/how-to-install-elasticsearch-logstash-and-kibana-elk-stack-on-ubuntu-14-04

audit by two canoes
https://github.com/twocanoes/audit

Sawmill: Universal Log File Analysis and Reporting
https://www.sawmill.net/cgi-bin/download.pl

Sentry Tools: event logging platform focused on capturing and aggregating exceptions
https://getsentry.com/welcome/

Log watch: Logwatch is a customizable log analysis system.
https://sourceforge.net/projects/logwatch/

Watcher: Alerting for Elasticsearch
https://www.elastic.co/products/watcher

MacResponse LE
http://macresponseforensics.com/

LiveResponseCollection-Allosaurus
http://www.brimorlabsblog.com/2016/01/live-response-collection-allosaurus.html

OSXcollector
https://github.com/Yelp/osxcollector

THANK YOU