Logging

About Needles in the Modern Haystack

zentral.pro

Who are we ?

zentral.pro

- Founded in Q1 2019
- Based in Germany
- Small, skilled team
- Professional Services

  Research and Development
- Business & Enterprises customers
- B2B Partners

Who am I

Henry Stamerjohann

zentral.pro

- Based in Hamburg, Germany
- Zentral Pro Services *(co-founder)*
- Started the Zentral open source Event Hub Project with Éric Falconnier *(co-founder)*
- Zentral was first shown in public at MacSysAdmin 2015

Landscape

zentral.pro

Landscape

Logs & Events

- Computing / Technology

“A lot more events, from many more sources…”

Landscape

Logs & Events

- Computing / Technology

- Cloud Computing Platforms and SaaS
- Linux *(incl. ChromeOS)*
- Microsoft:
  - Azure, Intune, Windows 10

    (new norm, great integrations)
- Apple:
  - macOS, iOS, iPadOS, tvOS
  - Client Management & MDM Provider

    (well known challenge w/ integrations)

Landscape

Logs & Events

- Computing / Technology

“Where, when and what ? “

Landscape

Logs & Events

- Computing / Technology

“Where, when and what ? “

- Created by apps, systems, network and user activity
- Event flow, time stamps, and Frequency
- Common use:
  - Check-based fault detection
  - Log-based monitoring
  - Metrics-based monitoring
  - Collect telemetry data

Event sources and types

Event sources and types

On the endpoints

▸ Sources

OS

- Installer
- MDMclient
- LaunchServices

Software

- Business apps
- Other apps
- Security Agents
  - Osquery
  - Santa
  - Xnumon

Event sources and types

On the endpoints

- Sources
  - Security Agents: Osquery

Osquery

- Cloud Native Foundation Project
- Powerful Change Detection
- SQL like view of the system

Based on

- OS
- Multi Platform *(Mac, Linux, Windows)*

Event sources and types

On the endpoints

- Sources
  - Security Agents: Google Santa

Santa

- Binary Whitelisting / Blacklisting
- TLS Server *(Backend)*
- Dynamic Config
- Local Log file

Based on

- Kernel extension
- *(soon)* Security Extention

Event sources and types

On the endpoints

- Sources
  - Security Agents: Xnumon

Xnumon

- Log Information on
  - pid
  - path
  - ancestory
  - arguments
  - code-signing information
- Trace activity *(good/bad)*

Based on

- Open BSM
- Kernel extension

Event sources and types

On the endpoints

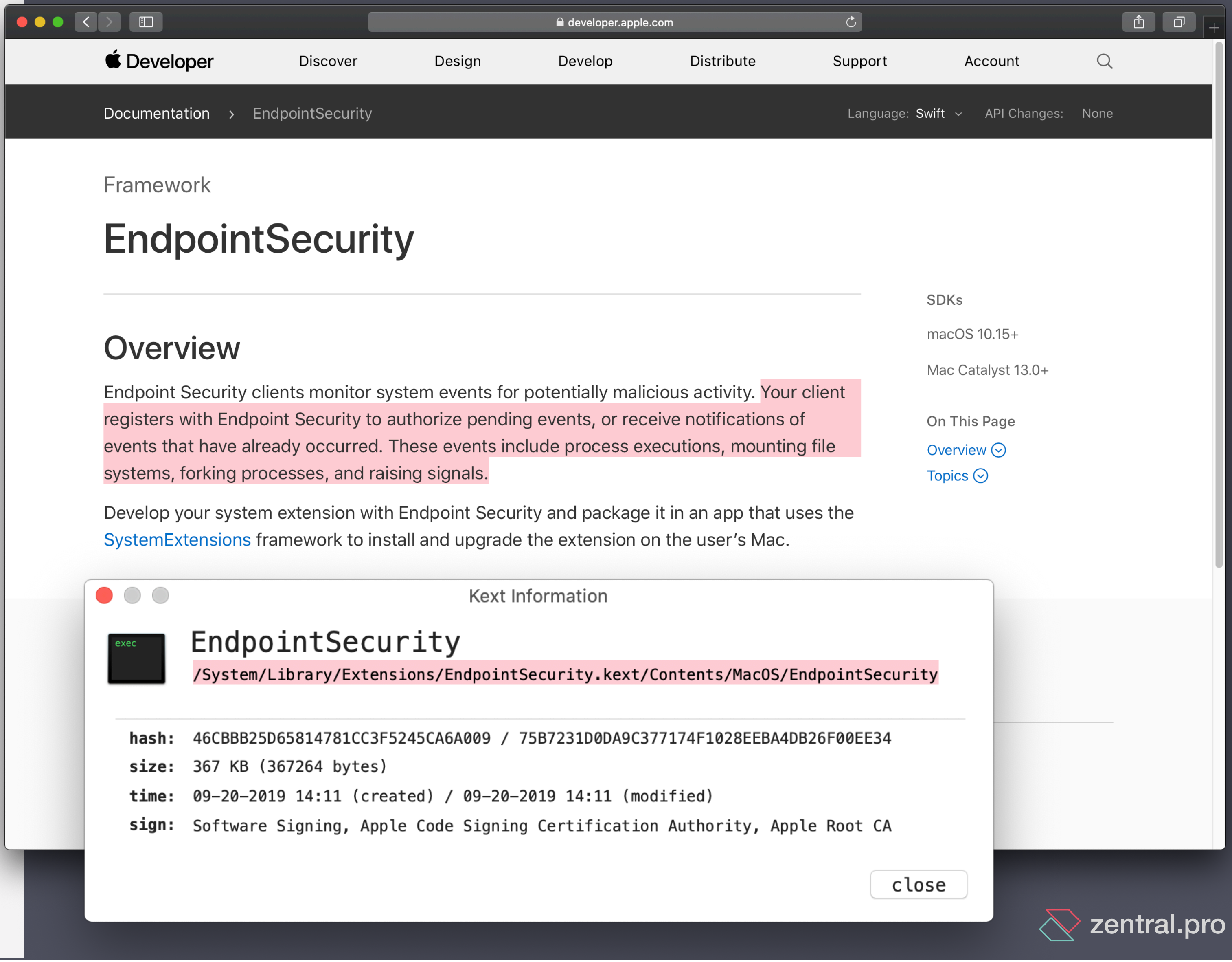
- Sources
  - Security Agents: System Extensions

zentral.pro

Event sources and types

On the endpoints

- Sources
  - Security Agents: System Extensions



Framework

EndpointSecurity

Overview

Endpoint Security clients monitor system events for potentially malicious activity. Your client registers with Endpoint Security to authorize pending events, or receive notifications of events that have already occurred. These events include process executions, mounting file systems, forking processes, and raising signals.

Develop your system extension with Endpoint Security and package it in an app that uses the SystemExtensions framework to install and upgrade the extension on the user's Mac.

SDKs

macOS 10.15+

Mac Catalyst 13.0+

On This Page

Overview

Topics

Kext Information

EndpointSecurity

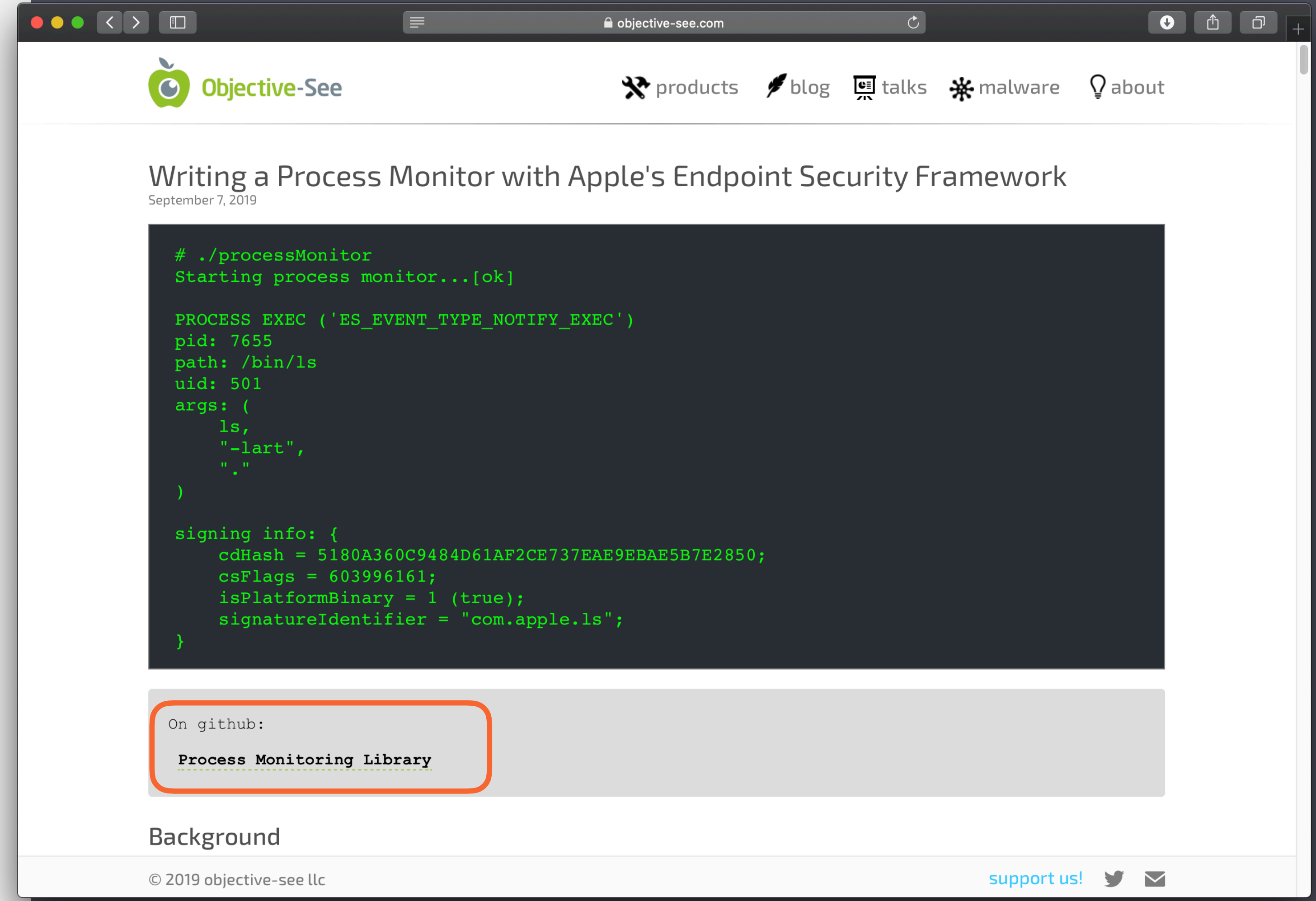
/System/Library/Extensions/EndpointSecurity.kext/Contents/MacOS/EndpointSecurity

```
hash:  46CBBB25D65814781CC3F5245CA6A009 / 75B7231D0DA9C377174F1028EEBA4DB26F00EE34
size:  367 KB (367264 bytes)
time:  09-20-2019 14:11 (created) / 09-20-2019 14:11 (modified)
sign:  Software Signing, Apple Code Signing Certification Authority, Apple Root CA
```

Event sources and types

On the endpoints

- Sources
  - Security Agents: System Extensions



Writing a Process Monitor with Apple's Endpoint Security Framework

September 7, 2019

```
# ./processMonitor
Starting process monitor...[ok]

PROCESS EXEC ('ES_EVENT_TYPE_NOTIFY_EXEC')
pid: 7655
path: /bin/ls
uid: 501
args: (
    ls,
    "-lart",
    "."
)

signing info: {
    cdHash = 5180A360C9484D61AF2CE737EAE9EBAE5B7E2850;
    csFlags = 603996161;
    isPlatformBinary = 1 (true);
    signatureIdentifier = "com.apple.ls";
}
```

On github:

Process Monitoring Library

Background

© 2019 objective-see llc

zentral.pro

Event sources and types

On the endpoints

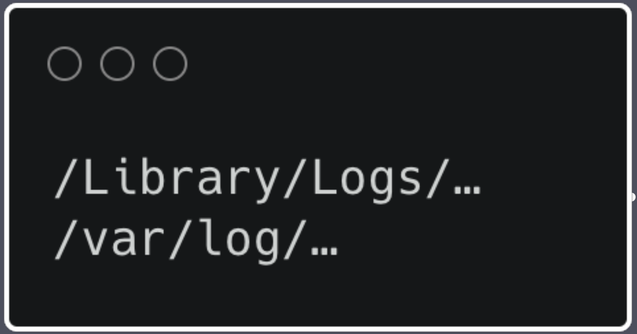
▸ Outputs

- Written to File
- Written to local Database
- Written to a Backend
- Transferred by an Agent

Event sources and types

On the endpoints

- Outputs
  - File based



```
/Library/Logs/…
/var/log/…
```

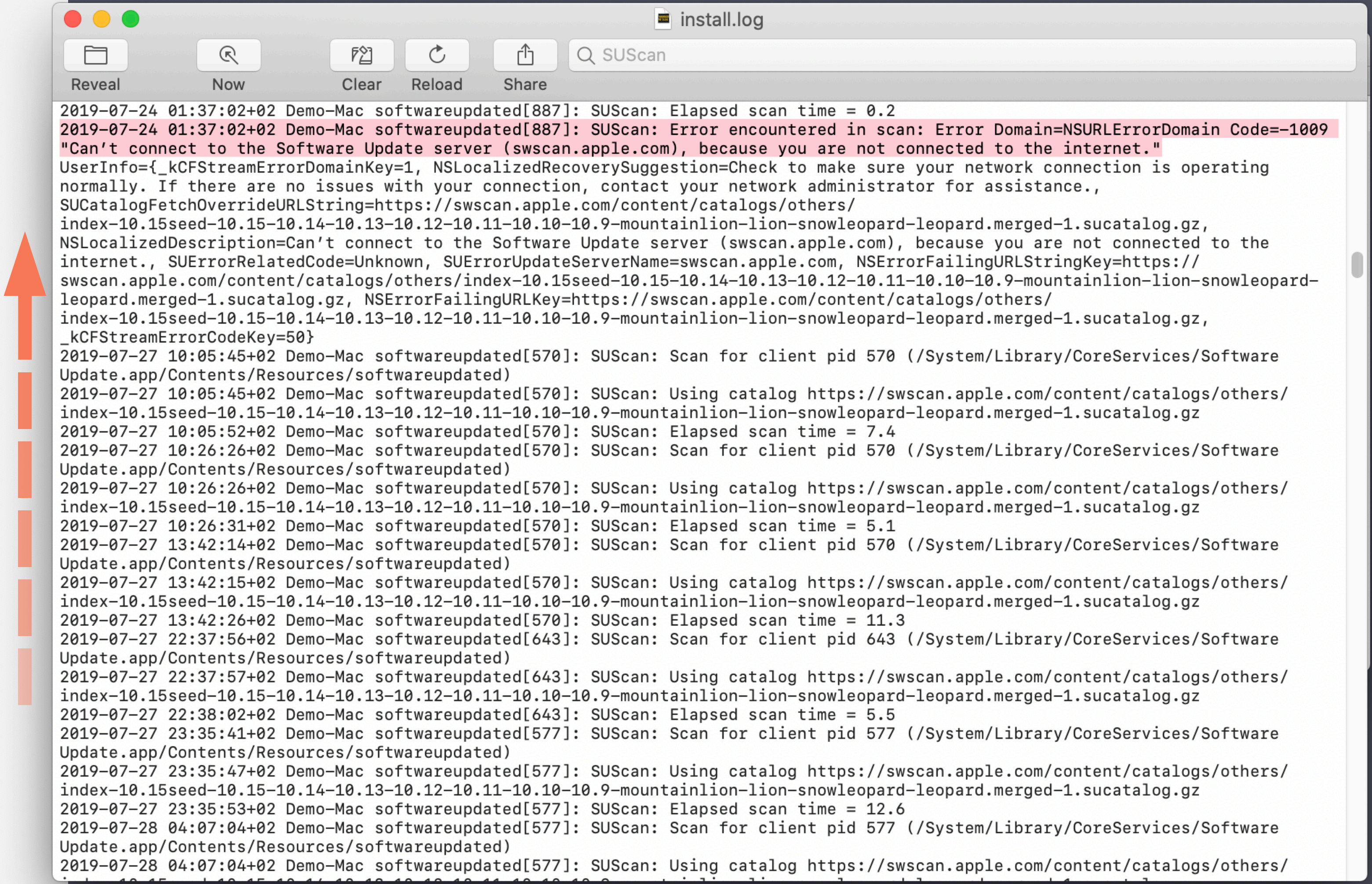
File based - the “classic” use case

- mostly with not so well integrated apps
- Text data in files *(rotated)*
- Sometimes JSON *(1 object per line)*

Event sources and types

On the endpoints

- Outputs
  - File based



```
2019-07-24 01:37:02+02 Demo-Mac softwareupdated[887]: SUScan: Elapsed scan time = 0.2
2019-07-24 01:37:02+02 Demo-Mac softwareupdated[887]: SUScan: Error encountered in scan: Error Domain=NSURLErrorDomain Code=-1009
"Can't connect to the Software Update server (swscan.apple.com), because you are not connected to the internet."
UserInfo={_kCFStreamErrorDomainKey=1, NSLocalizedRecoverySuggestion=Check to make sure your network connection is operating
normally. If there are no issues with your connection, contact your network administrator for assistance.,
SUCatalogFetchOverrideURLString=https://swscan.apple.com/content/catalogs/others/
index-10.15seed-10.15-10.14-10.13-10.12-10.11-10.10-10.9-mountainlion-lion-snowleopard-leopard.merged-1.sucatalog.gz,
NSLocalizedDescription=Can't connect to the Software Update server (swscan.apple.com), because you are not connected to the
internet., SUErrorRelatedCode=Unknown, SUErrorUpdateServerName=swscan.apple.com, NSErrorFailingURLStringKey=https://
swscan.apple.com/content/catalogs/others/index-10.15seed-10.15-10.14-10.13-10.12-10.11-10.10-10.9-mountainlion-lion-snowleopard-
leopard.merged-1.sucatalog.gz, NSErrorFailingURLKey=https://swscan.apple.com/content/catalogs/others/
index-10.15seed-10.15-10.14-10.13-10.12-10.11-10.10-10.9-mountainlion-lion-snowleopard-leopard.merged-1.sucatalog.gz,
_kCFStreamErrorCodeKey=50}
2019-07-27 10:05:45+02 Demo-Mac softwareupdated[570]: SUScan: Scan for client pid 570 (/System/Library/CoreServices/Software
Update.app/Contents/Resources/softwareupdated)
2019-07-27 10:05:45+02 Demo-Mac softwareupdated[570]: SUScan: Using catalog https://swscan.apple.com/content/catalogs/others/
index-10.15seed-10.15-10.14-10.13-10.12-10.11-10.10-10.9-mountainlion-lion-snowleopard-leopard.merged-1.sucatalog.gz
2019-07-27 10:05:52+02 Demo-Mac softwareupdated[570]: SUScan: Elapsed scan time = 7.4
2019-07-27 10:26:26+02 Demo-Mac softwareupdated[570]: SUScan: Scan for client pid 570 (/System/Library/CoreServices/Software
Update.app/Contents/Resources/softwareupdated)
2019-07-27 10:26:26+02 Demo-Mac softwareupdated[570]: SUScan: Using catalog https://swscan.apple.com/content/catalogs/others/
index-10.15seed-10.15-10.14-10.13-10.12-10.11-10.10-10.9-mountainlion-lion-snowleopard-leopard.merged-1.sucatalog.gz
2019-07-27 10:26:31+02 Demo-Mac softwareupdated[570]: SUScan: Elapsed scan time = 5.1
2019-07-27 13:42:14+02 Demo-Mac softwareupdated[570]: SUScan: Scan for client pid 570 (/System/Library/CoreServices/Software
Update.app/Contents/Resources/softwareupdated)
2019-07-27 13:42:15+02 Demo-Mac softwareupdated[570]: SUScan: Using catalog https://swscan.apple.com/content/catalogs/others/
index-10.15seed-10.15-10.14-10.13-10.12-10.11-10.10-10.9-mountainlion-lion-snowleopard-leopard.merged-1.sucatalog.gz
2019-07-27 13:42:26+02 Demo-Mac softwareupdated[570]: SUScan: Elapsed scan time = 11.3
2019-07-27 22:37:56+02 Demo-Mac softwareupdated[643]: SUScan: Scan for client pid 643 (/System/Library/CoreServices/Software
Update.app/Contents/Resources/softwareupdated)
2019-07-27 22:37:57+02 Demo-Mac softwareupdated[643]: SUScan: Using catalog https://swscan.apple.com/content/catalogs/others/
index-10.15seed-10.15-10.14-10.13-10.12-10.11-10.10-10.9-mountainlion-lion-snowleopard-leopard.merged-1.sucatalog.gz
2019-07-27 22:38:02+02 Demo-Mac softwareupdated[643]: SUScan: Elapsed scan time = 5.5
2019-07-27 23:35:41+02 Demo-Mac softwareupdated[577]: SUScan: Scan for client pid 577 (/System/Library/CoreServices/Software
Update.app/Contents/Resources/softwareupdated)
2019-07-27 23:35:47+02 Demo-Mac softwareupdated[577]: SUScan: Using catalog https://swscan.apple.com/content/catalogs/others/
index-10.15seed-10.15-10.14-10.13-10.12-10.11-10.10-10.9-mountainlion-lion-snowleopard-leopard.merged-1.sucatalog.gz
2019-07-27 23:35:53+02 Demo-Mac softwareupdated[577]: SUScan: Elapsed scan time = 12.6
2019-07-28 04:07:04+02 Demo-Mac softwareupdated[577]: SUScan: Scan for client pid 577 (/System/Library/CoreServices/Software
Update.app/Contents/Resources/softwareupdated)
2019-07-28 04:07:04+02 Demo-Mac softwareupdated[577]: SUScan: Using catalog https://swscan.apple.com/content/catalogs/others/
```

Event sources and types

On the endpoints

- Outputs
  - OS log facility

OS log facilities -

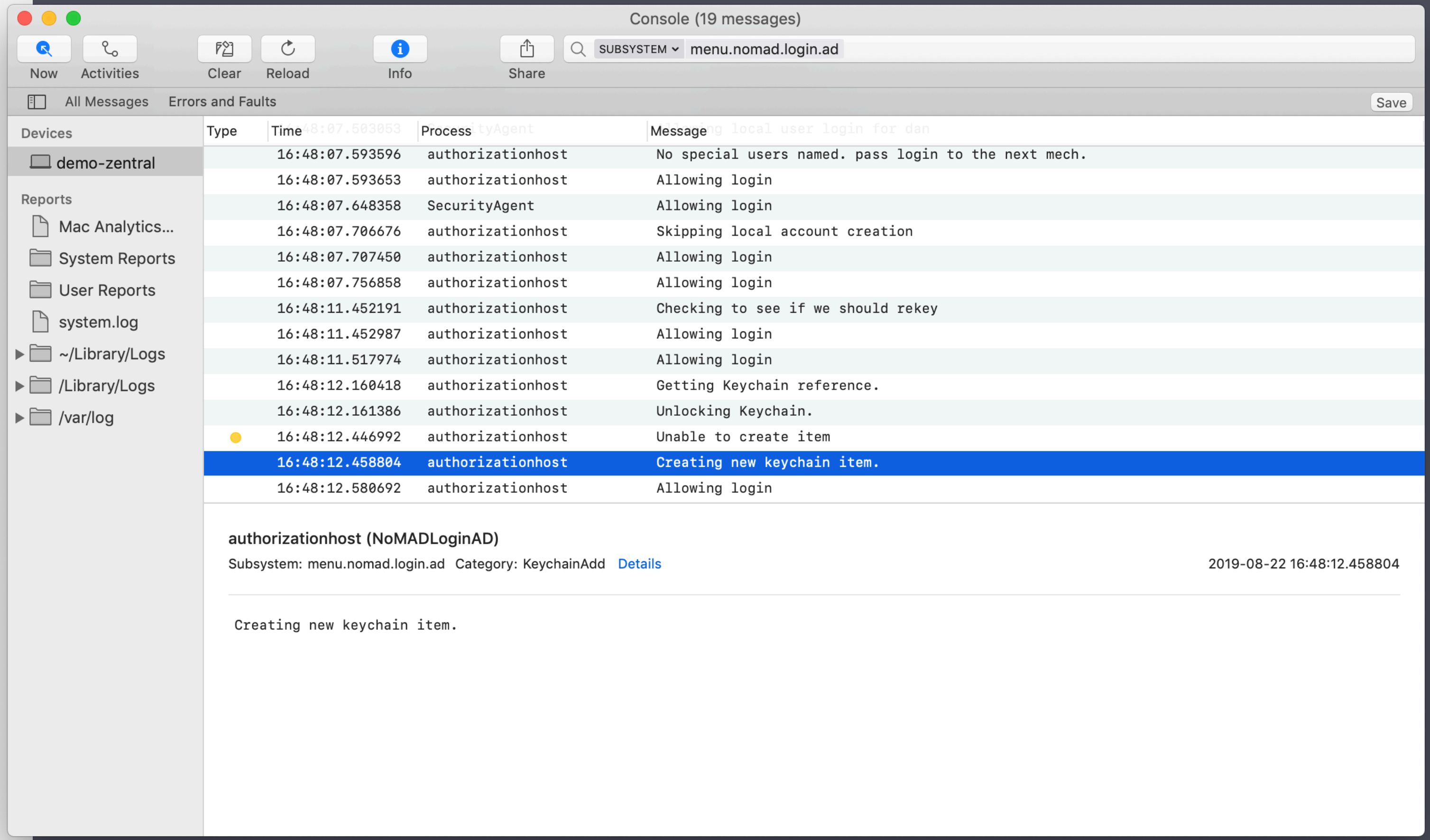
for OS and well behaved / integrated apps

- Apple Unified Logging
  - More structure
  - JSON output possible
  - Configurable persistence
- Syslog *(old in macOS)*

Event sources and types

On the endpoints

- Outputs
  - Unified Logging



```
Type  Time             Process            Message
      16:48:07.593596  authorizationhost  No special users named. pass login to the next mech.
      16:48:07.593653  authorizationhost  Allowing login
      16:48:07.648358  SecurityAgent      Allowing login
      16:48:07.706676  authorizationhost  Skipping local account creation
      16:48:07.707450  authorizationhost  Allowing login
      16:48:07.756858  authorizationhost  Allowing login
      16:48:11.452191  authorizationhost  Checking to see if we should rekey
      16:48:11.452987  authorizationhost  Allowing login
      16:48:11.517974  authorizationhost  Allowing login
      16:48:12.160418  authorizationhost  Getting Keychain reference.
      16:48:12.161386  authorizationhost  Unlocking Keychain.
  ●   16:48:12.446992  authorizationhost  Unable to create item
      16:48:12.458804  authorizationhost  Creating new keychain item.
      16:48:12.580692  authorizationhost  Allowing login
```

authorizationhost (NoMADLoginAD)

Subsystem: menu.nomad.login.ad Category: KeychainAdd Details 2019-08-22 16:48:12.458804

```
Creating new keychain item.
```

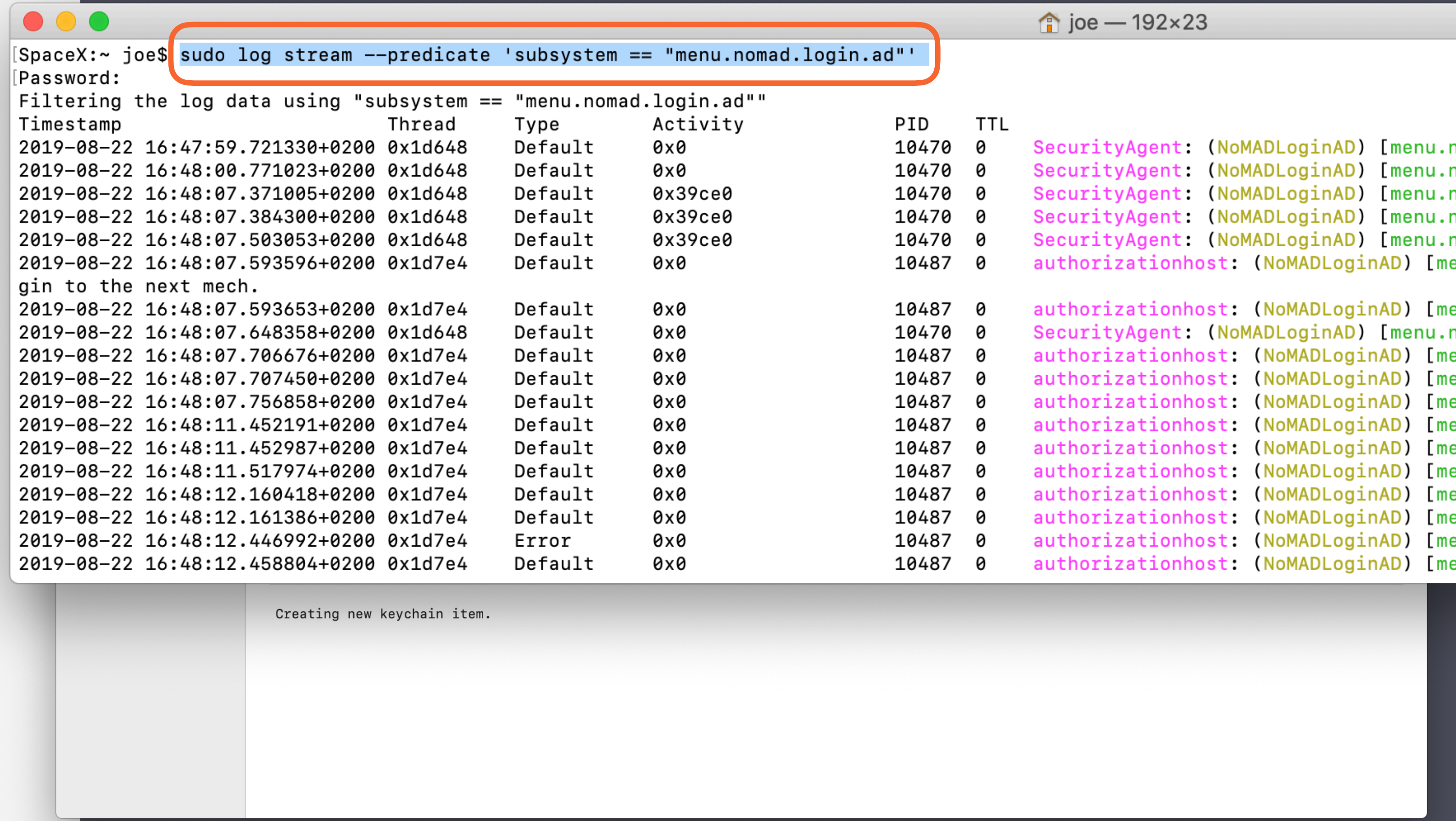
In-memory or persist into **.tracev3** files

zentral.pro

Event sources and types

On the endpoints

- Outputs
  - Unified Logging



```
SpaceX:~ joe$ sudo log stream --predicate 'subsystem == "menu.nomad.login.ad"'
Password:
Filtering the log data using "subsystem == "menu.nomad.login.ad""
Timestamp                       Thread     Type        Activity             PID    TTL
2019-08-22 16:47:59.721330+0200 0x1d648    Default     0x0                  10470  0    SecurityAgent: (NoMADLoginAD) [menu.
2019-08-22 16:48:00.771023+0200 0x1d648    Default     0x0                  10470  0    SecurityAgent: (NoMADLoginAD) [menu.
2019-08-22 16:48:07.371005+0200 0x1d648    Default     0x39ce0              10470  0    SecurityAgent: (NoMADLoginAD) [menu.
2019-08-22 16:48:07.384300+0200 0x1d648    Default     0x39ce0              10470  0    SecurityAgent: (NoMADLoginAD) [menu.
2019-08-22 16:48:07.503053+0200 0x1d648    Default     0x39ce0              10470  0    SecurityAgent: (NoMADLoginAD) [menu.
2019-08-22 16:48:07.593596+0200 0x1d7e4    Default     0x0                  10487  0    authorizationhost: (NoMADLoginAD) [me
gin to the next mech.
2019-08-22 16:48:07.593653+0200 0x1d7e4    Default     0x0                  10487  0    authorizationhost: (NoMADLoginAD) [me
2019-08-22 16:48:07.648358+0200 0x1d648    Default     0x0                  10470  0    SecurityAgent: (NoMADLoginAD) [menu.
2019-08-22 16:48:07.706676+0200 0x1d7e4    Default     0x0                  10487  0    authorizationhost: (NoMADLoginAD) [me
2019-08-22 16:48:07.707450+0200 0x1d7e4    Default     0x0                  10487  0    authorizationhost: (NoMADLoginAD) [me
2019-08-22 16:48:07.756858+0200 0x1d7e4    Default     0x0                  10487  0    authorizationhost: (NoMADLoginAD) [me
2019-08-22 16:48:11.452191+0200 0x1d7e4    Default     0x0                  10487  0    authorizationhost: (NoMADLoginAD) [me
2019-08-22 16:48:11.452987+0200 0x1d7e4    Default     0x0                  10487  0    authorizationhost: (NoMADLoginAD) [me
2019-08-22 16:48:11.517974+0200 0x1d7e4    Default     0x0                  10487  0    authorizationhost: (NoMADLoginAD) [me
2019-08-22 16:48:12.160418+0200 0x1d7e4    Default     0x0                  10487  0    authorizationhost: (NoMADLoginAD) [me
2019-08-22 16:48:12.161386+0200 0x1d7e4    Default     0x0                  10487  0    authorizationhost: (NoMADLoginAD) [me
2019-08-22 16:48:12.446992+0200 0x1d7e4    Error       0x0                  10487  0    authorizationhost: (NoMADLoginAD) [me
2019-08-22 16:48:12.458804+0200 0x1d7e4    Default     0x0                  10487  0    authorizationhost: (NoMADLoginAD) [me
```

```
Creating new keychain item.
```

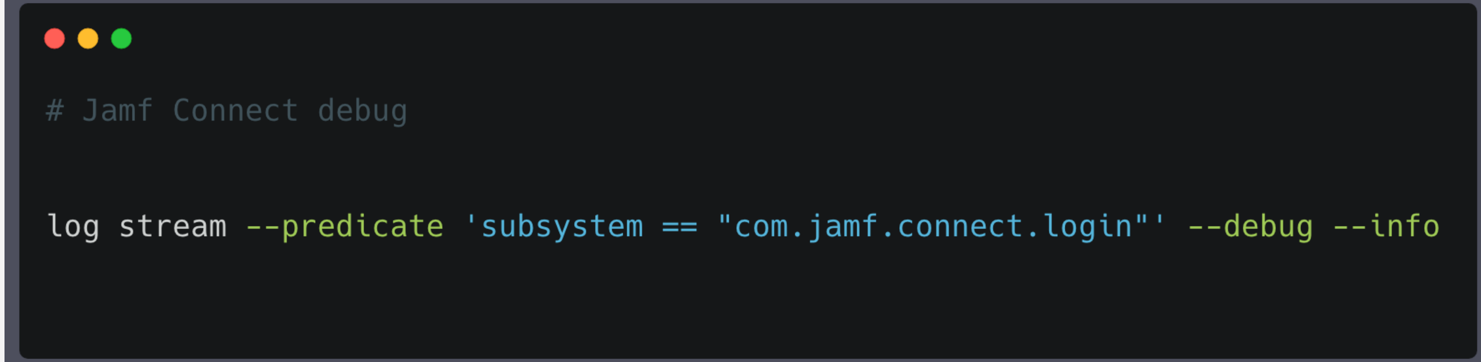
In-memory or persist into **.tracev3** files

zentral.pro

Event sources and types

On the endpoints

- Outputs
  - Unified Logging



```
# Jamf Connect debug

log stream --predicate 'subsystem == "com.jamf.connect.login"' --debug --info
```

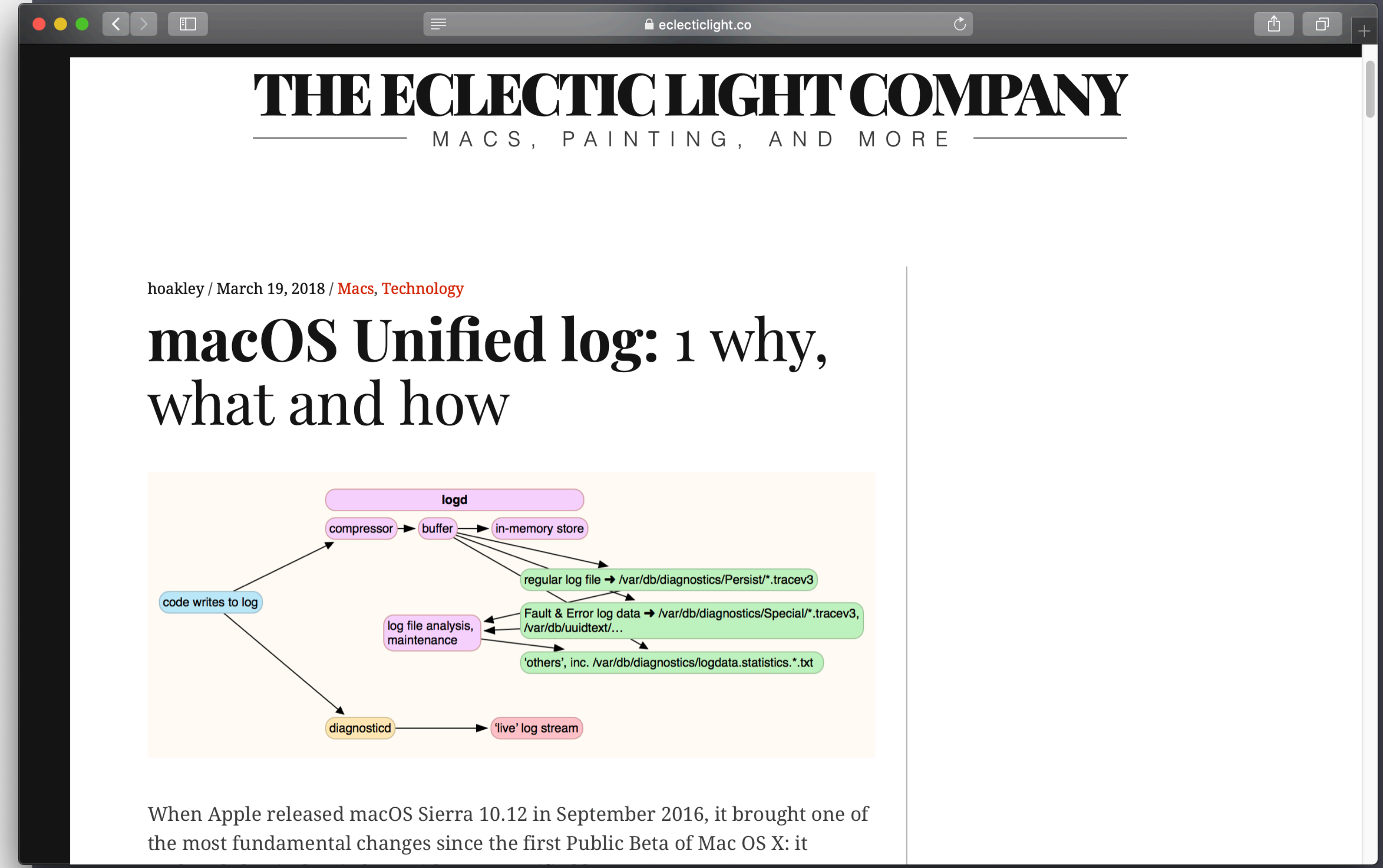
`--predicate`	Filter element *(subsystem type)*
`--debug`	Details depth
`--style`	Formatting *(json)*

Event sources and types

On the endpoints

- Outputs
  - Unified Logging

https://eclecticlight.co/2018/03/19/macos-unified-log-1-why-what-and-how/



THE ECLECTIC LIGHT COMPANY

MACS, PAINTING, AND MORE

hoakley / March 19, 2018 / Macs, Technology

macOS Unified log: 1 why, what and how

logd
compressor
buffer
in-memory store
code writes to log
regular log file ➜ /var/db/diagnostics/Persist/*.tracev3
Fault & Error log data ➜ /var/db/diagnostics/Special/*.tracev3, /var/db/uuidtext/…
log file analysis, maintenance
'others', inc. /var/db/diagnostics/logdata.statistics.*.txt
diagnosticd
'live' log stream

When Apple released macOS Sierra 10.12 in September 2016, it brought one of the most fundamental changes since the first Public Beta of Mac OS X: it

Howard Oakley @ Electriclight Company

Event sources and types

On the endpoints

- Outputs
  - Custom

- JSON payload posted on a HTTPS endpoint *(Osquery, Santa,…)*
- Publish to Kafka *(Osquery)*
- Other custom variants…

Event sources and types

Server / Cloud

- Sources

Identity Provider

- Sign-ins / Sign-in errors *(AzureAD, Okta, ...)*

Inventory

- Computer check-in *(Jamf Pro, WorkspaceOne, ...)*
- Group changes *(SimpleMDM, Jamf Pro, ...)*

MDM *(SaaS, open source MDM)*

- Configuration profile pushed
- Device Enrollments

Security providers

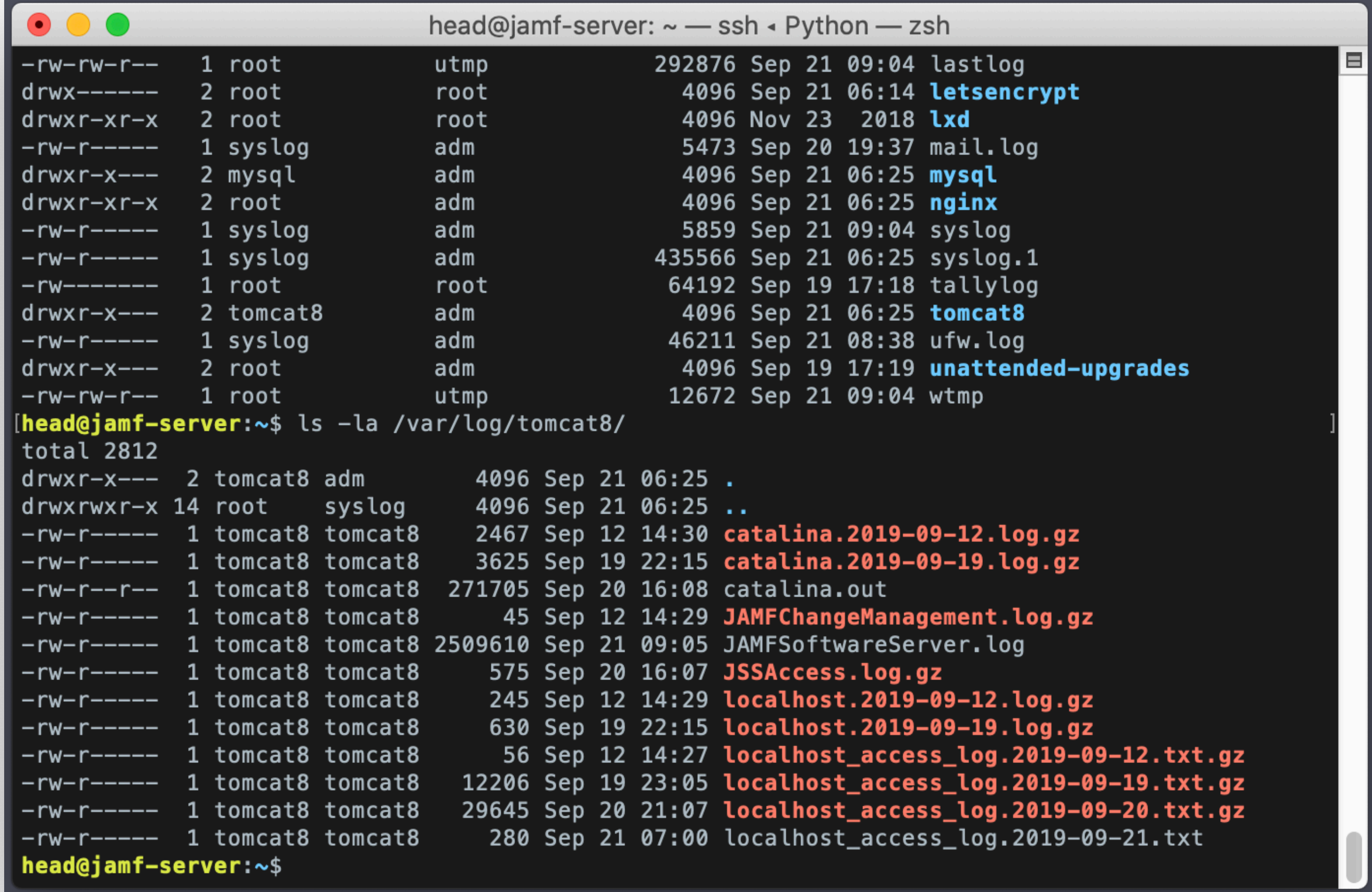
- Malware detected/removed

  (Microsoft Defender ATP, Malwarebytes)

Event sources and types

Server / Cloud

- Outputs

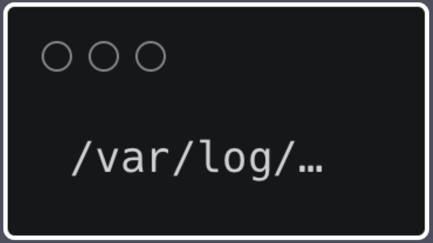


```
-rw-rw-r--   1 root           utmp           292876 Sep 21 09:04 lastlog
drwx------   2 root           root             4096 Sep 21 06:14 letsencrypt
drwxr-xr-x   2 root           root             4096 Nov 23  2018 lxd
-rw-r-----   1 syslog         adm              5473 Sep 20 19:37 mail.log
drwxr-x---   2 mysql          adm              4096 Sep 21 06:25 mysql
drwxr-xr-x   2 root           adm              4096 Sep 21 06:25 nginx
-rw-r-----   1 syslog         adm              5859 Sep 21 09:04 syslog
-rw-r-----   1 syslog         adm            435566 Sep 21 06:25 syslog.1
-rw-------   1 root           root            64192 Sep 19 17:18 tallylog
drwxr-x---   2 tomcat8        adm              4096 Sep 21 06:25 tomcat8
-rw-r-----   1 syslog         adm             46211 Sep 21 08:38 ufw.log
drwxr-x---   2 root           adm              4096 Sep 19 17:19 unattended-upgrades
-rw-rw-r--   1 root           utmp            12672 Sep 21 09:04 wtmp
[head@jamf-server:~$ ls -la /var/log/tomcat8/
total 2812
drwxr-x---  2 tomcat8 adm        4096 Sep 21 06:25 .
drwxrwxr-x 14 root    syslog     4096 Sep 21 06:25 ..
-rw-r-----  1 tomcat8 tomcat8    2467 Sep 12 14:30 catalina.2019-09-12.log.gz
-rw-r-----  1 tomcat8 tomcat8    3625 Sep 19 22:15 catalina.2019-09-19.log.gz
-rw-r--r--  1 tomcat8 tomcat8  271705 Sep 20 16:08 catalina.out
-rw-r-----  1 tomcat8 tomcat8      45 Sep 12 14:29 JAMFChangeManagement.log.gz
-rw-r-----  1 tomcat8 tomcat8 2509610 Sep 21 09:05 JAMFSoftwareServer.log
-rw-r-----  1 tomcat8 tomcat8     575 Sep 20 16:07 JSSAccess.log.gz
-rw-r-----  1 tomcat8 tomcat8     245 Sep 12 14:29 localhost.2019-09-12.log.gz
-rw-r-----  1 tomcat8 tomcat8     630 Sep 19 22:15 localhost.2019-09-19.log.gz
-rw-r-----  1 tomcat8 tomcat8      56 Sep 12 14:27 localhost_access_log.2019-09-12.txt.gz
-rw-r-----  1 tomcat8 tomcat8   12206 Sep 19 23:05 localhost_access_log.2019-09-19.txt.gz
-rw-r-----  1 tomcat8 tomcat8   29645 Sep 20 21:07 localhost_access_log.2019-09-20.txt.gz
-rw-r-----  1 tomcat8 tomcat8     280 Sep 21 07:00 localhost_access_log.2019-09-21.txt
head@jamf-server:~$
```

Event sources and types

Server / Cloud

▸ Outputs



```
/var/log/…
```

- File based - for most of the logs
  - Text data in files *(rotated)*
  - Log archives
- Service logs *(systemd / journalctl)*

Event sources and types

Server / Cloud

▸ Outputs

- API *(Jamf Pro, Microsoft Graph SecurityAPI)*
- Webhooks *(Jamf Pro, Okta, …)*
- Files on a server

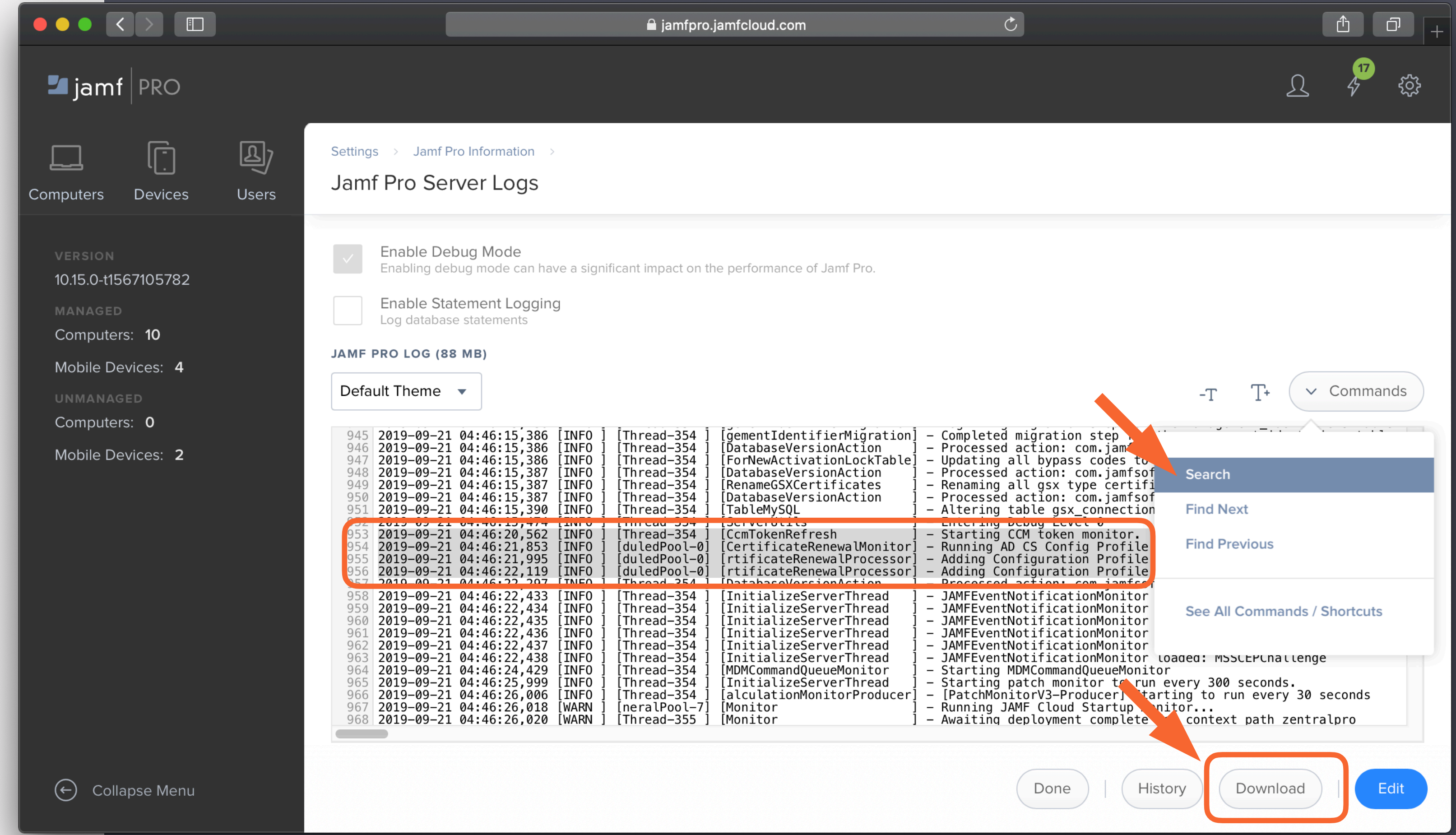
  (i.e.Jamf Pro in custom deployment)
- Blobs on a storage service
- GUI + manual download
- Events in a Message Broker

  (Azure Event Hubs)

Event sources and types

Server / Cloud

- Outputs
  - Jamf Pro



Jamf Pro Server Logs

VERSION
10.15.0-t1567105782

MANAGED
Computers: 10
Mobile Devices: 4

UNMANAGED
Computers: 0
Mobile Devices: 2

☑ Enable Debug Mode
Enabling debug mode can have a significant impact on the performance of Jamf Pro.

□ Enable Statement Logging
Log database statements

JAMF PRO LOG (88 MB)

```
2019-09-21 04:46:15,386 [INFO ] [Thread-354 ] [gementIdentifierMigration] - Completed migration step
2019-09-21 04:46:15,386 [INFO ] [Thread-354 ] [DatabaseVersionAction    ] - Processed action: com.jam
2019-09-21 04:46:15,386 [INFO ] [Thread-354 ] [ForNewActivationLockTable] - Updating all bypass codes to
2019-09-21 04:46:15,387 [INFO ] [Thread-354 ] [DatabaseVersionAction    ] - Processed action: com.jamfsof
2019-09-21 04:46:15,387 [INFO ] [Thread-354 ] [RenameGSXCertificates    ] - Renaming all gsx type certifi
2019-09-21 04:46:15,387 [INFO ] [Thread-354 ] [DatabaseVersionAction    ] - Processed action: com.jamfsof
2019-09-21 04:46:15,390 [INFO ] [Thread-354 ] [TableMySQL               ] - Altering table gsx_connection
2019-09-21 04:46:15,474 [INFO ] [Thread-354 ] [ServerUtils              ] - Entering Debug Level 0
2019-09-21 04:46:20,562 [INFO ] [Thread-354 ] [CcmTokenRefresh          ] - Starting CCM token monitor.
2019-09-21 04:46:21,853 [INFO ] [duledPool-0] [CertificateRenewalMonitor] - Running AD CS Config Profile
2019-09-21 04:46:21,995 [INFO ] [duledPool-0] [rtificateRenewalProcessor] - Adding Configuration Profile
2019-09-21 04:46:22,119 [INFO ] [duledPool-0] [rtificateRenewalProcessor] - Adding Configuration Profile
2019-09-21 04:46:22,297 [INFO ] [Thread-354 ] [DatabaseVersionAction    ] - Processed action: com.jamfso
2019-09-21 04:46:22,433 [INFO ] [Thread-354 ] [InitializeServerThread   ] - JAMFEventNotificationMonitor
2019-09-21 04:46:22,434 [INFO ] [Thread-354 ] [InitializeServerThread   ] - JAMFEventNotificationMonitor
2019-09-21 04:46:22,435 [INFO ] [Thread-354 ] [InitializeServerThread   ] - JAMFEventNotificationMonitor
2019-09-21 04:46:22,436 [INFO ] [Thread-354 ] [InitializeServerThread   ] - JAMFEventNotificationMonitor
2019-09-21 04:46:22,437 [INFO ] [Thread-354 ] [InitializeServerThread   ] - JAMFEventNotificationMonitor
2019-09-21 04:46:22,438 [INFO ] [Thread-354 ] [InitializeServerThread   ] - JAMFEventNotificationMonitor loaded: MSSCEPChallenge
2019-09-21 04:46:24,429 [INFO ] [Thread-354 ] [MDMCommandQueueMonitor   ] - Starting MDMCommandQueueMonitor
2019-09-21 04:46:25,999 [INFO ] [Thread-354 ] [InitializeServerThread   ] - Starting patch monitor to run every 300 seconds.
2019-09-21 04:46:26,006 [INFO ] [Thread-354 ] [alculationMonitorProducer] - [PatchMonitorV3-Producer] Starting to run every 30 seconds
2019-09-21 04:46:26,018 [WARN ] [neralPool-7] [Monitor                  ] - Running JAMF Cloud Startup Monitor...
2019-09-21 04:46:26,020 [WARN ] [Thread-355 ] [Monitor                  ] - Awaiting deployment complete     context path zentralpro
```

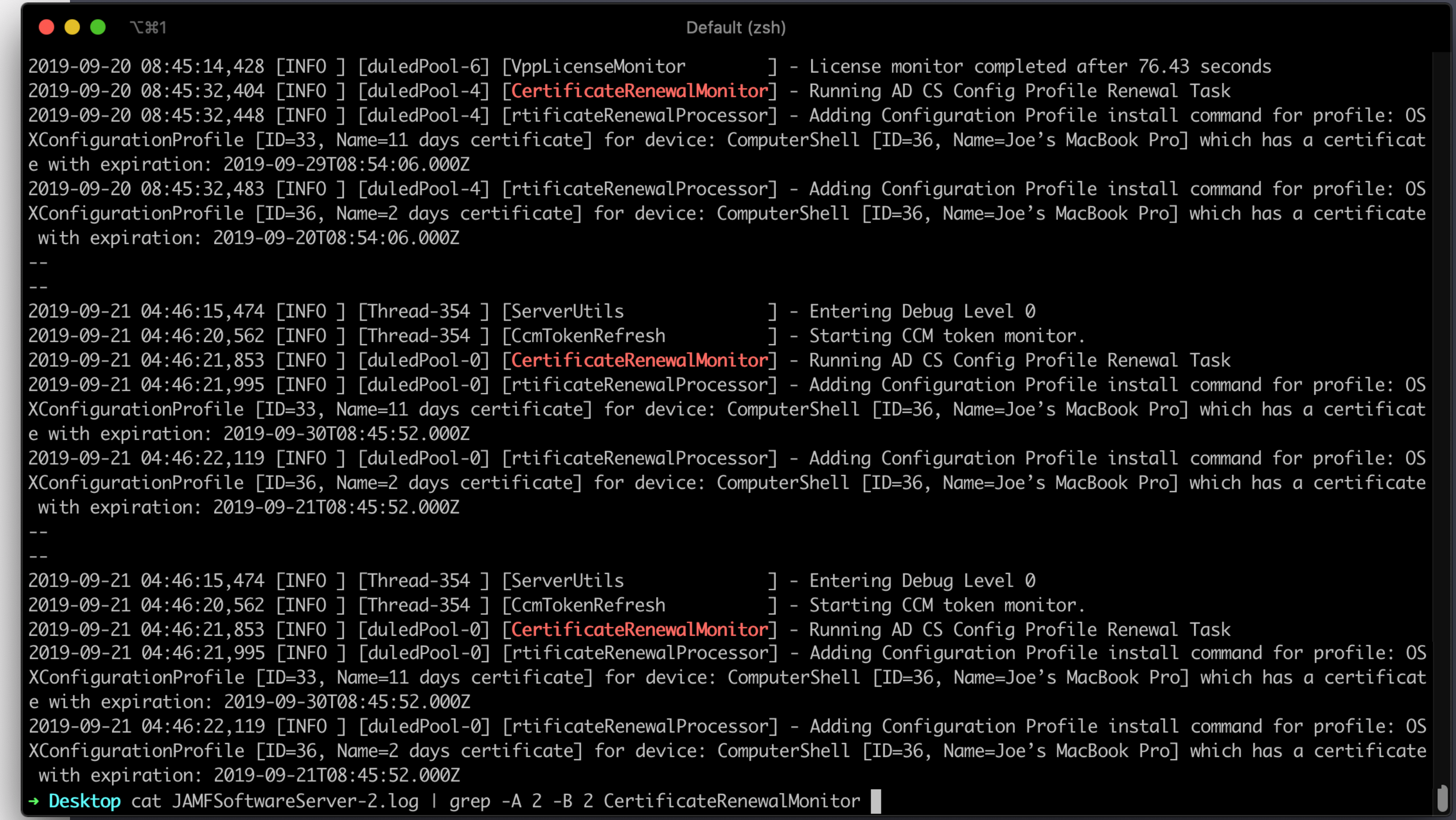
Search in browser or download

zentral.pro

Event sources and types

Server / Cloud

- Outputs
  - Jamf Pro



```
2019-09-20 08:45:14,428 [INFO ] [duledPool-6] [VppLicenseMonitor         ] - License monitor completed after 76.43 seconds
2019-09-20 08:45:32,404 [INFO ] [duledPool-4] [CertificateRenewalMonitor] - Running AD CS Config Profile Renewal Task
2019-09-20 08:45:32,448 [INFO ] [duledPool-4] [rtificateRenewalProcessor] - Adding Configuration Profile install command for profile: OS
XConfigurationProfile [ID=33, Name=11 days certificate] for device: ComputerShell [ID=36, Name=Joe’s MacBook Pro] which has a certificat
e with expiration: 2019-09-29T08:54:06.000Z
2019-09-20 08:45:32,483 [INFO ] [duledPool-4] [rtificateRenewalProcessor] - Adding Configuration Profile install command for profile: OS
XConfigurationProfile [ID=36, Name=2 days certificate] for device: ComputerShell [ID=36, Name=Joe’s MacBook Pro] which has a certificate
 with expiration: 2019-09-20T08:54:06.000Z
--
--
2019-09-21 04:46:15,474 [INFO ] [Thread-354 ] [ServerUtils               ] - Entering Debug Level 0
2019-09-21 04:46:20,562 [INFO ] [Thread-354 ] [CcmTokenRefresh           ] - Starting CCM token monitor.
2019-09-21 04:46:21,853 [INFO ] [duledPool-0] [CertificateRenewalMonitor] - Running AD CS Config Profile Renewal Task
2019-09-21 04:46:21,995 [INFO ] [duledPool-0] [rtificateRenewalProcessor] - Adding Configuration Profile install command for profile: OS
XConfigurationProfile [ID=33, Name=11 days certificate] for device: ComputerShell [ID=36, Name=Joe’s MacBook Pro] which has a certificat
e with expiration: 2019-09-30T08:45:52.000Z
2019-09-21 04:46:22,119 [INFO ] [duledPool-0] [rtificateRenewalProcessor] - Adding Configuration Profile install command for profile: OS
XConfigurationProfile [ID=36, Name=2 days certificate] for device: ComputerShell [ID=36, Name=Joe’s MacBook Pro] which has a certificate
 with expiration: 2019-09-21T08:45:52.000Z
--
--
2019-09-21 04:46:15,474 [INFO ] [Thread-354 ] [ServerUtils               ] - Entering Debug Level 0
2019-09-21 04:46:20,562 [INFO ] [Thread-354 ] [CcmTokenRefresh           ] - Starting CCM token monitor.
2019-09-21 04:46:21,853 [INFO ] [duledPool-0] [CertificateRenewalMonitor] - Running AD CS Config Profile Renewal Task
2019-09-21 04:46:21,995 [INFO ] [duledPool-0] [rtificateRenewalProcessor] - Adding Configuration Profile install command for profile: OS
XConfigurationProfile [ID=33, Name=11 days certificate] for device: ComputerShell [ID=36, Name=Joe’s MacBook Pro] which has a certificat
e with expiration: 2019-09-30T08:45:52.000Z
2019-09-21 04:46:22,119 [INFO ] [duledPool-0] [rtificateRenewalProcessor] - Adding Configuration Profile install command for profile: OS
XConfigurationProfile [ID=36, Name=2 days certificate] for device: ComputerShell [ID=36, Name=Joe’s MacBook Pro] which has a certificate
 with expiration: 2019-09-21T08:45:52.000Z
➜ Desktop cat JAMFSoftwareServer-2.log | grep -A 2 -B 2 CertificateRenewalMonitor
```

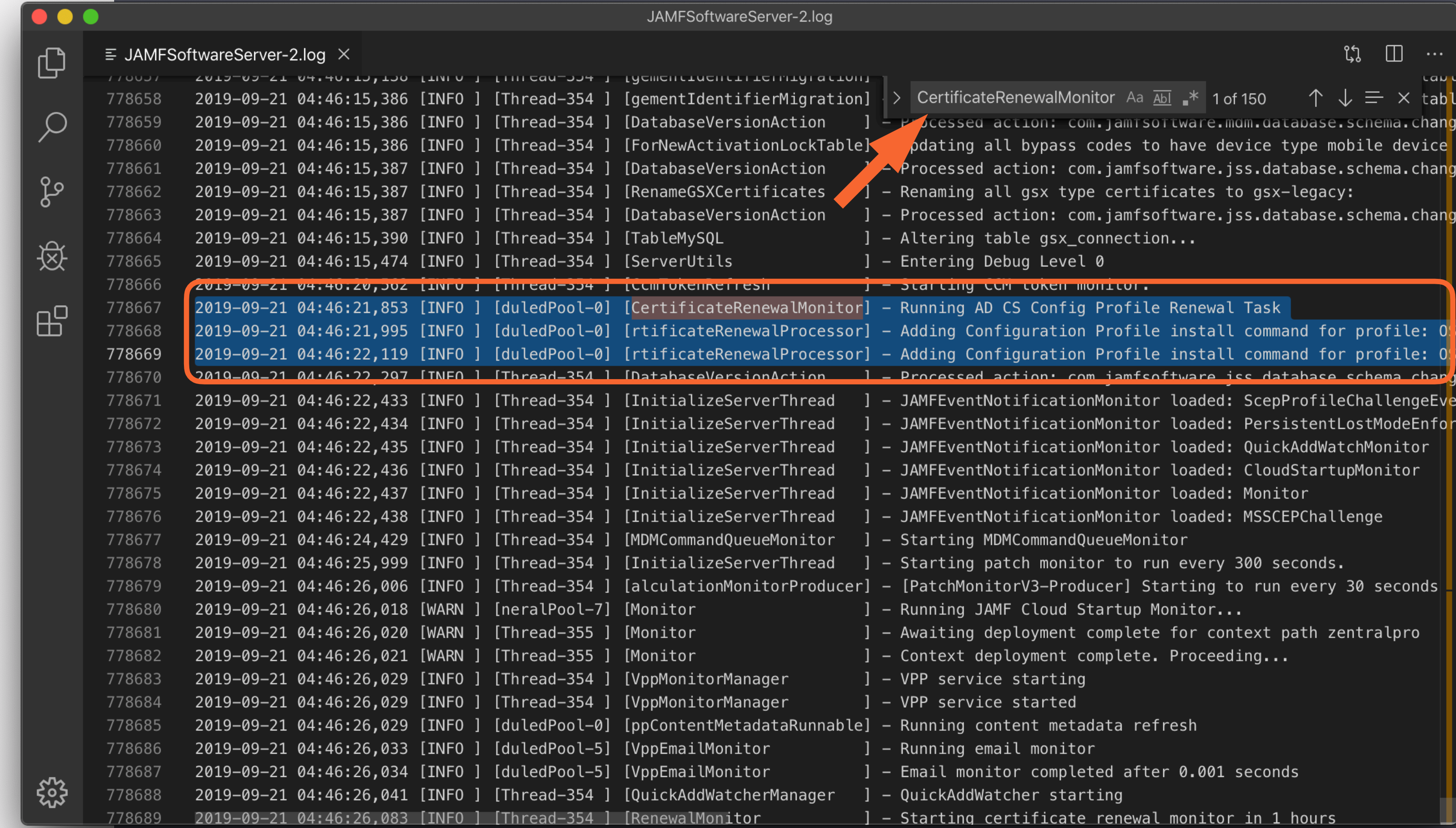
Search and grep *(keywords, errors, …)*

zentral.pro

Event sources and types

Server / Cloud

- Outputs
  - Jamf Pro



```
2019-09-21 04:46:15,158 [INFO ] [Thread-354 ] [gementIdentifierMigration]
2019-09-21 04:46:15,386 [INFO ] [Thread-354 ] [gementIdentifierMigration]
2019-09-21 04:46:15,386 [INFO ] [Thread-354 ] [DatabaseVersionAction    ] - Processed action: com.jamfsoftware.mdm.database.schema.chang
2019-09-21 04:46:15,386 [INFO ] [Thread-354 ] [ForNewActivationLockTable] - Updating all bypass codes to have device type mobile device
2019-09-21 04:46:15,387 [INFO ] [Thread-354 ] [DatabaseVersionAction    ] - Processed action: com.jamfsoftware.jss.database.schema.chang
2019-09-21 04:46:15,387 [INFO ] [Thread-354 ] [RenameGSXCertificates    ] - Renaming all gsx type certificates to gsx-legacy:
2019-09-21 04:46:15,387 [INFO ] [Thread-354 ] [DatabaseVersionAction    ] - Processed action: com.jamfsoftware.jss.database.schema.chang
2019-09-21 04:46:15,390 [INFO ] [Thread-354 ] [TableMySQL               ] - Altering table gsx_connection...
2019-09-21 04:46:15,474 [INFO ] [Thread-354 ] [ServerUtils              ] - Entering Debug Level 0
2019-09-21 04:46:20,362 [INFO ] [Thread-354 ] [CcmTokenRefresh          ] - Starting CCM token monitor.
2019-09-21 04:46:21,853 [INFO ] [duledPool-0] [CertificateRenewalMonitor] - Running AD CS Config Profile Renewal Task
2019-09-21 04:46:21,995 [INFO ] [duledPool-0] [rtificateRenewalProcessor] - Adding Configuration Profile install command for profile: O
2019-09-21 04:46:22,119 [INFO ] [duledPool-0] [rtificateRenewalProcessor] - Adding Configuration Profile install command for profile: O
2019-09-21 04:46:22,297 [INFO ] [Thread-354 ] [DatabaseVersionAction    ] - Processed action: com.jamfsoftware.jss.database.schema.chang
2019-09-21 04:46:22,433 [INFO ] [Thread-354 ] [InitializeServerThread   ] - JAMFEventNotificationMonitor loaded: ScepProfileChallengeEve
2019-09-21 04:46:22,434 [INFO ] [Thread-354 ] [InitializeServerThread   ] - JAMFEventNotificationMonitor loaded: PersistentLostModeEnfor
2019-09-21 04:46:22,435 [INFO ] [Thread-354 ] [InitializeServerThread   ] - JAMFEventNotificationMonitor loaded: QuickAddWatchMonitor
2019-09-21 04:46:22,436 [INFO ] [Thread-354 ] [InitializeServerThread   ] - JAMFEventNotificationMonitor loaded: CloudStartupMonitor
2019-09-21 04:46:22,437 [INFO ] [Thread-354 ] [InitializeServerThread   ] - JAMFEventNotificationMonitor loaded: Monitor
2019-09-21 04:46:22,438 [INFO ] [Thread-354 ] [InitializeServerThread   ] - JAMFEventNotificationMonitor loaded: MSSCEPChallenge
2019-09-21 04:46:24,429 [INFO ] [Thread-354 ] [MDMCommandQueueMonitor   ] - Starting MDMCommandQueueMonitor
2019-09-21 04:46:25,999 [INFO ] [Thread-354 ] [InitializeServerThread   ] - Starting patch monitor to run every 300 seconds.
2019-09-21 04:46:26,006 [INFO ] [Thread-354 ] [alculationMonitorProducer] - [PatchMonitorV3-Producer] Starting to run every 30 seconds
2019-09-21 04:46:26,018 [WARN ] [neralPool-7] [Monitor                  ] - Running JAMF Cloud Startup Monitor...
2019-09-21 04:46:26,020 [WARN ] [Thread-355 ] [Monitor                  ] - Awaiting deployment complete for context path zentralpro
2019-09-21 04:46:26,021 [WARN ] [Thread-355 ] [Monitor                  ] - Context deployment complete. Proceeding...
2019-09-21 04:46:26,029 [INFO ] [Thread-354 ] [VppMonitorManager        ] - VPP service starting
2019-09-21 04:46:26,029 [INFO ] [Thread-354 ] [VppMonitorManager        ] - VPP service started
2019-09-21 04:46:26,029 [INFO ] [duledPool-0] [ppContentMetadataRunnable] - Running content metadata refresh
2019-09-21 04:46:26,033 [INFO ] [duledPool-5] [VppEmailMonitor          ] - Running email monitor
2019-09-21 04:46:26,034 [INFO ] [duledPool-5] [VppEmailMonitor          ] - Email monitor completed after 0.001 seconds
2019-09-21 04:46:26,041 [INFO ] [Thread-354 ] [QuickAddWatcherManager   ] - QuickAddWatcher starting
2019-09-21 04:46:26,083 [INFO ] [Thread-354 ] [RenewalMonitor           ] - Starting certificate renewal monitor in 1 hours
```

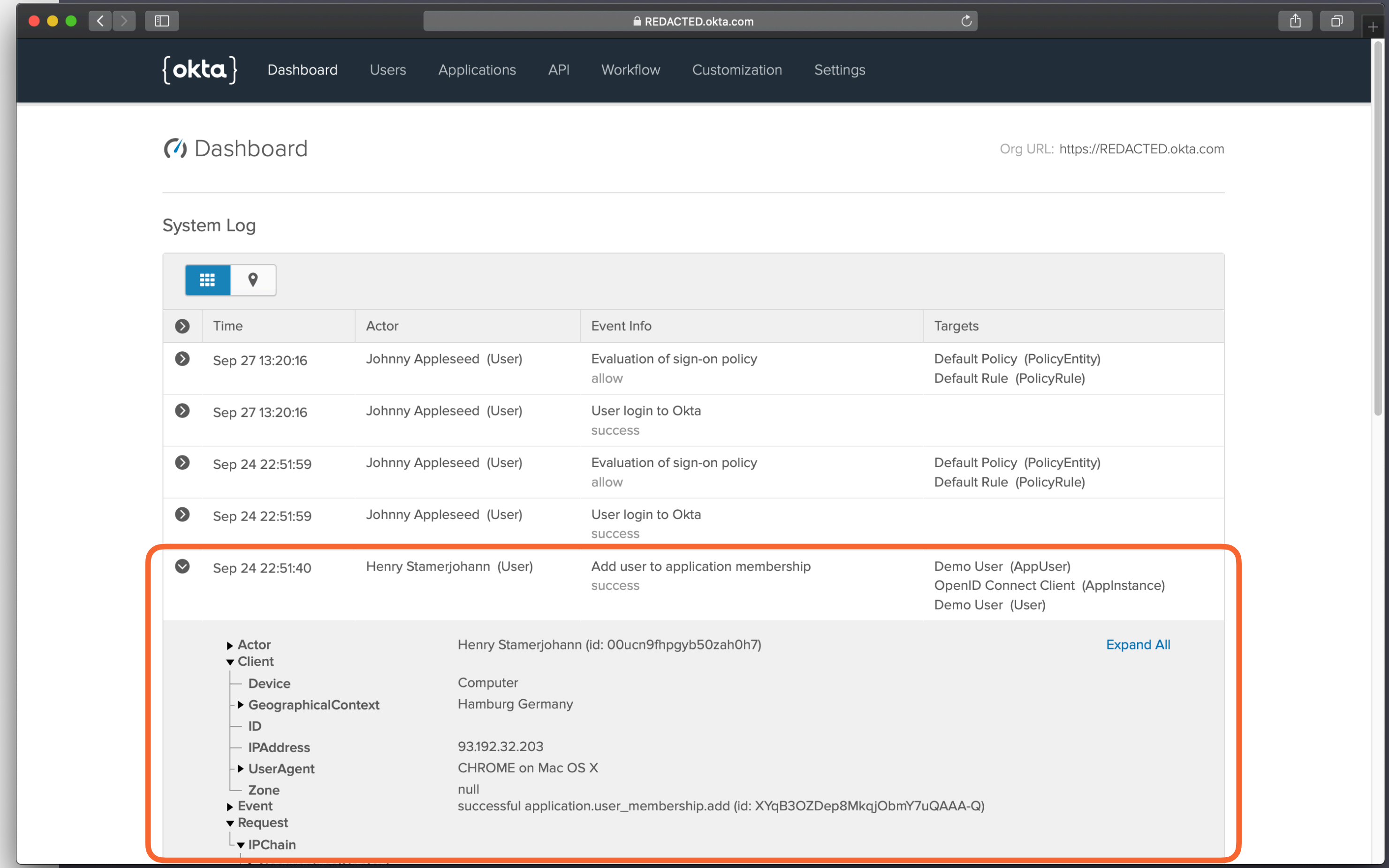
Search and grep *(keywords, errors, ...)*

zentral.pro

Event sources and types

Server / Cloud

- Outputs
  - IDP - Okta



REDACTED.okta.com

Dashboard

Org URL: https://REDACTED.okta.com

System Log

Time	Actor	Event Info	Targets
Sep 27 13:20:16	Johnny Appleseed (User)	Evaluation of sign-on policy allow	Default Policy (PolicyEntity) Default Rule (PolicyRule)
Sep 27 13:20:16	Johnny Appleseed (User)	User login to Okta success	
Sep 24 22:51:59	Johnny Appleseed (User)	Evaluation of sign-on policy allow	Default Policy (PolicyEntity) Default Rule (PolicyRule)
Sep 24 22:51:59	Johnny Appleseed (User)	User login to Okta success	
Sep 24 22:51:40	Henry Stamerjohann (User)	Add user to application membership success	Demo User (AppUser) OpenID Connect Client (AppInstance) Demo User (User)

```
▸ Actor                      Henry Stamerjohann (id: 00ucn9fhpgyb50zah0h7)             Expand All
▾ Client
  ├ Device                   Computer
  ├▸ GeographicalContext     Hamburg Germany
  ├ ID
  ├ IPAddress                93.192.32.203
  ├▸ UserAgent               CHROME on Mac OS X
  └ Zone                     null
▸ Event                      successful application.user_membership.add (id: XYqB3OZDep8MkqjObmY7uQAAA-Q)
▾ Request
  └▾ IPChain
```

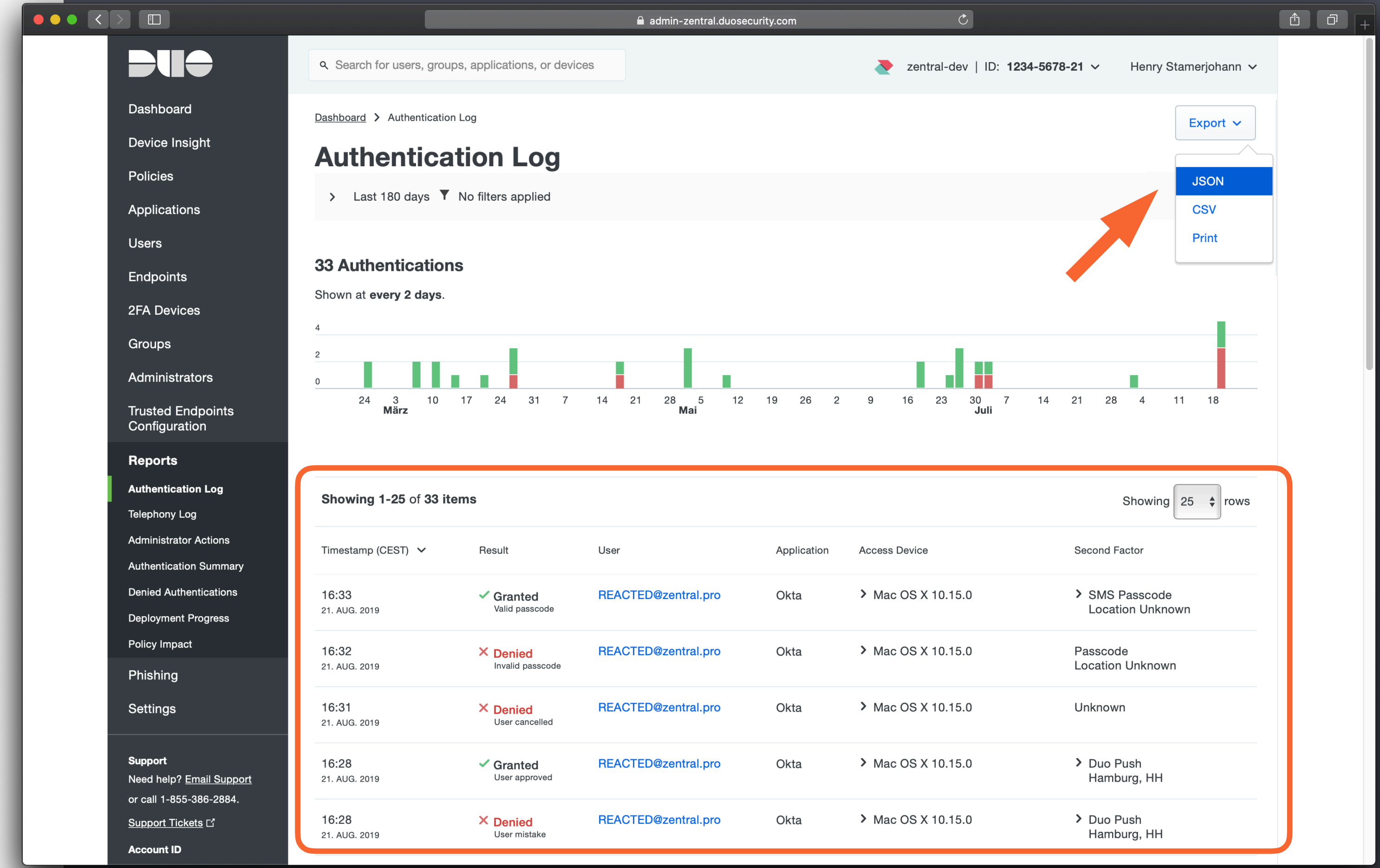
Event audit trail *(sign-ins, edits or changes)*

zentral.pro

Event sources and types

Server / Cloud

- Outputs
  - IDP - Duo



Authentication Log

Last 180 days No filters applied

33 Authentications

Shown at **every 2 days**.

Showing 1-25 of **33 items** Showing 25 rows

Timestamp (CEST)	Result	User	Application	Access Device	Second Factor
16:33 21. AUG. 2019	✓ Granted Valid passcode	REACTED@zentral.pro	Okta	Mac OS X 10.15.0	SMS Passcode Location Unknown
16:32 21. AUG. 2019	✕ Denied Invalid passcode	REACTED@zentral.pro	Okta	Mac OS X 10.15.0	Passcode Location Unknown
16:31 21. AUG. 2019	✕ Denied User cancelled	REACTED@zentral.pro	Okta	Mac OS X 10.15.0	Unknown
16:28 21. AUG. 2019	✓ Granted User approved	REACTED@zentral.pro	Okta	Mac OS X 10.15.0	Duo Push Hamburg, HH
16:28 21. AUG. 2019	✕ Denied User mistake	REACTED@zentral.pro	Okta	Mac OS X 10.15.0	Duo Push Hamburg, HH

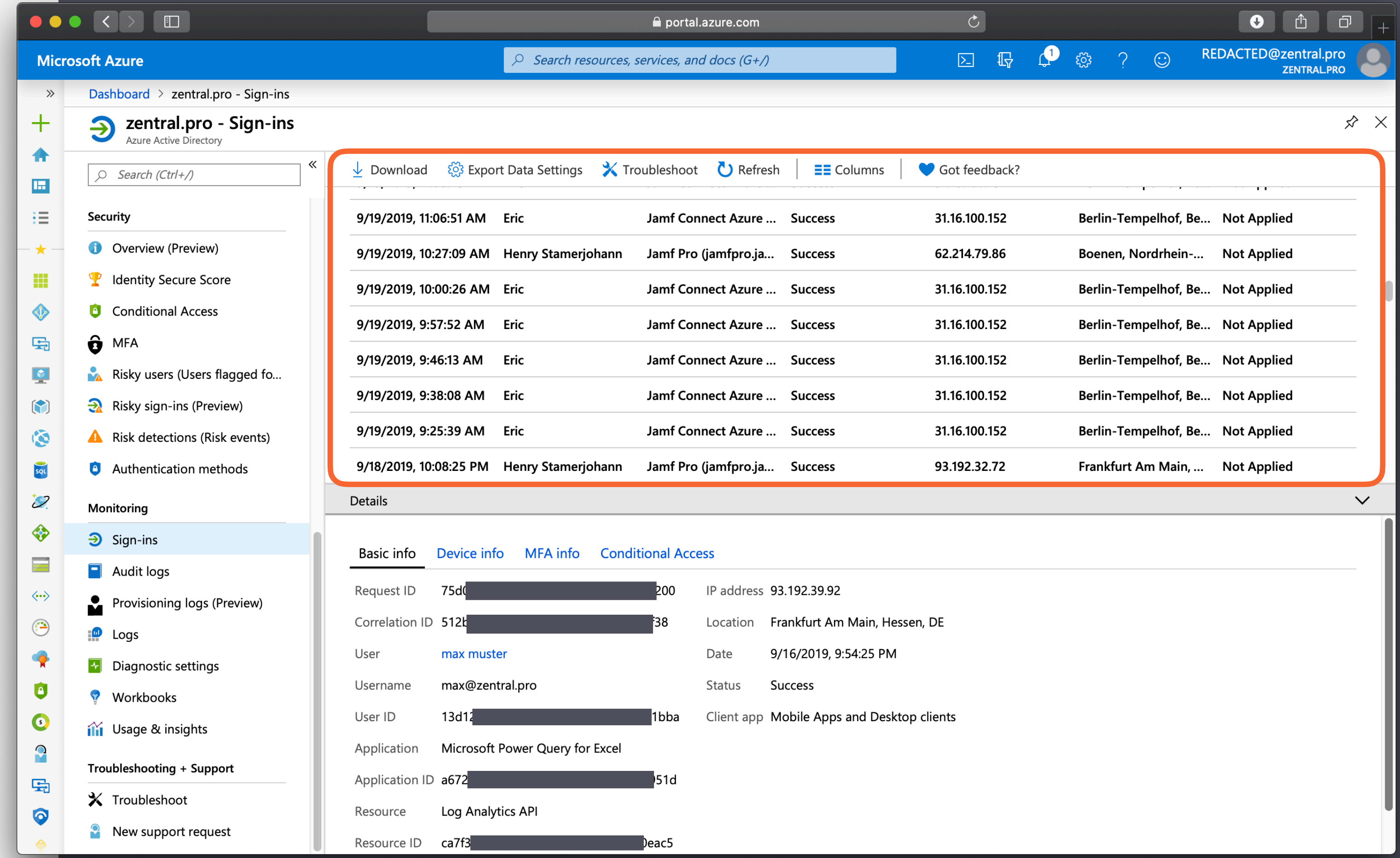
Authentications *(export json, csv)*

zentral.pro

Event sources and types

Server / Cloud

- Outputs
  - IDP - Azure AD



portal.azure.com
Microsoft Azure
Search resources, services, and docs (G+/)
REDACTED@zentral.pro
ZENTRAL.PRO
Dashboard > zentral.pro - Sign-ins

zentral.pro - Sign-ins
Azure Active Directory

9/19/2019, 11:06:51 AM	Eric	Jamf Connect Azure ...	Success	31.16.100.152	Berlin-Tempelhof, Be...	Not Applied
9/19/2019, 10:27:09 AM	Henry Stamerjohann	Jamf Pro (jamfpro.ja...	Success	62.214.79.86	Boenen, Nordrhein-...	Not Applied
9/19/2019, 10:00:26 AM	Eric	Jamf Connect Azure ...	Success	31.16.100.152	Berlin-Tempelhof, Be...	Not Applied
9/19/2019, 9:57:52 AM	Eric	Jamf Connect Azure ...	Success	31.16.100.152	Berlin-Tempelhof, Be...	Not Applied
9/19/2019, 9:46:13 AM	Eric	Jamf Connect Azure ...	Success	31.16.100.152	Berlin-Tempelhof, Be...	Not Applied
9/19/2019, 9:38:08 AM	Eric	Jamf Connect Azure ...	Success	31.16.100.152	Berlin-Tempelhof, Be...	Not Applied
9/19/2019, 9:25:39 AM	Eric	Jamf Connect Azure ...	Success	31.16.100.152	Berlin-Tempelhof, Be...	Not Applied
9/18/2019, 10:08:25 PM	Henry Stamerjohann	Jamf Pro (jamfpro.ja...	Success	93.192.32.72	Frankfurt Am Main, ...	Not Applied

Details

Basic info | Device info | MFA info | Conditional Access

Request ID	75d[redacted]200	IP address	93.192.39.92
Correlation ID	512[redacted]38	Location	Frankfurt Am Main, Hessen, DE
User	max muster	Date	9/16/2019, 9:54:25 PM
Username	max@zentral.pro	Status	Success
User ID	13d1[redacted]1bba	Client app	Mobile Apps and Desktop clients
Application	Microsoft Power Query for Excel		
Application ID	a672[redacted]51d		
Resource	Log Analytics API		
Resource ID	ca7f3[redacted]eac5		

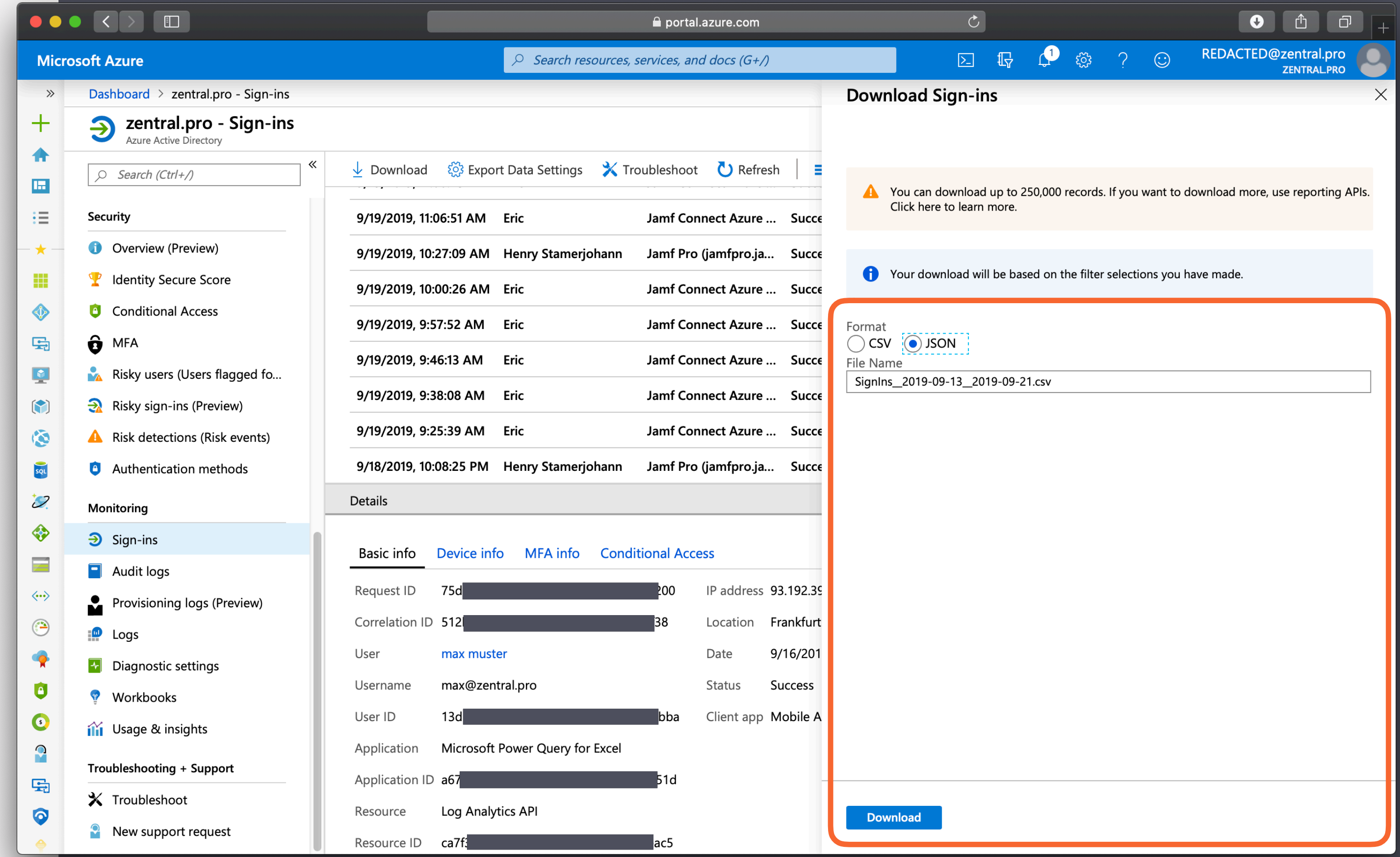
Sign-in Logs *(export json, csv)*

zentral.pro

Event sources and types

Server / Cloud

- Outputs
  - IDP - Azure AD



portal.azure.com

Microsoft Azure

Search resources, services, and docs (G+/)

REDACTED@zentral.pro
ZENTRAL.PRO

Dashboard > zentral.pro - Sign-ins

zentral.pro - Sign-ins
Azure Active Directory

Search (Ctrl+/)

Security
- Overview (Preview)
- Identity Secure Score
- Conditional Access
- MFA
- Risky users (Users flagged fo...
- Risky sign-ins (Preview)
- Risk detections (Risk events)
- Authentication methods

Monitoring
- Sign-ins
- Audit logs
- Provisioning logs (Preview)
- Logs
- Diagnostic settings
- Workbooks
- Usage & insights

Troubleshooting + Support
- Troubleshoot
- New support request

Download | Export Data Settings | Troubleshoot | Refresh

9/19/2019, 11:06:51 AM	Eric	Jamf Connect Azure ...	Succe
9/19/2019, 10:27:09 AM	Henry Stamerjohann	Jamf Pro (jamfpro.ja...	Succe
9/19/2019, 10:00:26 AM	Eric	Jamf Connect Azure ...	Succe
9/19/2019, 9:57:52 AM	Eric	Jamf Connect Azure ...	Succe
9/19/2019, 9:46:13 AM	Eric	Jamf Connect Azure ...	Succe
9/19/2019, 9:38:08 AM	Eric	Jamf Connect Azure ...	Succe
9/19/2019, 9:25:39 AM	Eric	Jamf Connect Azure ...	Succe
9/18/2019, 10:08:25 PM	Henry Stamerjohann	Jamf Pro (jamfpro.ja...	Succe

Details

Basic info | Device info | MFA info | Conditional Access

Request ID	75d[redacted]200	IP address	93.192.3!
Correlation ID	512[redacted]38	Location	Frankfurt
User	max muster	Date	9/16/201
Username	max@zentral.pro	Status	Success
User ID	13d[redacted]bba	Client app	Mobile A
Application	Microsoft Power Query for Excel		
Application ID	a67[redacted]51d		
Resource	Log Analytics API		
Resource ID	ca7f[redacted]ac5		

Download Sign-ins

You can download up to 250,000 records. If you want to download more, use reporting APIs. Click here to learn more.

Your download will be based on the filter selections you have made.

Format
○ CSV ● JSON

File Name
SignIns__2019-09-13__2019-09-21.csv

Download

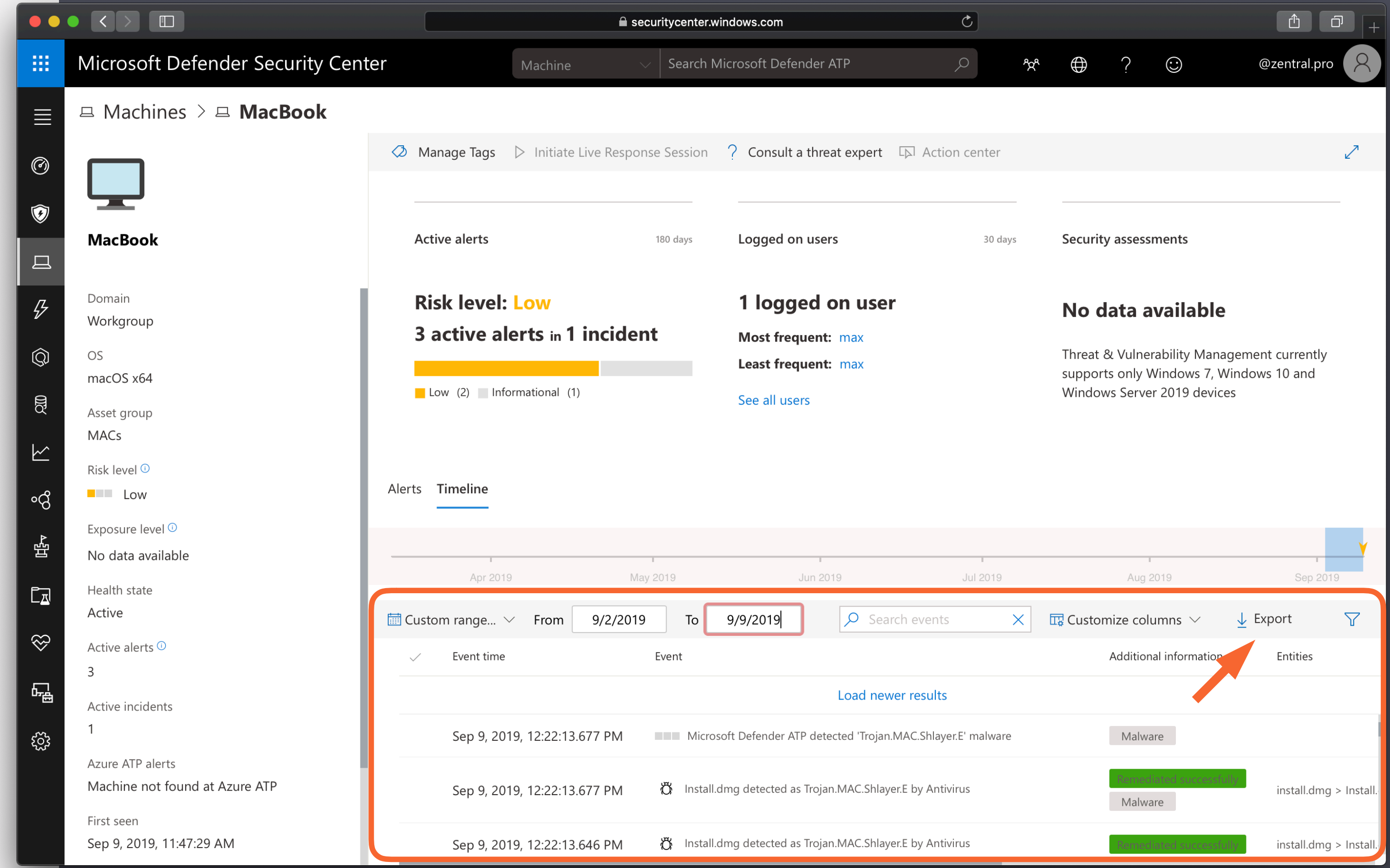
Sign-in Logs *(export json, csv)*

zentral.pro

Event sources and types

Server / Cloud

- Outputs
  - ATP Defender



securitycenter.windows.com

Microsoft Defender Security Center

Machine | Search Microsoft Defender ATP | @zentral.pro

Machines > MacBook

MacBook

Domain
Workgroup

OS
macOS x64

Asset group
MACs

Risk level
Low

Exposure level
No data available

Health state
Active

Active alerts
3

Active incidents
1

Azure ATP alerts
Machine not found at Azure ATP

First seen
Sep 9, 2019, 11:47:29 AM

Manage Tags | Initiate Live Response Session | Consult a threat expert | Action center

Active alerts — 180 days

Risk level: Low

3 active alerts in 1 incident

Low (2) Informational (1)

Logged on users — 30 days

1 logged on user

Most frequent: max

Least frequent: max

See all users

Security assessments

No data available

Threat & Vulnerability Management currently supports only Windows 7, Windows 10 and Windows Server 2019 devices

Alerts | Timeline

Custom range... From 9/2/2019 To 9/9/2019 | Search events | Customize columns | Export

Event time	Event	Additional information	Entities
	Load newer results		
Sep 9, 2019, 12:22:13.677 PM	Microsoft Defender ATP detected 'Trojan.MAC.Shlayer.E' malware	Malware	
Sep 9, 2019, 12:22:13.677 PM	Install.dmg detected as Trojan.MAC.Shlayer.E by Antivirus	Remediated successfully Malware	install.dmg > Install.
Sep 9, 2019, 12:22:13.646 PM	Install.dmg detected as Trojan.MAC.Shlayer.E by Antivirus	Remediated successfully	install.dmg > Install.

AV Activity / Remediation *(export csv)*

zentral.pro

Event sources and types

Server / Cloud

- Outputs
  - Post processing

- Build reports from CSV
- Analyze/process JSON
- Upload and repurpose event data
- Share with other Teams
- Store for Compliance *(Backups)*
- Use to get support from a Vendor

Ship and collect the events

Ship and collect the events

Problems / Issues

- Reality

- Many different sources
- Many different formats
- No single place where to look at events / search for events
- Too many events

Ship and collect the events

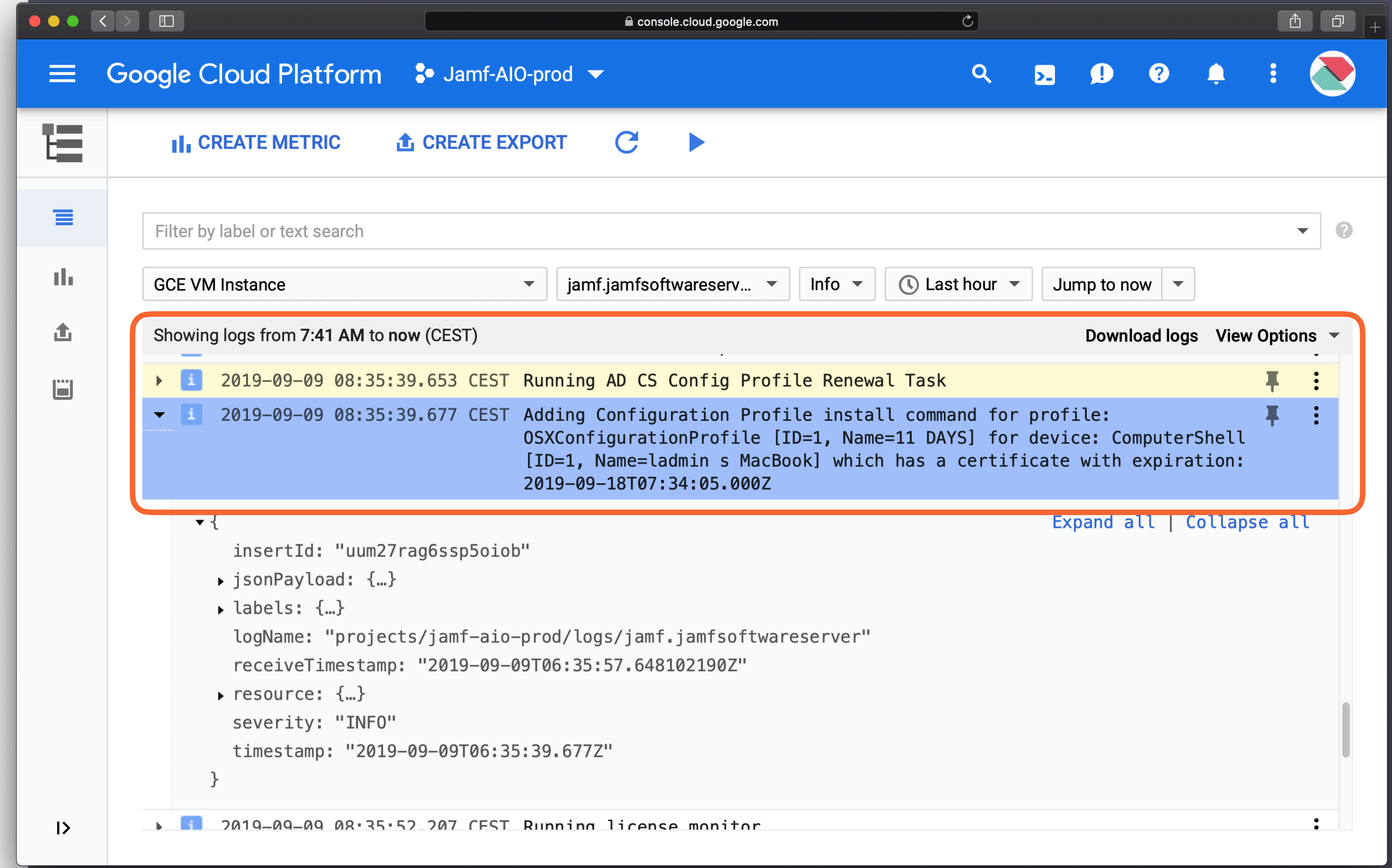
Existing Solutions

- Elastic Stack *(formerly ELK Stack)*
- Splunk
- Sumo Logic
- Stackdriver
- Zentral
- et.al

Ship and collect the events

Existing Solutions

- Log Facilities
  - Stackdriver Logging



Showing logs from 7:41 AM to now (CEST)

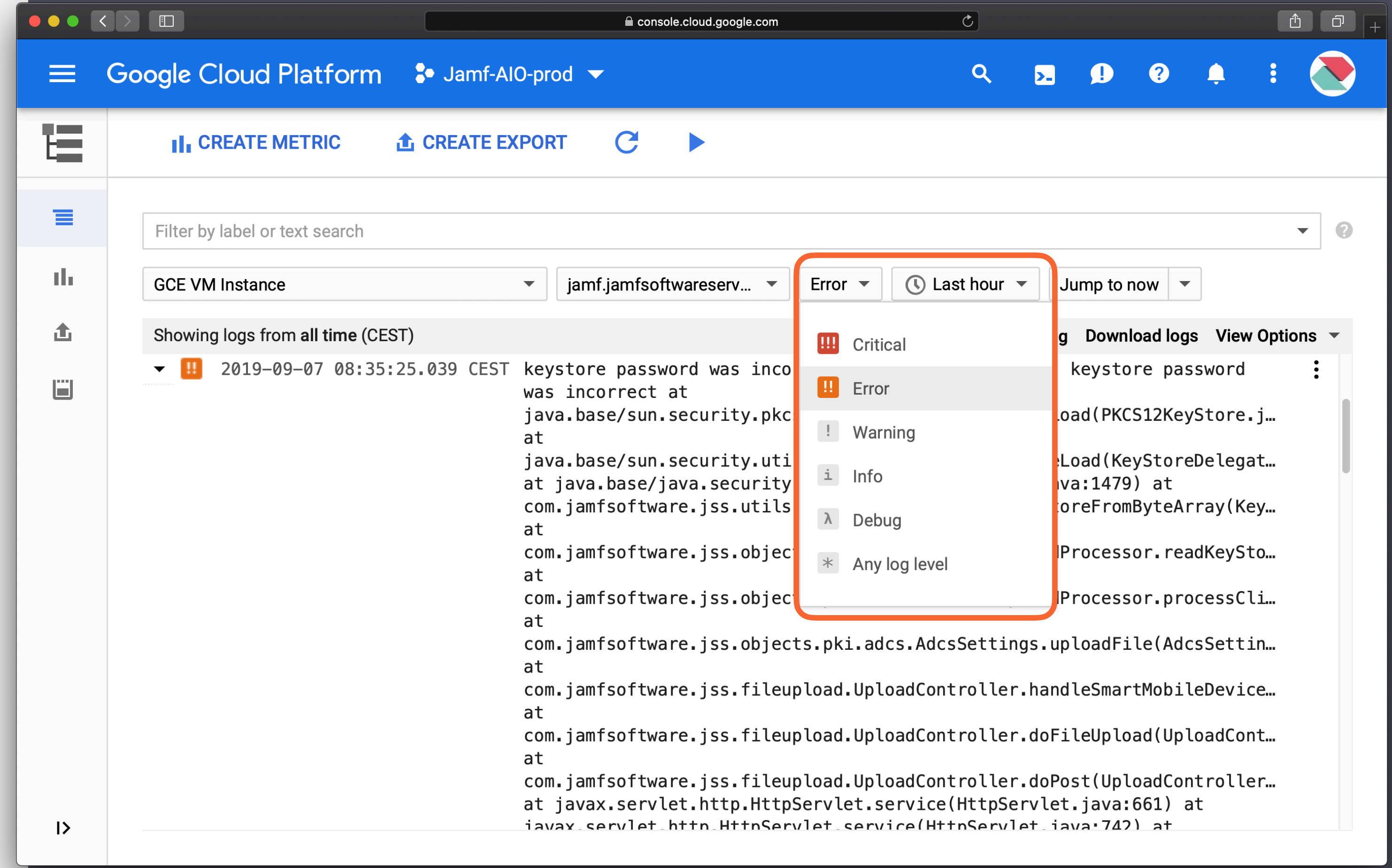
```
2019-09-09 08:35:39.653 CEST  Running AD CS Config Profile Renewal Task
2019-09-09 08:35:39.677 CEST  Adding Configuration Profile install command for profile:
                              OSXConfigurationProfile [ID=1, Name=11 DAYS] for device: ComputerShell
                              [ID=1, Name=ladmin s MacBook] which has a certificate with expiration:
                              2019-09-18T07:34:05.000Z
  {
    insertId: "uum27rag6ssp5oiob"
    jsonPayload: {…}
    labels: {…}
    logName: "projects/jamf-aio-prod/logs/jamf.jamfsoftwareserver"
    receiveTimestamp: "2019-09-09T06:35:57.648102190Z"
    resource: {…}
    severity: "INFO"
    timestamp: "2019-09-09T06:35:39.677Z"
  }
2019-09-09 08:35:52.207 CEST  Running license monitor
```

zentral.pro

Ship and collect the events

Existing Solutions

- Log Facilities
  - Stackdriver Logging



Showing logs from **all time** (CEST)

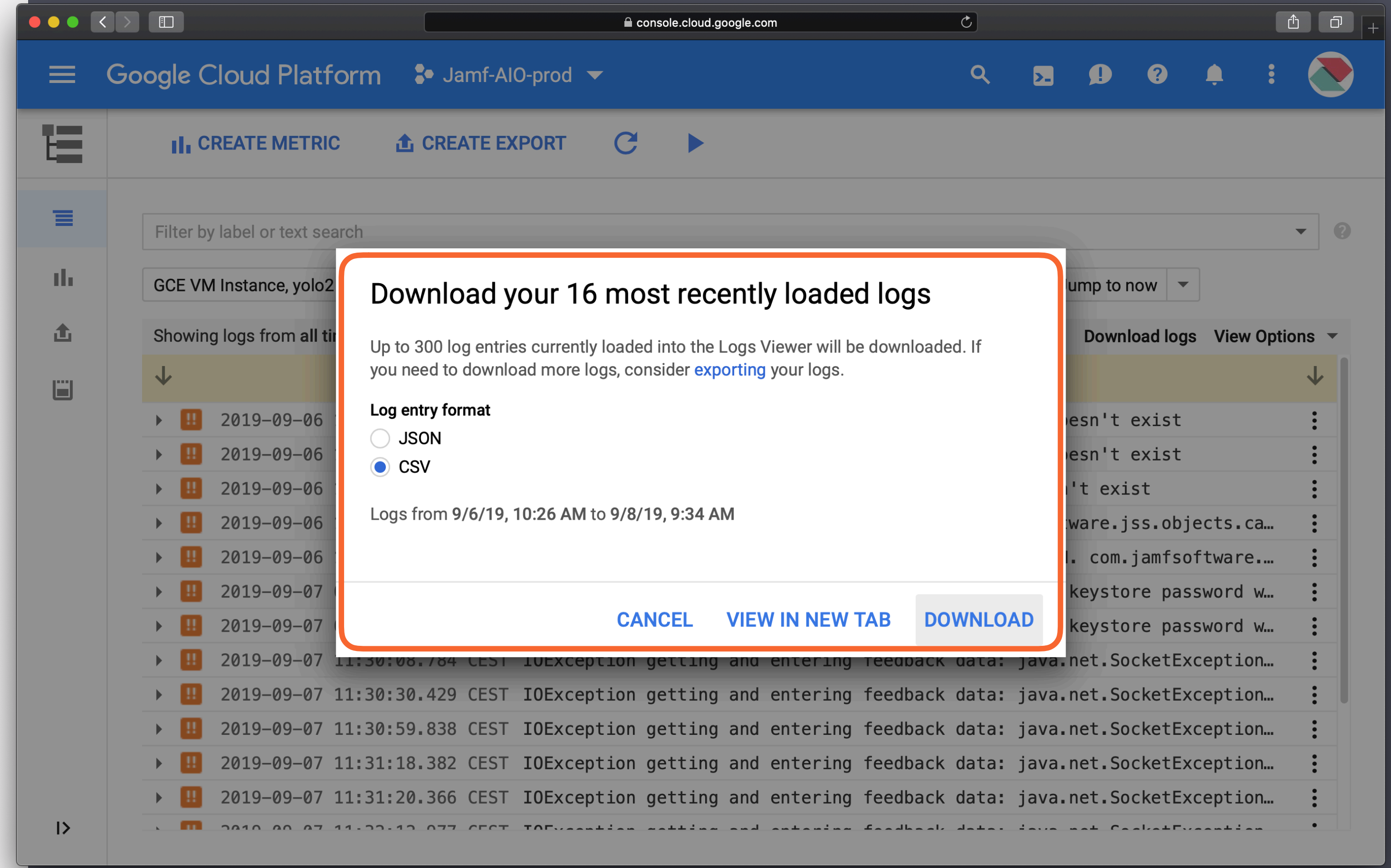
```
2019-09-07 08:35:25.039 CEST  keystore password was inco...keystore password
was incorrect at
java.base/sun.security.pkc...oad(PKCS12KeyStore.j…
at
java.base/sun.security.uti...Load(KeyStoreDelegat…
at java.base/java.security...va:1479) at
com.jamfsoftware.jss.utils...oreFromByteArray(Key…
at
com.jamfsoftware.jss.objec...Processor.readKeySto…
at
com.jamfsoftware.jss.objec...Processor.processCli…
at
com.jamfsoftware.jss.objects.pki.adcs.AdcsSettings.uploadFile(AdcsSettin…
at
com.jamfsoftware.jss.fileupload.UploadController.handleSmartMobileDevice…
at
com.jamfsoftware.jss.fileupload.UploadController.doFileUpload(UploadCont…
at
com.jamfsoftware.jss.fileupload.UploadController.doPost(UploadController…
at javax.servlet.http.HttpServlet.service(HttpServlet.java:661) at
javax.servlet.http.HttpServlet.service(HttpServlet.java:742) at
```

zentral.pro

Ship and collect the events

Existing Solutions

- Log Facilities
  - Stackdriver Logging



Download your 16 most recently loaded logs

Up to 300 log entries currently loaded into the Logs Viewer will be downloaded. If you need to download more logs, consider exporting your logs.

Log entry format

○ JSON
● CSV

Logs from 9/6/19, 10:26 AM to 9/8/19, 9:34 AM

```
2019-09-06                                             esn't exist
2019-09-06                                             esn't exist
2019-09-06                                             't exist
2019-09-06                                             ware.jss.objects.ca…
2019-09-06                                             . com.jamfsoftware.…
2019-09-07                                             keystore password w…
2019-09-07                                             keystore password w…
2019-09-07 11:30:08.784 CEST IOException getting and entering feedback data: java.net.SocketException…
2019-09-07 11:30:30.429 CEST IOException getting and entering feedback data: java.net.SocketException…
2019-09-07 11:30:59.838 CEST IOException getting and entering feedback data: java.net.SocketException…
2019-09-07 11:31:18.382 CEST IOException getting and entering feedback data: java.net.SocketException…
2019-09-07 11:31:20.366 CEST IOException getting and entering feedback data: java.net.SocketException…
```

Ship and collect the events

How to connect the sources

- Endpoints

- Collect file based logs *(by agents)*
- Run agents directly
- RPC / HTTPS Osquery events to Kolide or similar services
- Unified logging to Elastic Stack on Mac endpoints *(i.e. Filebeat)*

Ship and collect the events

How to connect the sources

- Endpoints
  - Agents

    FileBeat

FileBeat (by Elastic)

- Read local file based logs
  - Build-in Modules
- Pre-filter, Normalize events
- Ship to Elastic Stack *(Kibana, Logstash)*

Based on

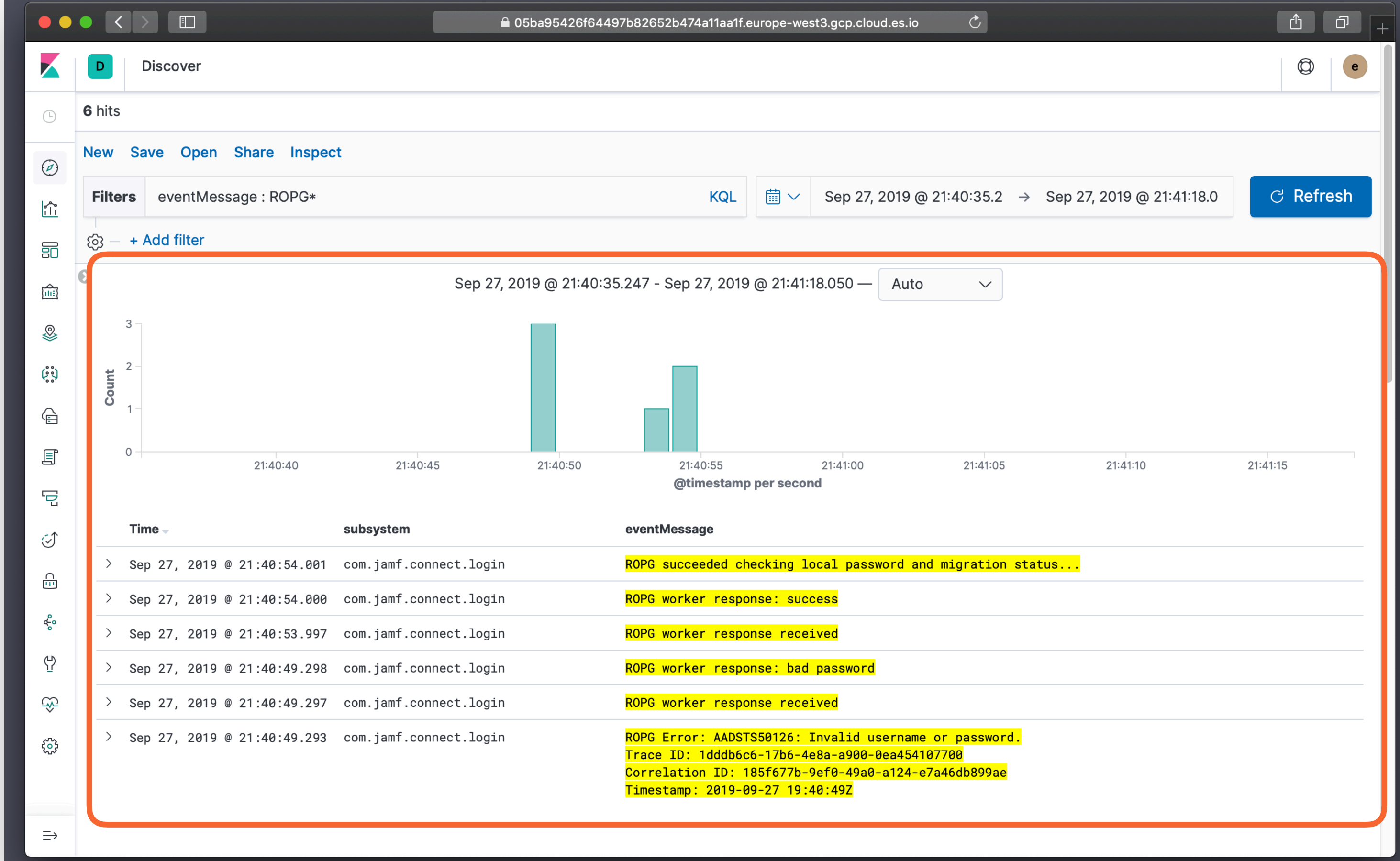
- Open source code - Beats family
- Elastic core component
- `filebeat.yml` config file

Ship and collect the events

How to connect the sources

- Endpoints
  - Agents

    Endpoint logs to ElasticStack



6 hits

Filters: eventMessage : ROPG*

Sep 27, 2019 @ 21:40:35.2 → Sep 27, 2019 @ 21:41:18.0

Sep 27, 2019 @ 21:40:35.247 - Sep 27, 2019 @ 21:41:18.050 —

```
Time                          subsystem                eventMessage
Sep 27, 2019 @ 21:40:54.001   com.jamf.connect.login   ROPG succeeded checking local password and migration status...
Sep 27, 2019 @ 21:40:54.000   com.jamf.connect.login   ROPG worker response: success
Sep 27, 2019 @ 21:40:53.997   com.jamf.connect.login   ROPG worker response received
Sep 27, 2019 @ 21:40:49.298   com.jamf.connect.login   ROPG worker response: bad password
Sep 27, 2019 @ 21:40:49.297   com.jamf.connect.login   ROPG worker response received
Sep 27, 2019 @ 21:40:49.293   com.jamf.connect.login   ROPG Error: AADSTS50126: Invalid username or password.
                                                       Trace ID: 1dddb6c6-17b6-4e8a-a900-0ea454107700
                                                       Correlation ID: 185f677b-9ef0-49a0-a124-e7a46db899ae
                                                       Timestamp: 2019-09-27 19:40:49Z
```

Subsystem shipped to Elastic Stack

Ship and collect the events

How to connect the sources

- Server / Cloud

- Internal routing *(Azure AD monitoring to Azure Sentinel)*
- Interconnect Services with Message Brokers *(Azure Event Hubs connect to Sumo Logic)*
- Webhooks to push event data *(Jamf, SimpleMDM)*
- API pulling data *(Custom Apps for Reporting, Dashboards)*

Ship and collect the events

How to connect the sources

- Dedicated Event Hub
  Zentral
  (Open Source)

zentral

- Productive and Research Platform
- Collect Events in parallel
  - Inventory *(Jamf, Intune, Munki, et.all…)*
  - Identity Providers *(Okta, AzureAD)*
  - Endpoint Agents *(Santa, Osquery, Filebeat)*
- Normalize and attribute Event Data
- Historic Data stored in Elastic Search
- Connect with other Event Hubs
  (Azure Event Hub, SIEM Systems)

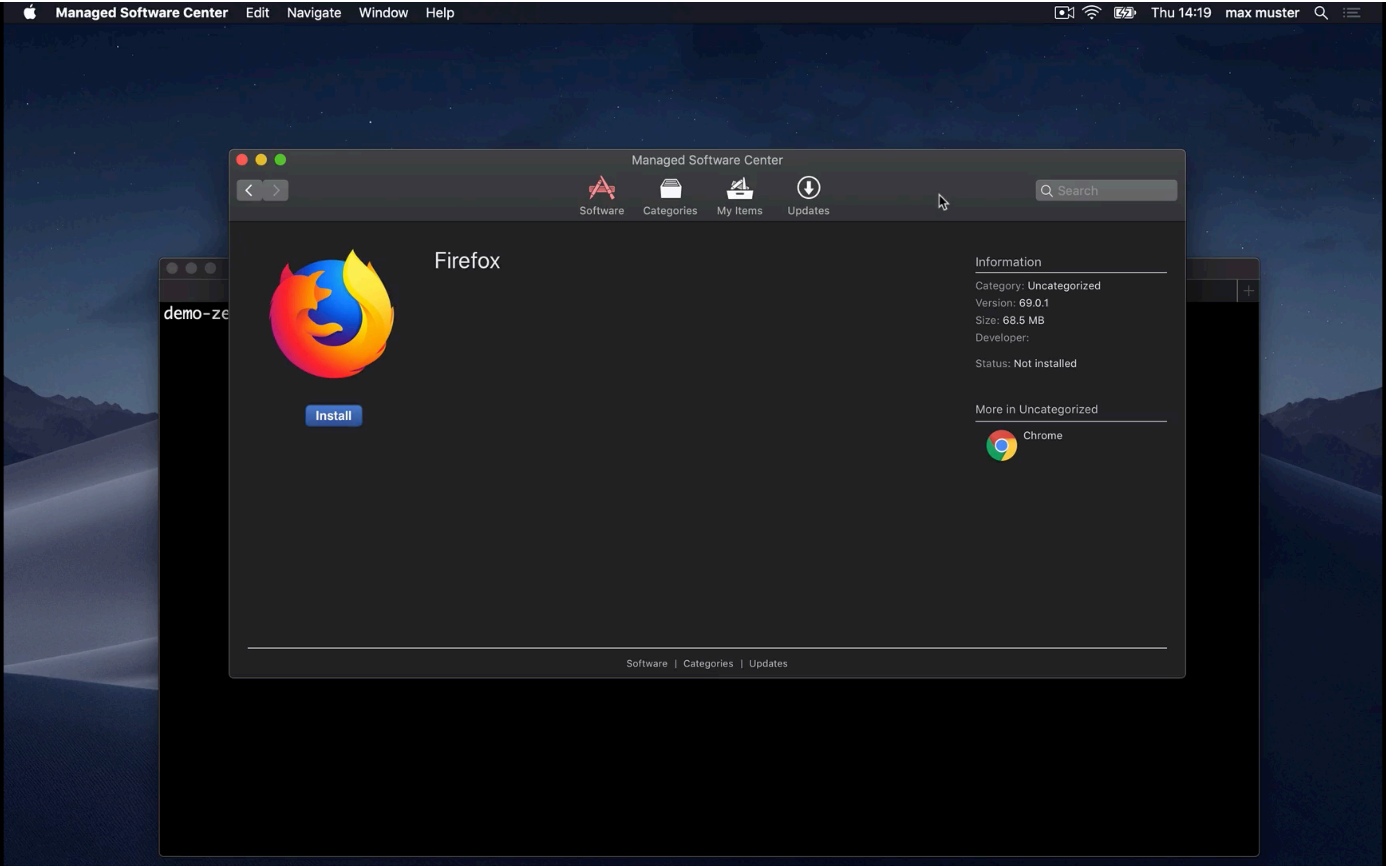
Ship and collect the events

How to connect the sources

- Demo 1
  Binary Auditing

DEMO #1

- Binary Auditing with Xnumon
- Inspect a Software install and launch
- Look into the local log file *(JSON)*
  - See process logs, with SHA-256 and code sigining informtation
- Ship the logs to Elastic Stack *(w/ FileBeat)*
- Run a quick filtering in Zentral
- See filtered Events in Kibana UI



Firefox

Information

Category: Uncategorized

Version: 69.0.1

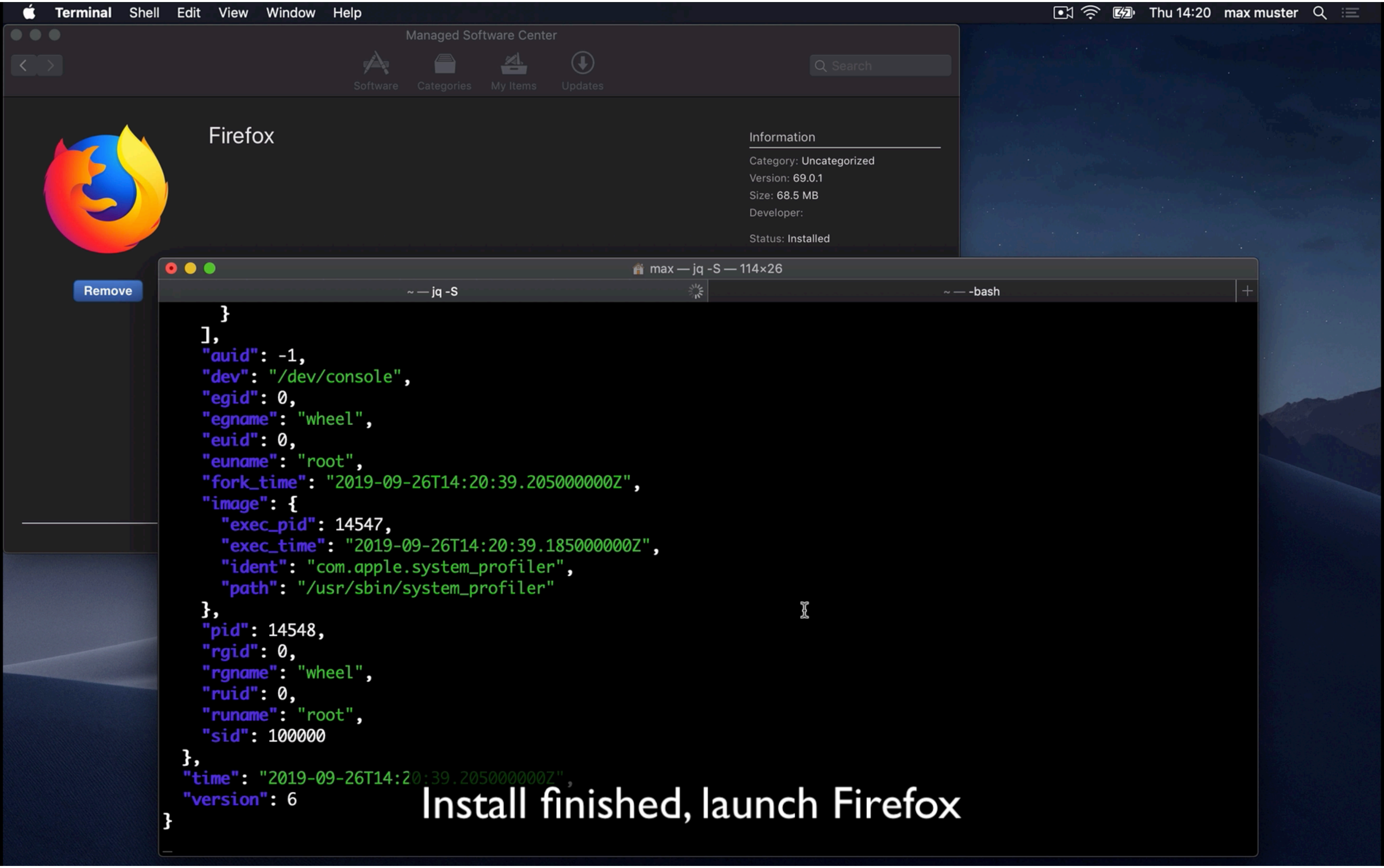
Size: 68.5 MB

Developer:

Status: Not installed

More in Uncategorized

Chrome



Firefox

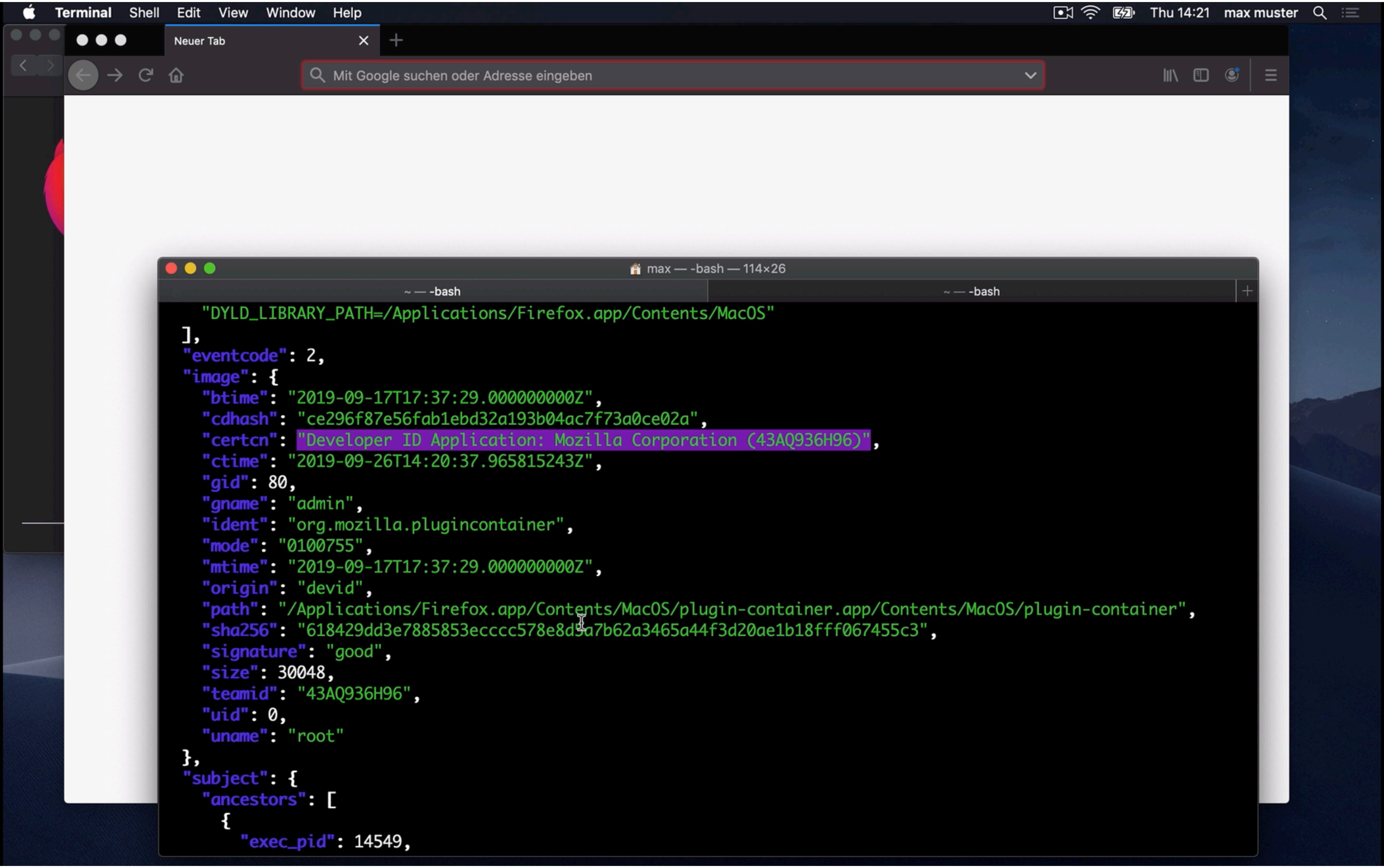
Information

Category: Uncategorized
Version: 69.0.1
Size: 68.5 MB
Developer:

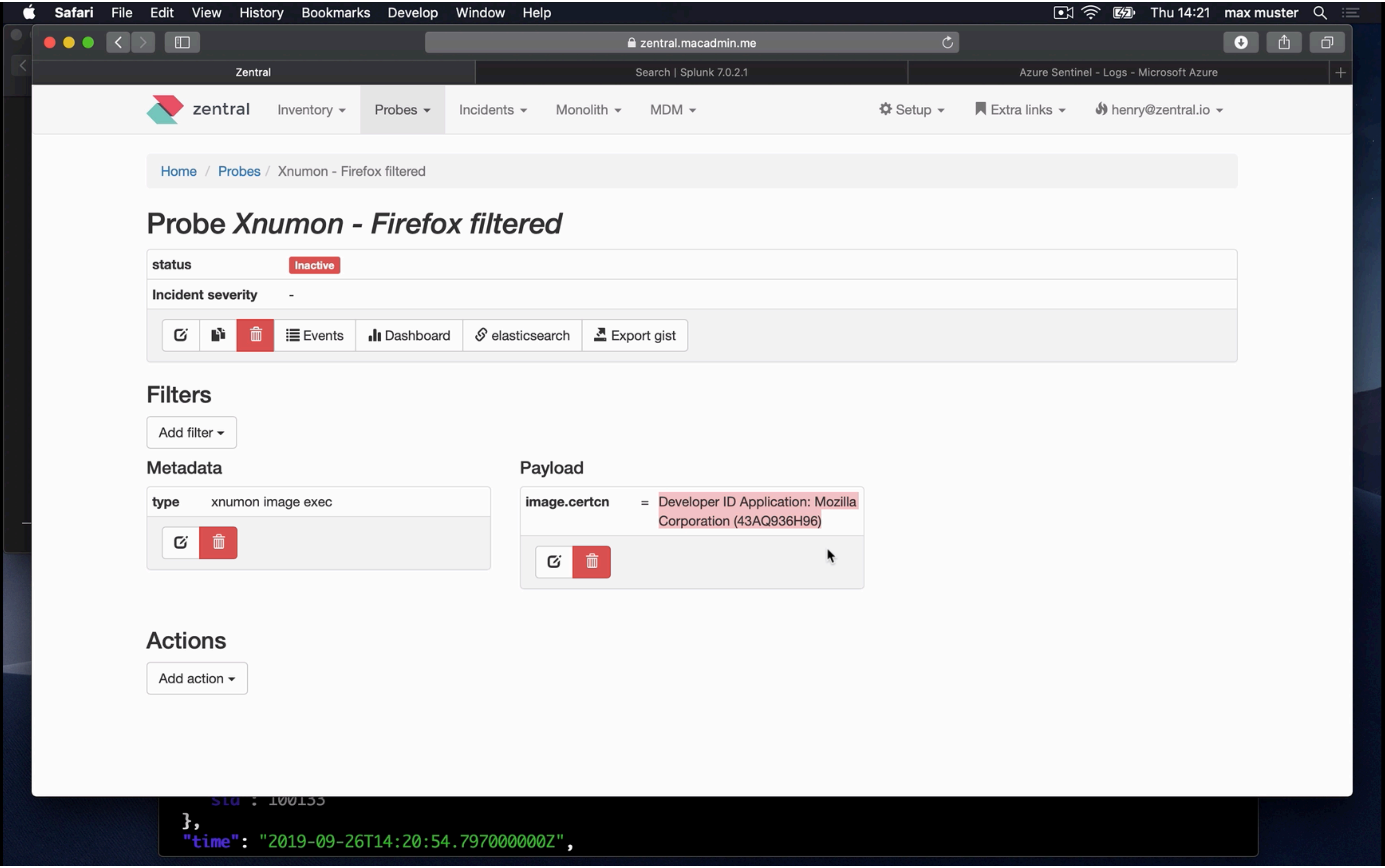
Status: Installed

```
      }
    ],
    "auid": -1,
    "dev": "/dev/console",
    "egid": 0,
    "egname": "wheel",
    "euid": 0,
    "euname": "root",
    "fork_time": "2019-09-26T14:20:39.205000000Z",
    "image": {
      "exec_pid": 14547,
      "exec_time": "2019-09-26T14:20:39.185000000Z",
      "ident": "com.apple.system_profiler",
      "path": "/usr/sbin/system_profiler"
    },
    "pid": 14548,
    "rgid": 0,
    "rgname": "wheel",
    "ruid": 0,
    "runame": "root",
    "sid": 100000
  },
  "time": "2019-09-26T14:20:39.205000000Z",
  "version": 6
}
```

Install finished, launch Firefox



```
    "DYLD_LIBRARY_PATH=/Applications/Firefox.app/Contents/MacOS"
  ],
  "eventcode": 2,
  "image": {
    "btime": "2019-09-17T17:37:29.000000000Z",
    "cdhash": "ce296f87e56fab1ebd32a193b04ac7f73a0ce02a",
    "certcn": "Developer ID Application: Mozilla Corporation (43AQ936H96)",
    "ctime": "2019-09-26T14:20:37.965815243Z",
    "gid": 80,
    "gname": "admin",
    "ident": "org.mozilla.plugincontainer",
    "mode": "0100755",
    "mtime": "2019-09-17T17:37:29.000000000Z",
    "origin": "devid",
    "path": "/Applications/Firefox.app/Contents/MacOS/plugin-container.app/Contents/MacOS/plugin-container",
    "sha256": "618429dd3e7885853eccc578e8d5a7b62a3465a44f3d20ae1b18fff067455c3",
    "signature": "good",
    "size": 30048,
    "teamid": "43AQ936H96",
    "uid": 0,
    "uname": "root"
  },
  "subject": {
    "ancestors": [
      {
        "exec_pid": 14549,
```



Home / Probes / Xnumon - Firefox filtered

Probe *Xnumon - Firefox filtered*

status	Inactive
Incident severity	-

Filters

Metadata

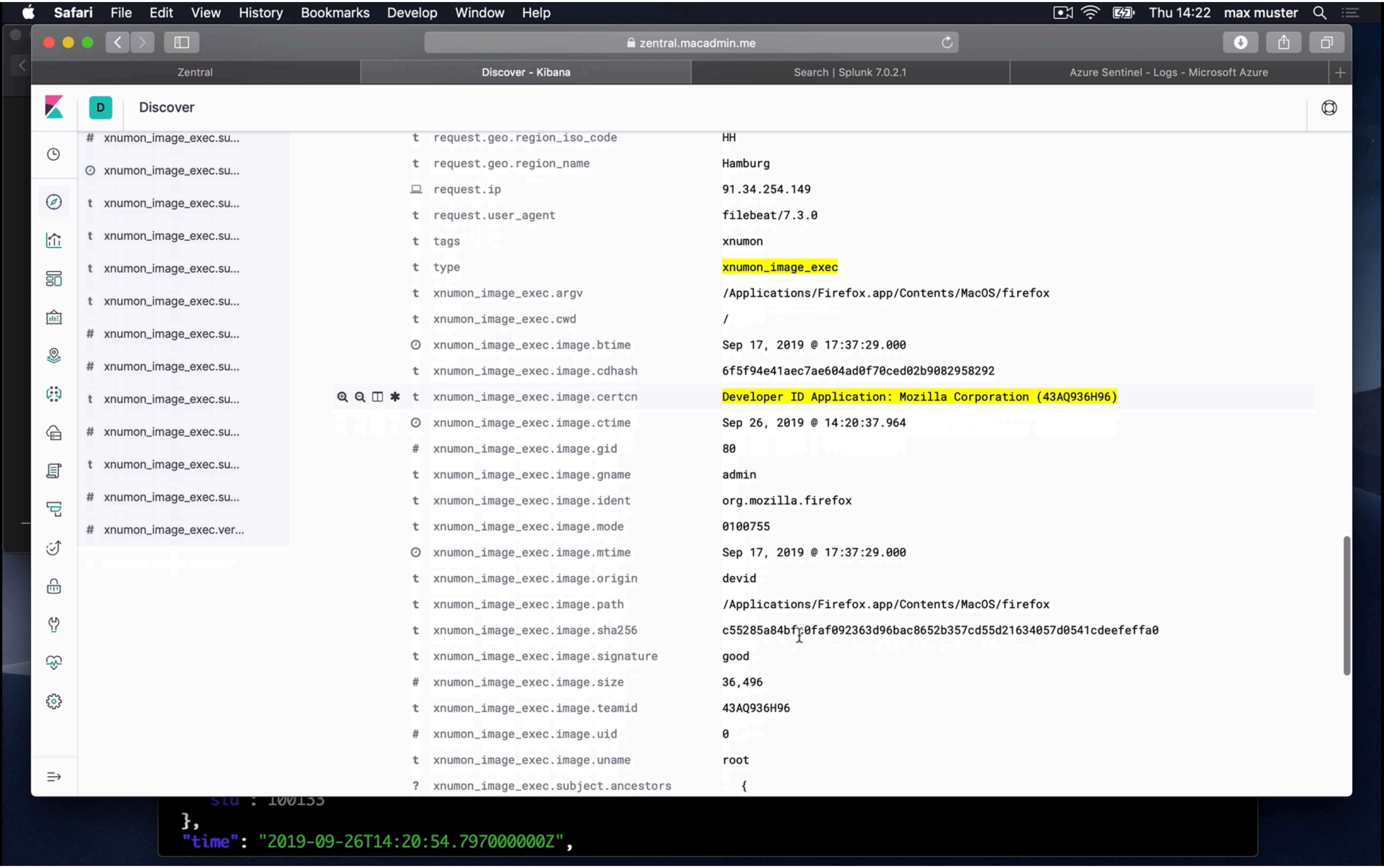
type	xnumon image exec

Payload

image.certcn	=	Developer ID Application: Mozilla Corporation (43AQ936H96)

Actions

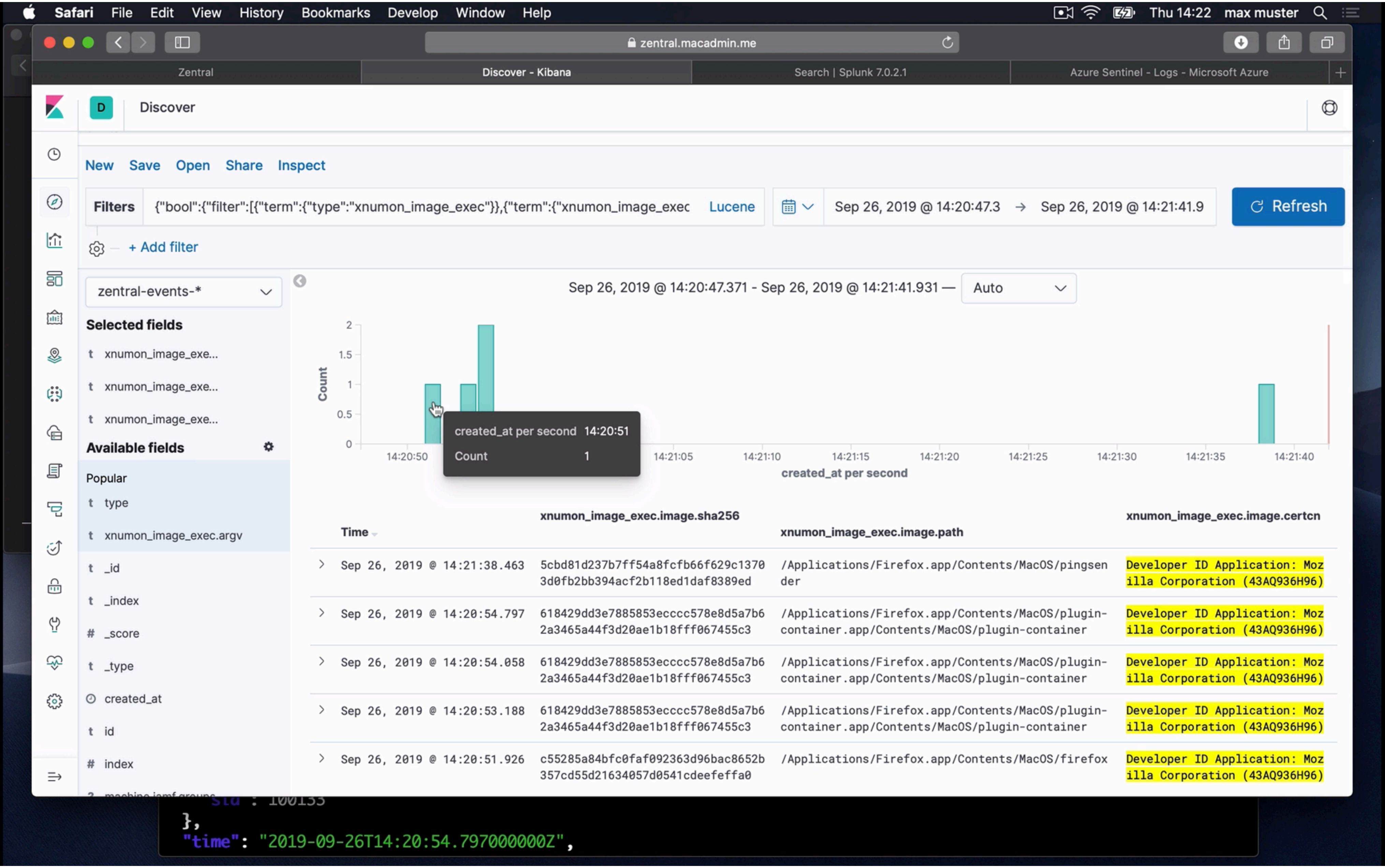
```
    "sid": 100133
  },
  "time": "2019-09-26T14:20:54.797000000Z",
```



```
# xnumon_image_exec.su...
⊙ xnumon_image_exec.su...
t xnumon_image_exec.su...
t xnumon_image_exec.su...
t xnumon_image_exec.su...
t xnumon_image_exec.su...
# xnumon_image_exec.su...
# xnumon_image_exec.su...
t xnumon_image_exec.su...
# xnumon_image_exec.su...
t xnumon_image_exec.su...
# xnumon_image_exec.su...
# xnumon_image_exec.ver...
```

```
t  request.geo.region_iso_code         HH
t  request.geo.region_name             Hamburg
   request.ip                          91.34.254.149
t  request.user_agent                  filebeat/7.3.0
t  tags                                xnumon
t  type                                xnumon_image_exec
t  xnumon_image_exec.argv              /Applications/Firefox.app/Contents/MacOS/firefox
t  xnumon_image_exec.cwd               /
⊙  xnumon_image_exec.image.btime       Sep 17, 2019 @ 17:37:29.000
t  xnumon_image_exec.image.cdhash      6f5f94e41aec7ae604ad0f70ced02b9082958292
t  xnumon_image_exec.image.certcn      Developer ID Application: Mozilla Corporation (43AQ936H96)
⊙  xnumon_image_exec.image.ctime       Sep 26, 2019 @ 14:20:37.964
#  xnumon_image_exec.image.gid         80
t  xnumon_image_exec.image.gname       admin
t  xnumon_image_exec.image.ident       org.mozilla.firefox
t  xnumon_image_exec.image.mode        0100755
⊙  xnumon_image_exec.image.mtime       Sep 17, 2019 @ 17:37:29.000
t  xnumon_image_exec.image.origin      devid
t  xnumon_image_exec.image.path        /Applications/Firefox.app/Contents/MacOS/firefox
t  xnumon_image_exec.image.sha256      c55285a84bfc0faf092363d96bac8652b357cd55d21634057d0541cdeefeffa0
t  xnumon_image_exec.image.signature   good
#  xnumon_image_exec.image.size        36,496
t  xnumon_image_exec.image.teamid      43AQ936H96
#  xnumon_image_exec.image.uid         0
t  xnumon_image_exec.image.uname       root
?  xnumon_image_exec.subject.ancestors   {
```

```
    "sid": 100133
  },
  "time": "2019-09-26T14:20:54.797000000Z",
```



Filters: {"bool":{"filter":[{"term":{"type":"xnumon_image_exec"}},{"term":{"xnumon_image_exec

Sep 26, 2019 @ 14:20:47.3 → Sep 26, 2019 @ 14:21:41.9

Selected fields

- t xnumon_image_exe...
- t xnumon_image_exe...
- t xnumon_image_exe...

Available fields

Popular

- t type
- t xnumon_image_exec.argv
- t _id
- t _index
- # _score
- t _type
- ⊙ created_at
- t id
- # index

Sep 26, 2019 @ 14:20:47.371 - Sep 26, 2019 @ 14:21:41.931 — Auto

created_at per second 14:20:51
Count 1

	Time	xnumon_image_exec.image.sha256	xnumon_image_exec.image.path	xnumon_image_exec.image.certcn
>	Sep 26, 2019 @ 14:21:38.463	5cbd81d237b7ff54a8fcfb66f629c1370 3d0fb2bb394acf2b118ed1daf8389ed	/Applications/Firefox.app/Contents/MacOS/pingsender	Developer ID Application: Mozilla Corporation (43AQ936H96)
>	Sep 26, 2019 @ 14:20:54.797	618429dd3e7885853ecccc578e8d5a7b6 2a3465a44f3d20ae1b18fff067455c3	/Applications/Firefox.app/Contents/MacOS/plugin-container.app/Contents/MacOS/plugin-container	Developer ID Application: Mozilla Corporation (43AQ936H96)
>	Sep 26, 2019 @ 14:20:54.058	618429dd3e7885853ecccc578e8d5a7b6 2a3465a44f3d20ae1b18fff067455c3	/Applications/Firefox.app/Contents/MacOS/plugin-container.app/Contents/MacOS/plugin-container	Developer ID Application: Mozilla Corporation (43AQ936H96)
>	Sep 26, 2019 @ 14:20:53.188	618429dd3e7885853ecccc578e8d5a7b6 2a3465a44f3d20ae1b18fff067455c3	/Applications/Firefox.app/Contents/MacOS/plugin-container.app/Contents/MacOS/plugin-container	Developer ID Application: Mozilla Corporation (43AQ936H96)
>	Sep 26, 2019 @ 14:20:51.926	c55285a84bfc0faf092363d96bac8652b 357cd55d21634057d0541cdeefeffa0	/Applications/Firefox.app/Contents/MacOS/firefox	Developer ID Application: Mozilla Corporation (43AQ936H96)

```
      "sid" : 100133
    },
    "time": "2019-09-26T14:20:54.797000000Z",
```

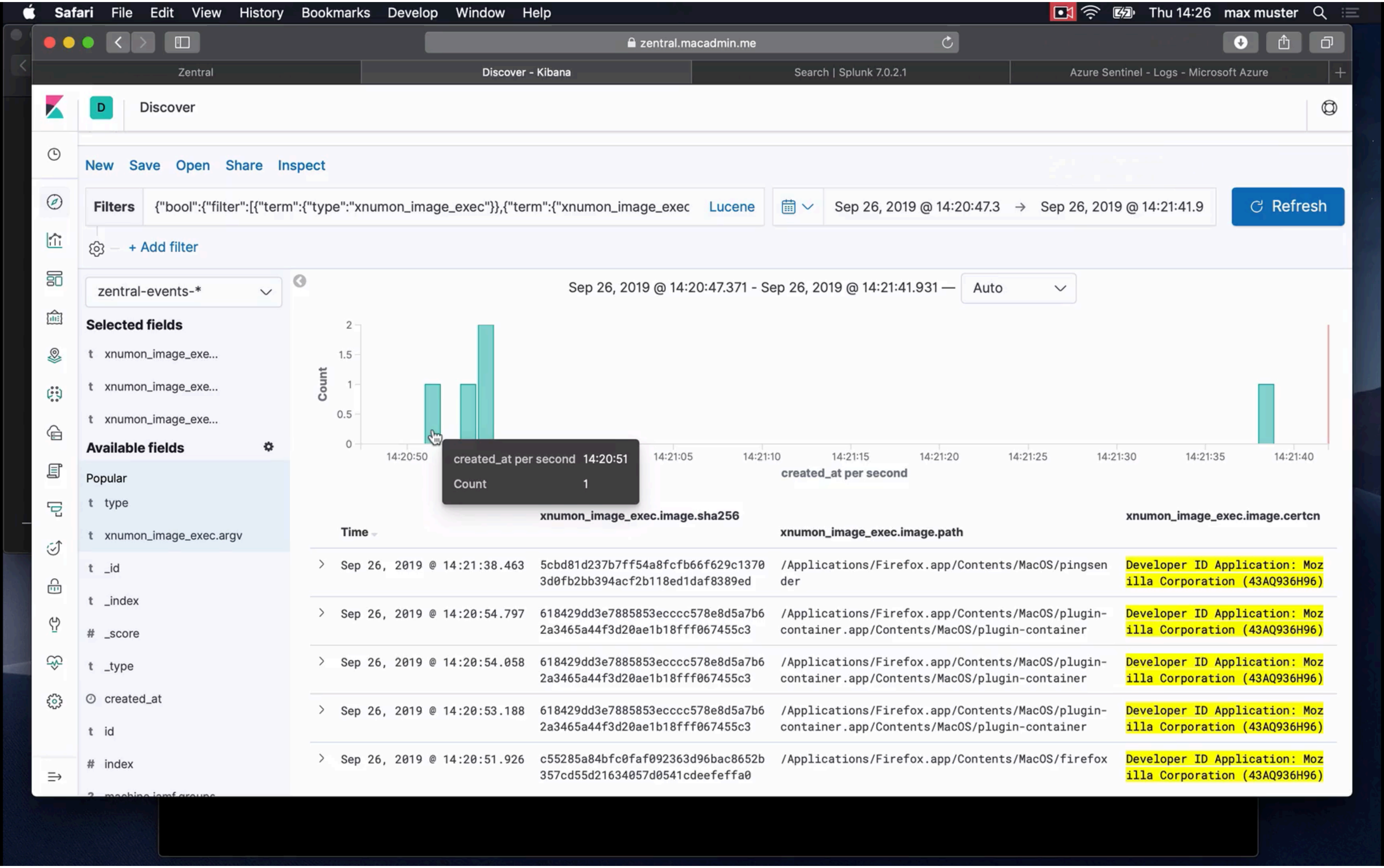
Ship and collect the events

How to connect the sources

- Demo 2
  Binary Auditing

DEMO #2

- Ship same log to a commercial SaaS
- Look into events in the SaaS
- Next level - interconnecting
  Event Hubs and normalized event stream
- See Events filtered in a SIEM
  (Security Incident Event Management)



Filters {"bool":{"filter":[{"term":{"type":"xnumon_image_exec"}},{"term":{"xnumon_image_exec Lucene

Sep 26, 2019 @ 14:20:47.3 → Sep 26, 2019 @ 14:21:41.9

zentral-events-*

Selected fields

- t xnumon_image_exe...
- t xnumon_image_exe...
- t xnumon_image_exe...

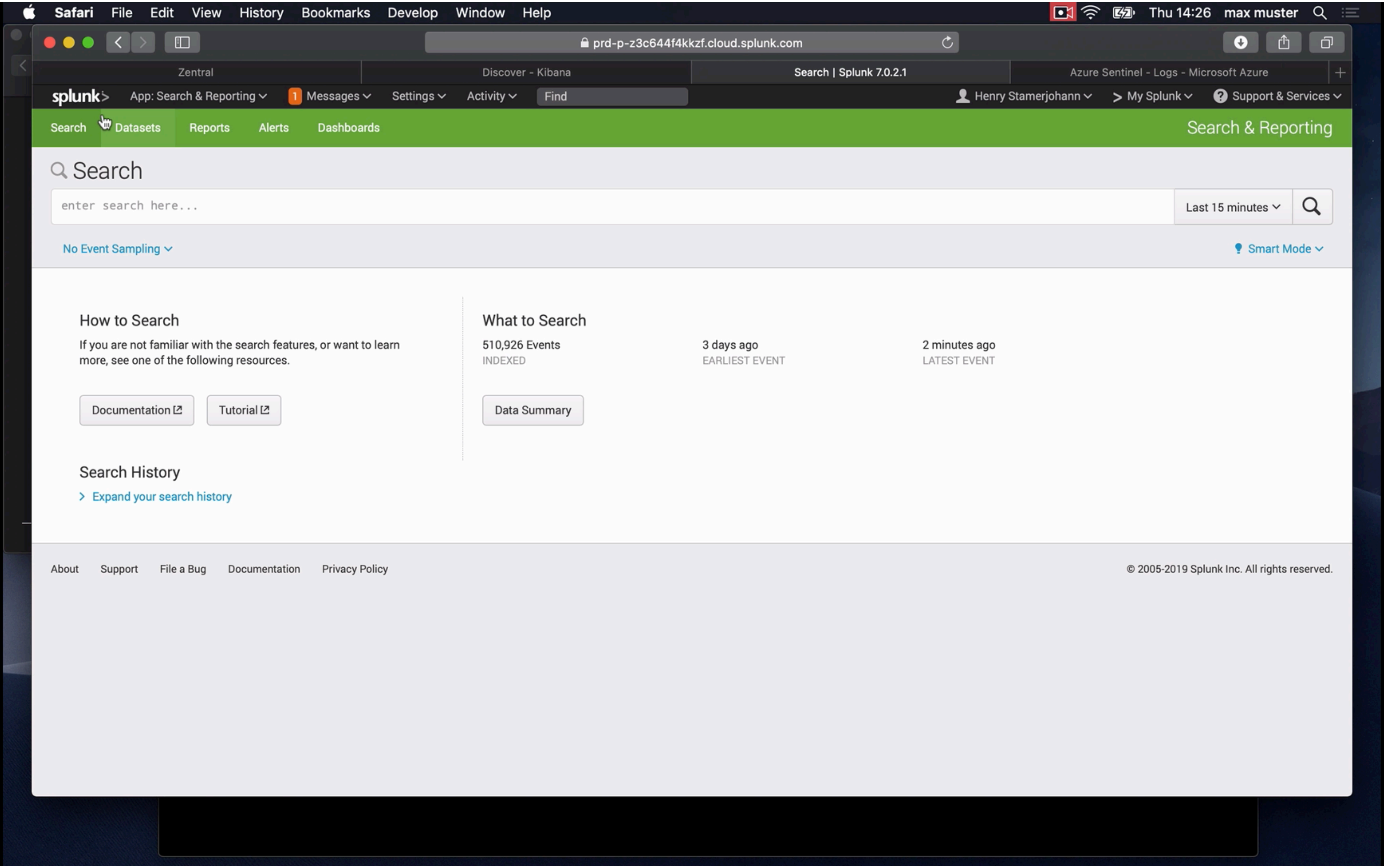
Available fields

Popular

- t type
- t xnumon_image_exec.argv
- t _id
- t _index
- # _score
- t _type
- created_at
- t id
- # index
- ? machine.jamf.groups

Sep 26, 2019 @ 14:20:47.371 - Sep 26, 2019 @ 14:21:41.931 — Auto

Time	xnumon_image_exec.image.sha256	xnumon_image_exec.image.path	xnumon_image_exec.image.certcn
Sep 26, 2019 @ 14:21:38.463	5cbd81d237b7ff54a8fcfb66f629c1370 3d0fb2bb394acf2b118ed1daf8389ed	/Applications/Firefox.app/Contents/MacOS/pingsender	Developer ID Application: Mozilla Corporation (43AQ936H96)
Sep 26, 2019 @ 14:20:54.797	618429dd3e7885853ecccc578e8d5a7b6 2a3465a44f3d20ae1b18fff067455c3	/Applications/Firefox.app/Contents/MacOS/plugin-container.app/Contents/MacOS/plugin-container	Developer ID Application: Mozilla Corporation (43AQ936H96)
Sep 26, 2019 @ 14:20:54.058	618429dd3e7885853ecccc578e8d5a7b6 2a3465a44f3d20ae1b18fff067455c3	/Applications/Firefox.app/Contents/MacOS/plugin-container.app/Contents/MacOS/plugin-container	Developer ID Application: Mozilla Corporation (43AQ936H96)
Sep 26, 2019 @ 14:20:53.188	618429dd3e7885853ecccc578e8d5a7b6 2a3465a44f3d20ae1b18fff067455c3	/Applications/Firefox.app/Contents/MacOS/plugin-container.app/Contents/MacOS/plugin-container	Developer ID Application: Mozilla Corporation (43AQ936H96)
Sep 26, 2019 @ 14:20:51.926	c55285a84bfc0faf092363d96bac8652b 357cd55d21634057d0541cdeefeffa0	/Applications/Firefox.app/Contents/MacOS/firefox	Developer ID Application: Mozilla Corporation (43AQ936H96)



How to Search

If you are not familiar with the search features, or want to learn more, see one of the following resources.

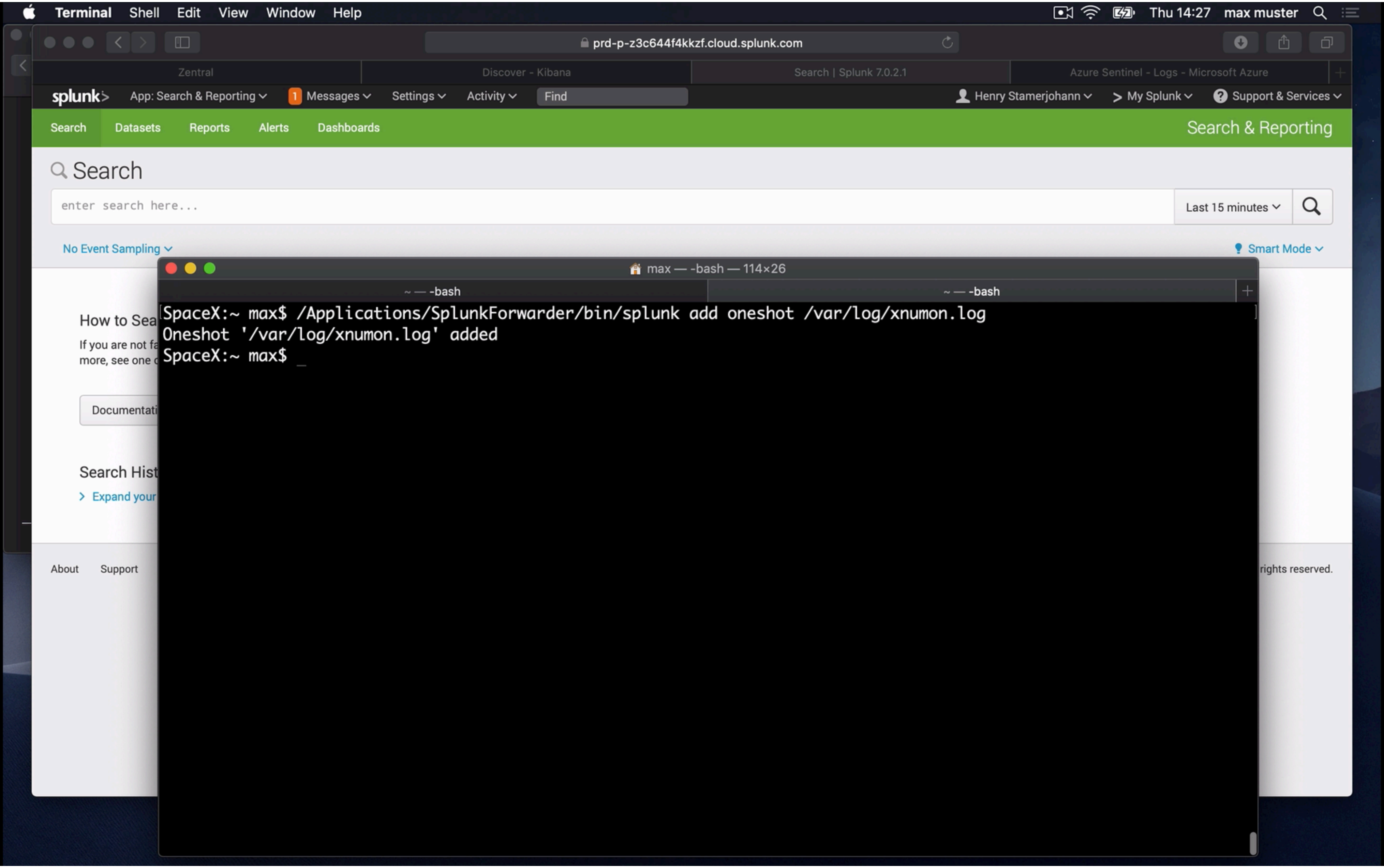
What to Search

510,926 Events	3 days ago	2 minutes ago
INDEXED	EARLIEST EVENT	LATEST EVENT

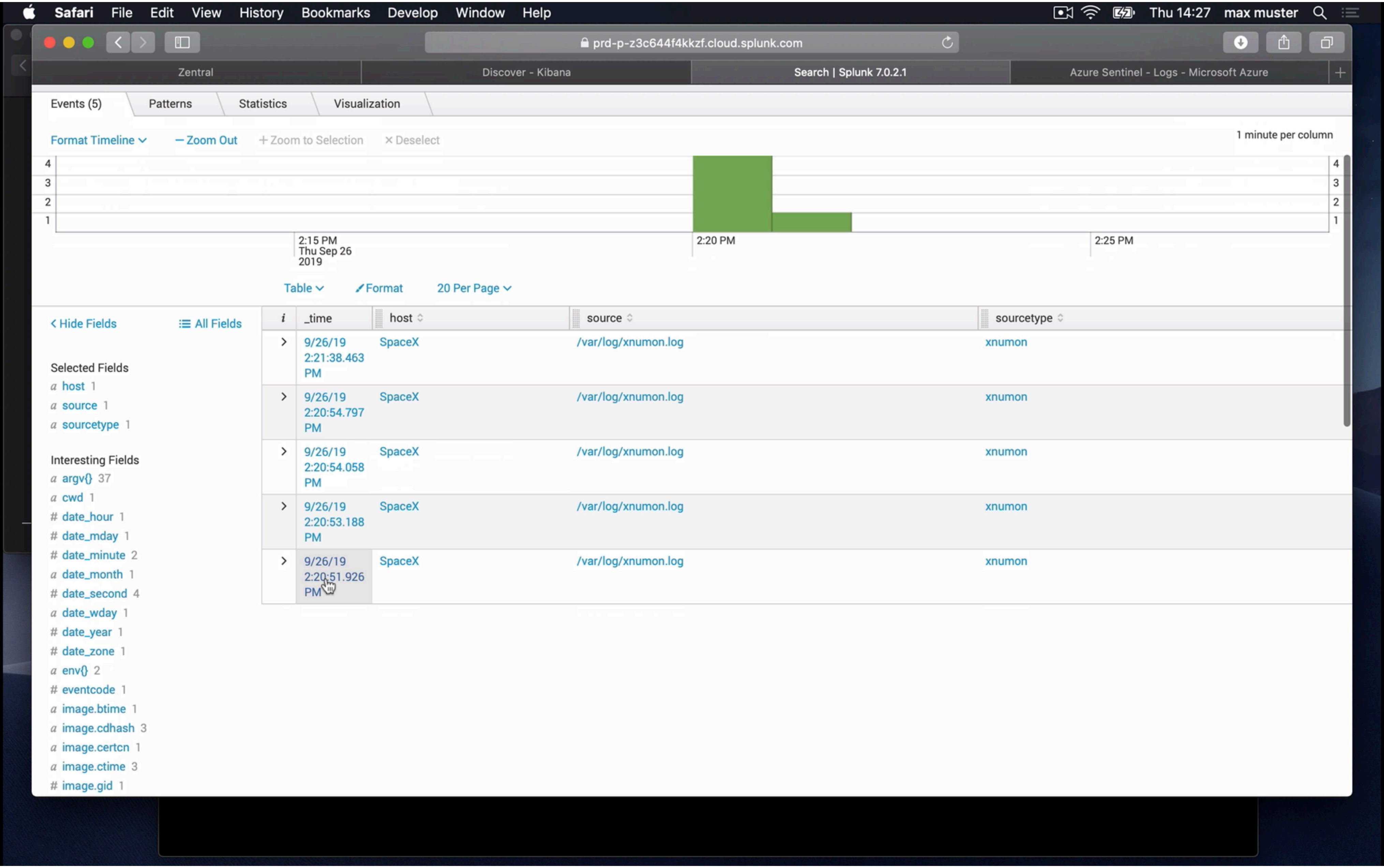
Search History

> Expand your search history

© 2005-2019 Splunk Inc. All rights reserved.



```
SpaceX:~ max$ /Applications/SplunkForwarder/bin/splunk add oneshot /var/log/xnumon.log
Oneshot '/var/log/xnumon.log' added
SpaceX:~ max$ _
```



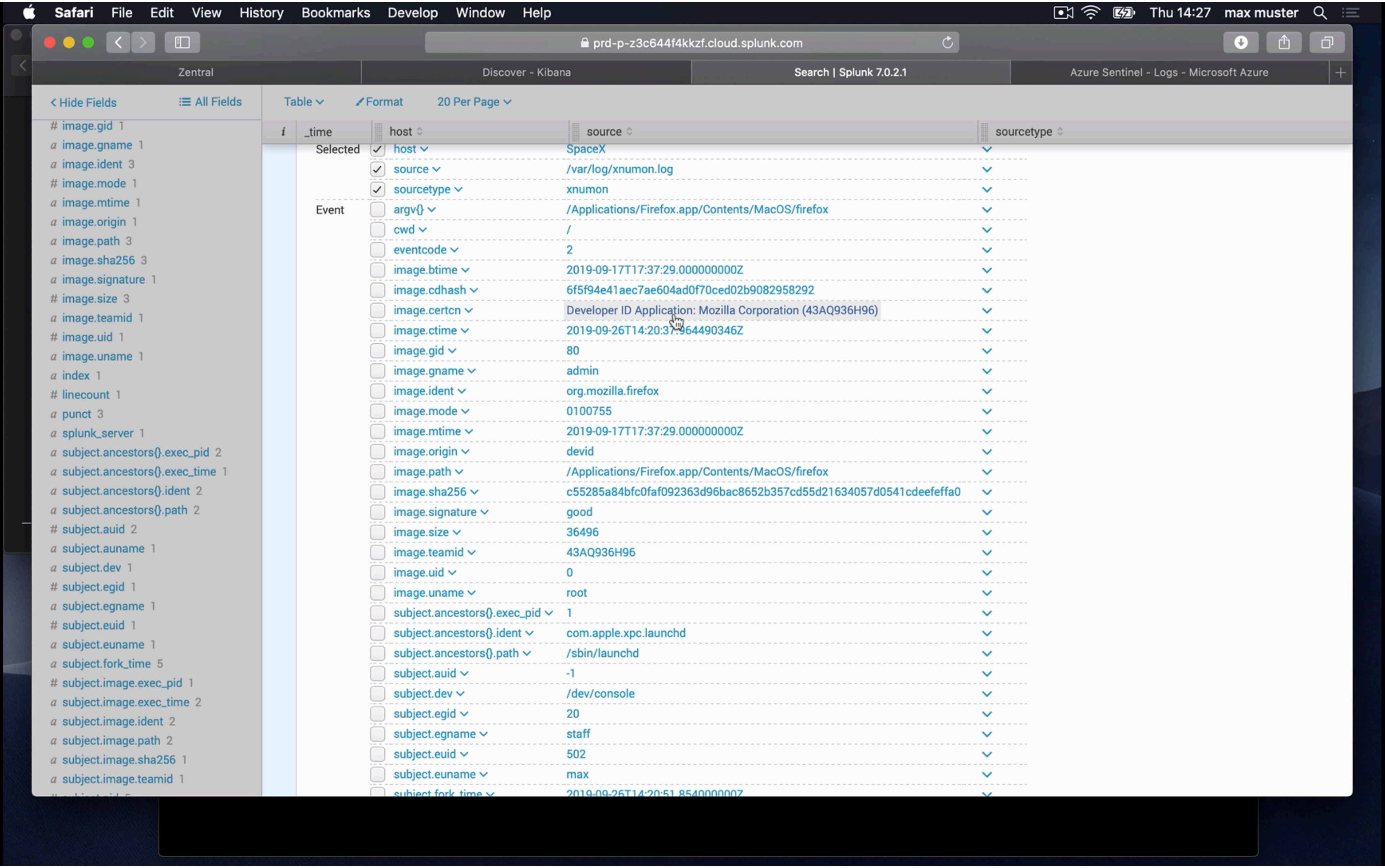
i	_time	host	source	sourcetype
>	9/26/19 2:21:38.463 PM	SpaceX	/var/log/xnumon.log	xnumon
>	9/26/19 2:20:54.797 PM	SpaceX	/var/log/xnumon.log	xnumon
>	9/26/19 2:20:54.058 PM	SpaceX	/var/log/xnumon.log	xnumon
>	9/26/19 2:20:53.188 PM	SpaceX	/var/log/xnumon.log	xnumon
>	9/26/19 2:20:51.926 PM	SpaceX	/var/log/xnumon.log	xnumon

Selected Fields

a	host	1
a	source	1
a	sourcetype	1

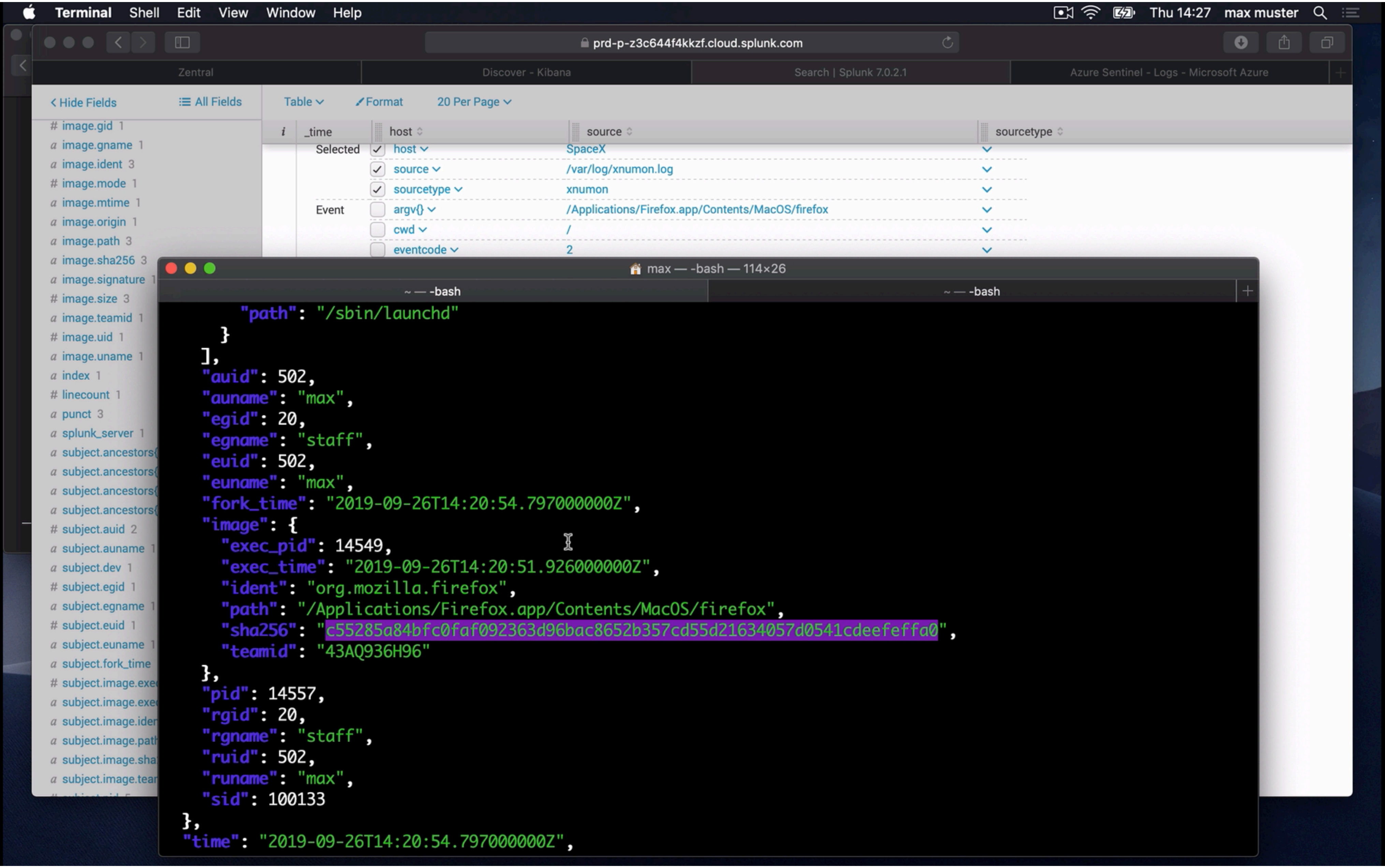
Interesting Fields

a	argv{}	37
a	cwd	1
#	date_hour	1
#	date_mday	1
#	date_minute	2
a	date_month	1
#	date_second	4
a	date_wday	1
#	date_year	1
#	date_zone	1
a	env{}	2
#	eventcode	1
a	image.btime	1
a	image.cdhash	3
a	image.certcn	1
a	image.ctime	3
#	image.gid	1



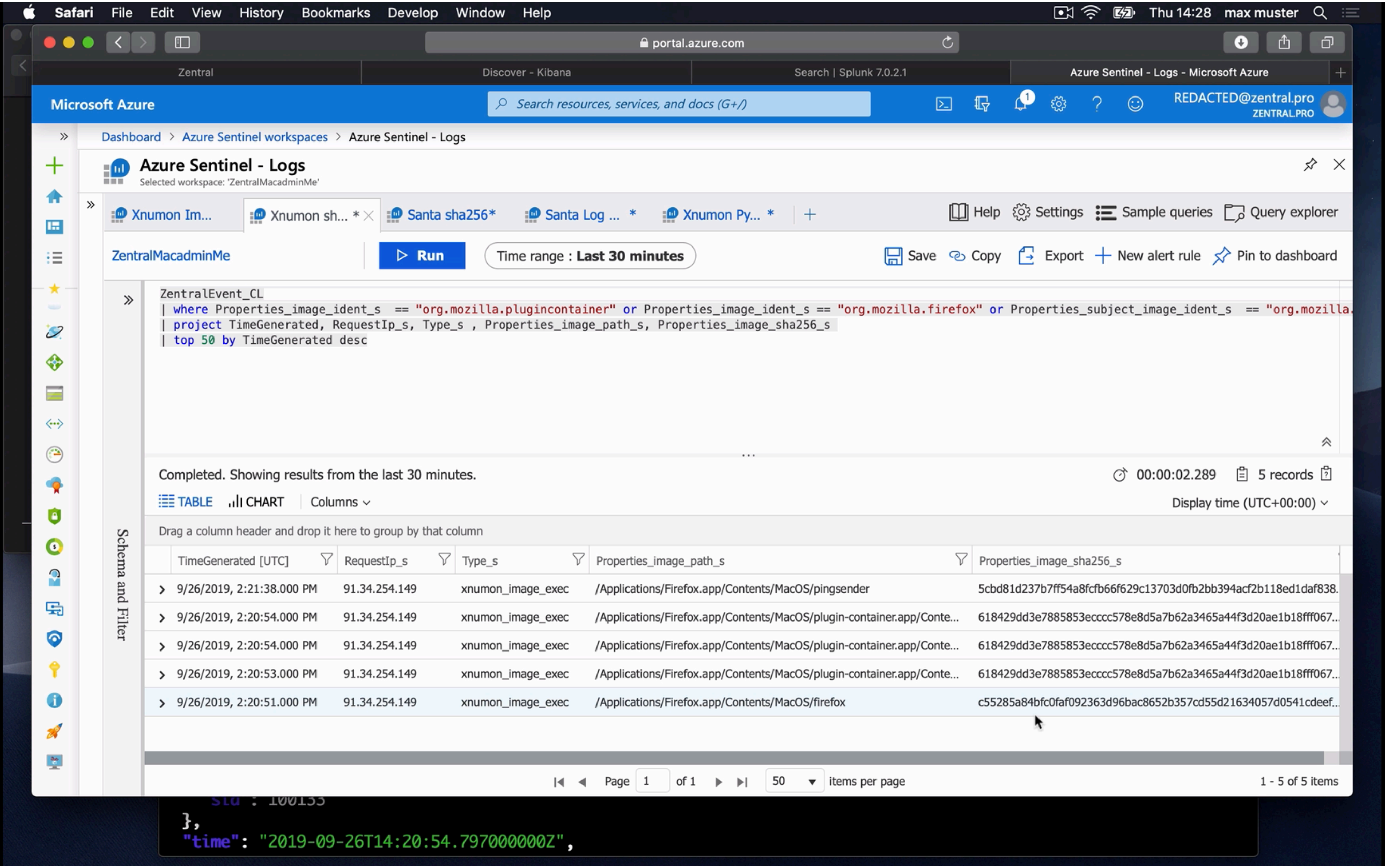
# image.gid 1
a image.gname 1
a image.ident 3
# image.mode 1
a image.mtime 1
a image.origin 1
a image.path 3
a image.sha256 3
a image.signature 1
# image.size 3
a image.teamid 1
# image.uid 1
a image.uname 1
a index 1
# linecount 1
a punct 3
a splunk_server 1
a subject.ancestors{}.exec_pid 2
a subject.ancestors{}.exec_time 1
a subject.ancestors{}.ident 2
a subject.ancestors{}.path 2
# subject.auid 2
a subject.auname 1
a subject.dev 1
# subject.egid 1
a subject.egname 1
# subject.euid 1
a subject.euname 1
a subject.fork_time 5
# subject.image.exec_pid 1
a subject.image.exec_time 2
a subject.image.ident 2
a subject.image.path 2
a subject.image.sha256 1
a subject.image.teamid 1

i	_time	host	source	sourcetype
	Selected	☑ host	SpaceX	
		☑ source	/var/log/xnumon.log	
		☑ sourcetype	xnumon	
	Event	□ argv{}	/Applications/Firefox.app/Contents/MacOS/firefox	
		□ cwd	/	
		□ eventcode	2	
		□ image.btime	2019-09-17T17:37:29.000000000Z	
		□ image.cdhash	6f5f94e41aec7ae604ad0f70ced02b9082958292	
		□ image.certcn	Developer ID Application: Mozilla Corporation (43AQ936H96)	
		□ image.ctime	2019-09-26T14:20:37.964490346Z	
		□ image.gid	80	
		□ image.gname	admin	
		□ image.ident	org.mozilla.firefox	
		□ image.mode	0100755	
		□ image.mtime	2019-09-17T17:37:29.000000000Z	
		□ image.origin	devid	
		□ image.path	/Applications/Firefox.app/Contents/MacOS/firefox	
		□ image.sha256	c55285a84bfc0faf092363d96bac8652b357cd55d21634057d0541cdeefeffa0	
		□ image.signature	good	
		□ image.size	36496	
		□ image.teamid	43AQ936H96	
		□ image.uid	0	
		□ image.uname	root	
		□ subject.ancestors{}.exec_pid	1	
		□ subject.ancestors{}.ident	com.apple.xpc.launchd	
		□ subject.ancestors{}.path	/sbin/launchd	
		□ subject.auid	-1	
		□ subject.dev	/dev/console	
		□ subject.egid	20	
		□ subject.egname	staff	
		□ subject.euid	502	
		□ subject.euname	max	
		□ subject.fork_time	2019-09-26T14:20:51.854000000Z	



Selected	☑	host	SpaceX
	☑	source	/var/log/xnumon.log
	☑	sourcetype	xnumon
Event	□	argv{}	/Applications/Firefox.app/Contents/MacOS/firefox
	□	cwd	/
	□	eventcode	2

```
        "path": "/sbin/launchd"
      }
    ],
    "auid": 502,
    "auname": "max",
    "egid": 20,
    "egname": "staff",
    "euid": 502,
    "euname": "max",
    "fork_time": "2019-09-26T14:20:54.797000000Z",
    "image": {
      "exec_pid": 14549,
      "exec_time": "2019-09-26T14:20:51.926000000Z",
      "ident": "org.mozilla.firefox",
      "path": "/Applications/Firefox.app/Contents/MacOS/firefox",
      "sha256": "c55285a84bfc0faf092363d96bac8652b357cd55d21634057d0541cdeefeffa0",
      "teamid": "43AQ936H96"
    },
    "pid": 14557,
    "rgid": 20,
    "rgname": "staff",
    "ruid": 502,
    "runame": "max",
    "sid": 100133
  },
  "time": "2019-09-26T14:20:54.797000000Z",
```



```
ZentralEvent_CL
| where Properties_image_ident_s  == "org.mozilla.plugincontainer" or Properties_image_ident_s == "org.mozilla.firefox" or Properties_subject_image_ident_s  == "org.mozilla.
| project TimeGenerated, RequestIp_s, Type_s , Properties_image_path_s, Properties_image_sha256_s
| top 50 by TimeGenerated desc
```

Completed. Showing results from the last 30 minutes.

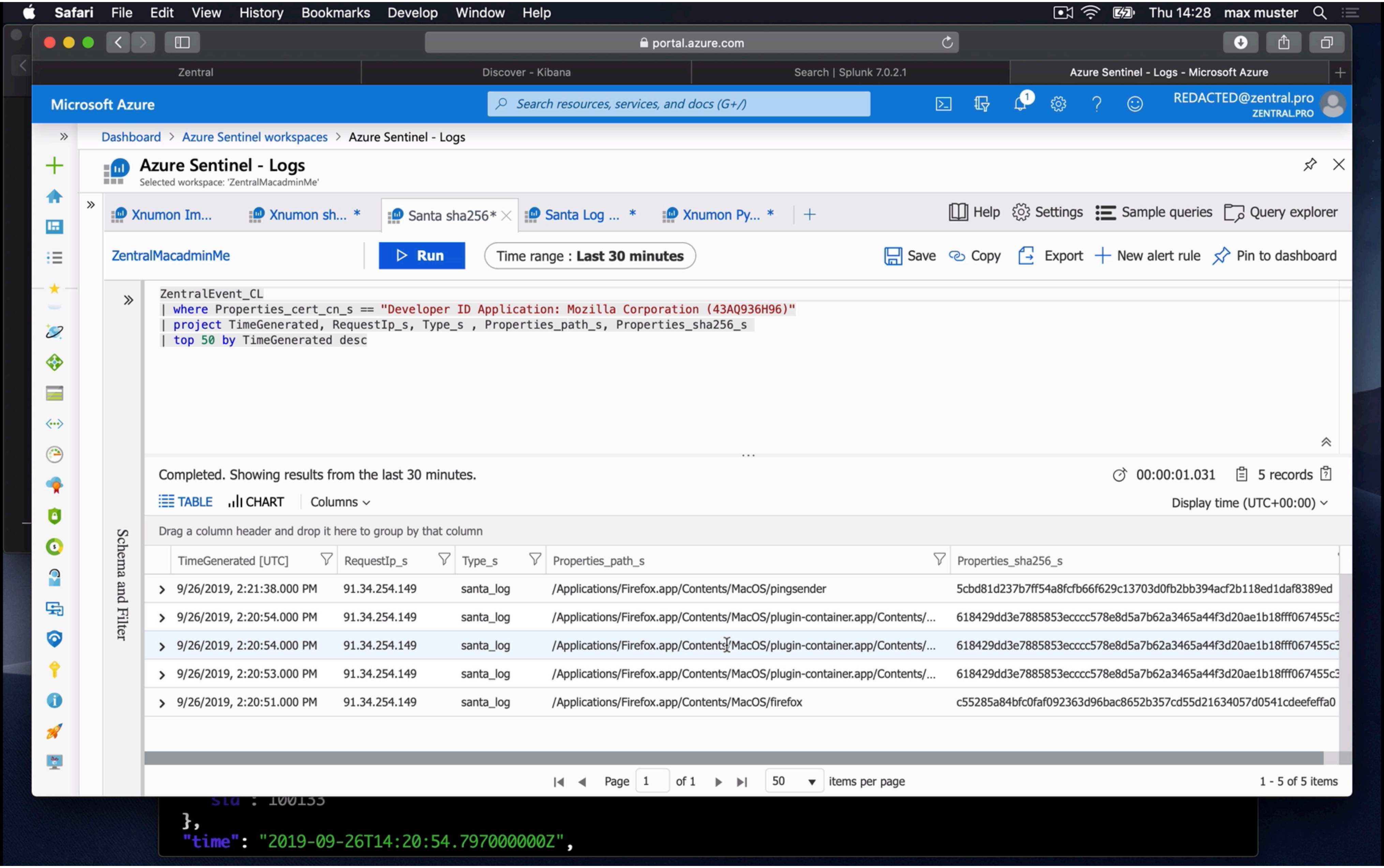
00:00:02.289 5 records

TABLE
CHART
Columns
Display time (UTC+00:00)
Drag a column header and drop it here to group by that column

TimeGenerated [UTC]	RequestIp_s	Type_s	Properties_image_path_s	Properties_image_sha256_s
9/26/2019, 2:21:38.000 PM	91.34.254.149	xnumon_image_exec	/Applications/Firefox.app/Contents/MacOS/pingsender	5cbd81d237b7ff54a8fcfb66f629c13703d0fb2bb394acf2b118ed1daf838.
9/26/2019, 2:20:54.000 PM	91.34.254.149	xnumon_image_exec	/Applications/Firefox.app/Contents/MacOS/plugin-container.app/Conte...	618429dd3e7885853ecccc578e8d5a7b62a3465a44f3d20ae1b18fff067...
9/26/2019, 2:20:54.000 PM	91.34.254.149	xnumon_image_exec	/Applications/Firefox.app/Contents/MacOS/plugin-container.app/Conte...	618429dd3e7885853ecccc578e8d5a7b62a3465a44f3d20ae1b18fff067...
9/26/2019, 2:20:53.000 PM	91.34.254.149	xnumon_image_exec	/Applications/Firefox.app/Contents/MacOS/plugin-container.app/Conte...	618429dd3e7885853ecccc578e8d5a7b62a3465a44f3d20ae1b18fff067...
9/26/2019, 2:20:51.000 PM	91.34.254.149	xnumon_image_exec	/Applications/Firefox.app/Contents/MacOS/firefox	c55285a84bfc0faf092363d96bac8652b357cd55d21634057d0541cdeef...

Page 1 of 1 50 items per page 1 - 5 of 5 items

```
    "sid": 100133
  },
  "time": "2019-09-26T14:20:54.797000000Z",
```



```
ZentralEvent_CL
| where Properties_cert_cn_s == "Developer ID Application: Mozilla Corporation (43AQ936H96)"
| project TimeGenerated, RequestIp_s, Type_s , Properties_path_s, Properties_sha256_s
| top 50 by TimeGenerated desc
```

Completed. Showing results from the last 30 minutes.

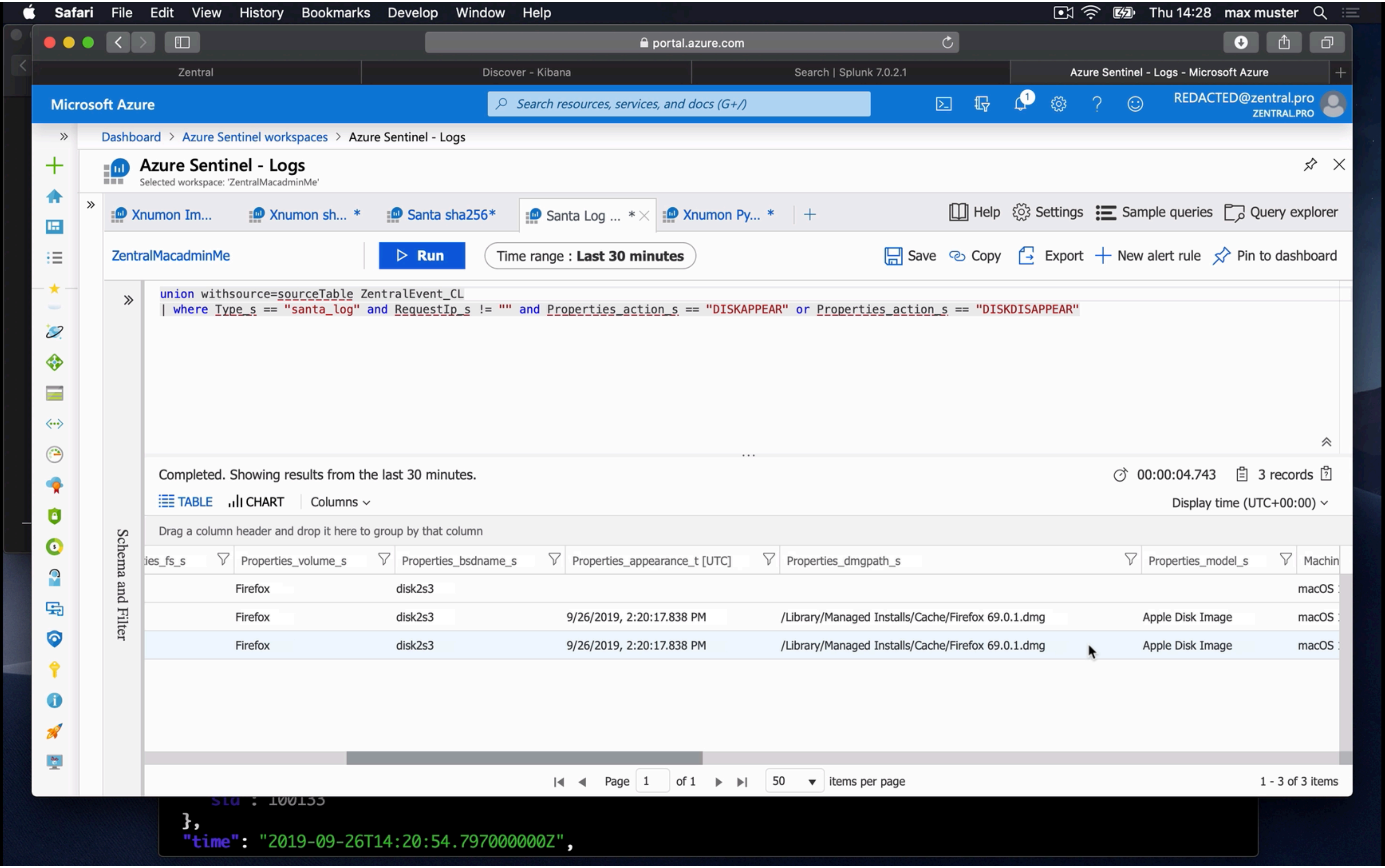
00:00:01.031 5 records

TABLE
CHART
Columns
Display time (UTC+00:00)
Drag a column header and drop it here to group by that column

TimeGenerated [UTC]	RequestIp_s	Type_s	Properties_path_s	Properties_sha256_s
9/26/2019, 2:21:38.000 PM	91.34.254.149	santa_log	/Applications/Firefox.app/Contents/MacOS/pingsender	5cbd81d237b7ff54a8fcfb66f629c13703d0fb2bb394acf2b118ed1daf8389ed
9/26/2019, 2:20:54.000 PM	91.34.254.149	santa_log	/Applications/Firefox.app/Contents/MacOS/plugin-container.app/Contents/...	618429dd3e7885853ecccc578e8d5a7b62a3465a44f3d20ae1b18fff067455c3
9/26/2019, 2:20:54.000 PM	91.34.254.149	santa_log	/Applications/Firefox.app/Contents/MacOS/plugin-container.app/Contents/...	618429dd3e7885853ecccc578e8d5a7b62a3465a44f3d20ae1b18fff067455c3
9/26/2019, 2:20:53.000 PM	91.34.254.149	santa_log	/Applications/Firefox.app/Contents/MacOS/plugin-container.app/Contents/...	618429dd3e7885853ecccc578e8d5a7b62a3465a44f3d20ae1b18fff067455c3
9/26/2019, 2:20:51.000 PM	91.34.254.149	santa_log	/Applications/Firefox.app/Contents/MacOS/firefox	c55285a84bfc0faf092363d96bac8652b357cd55d21634057d0541cdeefeffa0

Page 1 of 1 50 items per page 1 - 5 of 5 items

```
   "sid": 100133
 },
 "time": "2019-09-26T14:20:54.797000000Z",
```



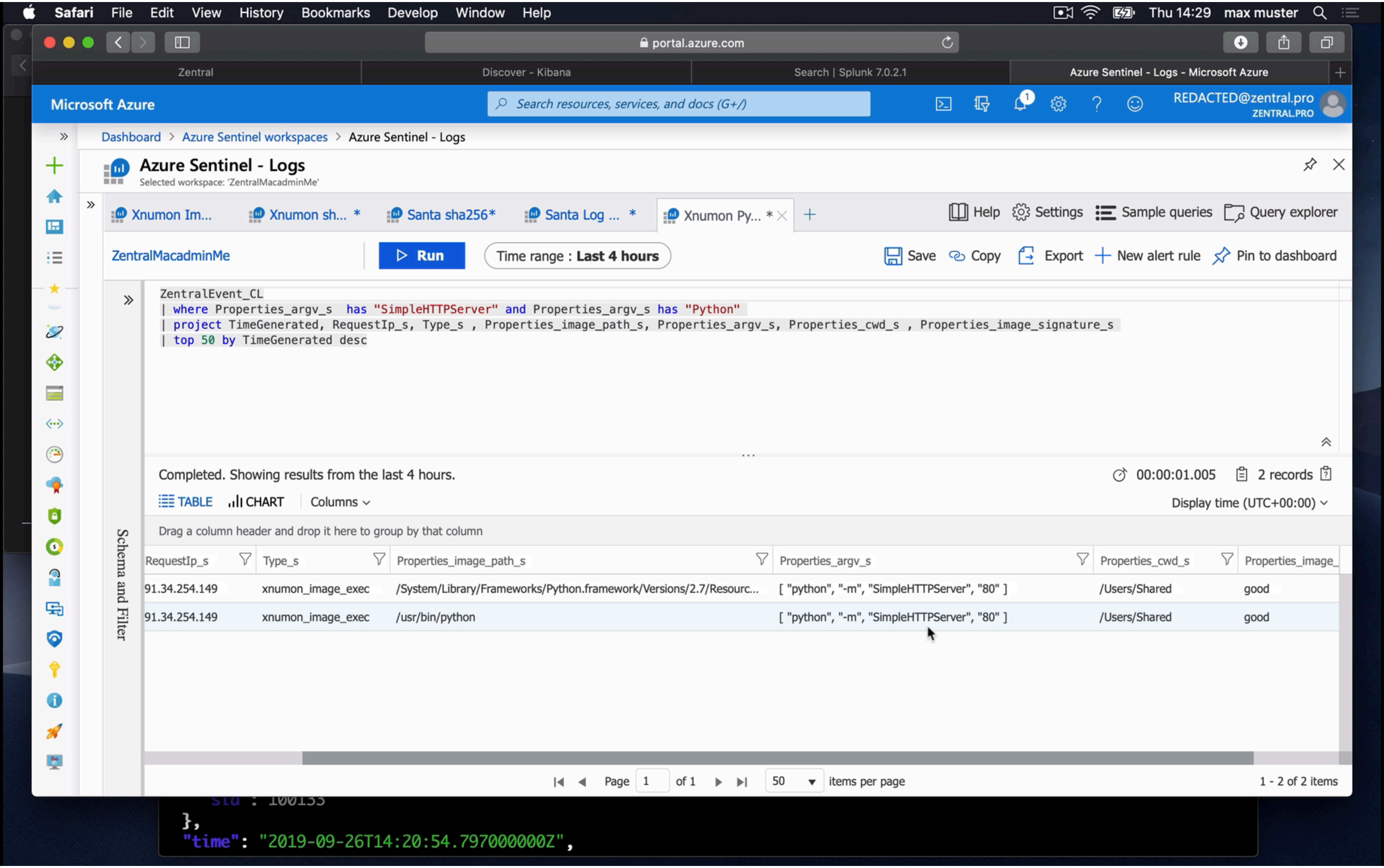
```
union withsource=sourceTable ZentralEvent_CL
| where Type_s == "santa_log" and RequestIp_s != "" and Properties_action_s == "DISKAPPEAR" or Properties_action_s == "DISKDISAPPEAR"
```

Completed. Showing results from the last 30 minutes.

00:00:04.743 3 records

ies_fs_s	Properties_volume_s	Properties_bsdname_s	Properties_appearance_t [UTC]	Properties_dmgpath_s	Properties_model_s	Machin
	Firefox	disk2s3				macOS
	Firefox	disk2s3	9/26/2019, 2:20:17.838 PM	/Library/Managed Installs/Cache/Firefox 69.0.1.dmg	Apple Disk Image	macOS
	Firefox	disk2s3	9/26/2019, 2:20:17.838 PM	/Library/Managed Installs/Cache/Firefox 69.0.1.dmg	Apple Disk Image	macOS

```
    "sid": 100133
  },
  "time": "2019-09-26T14:20:54.7970000000Z",
```



Time range : **Last 4 hours**

```
ZentralEvent_CL
| where Properties_argv_s  has "SimpleHTTPServer" and Properties_argv_s has "Python"
| project TimeGenerated, RequestIp_s, Type_s , Properties_image_path_s, Properties_argv_s, Properties_cwd_s , Properties_image_signature_s
| top 50 by TimeGenerated desc
```

Completed. Showing results from the last 4 hours.

00:00:01.005 2 records

Display time (UTC+00:00)

RequestIp_s	Type_s	Properties_image_path_s	Properties_argv_s	Properties_cwd_s	Properties_image_
91.34.254.149	xnumon_image_exec	/System/Library/Frameworks/Python.framework/Versions/2.7/Resourc...	["python", "-m", "SimpleHTTPServer", "80"]	/Users/Shared	good
91.34.254.149	xnumon_image_exec	/usr/bin/python	["python", "-m", "SimpleHTTPServer", "80"]	/Users/Shared	good

```
    "sid": 100133
  },
  "time": "2019-09-26T14:20:54.7970000000Z",
```

Ship and collect the events

How to connect the sources

- Server / Cloud
  - Log analytics

Commercial Log Analytics

- SumoLogic
- Splunk
- DataDog
- Elastic Cloud

et.al

Benefits

- Managed Platform
- High volume capability
- Cost based on volume

Ship and collect the events

How to connect the sources

- Server / Cloud
  - EDR / SIEM Solutions

Commercial SIEM

- ArcSite
- Azure Sentinel
- Chronicle Security
- PaloAlto Cortex XDR
- Q-Radar (IBM)

et.al

Benefits

- Managed Platform
- High volume capability

Conclusion

Conclusion

What can be improved

- Benefits / Next Level

- Better organize event aggregation
- Consolidate data in Event Hubs
- SIEM alerting, Machine Learning
  (too many sign-in errors, …)
- Bring together the admins and the security engineers

Conclusion

What can be improved

- Benefits / Next Level

“Bring together the admins and the security engineers“

zentral.pro

https://github.com/zentralopensource/MacSysAdmin-Conference-2019

Thank you !

Q & A

https://int.zentral.pro

Support our open source development

https://www.patreon.com/zentral

✉ hi@zentral.pro

🌐 https://int.zentral.pro

🐦 zentral_io

zentral.pro

MacSysAdmin 2019

zentral.pro