



Zentral

Open hub for monitoring

20. April 2017 London Apple Admin Meetup



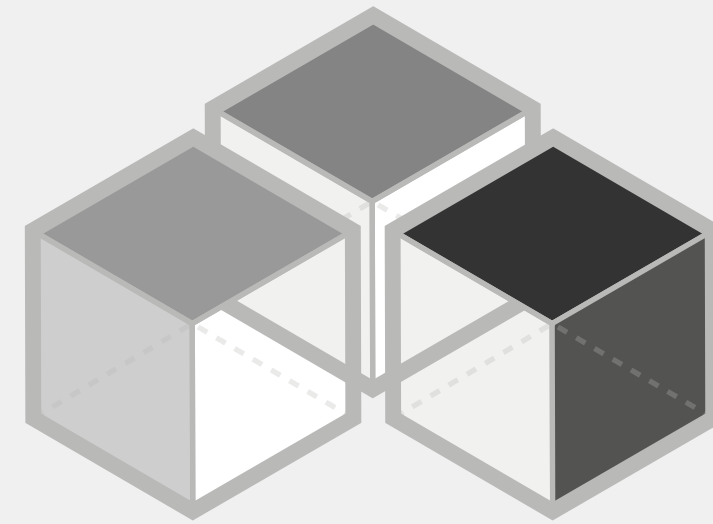
event stream processing
and alerting



solution to verify integrity
and monitor endpoints

Framework

- Organised deployment of open source tools
- Modular architecture
- Python3 / Django



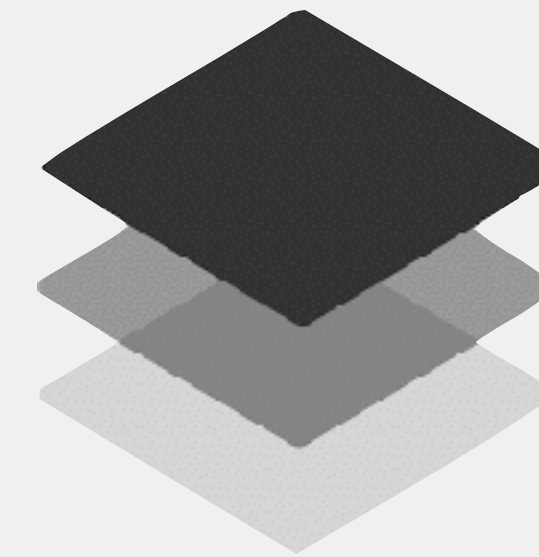
TLS server

- Event logging APIs
- Dedicated log / configuration for Osquery & Santa



Inventory

- Multiple sources
- Parallel processing
- Store change history



Zentral -
open hub for monitoring

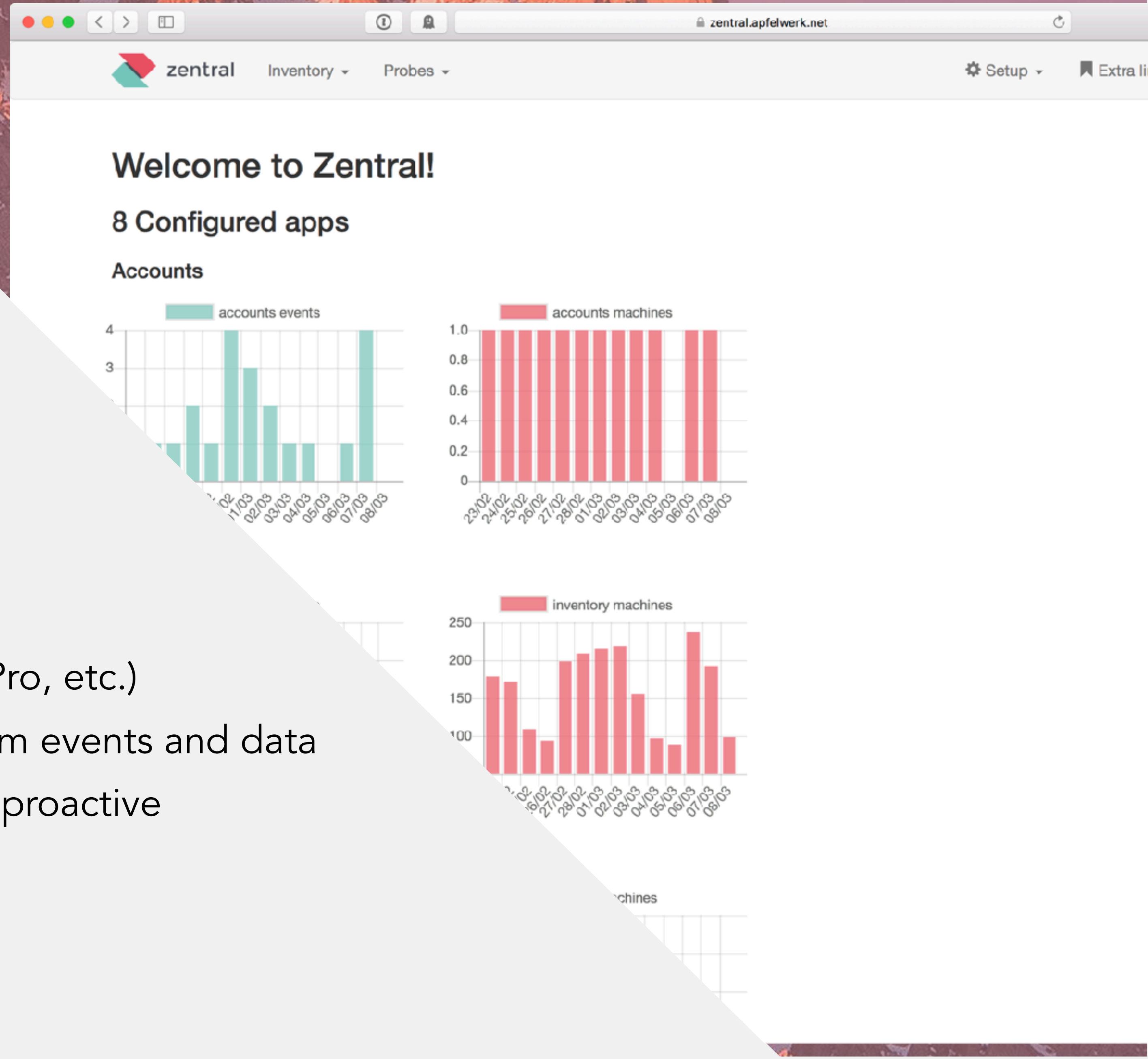


Zentral

Open hub for monitoring

Monitor events / link to an inventory setup:

1. Enroll devices and connect inventory (JamfPro, etc.)
2. Near-real-time capture and analysis of system events and data
3. Run probes for event filtering, alerting, and proactive automations (IFTTT)



Elastic Stack

Database, log aggregation, visualization



elasticsearch



logstash



kibana



Osquery

Intrusion detection, infrastructure reliability,
and compliance

- Sync config, push events to Zentral (TLS server)
- Low-level operating system analytics
- Query system state with simple SQL syntax
- Distributed queries, file integrity monitoring (FIM)

```
head — osqueryi — osqueryi — osqueryi — 87x45
osquery> select key, datetime(value, 'unixepoch') as last_update, cast(julianday('now')
- julianday(datetime(value, 'unixepoch'))) as int) as days_ago from preferences where p
ath = '/Library/Preferences/com.apple.SoftwareUpdate.plist' and key like '%Date';
+-----+-----+-----+
| key | last_update | days_ago |
+-----+-----+-----+
| LastFullSuccessfulDate | 2017-03-04 13:32:59 | 0 |
| LastBackgroundSuccessfulDate | 2017-03-04 13:33:55 | 0 |
| LastSuccessfulDate | 2017-03-04 15:08:05 | 0 |
+-----+-----+-----+
osquery> _
```

```
head — osqueryi — osqueryi — osqueryi — 87x45
[osquery> select * from sip_config;
+-----+-----+-----+
| config_flag | enabled | enabled_nvram |
+-----+-----+-----+
| sip | 1 | 1 |
| allow_apple_internal | 0 | 0 |
| allow_device_configuration | 0 | 0 |
| allow_kernel_debugger | 0 | 0 |
| allow_task_for_pid | 0 | 0 |
| allow_unrestricted_dtrace | 0 | 0 |
| allow_unrestricted_fs | 0 | 0 |
| allow_unrestricted_nvram | 0 | 0 |
| allow_untrusted_kexts | 0 | 0 |
+-----+-----+-----+
osquery> _
```




Google Santa

Binary logging, blacklisting/whitelisting
for macOS

- Sync config, push events to Zentral (TLS server)
- All binary launches are logged
- Client mode: MONITOR
- Client mode: LOCKDOWN (defaults deny)

```
MacBook-Dev:~ std$ santactl fileinfo /Applications/Android\ Studio.app
Path                : /Applications/Android Studio.app/Contents/MacOS/studio
SHA-256             : 346f84d059d652674bbb51c7692005d527cbd6461d3c7d92eb77bd1b88c87500
SHA-1               : 92fd1c9ad1e295b1c35f08e972aea9a1d008c442
Bundle Name         : Android Studio
Bundle Version      : AI-162.3764568
Bundle Version Str  : 2.3
Type                : Executable (x86-64, i386)
Code-signed         : Yes
Rule                : Whitelisted (Certificate)
Signing Chain:
  1. SHA-256         : 33b9aee3b089c922952c9240a40a0daa271bebf192cf3f7d964722e8f2170e48
     SHA-1           : 34f0bdf7f87d4f3a955862c351472e52250e4c2b
     Common Name     : Developer ID Application: Google, Inc. (EQHXZ8M8AV)
     Organization    : Google, Inc.
     Organizational Unit :
     From            :
     Mail            :
     :
     :
     :
     :
     :
```

Santa

The following application has been blocked from executing
because its trustworthiness cannot be determined.

Filename	Path
jspawnhelper	/Applications/Android Studio.app/Contents/jre/ jdk/Contents/Home/jre/lib/jspawnhelper
	Not code-signed
	ba60ef8fffb373cd1ae047368146ab8d8 fdb03e8a08fb31125544a04cc567b0f
	hd (1)

this application for a day



Probe

Bundle filters, actions and optional configuration

- Filter on events, inventory, metadata
- Organize Santa rules or Osquery SQL (dynamic config)
- Control and minimize event overhead
- Trigger actions (API calls, notify)
- Export, share as Gist (GitHub)

The screenshot shows the Zentral web interface. The top navigation bar includes the Zentral logo, 'Inventory', and 'Probes'. The breadcrumb trail is 'Home / Probes / 1Password security settings'. The main heading is 'Probe 1Password security settings'. Below this, there are three rows of configuration: 'status' set to 'Active', 'feed' set to 'Osquery demo', and 'feed probe' set to '1Password security settings'. A toolbar contains icons for a document, a trash can, 'Events', 'Dashboard', 'elasticsearch', and 'Export gist'. Below the toolbar are sections for 'Filters' (with an 'Add filter' button), 'Osquery compliance' (with an 'Add' button), and 'Preference file'. The preference file path is '/Users/%/Library/Preferences/2BUA8C4S2C.com.agilebits.onepassword4-helper.plist'. A table lists several preferences, all set to 1, including 'ClearPasteboardAfterTimeout', 'ConcealPasswords', 'Idle', and 'ScreenSaver'. The table also shows constraints like 'integer ≤ 5' and 'integer ≤ 90', and a note 'Agilebits recommended defaults'.

Preference	Value
ClearPasteboardAfterTimeout	= 1
ConcealPasswords	= 1
Idle	= 1
ScreenSaver	= 1
	= 1
	= 1
	integer ≤ 5
	integer ≤ 90
Agilebits recommended defaults	



Open hub for deployed tools

Combine powerful existing tools to meet your operational requirements



JamfPro

Client management
Inventory
MDM solution



Munki

Munki

Client management
Inventory



Filewave

Client management
Inventory



Watchman Monitoring

Health monitoring
agent

Supported inventory



Open hub for deployed tools

Combine powerful existing tools to meet your operational requirements



Slack

Team chat
notifications



Trello

Kanban Board
workflows



Zendesk

Ticketing system
workflows



Jira

Ticketing system
workflows

Supported actions

+ actions / notifications available for
GitHub, Email, SMS, Push Notifications,...

Workshop / Demo





Deployment options



GoogleCloudPlatform

zentral-all-in-one image

SaaS Zentral
+ Support contract

production



Amazon AWS

zentral-all-in-one AMI

SaaS Zentral
+ Support contract

production



Docker

Docker-Compose
(development env)



OVA / Vagrant

VMware ESXi / vSphere
+ on prem support
option

Vagrant (eval)

Combine tools & meet operational requirements

- Integrate services already deployed
- Enhance control and monitor endpoints
- Tight integration with JamfPro and other APIs
- Combine system monitoring and automation
- Full audit trail for management frameworks



Flexible, proactive, actionable



Service / Support

- SaaS (Cloud based service)
- Professional services, custom development
- Integration support (on premise)

Community support via github (free)

Paid support / integration / development (on request)



info@zentral.io



Thank you !