Логирование

Эдуард Медведев
@ohaithear

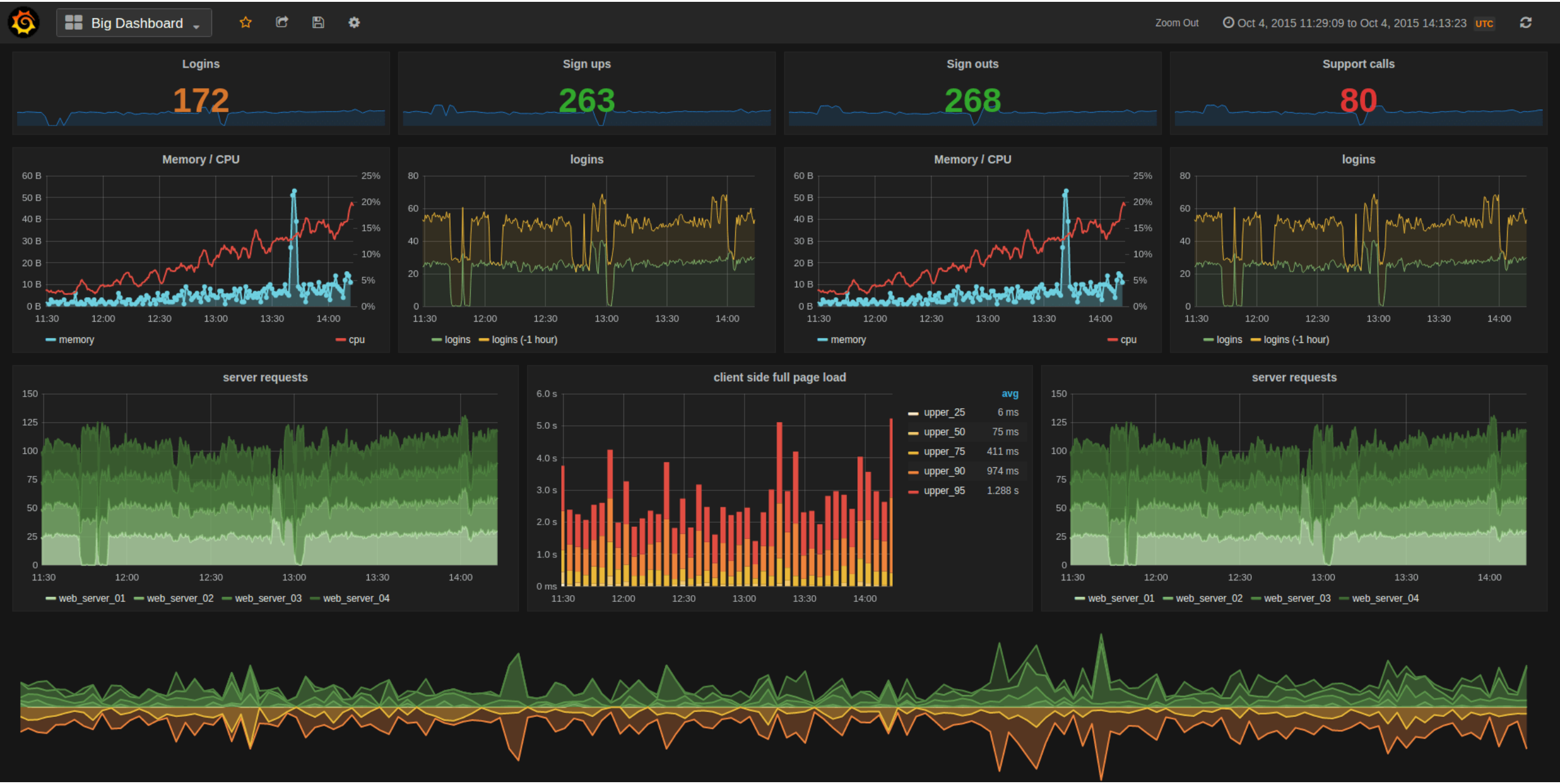
slurm.io

Мониторинг
Трейсинг
Логирование

Мониторинг

- Сбор метрик
- Изменение параметров системы во времени
- Диагностика и реагирование на аномалии

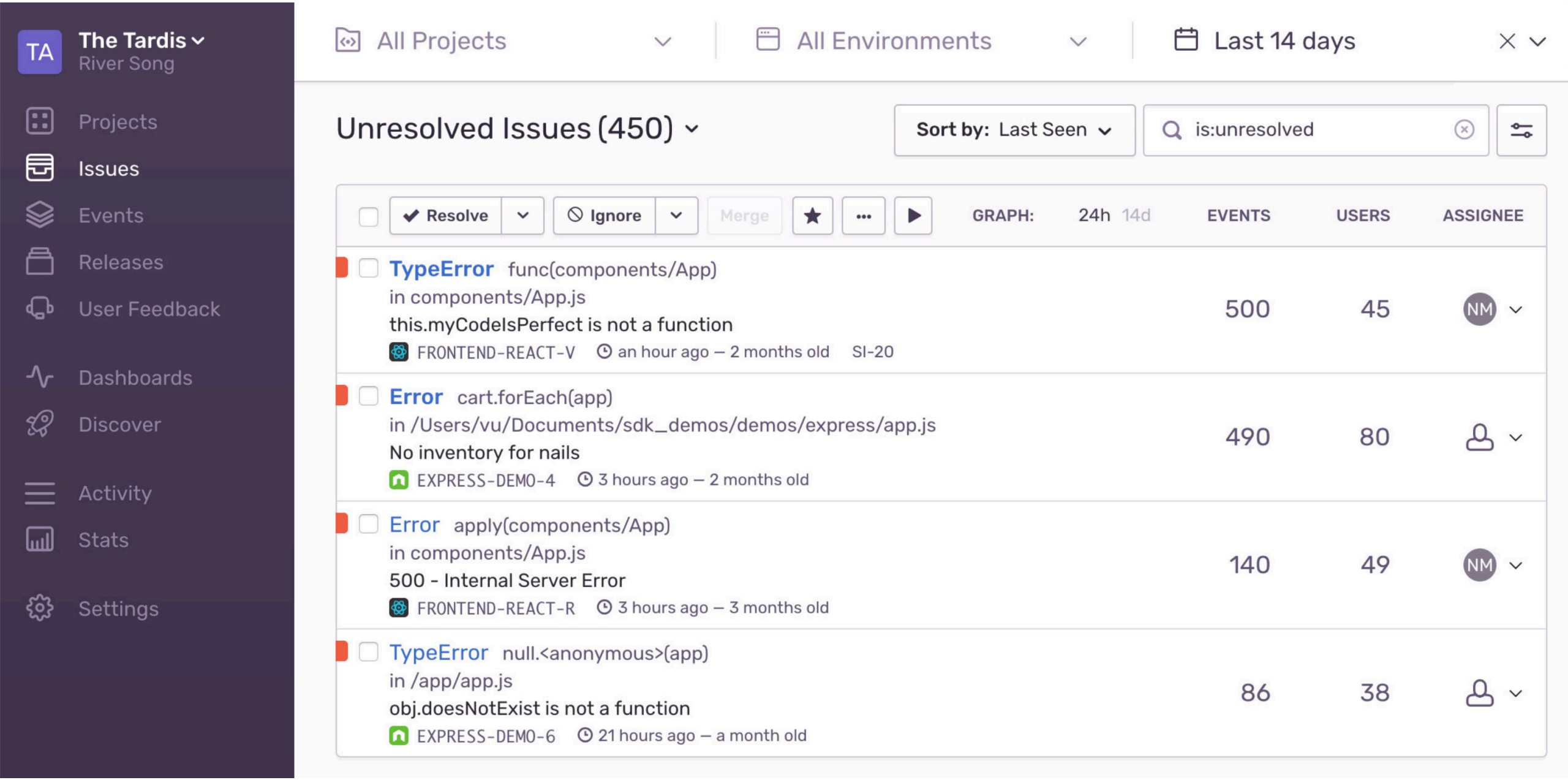
СЛЁРМ


Big Dashboard
Zoom Out
Oct 4, 2015 11:29:09 to Oct 4, 2015 14:13:23
UTC
Logins
172
Sign ups
263
Sign outs
268
Support calls
80
Memory / CPU
logins
Memory / CPU
logins
memory
cpu
logins
logins (-1 hour)
server requests
client side full page load
avg
upper_25 6 ms
upper_50 75 ms
upper_75 411 ms
upper_90 974 ms
upper_95 1.288 s
server requests
web_server_01
web_server_02
web_server_03
web_server_04

Трейсинг

- Информация о «пути» выполнения кода
- Чаще всего — трейсинг ошибок
- Определение проблемного этапа

СЛЁРМ


TA
The Tardis
River Song
Projects
Issues
Events
Releases
User Feedback
Dashboards
Discover
Activity
Stats
Settings
All Projects
All Environments
Last 14 days
Unresolved Issues (450)
Sort by: Last Seen
is:unresolved
Resolve
Ignore
Merge
GRAPH:
24h
14d
EVENTS
USERS
ASSIGNEE
TypeError func(components/App)
in components/App.js
this.myCodeIsPerfect is not a function
FRONTEND-REACT-V
an hour ago — 2 months old
SI-20
500
45
NM
Error cart.forEach(app)
in /Users/vu/Documents/sdk_demos/demos/express/app.js
No inventory for nails
EXPRESS-DEMO-4
3 hours ago — 2 months old
490
80
Error apply(components/App)
in components/App.js
500 - Internal Server Error
FRONTEND-REACT-R
3 hours ago — 3 months old
140
49
NM
TypeError null.<anonymous>(app)
in /app/app.js
obj.doesNotExist is not a function
EXPRESS-DEMO-6
21 hours ago — a month old
86
38

Логирование

- Сбор информации о событиях
- Отслеживает изменения состояния
- Дает широкий контекст

СЛЁРМ

Discover
Visualize
Dashboard
Timelion
Machine Learning
Graph
Dev Tools
Monitoring
Management

logstash-*

Selected Fields

? _source

Available Fields

Popular

t host

t **machine.os** add

Top 5 values in 456 / 500 records

ios 25.0%

win 7 23.5%

win xp 21.7%

win 8 20.8%

osx 9.0%

t @message

t @tags

@timestamp

t _id

t _index

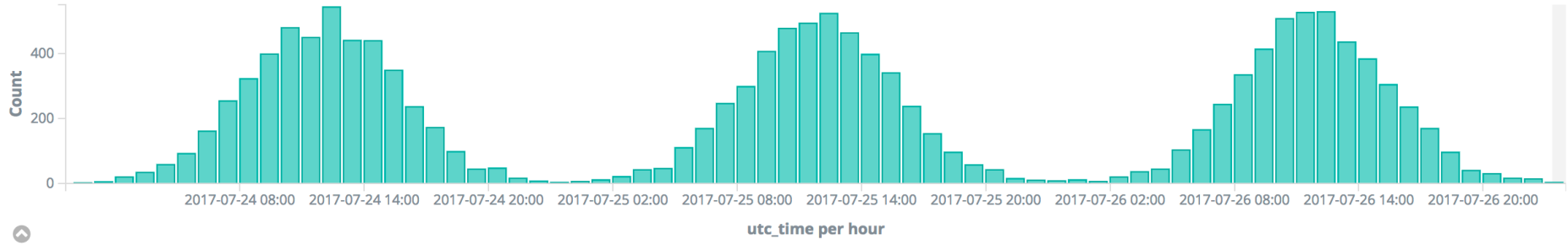
_score

t _type

t agent

bytes

July 23rd 2017, 23:35:39.000 - July 26th 2017, 23:20:22.000 — Auto



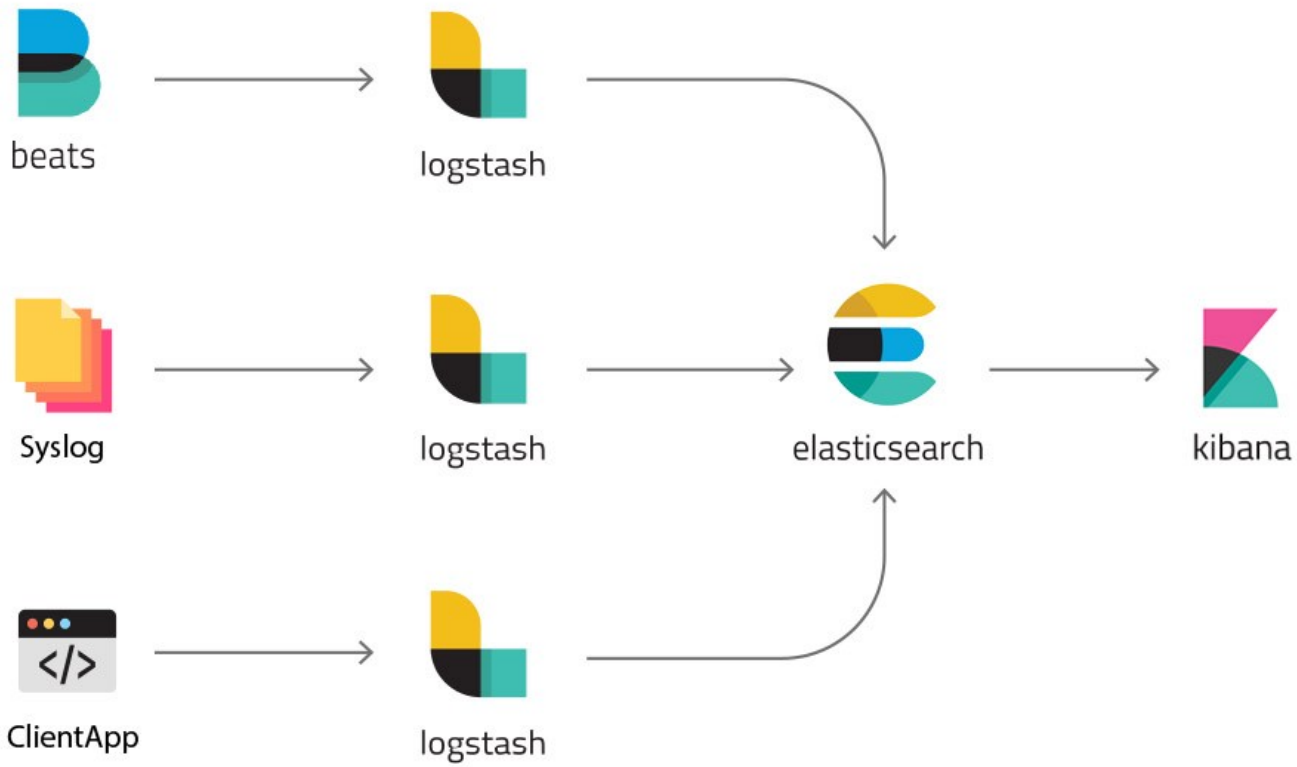
Time	_source
July 26th 2017, 23:16:12.701	**index:** logstash-0 **@timestamp:** July 26th 2017, 23:16:12.701 **ip:** 164.29.124.90 **extension:** jpg **response:** 200 **geo.coordinates:** { "lat": 46.91630556, "lon": -114.0905556 } **geo.src:** IN **geo.dest:** PE **geo.srcdest:** IN:PE **@tags:** success, info **utc_time:** July 26th 2017, 23:16:12.701 **referer:** http://www.slate.com/success/daniel-burbank **agent:** Mozilla/5.0 (X11; Linux x86_64; rv:6.0a1) Gecko/20110421 Firefox/6.0a1 **clientip:** 164.29.124.90 **bytes:** 4,250 **host:** media-for-the-masses.theacademyofperformingartsandscience.org **request:** /uploads/liu-yang.jpg **url:** https://media-for-the-masses.theacademyofperformingartsandscience.org/uploads/liu-yang.jpg
July 26th 2017, 23:09:27.796	**index:** logstash-0 **@timestamp:** July 26th 2017, 23:09:27.796 **ip:** 207.65.182.104 **extension:** jpg **response:** 200 **geo.coordinates:** { "lat": 39.78525, "lon": -104.5431389 } **geo.src:** NP **geo.dest:** PK **geo.srcdest:** NP:PK **@tags:** warning, security **utc_time:** July 26th 2017, 23:09:27.796 **referer:** http://www.slate.com/success/richard-truly **agent:** Mozilla/5.0 (X11; Linux x86_64; rv:6.0a1) Gecko/20110421 Firefox/6.0a1 **clientip:** 207.65.182.104 **bytes:** 2,600 **host:** media-for-the-masses.theacademyofperformingartsandscience.org **request:** /uploads/hans-schlegel.jpg **url:** https://media-for-the-masses.theacademyofperformingartsandscience.org/uploads/hans-schle
July 26th 2017, 23:07:24.502	**index:** logstash-0 **@timestamp:** July 26th 2017, 23:07:24.502 **ip:** 63.111.75.67 **extension:** css **response:** 200 **geo.coordinates:** { "lat": 36.43243111, "lon": -81.41968472 } **geo.src:** TZ **geo.dest:** US **geo.srcdest:** TZ:US **@tags:** warning, info **utc_time:** July 26th 2017, 23:07:24.502 **referer:** http://www.slate.com/success/valentin-lebedev **agent:** Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322) **clientip:** 63.111.75.67 **bytes:** 6,730 **host:** cdn.theacademyofperformingartsandscience.org **request:** /styles/pretty-layout.css **url:** https://cdn.theacademyofperformingartsandscience.org/styles/pretty-layout.css **@message:** 63.111.75.67 -
July 26th 2017, 22:56:49.931	**index:** logstash-0 **@timestamp:** July 26th 2017, 22:56:49.931 **ip:** 254.119.28.102 **extension:** png **response:** 200 **geo.coordinates:** { "lat": 42.75840889, "lon": -74.13290472 } **geo.src:** IN **geo.dest:** PH **geo.srcdest:** IN:PH **@tags:** success, info **utc_time:** July 26th 2017, 22:56:49.931 **referer:** http://www.slate.com/success/vladimir-titov **agent:** Mozilla/5.0 (X11; Linux i686) AppleWebKit/534.24 (KHTML, like Gecko) Chrome/11.0.696.50 Safari/534.24 **clientip:** 254.119.28.102 **bytes:** 2,218 **host:** media-for-the-masses.theacademyofperformingartsandscience.org **request:** /uploads/william-gregory.png **url:** https://media-for-the-masses.theacademyofperformingarts
July 26th 2017, 22:48:14.086	**index:** logstash-0 **@timestamp:** July 26th 2017, 22:48:14.086 **ip:** 41.252.90.54 **extension:** jpg **response:** 200 **geo.coordinates:** {

The Elastic Stack

ELK Stack

- **E**lasticsearch: хранение и поиск
- **L**ogstash: сбор данных
- **K**ibana: отображение и аналитика

СЛЁРМ


beats
logstash
Syslog
logstash
elasticsearch
kibana
ClientApp
logstash

~~ELK~~ EFK Stack

- **E**lasticsearch: хранение и поиск
- ~~Logstash~~ **F**luentd: сбор данных
- **K**ibana: отображение и аналитика

СЛЁРМ

Fluentd

- Легче, меньше зависимостей
- Больше плагинов
- Удобный синтаксис (но это не точно)
- Экспорт совместим с Logstash

СЛЁРМ

The Elastic Stack++

Open Distro

- Безопасность (Active Directory, аудит, шифрование)
- Мониторинг и алертинг
- SQL-запросы
- Диагностика
- Open source (Apache 2.0): opendistro.github.io

СЛЁРМ

X-pack

- Безопасность
- Мониторинг и алертинг
- Построение графов
- Машинное обучение (тренды)
- Платный: elastic.co/downloads/x-pack

СЛЁРМ

Практика

Best Practices

Хранение

- В другой availability zone
- Крупные предприятия: ~2–4 Гб данных в день

СЛЁРМ

Использование

- Хранимые логи должны быть полезными
- Создайте дэшборды для общего пользования

СЛЁРМ

Ревью

- Тестируйте логи!
- Проводите периодические ревью

СЛЁРМ

Безопасность

СЛЁРМ


Mar 26, 2018 - Kathy Wang
Summary of limited GitLab credentials exposed in an internal logging system
Some GitLab.com personal access tokens and third-party credentials were inadvertently exposed publicly. This has since been resolved and all affected users notified. Read on for more details.

[GitHub Security] Please reset your password

Today at 1:24 AM

Hi there,

During the course of regular auditing, GitHub discovered that a recently introduced bug exposed a small number of users' passwords to our internal logging system, including yours. We have corrected this, but you'll need to reset your password to regain access to your account.


СЛЁРМ

Keeping your account secure

When you set a password for your Twitter account, we use technology that masks it so no one at the company can see it. We recently identified a bug that stored passwords unmasked in an internal log. We have fixed the bug, and our investigation shows no indication of breach or misuse by anyone.


СЛЁРМ

Безопасность

- **Что попадает в логи?**
- У кого есть доступ к логам? Есть ли аудит?
- Соответствие законодательству (152-ФЗ, GDPR)

Бонус: Чек-лист для ревью логов

- Полезны ли эти записи?
- Достаточно ли в записях контекста?
- Хорошо ли записи структурированы?
- Правильно ли назначена важность?
- Содержат ли записи персональные данные?
- Если запись требует действия, есть ли алерт?

СЛЁРМ

Спасибо!

Эдуард Медведев
@ohaithear

slurm.io