

Elastic Meetup Changsha #1



Introduction to Elastic

What is Elastic?

Platform around a distributed data store

elastic


Documents


Social


Logs


User Activity


Location


Sensor



Search



GitHub

Goldman Sachs

Logging

verizon

DHL

NETFLIX

Analytics

Eventbrite

theguardian

salesforce

Security

USAA

CISCO

tinder

Metrics

NASA JPL

BLIZZARD ENTERTAINMENT

RIOT GAMES

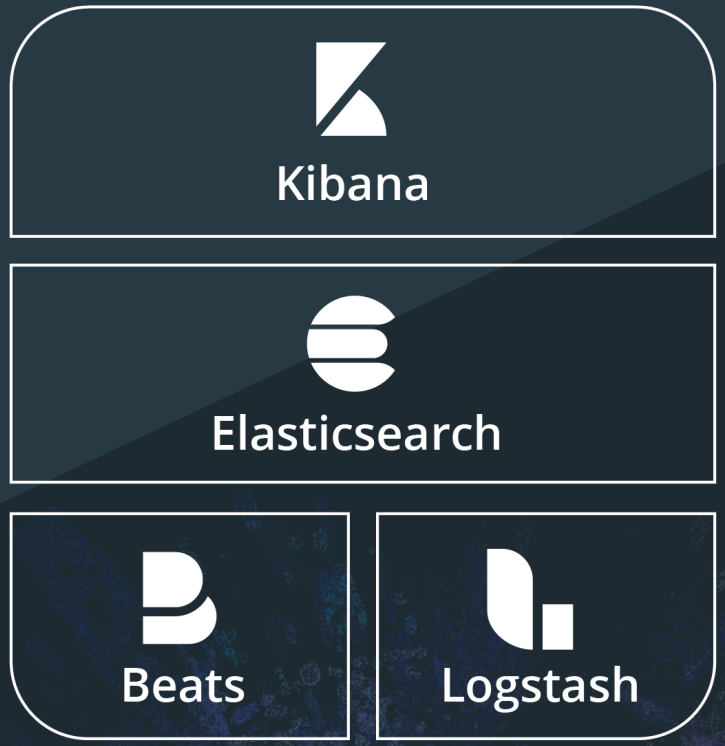
elastic

1.5亿+

自2012下载次数

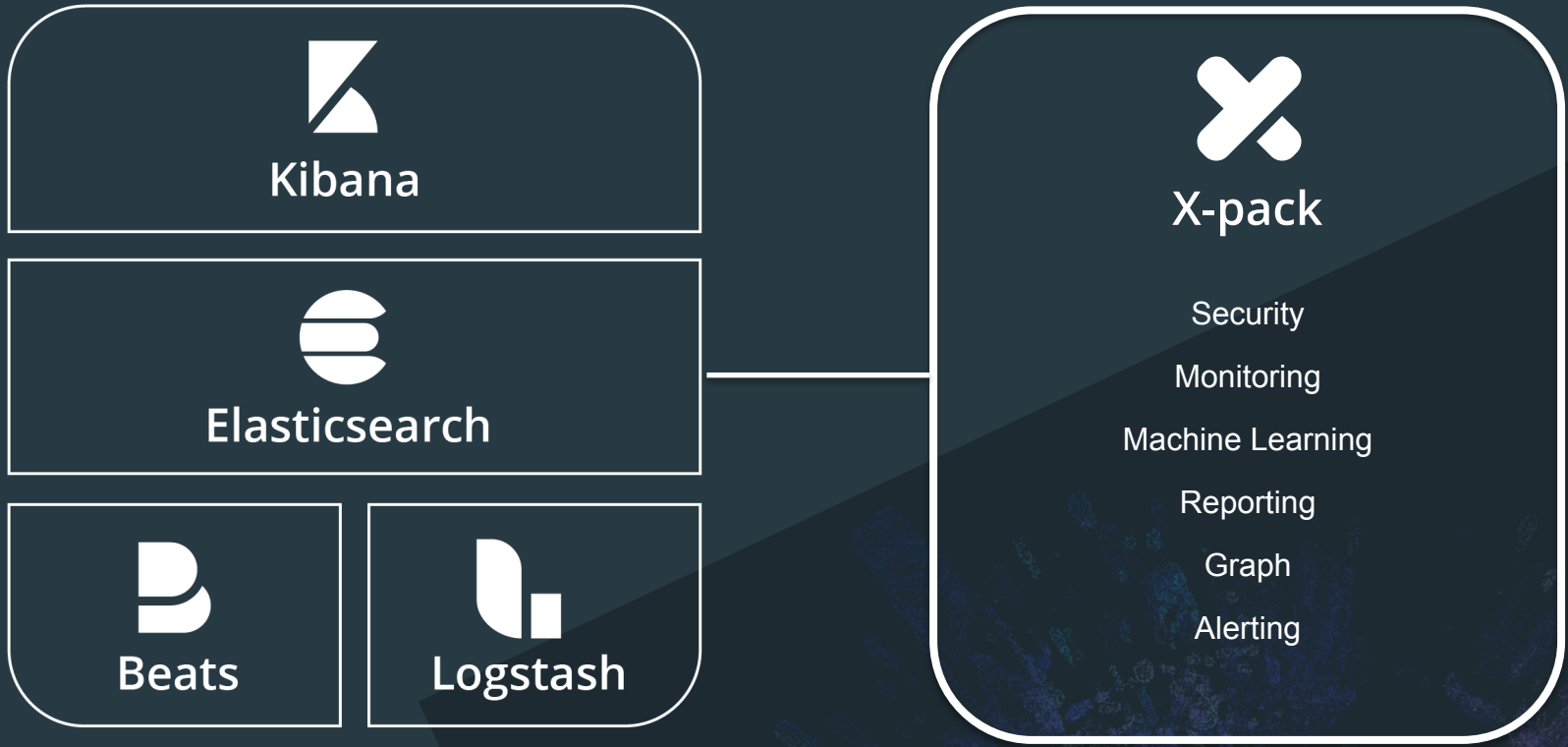
10万+

社区成员遍布全球
100 多个国家

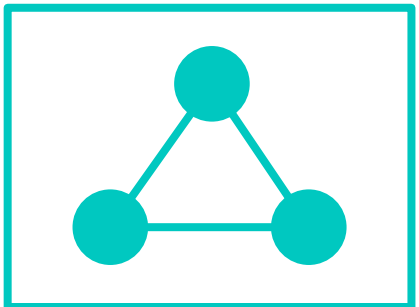



中国的下载总数
下载
6,000,000
4,000,000
2,000,000
1,000,000
0
2015
2016
2017
年度


阿里云
elastic


Kibana
Elasticsearch
Beats
Logstash
X-pack
Security
Monitoring
Machine Learning
Reporting
Graph
Alerting

Elasticsearch: Store, Index & Analyze



Distributed

Scaleable

Highly Available



API

JSON

Language clients



Search

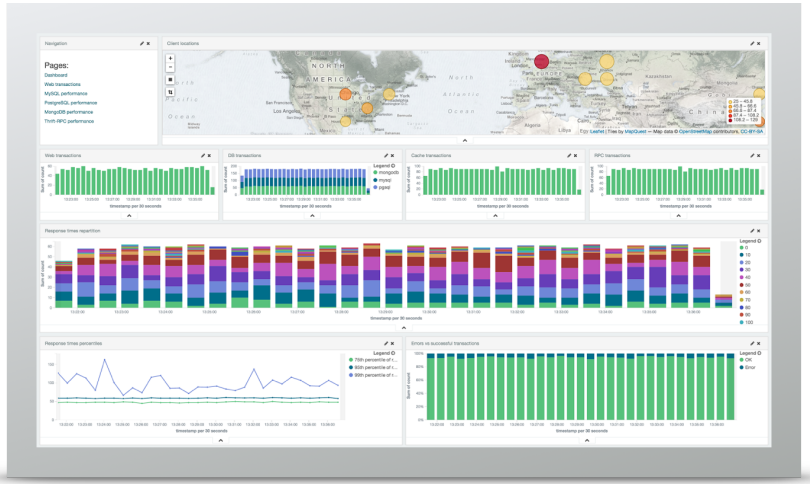
Aggregations

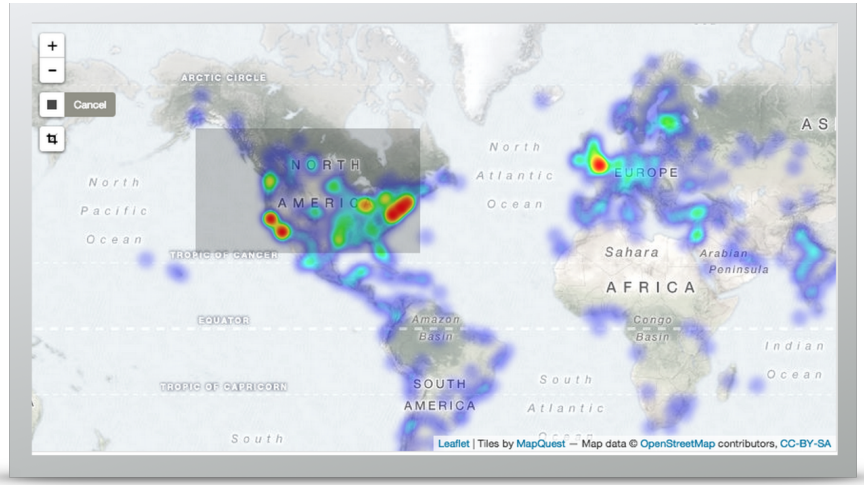
Geospatial

elastic

Visualize and Explore

kibana





Easily create bar charts, line and scatter plots, histograms, pie charts, and maps

elastic

Ingest

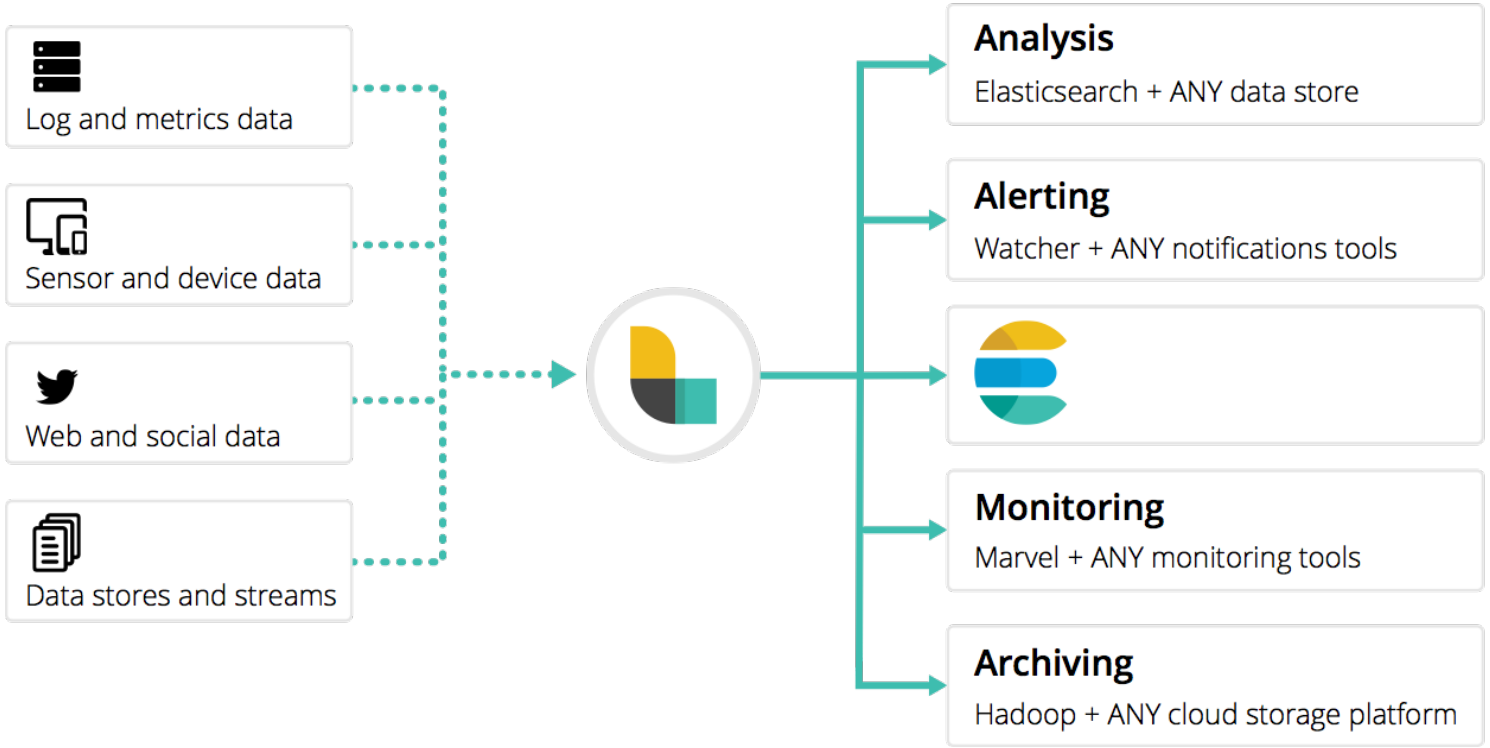




ES-Hadoop

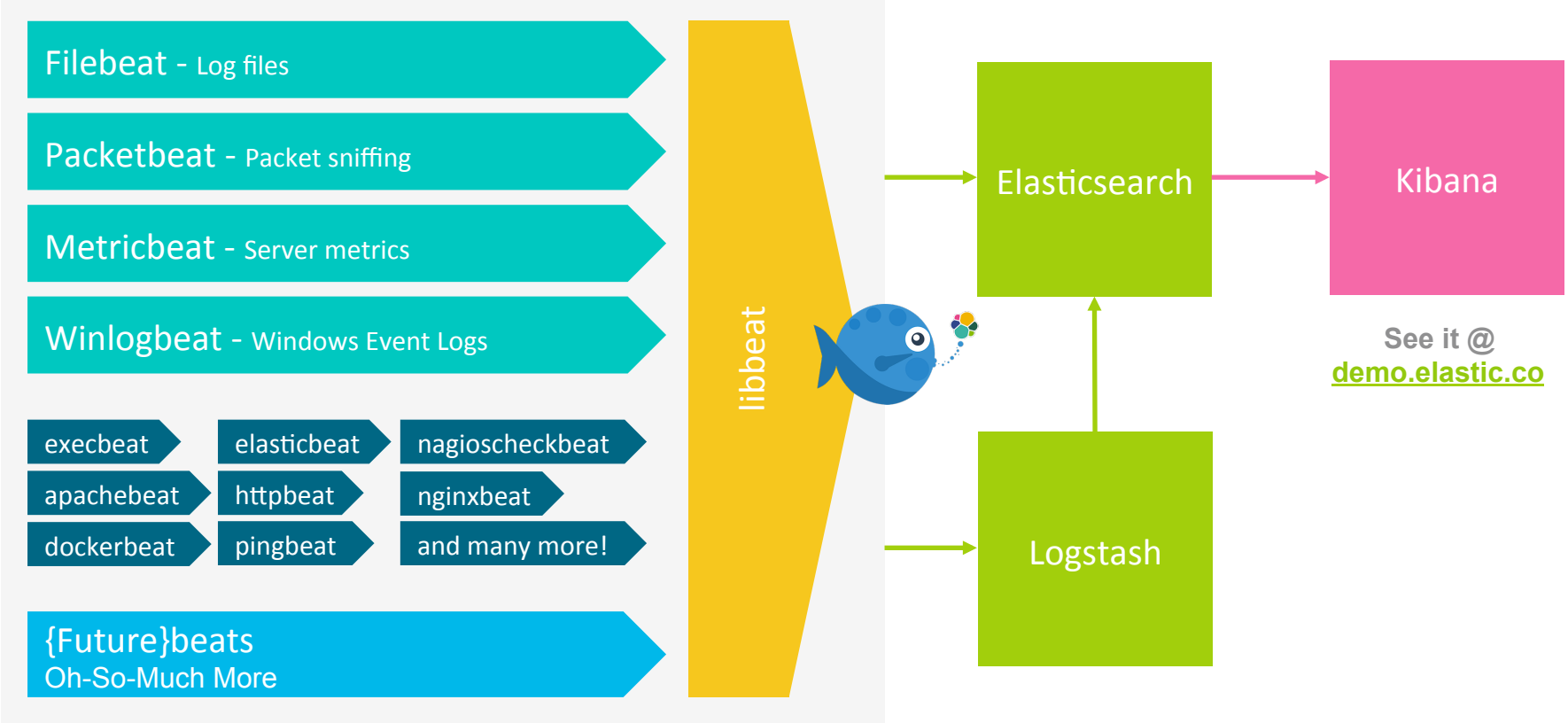
Collect, Enrich, and Transport

logstash



elastic

Beats: Lightweight Data Shippers



elastic

x-pack A Single Extension

Security

Security for the Elastic Stack (Shield)

Alerting

Notifications for the Elastic Stack (Watcher)

Monitoring

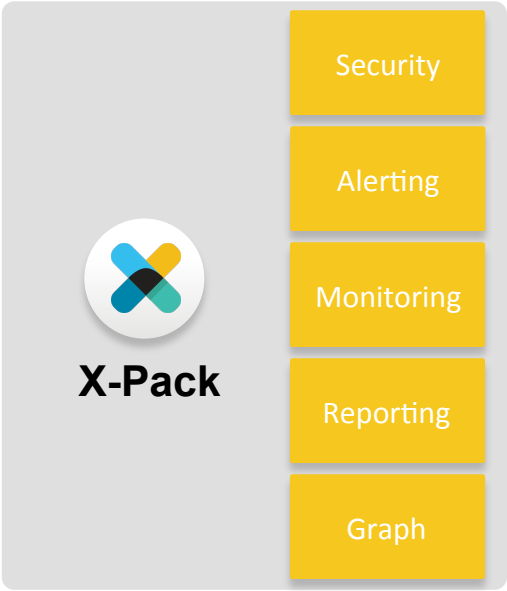
Monitoring for the Elastic Stack (Marvel)

Reporting

Automated reporting for the Elastic Stack

Graph

Real-time graph analytics for the Elastic Stack



elastic

elastic

6.0 is coming

Medcl
Developer @ Elastic

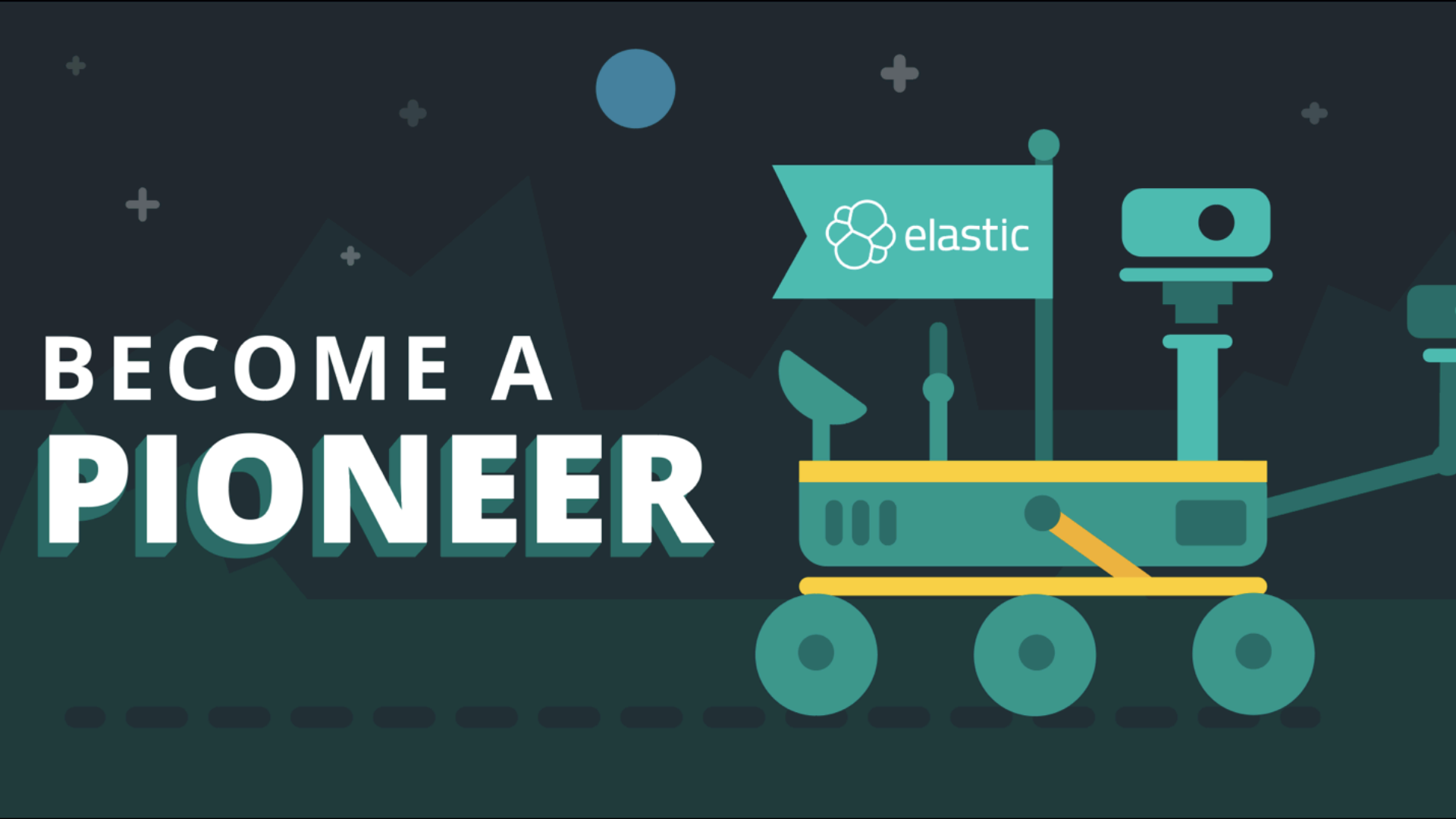


About me

- 曾勇（Medcl）
- Developer @ Elastic
  - Follow Elasticsearch since v0.5, 2010
  - Joined Elastic since September, 2015
- @medcl
- medcl@elastic.co
- http://github.com/medcl



elastic


BECOME A
PIONEER
elastic

Elastic Pioneer Program

We want your feedback!

1. Download 6.0 preview release (alpha, beta, etc)
2. Provide feedback via GitHub or Discuss forum
3. Get limited edition Pioneer swag

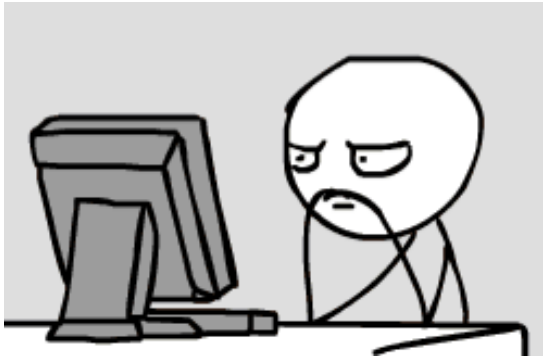


Elasticsearch

Brand new upgrade experience

Upgrades just got oh so simpler

Upgrading to 2.x



Upgrading to 5.x



Upgrading to 6.x

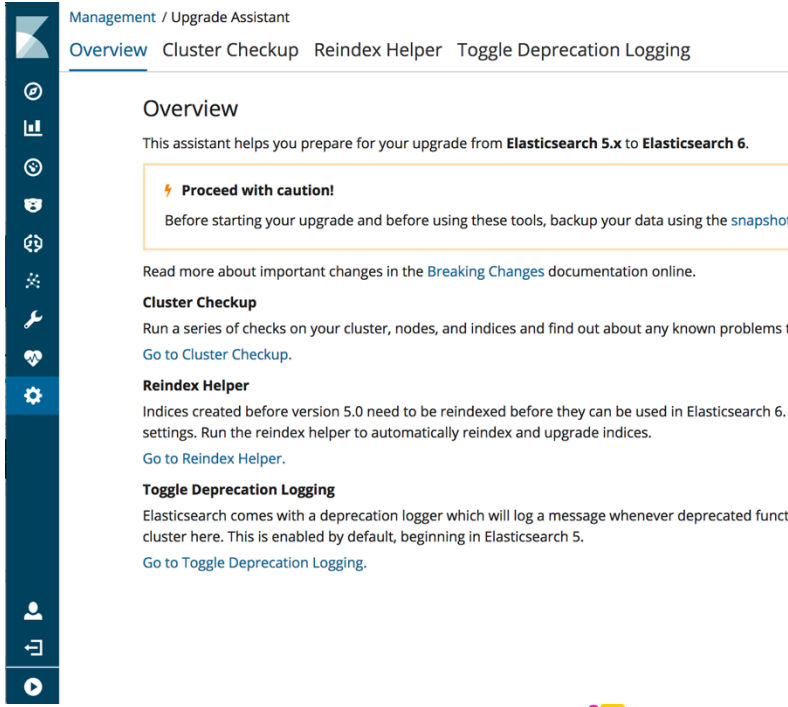


elastic

Brand new upgrade experience

Upgrades just got oh so simpler

- New Upgrade Assistant (UI & API)
- Zero downtime upgrades
  - Rolling restarts from latest 5.x to 6.x
  - Cross-cluster search across major version



elastic

Space-saving columnar store

Tapping into Lucene 7 goodness (`sparse doc value`)

- Better for storing sparse fields
- Save on disk space & file system cache

user	first	middle	last	age	phone
johns	Alex		Smith		
jrice	Jill	Amy	Rice		508.567.1211
mt123	Jeff		Twain	56	
sadams	Sue		Adams		
adoe	Amy		Doe	31	
lp12	Liz		Potter		

elastic

Much speedier sorted queries

Tapping into Lucene 7 goodness (`index sorting`)

Sort at index time vs. query time

Optimize on-disk format for some use cases

Improve query performance at the cost of index performance



elastic

Large Improvements to Replication

New operation-based approach to recovery (sequence numbers)

- Limit syncs to only changed documents (instead of file-based recovery)
- Fast replica recovery after temporary unavailability (network issues, etc.)
- Re-sync on primary failure
- Laying foundation for future big league features
  - Cross-datacenter replication
  - Changes API (tbd)

elastic

Large Improvements to Replication

New operation-based approach to recovery (sequence numbers)



elastic

Breaking changes

Because major releases is time for major cleanup

- Improved tools to handle breaking changes
  - Deprecation logging
  - Upgrade Assistant (UI & APIs)
- Refer to Release Notes for complete list
- Test, test, test

elastic

Simpler data models with type removal

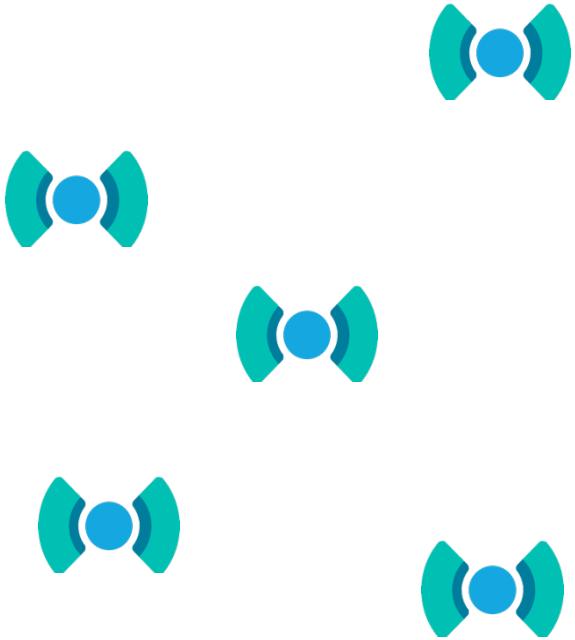
Say goodbye to _type confusion

- Breaking change
- Gradual migration path
  - 6.0 indices can be created with only one type
  - Existing 5.x indices using _type will continue to function
- Introducing new APIs for type-less operations

elastic

Distributed watch execution

- Watches are no longer executed on only the master node
- They are executed on nodes which hold shards of the `.watches` index
- Configure all or specific nodes dedicated to watch execution

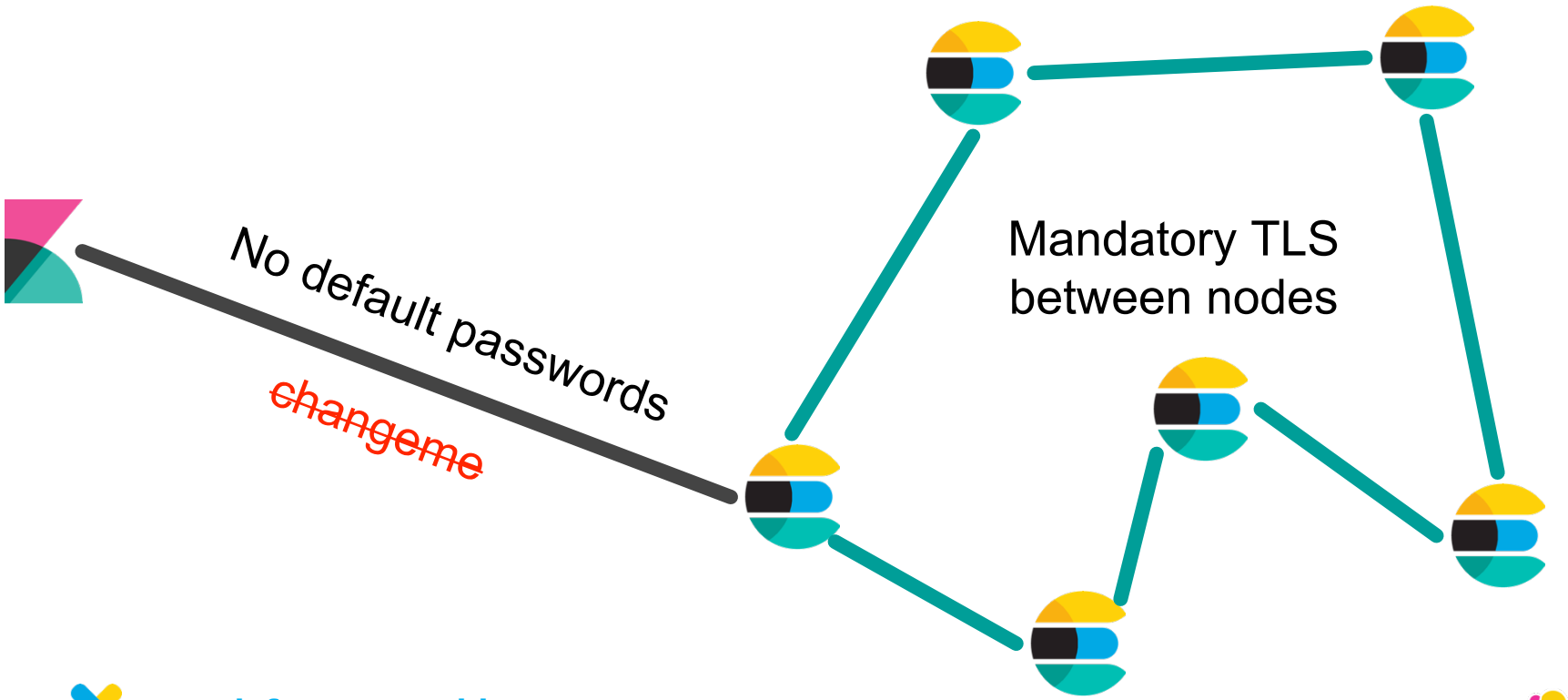


X-Pack feature (Gold)

elastic

Secure all the things

Default security



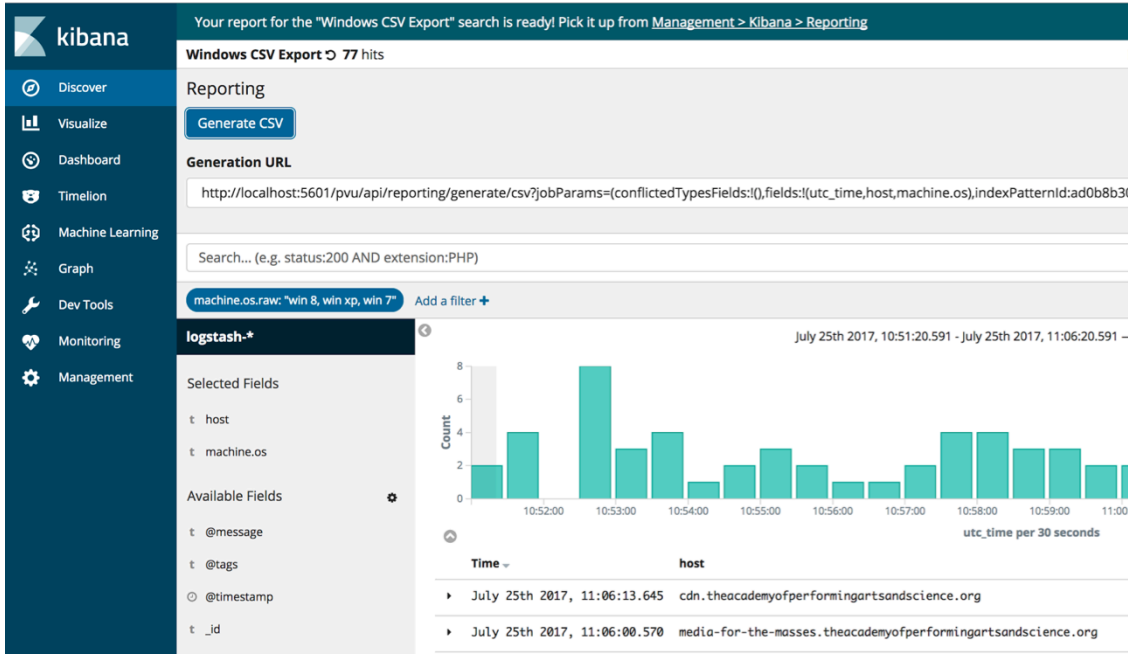
X-Pack feature (Gold)

elastic

Kibana

Export saved searches to CSV with a single click

Highly requested feature
Trigger export via Watcher

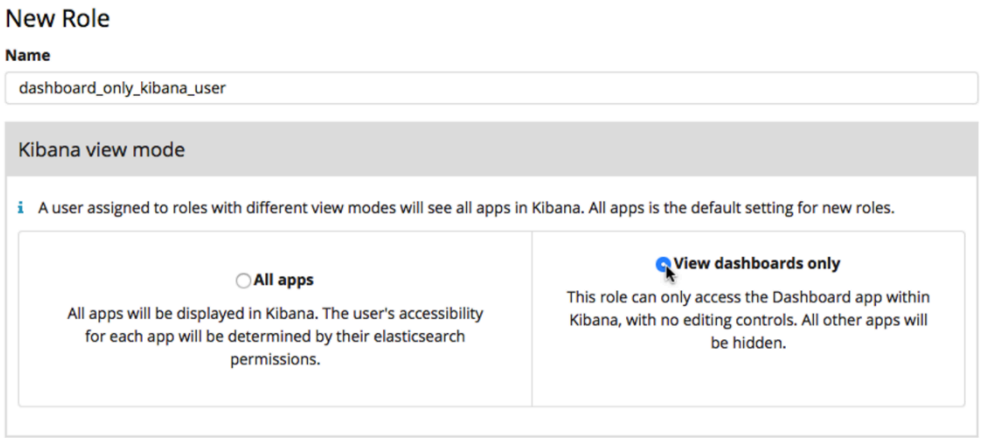


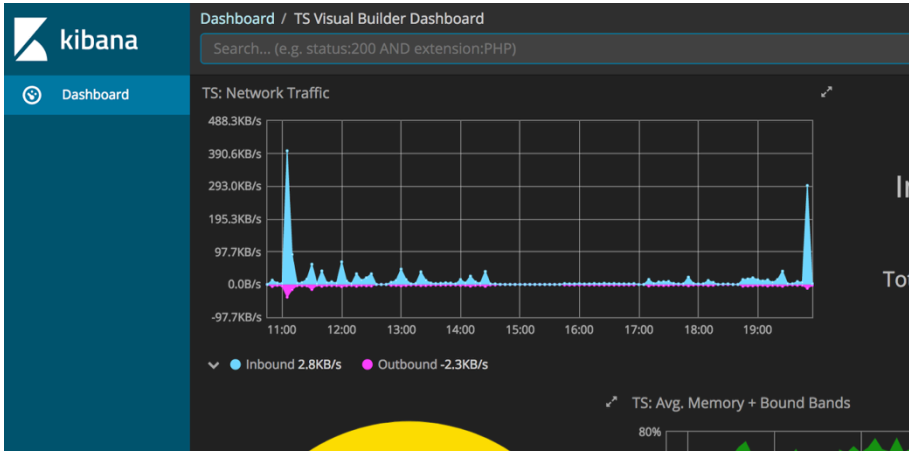
X-Pack feature (Basic, free)

elastic

Lock down edits with Dashboard Only mode

Share dashboards without worrying about accidental changes





X-Pack feature (Gold)

elastic

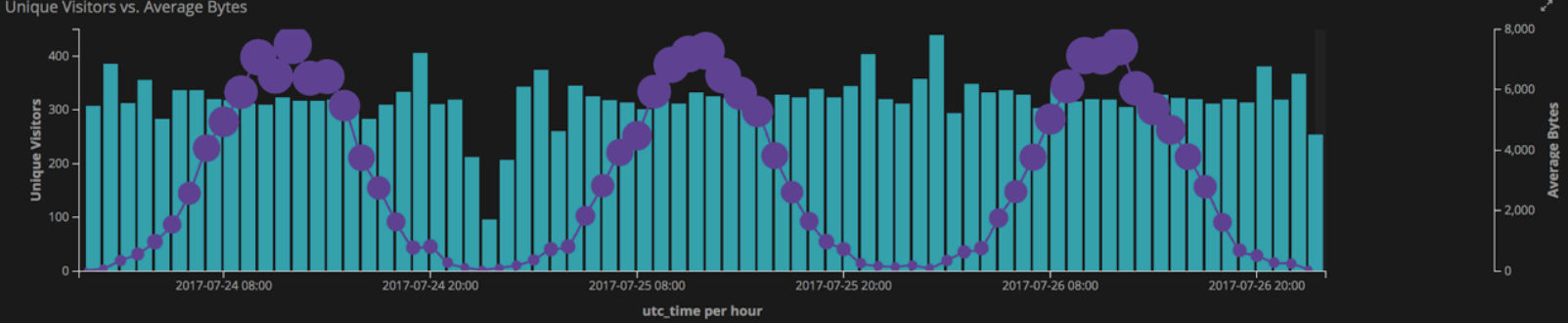
Maximize screen space with Full Screen mode

Optimized viewing for your NOCs & SOCs



elastic

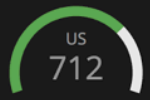
Unique Visitors vs. Average Bytes



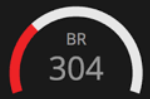
Gauges



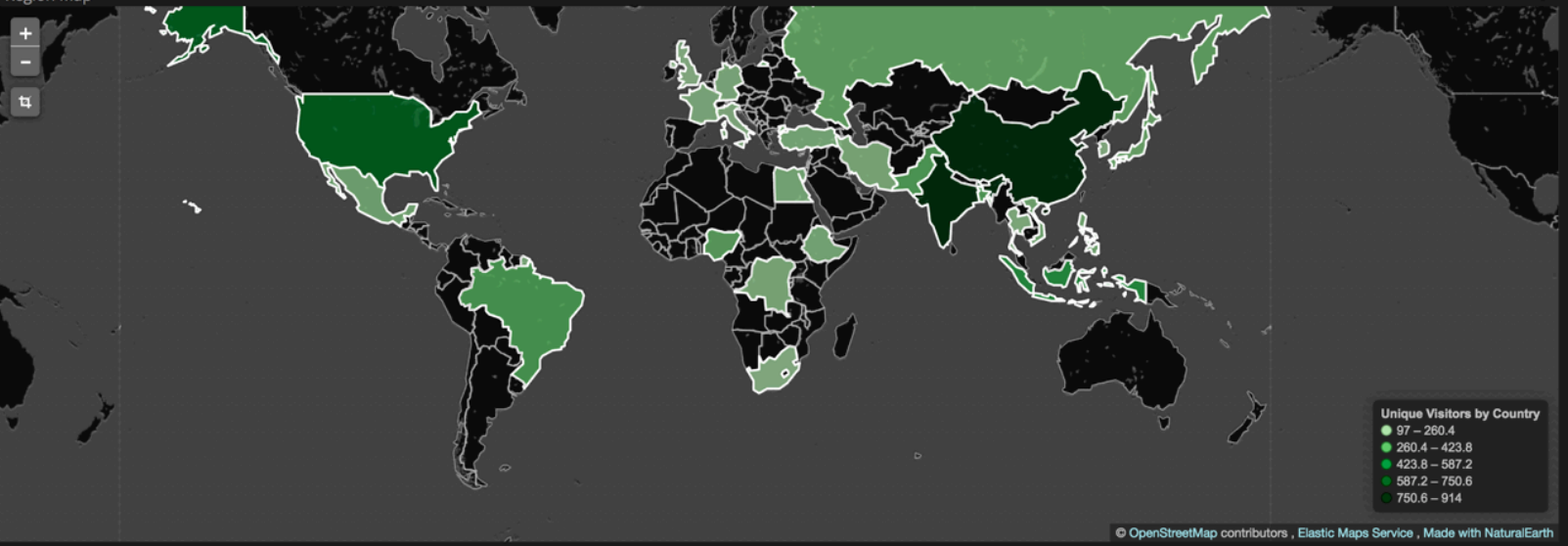








Region Map



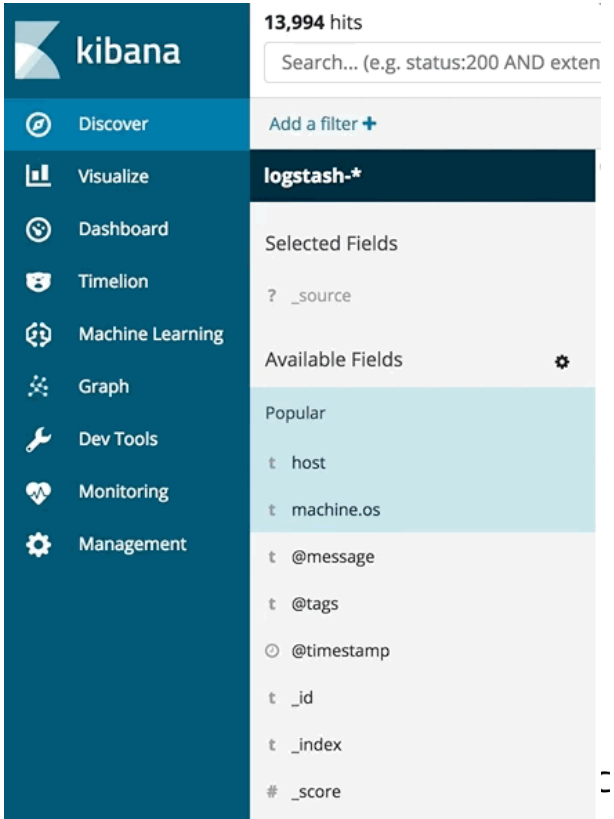
Unique Visitors by Country

kibana Exit full screen

6.0 starts Kibana on the accessibility path

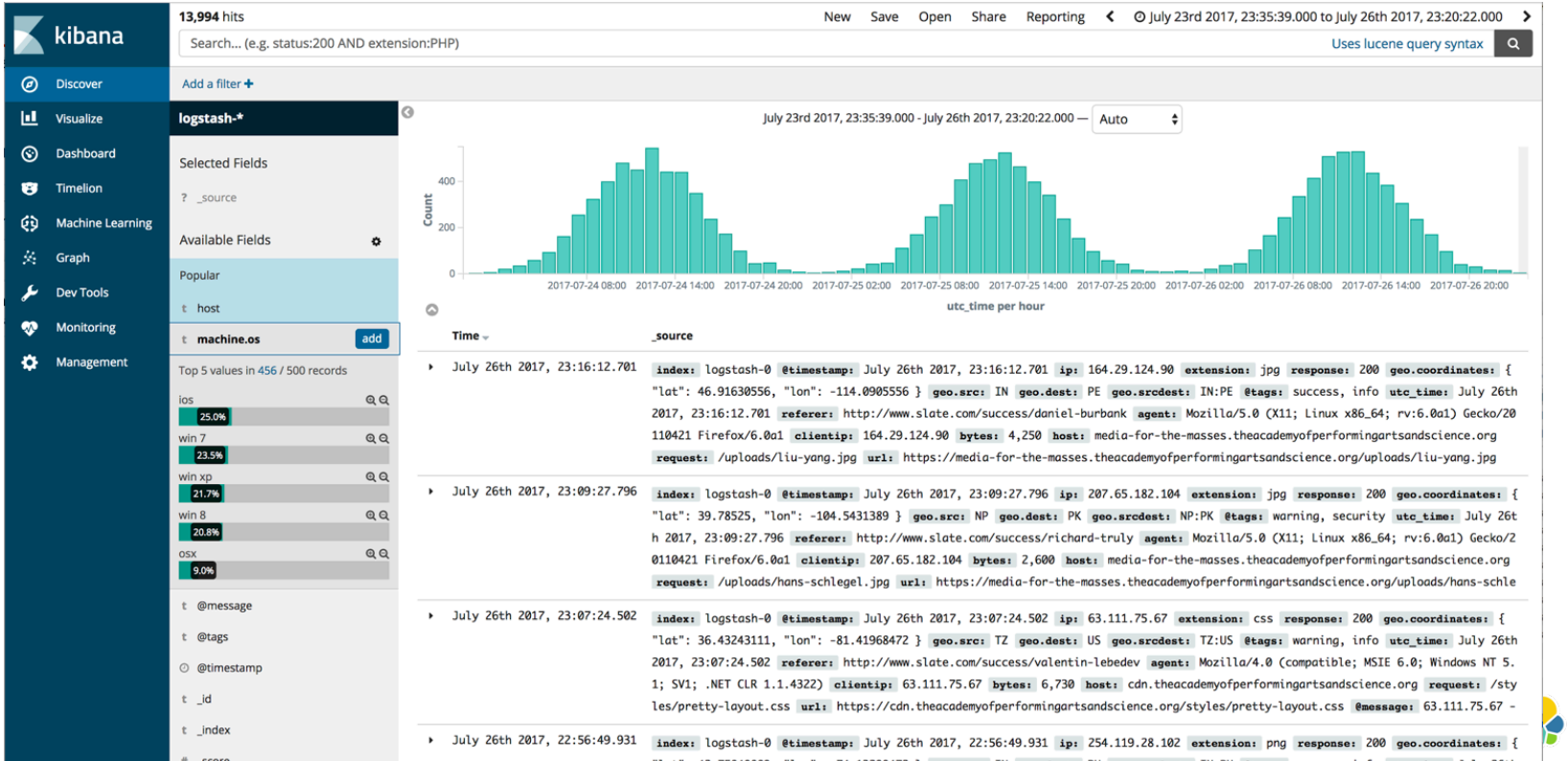
Accessibility improvements

- High contrast color scheme
- Keyboard accessibility
- Screen reader support
- More improvements on the way



6.0 starts Kibana on the accessibility path

Accessibility improvements



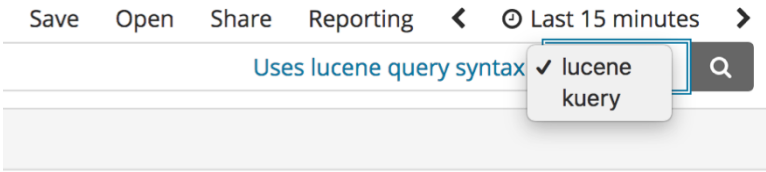
elastic

More ways to query with Kuery

Consistent syntax and simple to get started

Kibana now supports multiple query languages

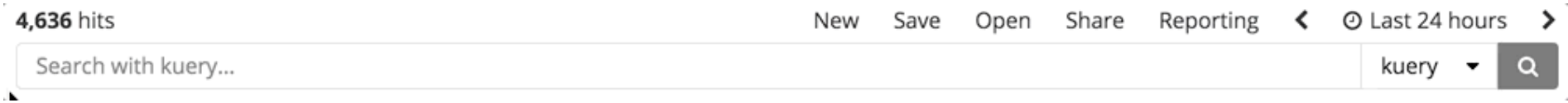
- **Lucene Query Language** (default)
- **Kuery** (off by default, experimental in 6.0)



- … perhaps others in the future

We want your feedback!

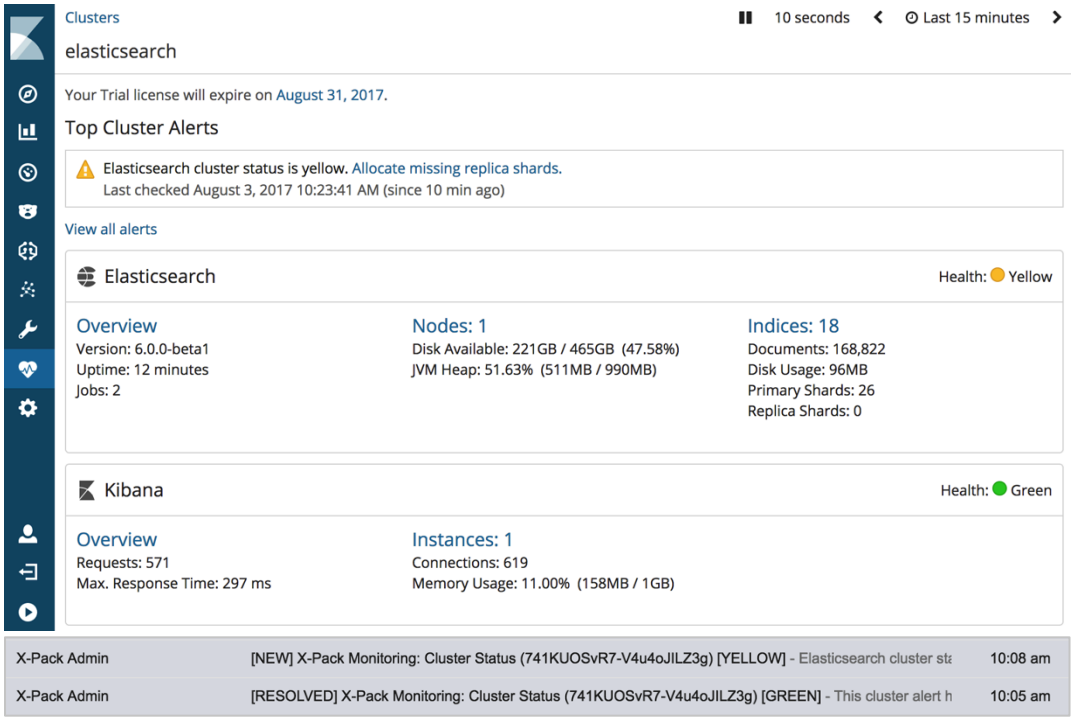
- Enable Kuery from Advanced Settings



elastic

Get e-mail alerts on Cluster Alerts

- Cluster Alerts are built-in Watches for cluster issues
- Get e-mails when Cluster Alerts get triggered and resolved
- Add admin e-mail in Kibana Advanced Settings



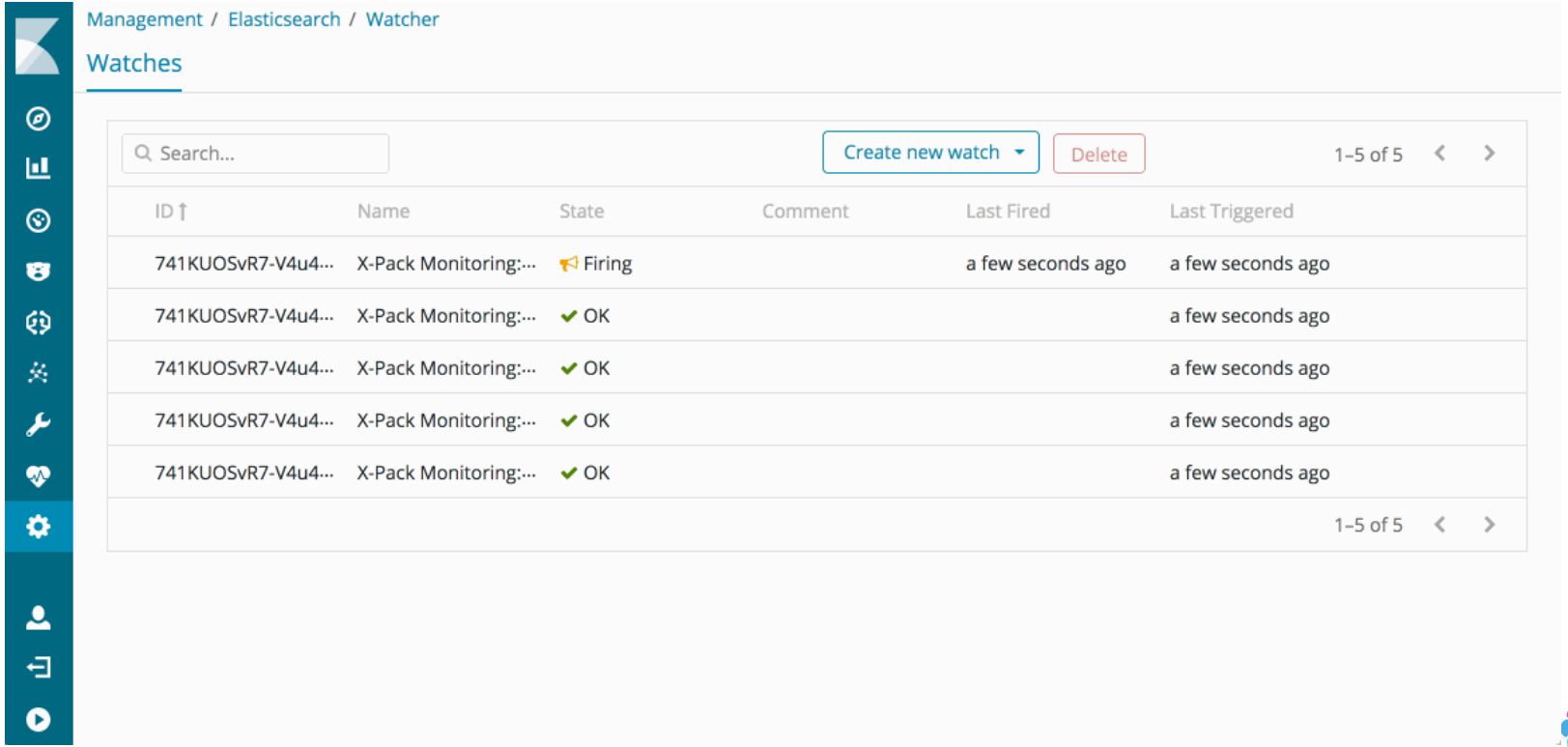
X-Pack feature (Gold)

elastic

X-Pack feature (Gold)

Easily create simple threshold alerts

New form based UI for threshold alerts

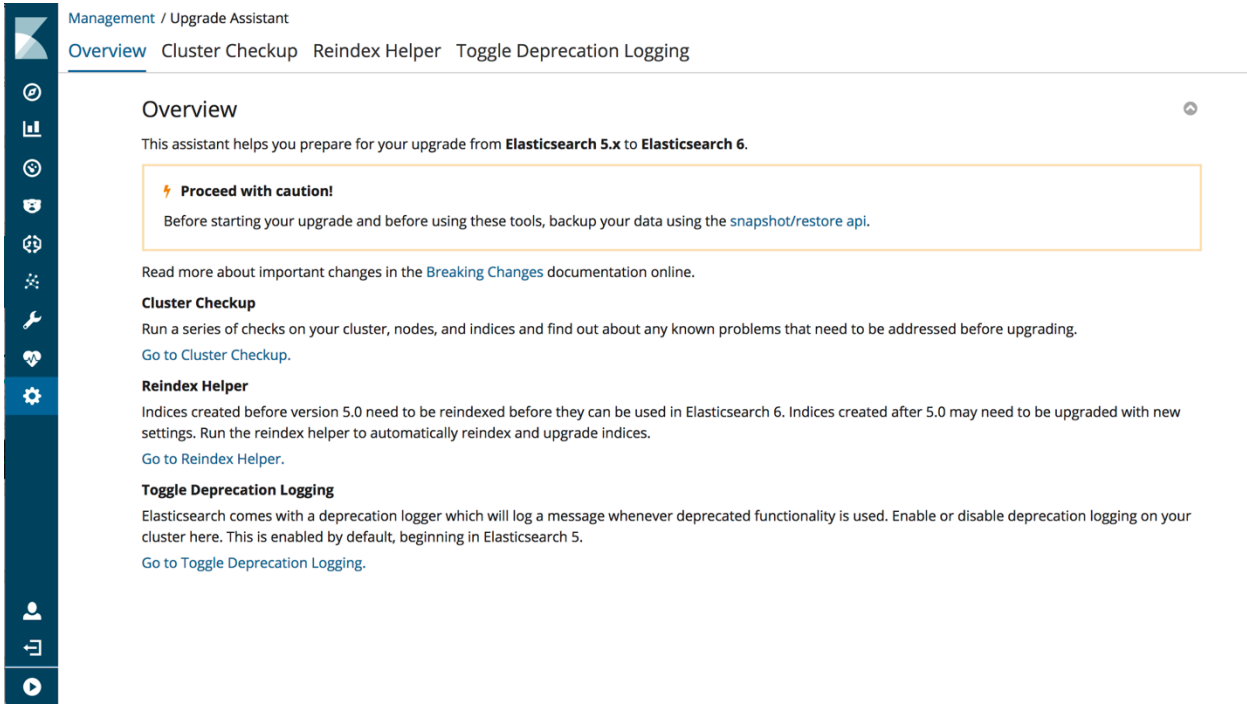


elastic

Migration is easier with a UI

Upgrade Assistant UI

- UI ships with 5.6



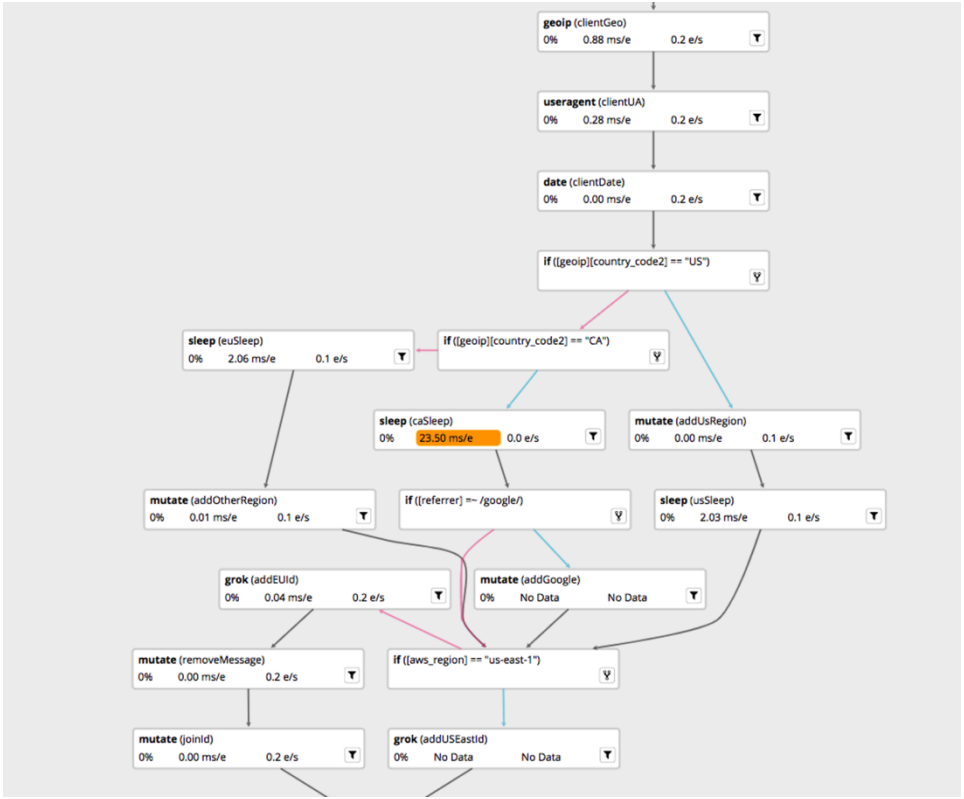
X-Pack feature (Basic, free)

elastic

Zoom in on your Pipelines

Pipeline Viewer

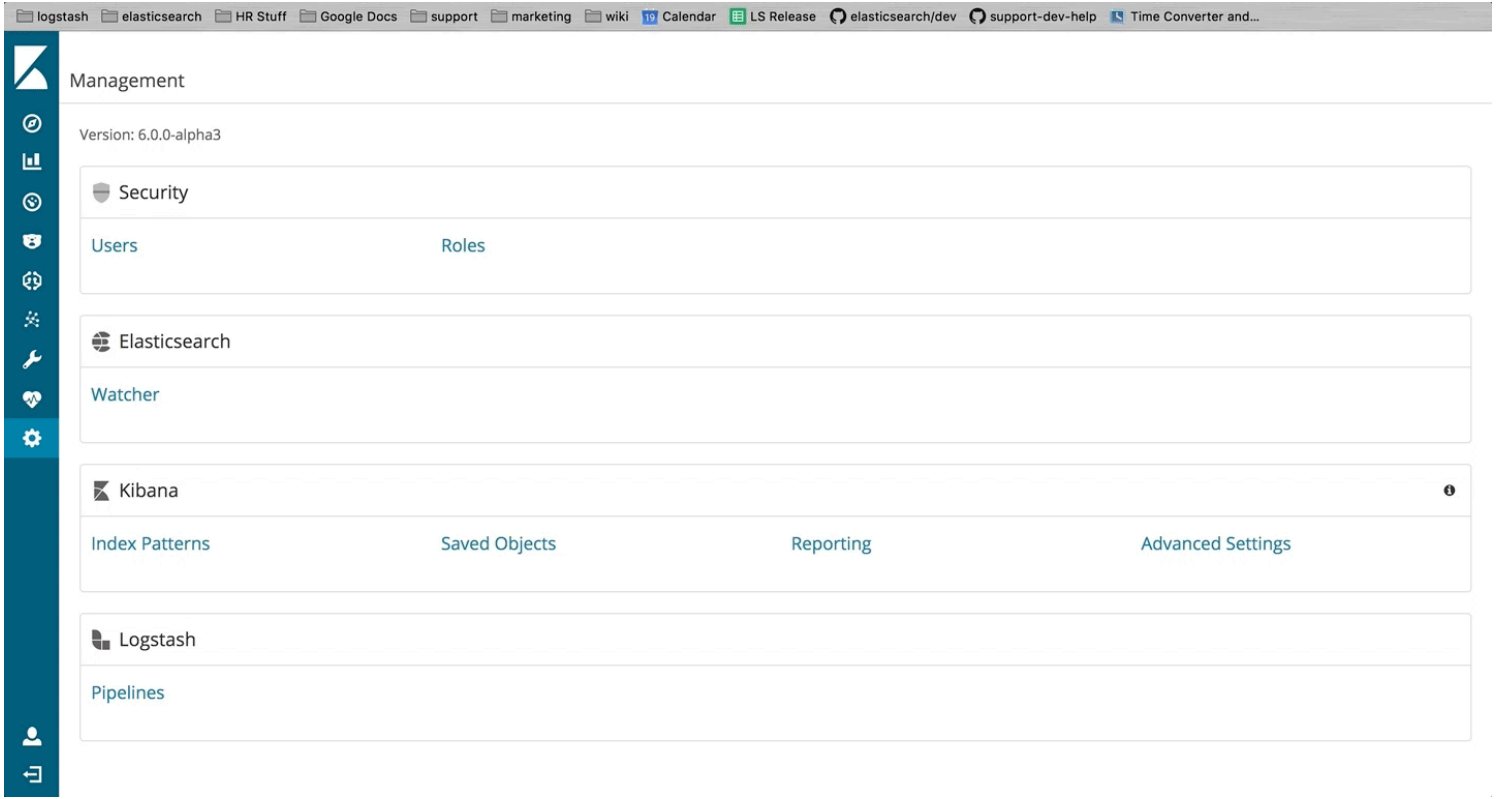
- Visualize pipeline topologies as graphs
- Reveal bottlenecks at the plugin level
- Optimize dataflow with better metrics
- Integrated with Monitoring UI



X-Pack feature (Basic, free)

elastic

Centrally manage Logstash pipelines



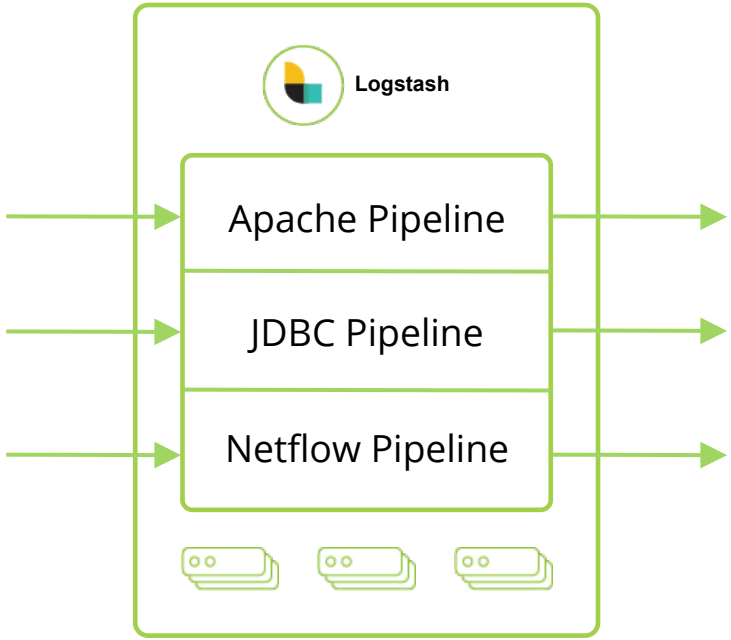
X-Pack feature (Gold)

elastic

Logstash

Multiple Pipelines, One Logstash

- Run multiple, distinct workloads on a single Logstash JVM
- Simplify dataflow logic by managing per data source logic independently
- Monitor each pipeline separately with the new Pipeline Viewer

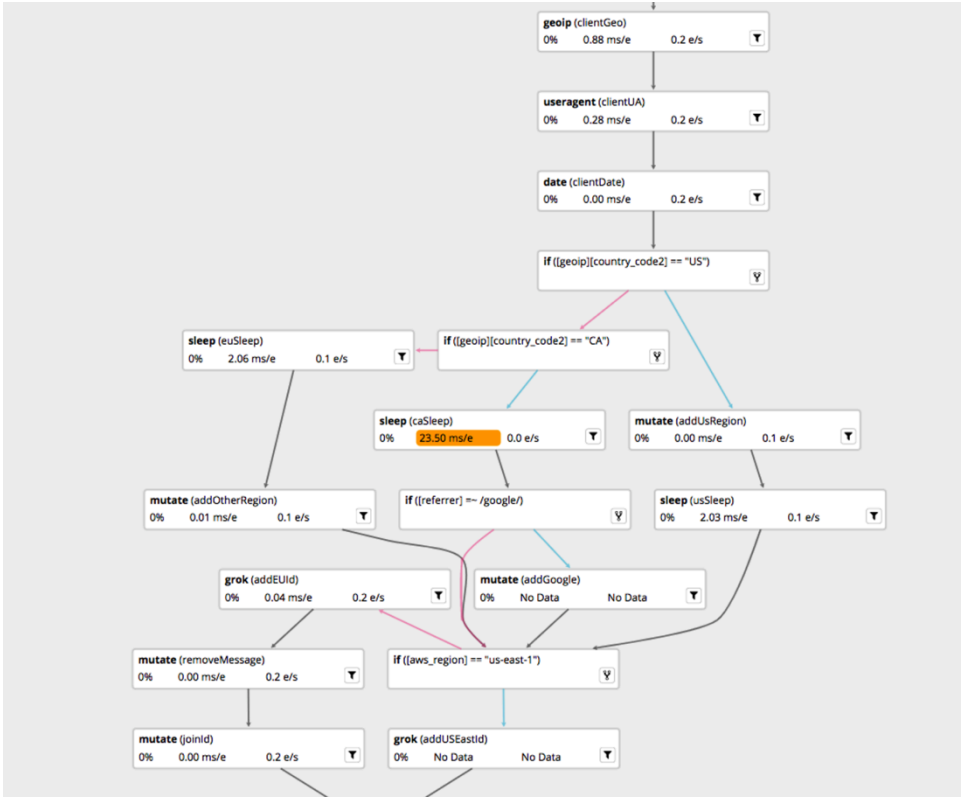


elastic

Zoom in on your Pipelines

Pipeline Viewer

- Visualize pipeline topologies as graphs
- Reveal bottlenecks at the plugin level
- Optimize dataflow with better metrics
- Integrated with Monitoring UI



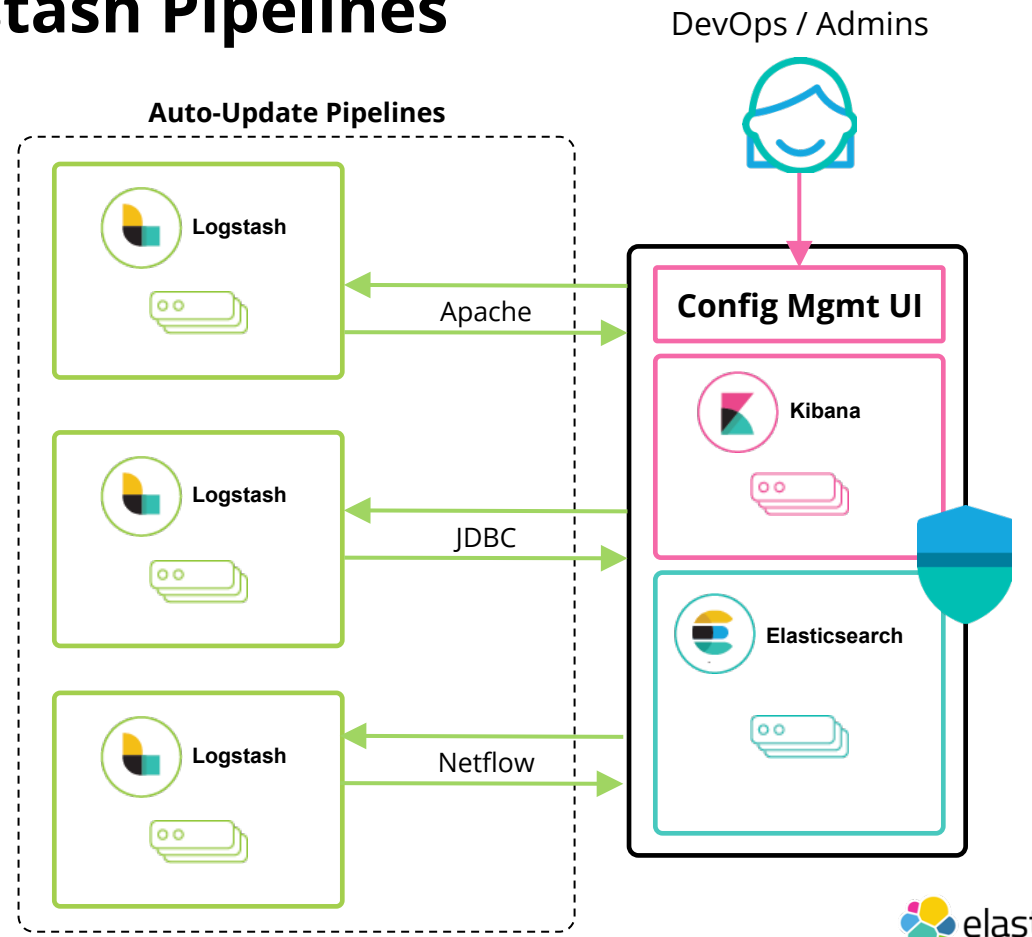
X-Pack feature (Basic, free)

elastic

Centrally Manage Logstash Pipelines

Pipeline Management

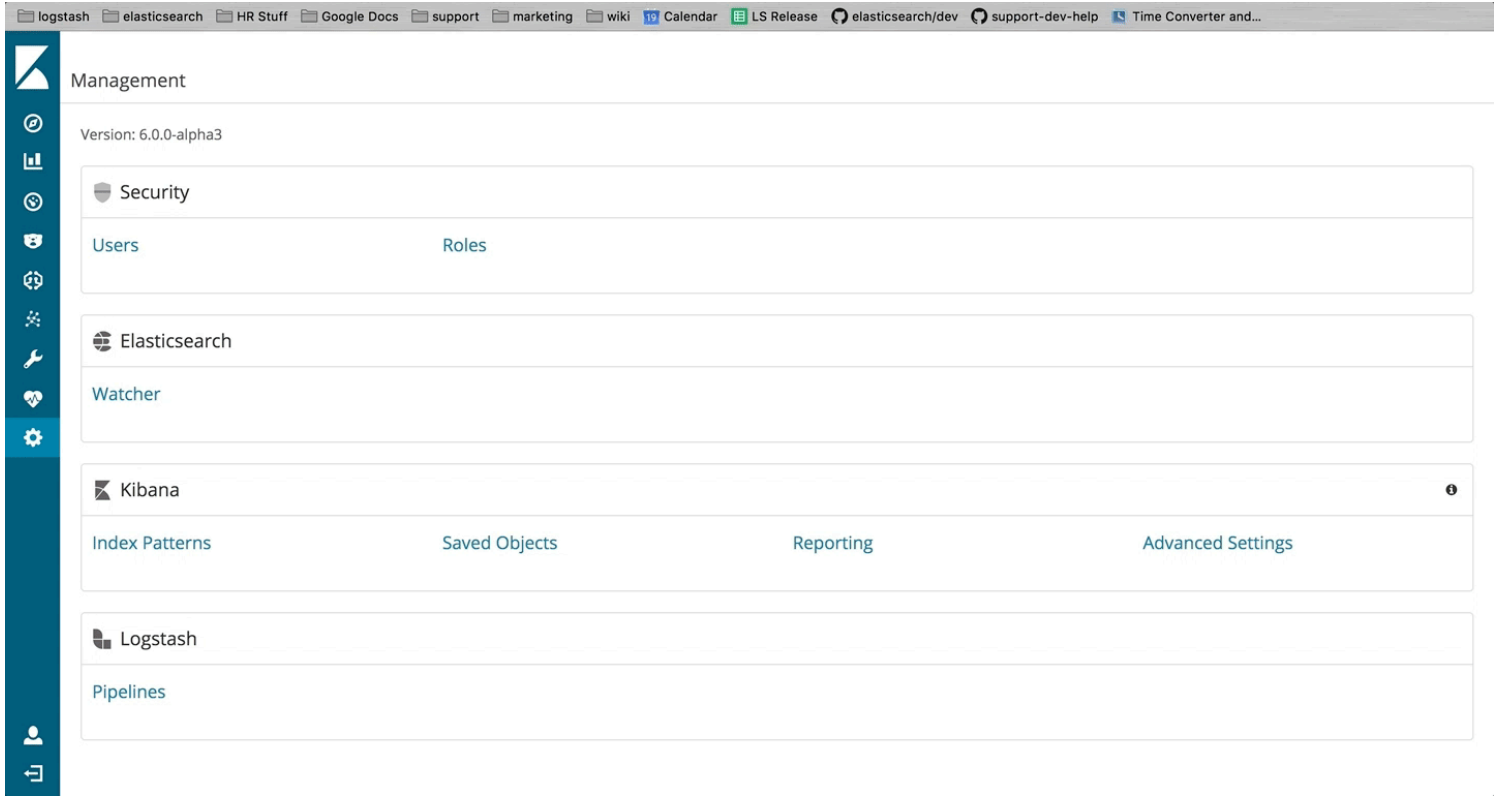
- Manage multiple pipelines from multiple nodes in a single UI
- Logstash nodes can poll and dynamically reload pipelines on configuration change
- Secure access to configuration management with X-Pack



X-Pack feature (Gold)

elastic

Centrally Manage Logstash Pipelines



X-Pack feature (Gold)

elastic

Easily Migrate from Ingest Node Pipelines

Ingest Node Converter

Convert ingest node to Logstash pipelines with a CLI tool

Why Logstash?

- More input sources
- Multiple outputs
- Richer transformations
- Buffering, persistent queues

```
$LS_HOME/bin/ingest-convert.sh
  --input file:///path/to/ingest_pipeline.json
  --output file:///path/to/logstash_pipeline.conf
```


elastic

Beats

Beats <3 containerization

Monitor your Docker and Kubernetes deployments with ease

- New Kubernetes module in Metricbeat
  - CPU, memory, bytes on network and more.
- New processor to add_docker_metadata
  - Container ID, name, image, labels
- New processor to add_kubernetes_metadata
  - Pod name, pod namespace, container name, pod labels





More modules for more data sources

New Metricbeat Modules



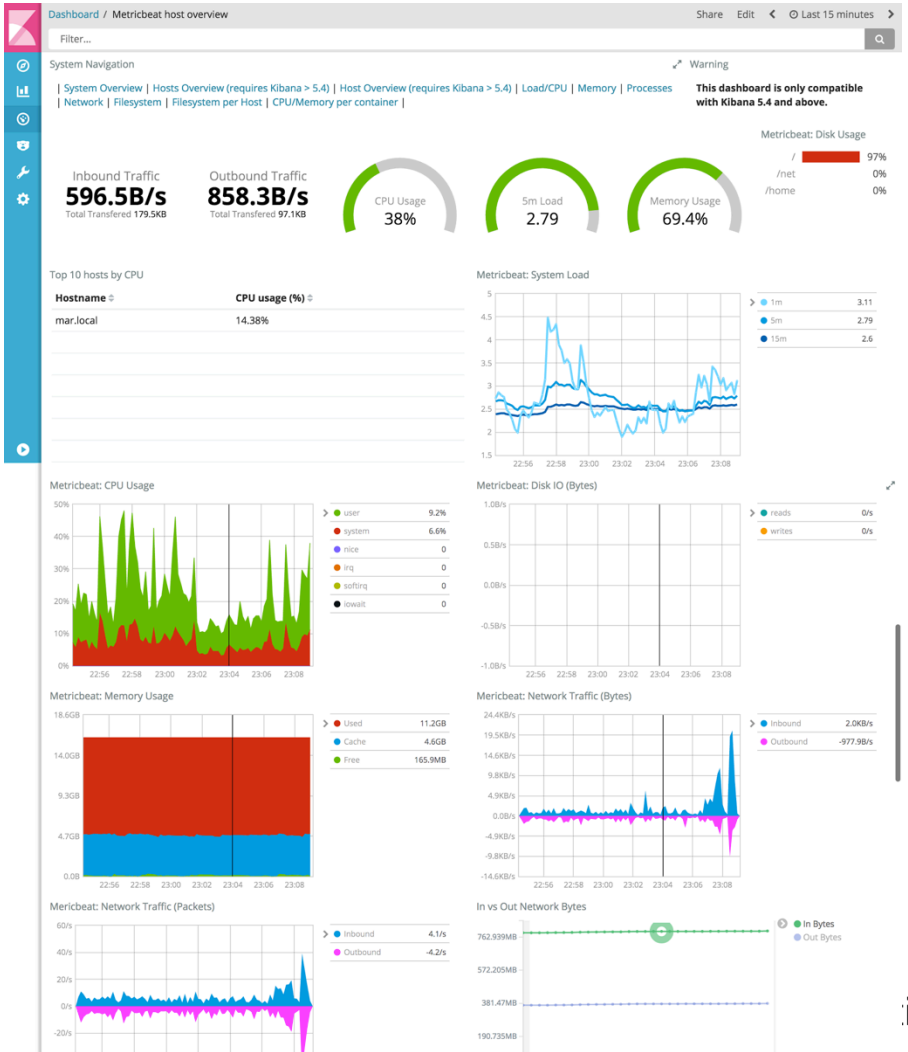
New Filebeat modules



elastic

Better Modules

- Improved dashboards for Metricbeat system module



Auditbeat - a simpler way to track audit logs

An alternative to `auditd` on Linux

- Skip the hassle of parsing `auditd` logs
  - Auditbeat subscribes to the kernel directly
- Reuse `auditd` rule formats (no need to learn new rule formats)
- Plus, file integrity checks on Linux, macOS, and Windows
  - Watch files or directories (non-recursively) for changes
  - Report file metadata and MD5, SHA1, SHA256 hashes on changes

elastic

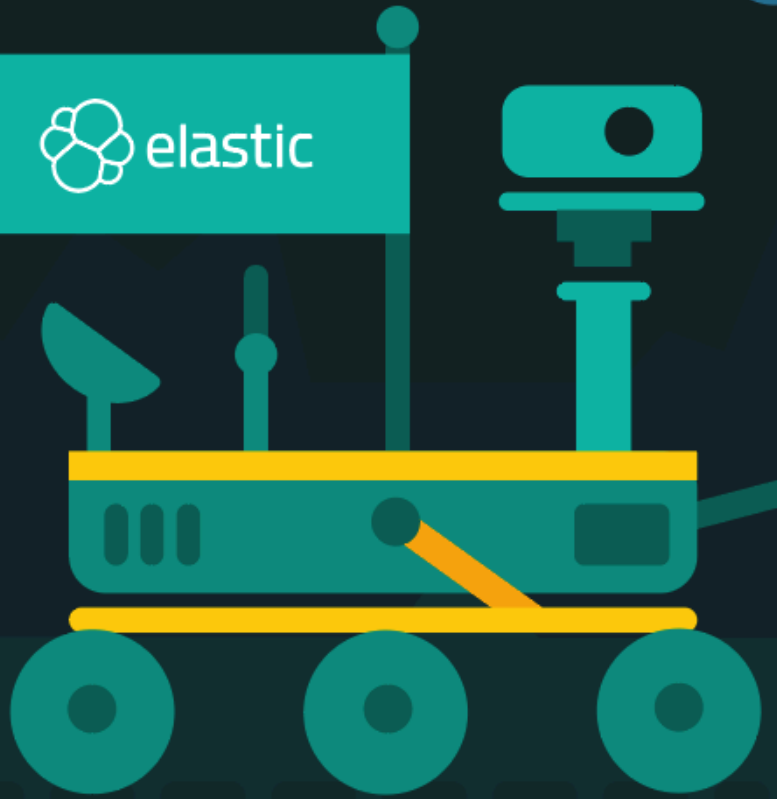
And moar awesome all around

- Index pattern versions
- Simpler configuration
  - Module commands and configuration files
    - module.d directory
    - ./metricbeat module enable system
  - Dashboards are easier to load and packaged with the Beat

elastic

BECOME A PIONEER

6.0 BETA



Elastic Pioneer Program

We want your feedback!

1. Download 6.0 preview release (Beta, RC, etc)
2. Provide feedback via GitHub or Discuss forum
3. Get limited edition Pioneer swag

elastic

Try 6.0 Beta!

Thank you!