

Elasticsearch 2.0

What's cooking?



Alexander Reelsen

@spinscale

alex@elastic.co

Agenda

 Simplification

 Security

 Resiliency

 Features

 Plugins

About



2012

 Elasticsearch got founded

 Series A investment

 Trainings

 Supports subscriptions

About



2012

2013

-  Series B investment
-  Kibana
-  Elasticsearch for Apache Hadoop Integration
-  Logstash
-  Elasticsearch Clients



About



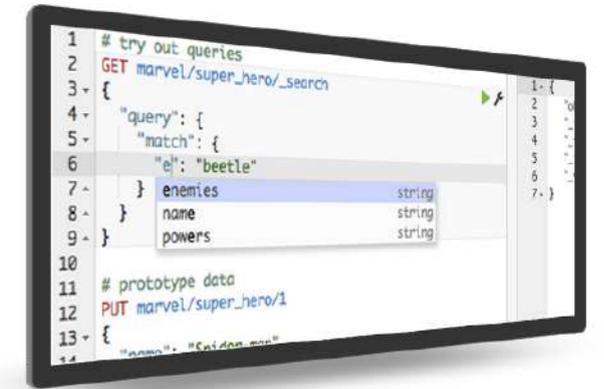
2012

2013

2014

 Series C investment

 Marvel released



About



2012

2013

2014

2015

 Shield goes GA



 First user conference & rebrand

 Found acquired

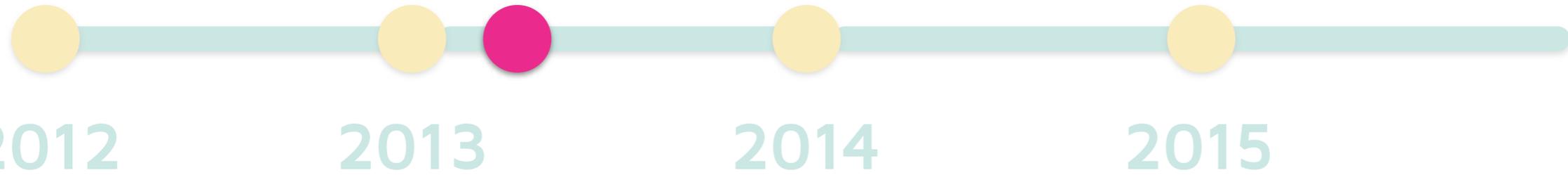


 Packetbeat joins



 Watcher in beta

About



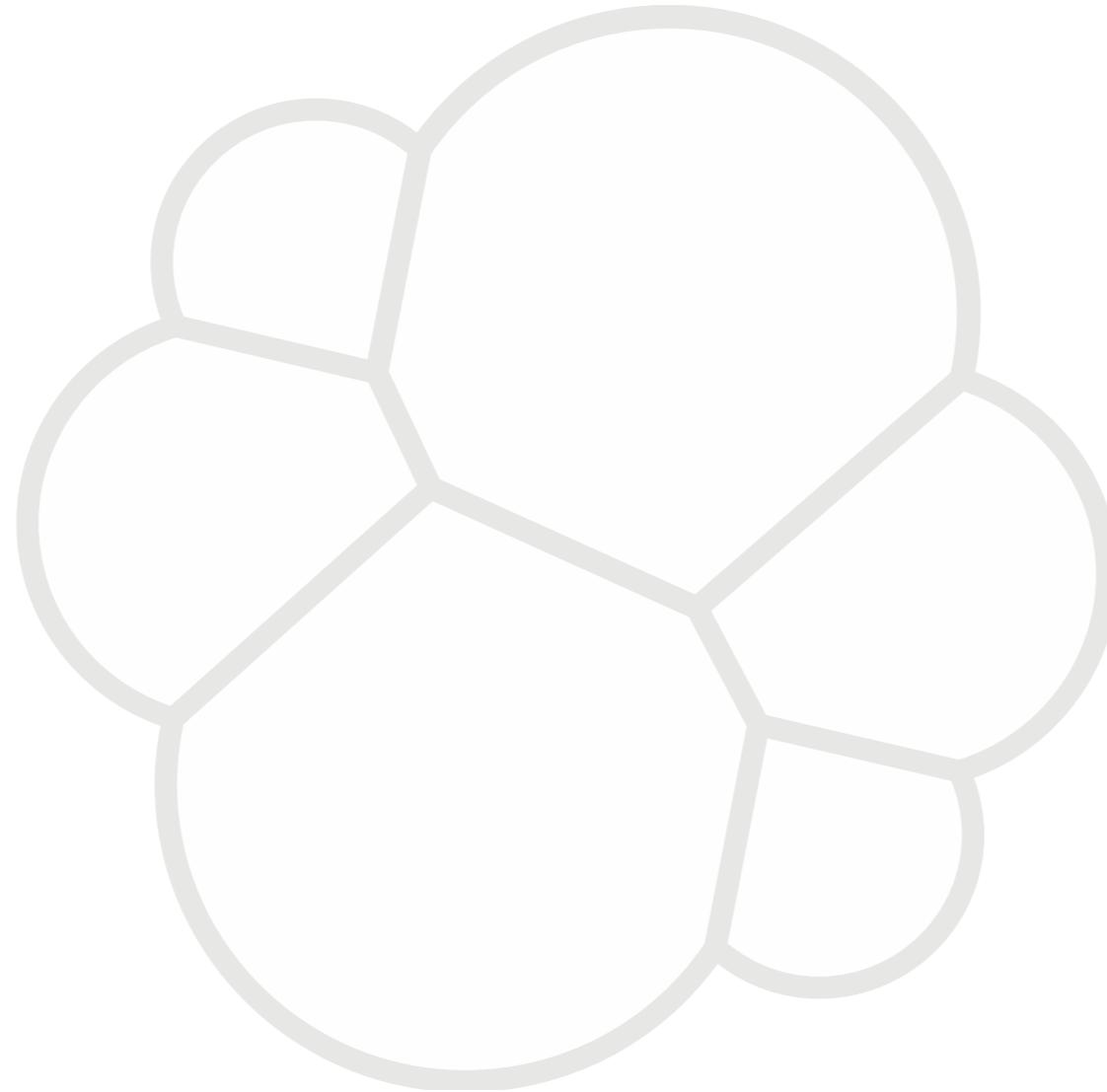
 Joined in March 2013

 Working on Elasticsearch, Shield & Watcher

 Development, Trainings, Conferences, Support, Blog posts

 We're hiring...

Cleanups



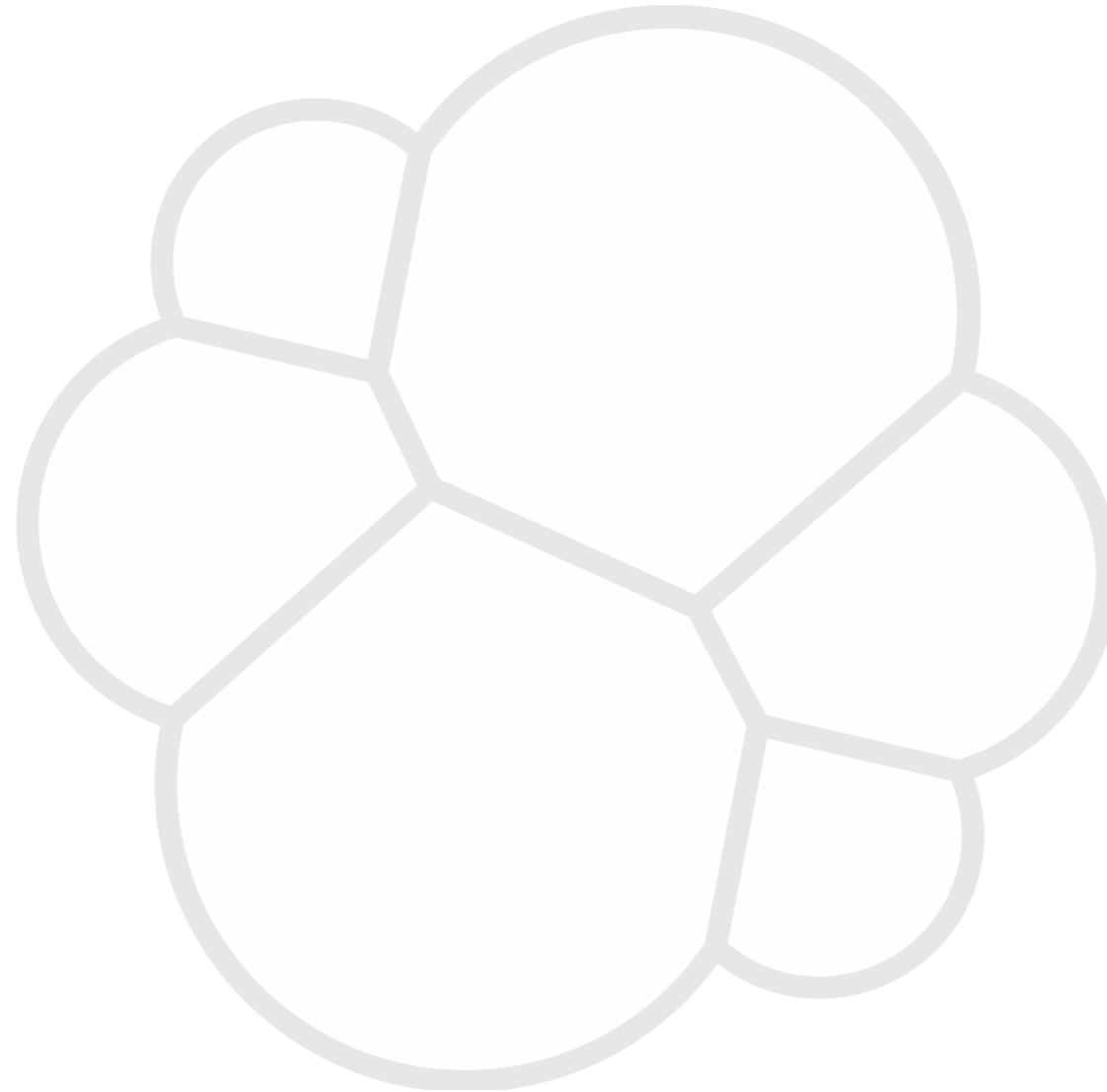
Cleanups

- 🌸 Replaced: Facets
- 🌸 Removed: shutdown API
- 🌸 Removed: Thrift/Memcached protocol support
- 🌸 Removed: Rivers
- 🌸 Removed: Bulk UDP

Moved into plugins

-  Delete-by-query
-  murmur3/size types
-  Multicast discovery

Mapping changes



Mapping changes

Fields

-  ... must be referenced by full name
-  ... names cannot be referenced using type name prefix
-  ... names cannot contain dots

Types

-  Type names cannot start with a dot
-  Type may no longer be deleted

 Removed: `index_analyzer` & `_analyzer`

 date format changes

Mapping changes

Fields

 ... must be referenced by full name

 ... names cannot be referenced using type name prefix

 ... names cannot contain dots

Types

 Type names cannot start with a dot

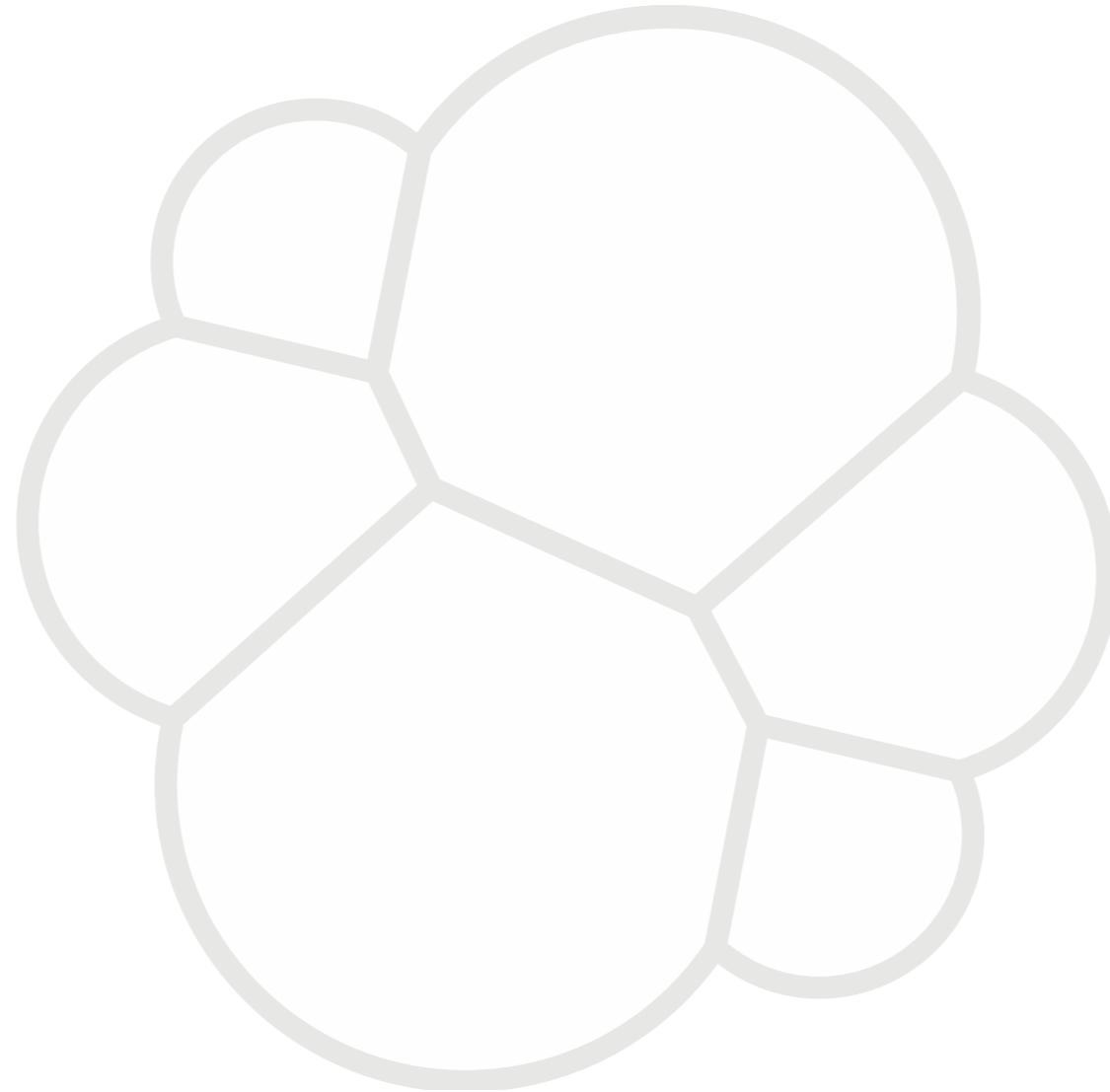
 Type may no longer be deleted

 Removed: `index_analyzer` & `_analyzer`

 date format changes

<https://www.elastic.co/blog/great-mapping-refactoring>

Query/Filter changes



Query/Filter changes

- 🌸 Queries/Filters merged into queries

 - 🌸 context decides over scoring

- 🌸 Two-Phase Execution

 - 🌸 approximation and verification

- 🌸 Query Caching

 - 🌸 based on usage pattern by tracking queries

 - 🌸 Using roaring bitmaps for caches

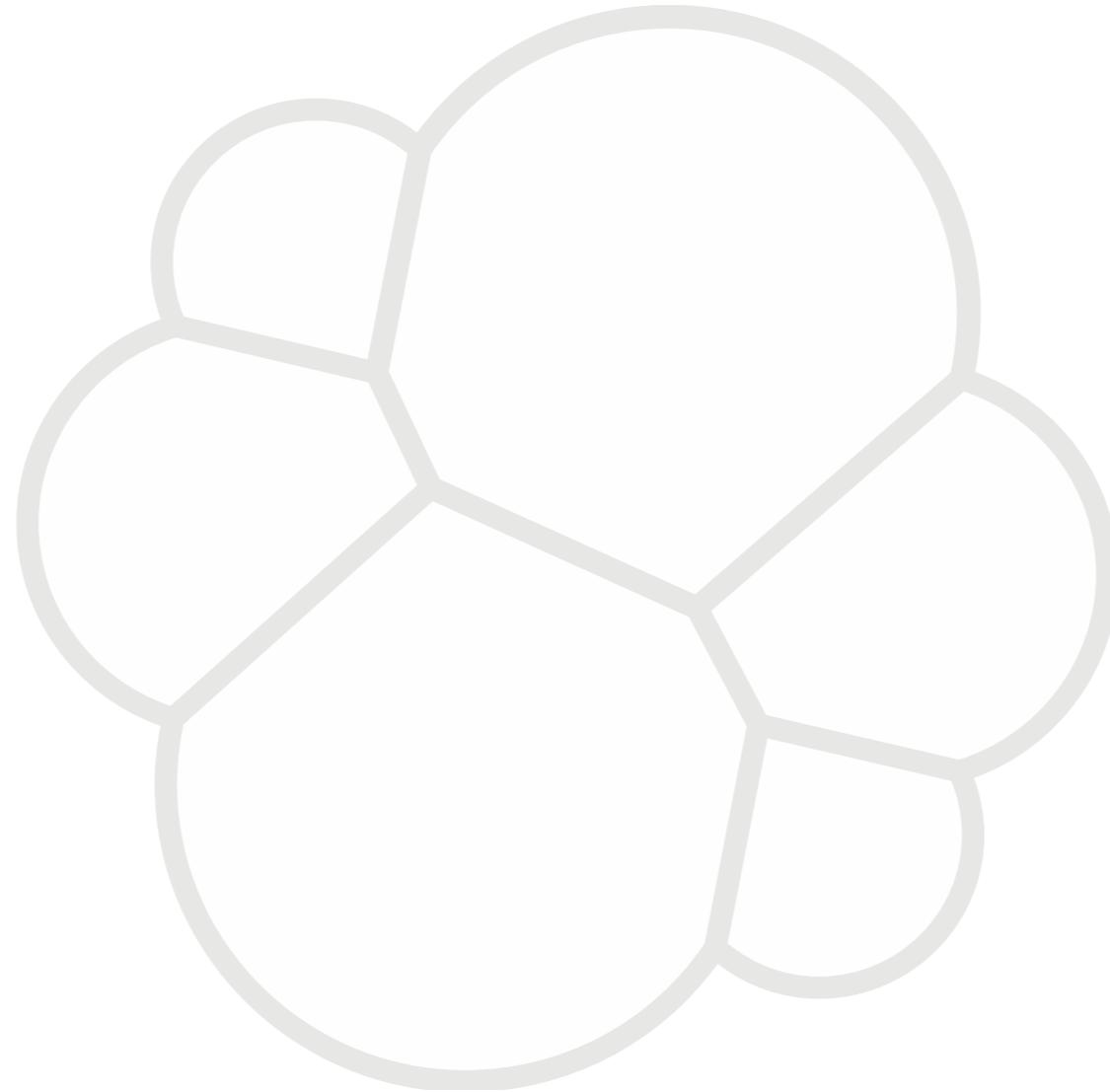
Query/Filter changes

```
{  
  "filtered" : {  
    "query" : { query definition },  
    "filter" : { filter definition }  
  }  
}
```

Query/Filter changes

```
{  
  "bool" : {  
    "must" : { query definition },  
    "filter" : { filter definition }  
  }  
}
```

Security



Security

- 🌿 Security Manager enabled by default

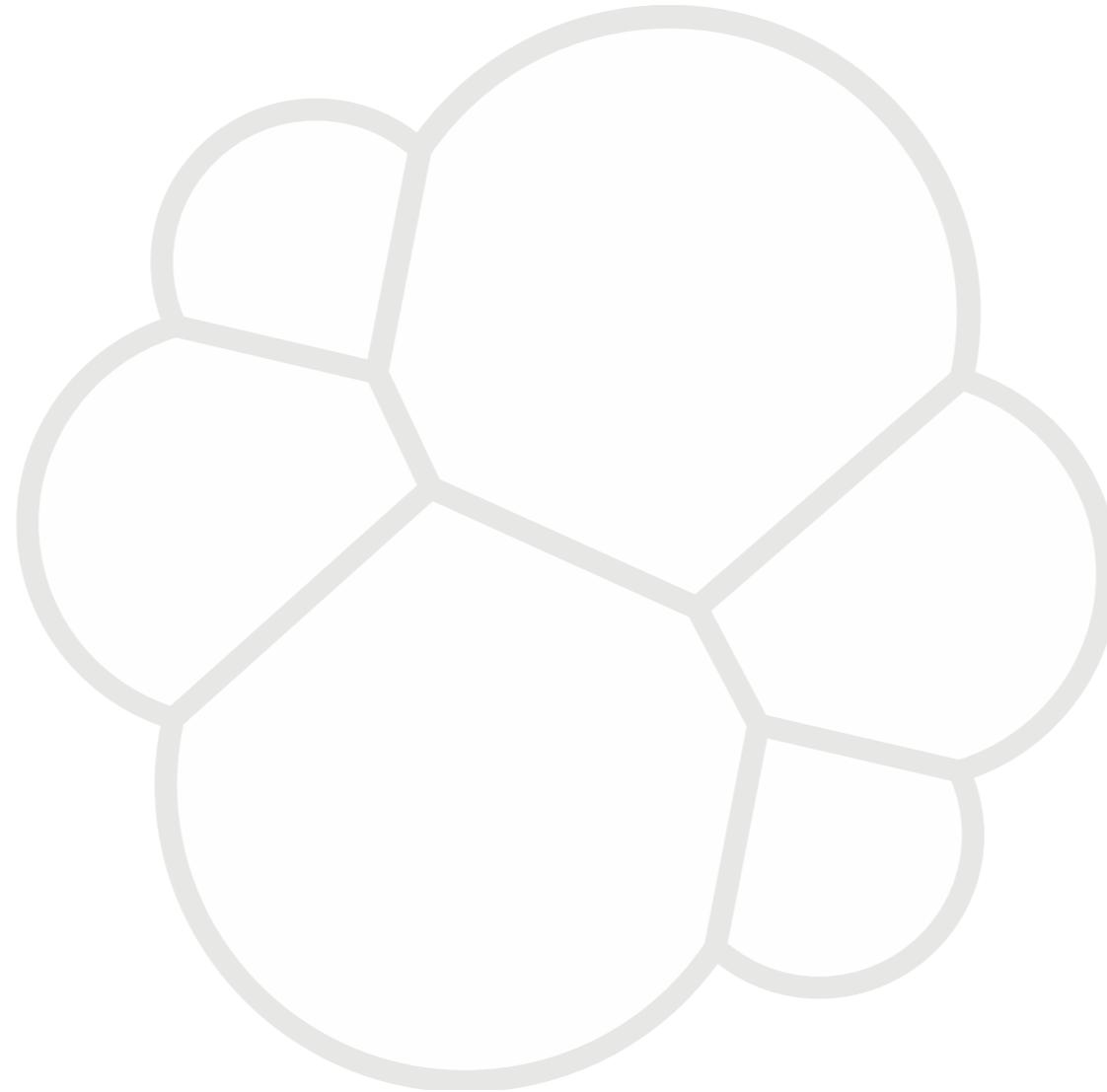
 - 🌿 Very reduced permission set after startup

- 🌿 Networking

 - 🌿 Unicast by default

 - 🌿 Binds to local interfaces only by default

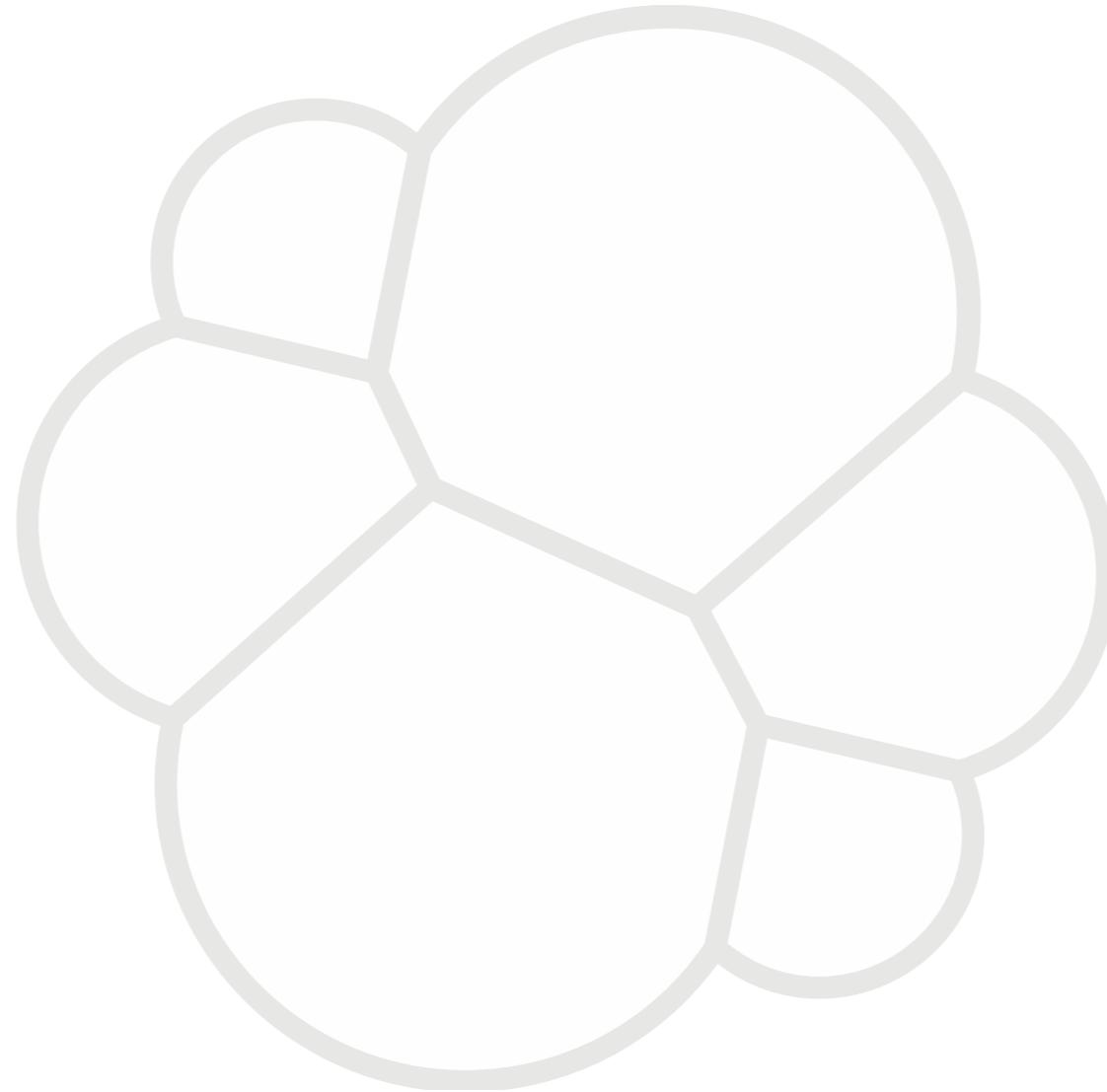
Reliability



Reliability

- Transaction log: `fsync()` after each operation
- Multiple path data striping
- Cluster state diffs
- Doc values by default
- Units are required (“1m”)
- 1.6: Synced flush, async shard allocation fix
- 1.7: delayed allocation

Features



Features

Pipeline Aggs

 Derivatives, moving avg, holt winters, time series!

Index compression

Structured exceptions

Plugins

 22 plugins are part of main repo now

 `bin/plugin install clouds-aws`

 Shield/Watcher/Marvel releases aligned now

 `bin/plugin install watcher`

 Helper: Migration plugin!

Plugins

http://localhost:9200

Filter indices: eg. logstash-*

Run checks now ▶

Show green test results

✘ Checks completed. The cluster requires action before upgrading.

● Elasticsearch version: 1.5.2

Cluster settings

● Units for time and byte cluster settings ⓘ

Units are required for byte and time settings: `indices.ttl.interval`

Index: `conflicting_fields-bad`

● Conflicting field mappings ⓘ

Mapping for field one:aaa conflicts with: two:aaa. Check parameters: format, type

Mapping for field one:bbb.ccc conflicts with: two:bbb.ccc. Check parameters: format, type

Mapping for field one:ddd conflicts with: two:ddd. Check parameter: `fielddata.format`

Index: `conflicting_fields-good`

● Conflicting field mappings ⓘ

Plugins

Shield

 document/field level security, realms API

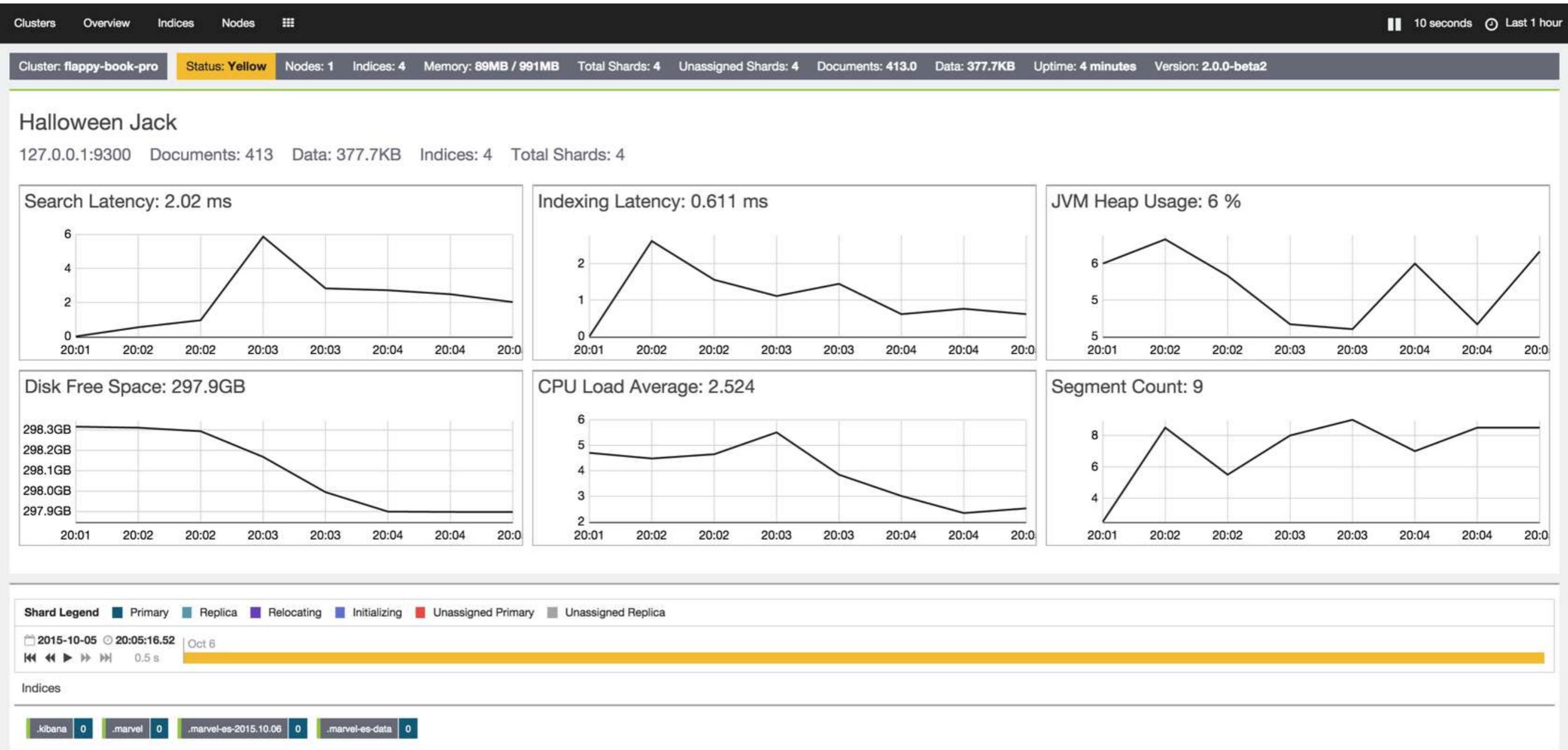
Watcher

 hipchat/slack actions, activate/deactivate API

Marvel

 new UI, less but more useful metrics

Plugins



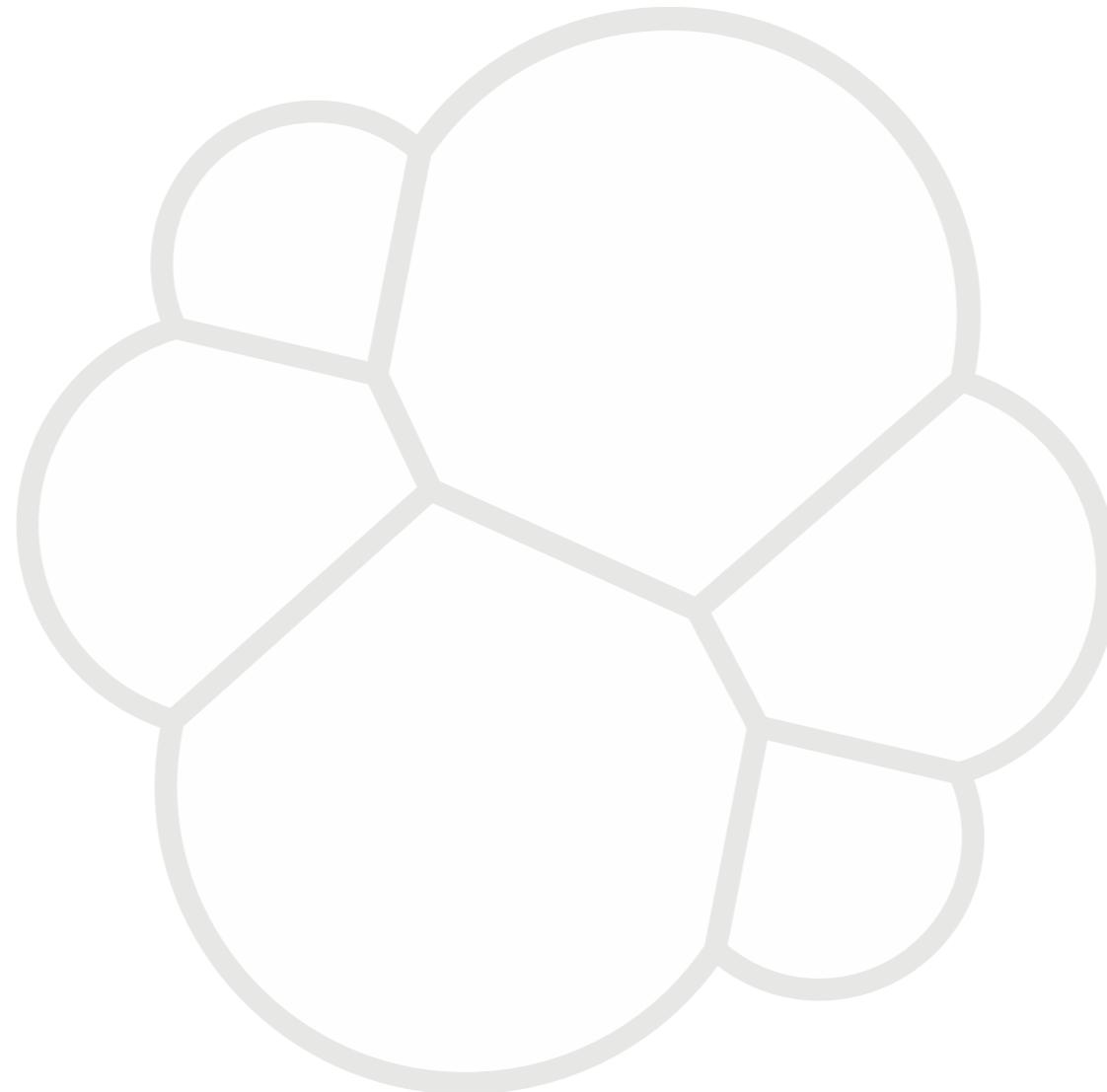
Sense is back!

```
Server localhost:9200 Development Trial Dashboards ⌵ ⌚ ⚙️ ?
```

```
1 DELETE /_all
2
3 PUT /test
4 {
5   "warmers" : {
6     "warmer_1" : {
7       "types" : [],
8       "source" : {
9         "query" : {
10          "match_all" : {}
11        }
12      }
13    }
14  }
15 }
16
17 GET /_all/_warmer
18
```

```
1 {
2   ".marvel-2015.10.26": {
3     "warmers": {}
4   },
5   "test": {
6     "warmers": {
7       "warmer_1": {
8         "types": [],
9         "source": {
10          "query": {
11            "match_all": {}
12          }
13        }
14      }
15    }
16  }
17 }
```

Resources





elastic **on** TOUR

We're bringing Elastic{ON} to you.

3 months, 12 cities, 7 countries.

Join us on tour.

Washington, D.C.

Oct 6

Amsterdam

Oct 29

London

Nov 3

Paris

Nov 5

München

Nov 10

New York

Nov 17

Chicago

Nov 19

Los Angeles

Dec 1

Seattle

Dec 3

Sydney

Dec 8

Melbourne

Dec 10

Tokyo

Dec 16

elastic **on** '16

Feb 17-19, 2016

Pier 48, San Francisco, CA

Last year, Elastic{ON} sold out in just one week.
The next one is in the works.
Sign up now to get updates so you don't miss out.

Be an Elastic{ON} speaker. We love a good story.

[Submit Your Talk](#)

(Updates include agenda announcements, priority registration openings, public ticket sales, and more.)

What happens at Elastic{ON}? [Check out the content from 2015.](#)

Interested in sponsoring? Send an e-mail to sponsor@elastic.co

#Elasticsearch 2.0 is coming...join
@ZacharyTong this Wed for a demo, feature
Qs, and more!
go.es.io/1XtBjsH



<https://www.elastic.co/webinars/elasticsearch-2-0-overview/>

Resources

- <https://imotov.github.io/presentations/what-s-new-in-elasticsearch-20.html>
- <https://www.elastic.co/blog/to-shade-or-not-to-shade>
- <https://www.elastic.co/blog/elasticsearch-unplugged>
- <https://www.elastic.co/blog/core-delete-by-query-is-a-plugin>
- <https://www.elastic.co/blog/staying-in-control-with-moving-averages-part-1>
- <https://www.elastic.co/blog/staying-in-control-with-moving-averages-part-2>
- <https://www.elastic.co/blog/better-query-execution-coming-elasticsearch-2-0>
- <https://www.elastic.co/blog/out-of-this-world-aggregations>
- <https://www.elastic.co/blog/store-compression-in-lucene-and-elasticsearch>
- <https://www.elastic.co/blog/great-mapping-refactoring>
- <https://www.elastic.co/blog/frame-of-reference-and-roaring-bitmaps>
- <https://www.elastic.co/blog/elasticsearch-2-0-0-beta1-released>
- <https://www.elastic.co/blog/elasticsearch-2-0-0-beta2-released>
- <https://www.elastic.co/blog/elasticsearch-2-0-0-rc1-released>

- <https://www.elastic.co/elasticon/tour/2015/muenchen>
- <https://www.elastic.co/elasticon/conf/2016/sf>

Q & A

Thanks for listening!

Alexander Reelsen
@spinscale
alex@elastic.co

We're hiring
<https://www.elastic.co/about/careers>

We're helping
<https://www.elastic.co/subscriptions>