

# Shield your cluster

Security with Elasticsearch



elastic

Alexander Reelsen

@spinscale

alex@elastic.co

# Agenda



# 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



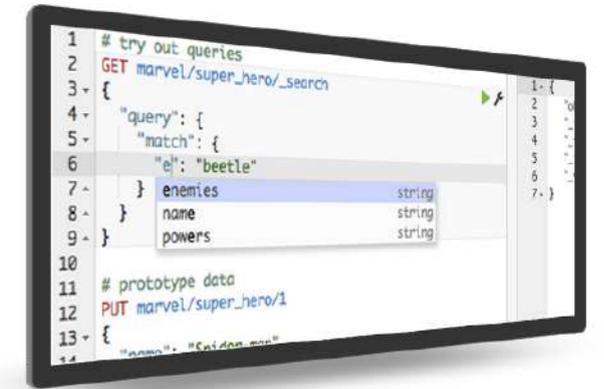
2012

2013

2014

 Series C investment

 Marvel released



# About



2012

2013

2014

2015

 Shield goes GA



 First user conference & rebrand

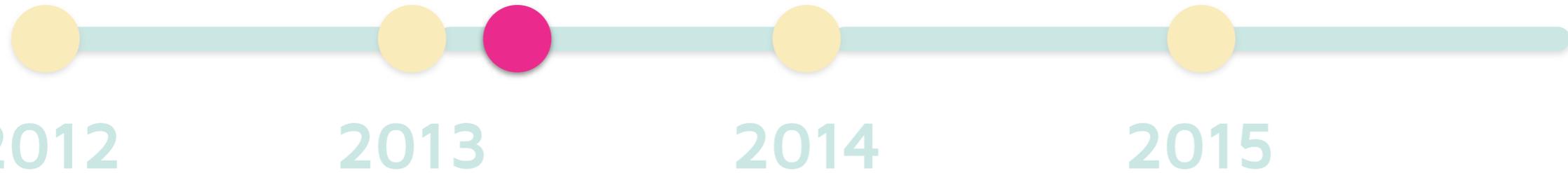


 Found acquired

 Packetbeat joins

 Watcher in beta

# About



 Joined in March 2013

 Working on Elasticsearch & Shield

 Development, Trainings, Conferences, Support, Blog posts

 We're hiring...



# Why?

 Elasticsearch: No security OOTB

 No encrypted communication

 No Authorization

 No Authentication

 No Audit Logging

# nginx in front



- 🐾 Filter by HTTP method, URI or IP
- 🐾 User management via basic auth
- 🐾 Use aliases & filters

# nginx in front



🐾 How to solve multi index operations?

```
GET /logs-2015.10.10,evil,logs-2015.10.11
{
  "query" : { "match_all" : {} }
}
```

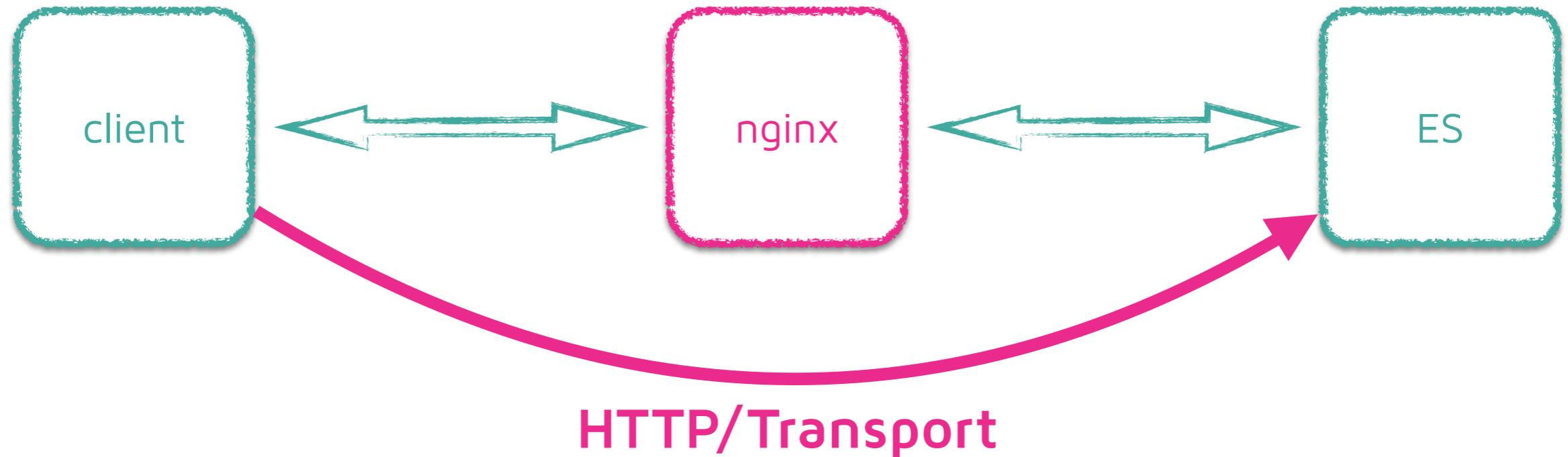
# nginx in front



🐾 How to solve bulk/multi operations?

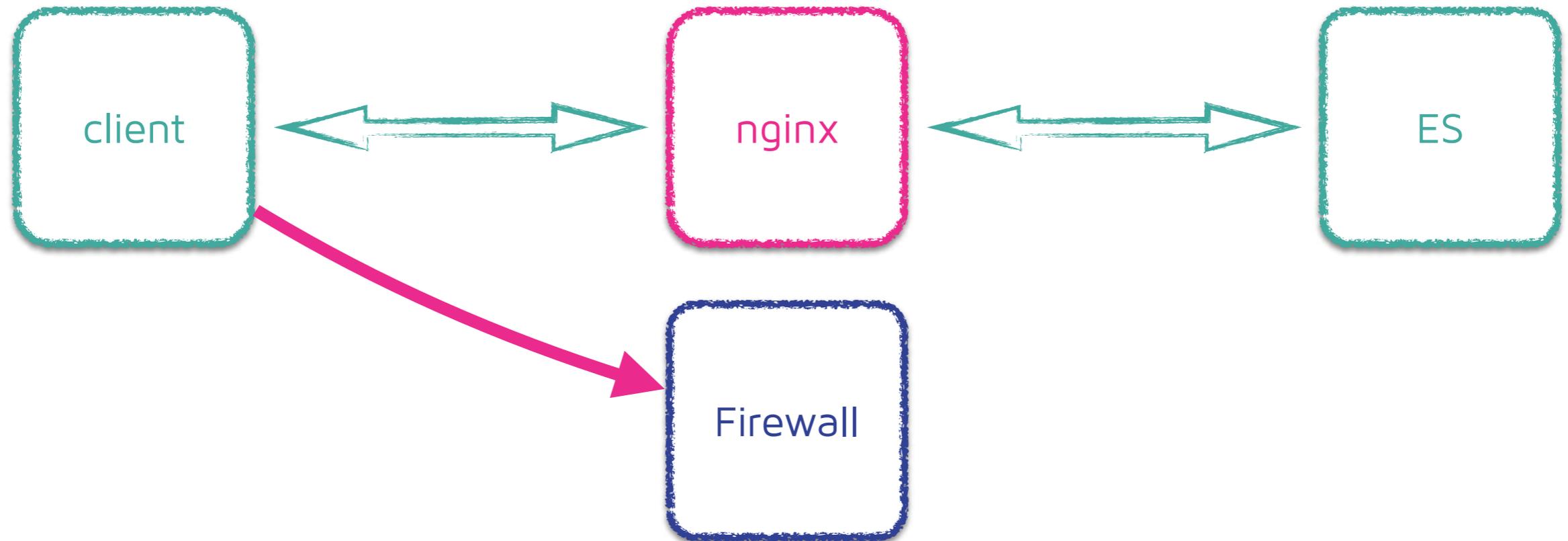
```
{ "index" : { "_index" : "test1", "_type" : "type1", "_id" : "1" } }  
{ "field1" : "value1" }  
{ "delete" : { "_index" : "test2", "_type" : "type1", "_id" : "2" } }  
{ "create" : { "_index" : "test3", "_type" : "type1", "_id" : "3" } }  
{ "field1" : "value3" }  
{ "update" : { "_id" : "1", "_type" : "type1", "_index" : "test4" } }  
{ "doc" : { "field2" : "value2" } }
```

# nginx in front

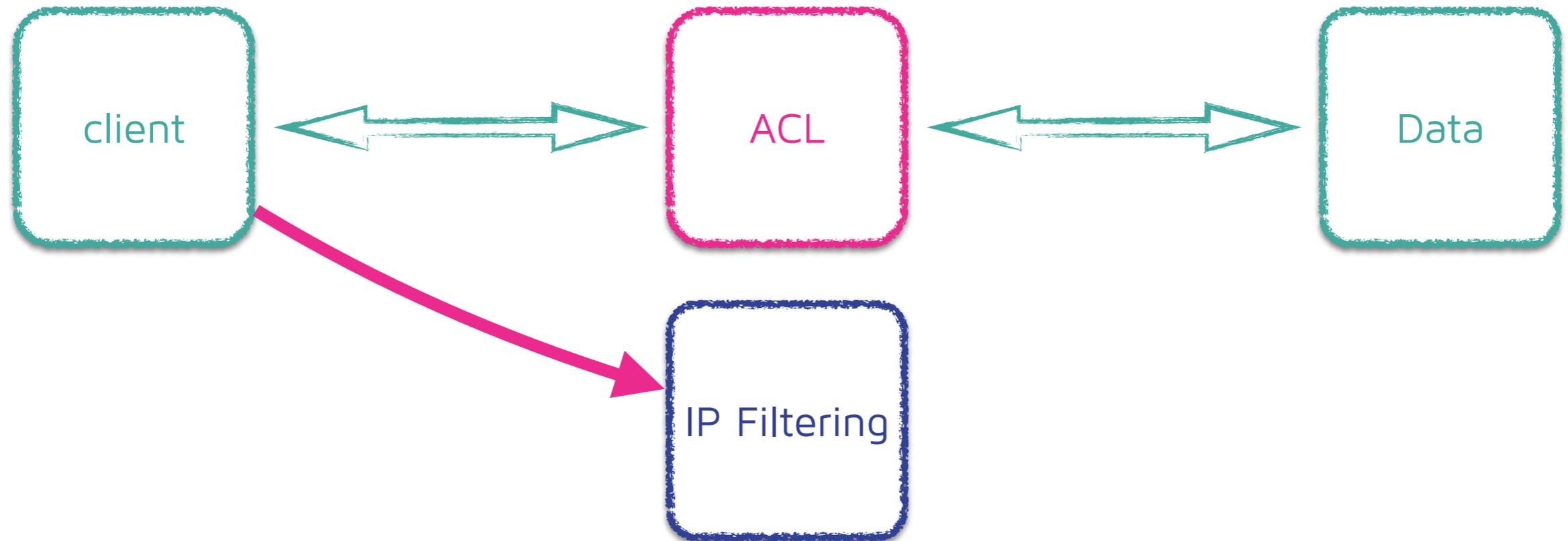


 Prevent unwanted accesses

# nginx in front

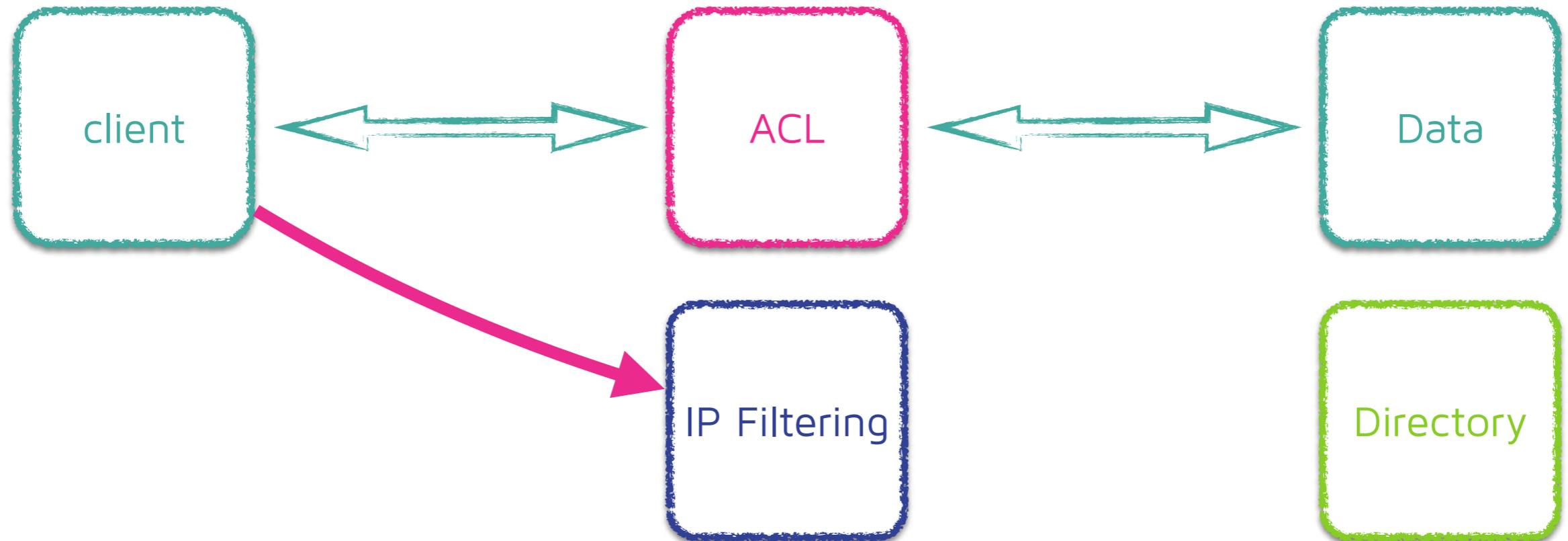


# operational overhead



🌐 Configuration scattered across systems

# operational overhead



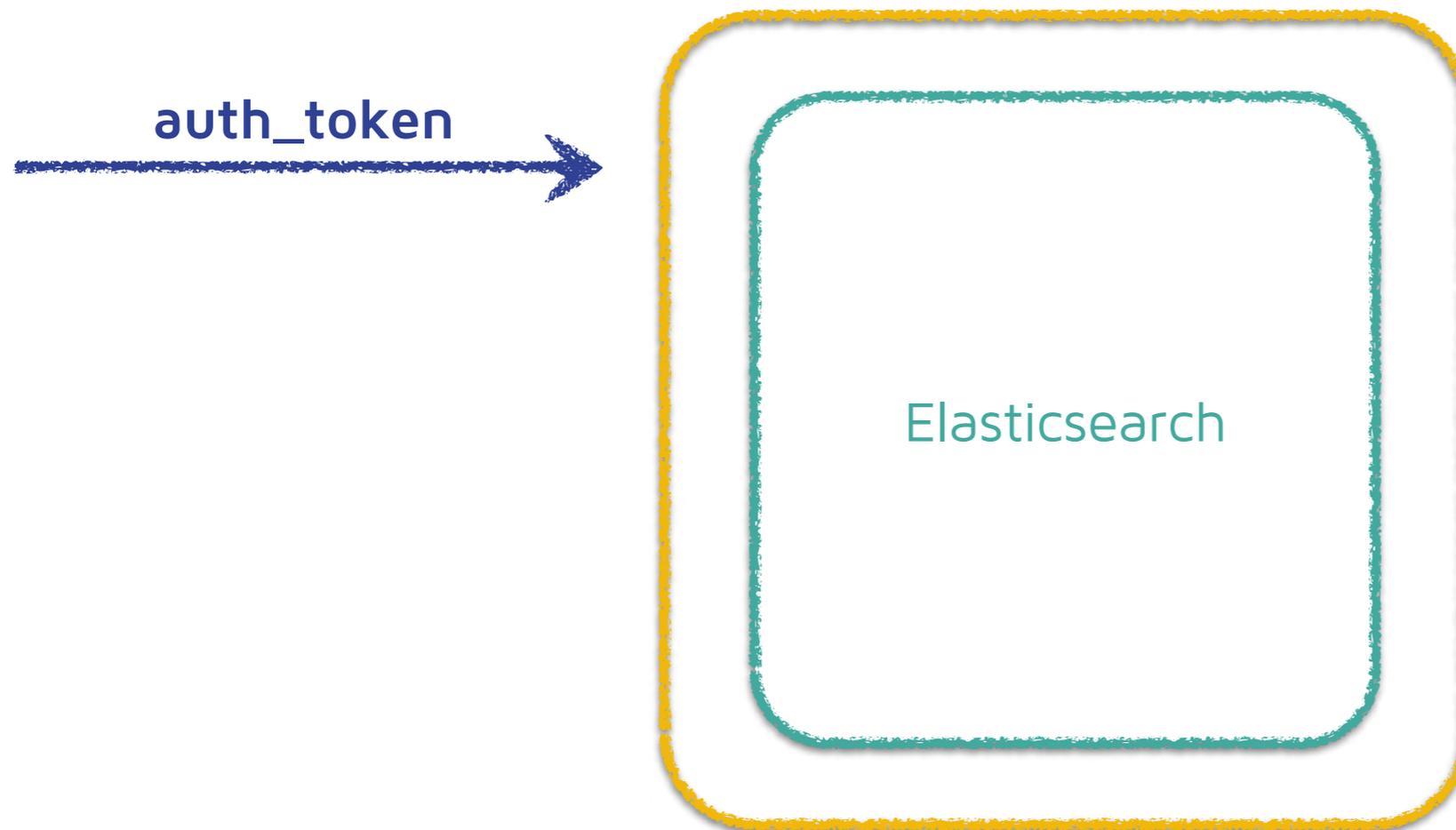
🌐 Configuration scattered across systems



# How?

- 🌸 Elasticsearch modular & pluggable
- 🌸 Security as a plugin
- 🌸 HTTP + Transport protocols
- 🌸 Integration into the ELK stack!

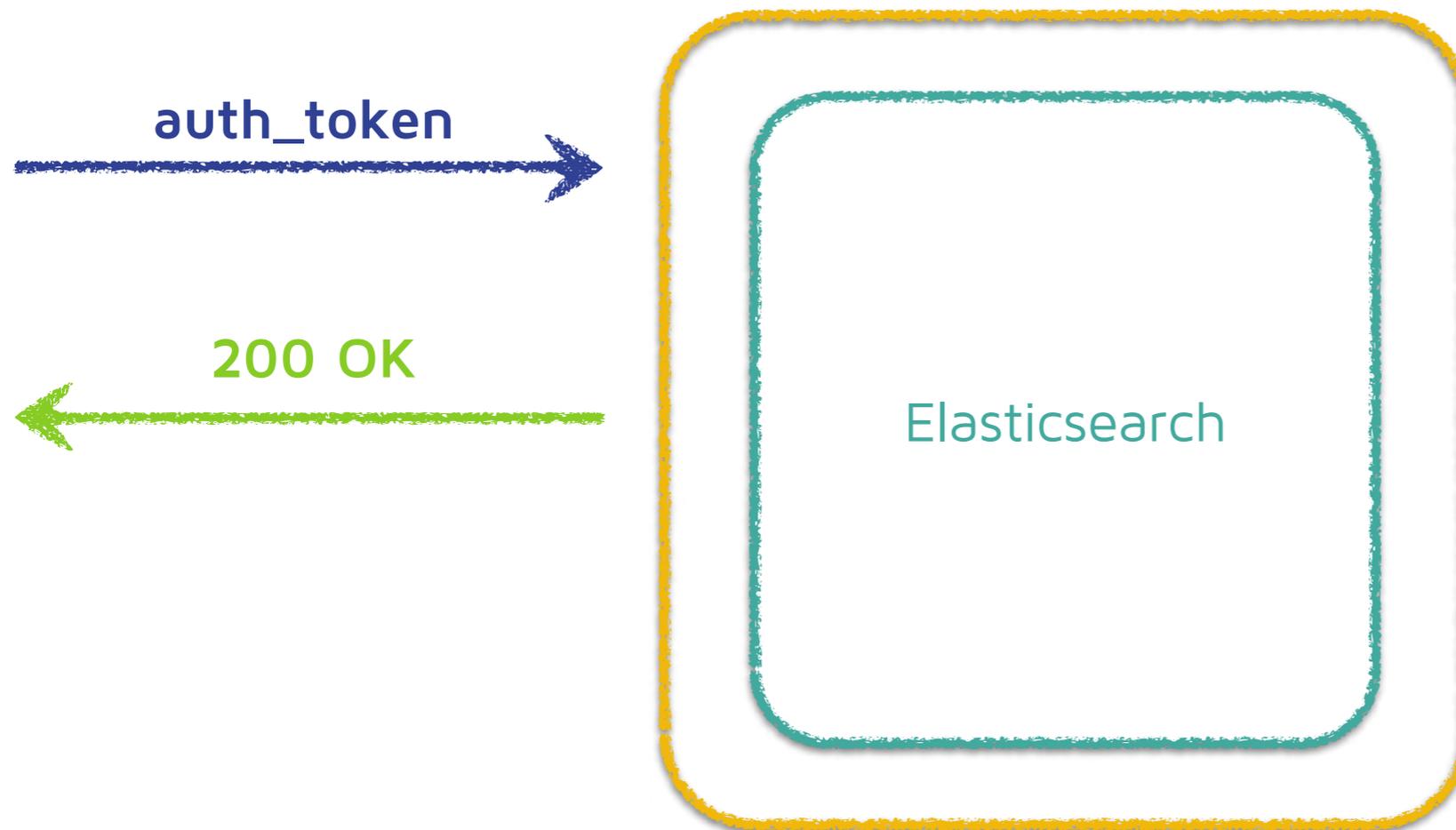
# How?



**Authentication**

**Authorization**

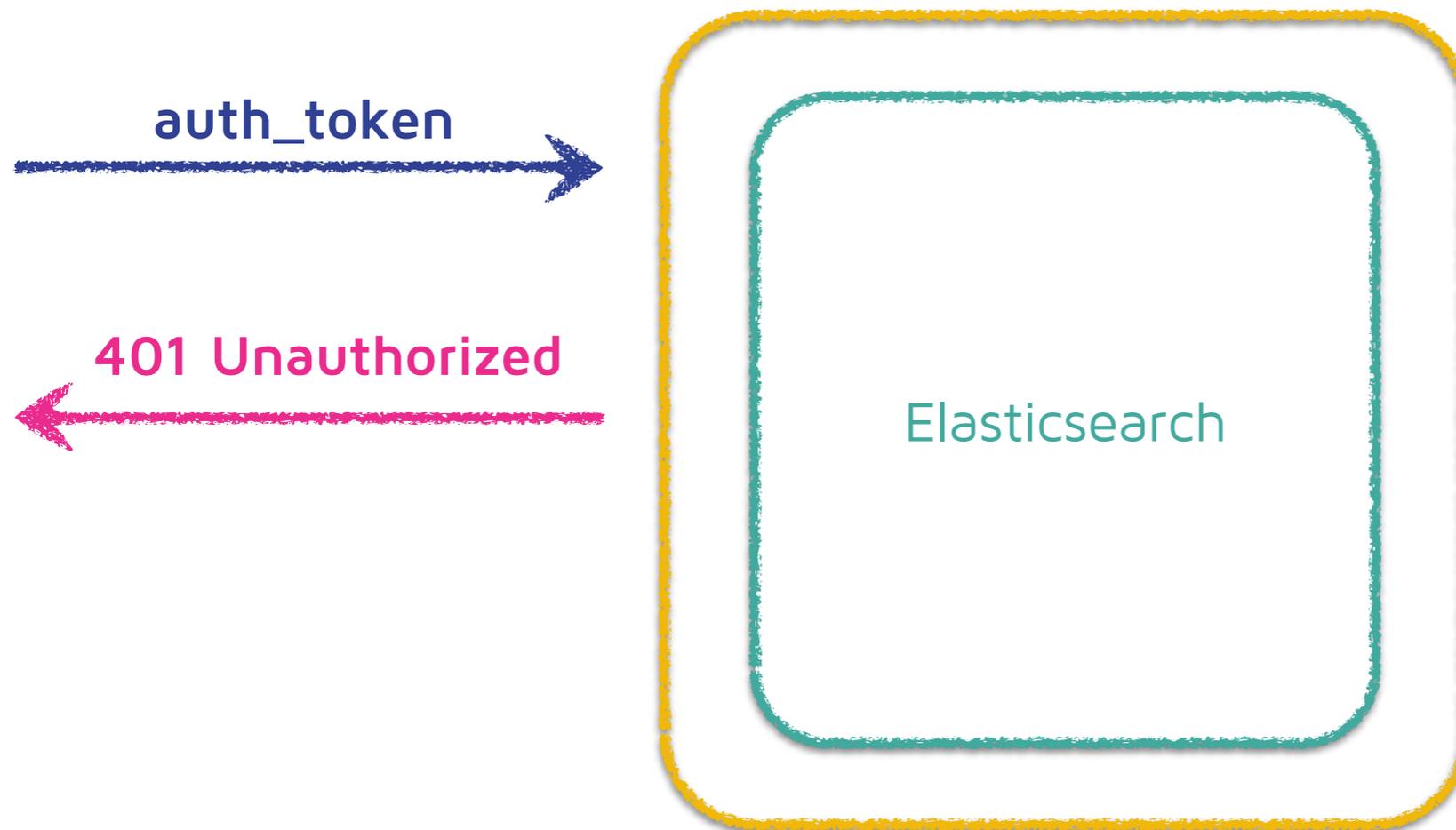
# How?



**Authentication**

**Authorization**

# How?



Authentication

Authorization

# How?

 Getting up and running is easy

 Install elasticsearch 1.6

```
bin/plugin install elasticsearch/license/latest
```

```
bin/plugin install elasticsearch/shield/latest
```



# What?

 IP Filtering

 Encrypted communication

 Authentication

 Authorization

 Audit Trail

# IP Filtering

- 🌸 Configurable in `elasticsearch.yml`
- 🌸 Can be updated dynamically via cluster update settings API

```
shield.transport.filter:  
  allow: "192.168.0.1"  
  deny: "192.168.0.0/24"
```

# Encrypted communication

 keystore required

 different config for HTTP and transport protocol (+profiles)

```
shield.ssl.keystore.path: /path/to/keystore.jks
shield.ssl.keystore.password: secret
shield.transport.ssl: true
shield.http.ssl: true
```

# Authentication

- 🌸 "Who are you?"
- 🌸 Auth mechanisms are called **realms**
- 🌸 Available: **esusers, ldap, ad, pki**
- 🌸 Realms can be chained
- 🌸 Support for caching & API for clearing

# Authentication

```
shield.authc:  
  realms:  
    esusers:  
      type: esusers  
      order: 0  
  
    ldap1:  
      type: ldap  
      order: 1  
      enabled: false  
      url: 'url_to_ldap1'  
      ...  
  
    ad1:  
      type: active_directory  
      order: 3  
      url: 'url_to_ad'
```

# ESUsers realm

- 🌿 Local files, can be changed via CLI
- 🌿 Elasticsearch watches file changes & reloads
- 🌿 `config/shield/users`
- 🌿 `config/shield/users_roles`

# ESusers realm

```
bin/shield/esusers useradd alex
```

```
bin/shield/esusers roles alex -a  
admin -r user
```

```
bin/shield/esusers list
```

```
bin/shield/esusers userdel alex
```

# Anonymous access

- 🌸 Fallback to configurable user
- 🌸 Disabled by default

```
shield.authc:  
  anonymous:  
    username: anonymous_user  
    roles: role1, role2
```



# Authorization

- 🌸 "Are you allowed to do that?"
- 🌸 `File: config/shield/roles.yml`

```
admin:  
  cluster: all  
  indices:  
    '*': all
```

# Role Based Access Control

## role

named set of permissions

## permission

set of cluster wide privileges

set of indices/aliases specific privileges

## privilege

set of one or more action names

`/_search` ↔ `indices:data/read/search`

# Role Based Access Control

role

permission

```
admin:  
  cluster: all  
  indices:  
    '*': all
```

# Authorization

```
user:  
  indices:  
    '*': read
```

```
events_user:  
  indices:  
    'events_*': read
```

# Authorization

```
logfile_user_readonly:  
  indices:  
    "logstash-201?-*": read
```

```
get_user:  
  indices:  
    'events_index': 'indices:data/read/get'
```

# Audit Trail

- Writes an own audit log file
- Implemented as logger
- Logs different types of event based on log level  
(ip filtering, tampered requests, access denied, auth failed)

```
shield.audit.enabled: true
```

# Integration

 Transport Client

 Logstash

 Kibana 3/4

 Watcher

 Marvel

# Transport Client

```
TransportClient client = new TransportClient(builder()
    .put("cluster.name", "myClusterName")

    .put("shield.user", "test_user:changeme")

    .put("shield.ssl.keystore.path", "/path/to/client.jks")
    .put("shield.ssl.keystore.password", "password")
    .put("shield.transport.ssl", "true"))

    .addTransportAddress(new
InetSocketAddressTransportAddress("localhost", 9300));
```



# Who?

 Use-case 1: Monitoring application

 No write access

 Cluster Health

 Nodes stats/info

 Indices Stats

# Use-case 2: Logstash

- 🌸 No read access (unless input is used)
- 🌸 Indices: Indexing
- 🌸 Cluster: Index templates

# Use-case 3: Marvel

```
marvel_user:
  cluster: cluster:monitor/nodes/info,
           cluster:admin/plugin/license/get
  indices:
    '.marvel-*': all

marvel_agent:
  cluster: indices:admin/template/get,
           indices:admin/template/put
  indices:
    '.marvel-*': indices:data/write/bulk, create_index
```

# Use-case 4: Ecommerce

```
bulk:  
  indices:  
    'products_*': write, manage, read  
  
updater:  
  indices:  
    'products': index, delete, indices:admin/optimize  
  
webshop:  
  indices:  
    'products': search, get
```

# Use-case 4: Ecommerce

```
monitoring:  
  cluster: monitor  
  indices:  
    '*': monitor  
  
sales_rep :  
  indices:  
    'sales_*' : all  
    'social_events' : data_access, monitor
```



# Next?

- 🌸 Simplify SSL configuration
- 🌸 API driven user/role management
- 🌸 Open up realms API
- 🌸 Field-level security
- 🌸 Index Audit Trail into ES



# 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>

# Resources



## Shield documentation

<https://www.elastic.co/guide/en/shield/current/index.html>



## Shield: Security in ELK

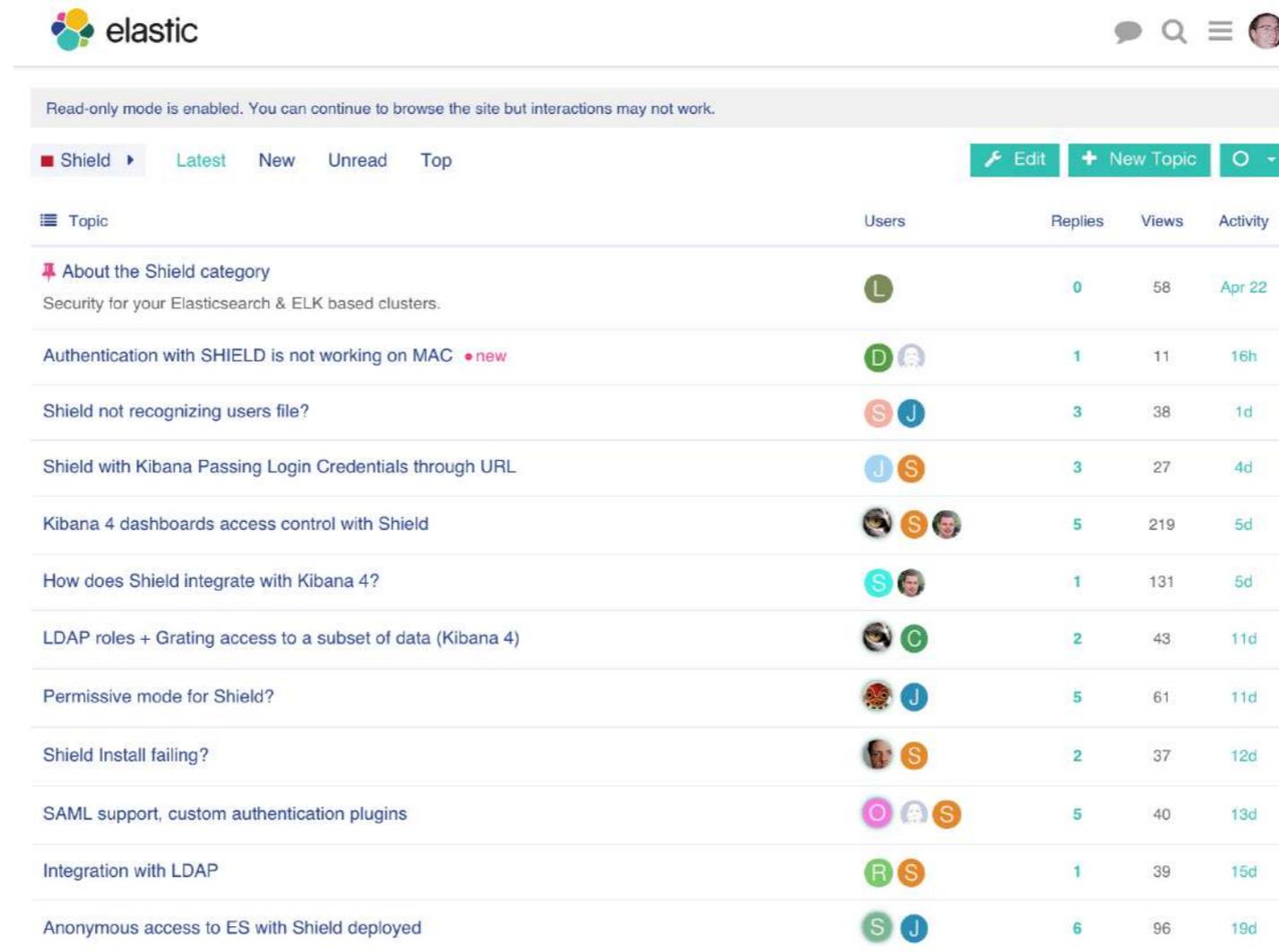
<https://www.elastic.co/elasticon/2015/sf/security-in-elk>



## Shield and Beyond: Recommendations for a Secure ELK Environment

<https://www.elastic.co/webinars/shield-and-beyond>

# Resources



elastic

Read-only mode is enabled. You can continue to browse the site but interactions may not work.

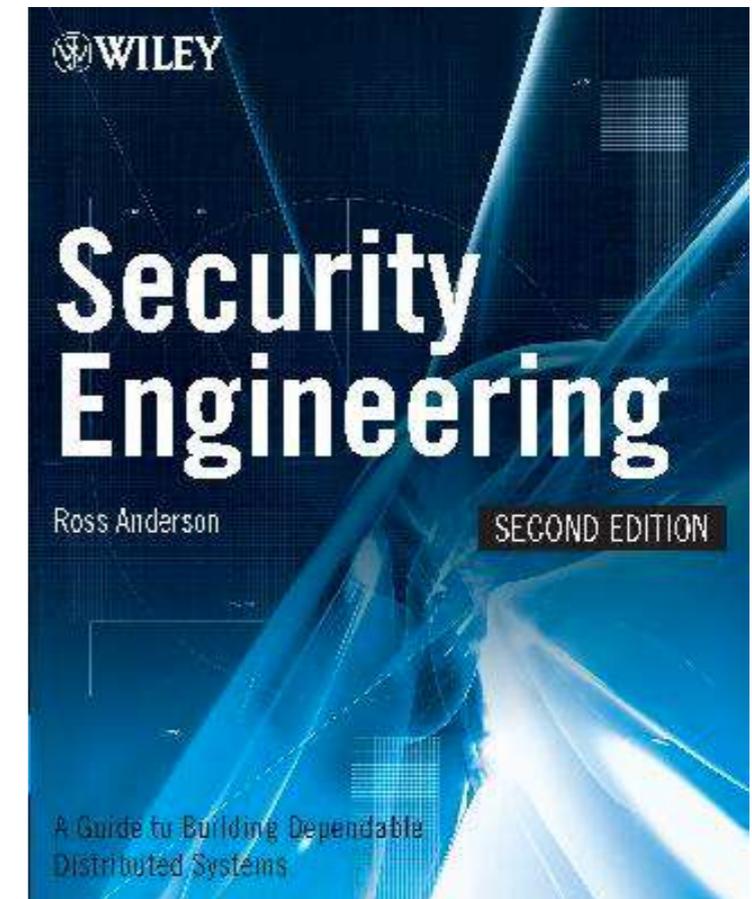
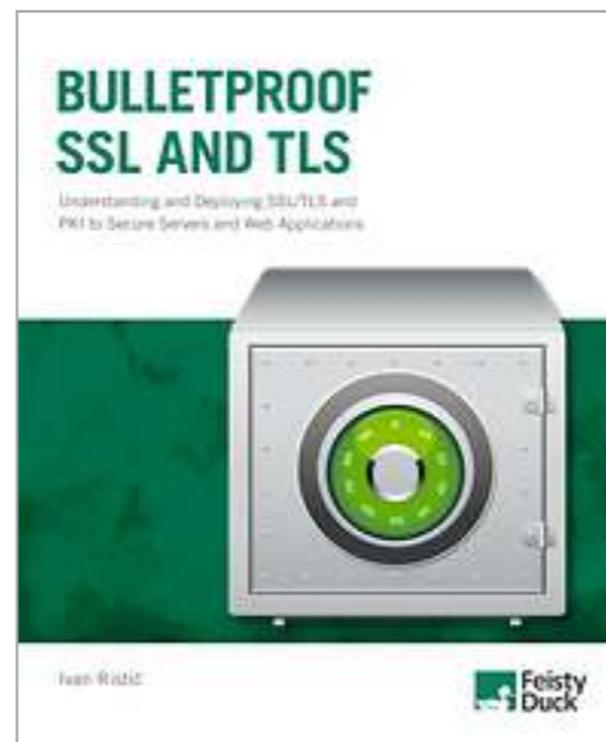
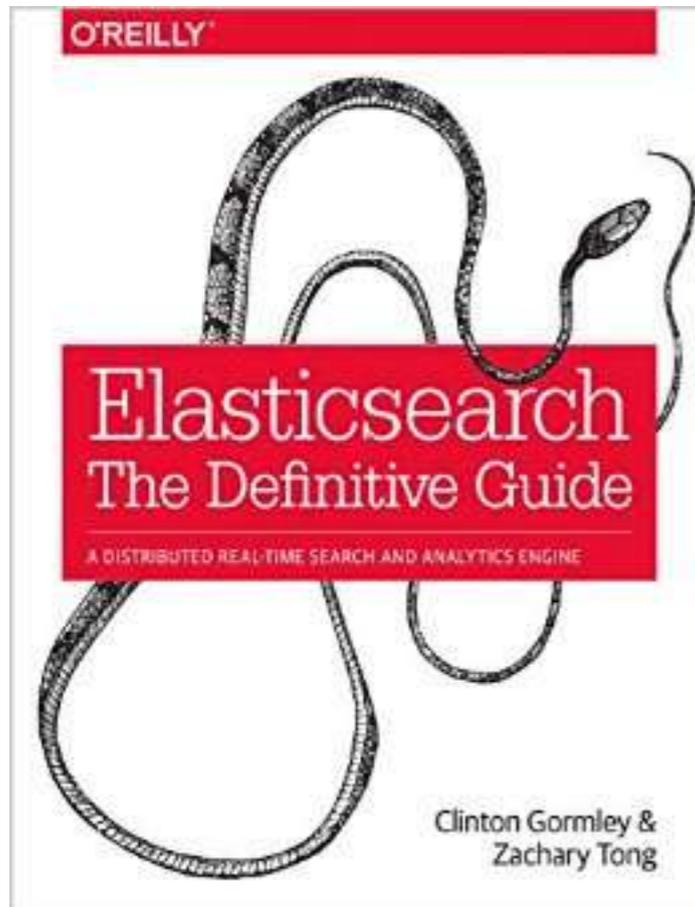
Shield ▾ Latest New Unread Top

Edit + New Topic

Topic	Users	Replies	Views	Activity
<b>About the Shield category</b> Security for your Elasticsearch & ELK based clusters.	L	0	58	Apr 22
Authentication with SHIELD is not working on MAC • new	D	1	11	16h
Shield not recognizing users file?	S J	3	38	1d
Shield with Kibana Passing Login Credentials through URL	J S	3	27	4d
Kibana 4 dashboards access control with Shield	S	5	219	5d
How does Shield integrate with Kibana 4?	S	1	131	5d
LDAP roles + Grating access to a subset of data (Kibana 4)	C	2	43	11d
Permissive mode for Shield?	J	5	61	11d
Shield Install failing?	S	2	37	12d
SAML support, custom authentication plugins	O S	5	40	13d
Integration with LDAP	R S	1	39	15d
Anonymous access to ES with Shield deployed	S J	6	96	19d

<https://discuss.elastic.co/c/shield>

# Resources



# Resources



**Find**  
a Meetup Group

**Start**  
a Meetup Group

## ElasticSearch Meetups

Find out what's happening in ElasticSearch Meetup groups around the world and start meeting up with the ones near you.



**Groups**  
**114**

**Members**  
**27,667**

**Interested**  
**2,229**

**Cities**  
**81**

**Countries**  
**29**

# 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>