

ELK_01_Andrei_Sheihus Report.

Applications Places Firefox en Tue 06:39

Kibana - Mozilla Firefox


centos7 [Elastic [justmeai M Входящ G Create G google Create logstash Logstash M Gist con Logstash 192.168 Kiban Apache

192.168.56.101:5601/app/kibana#/home?_g=()

Home

Add Data to Kibana


Use these solutions to quickly turn your data into pre-built dashboards and monitoring systems.



APM

APM automatically collects in-depth performance metrics and errors from inside your applications.


[Add APM](#)



Logging

Ingest logs from popular data sources and easily visualize in preconfigured dashboards.


[Add log data](#)



Metrics

Collect metrics from the operating system and services running on your servers.

[Add metric data](#)



Security analytics

Centralize security events for interactive investigation in ready-to-go visualizations.

[Add security events](#)

[Add sample data](#)
Load a data set and a Kibana dashboard

[Upload data from log file](#)
Import a CSV, NDJSON, or log file

[Use Elasticsearch data](#)
Connect to your Elasticsearch index

192.168.56.101:5601/app/kibana#/home/tutorial_directory/security

Kibana - Mozilla Firefox mc [user@myhost]:~/.elk mc [root@tomcat]:/var/log/logstash elk 1 / 4

Applications Places Firefox en Tue 06:43

Kibana - Mozilla Firefox

centos7 [Elastic [justmeai M Входящ G Create G google Create logstash Logstash M Gist con Logstash 192.168 Kiban Apache

192.168.56.101:5601/app/kibana#/management/kibana/index_pattern?_g=()

Management / Index patterns / Create index pattern

Create index pattern

Kibana uses index patterns to retrieve data from Elasticsearch indices for things like visualizations.

☐ Include system indices

Step 1 of 2: Define index pattern

Index pattern

fil*

You can use a * as a wildcard in your index pattern.
You can't use spaces or the characters \, /, ?, *, <, >, |.

[Next step](#)

✓ **Success!** Your index pattern matches **1 index**.

filebeat-2019.07.09

Rows per page: 10

Kibana

- Index Management
- Index Lifecycle Policies
- Rollup Jobs
- Cross-Cluster Replication
- Remote Clusters
- Snapshot Repositories
- License Management
- 8.0 Upgrade Assistant

- Index Patterns
- Saved Objects
- Spaces
- Reporting
- Advanced Settings

Kibana - Mozilla Firefox mc [user@myhost]:~/.elk mc [root@tomcat]:/var/log/logstash elk ELK_01_Andrei_Sheihus.odt - Libre... 1 / 4

ApplicationsPlacesFirefox

enTue 06:43

Kibana - Mozilla Firefox

centos7[Elastic]justmeaiВходящCreateGgooglehCreateGlogstashLogstashMLogstasGist conLogstas192.168KibanxApache

192.168.56.101:5601/app/kibana#/management/kibana/index._pattern?_g=()

Management / Index patterns / Create index pattern

Elasticsearch

Index Management

Index Lifecycle Policies

Rollup Jobs

Cross-Cluster Replication

Remote Clusters

Snapshot Repositories

License Management

8.0 Upgrade Assistant

Kibana

Index Patterns

Saved Objects

Spaces

Reporting

Advanced Settings

Create index pattern

Kibana uses index patterns to retrieve data from Elasticsearch indices for things like visualizations.

☐ Include system indices

Step 2 of 2: Configure settings

You've defined **fil*** as your index pattern. Now you can specify some settings before we create it.

Time Filter field name Refresh

@timestamp

The Time Filter will use this field to filter your data by time. You can choose not to have a time field, but you will not be able to narrow down your data by a time range.

[Show advanced options](#)

[< Back](#) [Create index pattern](#)

Kibana - Mozilla Firefoxmc [user@myhost]:~/elkmc [root@tomcat]:/var/log/logstashelkELK_01_Andrei_Sheihus.odt - Libre...1 / 4

ApplicationsPlacesFirefox

enTue 06:44

fil* - Kibana - Mozilla Firefox

centos7[Elastic]justmeaiВходящCreateGgooglehCreateGlogstashLogstashMLogstasGist conLogstas192.168fil* - xApache

192.168.56.101:5601/app/kibana#/management/kibana/index._patterns/e05d39a0-a1fb-11e9-ad0a-bf333de565

Management / Index patterns / fil*

Elasticsearch

Index Management

Index Lifecycle Policies

Rollup Jobs

Cross-Cluster Replication

Remote Clusters

Snapshot Repositories

License Management

8.0 Upgrade Assistant

Kibana

Index Patterns

Saved Objects

Spaces

Reporting

Advanced Settings

★ fil*

Time Filter field name: @timestamp

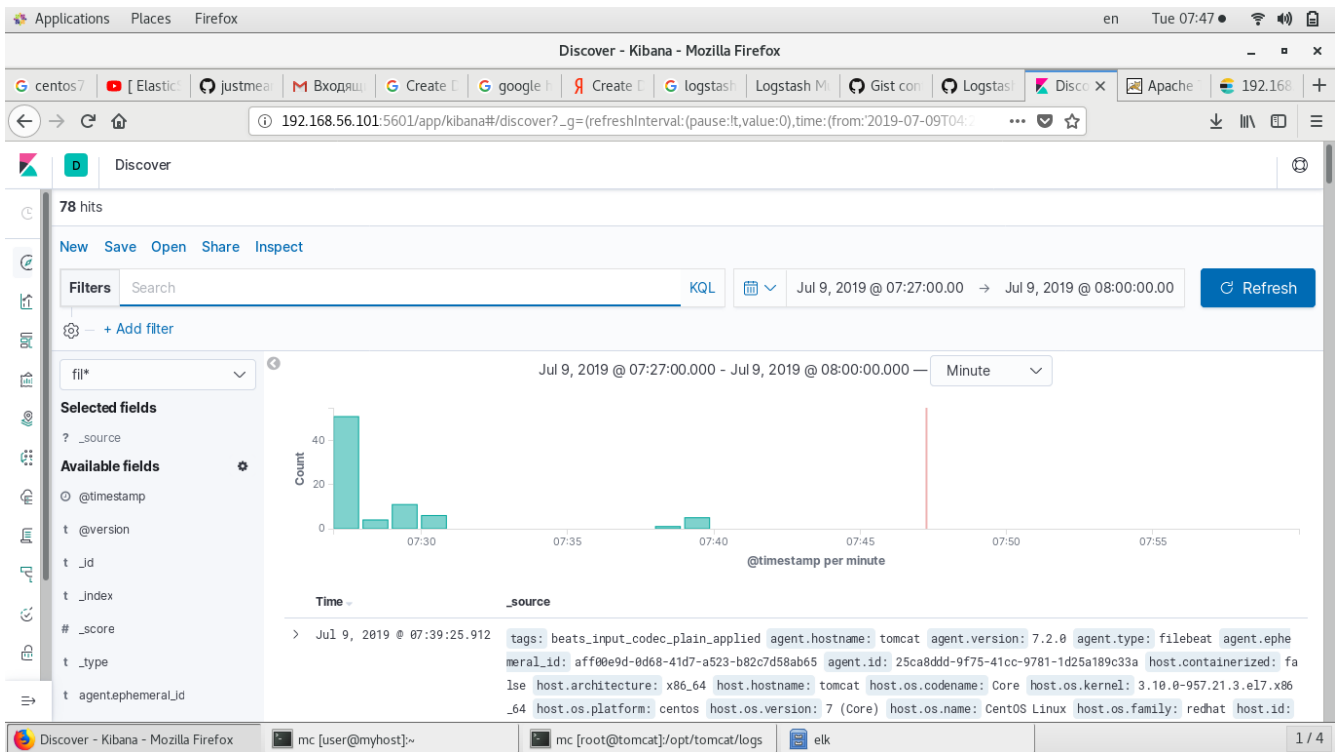
This page lists every field in the **fil*** index and the field's associated core type as recorded by Elasticsearch. To change a field type, use the Elasticsearch [Mapping API](#)

Fields (60)Scripted fields (0)Source filters (0)

Q FilterAll field types

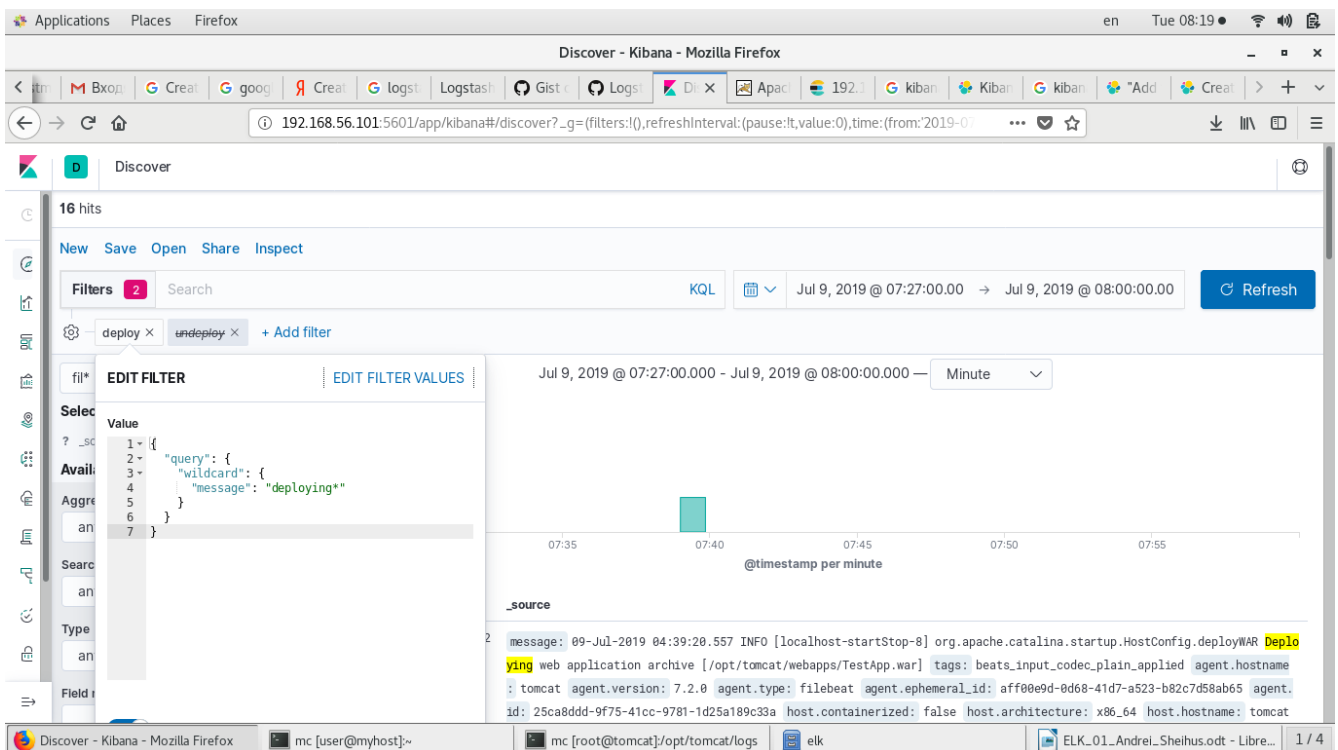
Name	Type	Format	Searchable	Aggregatable	Excluded
@timestamp	date		•	•	✎
@version	string		•		✎
@version.keyword	string		•	•	✎
_id	string		•	•	✎
_index	string		•	•	✎

fil* - Kibana - Mozilla Firefoxmc [user@myhost]:~/elkmc [root@tomcat]:/var/log/logstashelkELK_01_Andrei_Sheihus.odt - Libre...1 / 4

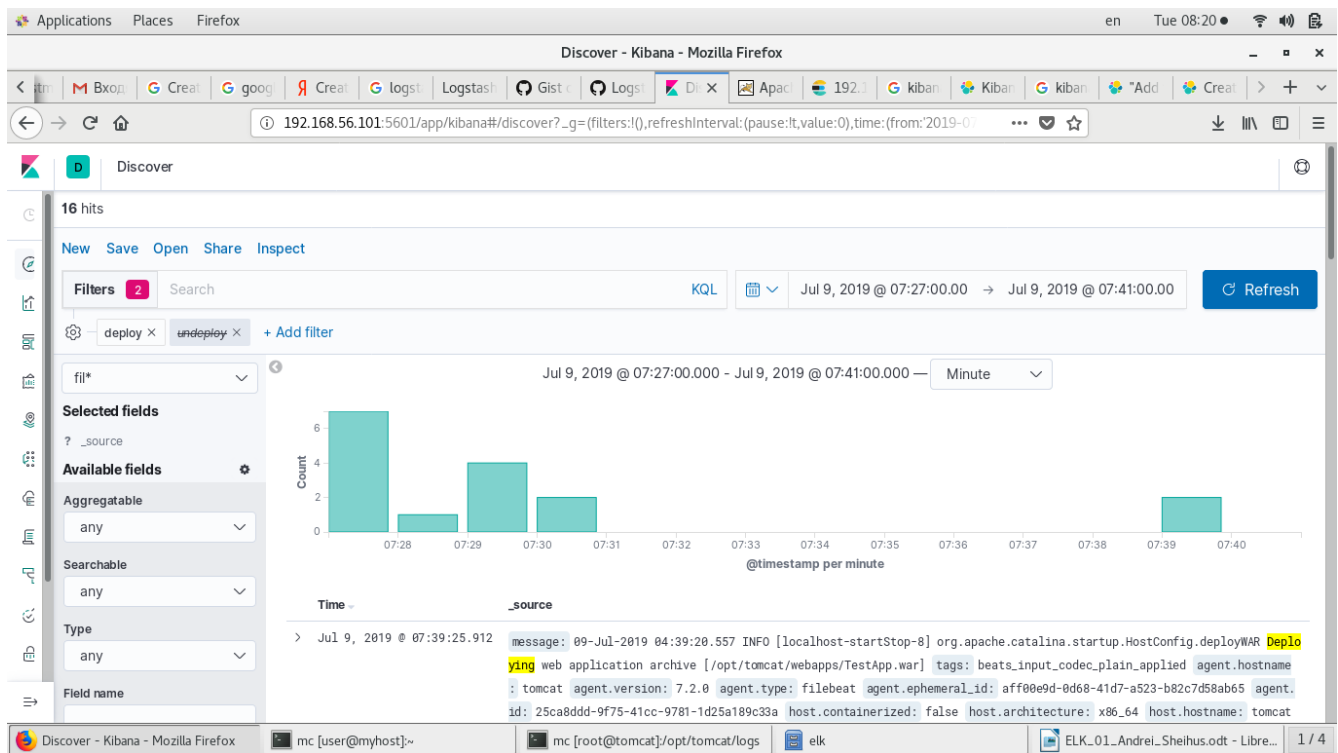


Creating kibana filters:

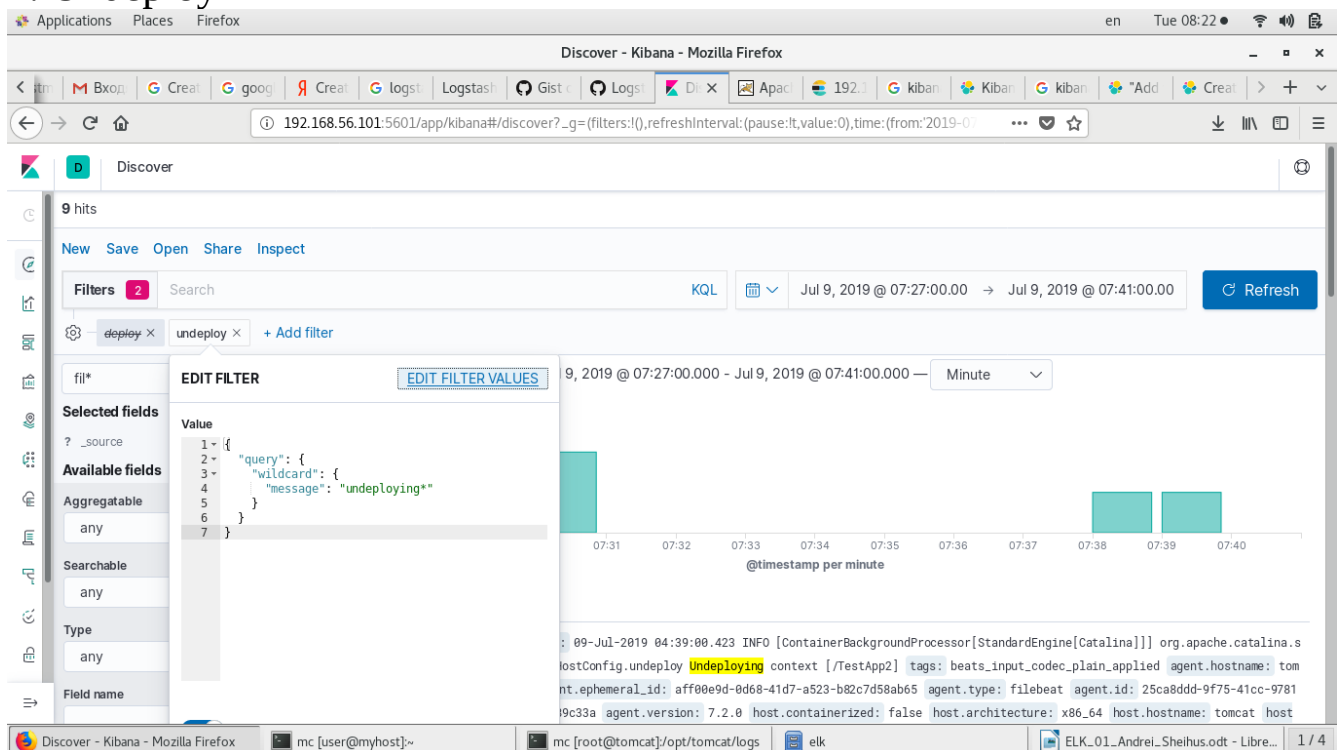
1. Deploy



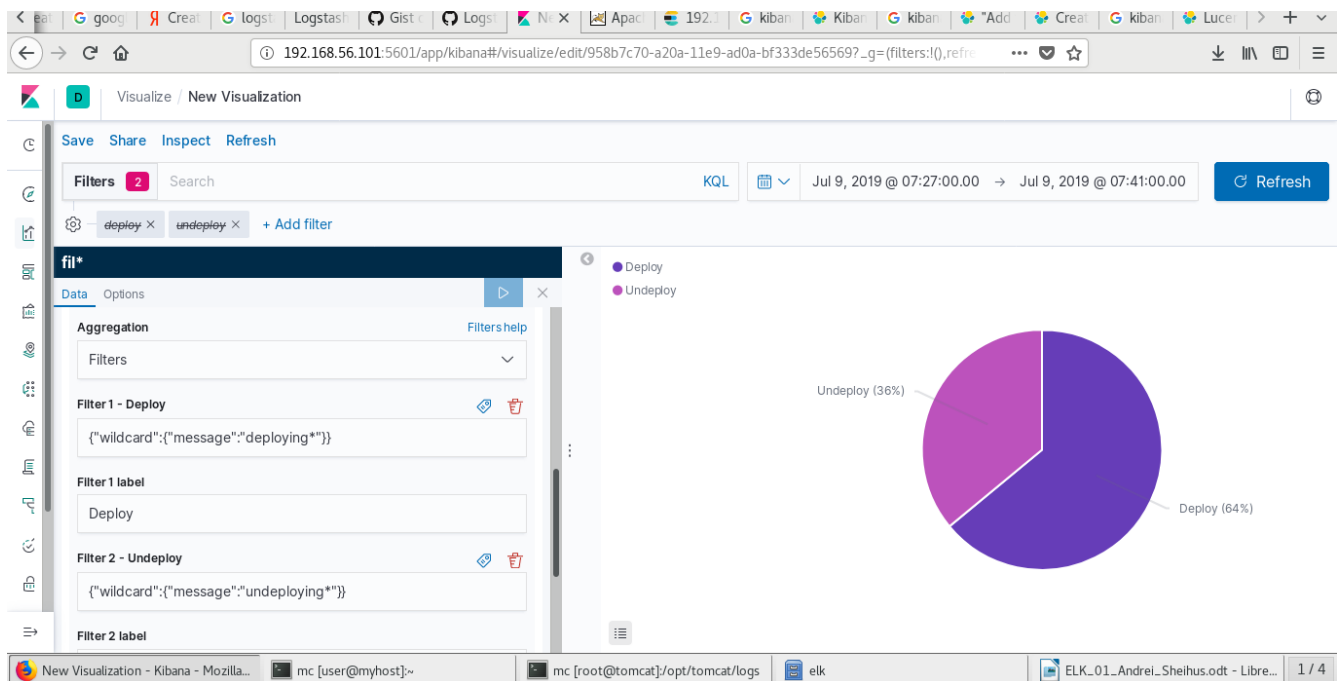
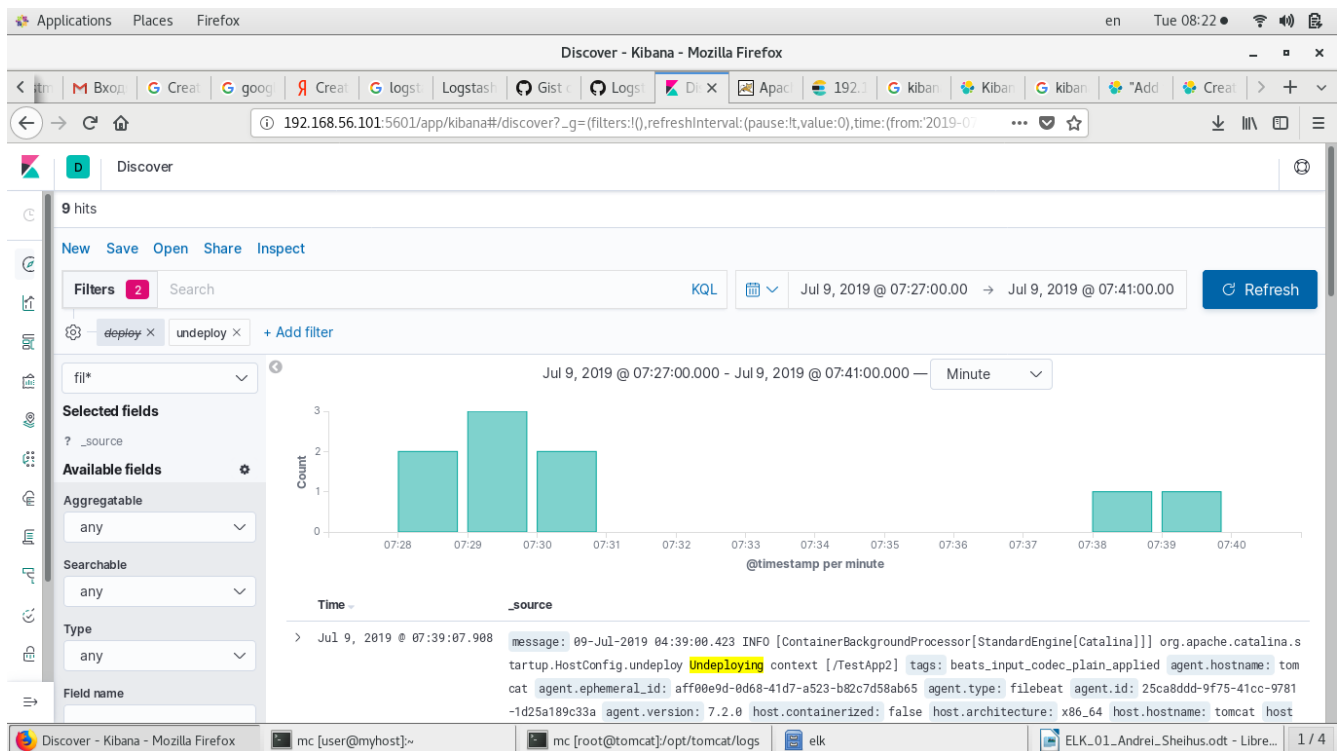
Total deployments:

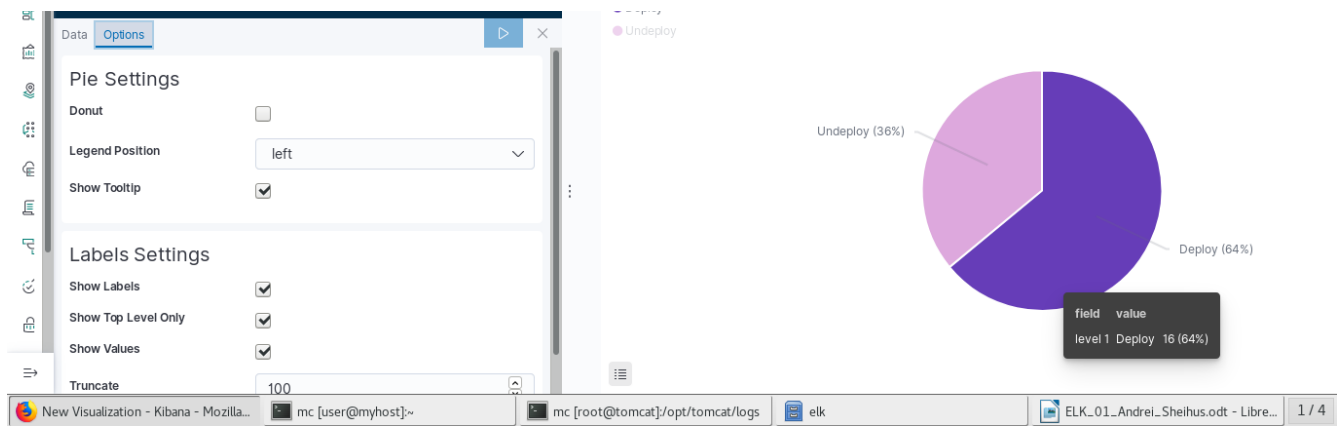


2. Undeploy



Total undeployments:





Elasticsearch health status:
http://192.168.56.101:9200/_cat/health?v

epoch	timestamp	cluster	status	node.total	node.data	shards	pri	relo	init	unassign	pending_tasks	max_task_wait_time	active_shards_percent
1562646689	04:31:29	my-application	yellow	1	1	3	3	0	0	1	0	-	75.0%

Elasticsearch indexes:

health	status	index	uuid	pri	rep	docs.count	docs.deleted	store.size	pri.store.size
green	open	.kibana_task_manager	4jul6TU0R6qIMb2V_8ctwQ	1	0	2	0	45.6kb	45.6kb
yellow	open	filebeat-2019.07.09	0IabnIvSS3Snlg1f4d0u0g	1	1	78	0	177.3kb	177.3kb
green	open	.kibana_1	h7eU51k_SLOEXI2B64Ps6Q	1	0	7	0	52.6kb	52.6kb