

Elasticsearch sees appropriate log (logstash-*)

```
[root@elastic tomcat]# curl 192.168.10.20:9200/_cat/indices
green open .kibana_1 yz-isK0IQcaYHBaWtVrzZA 1 0 4 0 30.8kb 30.8kb
yellow open logstash-2019.07.08-000001 V4FmySNiTBiQZtipG0DQrg 1 1 220 0 50.6kb 50.6kb
green open .kibana_task_manager qEda0rxTQamfKpQcViuEWw 1 0 2 0 45.6kb 45.6kb
[root@elastic tomcat]#
```

Creating index pattern

Help us improve the Elastic Stack by providing usage statistics for basic features. We will not share this data outside of Elastic. [Read more](#)

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 1 of 2: Define index pattern

Index pattern

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

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

logstash-2019.07.08-000001

Rows per page: 10 ▾

[> Next step](#)

Help us improve the Elastic Stack by providing usage statistics for basic features. We will not share this data outside of Elastic. [Read more](#)

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 **logstash-*** 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](#)

Yes

No

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

logstash-*

Time Filter field name: @timestamp

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

Fields (16)

Scripted fields (0)

Source filters (0)

Filter

All field types

Name	Type	Format	Searchable	Aggregatable	Excluded
@timestamp	date		•	•	
@version	string		•	•	
_id	string		•	•	
_index	string		•	•	
_score	number				
_source	_source				
_type	string		•	•	
geoip.ip	ip		•	•	
geoip.latitude	number		•	•	
geoip.location	geo_point		•	•	

Heath status

```
[root@tomcat conf.d]# curl -XGET 'http://192.168.10.20:9200/_cluster/health?pretty'
{
  "cluster_name" : "elasticsearch",
  "status" : "yellow",
  "timed_out" : false,
  "number_of_nodes" : 1,
  "number_of_data_nodes" : 1,
  "active_primary_shards" : 4,
  "active_shards" : 4,
  "relocating_shards" : 0,
  "initializing_shards" : 0,
  "unassigned_shards" : 1,
  "delayed_unassigned_shards" : 0,
  "number_of_pending_tasks" : 0,
  "number_of_in_flight_fetch" : 0,
  "task_max_waiting_in_queue_millis" : 0,
  "active_shards_percent_as_number" : 80.0
}
```

Management / Index management

Help us improve the Elastic Stack by providing usage statistics for basic features. We will not share this data outside of Elastic. Read more

YesNo

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

Index Management

Update your Elasticsearch indices individually or in bulk.

Include rollout indices

Include system indices

Search

Lifecycle status

Lifecycle phase

Reload indices

Name	Health	Status	Primaries	Replicas	Docs count	Storage size
<input type="checkbox"/> kibana_sample_data_logs	green	open	1	0	14074	11.5mb
<input type="checkbox"/> logstash-2019.0708-000001	yellow	open	1	1	106	19.1kb

Rows per page: 10

Creating filters (Deployment/undeployment)

Discover

Help us improve the Elastic Stack by providing usage statistics for basic features. We will not share this data outside of Elastic. Read more

YesNo

3 hits

New Save Open Share Inspect

Filters

message is one of Deployment

log: message is one of Deployment

EDIT FILTER

Field: message

Operator: is one of

Values: Deployment

Create custom label?

Save

Jul 8, 2019 @ 13:53:59.821 - Jul 8, 2019 @ 18:53:59.822

Auto

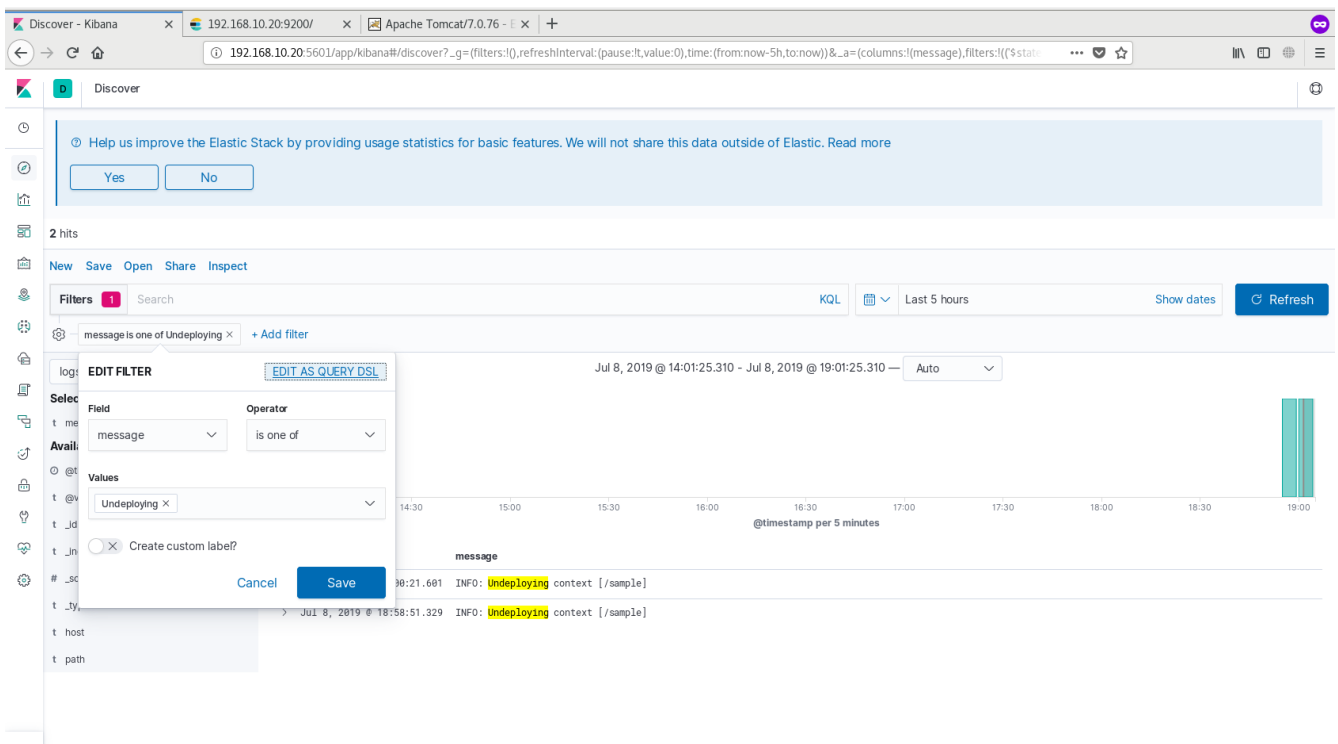
@timestamp per 5 minutes

message

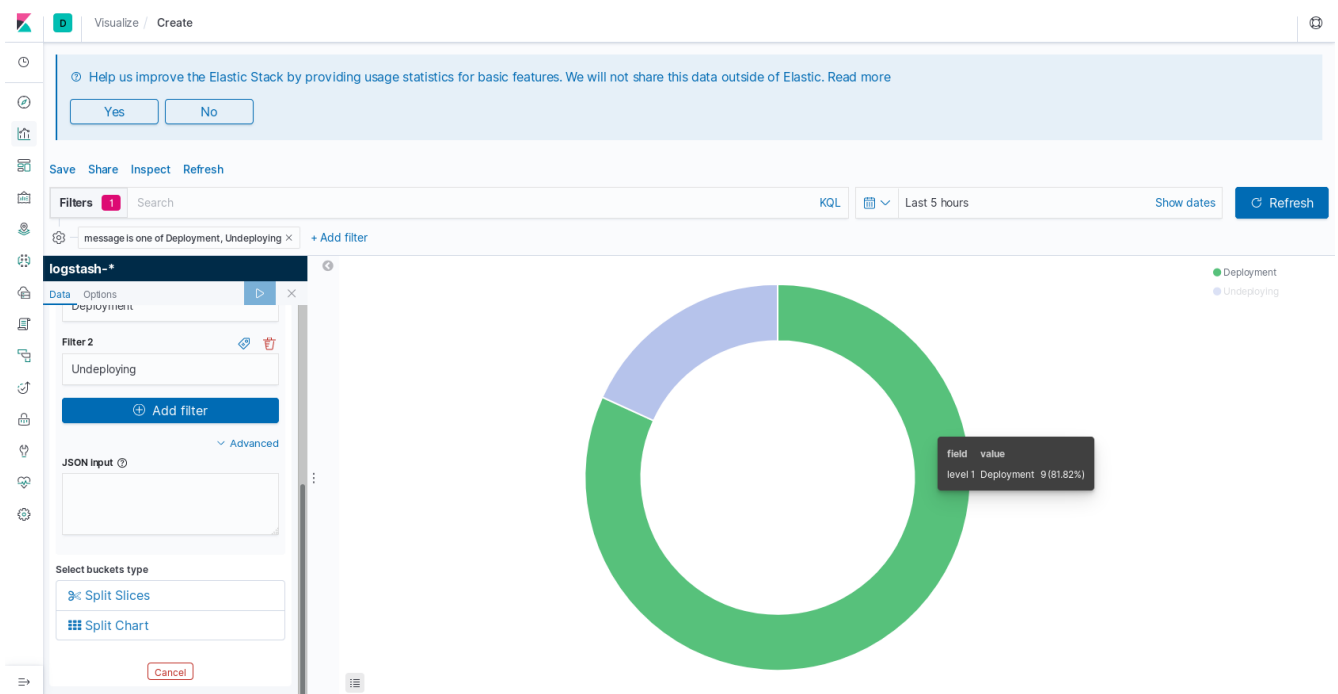
14:20.218 INFO: Deployment of web application directory /var/lib/tomcat/webapps/sample has finished in 139 ms

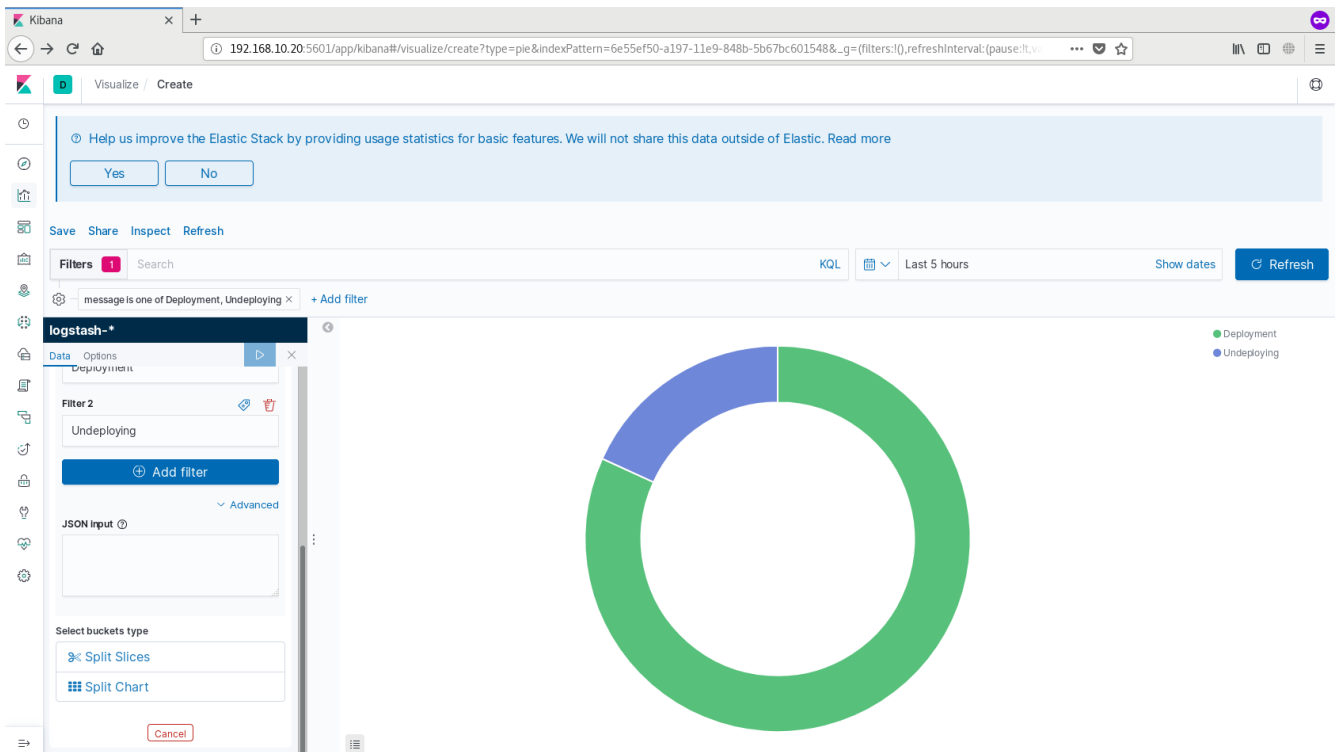
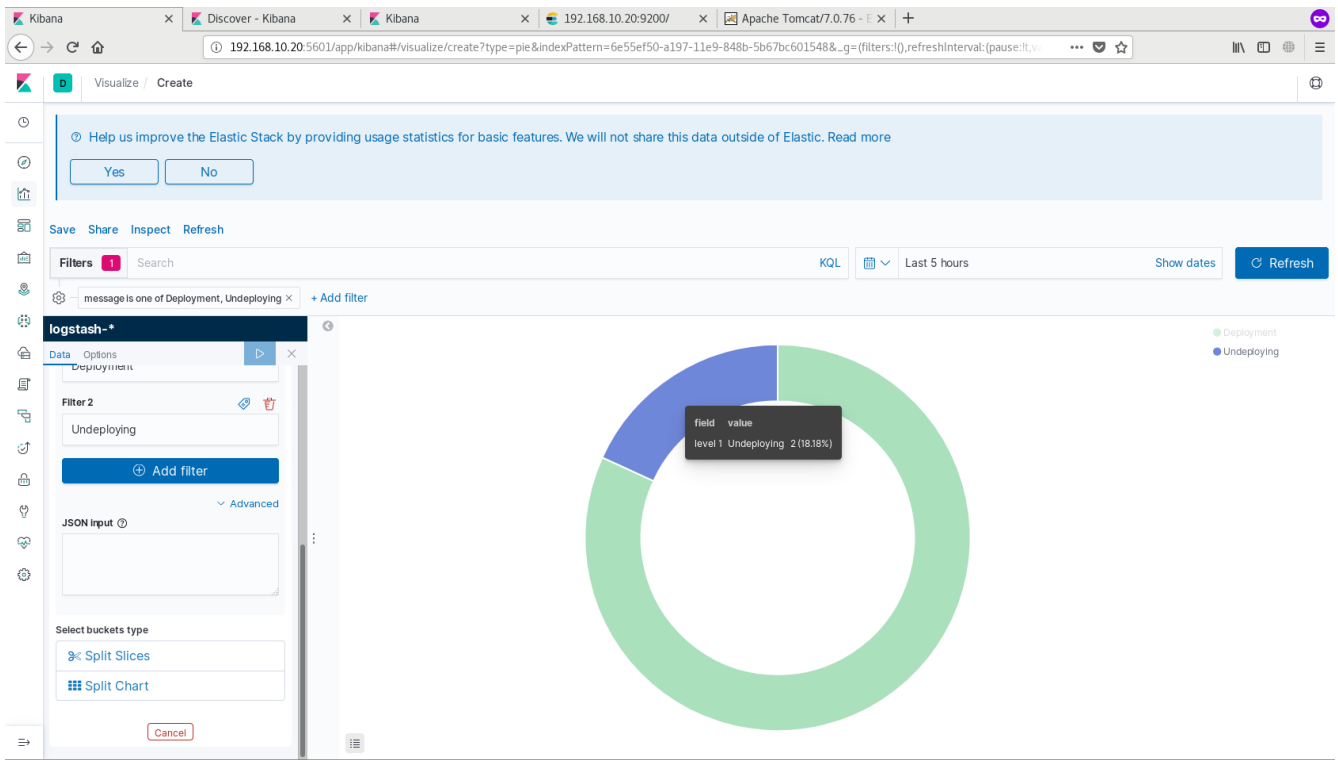
> Jul 8, 2019 @ 18:44:20.217 INFO: Deployment of web application directory /var/lib/tomcat/webapps/examples has finished in 402 ms

> Jul 8, 2019 @ 18:44:20.288 INFO: Deployment of web application directory /var/lib/tomcat/webapps/ROOT has finished in 500 ms



Creating “pie” visualization





Visualizing “Starting/stopping tomcat” (horizontal bar)

