```
[root@ELK vagrant]# curl -s 192.168.198.102:9200/_cluster/health | jq
{
  "cluster_name": "elasticsearch",
  "status": "yellow",
  "timed_out": false,
  "number_of_nodes": 1,
  "number_of_data_nodes": 1,
  "active_primary_shards": 3,
  "active_shards": 3,
  "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": 75
}
```

Discover - Kibana - Mozilla Firefox

192.168.198.102:5601/app/kibana#/discover?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:'2019-07-08T15:46:30.000Z',to:now))&_a=(column

Discover

1 hit

New Save Open Share Inspect

Filters 2 | Search | KQL | Jul 8, 2019 @ 18:46:30.000 → now | Refresh

NOT Deploying × | Undeploy × | + Add filter

logstash-2019.07.08-000001

Selected fields

? _source

Available fields

Aggregatable: any

Searchable: any

Type: any

Field name

Hide missing fields

Reset filters

@timestamp
t @version
t _id
t _index
_score

Jul 8, 2019 @ 18:46:30.000 - Jul 8, 2019 @ 19:05:56.827 — Auto

Time	_source
Jul 8, 2019 @ 19:02:17.135	message: INFO: Undeploying context [/hello-world] tags: _grokparsefailure path: /var/log/tomcat/catalina.2019-07-08.log host: tomcat @timestamp: Jul 8, 2019 @ 19:02:17.135 @version: 1 _id: DddS0msBVznVyDf2TA3N _type: _doc _index: logstash-2019.07.08-000001 _score: -

```
input {
        beats
        {
        port => "5044"
        }
        file {
                path => "/var/log/tomcat/catalina.2019-07-08.log"
                start_position => "beginning"
                }
        }
filter {
        grok {
                match => { "message" => "%{TIMESTAMP_ISO8601:timestamp} [%{LOGLEVEL:level}]%{GREEDYDATA:messageText}%{IP:client}" }
                }
        date {
                match => ["timestamp", "yyyy-MM-dd HH:mm:ss.SSS", "ISO8601"]
                timezone => "UTC"
                }


output {
        elasticsearch {
                hosts => ["192.168.198.102:9200"]
                        }
        stdout { codec => rubydebug }
}
```

Discover: Deploy - Kibana - Mozilla Firefox

192.168.198.102:5601/app/kibana#/discover/2a546e90-a19b-11e9-8e44-9770ade6dd8e?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:'2019-

D Discover / Deploy

Recent items

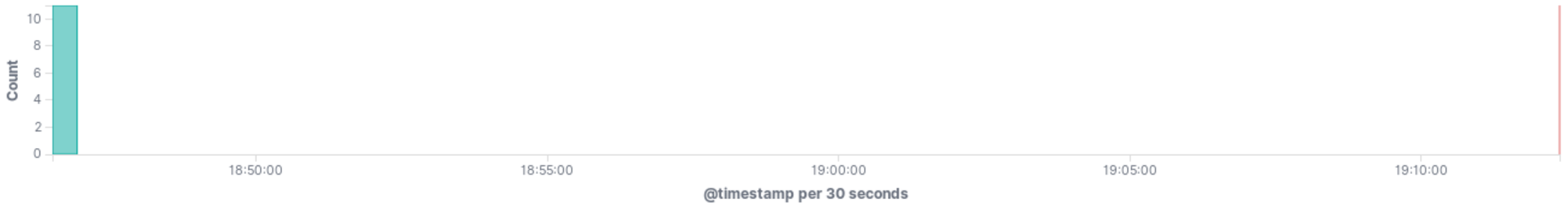
- Deploy
- Undeploy
- [eCommerce] Revenue Dashboard

ect

KQL | Jul 8, 2019 @ 18:46:30.000 → now | Refresh

filter

Jul 8, 2019 @ 18:46:30.000 - Jul 8, 2019 @ 19:12:22.255 — Auto



Time	_source
Jul 8, 2019 @ 18:46:36.600	message: INFO: Deploying web application archive /var/lib/tomcat/webapps/hello-world.war @version: 1 tags: _grokparsefailure @timestamp: Jul 8, 2019 @ 18:46:36.600 host: tomcat path: /var/log/tomcat/catalina.2019-07-08.log _id: ktdD0msBVznVyDf28gz2 _type: _doc _index: logstash-2019.07.08-000001 _score: -
Jul 8, 2019 @ 18:46:36.598	message: INFO: Deploying web application directory /var/lib/tomcat/webapps/sample @version: 1 tags: _grokparsefailure @timestamp: Jul 8, 2019 @ 18:46:36.598 host: tomcat path: /var/log/tomcat/catalina.2019-07-08.log _id: htdD0msBVznVyDf28gz2 _type: _doc _index: logstash-2019.07.08-000001 _score: -
Jul 8, 2019 @ 18:46:36.592	message: INFO: Deploying web application directory /var/lib/tomcat/webapps/examples @version: 1 tags: _grokparsefailure @timestamp: Jul 8, 2019 @ 18:46:36.592 host: tomcat path: /var/log/tomcat/catalina.2019-07-08.log _id: YtdD0msBVznVyDf28gz2 _type: _doc _index: logstash-2019.07.08-000001 _score: -
Jul 8, 2019 @ 18:46:36.570	message: INFO: Deploying web application directory /var/lib/tomcat/webapps/ROOT @version: 1 tags: _grokparsefailure @timestamp: Jul 8, 2019 @ 18:46:36.570 host: tomcat path: /var/log/tomcat/catalina.2019-07-08.log _id: CNdD0msBVznVyDf28w0h _type: _doc _index: logstash-2019.07.08-000001 _score: -
Jul 8, 2019 @ 18:46:36.569	message: INFO: Deploying web application directory /var/lib/tomcat/webapps/manager @version: 1 tags: _grokpar... 6.569 host: tomcat path: /var/log/tomcat/catalina.2019-07-08.log _id: AtdD0msBVznVyDf28w0h _type: _doc _ind...

✓ Search 'Deploy' was saved

Recent items

Deploy

Undeploy

[eCommerce] Revenue Dashboard

Save Share Inspect Refresh

Filters Search KQL Jul 8, 2019 @ 18:46:30.000 → now Refresh

+ Add filter

logstash-2019.07.08-000001

Data Options

Metrics

Slice Size Count

Buckets

Split Slices

Aggregation Filters help

Filters

Filter 1

deployment

Filter 2

Undeploying

Add filter

Advanced

Add sub-buckets