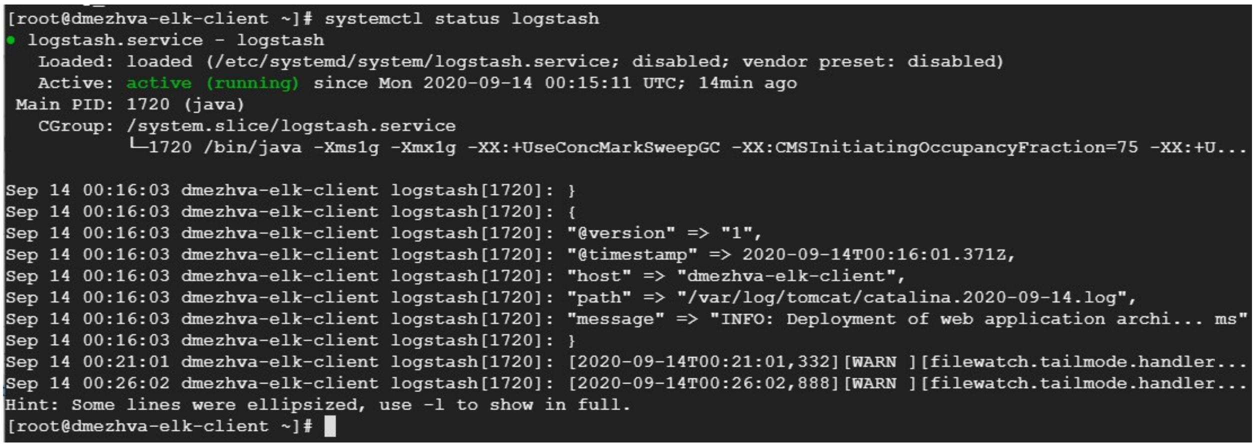
DevOps Lab

ELK

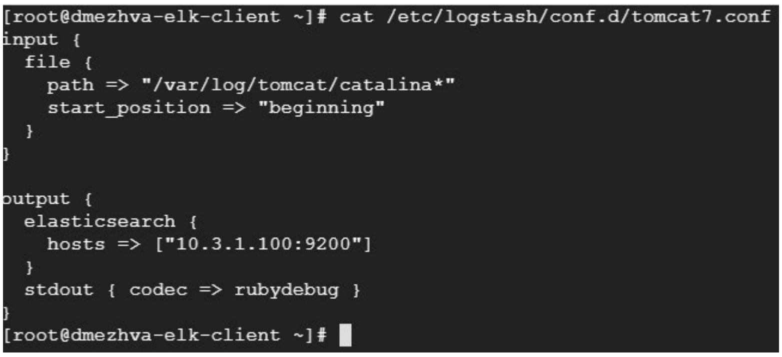
Home tasks

1. Build client (Logstash)



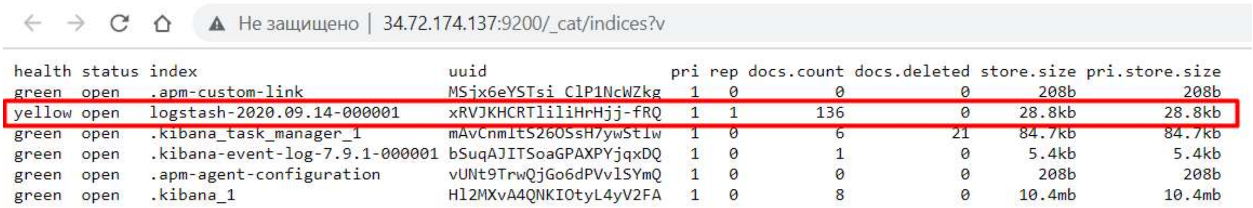
```
[root@dmezhva-elk-client ~]# systemctl status logstash
● logstash.service - logstash
   Loaded: loaded (/etc/systemd/system/logstash.service; disabled; vendor preset: disabled)
   Active: active (running) since Mon 2020-09-14 00:15:11 UTC; 14min ago
 Main PID: 1720 (java)
   CGroup: /system.slice/logstash.service
           └─1720 /bin/java -Xms1g -Xmx1g -XX:+UseConcMarkSweepGC -XX:CMSInitiatingOccupancyFraction=75 -XX:+U...

Sep 14 00:16:03 dmezhva-elk-client logstash[1720]: }
Sep 14 00:16:03 dmezhva-elk-client logstash[1720]: {
Sep 14 00:16:03 dmezhva-elk-client logstash[1720]: "@version" => "1",
Sep 14 00:16:03 dmezhva-elk-client logstash[1720]: "@timestamp" => 2020-09-14T00:16:01.371Z,
Sep 14 00:16:03 dmezhva-elk-client logstash[1720]: "host" => "dmezhva-elk-client",
Sep 14 00:16:03 dmezhva-elk-client logstash[1720]: "path" => "/var/log/tomcat/catalina.2020-09-14.log",
Sep 14 00:16:03 dmezhva-elk-client logstash[1720]: "message" => "INFO: Deployment of web application archi... ms"
Sep 14 00:16:03 dmezhva-elk-client logstash[1720]: }
Sep 14 00:21:01 dmezhva-elk-client logstash[1720]: [2020-09-14T00:21:01,332][WARN ][filewatch.tailmode.handler...
Sep 14 00:26:02 dmezhva-elk-client logstash[1720]: [2020-09-14T00:26:02,888][WARN ][filewatch.tailmode.handler...
Hint: Some lines were ellipsized, use -l to show in full.
[root@dmezhva-elk-client ~]#
```

2. Logstash configuration



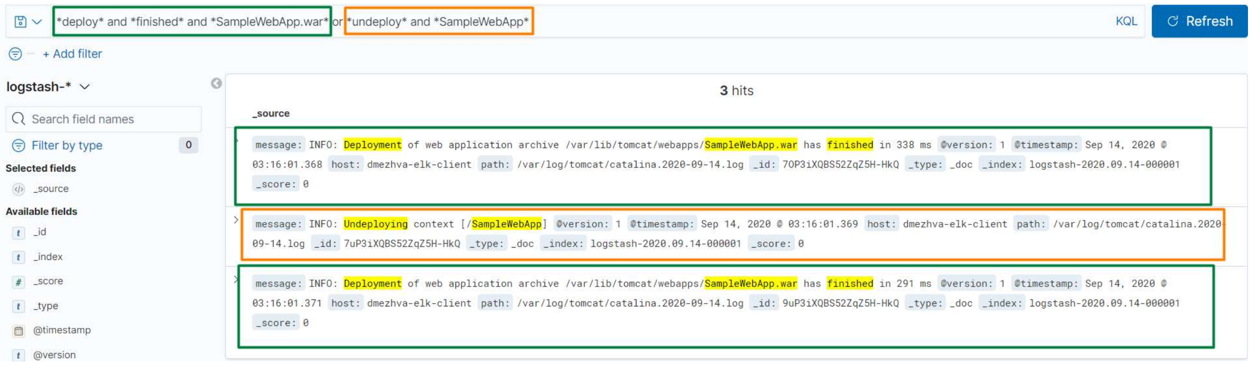
```
[root@dmezhva-elk-client ~]# cat /etc/logstash/conf.d/tomcat7.conf
input {
  file {
    path => "/var/log/tomcat/catalina*"
    start_position => "beginning"
  }
}

output {
  elasticsearch {
    hosts => ["10.3.1.100:9200"]
  }
  stdout { codec => rubydebug }
}
[root@dmezhva-elk-client ~]#
```

3. Index



```
health status index                          uuid                   pri rep docs.count docs.deleted store.size pri.store.size
green  open   .apm-custom-link               MSjx6eYSTsi_ClP1NcWZkg   1   0          0            0       208b           208b
yellow open   logstash-2020.09.14-000001     xRVJKHCRTliliHrHjj-fRQ   1   1        136            0     28.8kb         28.8kb
green  open   .kibana_task_manager_1         mAvCnmltS26OSsH7ywStlw   1   0          6           21     84.7kb         84.7kb
green  open   .kibana-event-log-7.9.1-000001 bSuqAJITSoaGPAXPYjqxDQ   1   0          1            0      5.4kb          5.4kb
green  open   .apm-agent-configuration       vUNt9TrwQjGo6dPVvlSYmQ   1   0          0            0       208b           208b
green  open   .kibana_1                      Hl2MXvA4QNKIOtyL4yV2FA   1   0          8            0     10.4mb         10.4mb
```

4. Filter



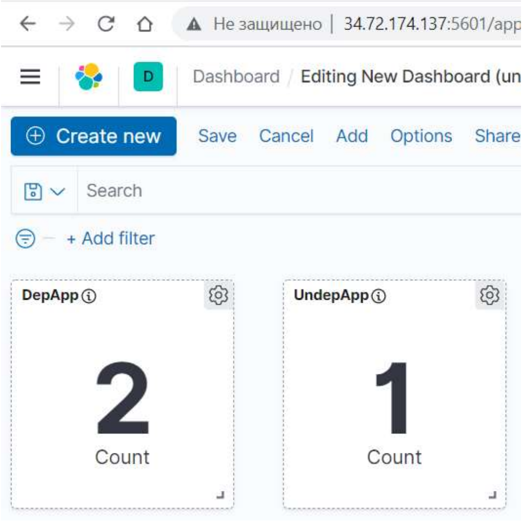
deploy and *finished* and *SampleWebApp.war* or *undeploy* and *SampleWebApp*

3 hits

_source

```
message: INFO: Deployment of web application archive /var/lib/tomcat/webapps/SampleWebApp.war has finished in 338 ms @version: 1 @timestamp: Sep 14, 2020 @ 03:16:01.368 host: dmezhva-elk-client path: /var/log/tomcat/catalina.2020-09-14.log _id: 7OP3iXQBS52ZqZ5H-HkQ _type: _doc _index: logstash-2020.09.14-000001 _score: 0

message: INFO: Undeploying context [/SampleWebApp] @version: 1 @timestamp: Sep 14, 2020 @ 03:16:01.369 host: dmezhva-elk-client path: /var/log/tomcat/catalina.2020-09-14.log _id: 7uP3iXQBS52ZqZ5H-HkQ _type: _doc _index: logstash-2020.09.14-000001 _score: 0

message: INFO: Deployment of web application archive /var/lib/tomcat/webapps/SampleWebApp.war has finished in 291 ms @version: 1 @timestamp: Sep 14, 2020 @ 03:16:01.371 host: dmezhva-elk-client path: /var/log/tomcat/catalina.2020-09-14.log _id: 9uP3iXQBS52ZqZ5H-HkQ _type: _doc _index: logstash-2020.09.14-000001 _score: 0
```

5. Dashboard



Не защищено | 34.72.174.137:5601/app
D
Dashboard / Editing New Dashboard (un
Create new
Save
Cancel
Add
Options
Share
Search
+ Add filter

DepApp

2

Count

UndepApp

1

Count