



**DevOps Lab**

# **ELK INTRODUCTION**

**Home tasks**

**Legal Notice:** This document contains privileged and/or confidential information and may not be disclosed, distributed or reproduced without the prior written permission of EPAM®.

---

CONFIDENTIAL | Effective Date: 09-Sep-19

## TASK 1

1. Spin-up VM-1 using by Vagrant. It must match next conditions:
  - a. OS Centos should be installed (use sbeliakou/centos image)
  - b. Tomcat appserver should be installed
  - c. “Testapp” application should be deployed and running on the server
  - d. Logstash should be installed and configured for working with VM-2

## TASK 2

1. Spin-up second VM-2 using by Vagrant. It must match next conditions:
  - a. OS Centos should be installed (use sbeliakou/centos image)
  - b. Elasticsearch should be installed and configured
  - c. Kibana should be installed and configured

## TASK 3

1. Analyze application workflow using by Kibana, provide screenshots
2. Perform several deploying-undeploying operations (Testapp), check changes, overview logstash logs using by Kibana UI; provide appropriate screenshots

## HOMETASK REQUIREMENTS

1. Vagrantfile for provisioning required infrastructure
2. SH - scripts for installation/configuring of the necessary applications
3. Screenshots of the application’s state (from Kibana)

## HELPFUL MATERIALS

- “ELK introduction” presentation
- <https://www.elastic.co/guide/en/logstash/current/installing-logstash.html>
- <https://www.elastic.co/guide/en/elasticsearch/reference/current/rpm.html#install-rpm>
- <https://www.elastic.co/guide/en/kibana/7.2/rpm.html#rpm-repo>

Applications

Places

Google Chrome

Kibana

Sample "Hello, World" Ap...

192.168.56.169:9200/...

Not secure

192.168.56.169:5601/app/kibana#/management/elasticsearch/index\_management/indices?.g=()

Management / Index Management

Elasticsearch

Index Management

Index Lifecycle Policies

Rollup Jobs

Cross-Cluster Replication

Remote Clusters

Snapshot and Restore

License Management

8.0 Upgrade Assistant

Kibana

Index Patterns

Saved Objects

Spaces

Reporting

Advanced Settings

Index Management

Index Management docs

Indices Index Templates

Update your Elasticsearch indices individually or in bulk.

☐ Include rollup indices
☐ Include system indices

<input type="checkbox"/> Name	Health	Status	Primaries	Replicas	Docs count	Storage size
<input type="checkbox"/> logstash-2019.10.22-000001	yellow	open	1	1	0	283b

Rows per page: 10

Discover - Kibana

Sample "Hello, World" Ap...

192.168.56.169:5601/app/kibana#/discover?\_g=()&\_a=(columns:!(\_source),index:ed1a900-f4c7-11e9-8a4a-e58344d81c0a,interval:auto,query:(language:kuery,query:''),sort:!(@timestamp,desc))

Discover

New Save Open Share Inspect

# Search KQL Last 15 minutes Show dates Refresh

+ Add filter

logstash-2019.10.22-000001

Selected fields

Available fields

@timestamp

@version

\_id

\_index

\_score

\_type

host

message

path

464 hits

Oct 22, 2019 @ 15:20:15.580 - Oct 22, 2019 @ 15:35:15.580 — Auto

Count

@timestamp per 30 seconds

Time

Oct 22, 2019 @ 15:34:45.844

host: tomcat @version: 1 path: /opt/tomcat/logs/catalina.2019-10-22.log @timestamp: Oct 22, 2019 @ 15:34:45.844 message: 22-Oct-2019 12:34:44.853 INFO [main] org.apache.catalina.startup.HostConfig.deployDirectory Deploying web application directory [/opt/tomcat/webapps/host-manager] \_id: IAF282080bH8cF6-Y3hb \_type: \_doc \_index: logstash-2019.10.22-000001 \_score: -

Oct 22, 2019 @ 15:34:45.844

host: tomcat @version: 1 path: /opt/tomcat/logs/catalina.2019-10-22.log @timestamp: Oct 22, 2019 @ 15:34:45.844 message: 22-Oct-2019 12:34:44.895 INFO [main] org.apache.catalina.startup.HostConfig.deployDirectory Deployment of web application directory [/opt/tomcat/webapps/host-manager] has finished in [42] ms \_id: IQF282080bH8cF6-Y3hb \_type: \_doc \_index: logstash-2019.10.22-000001 \_score: -

Oct 22, 2019 @ 15:34:45.844

host: tomcat @version: 1 path: /opt/tomcat/logs/catalina.2019-10-22.log @timestamp: Oct 22, 2019 @ 15:34:45.844 message: 22-Oct-2019 12:34:44.896 INFO [main] org.apache.catalina.startup.HostConfig.deployDirectory Deploying web application directory [/opt/tomcat/webapps/manager] \_id: IgF282080bH8cF6-Y3hb \_type: \_doc \_index: logstash-2019.10.22-000001 \_score: -

Oct 22, 2019 @ 15:34:45.844

host: tomcat @version: 1 path: /opt/tomcat/logs/catalina.2019-10-22.log @timestamp: Oct 22, 2019 @ 15:34:45.844 message: 22-Oct-2019 12:34:44.915 INFO [main] org.apache.catalina.startup.HostConfig.deployDirectory Deployment of web application directory [/opt/tomcat/webapps/manager] has finished in [19] ms \_id: IwF282080bH8cF6-Y3hb \_type: \_doc \_index: logstash-2019.10.22-000001 \_score: -

Oct 22, 2019 @ 15:34:45.844

host: tomcat @version: 1 path: /opt/tomcat/logs/catalina.2019-10-22.log @timestamp: Oct 22, 2019 @ 15:34:45.844 message: 22-Oct-2019 12:34:44.925 INFO [main] org.apache.coyote.AbstractProtocol.start Starting ProtocolHandler ["http-nio-8080"] \_id: JAF282080bH8cF6-Y3hb \_type: \_doc

vagrant...java

Hubstaff

vagrant...elk

[student@localhost:~/Do...

VisualVM 1.4.4

[student@localhost:~/Do...

Discover - Kibana - GoogL

elasticsearch.sh (~/Down...

1 / 4