



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

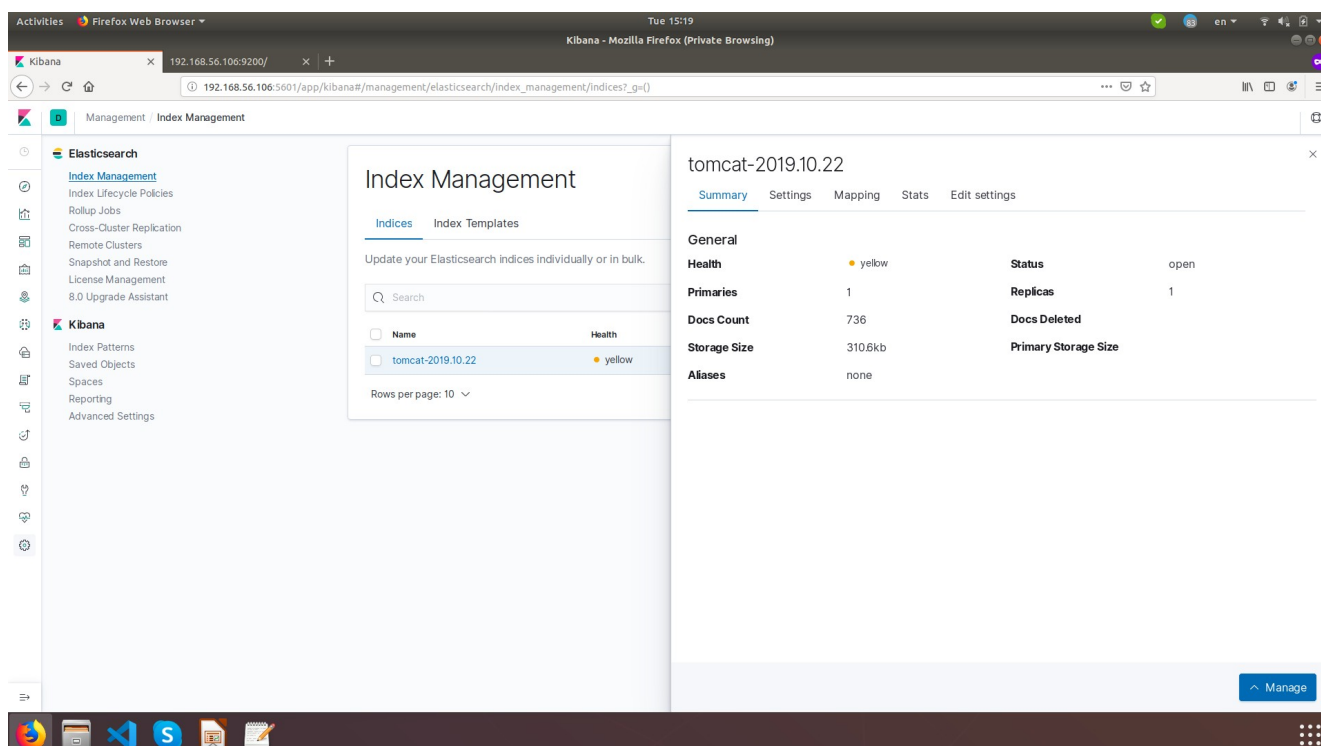
1. Spin-up second VM-2 using by Vagrant. It must match next conditions:
  - a. OS Centos should be installed (use sbeliakou/centos image)
  - b. Elasticsearch should be installed and configured
  - c. Kibana should be installed and configured

## 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)



The screenshot shows the Kibana 'Index Patterns' page for the 'tomcat-\*' index. The left sidebar contains navigation links for Elasticsearch (Index Management, Index Lifecycle Policies, Rollup Jobs, Cross-Cluster Replication, Remote Clusters, Snapshot and Restore, License Management, 8.0 Upgrade Assistant) and Kibana (Index Patterns, Saved Objects, Spaces, Reporting, Advanced Settings). The main content area displays the 'tomcat-\*' index with a time filter set to '@timestamp'. Below the filter, a table lists 14 fields with their types and formats. The table has columns for Name, Type, Format, Searchable, Aggregatable, and Excluded. The fields listed are: @timestamp (date), @version (string), @version.keyword (string), \_id (string), \_index (string), \_score (number), \_source (string), \_type (string), host (string), and host.keyword (string). The bottom of the table shows 'Rows per page: 10' and a pagination control for page 1 of 2.

Name	Type	Format	Searchable	Aggregatable	Excluded
@timestamp	date		•	•	
@version	string		•		
@version.keyword	string		•	•	
_id	string		•	•	
_index	string		•	•	
_score	number				
_source	string				
_type	string		•	•	
host	string		•		
host.keyword	string		•	•	

The screenshot shows the Kibana 'Discover' page for the 'tomcat-\*' index. The top bar includes a search bar with the query 'host', a time range filter set to 'Last 15 minutes', and buttons for 'Show dates' and 'Refresh'. The left sidebar shows the 'Selected fields' list with '\_source' selected and 'Available fields' list with '@timestamp', '@version', '\_id', '\_index', '\_score', '\_type', 'host', 'message', and 'path'. The main content area displays a bar chart showing the count of hits over time, with a peak around 15:12:00. Below the chart, a list of log entries is shown, each with a timestamp, message, and source. The log entries are filtered by the query 'host' and the time range 'Last 15 minutes'.

Time	_source
Oct 22, 2019 @ 15:13:38.960	message: 22-Oct-2019 12:13:38.147 WARNING [localhost-startStop-2] org.apache.catalina.startup.HostConfig.deployDescriptor A docBase [/opt/tomcat/webapps/manager] inside the host appBase has been specified, and will be ignored @version: 1 host: elk-node1 @timestamp: Oct 22, 2019 @ 15:13:38.960 path: /opt/tomcat/logs/catalina.out _id: QgtJ8208KSw17hQ7E0F6 _type: _doc _index: tomcat-2019.10.22 _score: -
Oct 22, 2019 @ 15:11:58.652	message: 22-Oct-2019 12:11:58.828 INFO [localhost-startStop-1] org.apache.catalina.startup.HostConfig.deployDescriptor Deployment of web application directory [/opt/tomcat/webapps/manager] has finished in [13] ms @version: 1 host: elk-node1 @timestamp: Oct 22, 2019 @ 15:11:58.652 path: /opt/tomcat/logs/catalina.out _id: Pqth8208KSw17hQ7100q _type: _doc _index: tomcat-2019.10.22 _score: -
Oct 22, 2019 @ 15:11:58.651	message: 22-Oct-2019 12:11:58.815 INFO [localhost-startStop-1] org.apache.catalina.startup.HostConfig.deployDescriptor Deploying web application directory [/opt/tomcat/webapps/manager] @version: 1 host: elk-node1 @timestamp: Oct 22, 2019 @ 15:11:58.651 path: /opt/tomcat/logs/catalina.out _id: P4th8208KSw17hQ7100q _type: _doc _index: tomcat-2019.10.22 _score: -
Oct 22, 2019 @ 15:11:57.644	message: 22-Oct-2019 12:11:57.480 WARNING [localhost-startStop-1] org.apache.catalina.startup.HostConfig.deployDescriptor A docBase [/opt/tomcat/webapps/manager] inside the host appBase has been specified, and will be ignored @version: 1 host: elk-node1 @timestamp: Oct 22, 2019 @ 15:11:57.644 path: /opt/tomcat/logs/catalina.out _id: MgtH8208KSw17hQ7hEg _type: _doc _index: tomcat-2019.10.22 _score: -
Oct 22, 2019 @ 15:06:23.615	message: 22-Oct-2019 12:06:23.821 INFO [localhost-startStop-1] org.apache.catalina.startup.HostConfig.deployDescriptor Deployment of web application directory [/opt/tomcat/webapps/manager] has finished in [13] ms @version: 1 host: elk-node1 @timestamp: Oct 22, 2019 @ 15:06:23.615 path: /opt/tomcat/logs/catalina.out _id: Pqth8208KSw17hQ7100q _type: _doc _index: tomcat-2019.10.22 _score: -

For creating config files I used “echo” and “cat>>EOF” functions.  
Best practice – use files, that stored in secure storage, download it with credentials, change values with variable.

But it is solution for learning, so I used just script with variable.