DevOps Lab

ELK INTRODUCTION

Home tasks

TASK 1

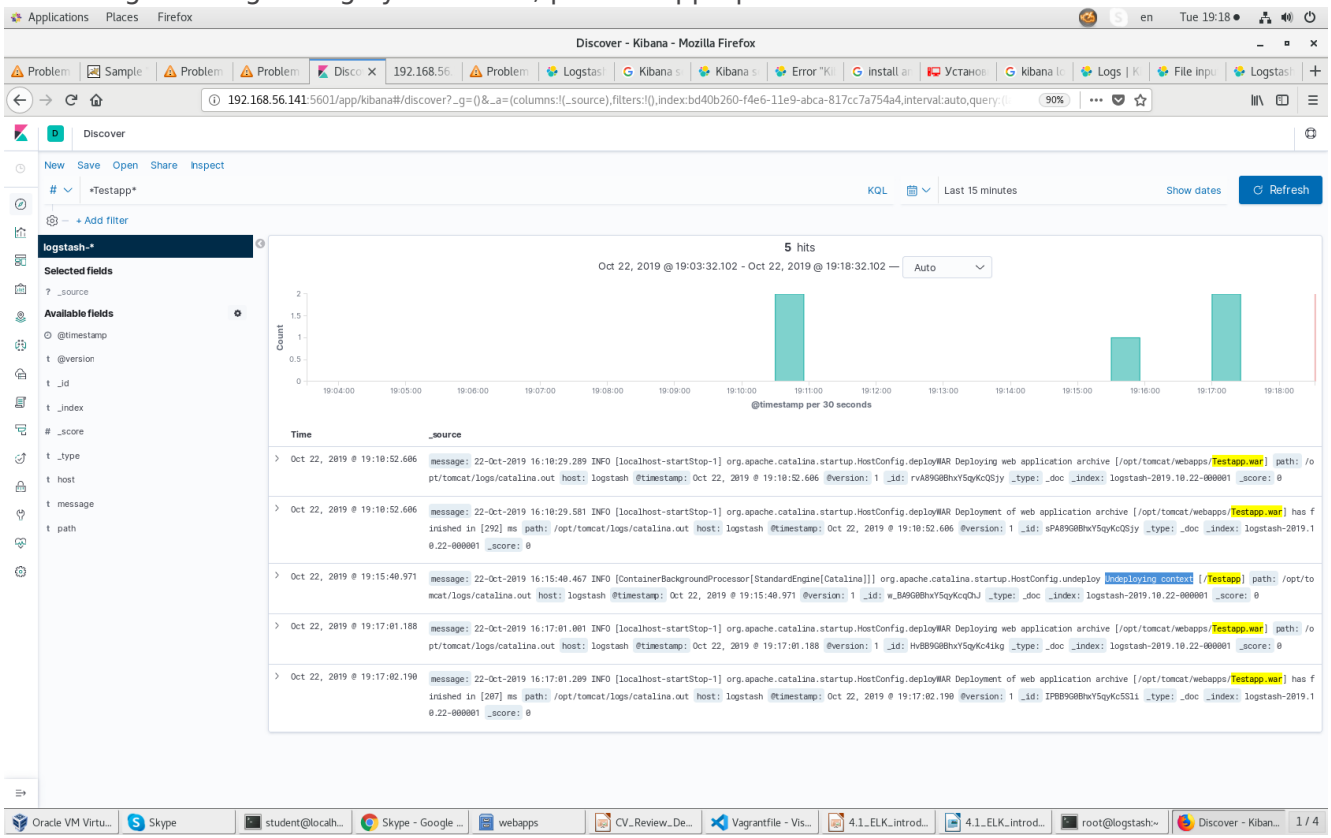
1. Spin-up VM-1 using by Vagrant. It must match next conditions:
    a. OS Centos should be installed (use sbeliakou/centos image)
    b. Tomcat appserver should be installed
    c. “Testapp” application should be deployed and running on the server
    d. Logstash should be installed and configured for 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. Preform several deploying-undeploying operations (Testapp), check changes, overview logstash logs using by Kibana UI; provide appropriate screenshots



HOMETASK REQUIREMENTS

1. Vargantfile for provisioning required infrastructure

```
Vagrant.configure("2") do |config|
 config.vm.define "esearch" do |server|
  server.vm.box = "sbeliakou/centos"
  server.vm.hostname = "esearch"
  server.vm.box_url = "https://app.vagrantup.com/sbeliakou/boxes/centos/versions/7.6.20190810"
  server.vm.provision "shell", path: "task4.sh"
  #server.vm.network "forwarded_port", guest: 80, host: 8080
  server.vm.network :private_network, ip: "192.168.56.141"
  server.vm.provider :virtualbox do |v|
   v.customize ["modifyvm", :id, "--natdnshostresolver1", "on"]
   v.customize ["modifyvm", :id, "--memory", 2048]
   v.customize ["modifyvm", :id, "--name", "esearch"]
  end
 end


 config.vm.define "logstash" do |logstash|
  logstash.vm.box = "sbeliakou/centos"
  logstash.vm.hostname = 'logstash'
  logstash.vm.box_url = "https://app.vagrantup.com/sbeliakou/boxes/centos/versions/7.6.20190810"
  logstash.vm.provision "shell", path: "task4.sh"
  logstash.vm.network :private_network, ip: "192.168.56.142"
  logstash.vm.provider :virtualbox do |v|
     v.customize ["modifyvm", :id, "--natdnshostresolver1", "on"]
     v.customize ["modifyvm", :id, "--memory", 2048]
    v.customize ["modifyvm", :id, "--name", "logstash"]

  end
 end
end
```

2. SH – scripts for installation/configuring of the necessary applications

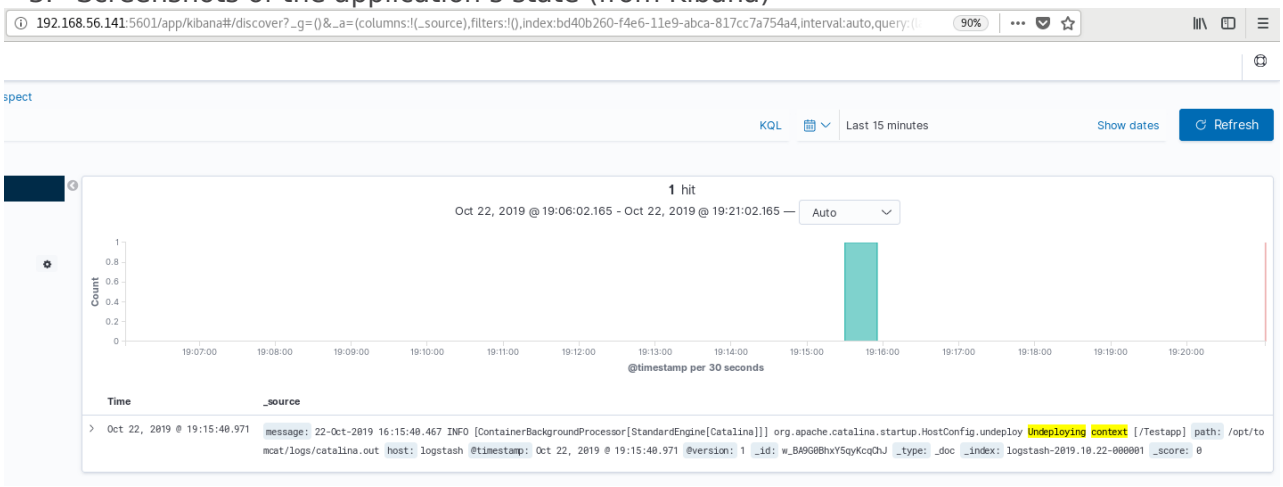
```
#!/bin/bash

allint='0.0.0.0'
elsserver='192.168.56.141'
logagent='192.168.56.142'


if [ "$(hostname)" = esearch ]
then

rpm --import https://artifacts.elastic.co/GPG-KEY-elasticsearch

cat <<EOF > /etc/yum.repos.d/elasticsearch.repo
[elasticsearch-7.x]
name=Elasticsearch repository for 7.x packages
baseurl=https://artifacts.elastic.co/packages/7.x/yum
gpgcheck=1
gpgkey=https://artifacts.elastic.co/GPG-KEY-elasticsearch
enabled=1
autorefresh=1
type=rpm-md
EOF

cat <<EOF > /etc/yum.repos.d/kibana.repo
[kibana-7.x]
name=Kibana repository for 7.x packages
baseurl=https://artifacts.elastic.co/packages/7.x/yum
gpgcheck=1
gpgkey=https://artifacts.elastic.co/GPG-KEY-elasticsearch
enabled=1
autorefresh=1
type=rpm-md
EOF




sudo yum install -y elasticsearch vim kibana

sudo systemctl daemon-reload
sudo systemctl enable elasticsearch.service kibana.service
sudo systemctl start elasticsearch.service kibana.service

sudo sed -i "s/#server.host:\ \"localhost\"/server.host: \""$allint"\"/" /etc/kibana/kibana.yml
sudo sed -i "s/#elasticsearch.hosts:*/elasticsearch.hosts:/" /etc/kibana/kibana.yml
```

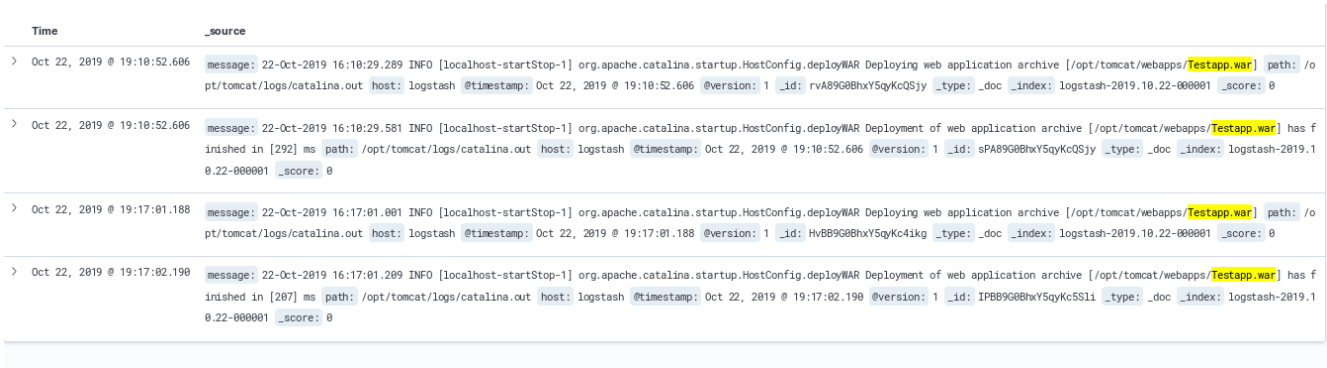
```
sudo sed -i "s/localhost:9200/"$allint":9200"/ /etc/kibana/kibana.yml

sudo sed -i "s/#network.host:\ 192.168.0.1/network.host: "$allint"/" /etc/elasticsearch/elasticsearch.yml
sudo sed -i "s/#discovery.seed_hosts:\ \[\"host1\",\ \"host2\"\]/discovery.seed_hosts: ["\"$logagent\""]/" /etc/elasticsearch/elasticsearch.yml

#localhost:9200
#elasticsearch.hosts:


sudo systemctl restart elasticsearch.service kibana.service

#########################################################################

else

rpm --import https://artifacts.elastic.co/GPG-KEY-elasticsearch

cat <<EOF > /etc/yum.repos.d/logstash.repo
[logstash-7.x]
name=Elastic repository for 7.x packages
baseurl=https://artifacts.elastic.co/packages/7.x/yum
gpgcheck=1
gpgkey=https://artifacts.elastic.co/GPG-KEY-elasticsearch
enabled=1
autorefresh=1
type=rpm-md
EOF


sudo yum install -y vim epel-release java java-devel logstash

curl -L -O https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-7.4.0-x86_64.rpm
sudo rpm -vi filebeat-7.4.0-x86_64.rpm

cat <<EOF > /etc/logstash/conf.d/logagent.conf
input {
 file {
  path => "/opt/tomcat/logs/catalina.out"
  start_position => "beginning"
```

```
  }
}

output {
  elasticsearch {
    hosts => ["$elsserver:9200"]
  }
  stdout { codec => rubydebug }
}
EOF

echo 'create user'
sudo mkdir /opt/tomcat
sudo groupadd tomcat
sudo useradd -s /bin/false -g tomcat -d /opt/tomcat tomcat

cd /opt/
sudo curl http://ftp.byfly.by/pub/apache.org/tomcat/tomcat-8/v8.5.47/bin/apache-tomcat-8.5.47.tar.gz --output ./apache-tomcat-8.5.47.tar.gz
sudo tar -xzvf apache-tomcat-8.5.47.tar.gz

sudo mv apache-tomcat-8.5.47/* tomcat/

sudo curl http://repo2.maven.org/maven2/org/apache/tomcat/tomcat-catalina-jmx-remote/8.5.6/tomcat-catalina-jmx-remote-8.5.6.jar --output /opt/tomcat/lib/tomcat-catalina-jmx-remote-8.5.6.jar

echo 'create systemd unit'
cd /opt

cat <<EOF > /etc/systemd/system/tomcat.service
[Unit]
Description=Apache Tomcat 9 Servlet Container
After=syslog.target network.target
[Service]
User=tomcat
Group=tomcat
Type=forking
Environment=CATALINA_PID=/opt/tomcat/tomcat.pid
Environment=CATALINA_HOME=/opt/tomcat
Environment=CATALINA_BASE=/opt/tomcat
ExecStart=/opt/tomcat/bin/startup.sh
ExecStop=/opt/tomcat/bin/shutdown.sh
Restart=on-failure
[Install]
WantedBy=multi-user.target
EOF

sudo curl https://tomcat.apache.org/tomcat-7.0-doc/appdev/sample/sample.war --output /opt/
```

```
tomcat/webapps/Testapp.war

sudo systemctl enable tomcat
sudo usermod -a -G tomcat logstash
sudo chown -hR tomcat:tomcat /opt/tomcat
sleep 3
sudo systemctl start logstash.service
sudo systemctl start tomcat

fi
```

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