DevOps

Containerization, CI/CD & Monitoring

February 2022
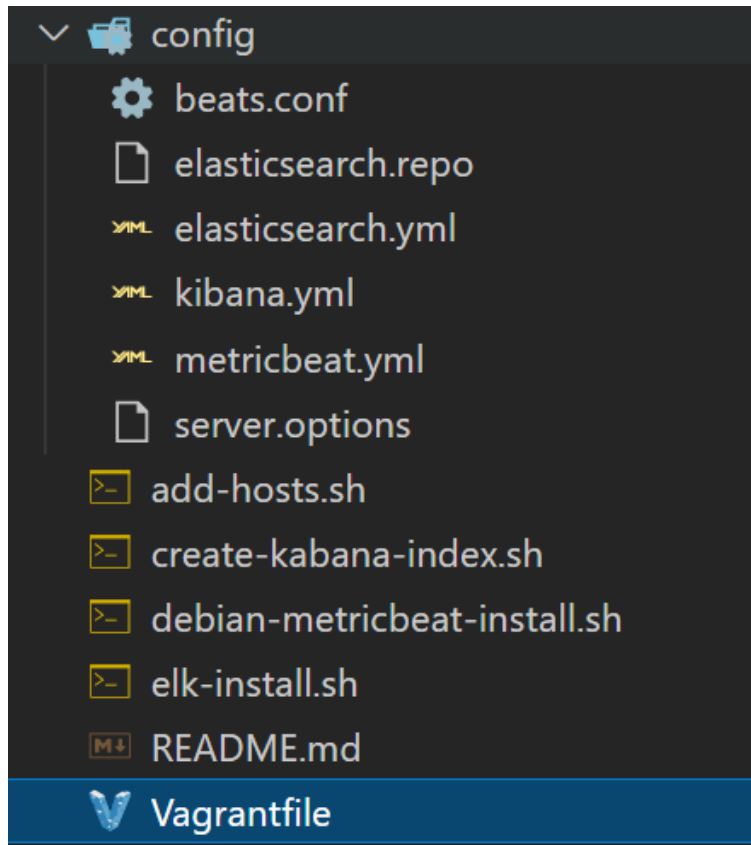
Elastic Stack
Home Work

Stefan Veselinov

config

- beats.conf
- elasticsearch.repo
- elasticsearch.yml
- kibana.yml
- metricbeat.yml
- server.options
- add-hosts.sh
- create-kabana-index.sh
- debian-metricbeat-install.sh
- elk-install.sh
- README.md
- Vagrantfile

Assignment

Utilizing what was discussed and shown during the lecture, try to do the following:

1. Build an infrastructure with three machines - one server for the **Elastic Stack** (**Elasticsearch**, **Logstash**, and **Kibana**) and two clients - one with **CentOS** and one with **Ubuntu**. For the server you can use either **CentOS** or **Ubuntu**
2. Install **Metricbeat** on the two client machines and make sure that the **system module** is **enabled**
3. Configure the **Logstash** to receive data from the beats and to forward the data to **Elasticsearch**
4. Using the **REST API** create an index pattern in **Kibana**

Please note that your solution should be automated to the extent possible

Preparation

- Host Machine - Windows 10 Pro 21H2 19044.1526
- Creating Project structure
  - config/ folder that is going to be shared throughout vm's (contains: configuration files for elasticsearch, logstash, kibana, metricbeat)
  - root – Vagrant file and all .sh scripts for vm's setup
- Vagrantfile – Three vm's. One server like, running elasticsearch, logstash and kibana. Two nodes, running metricbeat and providing metrics to elasticsearch

```ruby
Vagrant.configure("2") do |config|
  config.ssh.insert_key = false

  config.vm.define "server" do |server|
    server.vm.box = "shekeriev/centos-stream-8"
    server.vm.hostname = "server"
    server.vm.network "private_network", ip: "192.168.99.101"
    server.vm.provision "shell", path: "add-hosts.sh"
    server.vm.provision "shell", path: "elk-install.sh"
    # server.vm.provision "shell", path: "create-kabana-index.sh" # Sometimes Kibana is
not running -> set up is in trigger
    server.vm.provider "virtualbox" do |v|
      v.gui = false
      v.memory = 6144
      v.cpus = 2
    end
  end

  config.vm.define "node1" do |node1|
```

```
    node1.vm.box = "ubuntu/bionic64"
    node1.vm.hostname = "node1"
    node1.vm.network "private_network", ip: "192.168.99.102"
    node1.vm.provision "shell", path: "add-hosts.sh"
    node1.vm.provision "shell", path: "debian-metricbeat-install.sh"
    node1.vm.provider "virtualbox" do |v|
      v.gui = false
      v.memory = 512
      v.cpus = 1
    end
  end

  config.vm.define "node2" do |node2|
    node2.vm.box = "ubuntu/bionic64"
    node2.vm.hostname = "node2"
    node2.vm.network "private_network", ip: "192.168.99.103"
    node2.vm.provision "shell", path: "add-hosts.sh"
    node2.vm.provision "shell", path: "debian-metricbeat-install.sh"
    node2.vm.provider "virtualbox" do |v|
      v.gui = false
      v.memory = 512
      v.cpus = 1
    end
  end

  config.trigger.after :up do |trigger|
        trigger.only_on = "node2"
        trigger.info = "* Create Kibana index Trigger"
        trigger.run = {inline: "vagrant ssh -c 'sudo /vagrant/create-kabana-index.sh'
server"}
  end
end
```

- Add hosts sh

```
echo "192.168.99.101 server" >> /etc/hosts
echo "192.168.99.102 node1" >> /etc/hosts
echo "192.168.99.103 node2" >> /etc/hosts
```

- Elk install sh

```
echo "* Install Elastic Search"
sudo rpm --import https://artifacts.elastic.co/GPG-KEY-elasticsearch
sudo cp /vagrant/config/elasticsearch.repo /etc/yum.repos.d/elasticsearch.repo
sudo dnf install -y --enablerepo=elasticsearch elasticsearch

sudo cp /vagrant/config/elasticsearch.yml /etc/elasticsearch/elasticsearch.yml
sudo cp /vagrant/config/server.options /etc/elasticsearch/jvm.options.d/server.options

sudo systemctl daemon-reload
sudo systemctl enable --now elasticsearch
sudo systemctl start elasticsearch

echo "* Install Logstash"
```

```
sudo dnf install -y --enablerepo=elasticsearch logstash

sudo cp /vagrant/config/beats.conf /etc/logstash/conf.d/beats.conf

sudo systemctl daemon-reload
sudo systemctl enable --now logstash
sudo systemctl start logstash

echo "* Install Kibana"
sudo dnf install -y --enablerepo=elasticsearch kibana

sudo cp /vagrant/config/kibana.yml /etc/kibana/kibana.yml

sudo systemctl daemon-reload
sudo systemctl enable --now kibana
sudo systemctl start kibana

echo "* Enable Ports"
sudo firewall-cmd --add-port 5601/tcp --permanent
sudo firewall-cmd --reload
sudo firewall-cmd --add-port 9200/tcp --permanent
sudo firewall-cmd --reload
sudo firewall-cmd --add-port 5044/tcp --permanent
sudo firewall-cmd --reload
```

- Metric beat installation sh – debian version

```
echo "* Install Metric Beat"
curl -L -O https://artifacts.elastic.co/downloads/beats/metricbeat/metricbeat-8.1.0-
amd64.deb
sudo dpkg -i metricbeat-8.1.0-amd64.deb

echo "* Add Configuration"
sudo cp /vagrant/config/metricbeat.yml /etc/metricbeat/metricbeat.yml

echo "* Enable Module"
sudo metricbeat modules enable system

echo "* Start/Reload Service"
sudo systemctl daemon-reload
sudo systemctl enable metricbeat
sudo systemctl start metricbeat

echo "* Set up Elastic"
sudo metricbeat setup --index-management -E output.logstash.enabled=false -E
'output.elasticsearch.hosts=["http://192.168.99.101:9200"]'
```

- Kibana API index creation sh – for trigger

```
echo "* Create Kibana index"
curl -X POST http://192.168.99.101:5601/api/index_patterns/index_pattern -H 'kbn-xsrf:
true' -H 'Content-Type: application/json' -d '
{
  "index_pattern": {
```

```
    "title": "metricbeat*"
  }
}'
```

- Config/ files
  - elasticsearch.repo – dnf repository configuration
  - elasticsearch.yml – elastic search configuration

```
cluster.name: dolab
network.host: 192.168.99.101
http.port: 9200
# Enable security features
xpack.security.enabled: false
xpack.security.enrollment.enabled: false
```

  - java server option

-Xms1g

-Xmx1g

  - kibana configuration

```
server.port: 5601
server.host: "192.168.99.101"
server.name: "server"
elasticsearch.hosts: ["http://localhost:9200"]
```

  - logstash beats configuration

```
input {
  beats {
    port => 5044
  }
}
output {
  elasticsearch {
    hosts => ["http://localhost:9200"]
    index => "%{[@metadata][beat]}-%{[@metadata][version]}-%{+YYYY.MM.dd}"
  }
}
```

  - metricbeat configuration

```
output.logstash:
  # The Logstash hosts
  hosts: ["192.168.99.101:5044"]
```
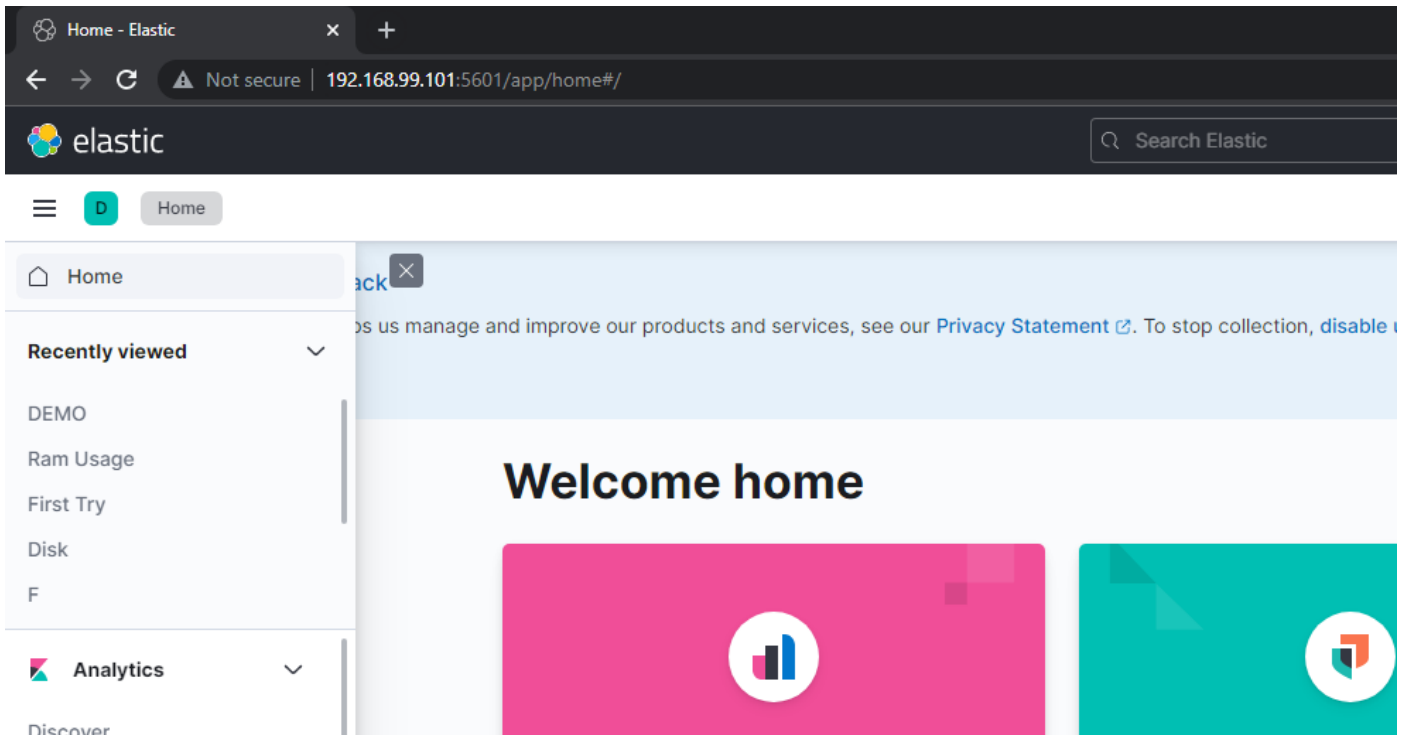
- Running Vagrant up
  - Successful act

```
node2: * Create Kibana index
node2:
node2:   % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
node2:                                  Dload  Upload   Total   Spent    Left  Speed
100 71483  100 71426  100    57  30933     24  0:00:02  0:00:02 --:--:-- 30958
node2:
node2: {"index_pattern":{"id":"5b019720-aa71-11ec-9639-7b6aaaa6565f","version":"WzE3LDFd","title":"metricbeat*","fields":{"@timestamp":{"count":0,"name":"@timestamp","type":"date","esTypes":["date"],"script
ed":false,"searchable":true,"aggregatable":true,"readFromDocValues":true,"format":{"id":"date"},"shortDotsEnable":false,"isMapped":true},"@version":{"count":0,"name":"@version","type":"string","esTypes":["text"
],"scripted":false,"searchable":true,"aggregatable":false,"readFromDocValues":false,"format":{"id":"string"},"shortDotsEnable":false,"isMa
pped":true},"esTypes":["keyword"],"scripted":false,"searchable":true,"aggregatable":true,"readFromDocValues":true,"subType":{"multi":{"parent":"@version"}},"format":{"id":"string"},"shortDotsEnable":false,"isMa
pped":true},"_id":{"count":0,"name":"_id","type":"string","esTypes":["_id"],"scripted":false,"searchable":true,"aggregatable":false,"readFromDocValues":false,"format":{"id":"string"},"shortDotsEnable":false,"is
Mapped":true},"_index":{"count":0,"name":"_index","type":"string","esTypes":["_index"],"scripted":false,"searchable":true,"aggregatable":true,"readFromDocValues":false,"format":{"id":"string"},"shortDotsEnable"
:false,"isMapped":true},"_score":{"count":0,"name":"_score","type":"number","scripted":false,"searchable":false,"aggregatable":false,"readFromDocValues":false,"format":{"id":"number"},"shortDotsEnable":false,"i
Mapped":true},"_source":{"count":0,"name":"_source","type":"_source","esTypes":["_source"],"scripted":false,"searchable":false,"aggregatable":false,"readFromDocValues":false,"format":{"id":"_source"},"shortDot
tEnable":false,"isMapped":true},"_type":{"count":0,"name":"_type","type":"string","scripted":false,"searchable":false,"aggregatable":false,"readFromDocValues":false,"format":{"id":"string"},"shortDotsEnable":fa
se,"isMapped":true},"agent.ephemeral_id":{"count":0,"name":"agent.ephemeral_id","type":"string","esTypes":["text"],"scripted":false,"searchable":true,"aggregatable":false,"readFromDocValues":false,"format":{"i
":"string"},"shortDotsEnable":false,"isMapped":true},"agent.ephemeral_id.keyword":{"count":0,"name":"agent.ephemeral_id.keyword","type":"string","esTypes":["keyword"],"scripted":false,"searchable":true,"aggreg
```

o Errors! Memory consumption of server vm is too much, so he lags a lot!

- Visiting Kibana

- Checking the metricbeats