# Solution M7: Elastic Stack

This is just one of the possible solutions

## Solution

The whole solution (or the bigger part) can be seen in the following **Vagrantfile**:

# -\*- mode: ruby -\*-

# vi: set ft=ruby :

Vagrant.configure("2") do |config|

  $hosts = <<HOSTS

    echo '127.0.0.1 localhost' | sudo tee /etc/hosts

    echo '::1 localhost' | sudo tee -a /etc/hosts

    echo '192.168.50.2 master' | sudo tee -a /etc/hosts

    echo '192.168.50.3 node1' | sudo tee -a /etc/hosts

    echo '192.168.50.4 node2' | sudo tee -a /etc/hosts

HOSTS

  $elastic = <<ELASTIC

    sudo dnf install -y java-1.8.0-openjdk

    echo 'x Install GPG Key, Repository, and Packages ...'

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

    cat > /tmp/elasticsearch.repo << EOF

[elasticsearch]

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=0

autorefresh=1

type=rpm-md

EOF

    sudo mv /tmp/elasticsearch.repo /etc/yum.repos.d/elasticsearch.repo

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

    echo 'x Adjust Configuration for Elasticsearch ...'

    echo 'node.name: master' | sudo tee -a /etc/elasticsearch/elasticsearch.yml

    echo 'network.host: ["localhost", "192.168.50.2"]' | sudo tee -a /etc/elasticsearch/elasticsearch.yml

    echo 'http.port: 9200' | sudo tee -a /etc/elasticsearch/elasticsearch.yml

    echo 'cluster.name: elastic-hw' | sudo tee -a /etc/elasticsearch/elasticsearch.yml

    echo 'cluster.initial\_master\_nodes: ["master"]' | sudo tee -a /etc/elasticsearch/elasticsearch.yml

    echo 'x Create Beats Configuration for Logstash ...'

    cat > /tmp/beats.conf << EOF

input {

  beats {

    port => 5044

  }

}

output {

  elasticsearch {

    hosts => ["http://master:9200"]

    index => "%{[@metadata][beat]}-%{[@metadata][version]}-%{+YYYY.MM.dd}"

  }

}

EOF

    sudo mv /tmp/beats.conf /etc/logstash/conf.d/beats.conf

    echo 'x Adjust Configuration for Kibana ...'

    echo 'server.port: 5601' | sudo tee -a /etc/kibana/kibana.yml

    echo 'server.host: "192.168.50.2"' | sudo tee -a /etc/kibana/kibana.yml

    echo 'server.name: "master"' | sudo tee -a /etc/kibana/kibana.yml

    echo 'elasticsearch.hosts: ["http://master:9200"]' | sudo tee -a /etc/kibana/kibana.yml

    echo 'x Start the Services ...'

    sudo systemctl daemon-reload

    sudo systemctl enable elasticsearch

    sudo systemctl start elasticsearch

    sudo systemctl enable logstash

    sudo systemctl start logstash

    sudo systemctl enable kibana

    sudo systemctl start kibana

    echo 'x Open Firewall Ports ...'

    sudo firewall-cmd --add-port 5044/tcp --permanent

    sudo firewall-cmd --add-port 5601/tcp --permanent

    sudo firewall-cmd --add-port 9200/tcp --permanent

    sudo firewall-cmd --reload

ELASTIC

  $metricrpm = <<METRICRPM

    echo 'x Install GPG Key, Repository, and Packages ...'

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

    cat > /tmp/elasticsearch.repo << EOF

[elasticsearch]

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=0

autorefresh=1

type=rpm-md

EOF

    sudo mv /tmp/elasticsearch.repo /etc/yum.repos.d/elasticsearch.repo

    sudo dnf install --enablerepo=elasticsearch -y metricbeat

    sudo cp -v /vagrant/beats/metricbeat.yml /etc/metricbeat/metricbeat.yml

    sudo metricbeat modules enable system

    sudo metricbeat setup --template -E output.logstash.enabled=false -E 'output.elasticsearch.hosts=["192.168.50.2:9200"]'

    sudo systemctl daemon-reload

    sudo systemctl enable --now metricbeat

METRICRPM

  $metricdeb = <<METRICDEB

  sudo apt-get remove -y unattended-upgrades

  wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -

  echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" | sudo tee /etc/apt/sources.list.d/elastic-7.x.list

  sudo apt-get update && sudo apt-get install -y metricbeat

  sudo cp -v /vagrant/beats/metricbeat.yml /etc/metricbeat/metricbeat.yml

  sudo metricbeat modules enable system

  sudo systemctl daemon-reload

  sudo systemctl enable --now metricbeat

  echo 'x Create the Index Pattern ...'

  curl -X POST master:5601/api/saved\_objects/index-pattern/my-pattern  -H 'kbn-xsrf: true' -H 'Content-Type: application/json' -d '{"attributes": {"title": "metricbeat-\*", "timeFieldName":"@timestamp"}}'

METRICDEB

  config.vm.synced\_folder ".", "/vagrant", type: "virtualbox"

  config.vm.provision "shell", inline: $hosts, privileged: false

  config.vm.define 'master' do |master|

    master.vm.box = "shekeriev/centos-8-minimal"

    master.vm.provider "virtualbox" do |vb|

      vb.memory = "4096"

    end

    master.vm.hostname = 'master'

    master.vm.network 'private\_network', ip: '192.168.50.2'

    master.vm.provision "shell", inline: $elastic, privileged: false

  end

  config.vm.define 'node1' do |node1|

    node1.vm.box = "shekeriev/centos-8-minimal"

    node1.vm.provider "virtualbox" do |vb|

      vb.memory = "512"

    end

    node1.vm.hostname = 'node1'

    node1.vm.network 'private\_network', ip: '192.168.50.3'

    node1.vm.provision "shell", inline: $metricrpm, privileged: false

  end

  config.vm.define 'node2' do |node2|

    node2.vm.box = "shekeriev/ubuntu-20-04-server"

    node2.vm.provider "virtualbox" do |vb|

      vb.memory = "512"

    end

    node2.vm.hostname = 'node2'

    node2.vm.network 'private\_network', ip: '192.168.50.4'

    node2.vm.provision "shell", inline: $metricdeb, privileged: false

  end

end

The environment can be brought up with:

**vagrant up**