Linux System administrator – response

**Task: ELK stack up and running**

I installed virtual machine on VirtualBox that runs Ubuntu Server 14.04 LTS. After that I installed Docker according to reference from this site:   
https://docs.docker.com/engine/installation/linux/ubuntulinux/

Created a file that shows on Docker repository on location /etc/apt/sources.list.d/**docker.list**

deb https://apt.dockerproject.org/repo ubuntu-trusty main

Also installed a Docker compose with this command:

curl -L https://github.com/docker/compose/releases/download/1.9.0-rc2/docker-compose-`uname -s`-`uname -m` > /usr/local/bin/docker-compose

And added execution parameter to file docker-compose:

chmod +x /usr/local/bin/docker-compose

**Configuring ELK stack**

As a “root” user I created ELK stack directory structure (separate folder for each service (Elasticsearch, Logstash, Kibana) on location: /root/elk-stack/**elk\_stack** according to this ELK configuration:   
 - https://github.com /deviantony/docker-elk

Each directory has a Dockerfile for each docker image which execute some parameters when container going to start. In Logstash config file (*logstash.conf*) is defined filter for *syslog* with date as a timestamp. Also created a docker-compose.yml which is the most important file for ELK stack configuration. With docker compose configuration we configure important settings for startup containers and conversation between them.

With command docker-compose up we can build a whole environment defined with our configuration files.

It is necessary to increase max\_map\_count to:

sysctl –w vm.max\_map\_count=262144

**Task: Automatic stack maintenance**

I created a rsync backup script for Elasticsearch data directory. Set this script to work as a cron job.

Also created bash script that alerting user when the disk space is low. This script work as a cron job and repeats hourly.

I set up mail to work on server and sending internal e-mail. In script for alerting when the disk space is low is defined root user mail address for receiving information about disk usage (root@ubuntu).

**Task: Utilities**

Alias which lists Docker images is added in .bashrc file on a location ~/.bashrc

Alias ls-images=’ docker images | awk ‘\’’{ print $1 “ “ $3 “ “ $7$8 }’\’’’