Instructions for creating a VM with Ubuntu 22.04, Plaso, OpenSearch and OpenSearch Dashboards

1. Install Virtual Box

Installing Virtual Box: https://www.virtualbox.org/wiki/Downloads

August 7, 2024: installing VirtualBox-7.0.20-163906-Win.exe

https://download.virtualbox.org/virtualbox/7.0.20/VirtualBox-7.0.20-163906-Win.exe

2. Install ubuntu 22.04.4 server LTS

***** SKIP THIS STEP IF YOU IMPORTED THE OVA AND YOUR VM IS WORKING *****

In the next four paragraphs you will install ubuntu server in the VM, VBoxGuestAdditions and port forwarding rules so you can reach the VM from your host.

2.1 preparations and starting virtual box

Download "ubuntu-22.04.4-live-server-amd64.iso" from https://ubuntu.com/download/server

https://releases.ubuntu.com/22.04.4/ubuntu-22.04.4-live-server-amd64.iso

Start VirtualBox. Under file select Check for Updates. This should ask to download and install the latest VirtualBox Extension Pack v7.20 (from https://download.virtualbox.org/virtualbox/7.0.20/Oracle_VM_VirtualBox_Extension_Pack-7.0.20.vbox-extpack)

2.2 installing ubuntu server

Create new VM. Select Linux/Ubuntu 64bit. Name is Ubuntu2204Opensearch. Select folder on disk with enough free space. Click Next.

Select the ubuntu-22.04.4-live-server-amd64.iso in your downloads folder

User opensearch with password opensearch. Check guesteditions. Click Next.

Set memory to 16Gb (less if you do not have that amount available. Try to stay in the green). Click Next.

Select create new virtual disk. Set size to 30GB. Click Next.

Check the overview and confirm to start the installation.

Select language: English

Confirm that you want to update the installer

Confirm network configuration (no changes)

No proxy is needed

Mirror is tested

Use entire disk (confirm)

Storage configuration. Select Done. Sure to continue choose Continue.

User: Mr Plaso

Server name: davday2

User: plaso

Password: plaso

Skip Ubuntu Pro

Choos to install SSH sever, do not import SSH key

No featured snaps

*** installation is now starting ***

Wait until installation is completed. Wait for updates to finish.Remove the ubuntu iso from the optical drive.

Select [reboot now]

Wait for the login prompt and login with username and password that you provided during the install. After logging in you should see the command line prompt.

2.3 Install VBoxGuestEditions

Insert the VBoxGuestAdditions_7.0.20.iso file in the virtual optical drive. This iso file is automatically made available as part of the VirtualBox extension pack that you installed earlier. Look in C:\Program Files\Oracle\VirtualBox and select VBoxGuestAdditions.iso.

Enter the following instructions:

Install dependencies for VirtualBox guest additions:

```
sudo apt-get install build-essential linux-headers-`uname -r`
sudo mkdir /media/cdrom
sudo mount - /dev/cdrom /media/cdrom
sudo /media/cdrom/VBoxLinuxAdditions.run
```

Next we need to find out the internal ip address of the VM. We use the ifconfig command but we first need to install that.

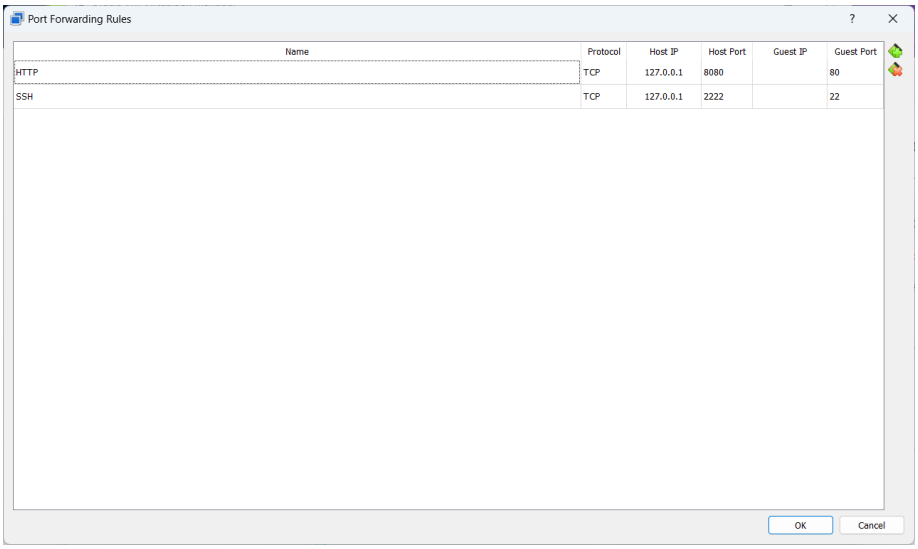
```
sudo apt install net-tools
ifconfig
```

take note of the ip-address (e.g. 10.0.2.15, ignore and 127.* addresses). Then switch off the VM.

sudo shutdown now

2.4 Configure port forwarding

Select the VM (which is powered off). Select network. In Adapter 1, check enable network adapter and select NAT. Click on advanced and select Port Forwarding. Because we use NAT, the VM has the same IP address as the host. Enter the rules as displayed in the following screenshot. Use the ip address that you obtained with ifconfig before shutting down the machine.



Select [OK] and close the dialogs. Start the VM.

Start a command prompt in windows (type cmd in search on the windows task bar).

At the command prompt type: ssh -p 2222 plaso@127.0.0.1

Enter yes to the continue connecting. Enter the password for plaso (=plaso)

If this works it means that the SSH port forward works. We can check the HTTP forward rule later after we have installed the webserver in the VM.

The nice thing about using the CMD.exe prompt is that you can copy paste command from your windows environment (e.g. from this step by step guide).

3. Installing Plaso, Nginx and the ELK-stack

***** SKIP THIS STEP IF YOU IMPORTED THE OVA AND YOUR VM IS WORKING *****

Before we install these packages need to get the system up to date:

sudo add-apt-repository ppa:gift/stable

sudo apt update

Remember that you can copy the commands from this manual and paste them with right mouse click in the cmd.exe windows command prompt if you are logged in the VM using ssh.

3.1 Install Plaso

Install plaso tools with the following command:

```
sudo apt install plaso-tools
```

Enter Y to agree with the installation. The install pinfo

```
sudo apt install pinfo
```

Now check if plaso tools have been installed by trying

```
log2timeline.py -V
```

You should see the commandline options (similar to what you have seen in colab in Exercise 3 and 4 yesterday).

We want to update the file_size field from type text to type long

```
sudo sed -e '/"file_size": {/,/},/c\"file_size": {\n    "type": "long"\n},'
/usr/share/plaso/opensearch.mappings -i
```

3.2 Install Opensearch

Following the instructions from (but changing to 2.15.0):

https://medium.com/@cybertoolguardian/installing-and-setting-up-opensearch-6fbf88b544ec

sudo apt install default-jre default-jdk

export JAVA_HOME=/usr/lib/jvm/java-11-openjdk-amd64
echo $JAVA_HOME

Before installing and setting up OpenSearch make sure that vm.max_map_count is set to at least 262144.

cat /proc/sys/vm/max_map_count

Add to /etc/sysctl.conf file

vm.max_map_count=262144

Reload to activate

sudo sysctl -p

Download opensearch deb package and install (note that as of 2.12.0 we must provide an initial password)

```
wget  https://artifacts.opensearch.org/releases/bundle/opensearch/2.15.0/opensearch-2.15.0-linux-x64.deb

export OPENSEARCH_INITIAL_ADMIN_PASSWORD='P?ssw0rd1'

sudo env OPENSEARCH_INITIAL_ADMIN_PASSWORD=P?ssw0rd1 dpkg -i opensearch-2.15.0-linux-x64.deb
```

Reload and enable opensearch,

```
sudo systemctl daemon-reload
sudo systemctl enable opensearch
```

Start and check the status of OpenSearch

```
sudo systemctl start opensearch
sudo systemctl status opensearch
```

Curl the opensearch url running on port 9200, with username admin and password P?ssw0rd1.

```
curl -X GET https://localhost:9200 -u 'admin:P?ssw0rd1' --insecure
```

In opensearch.yml file, located in /etc/opensearch make the following modifications using vi,

```
network.host: 0.0.0.0
discovery.type: single-node
plugins.security.disabled: false
```

Because opensearch is not readable for the plaso user, we make the root certificate available in ~plaso:

```
sudo cp /etc/opensearch/root-ca.pem ~

sudo chmod 644 root-ca.pem
```

3.3 OpenSearch dashboard and Nginx installation

Following instructions from :

https://medium.com/@cybertoolguardian/installing-and-setting-up-opensearch-dashboards-78b540905a29

Download deb package from official website https://opensearch.org/downloads.html

```
wget https://artifacts.opensearch.org/releases/bundle/opensearch-dashboards/2.15.0/opensearch-dashboards-2.15.0-linux-x64.deb

sudo dpkg -i opensearch-dashboards-2.15.0-linux-x64.deb
```

Reload and enable, opensearch. Start and check the status of Opensearch

```
sudo systemctl daemon-reload
sudo systemctl enable opensearch-dashboards
sudo systemctl start opensearch-dashboards
sudo systemctl status opensearch-dashboards
```

Edit /etc/opensearch-dashboards/opensearch-dashboards.yml file and add the following code.

```
server.port: 5601
server.host: "0.0.0.0"
opensearch.hosts: ["https://0.0.0.0:9200"]
opensearch.ssl.verificationMode: none
opensearch.username: "admin"
opensearch.password: " P?ssw0rd1”
```

Save the file and exit, now restart opensearch-dashboards.

```
sudo systemctl restart opensearch-dashboards
```

The following is not in the online tutorial but is a standard way to provide a reverse proxy

Install nginx as a reverse proxy so we can access the opensearch dashboard from our windows host

```
sudo apt install nginx
```

You can check if nginx is working by typing the following url http://127.0.0.1:8080/ in the browser of your windows host.

```
sudo vi /etc/nginx/sites-available/opensearch_dashboards
```

```
server {
    listen 80;
    location / {
        proxy_pass http://localhost:5601;
        proxy_http_version 1.1;
        proxy_set_header Upgrade $http_upgrade;
        proxy_set_header Connection 'upgrade';
        proxy_set_header Host $host;
        proxy_cache_bypass $http_upgrade;
    }
}
```

Create a symbolic link to the new NGINX site and remove the default site from sites-enabled

```
sudo ln -s /etc/nginx/sites-available/opensearch_dashboards /etc/nginx/sites-enabled/
sudo rm /etc/nginx/sites-enabled/default
sudo systemctl restart nginx
```

Then check the configuration for syntax errors:

```
sudo nginx -t
```

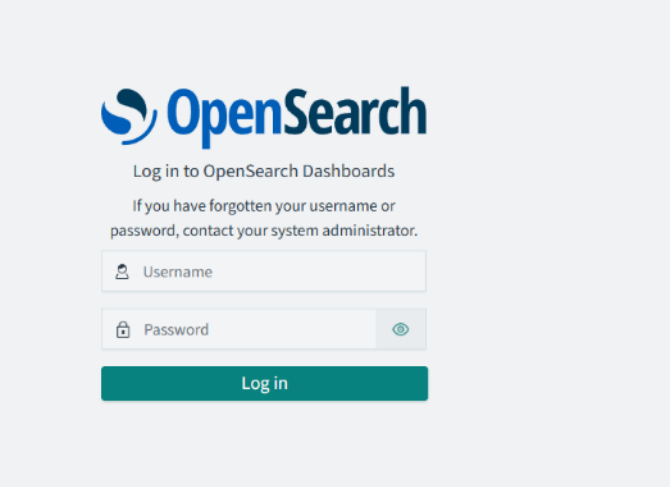
which should give:

nginx: the configuration file /etc/nginx/nginx.conf syntax is ok

nginx: configuration file /etc/nginx/nginx.conf test is successful

Now login the webbrowser with: http://127.0.0.1:8080/

You should see the login page



Login with admin and password P?ssw0rd1

TODO

Ingest data with plaso and build a visualisation. Here is a tutorial:

https://www.youtube.com/watch?v=xBeYcJ8hL1M

4. Extra: exporting as .ova

In case you want to create a new .ova file, the .vdi size can be reduced as follows:

4.1 Remove caches

remove APT cache:

```
sudo apt autoclean
sudo apt autoremove
```

remove Snap cache (probably not necessary):

```
sudo rm -rf /var/lib/snapd/cache/*
```

remove Maven cache (probably not necessary):

```
rm -rf /home/hansken/.m2/repository
```

remove Pip cache (probably not necessary):

```
pip cache purge
```

4.2 Clear journal

The journal typically is pretty big. To clean it as mich as possible, flush and rotate (to create archives), then vacuum everything older than 1 second:

```
sudo journalctl --flush --rotate
sudo journalctl --vacuum-time=1s
```

4.3 Clear unallocated space

To clear the unallocated space, we explicitely overwrite all unallocated space with 0's by creating a temp (as root) file and remove it.

```
sudo -i
dd if=/dev/zero of=/var/tmp/bigemptyfile bs=4096k
rm /var/tmp/bigemptyfile
```

4.4 Clear bash history

You probably have been messing around with a lot of commands (like the ones above). Clear the shell caches as follows:

```
sudo rm /root/.bash_history
rm ~/.bash_history
```

Press <ctrl>+D to close the console, open a new one and run again:

```
rm ~/.bash_history
```

Press <ctrl>+D to close the console.

Then under windows (start a CMD windows) compact the VDI file with the following command:

```
"c:\Program Files\Oracle\VirtualBox\VBoxManage.exe" modifyhd
D:\Projects\VMs\Ubuntu2204Opensearch\Ubuntu2204Opensearch.vdi compact
```