Tenable Security Center+ Labbox - Install Guide

Labbox is a specialized pre-configured install of Tenable.sc+, designed for Partner Engineers to be able to quickly spin up and demo the product. It also includes dummy data.
It is not meant for scanning or using API, etc. Mainly for demoing purposes and checking the solution capability.

Pre-requisites

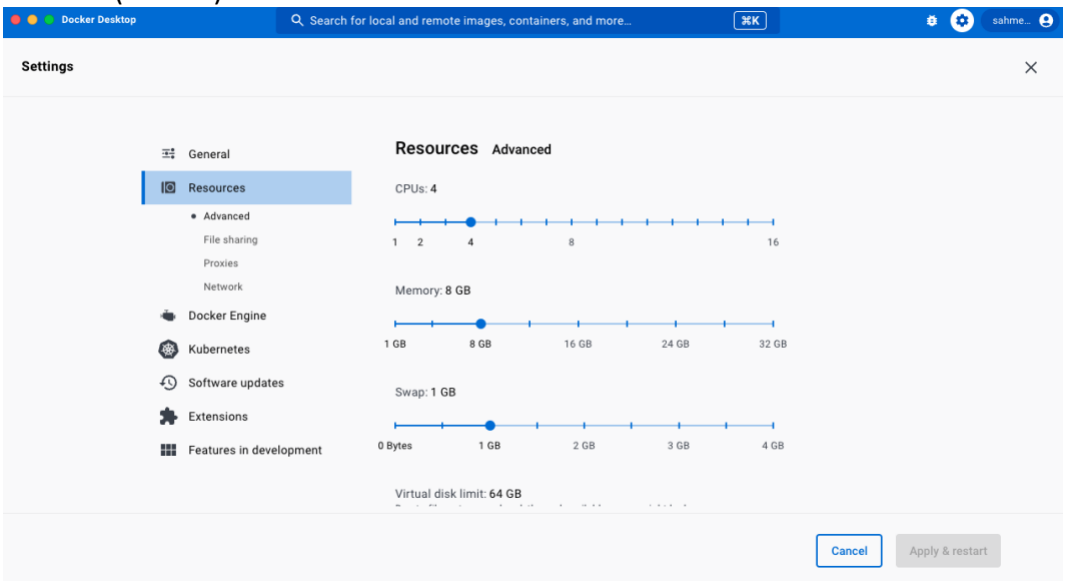
1. Download and Install Docker Desktop on your device (Latest Version) https://www.docker.com/products/docker-desktop/
    - Choose the image suitable for your Operating System. It works with MacBook/Linux and Windows.

2. Sign up/Sign Into Docker Desktop with your email.

3. Docker Desktop should be allocated 8 GB of RAM+ (The default is 2 GB). And 4 CPU.

    For MacBook

    Open **Docker Desktop**> **Settings** >**Resources**>**Advanced** and Assign your RAM(8GB+) and CPU(4 CPUs).

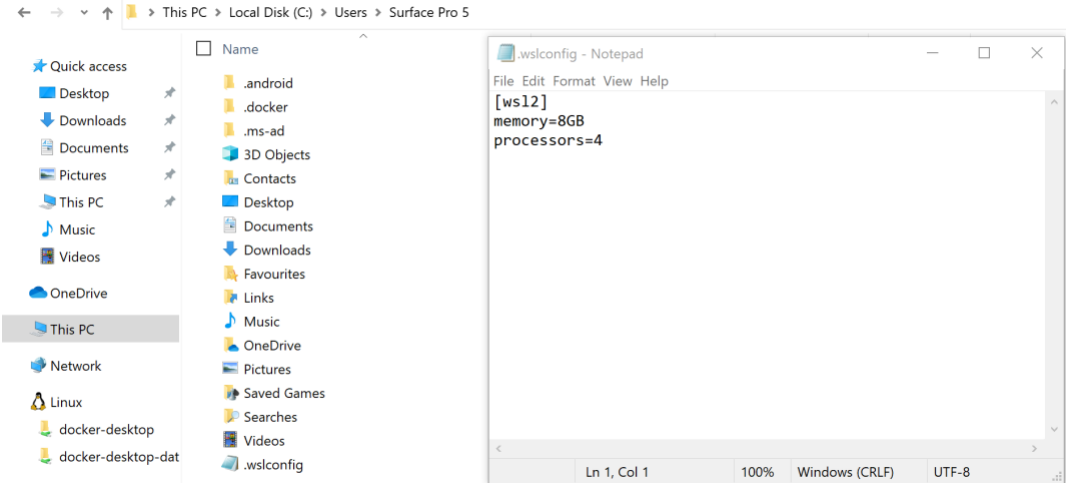


For Windows

Create new Notepad rename it to **.wslconfig** and paste the below values in the Notepad (Case sensitive) and place it under your main user profile directory.

Example: **This PC>Local Disk C > Users>"You User"**

[ws12]
memory=8GB
processors=4

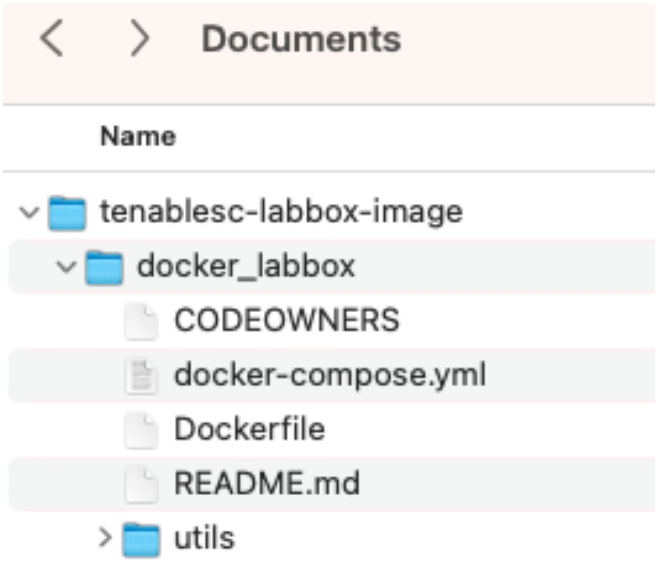


Then save it and restart Docker Desktop.

4. Make sure that your device doesn't go to sleep/lockout and that you have a stable internet connection during the installation.

Initial Setup:Building the Labbox into a Docker Image

- Create a new folder/directory on your system to hold the Labbox files and give it a name (**tenablesc-labbox-image**)
- Extract the zip file into that new directory. You should see a few files and a 'utils'. Directory.



- Build the Docker image by typing the following command in your Command Prompt/Terminal. (Make sure that you open the directory where the files are located before running the command).

$ **docker build ./ -f Dockerfile -t tenablesc-labbox-image**

This should take less than 30 minutes to complete and requires stable internet access. This is a one-time installation.

Below is the expected output of the command once completed.

```
TNS11870L:docker_labbox sahmed$ docker build ./ -f Dockerfile -t tenablesc-labbox-image
[+] Building 3.9s (12/12) FINISHED
 => [internal] load .dockerignore                                          0.0s
 => => transferring context: 2B                                            0.0s
 => [internal] load build definition from Dockerfile                       0.0s
 => => transferring dockerfile: 2.69kB                                     0.0s
 => [internal] load metadata for docker.io/library/centos:7.9.2009         3.8s
 => [auth] library/centos:pull token for registry-1.docker.io              0.0s
 => [compile-image 1/3] FROM docker.io/library/centos:7.9.2009@sha256:be6  0.0s
 => [internal] load build context                                          0.0s
 => => transferring context: 1.68kB                                        0.0s
 => CACHED [compile-image 2/3] COPY utils/python_setup.sh /root/python_se  0.0s
 => CACHED [compile-image 3/3] RUN /usr/bin/chmod +x /root/python_setup.s  0.0s
 => CACHED [build-image 2/4] COPY --from=compile-image /root /root         0.0s
 => CACHED [build-image 3/4] COPY utils/start.sh /                         0.0s
 => CACHED [build-image 4/4] RUN /usr/bin/yum -y install epel-release      0.0s
 => exporting to image                                                     0.0s
 => => exporting layers                                                    0.0s
 => => writing image sha256:a0f04d9d8e8ce6b1c5bd26b52062ad830aa5cf52c0613  0.0s
 => => naming to docker.io/library/tenablesc-labbox-image                  0.0s
```

- Build the Docker image by typing the following command in your Command Prompt/Terminal. (Make sure that you open the directory where the files are located before running the command).

$ **docker build ./ -f Dockerfile -t tenablesc-labbox-image**

Creating/Starting the Container

- After following the build steps (above), run the command below

$ **docker-compose up -d**

Below is the expected output of the command once completed(Last few lines).

```
Enforcing Labbox Tenable.sc Config...
2023-05-15 11:45:45,306 INFO spawned: 'Apache' with pid 2337
2023-05-15 11:45:45,309 INFO spawned: 'Jobd' with pid 2338
2023-05-15 11:45:47,362 INFO success: Apache entered RUNNING state, process has stayed up for > than 2 seconds (startsecs)
2023-05-15 11:45:47,362 INFO success: Jobd entered RUNNING state, process has stayed up for > than 2 seconds (startsecs)
TenableSC:Apache: started
TenableSC:Jobd: started
Tenable.sc is up and running, available at https://127.0.0.1:8443.
```

If you received this error message**: network docker_labbox_default declared as external, but could not be found.**

```
TNS11870L:docker_labbox sahmed$ docker-compose up -d
network docker_labbox_default declared as external, but could not be found
```

Run **docker network create "docker_labbox_default"** then run **docker-compose up -d**
(Do this only if you received the above error message after running the docker compose command).

Below is the expected output of the command once completed.

```
TNS11870L:docker_labbox sahmed$ docker network create "docker_labbox_default"
ee1f03f15f786bde786fbaa2b8890f7a3915c0b1595cc7884b0ba3a436cc9cf5
```

This command will start the labbox container.

- If this is the first time the container has been run, it will take *up to an hour* to download and install Tenable.sc+ and download the data for Labbox; the docker-compose up command will run relatively quickly. To see the status of the build, run the monitoring command below $ **docker logs tenablesc-labbox -f** (Right after the docker-compose up command to be able to see the installation progress.
- This requires internet access and will download approximately 4-5 GB of data.
- If this is a subsequent container start (it has been built before), it should take less than 30 seconds for Tenable.sc to be available in your browser at https://127.0.0.1:8443. If it's not available after 30 seconds, please review the logs with the monitoring command below.

Access and Credentials

After successful installation of labbox you will be able to access it from your web browser through the following link: https://127.0.0.1:8443/ then you will get the following page "Your connection is not private". To bypass this message, do the following:

Click Advanced>Proceed
Or
Type the following on your keyboard "**thisisunsafe**"

To access the Main GUI:
Username: **secmanager**
Password: **password**

To access the Admin GUI:
Username: **admin**
Password: **password**

There are several other accounts, feel free to modify/delete them as required.

Now you are ready to use the Labbox.

Maintenance and Upgrade

Update Labbox Files(When a new version of Labbox is released)

Most updates for Labbox on Docker should be straight forward. Unless other explicit instructions are given, simply replace the files in the labbox folder with updated ones. They will be automatically updated within the container at next start, if needed.

1. Download the new version and decompress it.
2. Stop the docker container if running
   $ **docker-compose stop**
3. Replace the files in your docker_labbox folder with the new versions.
4. Start the docker container
   $ **docker-compose up -d**
5. You may watch the progress of the update in Docker Desktop or by running:
   $ **docker logs tenablesc-labbox -f**

Upgrade Tenable.sc+ Only

This will attempt to ensure that the Labbox is running the latest GA version of Tenable.sc+. It will perform a backup before an upgrade is attempted.

$ **docker exec tenablesc-labbox touch /tsc_upgrade**

The container must be running and it will initiate within 60 seconds.

To see the status of the job, run the monitoring command above.
If you need to remove everything discussed in here:

Update Everything (Destructive!)

When you need labbox to update everything, type:

$ **docker exec tenablesc-labbox touch /update-all**

This is an equivalent command to "labbox sync all" or "labbox sync full" and is DESTRUCTIVE to labbox (you will lose all customizations). The container must be running and the sync will initiate within 60 seconds. To see the status of the job, run the monitoring command.

Monitoring

To monitor what is going on in the container, view the Logs section in Docker Desktop.

You can also type:

$ **docker logs tenablesc-labbox -f**

This will auto-tail the logs from the running container; CTRL-C will exit out of this (or stop the container by another terminal window/method). Remove the -f flag if you just want a snapshot of the current logs.

Clean Up

$ **docker-compose stop**
$ **docker rm tenablesc-labbox**
$ **docker volume rm tenablescdata**
$ **docker volume rm tenableyumcache**
$ **docker rmi tenablesc-labbox-image**