Assignment 1 : Nectar

Submitted by: Govind Reghunandanan
Student ID: 102865955

Overview:

This first section of this document is a guide (for Linux users) for deploying a simple web application in an LXC container on a Virtual Machine hosted by Nectar.
The second section of this document answers some questions about containers and public key cryptography.

Section I:

1. Create a pair of public and private keys:

a. Run the command `ssh-keygen` in a terminal window to create a private key and public key, referring to the following screenshot to answer any prompts:

2. Log in to Nectar:

a. Open https://dashboard.rc.nectar.org.au/auth/login/ in a browser and click on the button *Australian Log In via AAF*.
b. Search for and select your organisation and click on *Continue to your organisation*.
c. Enter your user name and password in your organisation's login page, and click on *Sign In*.

3. Create an instance:

a. Navigate to the *Compute -> Images* section via the menu on the left.
b. Find the image called *NeCTAR Ubuntu 18.04 LTS (Bionic) amd64* and click the *Launch* button on the right.
c. In the *Details* tab, fill out the required fields as shown in the following screenshot:
d. Navigate to the *Flavors* tab, and click on the icon with an up arrow on the row with the name *m3.small* to allocate it.
e. In the *Key Pair* tab, click on the *Import Key Pair* button.
f. In the *Import Key Pair* popup, upload the *id_rsa.pub* file (located at *~/.ssh* by default.) created in step 1.a, and fill out the remaining details as shown in the following screenshot:

g. In the *Security Groups* tab, click on the up arrow icon for the rows with names *http*, *ssh* and *icmp* to allow the ports 80 and 22 to listen (and to let ping packets through).
h. Click on the *Launch Instance* button to create and launch the instance.
i. Navigate to the *Compute -> Instances* section via the menu on the left, verify that the instance is running and note its IP address.

4. Log into the instance and install LXC and LXD:

a. Open a terminal and run the command `ssh ubuntu@ip_address` (where ip_address must be replaced by the ip address of the instance as noted in 3.i) to open a secure shell into the instance.
b. Run the commands `sudo apt update` (to update apt's repositories) and `sudo apt upgrade` to (update local library versions).
c. Run the command `sudo apt install lxc lxd` to install lxc and lxd.

5. Configure LXC and create a container:

a. Run the command `sudo usermod --append --groups lxd ubuntu` to add the user ubuntu to the group lxd.
b. Run the command `sudo lxd init` to initialize lxd, using the following screenshot as a reference to answer any prompts:
c. Run the command `lxc image list images: | grep -i -E 'alpine.*amd64'` to list out images of the Alpine OS.
d. Run the command `lxc launch images:alpine/3.12` test to create an Alpine container called test.
e. Run the command `lxc list` to verify that the container was created.

6. Start a shell inside the container and install the web application dependencies:

a. Run the command `lxc exec test ash` to open an Almquist shell inside the container test.
b. Run the command `apk add apache2 python3 pip`.
c. Run the command `pip install tinydb` to install the database.
d. Run the command `git pull repo` to pull the source for the database server and client.

7. Start the database server and web server:

a. Run the command `python3 server.py` to start the database server.
e. Run the command `rc-service apache2 start` to start the web server.
f. Run the command cp ./index.html /var/www/localhost/htdocs/index.html to copy the client source code to apache2's ROOT folder.

8. Enable port forwarding:

a. Run the command PORT=80 PUBLIC_IP=115.146.85.216 CONTAINER_IP=10.202.134.140 sudo -E bash -c 'iptables -t nat -I PREROUTING -i eth0 -p TCP -d $PUBLIC_IP --dport $PORT -j DNAT --to-destination $CONTAINER_IP:$PORT -m comment --comment "bind port 81 to lxc alpine container"' to forward all request on port 80 to port 80 (web server) on the container (IP addresses of the instance and container need to be replaced accordingly)
b. Run the command PORT=81 PUBLIC_IP=115.146.85.216 CONTAINER_IP=10.202.134.140 sudo -E bash -c 'iptables -t nat -I PREROUTING -i eth0 -p TCP -d $PUBLIC_IP --dport $PORT -j DNAT --to-destination $CONTAINER_IP:$PORT -m comment --comment "bind port 81 to lxc alpine container"' to forward all requests on port 81 to port 81 (database server) on the container.

9. **Modify security groups to:**

    c. Run the command PORT

Section II:

1. **What is a PEM file and what can it be used to contain?**

    a. A .PEM is a file format used for storing and sending cryptographic keys, certificates and other data. It contains the base64 encoded versions of a private key, and/or a CA certificate and any intermediate certificates, and/or a certificate request.

2. **What does PEM stand for?**

    a. PEM is an abbreviation of Privacy-Enhanced Mail.

3. **Why is it not used for its original purpose?**

    a. PEM relied on the presence of a single root certificate for its public key infrastructure, which was impractical. A competing format called PGP that relied on a more decentralized “web of trust” gained favour, and eventually supplanted PEM. However, the encoding used by PEM is still very popular.

4. **Why is the PEM private key different from a Putty ppk private key?**

    a. The PPK format exists because that’s the format that Putty expects. PEM and PPK files both store the same private key, but the difference is that Putty seems to split up the key into private and public sections, and stores metadata (about for example, how the key was generated) in plaintext.

5. **How can one be converted to the other?**

    a. On Linux, the following command can be used to convert a PEM to a PPK: sudo puttygen pemKey.pem -o ppkKey.ppk -O private
    b. The following command can be used to convert a PPK into a PEM: sudo puttygen pemKey.pem -o ppkKey.ppk -O private

6. **What type of system is used by Ubuntu to launch and manage daemons? How can you prove/demonstrate this?**

    a. systemd is used by ubuntu to launch and manage daemons. This can be seen by running the command systemctl (the basic command used to control systemd), which lists all dameons.

7. **Which editor is configured to edit passwd and group files (via vipw and vigr)??**

    a. vipw and vigr will first attempt to use the editor defined in the environment variable $VISUAL, then the editor defined in the environment variable $EDITOR, and finally the default editor vi.

8. **What is the group ID of your user account?**

    a. 1002

9. **What type of package manager is present on your Ubuntu instance?**

    a. apt (Advanced Package Tool), a front-end to dpkg, is the package manager in the Ubuntu instance. The LXC container uses apk, Alpine's package manager.

10. **What are the names and types of the files in your home directory?**

    a. *.bashrc*: A bash script that will run when a new terminal is opened by the user.
    b. *.bash_logout*: A bash script that will run when the terminal is closed by the user.
    c. *.bash_history*: A list of commands typed by the user.
    d. *.profile*: A bash script that set environment variables for the user.

11. Where is and what is the sudoers file? Can you show the contents?

a. */etc/sudoers* defines the list of users and groups that are allowed to run privileged commands, as well as the commands that a user or group is allowed to run.
b. Yes, I can show the contents of the file with the cat command, but I have to run it as superuser (sudo cat /etc/sudoers).

12. Where is the configuration settings of the PAM module?

a. The global PAM settings are at */etc/pam.conf*, and the settings for PAM-aware applications are under the */etc/pam.d* folder.

13. What does the PAM module do and what does PAM stand for??

b. The PAM module allows a system administrator to dynamically authenticate a user to applications (or services) in Linux.
c. PAM is an abbreviation of Pluggable Authentication Modules.

14. What services are running in your instance? What command did you use to find this out?

d. Other than the processes started by the kernel, the processes that are running in my instance include lxcfs and lxd, and the processes that it spawned, such as httpd.
e. I used the pstree command. Other commands include ps and top.

15. What is in the Linux journal (yours) and how did you get this information?

f. The Linx journal (of a user) logs the activity of all processes started by the user.
g. The command journalctl --user returns the human readable contents of the journal file.

16. Use a command to find the date/time when the public key was generated on your instance.

h. stat ~/ .ssh/authorized_keys returned the last access time, and last modified time. I was unable to find the time this file was created (my understanding is that Linux has no command to do this), but assuming that this file was not modified since creation, the last modified time can be considered the creation time.

17. What is the full (absolute) path to your home directory?

i. The command echo ~ returned */home/ubuntu*

18. Is Apache installed? How do you know?

j. Yes, it is installed
k. The command which apache2 returned the absolute path of apache2

19. Explain the difference between an LVM container and a Docker container.

l. An LVM is a device mapper that allows Linux to map multiple physical storage devices to a single virtual storage device. This allows Linux to partition existing storage devices or add additional ones without rebooting the computer.
m. Docker on the other hand, is a container technology. It allows applications to run in different containers on a Docker runtime, which itself runs on the host operating system and uses the OS resources. This means that Docker can be configured to use any device mapper used by the underlying OS, including LVM.

20. What is the systemd command for shutting down your Nectar VM?

n. sudo systemctl poweroff

https://softwareengineering.stackexchange.com/questions/163952/how-do-pgp-and-pem-differ

https://en.wikipedia.org/wiki/Privacy-Enhanced_Mail

https://aws.amazon.com/premiumsupport/knowledge-center/convert-pem-file-into-ppk/

https://www.tecmint.com/configure-pam-in-centos-ubuntu-linux/