Exercise 3.1: Install Kubernetes

Overview

There are several Kubernetes installation tools provided by various vendors. In this lab we will learn to use **kubeadm**. As a community-supported independent tool, it is planned to become the primary manner to build a Kubernetes cluster.

Platforms: GCP, AWS, VirtualBox, etc

The labs were written using **Ubuntu** instances running on **G**oogle **C**loud **P**latform (**GCP**). They have been written to be vendor-agnostic so could run on AWS, local hardware, or inside of virtualization to give you the most flexibility and options. Each platform will have different access methods and considerations. As of v1.14.1 the minimum (as in barely works) size for **VirtualBox** is 3vCPU/4G memory/5G minimal OS for `master` and 1vCPU/2G memory/5G minimal OS for worker node.

If using your own equipment you will have to disable swap on every node. There may be other requirements which will be shown as warnings or errors when using the **kubeadm** command. While most commands are run as a regular user, there are some which require root privilege. Please configure **sudo** access as shown in a previous lab. You If you are accessing the nodes remotely, such as with **GCP** or **AWS**, you will need to use an SSH client such as a local terminal or **PuTTY** if not using **Linux** or a Mac. You can download **PuTTY** from `www.putty.org`. You would also require a `.pem` or `.ppk` file to access the nodes. Each cloud provider will have a process to download or create this file. If attending in-person instructor led training the file will be made available during class.

Very Important

Please disable any firewalls while learning Kubernetes. While there is a list of required ports for communication between components, the list may not be as complete as necessary. If using **GCP** you can add a rule to the project which `allows all traffic to all ports`. Should you be using **VirtualBox** be aware that inter-VM networking will need to be set to `promiscuous mode`.

In the following exercise we will install Kubernetes on a single node then grow the cluster, adding more compute resources. Both nodes used are the same size, providing 2 vCPUs and 7.5G of memory. Smaller nodes could be used, but would run slower.

YAML files and White Space

Various exercises will use YAML files, which are included in the text. You are encouraged to write the files when possible, as the syntax of YAML has white space indentation requirements that are important to learn. An important note, **do not** use tabs in your YAML files, **white space only. Indentation matters.**

If using a PDF the use of copy and paste often does not paste the single quote correctly. It pastes as a back-quote instead. You will need to modify it by hand. The files have also been made available as a compressed **tar** file. You can view the resources by navigating to this URL:

`https://training.linuxfoundation.org/cm/LFS258`

To login use user: `LFtraining` and a password of: `Penguin2014`

Once you find the name and link of the current file, which will change as the course updates, use **wget** to download the file into your node from the command line then expand it like this:

```
$ wget https://training.linuxfoundation.org/cm/LFS258/LFS258_V2019-08-12_SOLUTIONS.tar.bz2 \
              --user=LFtraining --password=Penguin2014

$ tar -xvf LFS258_V2019-08-12_SOLUTIONS.tar.bz2
```

(**Note**: depending on your pdf viewer, if you are cutting and pasting the above instructions, the underscores may disappear and be replaced by spaces, so you may have to edit the command line by hand!)

Bionic

While **Ubuntu 18** `bionic` has become the typical version to deploy, the Kubernetes repository does not yet have compatible binaries at the time of this writing. While `xenial` binaries can be used there are many additional steps necessary to complete the labs. A **Ubuntu 18** version is expected to be available soon.

Install Kubernetes

Log into your nodes. If attending in-person instructor led training the node IP addresses will be provided by the instructor. You will need to use a `.pem` or `.ppk` key for access, depending on if you are using **ssh** from a terminal or **PuTTY**. The instructor will provide this to you.

1. Open a terminal session on your first node. For example, connect via **PuTTY** or **SSH** session to the first **GCP** node. The user name may be different than the one shown, `student`. The IP used in the example will be different than the one you will use.

```
[student@laptop ~]$  ssh -i LFS458.pem student@35.226.100.87
The authenticity of host '54.214.214.156 (35.226.100.87)' can't be established.
ECDSA key fingerprint is SHA256:IPvznbkx93/Wc+ACwXrCcDDgvBwmvEXC9vmYhk2Wo1E.
ECDSA key fingerprint is MD5:d8:c9:4b:b0:b0:82:d3:95:08:08:4a:74:1b:f6:e1:9f.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '35.226.100.87' (ECDSA) to the list of known hosts.
<output_omitted>
```

2. Become `root` and update and upgrade the system. Answer any questions to use the defaults.

```
student@lfs458-node-1a0a:~$ sudo -i

root@lfs458-node-1a0a:~# apt-get update && apt-get upgrade -y
<output_omitted>
```

3. The main choices for a container environment are **Docker** and **cri-o**. We will user **Docker** for class, as **cri-o** is not yet the default when building the cluster with **kubeadm**.

```
root@lfs458-node-1a0a:~# apt-get install -y docker.io
<output-omitted>
```

4. Add a new repo for kubernetes. You could also download a tar file or use code from GitHub. Create the file and add an entry for the main repo for your distribution. As we are still using `Ubuntu 16.04` add the `kubernetes-xenial` with the key word `main`. Note there are four sections to the entry.

```
root@lfs458-node-1a0a:~# vim /etc/apt/sources.list.d/kubernetes.list
deb  http://apt.kubernetes.io/  kubernetes-xenial  main
```


5. Add a GPG key for the packages. The command spans three lines. You can omit the backslash when you type. The `OK` is the expected output, not part of the command.

```
root@lfs458-node-1a0a:~# curl -s \
   https://packages.cloud.google.com/apt/doc/apt-key.gpg \
   | apt-key add -

OK
```

6. Update with the new repo declared, which will download updated repo information.

```
root@lfs458-node-1a0a:~# apt-get update

<output-omitted>
```

7. Install the software. There are regular releases the newest of which can be used by omitting the equal sign and version information on the command line. Historically new versions have lots of changes and a good chance of a bug or five.

```
root@lfs458-node-1a0a:~# apt-get install -y \
        kubeadm=1.15.1-00 kubelet=1.15.1-00 kubectl=1.15.1-00

<output-omitted>
```

8. Deciding which pod network to use for Container Networking Interface (**CNI**) should take into account the expected demands on the cluster. There can be only one pod network per cluster, although the **CNI-Genie** project is trying to change this.

   The network must allow container-to-container, pod-to-pod, pod-to-service, and external-to-service communications. As **Docker** uses host-private networking, using the `docker0` virtual bridge and `veth` interfaces would require being on that host to communicate.

   We will use **Calico** as a network plugin which will allow us to use `Network Policies` later in the course. Currently **Calico** does not deploy using CNI by default. The 3.3 version of **Calico** has more than one configuration file for flexibility with RBAC. Download the configuration files for Calico and RBAC. Once downloaded look for the expected IPV4 range for containers to use in the configuration file.

   A short url for each file is shown in the following **wget** commands. the longer URLs can be found here: https://docs.projectcalico.org/v3.3/getting-started/kubernetes/installation/hosted/rbac-kdd.yaml and: https://docs.projectcalico.org/v3.3/getting-started/kubernetes/installation/hosted/kubernetes-datastore/calico-networking/1.7/calico.yaml

```
root@lfs458-node-1a0a:~# wget https://tinyurl.com/yb4xturm -O rbac-kdd.yaml
root@lfs459-node-1a0a:~# wget https://tinyurl.com/y8lvqc9g -O calico.yaml
```

9. Use **less** to page through the file. Look for the IPV4 pool assigned to the containers. There are many different configuration settings in this file. Take a moment to view the entire file. The `CALICO_IPV4POOL_CIDR` must match the value given to **kubeadm init** in the following step, whatever the value may be.

```
root@lfs458-node-1a0a:~# less calico.yaml
```

calico.yaml

```
....
   # The default IPv4 pool to create on startup if none exists. Pod IPs will be
   # chosen from this range. Changing this value after installation will have
   # no effect. This should fall within `--cluster-cidr`.
            - name: CALICO_IPV4POOL_CIDR
              value: "192.168.0.0/16"
....
```

10. Find the IP address of the primary interface of the master server. The example below would be the `ens4` interface and an IP of `10.128.0.3`, yours may be different.


```
root@lfs458-node-1a0a:~# ip addr show
....
2: ens4: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1460 qdisc mq state UP group default qlen 1000
    link/ether 42:01:0a:80:00:18 brd ff:ff:ff:ff:ff:ff
    inet 10.128.0.3/32 brd 10.128.0.3 scope global ens4
       valid_lft forever preferred_lft forever
    inet6 fe80::4001:aff:fe80:18/64 scope link
       valid_lft forever preferred_lft forever
....
```

11. Add an local DNS alias for our master server. Edit the `/etc/hosts` file and add the above IP address and assign a name `k8smaster`.

```
root@lfs458-node-1a0a:~# vim /etc/hosts

10.128.0.3 k8smaster    #<-- Add this line
127.0.0.1 localhost
....
```

12. Create a configuration file for the cluster. There are many options we could include, but will only set the control plane endpoint, software version to deploy and podSubnet values. After our cluster is initialized we will view other default values used. Be sure to use the node alias, not the IP so the network certificates will continue to work when we deploy a load balancer in a future lab.

```
root@lfs458-node-1a0a:~# vim kubeadm-config.yaml
```

kubeadm-config.yaml

```
1 apiVersion: kubeadm.k8s.io/v1beta2
2 kind: ClusterConfiguration
3 kubernetesVersion: 1.15.1                #<-- Use the word stable for newest version
4 controlPlaneEndpoint: "k8smaster:6443"   #<-- Use the node alias not the IP
5 networking:
6   podSubnet: 192.168.0.0/16              #<-- Match the IP range from the Calico config file
```

13. Initialize the master. Read through the output line by line. Expect the output to change as the software matures. At the end are configuration directions to run as a non-root user. The token is mentioned as well. This information can be found later with the **kubeadm token list** command. The output also directs you to create a pod network to the cluster, which will be our next step. Pass the network settings **Calico** has in its configuration file, found in the previous step. **Please note:** the output lists several commands which following commands will complete.

```
root@lfs458-node-1a0a:~# kubeadm init --config=kubeadm-config.yaml --upload-certs \
      | tee kubeadm-init.out      # Save output for future review
```

Please Note

What follows is output of **kubeadm init**. Read the next step prior to further typing.

```
[init] Using Kubernetes version: v1.15.1
[preflight] Running pre-flight checks
[WARNING IsDockerSystemdCheck]: detected "cgroupfs" as the
Docker cgroup driver. The recommended driver is "systemd".

....

You can now join any number of the control-plane node
running the following command on each as root:
```



```
kubeadm join k8smaster:6443 --token vapzqi.et2p9zbkzk29wwth \
 --discovery-token-ca-cert-hash sha256:f62bf97d4fba6876e4c3ff645df3fca969c06169dee3865aab9d0bca8ec9f8cd \
 --control-plane --certificate-key 911d41fcada89a18210489afaa036cd8e192b1f122ebb1b79cce1818f642fab8

Please note that the certificate-key gives access to cluster sensitive
data, keep it secret!
As a safeguard, uploaded-certs will be deleted in two hours; If
necessary, you can use
"kubeadm init phase upload-certs --upload-certs" to reload certs afterward.

Then you can join any number of worker nodes by running the following
on each as root:

kubeadm join k8smaster:6443 --token vapzqi.et2p9zbkzk29wwth \
 --discovery-token-ca-cert-hash sha256:f62bf97d4fba6876e4c3ff645df3fca969c06169dee3865aab9d0bca8ec9f8cd
```

14. As suggested in the directions at the end of the previous output we will allow a `non-root` user admin level access to the cluster. Take a quick look at the configuration file once it has been copied and the permissions fixed.

```
root@lfs458-node-1a0a:~# exit
logout

student@lfs458-node-1a0a:~$ mkdir -p $HOME/.kube

student@lfs458-node-1a0a:~$ sudo cp -i /etc/kubernetes/admin.conf $HOME/.kube/config

student@lfs458-node-1a0a:~$ sudo chown $(id -u):$(id -g) $HOME/.kube/config

student@lfs458-node-1a0a:~$ less .kube/config
apiVersion: v1
clusters:
- cluster:
<output_omitted>
```

15. Apply the network plugin configuration to your cluster. Remember to copy the file to the current, non-root user directory first.

```
student@lfs458-node-1a0a:~$ sudo cp /root/rbac-kdd.yaml .

student@lfs458-node-1a0a:~$ kubectl apply -f rbac-kdd.yaml
clusterrole.rbac.authorization.k8s.io/calico-node created
clusterrolebinding.rbac.authorization.k8s.io/calico-node created

student@lfs458-node-1a0a:~$ sudo cp /root/calico.yaml .

student@lfs458-node-1a0a:~$ kubectl apply -f calico.yaml
configmap/calico-config created
service/calico-typha created
deployment.apps/calico-typha created
poddisruptionbudget.policy/calico-typha created
<output_omitted>
```

16. While many objects have short names, a **kubectl** command can be a lot to type. We will enable **bash** auto-completion. Begin by adding the settings to the current shell. Then update the `~/.bashrc` file to make it persistent.

```
student@lfs458-node-1a0a:~$ source <(kubectl completion bash)

student@lfs458-node-1a0a:~$ echo "source <(kubectl completion bash)" >> ~/.bashrc
```


17. Test by describing the node again. Type the first three letters of the sub-command then type the **Tab** key. Auto-completion assumes the `default` namespace. Pass the namespace first to use auto-completion with a different namespace. By pressing **Tab** multiple times you will see a list of possible values. Continue typing until a unique name is used. First look at the current node, then look at pods in the `kube-system` namespace.

```
student@lfs458-node-1a0a:~$ kubectl des<Tab> n<Tab><Tab> lfs458-<Tab>

student@lfs458-node-1a0a:~$ kubectl -n kube-s<Tab> g<Tab> po<Tab>
```

18. View other values we could have included in the `kubeadm-config.yaml` file when creating the cluster.

```
student@lfs458-node-1a0a:~$ sudo kubeadm config print init-defaults
apiVersion: kubeadm.k8s.io/v1beta2
bootstrapTokens:
- groups:
  - system:bootstrappers:kubeadm:default-node-token
  token: abcdef.0123456789abcdef
  ttl: 24h0m0s
  usages:
  - signing
  - authentication
kind: InitConfiguration
<output_omitted>
```

