Department of Computing

SE-315: Cloud Computing

Lab 15: Setting up a Private Kubernetes Cluster

CLO4: Display skills to effectively use cloud centric solutions such as serverless application development.

Date: 25.12.24

Lab 15: Setting up a Private Kubernetes Cluster

Introduction:

In Kubernetes Engine, a private cluster is a cluster that makes your master inaccessible from the public internet. In a private cluster, nodes do not have public IP addresses, only private addresses, so your workloads run in an isolated environment. Nodes and masters communicate with each other using VPC peering.

In the Kubernetes Engine API, address ranges are expressed as Classless Inter-Domain Routing (CIDR) blocks.

Lab Objectives: In this lab, you learn how to create a private Kubernetes cluster.

Lab Tasks

https://www.cloudskillsboost.google/course_templates/645/labs/489298

A. Set region and zone

```
sfatima_bese22seecs@cloudshell:~ (vid-city)$ gcloud config set compute/zone us-central1-a
WARNING: Property validation for compute/zone was skipped.
Updated property [compute/zone].
```

B. Creating a private cluster

```
gcloud beta container clusters create private-cluster --enable-private-nodes
--master-ipv4-cidr 172.16.0.16/28 --enable-ip-alias --create-subnetwork ""
```

```
kubeconfig entry generated for private-cluster.
NAME: private-cluster
LOCATION: us-central1-a
MASTER_VERSION: 1.30.6-gke.1125000
MASTER_IP: 34.59.147.98
MACHINE_TYPE: e2-medium
NODE_VERSION: 1.30.6-gke.1125000
NUM_NODES: 3
STATUS: RUNNING
```

C. View your subnet and secondary address range

List the subnets in the default network:

```
sfatima_bese22seecs@cloudshell:~ (vid-city)$ gcloud compute networks subnets list
--network default
NAME: default
REGION: us-central1
NETWORK: default
RANGE: 10.128.0.0/20
STACK_TYPE: IPV4_ONLY
IPV6_ACCESS_TYPE:
INTERNAL_IPV6_PREFIX:
EXTERNAL_IPV6_PREFIX:

NAME: gke-private-cluster-54494d5f-pe-subnet
REGION: us-central1
NETWORK: default
RANGE: 172.16.0.16/28
```

Now, I am getting the information for the automatically created subnetwork for my cluster. In the above screnhot we can see that it is **"gke-private-cluster-54494d5f-pe-subnet"**

```
sfatima_bese22seecs@cloudshell:~ (vid-city)$ gcloud compute networks subnets descr
ibe gke-private-cluster-54494d5f-pe-subnet --region=us-central1
creationTimestamp: '2024-12-28T04:24:52.453-08:00'
description: Control Plane Endpoint Subnetwork
fingerprint: My7YivaGHPU=
gatewayAddress: 172.16.0.17
id: '4029326883278704891'
ipCidrRange: 172.16.0.16/28
kind: compute#subnetwork
name: gke-private-cluster-54494d5f-pe-subnet
network: https://www.googleapis.com/compute/v1/projects/vid-city/global/networks/d
efault
privateIpGoogleAccess: false
privateIpv6GoogleAccess: DISABLE_GOOGLE_ACCESS
purpose: PRIVATE
```

D. Enable master authorized networks

Create a VM instance

```
sfatima_bese22seecs@cloudshell:~ (vid-city)$ gcloud compute instances create sourc
e-instance --zone=$ZONE --scopes 'https://www.googleapis.com/auth/cloud-platform'
Created [https://www.googleapis.com/compute/v1/projects/vid-city/zones/us-central1
-a/instances/source-instance].
NAME: source-instance
ZONE: us-central1-a
MACHINE_TYPE: n1-standard-1
PREEMPTIBLE:
INTERNAL_IP: 10.128.0.2
EXTERNAL_IP: 35.239.246.143
STATUS: RUNNING
```

We can see the External IP address as: **35.239.246.143**

```
sfatima_bese22seecs@cloudshell:~ (vid-city)$ gcloud compute instances describe
source-instance --zone=$ZONE | grep natIP
    natIP: 35.239.246.143
```

Authorizing my external address range by speicfiying **external IP Range** as **35.239.246.143/32**

```
sfatima_bese22seecs@cloudshell:~ (vid-city)$ gcloud container clusters update p
rivate-cluster     --enable-master-authorized-networks     --master-authorized-
networks  35.239.246.143/32
Updating private-cluster...done.
Updated [https://container.googleapis.com/v1/projects/vid-city/zones/us-central
1-a/clusters/private-cluster].
To inspect the contents of your cluster, go to: https://console.cloud.google.co
m/kubernetes/workload_/gcloud/us-central1-a/private-cluster?project=vid-city
```

Configuring SSH:

```
sfatima_bese22seecs@cloudshell:~ (vid-city)$ gcloud compute ssh source-instance
 --zone=$ZONE
Updating project ssh metadata...working..Updated [https://www.googleapis.com/co
mpute/v1/projects/vid-city].
Updating project ssh metadata...done.
Waiting for SSH key to propagate.
Warning: Permanently added 'compute.8294163776811452039' (ED25519) to the list
of known hosts.
Linux source-instance 6.1.0-28-cloud-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.11
9-1 (2024-11-22) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
```

Installing kubectl component of Cloud-SDK in SSH Shell:

```
sfatima_bese22seecs@source-instance:~$ sudo apt-get install kubectl
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  kubectl
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
```

Configuring access to the Kubernetes cluster from SSH shell:

```
sfatima_bese22seecs@source-instance:~$ sudo apt-get install google-cloud-sdk-gk
e-gcloud-auth-plugin
gcloud container clusters get-credentials private-cluster --zone=$ZONE
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  google-cloud-cli-gke-gcloud-auth-plugin
The following NEW packages will be installed:
  google-cloud-cli-gke-gcloud-auth-plugin
  google-cloud-sdk-gke-gcloud-auth-plugin
0 upgraded, 2 newly installed, 0 to remove and 0 not upgraded.
```

```
sfatima_bese22seecs@source-instance:~$ gcloud container clusters get-credential
s private-cluster --zone=us-central1-a
Fetching cluster endpoint and auth data.
kubeconfig entry generated for private-cluster.
```

Verifying that the private cluster nodes do not have external IP addresses:

```
sfatima_bese22seecs@source-instance:~$ kubectl get nodes --output yaml | grep -
A4 addresses
    addresses:
    - address: 10.33.168.3
      type: InternalIP
    allocatable:
      cpu: 940m
--
    addresses:
    - address: 10.33.168.2
      type: InternalIP
    allocatable:
      cpu: 940m
--
    addresses:
```

We can see that **EXTERNAL-IP is <none>**

```
sfatima_bese22seecs@source-instance:~$ kubectl get nodes --output wide
NAME                                          STATUS   ROLES    AGE   VERSION               INTERNAL-IP   EXTERNAL-IP
ERNEL-VERSION   CONTAINER-RUNTIME
gke-private-cluster-default-pool-7d9e0004-7hxp   Ready    <none>   50m   v1.30.6-gke.1125000   10.33.168.3   <none>
.1.112+         containerd://1.7.23
gke-private-cluster-default-pool-7d9e0004-gltj   Ready    <none>   50m   v1.30.6-gke.1125000   10.33.168.2   <none>
.1.112+         containerd://1.7.23
gke-private-cluster-default-pool-7d9e0004-qbpg   Ready    <none>   50m   v1.30.6-gke.1125000   10.33.168.4   <none>
.1.112+         containerd://1.7.23
sfatima_bese22seecs@source-instance:~$
```

E. Clean Up

Deleting the private cluster we created to free up resources:

```
sfatima_bese22seecs@cloudshell:~ (vid-city)$ gcloud container clusters delete private-cluster --
zone=us-central1-a
The following clusters will be deleted.
 - [private-cluster] in [us-central1-a]

Do you want to continue (Y/n)?  y

Deleting cluster private-cluster...done.
Deleted [https://container.googleapis.com/v1/projects/vid-city/zones/us-central1-a/clusters/priv
ate-cluster].
```

F. Create a private cluster that uses a custom subnetwork

Create a subnetwork and secondary ranges:

```
sfatima_bese22seecs@cloudshell:~ (vid-city)$ gcloud compute networks subnets create my-subnet \
    --network default \
    --range 10.0.4.0/22 \
    --enable-private-ip-google-access \
    --region=$REGION \
    --secondary-range my-svc-range=10.0.32.0/20,my-pod-range=10.4.0.0/14
Created [https://www.googleapis.com/compute/v1/projects/vid-city/regions/us-central1/subnetworks
/my-subnet].
NAME: my-subnet
REGION: us-central1
NETWORK: default
RANGE: 10.0.4.0/22
STACK_TYPE: IPV4_ONLY
IPV6_ACCESS_TYPE:
```

Create a private cluster that uses your subnetwork:

```
sfatima_bese22seecs@cloudshell:~ (vid-city)$ gcloud beta container clusters create private-clust
er2 \
    --enable-private-nodes \
    --enable-ip-alias \
    --master-ipv4-cidr 172.16.0.32/28 \
    --subnetwork my-subnet \
    --services-secondary-range-name my-svc-range \
    --cluster-secondary-range-name my-pod-range \
    --zone=$ZONE
```

Retrieve the external address range of the source instance:

```
sfatima_bese22seecs@cloudshell:~ (vid-city)$ gcloud compute instances describe source-instance
-zone=us-central1-a | grep natIP
    natIP: 35.239.246.143
```

External address = 35.239.246.143/32

Running the following to Authorize my external address range:

```
sfatima_bese22seecs@cloudshell:~ (vid-city)$ gcloud container clusters update private-cluster2
   --enable-master-authorized-networks     --zone=$ZONE     --master-authorized-networks 35.239.
246.143/32
Updating private-cluster2...done.
Updated [https://container.googleapis.com/v1/projects/vid-city/zones/us-central1-a/clusters/priv
ate-cluster2].
To inspect the contents of your cluster, go to: https://console.cloud.google.com/kubernetes/work
load_/gcloud/us-central1-a/private-cluster2?project=vid-city
```

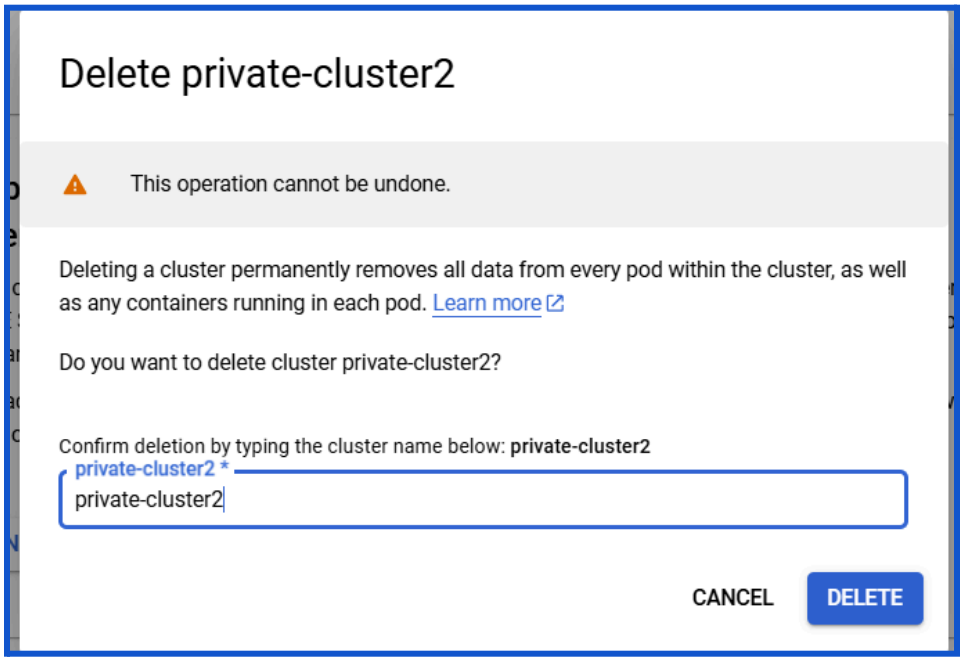
SSH into source-instance and configuring access to the Kubernetes cluster from SSH shell:

```
sfatima_bese22seecs@source-instance:~$ gcloud container clusters get-credentials private-cluster
2 --zone=us-central1-a
Fetching cluster endpoint and auth data.
kubeconfig entry generated for private-cluster2.
```

Verifying that my cluster nodes do not have external IP addresses:

```
sfatima_bese22seecs@source-instance:~$ kubectl get nodes --output wide
NAME                                          STATUS   ROLES    AGE     VERSION               INTERNAL-IP   EXTERNAL-IP
  KERNEL-VERSION   CONTAINER-RUNTIME
gke-private-cluster2-default-pool-29712df2-3rx2   Ready    <none>   5m13s   v1.30.6-gke.1125000   10.0.4.3      <none>
  6.1.112+         containerd://1.7.23
gke-private-cluster2-default-pool-29712df2-s9bp   Ready    <none>   5m13s   v1.30.6-gke.1125000   10.0.4.4      <none>
  6.1.112+         containerd://1.7.23
gke-private-cluster2-default-pool-29712df2-zltt   Ready    <none>   5m13s   v1.30.6-gke.1125000   10.0.4.2      <none>
  6.1.112+         containerd://1.7.23
```

Lastly delete the created cluster through lubernetes engine:



–the end–