Adding authorized networks for cluster master access

This page explains how to grant authorized network access to cluster masters in Google Kubernetes Engine clusters (https://cloud.google.com/kubernetes-engine/docs/concepts/cluster-architecture). For general information about GKE networking, visit the Network Overview (https://cloud.google.com/kubernetes-engine/docs/concepts/network-overview).

Overview

Authorized networks allow you to whitelist specific CIDR ranges and allow IP addresses in those ranges to access your cluster master (https://cloud.google.com/kubernetes-engine/docs/concepts/cluster-architecture#master) endpoint using HTTPS. Authorized networks are compatible with all clusters.

GKE uses both Transport Layer Security (TLS) and authentication to provide secure access to your cluster master endpoint from the public Internet. This provides you the flexibility to administer your cluster from anywhere. By using authorized networks, you can further restrict access to specified sets of IP addresses.

Note: Authorized networks block untrusted IP addresses from *outside Google Cloud*. Addresses from inside Google Cloud (such as traffic from Compute Engine VMs) can reach your master using HTTPS, provided that they have the necessary Kubernetes credentials.

Benefits

Adding authorized networks can provide additional security benefits for your cluster. Authorized networks grant access to a specific set of addresses that you designate, such as those that originate from your environment. This can help protect access to your cluster in the case of a vulnerability in the cluster's authentication or authorization mechanisms.

Note: To view the list of IP ranges used by Google Cloud, see Where can I find Compute Engine IP ranges? (https://cloud.google.com/compute/docs/faq#find_ip_range).

Benefits with private clusters

Private clusters (https://cloud.google.com/kubernetes-engine/docs/how-to/private-clusters) run nodes without external IP addresses, and optionally run their cluster master without a publicly-reachable endpoint. Additionally, private clusters do not allow Google Cloud IP addresses to access the cluster master endpoint by default. Using private clusters with authorized networks makes your cluster master reachable only by the whitelisted CIDRs, by nodes within your cluster's VPC, and by Google's internal production jobs that manage your master.

Limitations

- A cluster can have no more than 50 authorized network CIDR ranges.

Before you begin

To prepare for this task, perform the following steps:

- Ensure that you have enabled the Google Kubernetes Engine API.

  ENABLE GOOGLE KUBERNETES ENGINE API (HTTPS://CONSOLE.CLOUD.GOOGLE.COM/APIS/LIBRA

- Ensure that you have installed the Cloud SDK (https://cloud.google.com/sdk/downloads).
- Set your default project ID (https://support.google.com/cloud/answer/6158840):

```
gcloud config set project [PROJECT_ID]
```

- If you are working with zonal clusters, set your default compute zone (https://cloud.google.com/compute/docs/zones#available):

```
gcloud config set compute/zone [COMPUTE_ZONE]
```

- If you are working with regional clusters, set your default compute region (https://cloud.google.com/compute/docs/zones#available):

```
gcloud config set compute/region [COMPUTE_REGION]
```

- Update `gcloud` to the latest version:

```
gcloud components update
```

★ **Note:** You can override these default settings in `gcloud` commands using the `--project`, `--zone`, and `--region` operational flags.

Creating a cluster with authorized networks

You can create a cluster with one or more authorized networks using the `gcloud` command-line tool, or by using Google Cloud Console.

GCLOUD | CONSOLE | API

Run the following command:

```
gcloud container clusters create [CLUSTER_NAME] \
    --enable-master-authorized-networks \
    --master-authorized-networks [CIDR],[CIDR]...
```

With the `--master-authorized-networks` flag, you can specify up to 50 comma-delimited CIDRs (such as `8.8.8.0/24`) that you'd like to grant access your cluster master endpoint through HTTPS.

For example:

```
gcloud container clusters create example-cluster \
    --enable-master-authorized-networks \
    --master-authorized-networks 8.8.8.8/32,8.8.8.0/24
```

Creating a private cluster with authorized networks

To learn how to create a private cluster with one or more authorized networks, refer to Private Clusters (https://cloud.google.com/kubernetes-engine/docs/how-to/private-clusters).

Add an authorized network to an existing cluster

You can add an authorized network to an existing cluster using the `gcloud` command-line tool, or by using Cloud Console.

GCLOUD CONSOLE API

Run the following command:

```
gcloud container clusters update [CLUSTER_NAME] \
    --enable-master-authorized-networks \
    --master-authorized-networks [CIDR],[CIDR]...
```

With the `--master-authorized-networks` flag, you can specify up to 50 comma-delimited CIDRs (such as `8.8.8.0/24`) that you'd like to grant access your cluster master endpoint through HTTPS.

For example:

```
gcloud container clusters update example-cluster \
    --enable-master-authorized-networks \
    --master-authorized-networks 8.8.8.8/32,8.8.8.0/24
```

Verifying an authorized network

You can verify an authorized network in an existing cluster using the `gcloud` command-line tool, or by using Cloud Console.

GCLOUD CONSOLE API

Run the following command:

```
gcloud container clusters describe [CLUSTER_NAME]
```

In the command output, look for the `masterAuthorizedNetworksConfig` field:

```
  ...
masterAuthorizedNetworksConfig:
  cidrBlocks:
  - cidrBlock: 8.8.8.8/32
  - cidrBlock: 8.8.4.4/32
```

```
  enabled: true
  ...
```

Disable authorized networks

Caution: This allows the public Internet (`0.0.0.0/0`) to reach your cluster master endpoint through HTTPS.

You can disable authorized networks for an existing cluster using the `gcloud` command-line tool, or by using Cloud Console.

GCLOUD CONSOLE

Run the following command:

```
gcloud container clusters update [CLUSTER_NAME] \
--no-enable-master-authorized-networks
```

Troubleshooting

The following sections explain how to resolve common issues with authorized networks.

Too many CIDR blocks

`gcloud` returns the following error when attempting to create or update a cluster with more than 50 CIDR blocks:

```
ERROR: (gcloud.container.clusters.update) argument --master-authorized-networks: too
```

To resolve this issue, ensure that you specify fewer than 50 CIDR blocks.

Unable to connect to master

`kubectl` commands time out due to incorrectly configured CIDR blocks:

```
Unable to connect to the server: dial tcp MASTER_IP: getsockopt: connection timed ou
```

When you create or update a cluster, ensure that you specify the correct CIDR blocks (#verify).

What's next

- Read the GKE network overview (https://cloud.google.com/kubernetes-engine/docs/concepts/network-overview).
- Learn about VPC-native clusters (https://cloud.google.com/kubernetes-engine/docs/how-to/alias-ips).
- Learn about firewall rules (https://cloud.google.com/vpc/docs/firewalls).
- Learn how to create private clusters (https://cloud.google.com/kubernetes-engine/docs/how-to/private-clusters).

Last updated December 18, 2019.