# GKE POD Identity to Access Google API

1. 使用 GCE 默认 service account

在 GCP 上创建 GCE VM 时会关联一个默认 compute engine service account（账号特征：PROJECT\_NUMBER-compute@developer.gserviceaccount.com），当 GKE 集群中没有开始 workload identity 且在 pod 中没有通过 serect 带入自定义 service account 情况下，POD 会使用 GCE 节点的默认 compute engine service account， 即 POD 复用 compute engine service account 的权限。

**示例 --** [**GCloud SDK POD**](https://hub.docker.com/r/google/cloud-sdk/)

**创建 POD**

apiVersion: v1

kind: Pod

metadata:

name: workload-identity-test-defaultsa

spec:

containers:

- image: google/cloud-sdk:slim

name: workload-identity-test

command: ["sleep","infinity"]

**访问 POD**

kubectl exec --stdin --tty workload-identity-test-defaultsa -- /bin/bash

**查看 POD 当前身份**

gcloud auth list

**验证权限**

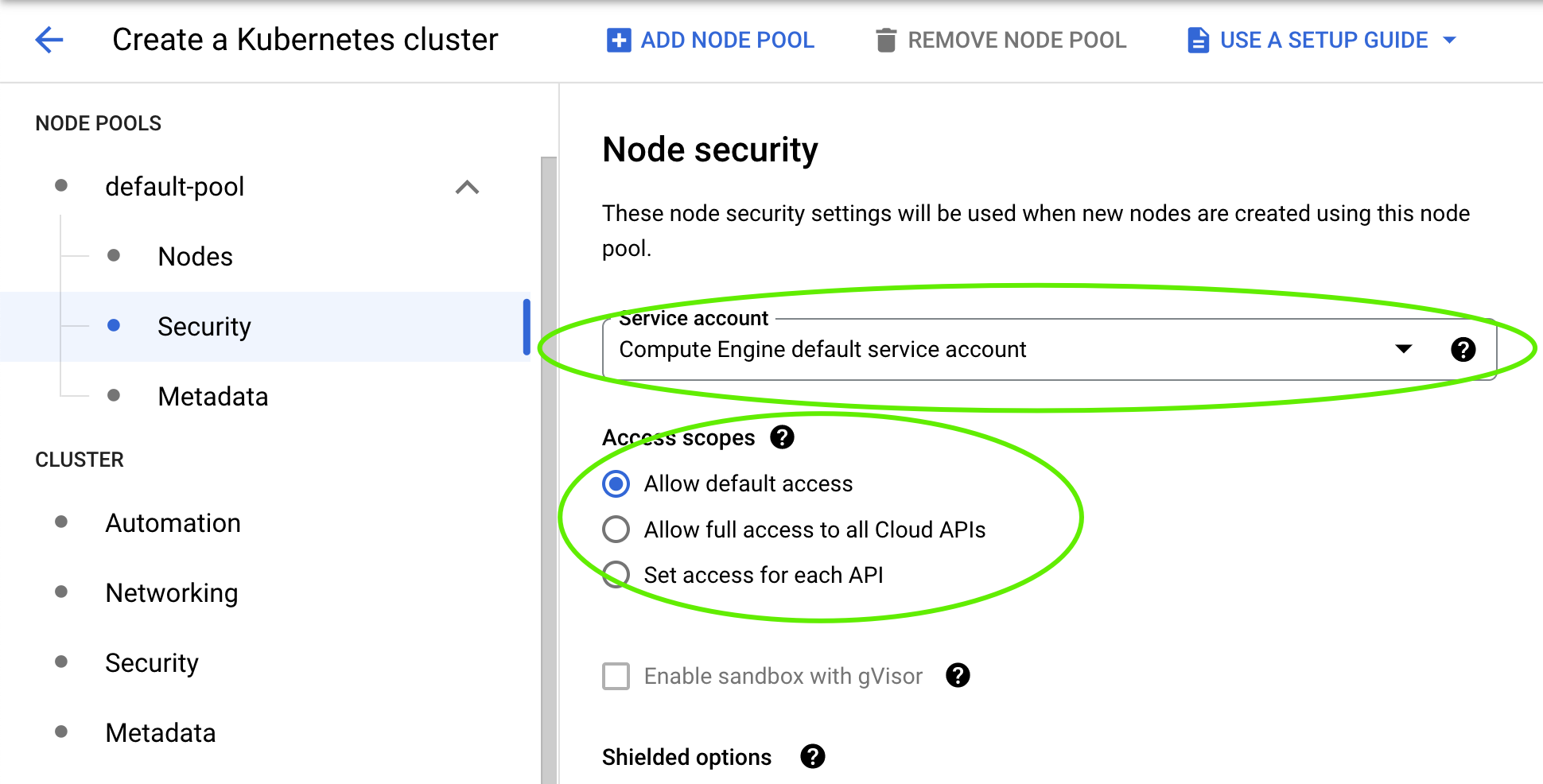
gsutil ls

**默认 service account 权限说明：**

#### **Default scopes**

* Read-only access to Cloud Storage:  
  https://www.googleapis.com/auth/devstorage.read\_only
* Write access to write Compute Engine logs:  
  https://www.googleapis.com/auth/logging.write
* Write access to publish metric data to your Google Cloud projects:  
  https://www.googleapis.com/auth/monitoring.write
* Read-only access to Service Management features required for Google Cloud Endpoints(Alpha):  
  https://www.googleapis.com/auth/service.management.readonly
* Read/write access to Service Control features required for Google Cloud Endpoints(Alpha):  
  https://www.googleapis.com/auth/servicecontrol
* Write access to [Cloud Trace](https://cloud.google.com/trace) allows an application running on a VM to write trace data to a project.  
  https://www.googleapis.com/auth/trace.append

**创建 GKE 集群时可指定默认 service account 权限：**



1. 使用自定义 service account

可在 GCP IAM 下创建 service account 并授予相应 GCP API 权限，通过将 service account 以 Kubernetes Secrets 资源形式带入进 POD，此时 POD 类似一个标准环境自带 service account，用户可以指定方式使用特定 service account。

**示例 --** [**GCloud SDK POD**](https://hub.docker.com/r/google/cloud-sdk/)

**创建 kubernetes secrets，** [**key.json 为 service account 密钥文件**](https://cloud.google.com/kubernetes-engine/docs/tutorials/authenticating-to-cloud-platform#step_3_create_service_account_credentials)

kubectl create secret generic svasecret --from-file=key.json=key.json

**创建 POD**

apiVersion: v1

kind: Pod

metadata:

name: workload-identity-test-customsa

spec:

containers:

- image: google/cloud-sdk:slim

name: workload-identity-test

command: ["sleep","infinity"]

volumeMounts:

- name: google-cloud-key

mountPath: /var/secrets/google

env:

- name: GOOGLE\_APPLICATION\_CREDENTIALS

value: /var/secrets/google/key.json

volumes:

- name: google-cloud-key

secret:

secretName: svasecret

**访问 POD**

kubectl exec --stdin --tty workload-identity-test-customsa -- /bin/bash

**查看 POD 当前身份**

gcloud auth list

**指定身份**

gcloud auth activate-service-account xxx@PROJECT\_ID.iam.gserviceaccount.com \

--key-file=/var/secrets/google/key.json

**查看 POD 当前身份**

gcloud auth list

**验证权限**

gsutil ls

1. Workload Identity 方式

传统 Kubernetes 内有自己的 service account 对象定义，该对象是于 GCP IAM 云台的身份系统无关的一套身份授权体系，用户可以通过将 GCP IAM 中的 service account 和 Kubernetes 内的 service account 相关联，从而将 GCP IAM 身份带入到 POD 中。

**示例 --** [**GCloud SDK POD**](https://hub.docker.com/r/google/cloud-sdk/)

**创建 kubernetes service account**

kubectl create serviceaccount ksademo --namespace default

**创建 GCP IAM service account**

gcloud iam service-accounts create ksademo --project=PROJECT\_ID

**赋权 GCP IAM service account，下面示例授权 project owner role 作为示例，**[**其他预设身份可参考**](https://cloud.google.com/iam/docs/understanding-roles#basic-definitions)

gcloud projects add-iam-policy-binding project-wekang-poc --member "serviceAccount:ksademo@PROJECT\_ID.iam.gserviceaccount.com" --role "roles/owner"

gcloud iam service-accounts add-iam-policy-binding ksademo@PROJECT\_ID.iam.gserviceaccount.com \

--role roles/iam.workloadIdentityUser \

--member "serviceAccount:PROJECT\_ID.svc.id.goog[default/ksademo]"

**关联 kubernetes service account 和 GCP IAM service account**

kubectl annotate serviceaccount ksademo --namespace default iam.gke.io/gcp-service-account=ksademo@PROJECT\_ID.iam.gserviceaccount.com

**创建 POD**

apiVersion: v1

kind: Pod

metadata:

name: workload-identity-test

namespace: default

spec:

containers:

- image: google/cloud-sdk:slim

name: workload-identity-test

command: ["sleep","infinity"]

serviceAccountName: ksademo

nodeSelector:

iam.gke.io/gke-metadata-server-enabled: "true"

**访问 POD**

kubectl exec --stdin --tty workload-identity-test -- /bin/bash

**查看 POD 当前身份**

gcloud auth list

**查看 POD 当前身份**

gcloud auth list

**验证权限**

gsutil ls