Service Accounts

Sunday, December 8, 2019 12:07 PM

Important Notes:

- Your application uses the service account to call the Google API of a service, so that the users aren't directly involved.
- Service account belongs to your applications rather than an individual end user.

Best practices

In general, Google recommends that each instance that needs to call a Google API should run as a service account with the minimum permissions necessary for that instance to do its job. In practice, this means you should configure service accounts for your instances with the following process:

1. Create a new service account rather than using the Compute Engine default service account.
2. Grant IAM roles to that service account for only the resources that it needs.
3. Configure the instance to run as that service account.
4. Grant the instance the https://www.googleapis.com/auth/cloud-platform scope to allow full access to all Google Cloud APIs, so that the IAM permissions of the instance are completely determined by the IAM roles of the service account.

   Avoid granting more access than necessary and regularly check your service account permissions to make sure they are up-to-date.

From <https://cloud.google.com/compute/docs/access/create-enable-service-accounts-for-instances>

Important Links:

https://cloud.google.com/iam/docs/understanding-service-accounts
https://cloud.google.com/compute/docs/access/create-enable-service-accounts-for-instances
https://cloud.google.com/sdk/gcloud/reference/compute/instances/set-service-account (for scopes)

Important Commands:

```
gcloud compute instances set-service-account instance-3 --service-account
demosvc@mercurial-smile-254413.iam.gserviceaccount.com --scopes cloud-platform
gcloud compute instances describe instance-4 --format json
```

Types of Roles

There are three types of roles in Cloud IAM:

- **Primitive roles**, which include the Owner, Editor, and Viewer roles that existed prior to the introduction of Cloud IAM.
- **Predefined roles**, which provide granular access for a specific service and are managed by GCP.
- **Custom roles**, which provide granular access according to a user-specified list of permissions.