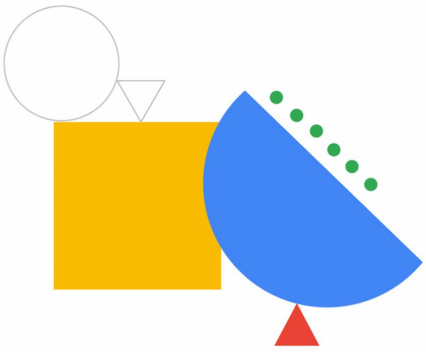
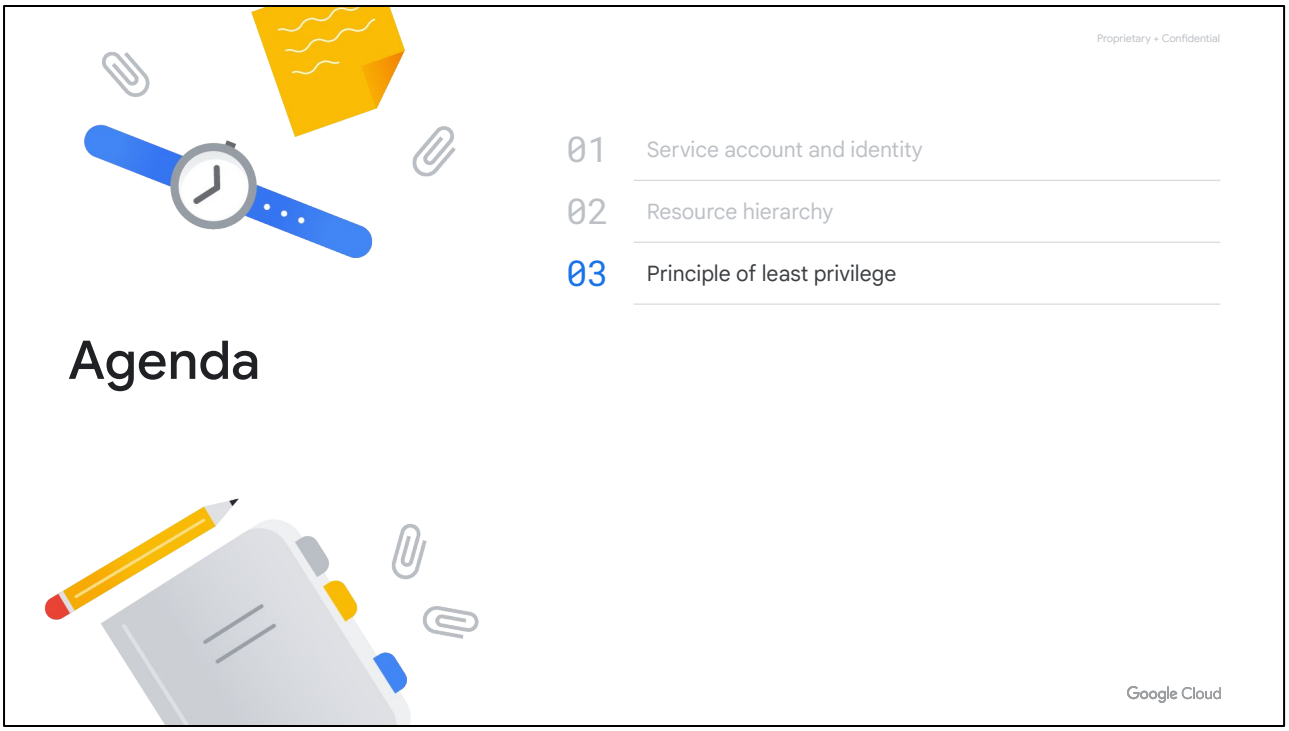
Google Cloud

Service Identity and Authentication



In this module, we discuss the fundamentals of service identity, and how you can invoke other Google Cloud services from your Cloud Run service.



As we continue the discussion on roles and permissions in Google Cloud, let's talk about the principle of least privilege.

Types of IAM roles

Basic	Predefined	Custom
Owner Editor Viewer Very powerful roles with permissions that span all services.	Examples: Cloud Run Admin Pub/Sub Publisher Cloud Tasks Enqueuer Granular roles to use a specific service.	 Build your own role from a list of permissions for your use case.

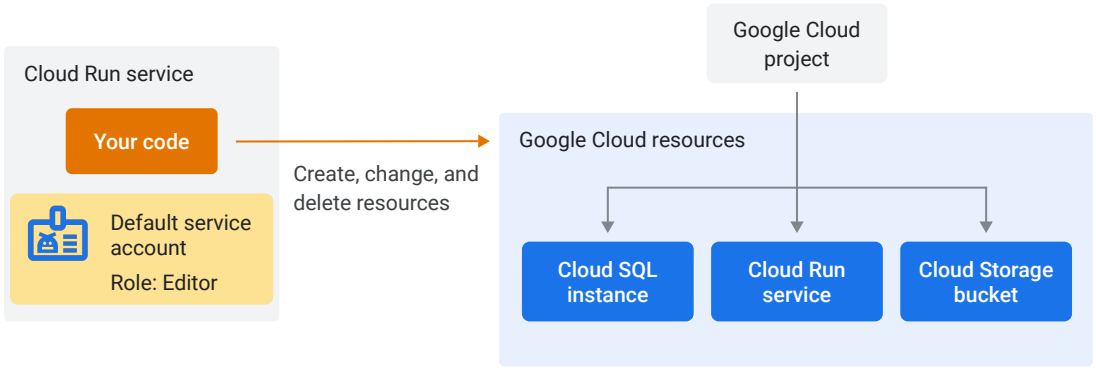
There are three types of roles in IAM:

Basic roles include the Owner, Editor, and Viewer roles. These roles include many permissions across all Google Cloud services. Do not grant these roles by default in production environments. Instead, grant the most limited predefined or custom roles that meet your needs.

Predefined roles, which provide granular access to a specific resource, and are managed by Google Cloud.

Custom roles, which provide granular access according to a user-specified list of permissions.

Default service account in Cloud Run



As previously mentioned, if you deploy a Cloud Run service and do not specify a service account, a default service account is used.

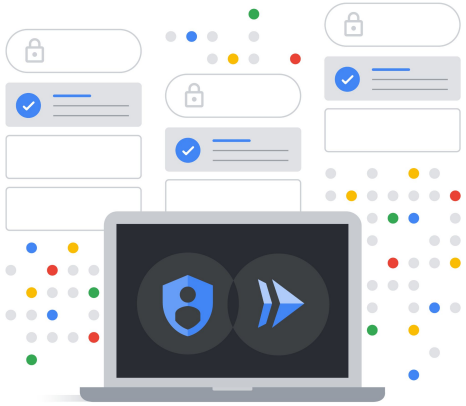
The default service account used is the Compute Engine service account which has the broad *Editor* role on the project.

Because of policy binding inheritance, the default service account has read and write permissions on most resources in your project.

While convenient, it's an inherent security risk as resources can be created, modified, or deleted with this service account.

Use the principle of least privilege

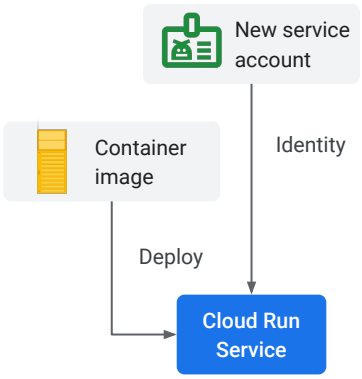
1. Create a new service account for a Cloud Run service.
2. Configure the service account as the Cloud Run service's identity.
3. Add policy bindings for the identity with predefined or custom roles to resources that your service needs to access.



To mitigate this security risk, you should:

1. Create a new service account for a Cloud Run service.
2. Configure the service account as the Cloud Run service's identity.
3. Add policy bindings for this identity with predefined or custom roles on resources that your service needs to access.

Create a new service account

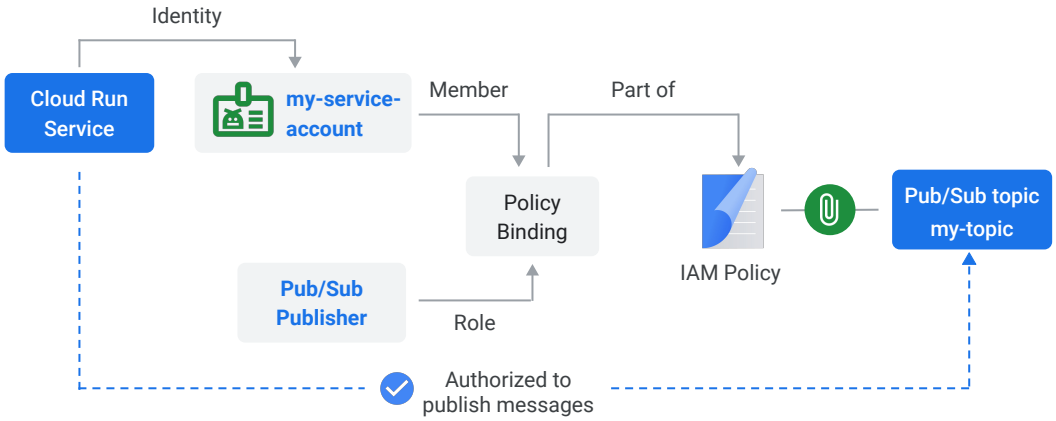


The first step is to create a new user-managed service account for a Cloud Run service, and set it as the service identity of the service.

You can create a service account in the Google Cloud console or with the gcloud CLI.

You can set the service account for a Cloud Run service when you create or update a service, and when you deploy a new service revision. This can be done in the Google Cloud console, the gcloud CLI, a YAML file, or with Terraform.

Add policy bindings with predefined roles




```
gcloud pubsub topics add-iam-policy-binding my-topic \
--member="my-service-account-email" --role="roles/pubsub.publisher"
```


By default, this service account does not have any permissions. You've just created it, and it doesn't appear in any policy binding.

If you call any Google Cloud API from code that runs as part of the Cloud Run service, the call will be rejected by IAM.

To grant the service account permissions, you add a policy binding with the appropriate role for the service account member, to the IAM policy that is attached to the required resource.

For example, to enable your Cloud Run service to publish a message to a Pub/Sub topic, add a policy binding with the role *Pub/Sub Publisher* to the IAM policy that's attached to the topic.

Remember

1. A Cloud Run service has access to a default service account.
2. Google client libraries use the default service account to call Google Cloud APIs.
3. The default service account has the Editor basic role, which has broad permissions across all services.
4. In production environments, you must replace the default service account with a user-managed per-service account with predefined roles.

In summary:

- A Cloud Run service has access to a default service account.
- Google client libraries use the default service account to call Google Cloud APIs.
- The default service account has the Editor basic role, which has broad permissions across all services.
- In production environments, you must replace the default service account with a user-managed per-service account with predefined roles.