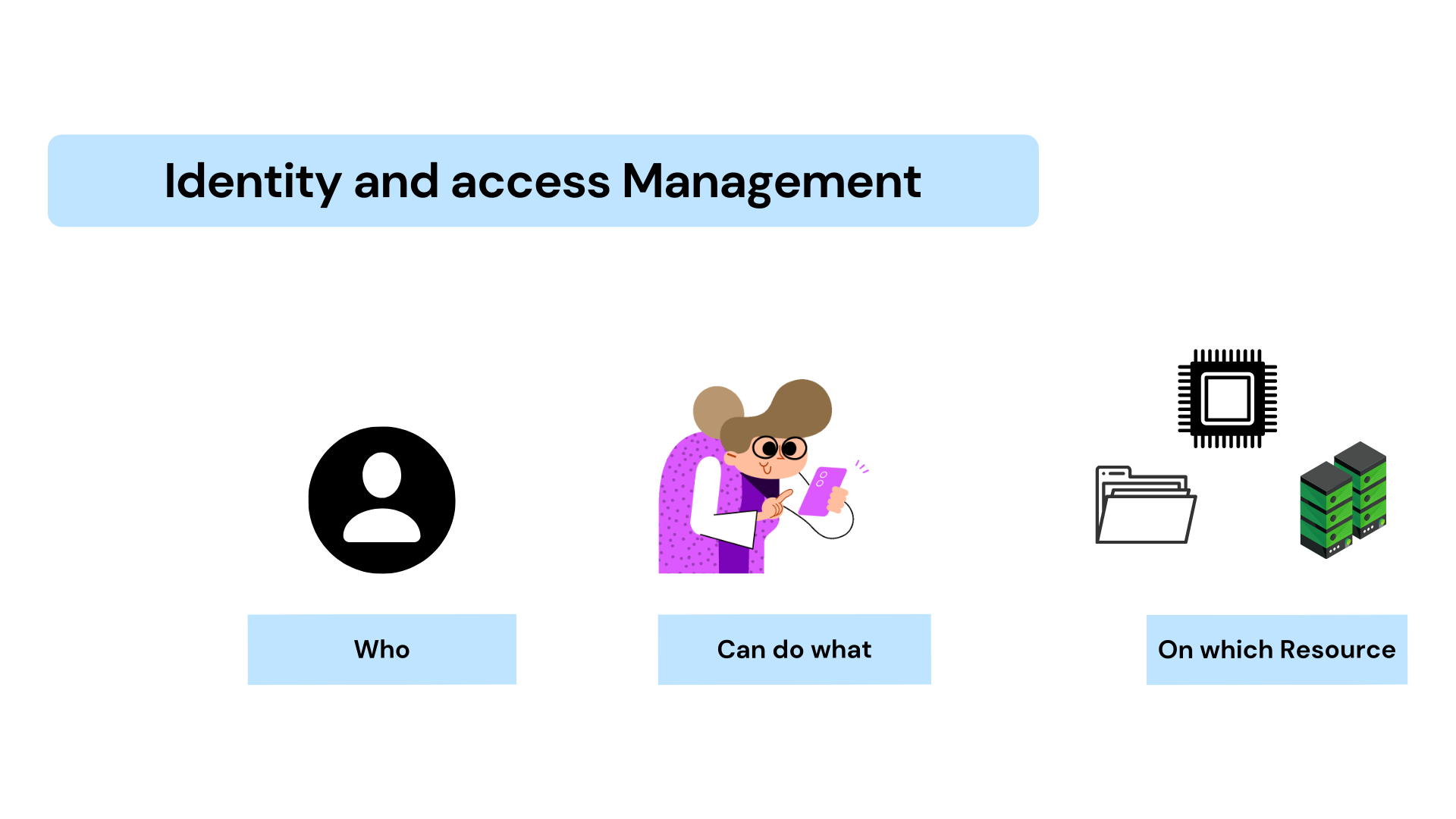
**Creating Custom Roles**

**What Is IAM?**

(Identity and Access Management) allows project administrators to specify who has permission to act on certain resources, providing the full control over the Google cloud services.

**IAM lets you manage access control by defining who can do what on which resources.**

Google has divided this into three pillars: **who, what and which resources.**

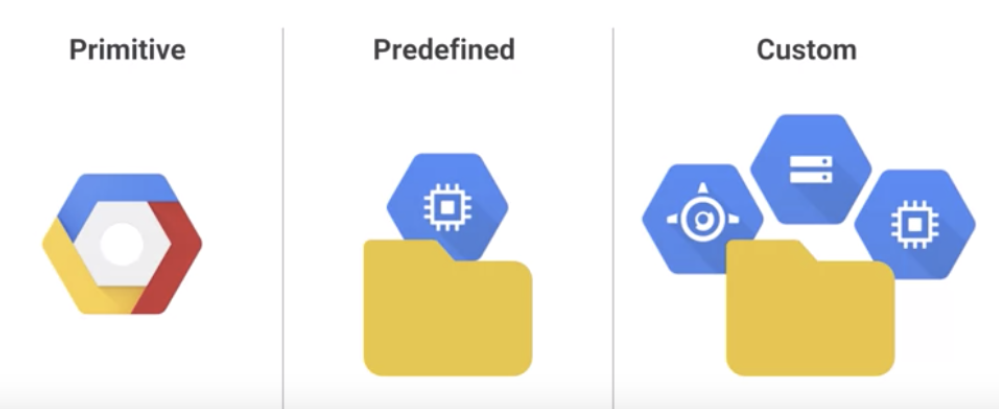


**Who:**

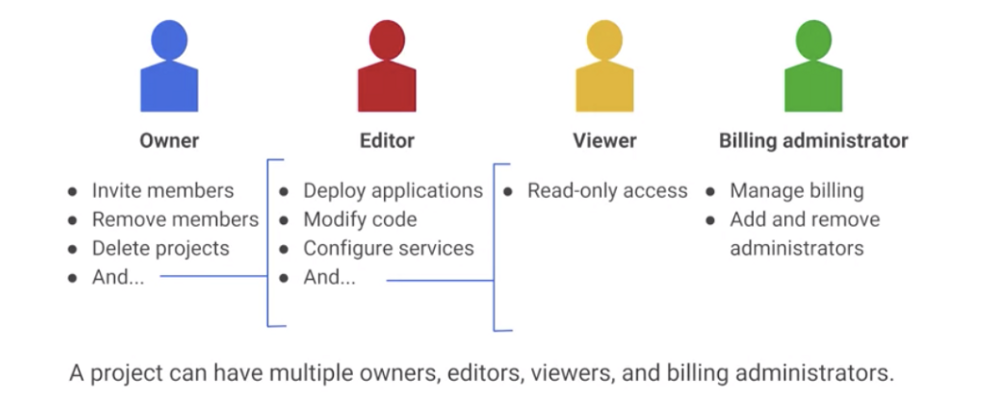
The “*Who”* pillar is defined as members or users. These identities are set up outside of IAM in the Google Cloud console. It can be found by going to admin.google.com.

**What:**

The *“What”* is determined by an IAM role. There are collections of permission, which are grouped in a role. You do not directly permit access to users.



* **Primitive Roles:** "Owner", "Editor" and "Viewer", are managed roles that existed prior to the introduction of Cloud IAM. These roles are concentric, where the viewer role is designed for viewing the resources but cannot make any changes. Editor role for modifying the resources.
* **Predefined Roles:** Predefined roles are roles created and maintained by Google, that provide granular access to specific Google Cloud Platform (GCP) resources and deny unwanted access to other resources.
* **Custom Roles:** Custom roles are user-defined roles that allow you to bundle one or more supported permissions to meet your specific needs. They are not maintained by Google or updated automatically. These roles are designed to be taken care of by yourself or your organization.

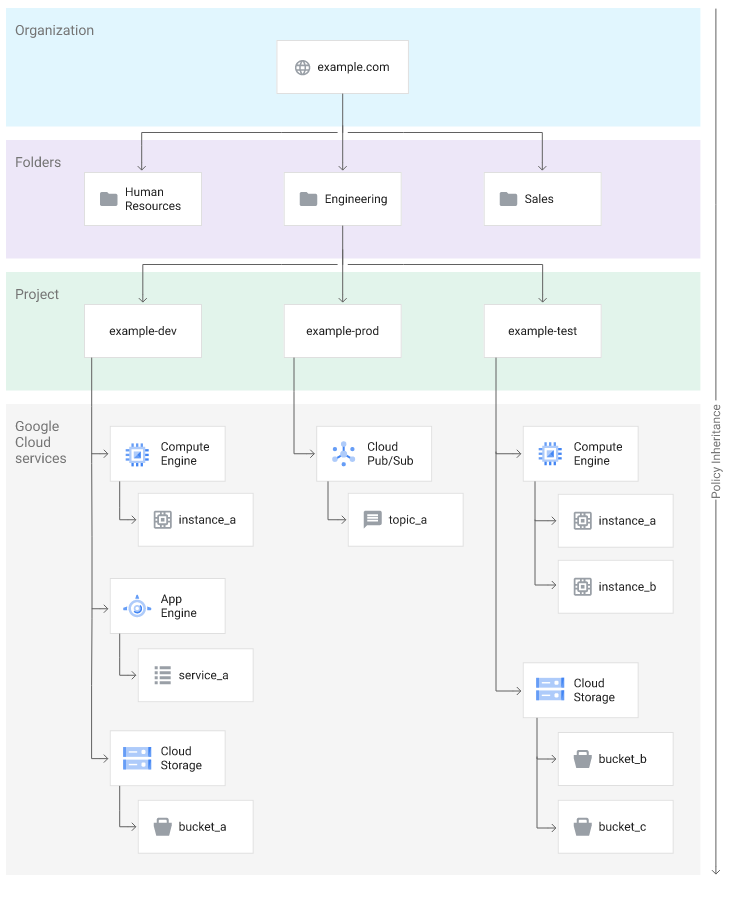


**Which Resources:**

*“Which”* resources refer to the various components of GCP. If a user needs access to a specific Google Cloud resource, you can grant the user a role for that resource. Some examples of resources are organizations, folders, projects, Compute Engine instances, and Cloud Storage buckets. **Policies** are needed to grant roles.

**Policies:**

You can set an allow policy at any level in the resource hierarchy: the organization level, the folder level, the project level, or the resource level. Resources inherit the allowed policies of all of their parent resources. The effective allow policy for a resource is the union of the allow policy set on that resource and the allow policies inherited from higher up in the hierarchy.



Google Cloud resource hierarchy.

**Creating Custom Roles:**

1. Once you first log in, your screen should look similar to this.



1. Click on the project selector drop-down menu at the top of the screen.



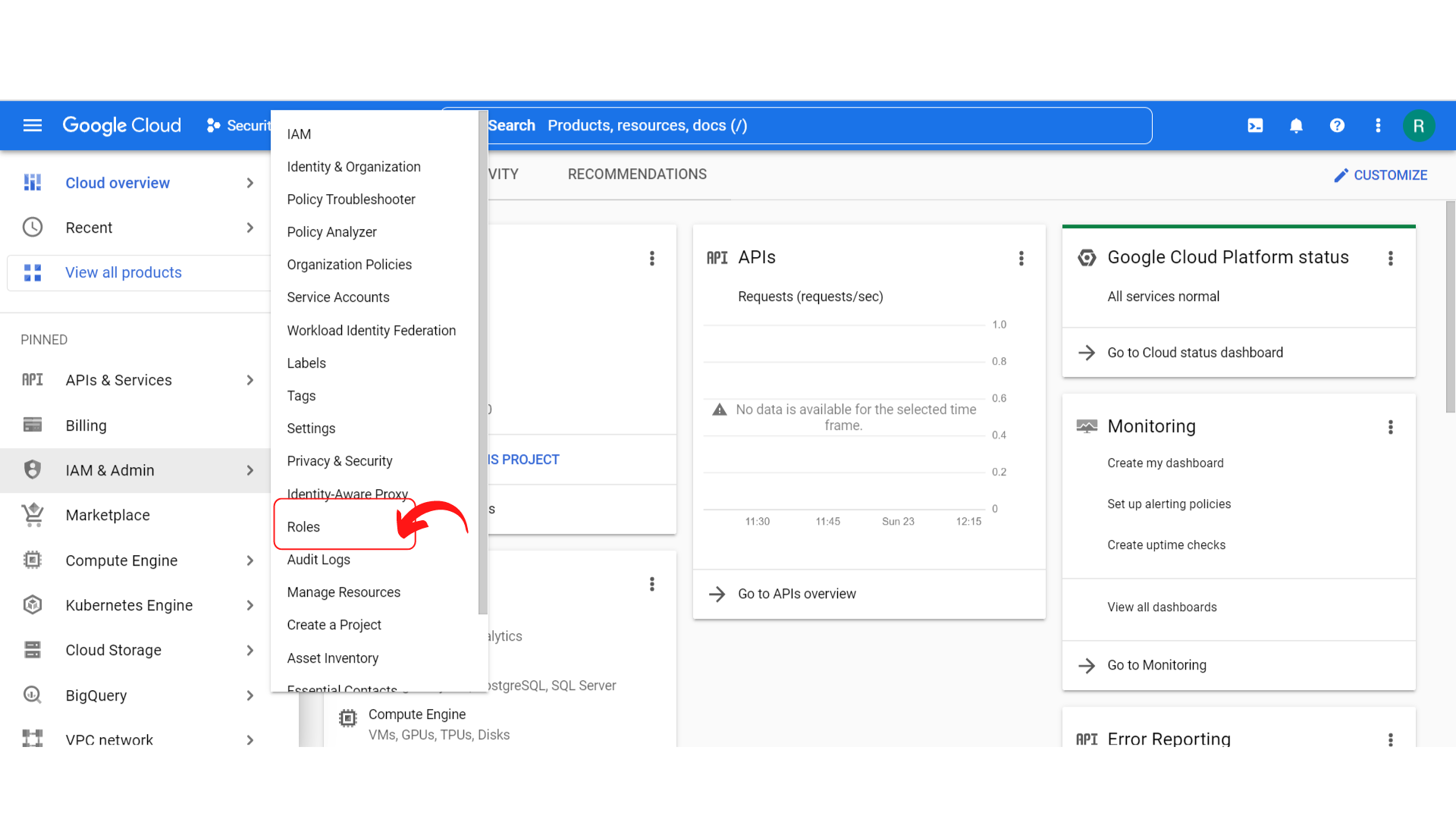
1. Since, we are doing labs on a Security Labs project, Click on *“Security Labs”*.



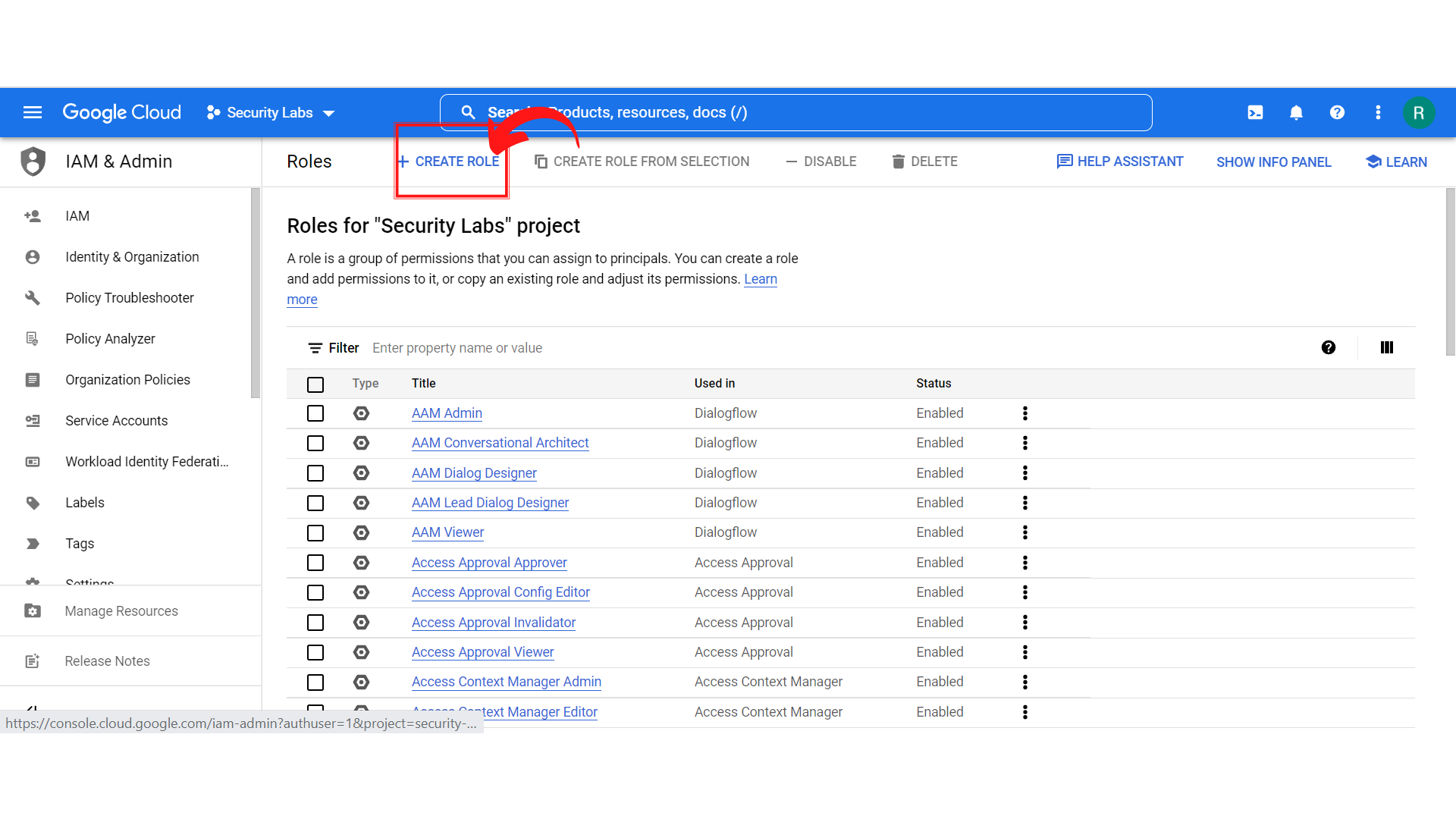
1. Your screen should look similar to this with project info changed to “*Security Labs”* project.



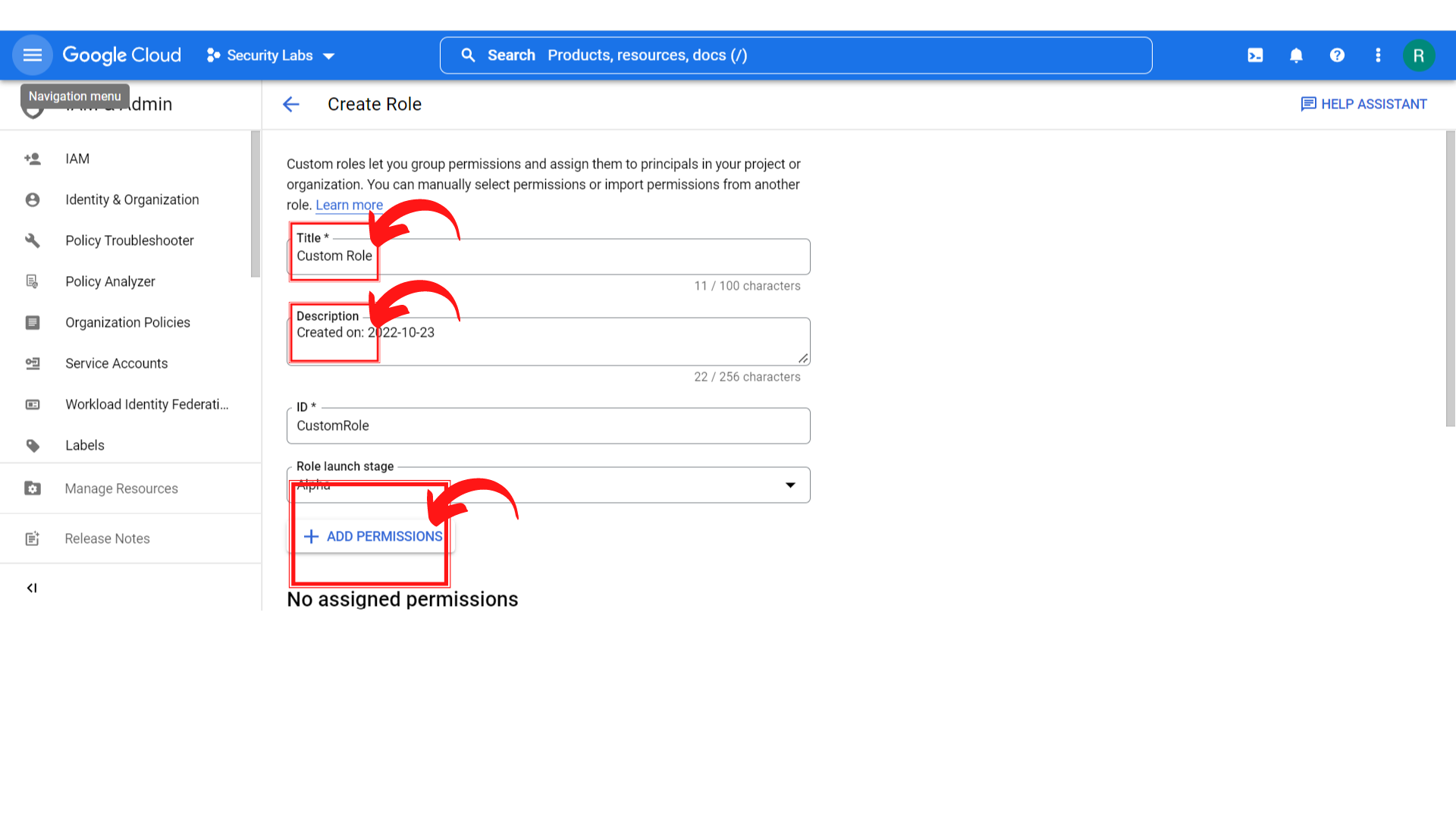
1. To create a new service account, click on “*IAM & Admin → Roles”.*



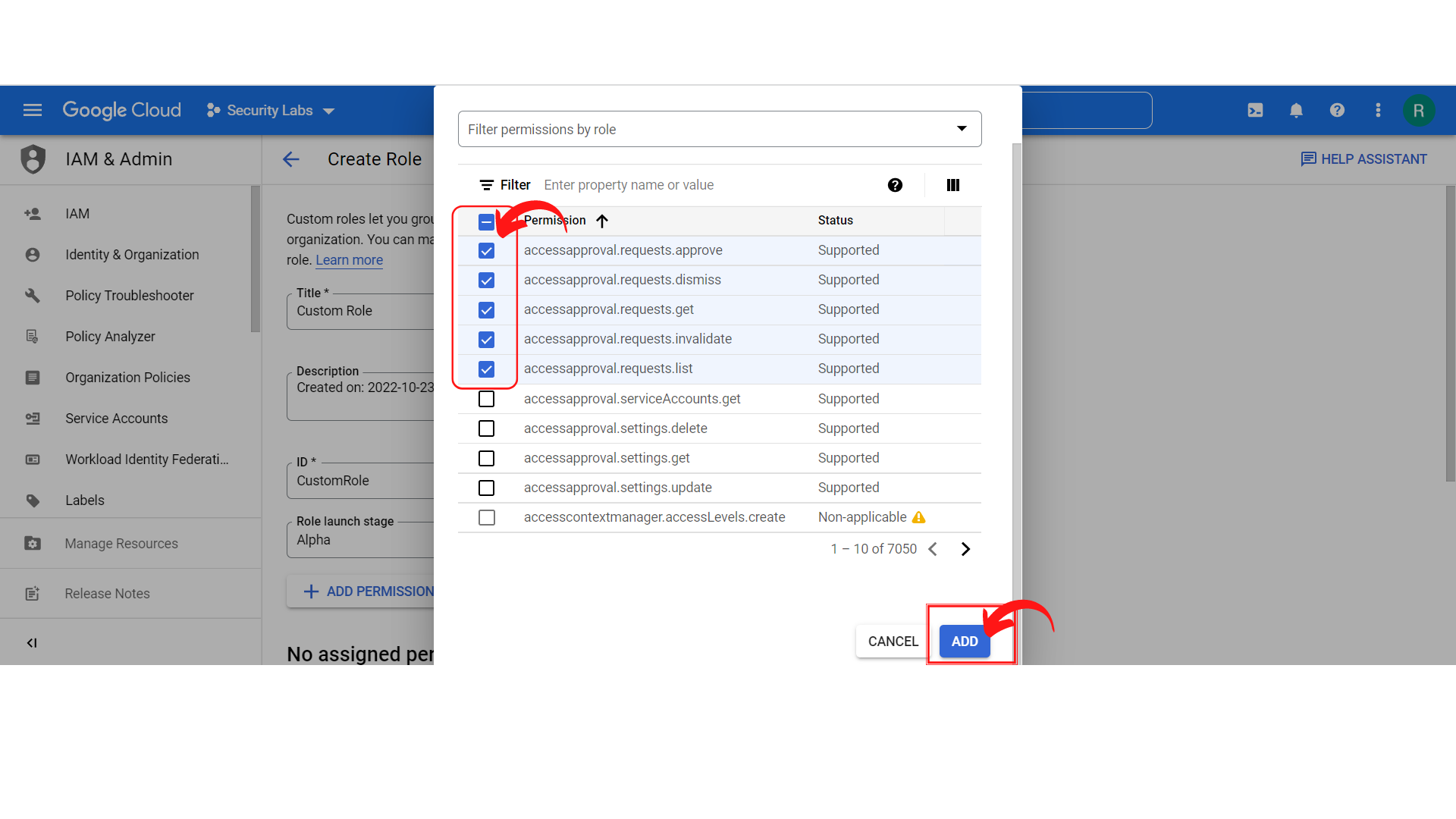
1. Your screen should look similar to this and click on *“Create Role”.*



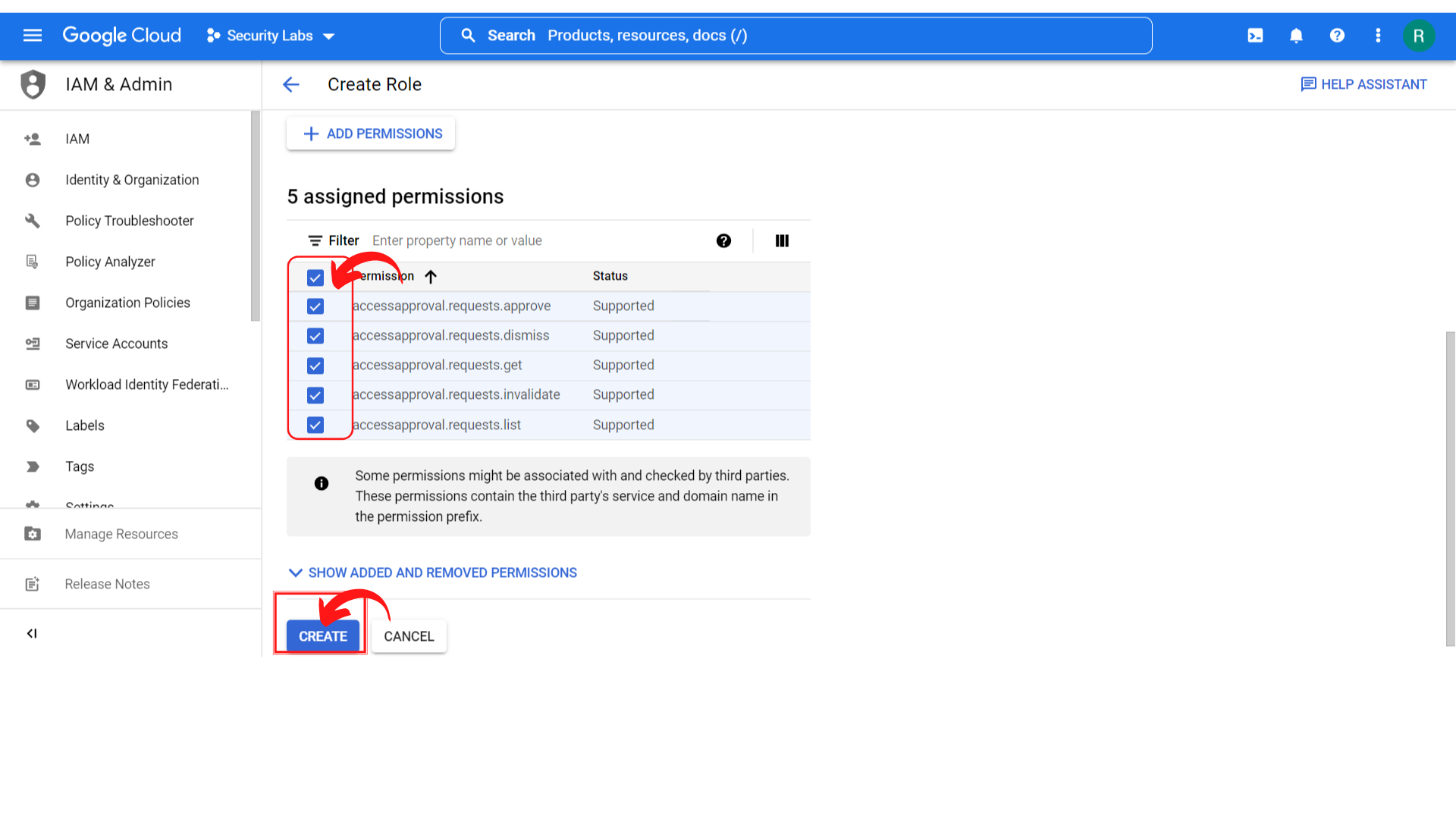
1. Your screen should look similar to this and fill the “*Title(custom Role) and Description”* and click on “*Add permissions”* Button.



1. Your screen should look similar to this and add whatever permissions you want as per your project *by ticking the permissions* and clicking on *“Add”.*



1. Your screen should look similar to this once you add a permissions list and then click on *“Create”.*



1. Your screen should look like this and you have successfully created a custom role.

