

GCP Network Engineer Crash Course Lab 3

IAM

Create a New role with conditions and review Analyzed Permissions on other accounts.

Log in to your Google Cloud Platform Account

- Determine the project you will be creating credentials in.
- Click the IAM & Admin link in the left-hand navigation bar and select IAM from the context menu.
- Your IAM console should look similar to the one shown in

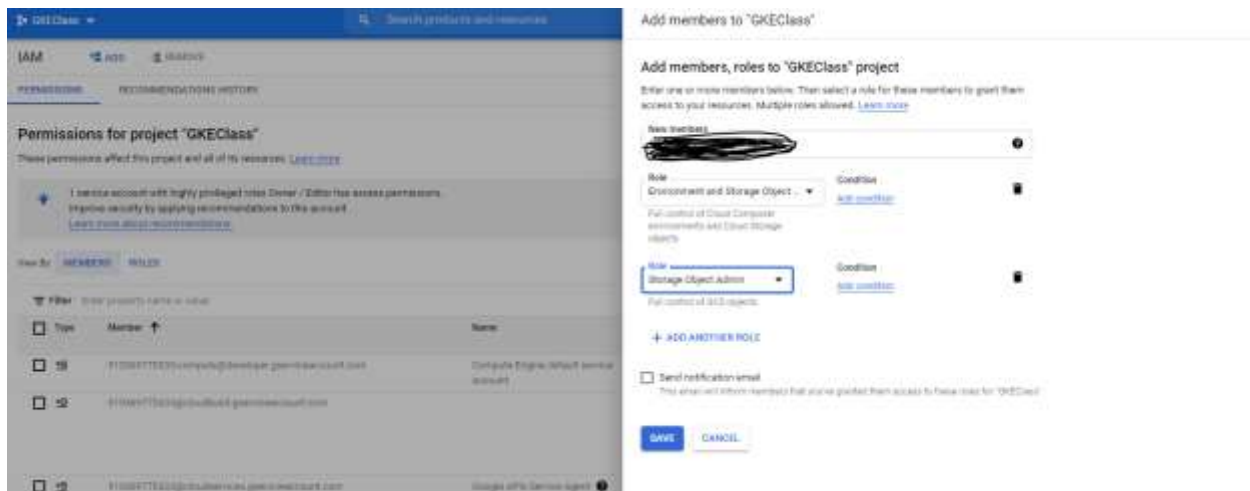
Figure 1 - IAM

The screenshot shows the Google Cloud IAM console for project 'GKEClass'. The left sidebar contains navigation links: Home, Identity & Organization, Policy Troubleshooter, Policy Analyzer, Organization Policies, Service Accounts, Android Identity Packager, Labels, Tags, Settings, Privacy & Security, Security Domain Proxy, Roles, Audit Logs, and Account Overview. The main content area is titled 'Permissions for project "GKEClass"' and includes a note: 'These permissions affect this project and all of its resources.' Below this, a message states: '1 service account with highly privileged roles Owner / Editor has explicit permissions, requires security for applying recommendations in this account.' A link 'View recommended roles in table' is provided. The 'View by' section shows 'Individuals' selected. A checkbox 'Include Google-provided role grants' is present. The table below lists the permissions:

Type	Member	Name	Role	Quota	Permissions	Service	Condition
Service Account	gcp-sa-gke@project-gkeclass.iam.gserviceaccount.com	Google Engine default service account	Editor	4096	gcp-engine-admin	Cloud Build service account	
Service Account	gcp-sa-gke@project-gkeclass.iam.gserviceaccount.com	Google Engine default service account	Editor	4096	gcp-engine-admin	Cloud Build service account	
Service Account	gcp-sa-gke@project-gkeclass.iam.gserviceaccount.com	Google Engine default service account	Editor	4096	gcp-engine-admin	Cloud Build service account	
Service Account	gcp-sa-gke@project-gkeclass.iam.gserviceaccount.com	Google Engine default service account	Editor	4096	gcp-engine-admin	Cloud Build service account	
Service Account	gcp-sa-gke@project-gkeclass.iam.gserviceaccount.com	Google Engine default service account	Editor	4096	gcp-engine-admin	Cloud Build service account	

Create a new set of IAM credentials and to set the accompanying role, click the “Add button”.

In **Figure 2**, the next screen will ask you to enter a member email address and then select a role(s). Take the liberty to select whatever



Before saving the role select the “Condition Builder” for a role and enter specific times for usage.

We want to limit login access to only 6am EST to 5PM EST.

Add a Title - Work Hours.

Select Condition Type. Time > Schedule > Day of Week > After 6 (6AM)

Select Condition Type. Time > Schedule > Day of Week > Before 17 (5PM)

Figure 3 – Condition Builder Menu Selecting the Condition Type

Edit condition

 DELETE

Resource

Title

Work Hours

Description

CONDITION BUILDER

CONDITION EDITOR

Condition type

X

ADD

Select condition type

Resource

Schedule

Expiring Access

Day of Week

Hour of Day

SAVE

CANCEL

Figure 4 - Enter Hour of Day and Time Zone here.

Edit condition

 DELETE

Resource

Title

Description

CONDITION BUILDER

CONDITION EDITOR

AND

OR

Condition type

Hour of Day

Operator

After

Hour of Day *

6

Choose a time zone

Eastern Daylight Time

Condition type

Hour of Day

Operator

Before

Hour of Day *

17

Choose a time zone

Eastern Daylight Time

ADD

SAVE

CANCEL

Now you can save the Condition.



When you are satisfied with the roles you have designated for a particular member, click the Save button to complete the process.

When you review the IAM console page, shown in **Figure 5**, you will see that a new or revised member, with a new role, has been added to the list.

You should also review the “Analyzed Permissions”. Note the new role will take a 90 days to update but for the exercise review other roles to see results for an idea of what the results are.

Analyzed permissions list the excess permissions not needed for this member. This was determined by analyzing 90 days of permissions utilization data using machine learning. Use the link to view the recommendation.



<input checked="" type="checkbox"/>				Environment and Storage Object Administrator Storage Object Admin	
<input type="checkbox"/>		fr-app-cs@gke/ass1.iam.gserviceaccount.com	HR App SA	App Engine Viewer	 11/11
<input type="checkbox"/>				BigQuery Data Viewer Datastore Engine Cluster Admin Storage Object Creator	 15/15  9/9  5/5

END