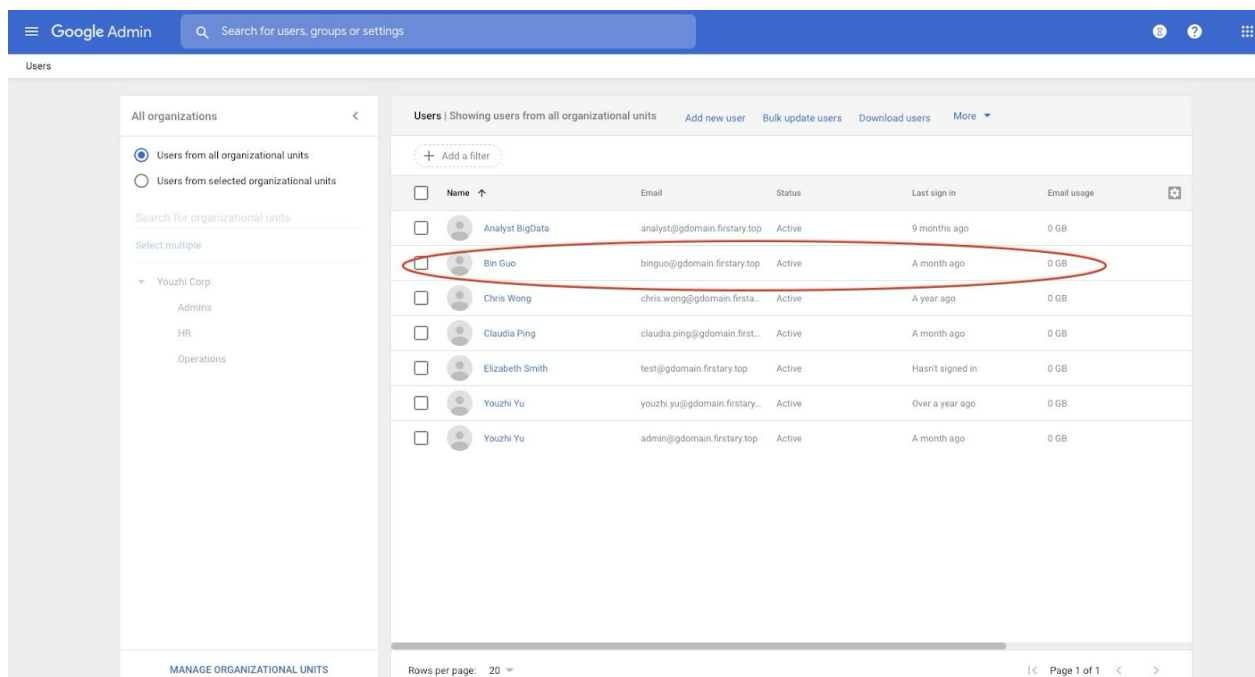


创建GCP组织管理员

Author: eugeneyu@google.com

本文指导如何创建一个GCP组织管理员，让其职能管理GCP的组织资源和配置，而无法操作Cloud Identity或者G Suite中的组织资源和配置，从而做到G Suite和GCP的组织管理权限隔离。

用Cloud Identity或者G Suite的Organization Admin管理员，比如admin@gdomain.firstary.top登录Google Admin Console，创建要成为GCP组织管理员的组织用户，比如binguo@gdomain.firstary.top。



然后用admin@gdomain.firstary.top登录GCP控制台，在项目下拉表选择组织，然后到IAM界面添加GCP组织管理员用户binguo@gdomain.firstary.top，并给予其Organization Admin角色。

打开项目选择下拉列表。

Google Cloud Platform

youzhi-lab

IAM & Admin

IAM

Identity & Organization

Policy Troubleshooter

Organization Policies

Quotas

IAM

ADD

REMOVE

PERMISSIONS

RECOMMENDATIONS LOG

Permissions for project "youzhi-lab"

These permissions affect this project and all of its resources. [Learn more](#)

View By: MEMBERS ROLES

Filter table

选择组织。

Select from

GDOMAIN.FIRSTARY.TOP

NEW PROJECT

Search projects and folders

RECENT

ALL

Name	ID
✓ youzhi-lab ?	youzhi-lab
binguo-test-admin ?	binguo-test-admin
gdomain.firstary.top ?	882592888799
bin-lab ?	bin-lab-286702

CANCEL

OPEN

到IAM界面添加用户并给予组织管理员角色。

The screenshot shows the Google Cloud Platform IAM & Admin console. The left sidebar lists various IAM-related tools. The main content area is titled 'Permissions for organization "gdomain.firstary.top"'. Below this, there's a 'View By' section with 'MEMBERS' and 'ROLES' tabs. The 'MEMBERS' tab is active, showing a table of current members. To the right, a modal window titled 'Add members to "gdomain.firstary.top"' is open. It prompts the user to 'Add members, roles to "gdomain.firstary.top" organization' and provides a search bar for 'New members'. A role of 'Organization Administrator' is selected, and a 'Condition' is set to 'Add condition'. There are buttons for '+ ADD ANOTHER ROLE', 'SEND notification email', 'SAVE', and 'CANCEL'.

Type	Member
<input type="checkbox"/>	247839977271-compute@developer.gserviceaccount.com
<input type="checkbox"/>	admin@gdomain.firstary.top

Type	Member
<input type="checkbox"/>	eugeneyu@google.com
<input type="checkbox"/>	gdomain.firstary.top
<input type="checkbox"/>	service-org-88259288799@security-center-api.iam.gserviceaccount.com

然后用新添加的GCP组织管理员binguo@gdomain.firstary.top身份登录GCP控制台，打开组织管理页面，确认可以进入，也可以尝试在组织下创建项目等操作，确认有相应权限。

The screenshot shows the Google Cloud Platform IAM & Admin console. The left sidebar lists various IAM-related tools. The main content area is titled 'Permissions for organization "gdomain.firstary.top"'. Below this, there's a 'View By' section with 'MEMBERS' and 'ROLES' tabs. The 'MEMBERS' tab is active, showing a table of current members. To the right, a modal window titled 'Add members to "gdomain.firstary.top"' is open. It prompts the user to 'Add members, roles to "gdomain.firstary.top" organization' and provides a search bar for 'New members'. A role of 'Organization Administrator' is selected, and a 'Condition' is set to 'Add condition'. There are buttons for '+ ADD ANOTHER ROLE', 'SEND notification email', 'SAVE', and 'CANCEL'.

Type	Member	Name	Role	Inheritance
<input type="checkbox"/>	247839977271-compute@developer.gserviceaccount.com	Compute Engine default service account	Access Context Manager Admin	
<input type="checkbox"/>	admin@gdomain.firstary.top	Youzhi Yu	Access Context Manager Admin Access Context Manager Editor Access Context Manager Reader Support Account Administrator Compute Shared VPC Admin Organization Policy Administrator Owner Folder Admin Organization Administrator Organization Viewer Project Creator	
<input type="checkbox"/>	binguo@gdomain.firstary.top	Bin Guo	Organization Administrator	
<input type="checkbox"/>	eugeneyu@google.com		Viewer	
<input type="checkbox"/>	gdomain.firstary.top		Billing Account Creator Project Creator	
<input type="checkbox"/>	service-org-88259288799@security-center-api.iam.gserviceaccount.com		Security Center Service Agent	