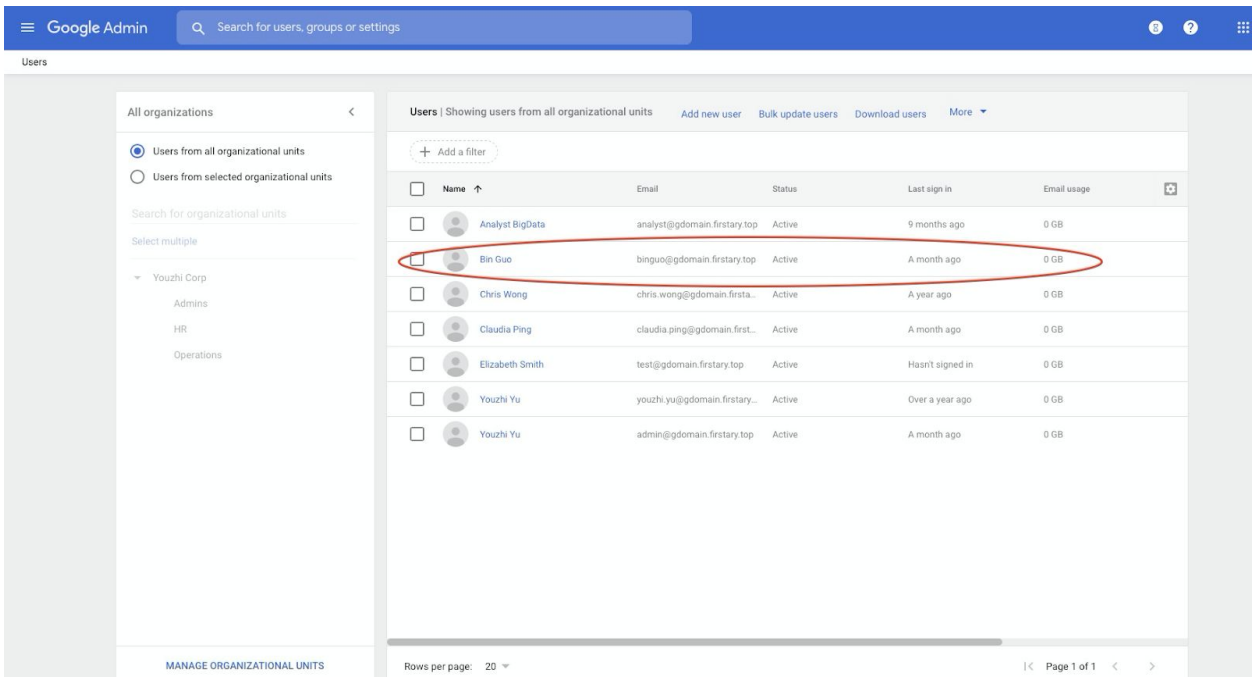
创建GCP组织管理员

Author: eugeneyu@google.com

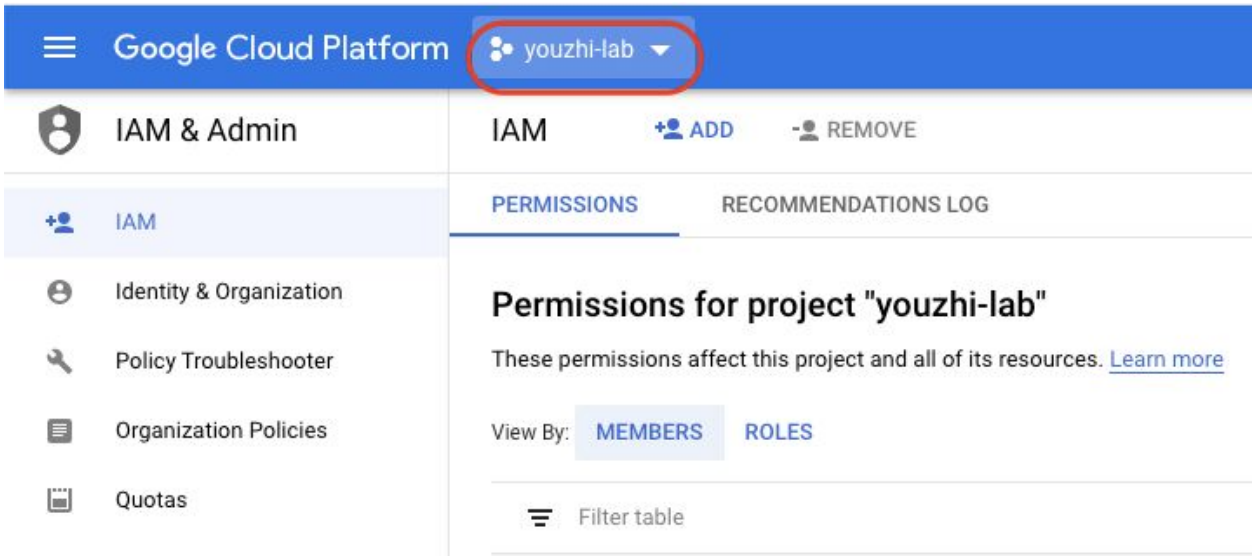
本文指导如何创建一个GCP组织管理员，让其职能管理GCP的组织资源和配置，而无法操作Cloud Identity或者G Suite中的组织资源和配置，从而做到G Suite和GCP的组织管理权限隔离。

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。

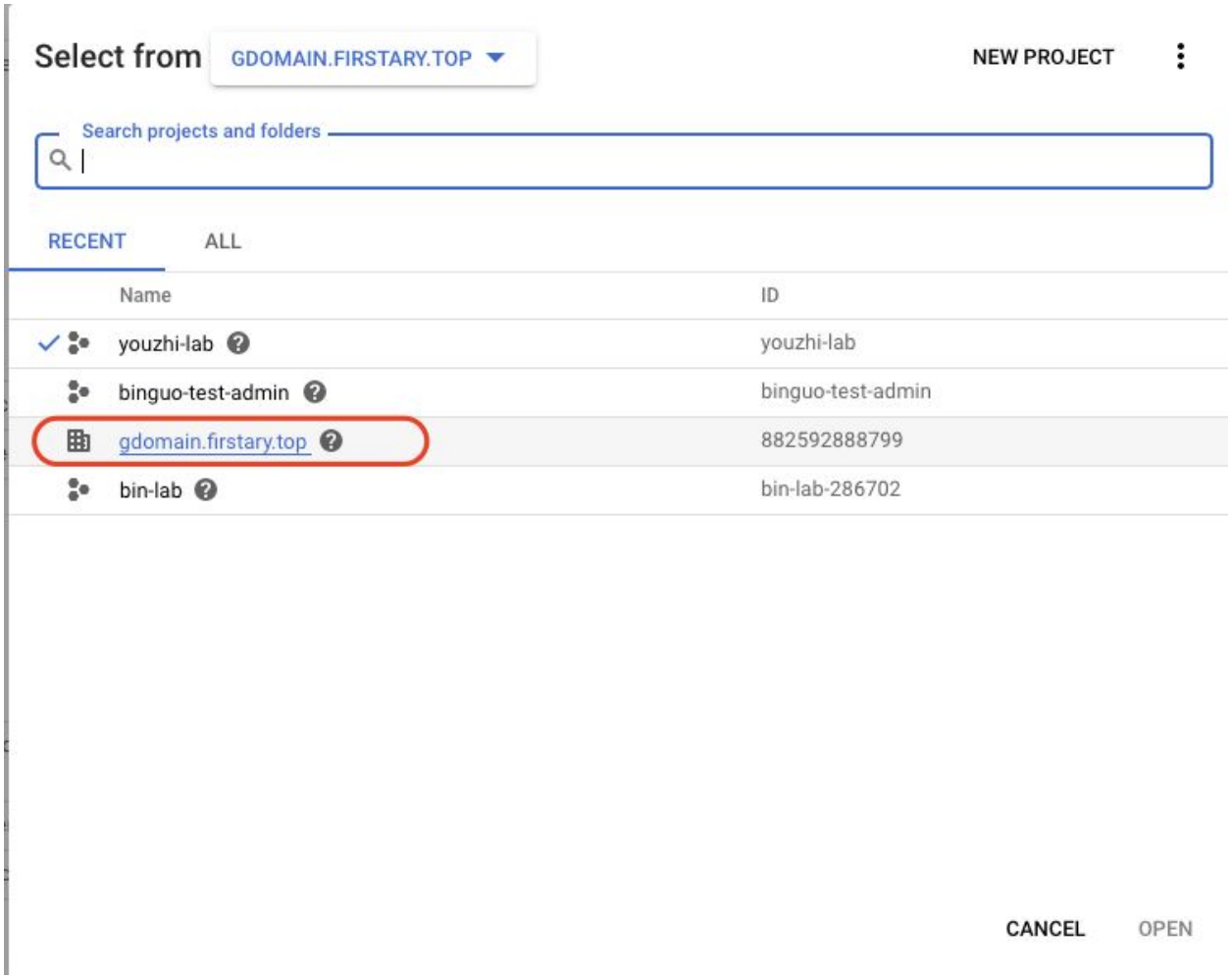


然后用admin@gdomain.firstary.top登录GCP控制台，在项目下拉表选择组织，然后到IAM界面添加GCP组织管理员用户binguo@gdomain.firstary.top，并给予其Organization Admin角色。

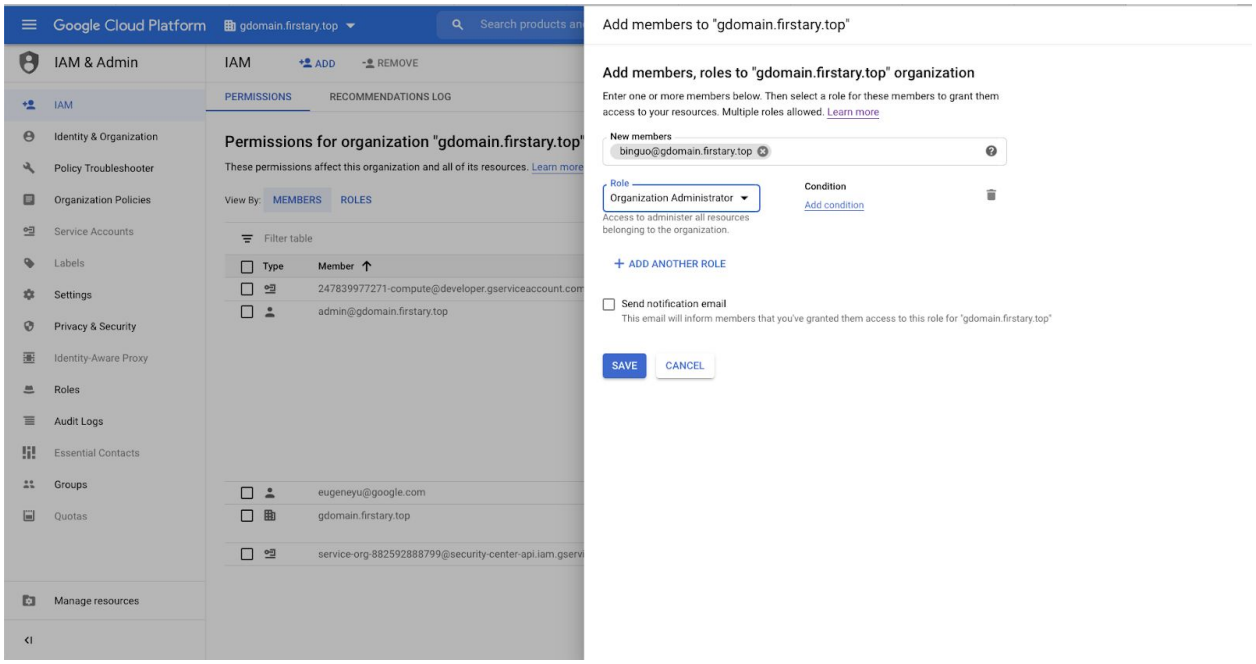
打开项目选择下拉列表。


Google Cloud Platform
youzhi-lab
IAM & Admin
IAM
ADD
REMOVE
IAM
Identity & Organization
Policy Troubleshooter
Organization Policies
Quotas
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。



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。