

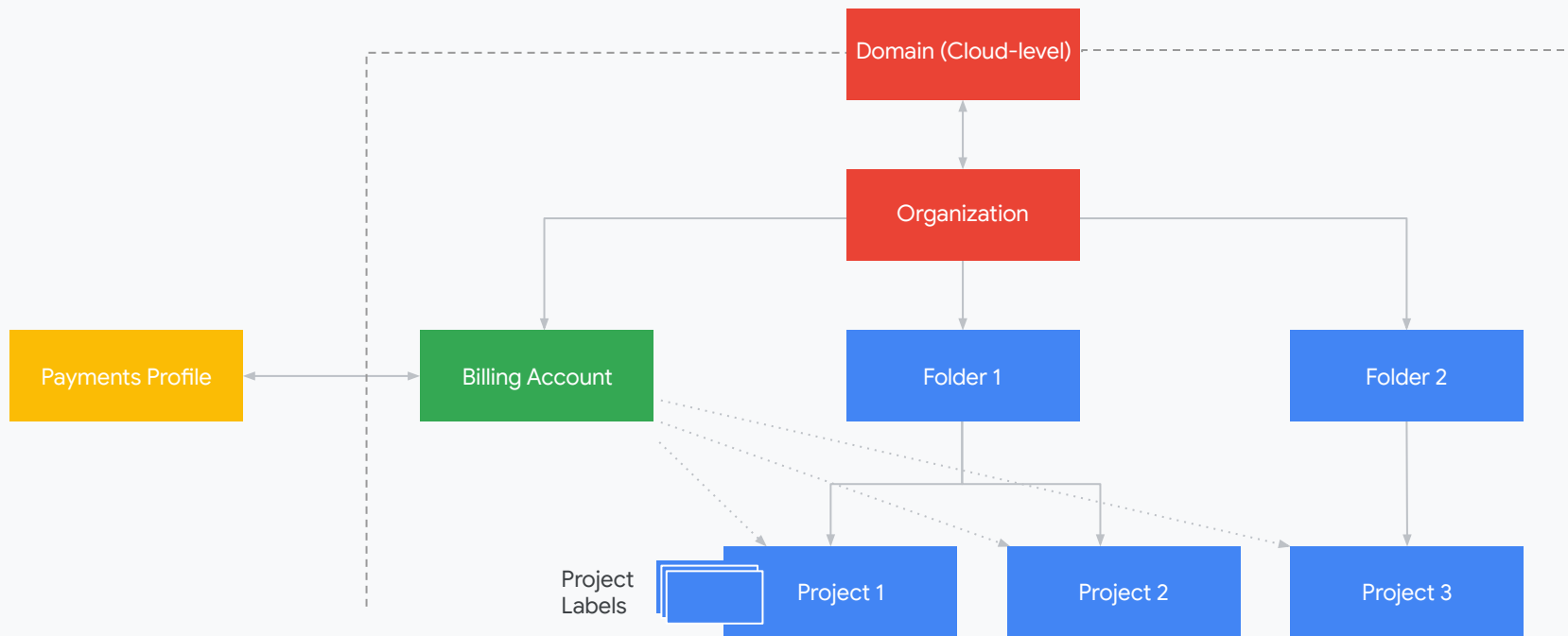
通过Cloud Identity创建 Organization

liuchenggang@google.com

资源组织管理层次结构

Key

- Owns
- Pays for
- - - - Cloud Resources



为什么要使用Organization？

- 支持资源的层次化结构：Org、Folder、Project、GCE/BQ...
- 支持Shared VPC
- 灵活的IAM: 通过层次化结构实现Permission的继承
- 统一管理Google Identity：使用企业email id代替个人gmail，实现基于Group的权限控制
- Organization Policy：常见的比如限制外网地址、限制嵌套虚拟化等
- 基于层次化资源的Firewall(Alpha)
- 创建Role Based Technical Support

前提条件

1. 拥有一个域名并且是域名的管理员：需要权限设置必要的DNS记录
2. 已经开通了一个GCP账号：通常是一个个人的gmail邮箱

Step 1

创建CloudIdentity

1. 通过GCP创建Organization

The screenshot displays the Google Cloud IAM & Admin console interface. On the left, a sidebar menu lists various administrative tools. The 'Identity & Organization' option is highlighted in blue. A red arrow points from the top of the sidebar to the 'IAM & admin' header, and another red arrow points from the 'Identity & Organization' menu item to the main content area. The main content area is titled 'Identity' and contains a card with information about Cloud Identity. A third red arrow points from the bottom of the main content area to the 'Sign up' button.

IAM & admin

Identity

IAM

Identity & Organization

Troubleshooter

Organization policies

Quotas

Service accounts

Labels

Settings

Privacy & Security

Cryptographic keys

Identity-Aware Proxy

Roles

Audit Logs

IAM & Admin

Identity

Cloud Identity will allow you to manage your enterprise identities and cloud resources on Google Cloud Platform. [Learn more](#)

What to expect

- You will sign up your enterprise for Cloud Identity
- You will agree to the Cloud Identity terms of service
- You will verify your domain
- You will configure Google Cloud Platform & import any existing projects and billing accounts
- You will create or sync accounts for all your users

Sign up

按照向导创建CloudIdentity的免费账号



Cloud Identity

一个简单的集成式解决方案，提供用户生命周期管理、目录服务、帐号安全、单点登录、设备管理和更多其他服务。**立即设置免费帐号。**

我们将一步步指导您为您的企业创建 Cloud Identity 帐号。

[下一页](#)

填写公司域名

您公司的域名是什么？

我们稍后会指导您验证贵企业对此域名的所有权。 



您的域名

goodvm.club

例如 example.com


下一页

在DNS服务提供商上设置MX记录做域名验证

MX	@	mxbiz1.qq.com（優先順序： 5）	1 小時	
<div>MX mx</div>	@	mxbiz2.qq.com（優先順序： 10）	1 小時	

设置CloudIdentity账号管理员:邮箱、密码

您叫什么名字?

您是帐号创建者, 因此将成为此帐号的管理员。请放心, 您稍后可以将此角色分配给其他人。 

姓氏

Liu

名字


C

管理员是指负责管理您企业的 Cloud Identity 的人。

管理员可以添加和移除用户、重置密码, 还能执行更多其他操作。

下一页

您将如何登录

您需要使用自己的用户名, 才能管理您的 Cloud Identity 用户。此帐号也会作为管理 Google Cloud Platform 用户的管理员帐号。 

用户名

goodvm

@goodvm.club

密码

●●●●●●●●



请至少输入 8 个字符

下一页

创建成功后设置CloudIdentity, 验证Domain的所有权



设置 Cloud Identity

管理的身份、SSO、移动设备管理等等。



设置 Cloud Identity 帐号

您将能为自己的整个团队管理 Cloud Identity。



验证网域所有权

验证您是贵公司网域的所有者，并保护网域安全。

开始



为您的 Cloud Identity 帐号添加用户

为您的团队创建新的 Cloud Identity 帐号，以开始管理用户和群组。



验证网域所有权

我们需要先与您的域名托管服务商联系，确认域名 **goodvm.club** 归您所有，然后您才能通过该域名使用 Cloud Identity。这样做有助于确保他人无法在 Cloud Identity 中冒充您。 [了解详情](#)

您的域名通过验证后，请为您自己和您的用户设置 Google 云端平台。

我们检测到 **goodvm.club** 由 **GoDaddy.com** 托管。如果您遇到了问题，可以尝试[点击此处验证网域](#)。

验证域名



需要帮助？请搜索 [帮助中心](#)

点击验证域名后，会自动定向到godaddy进行相应的操作

记录设定

GoDaddy® | 域名管理器



确认访问



单击**授权**允许 google.com 代表您更改 goodvm.club。

授权

取消

自动添加验证信息后进行域名验证

设置 Cloud Identity

管理的身份、SSO、移动设备管理等等。



设置 Cloud Identity 帐号

您将能为自己的整个团队管理 Cloud Identity。



验证网域所有权

正在验证域名...

大约还需 3 分钟...

域名托管服务商可能需要花些时间来更新您的信息。您随时可以返回此页面进行设置，只需访问

admin.google.com 并使用您的新 Cloud Identity 用户名 (goodvm@goodvm.club) 和密码登录即可。 [了解详情](#)



需要帮助？请搜索 [帮助中心](#)

NS	global	ns-165.awsdns-20.com	1 小时	
NS	global	ns-794.awsdns-35.net	1 小时	
SOA	@	主要域名服务器: ns21.domaincontrol.com.	1 小时	
TXT	@	google-site-verification=fOoX7LFjNC4CG...	1 小时	

可以自己登陆域名管理的后台，查看google自动添加的txt记录

如果自动添加不支持，也可以按照向导操作手动添加TXT记录



验证网域所有权

首先，请验证您对域名 **goodvm.club** 的所有权，然后您可以为自己和您的用户设置 Google 云端平台。[了解详情](#)



我已成功登录。



我已打开我网域的控制台。

向您的网域添加新的 TXT 记录。

TXT 记录是您网域的简单文字说明，不会影响您的电子邮件或网站。如果您的域名托管服务商不允许您添加 TXT 记录，您可以改为添加 [CNAME 记录](#)。

复制下面的值，并将其粘贴到您刚刚打开的页面上的“TXT 记录”部分。我们会通过查找此记录来验证您是否拥有该网域。

名称/主机/别名

@

值/应答/目标

google-site-verification=fOoX7LF-jNC4CGIfjoBliHuy2MFdnq6cy2WKqUnLCkk



我已添加 TXT 验证记录。

保存 TXT 记录并验证。



验证网域所有权

已完成域名验证！

您已成功验证自己的域名。接下来，我们会为您创建第一批用户。

创建用户



需要帮助？请搜索 [帮助中心](#)

确认用户添加后返回GCP, 完成CloudIdentity创建, 可以使用cloudIdentity管理员账号登陆admin.google.com



C, 欢迎您!

为goodvm.club接受 Google Cloud Platform (GCP) 服务条款, 以完成 Cloud Identity 的设置。

服务条款

☒ 我同意 [Google Cloud Platform 服务条款](#) 以及 [任何适用服务和 API 的服务条款](#)。

所在国家/地区

中国

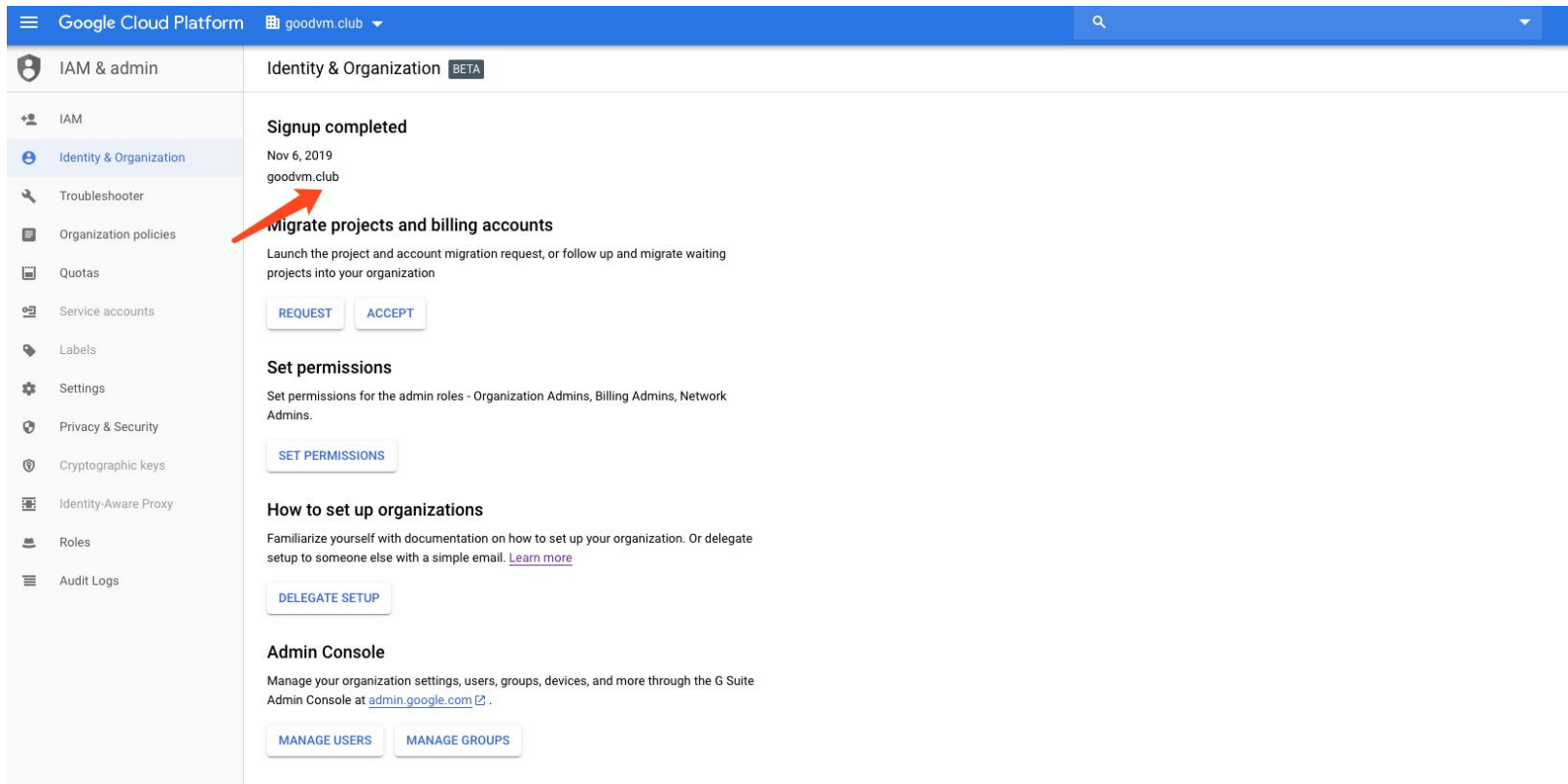
我希望定期收到来自 Google Cloud 和 Google Cloud 合作伙伴的电子邮件, 了解最新资讯、产品动态和特别优惠。

☐ 是 ☒ 否

同意并继续



确认Org已经创建完成



The screenshot displays the Google Cloud Platform console interface. The top navigation bar shows 'Google Cloud Platform' and the organization name 'goodvm.club'. The left sidebar lists various management tools, with 'Identity & Organization' selected. The main content area is titled 'Identity & Organization BETA' and shows a 'Signup completed' message dated 'Nov 6, 2019' for the organization 'goodvm.club'. A red arrow points to the 'goodvm.club' text. Below this, the 'Migrate projects and billing accounts' section provides instructions to launch a migration request, with 'REQUEST' and 'ACCEPT' buttons. The 'Set permissions' section offers a 'SET PERMISSIONS' button. The 'How to set up organizations' section includes a 'DELEGATE SETUP' button. Finally, the 'Admin Console' section provides links to 'MANAGE USERS' and 'MANAGE GROUPS'.

Google Cloud Platform goodvm.club

IAM & admin Identity & Organization BETA

IAM

Identity & Organization

Troubleshooter

Organization policies

Quotas

Service accounts

Labels

Settings

Privacy & Security

Cryptographic keys

Identity-Aware Proxy

Roles

Audit Logs

Signup completed

Nov 6, 2019
goodvm.club

Migrate projects and billing accounts

Launch the project and account migration request, or follow up and migrate waiting projects into your organization

REQUEST ACCEPT

Set permissions

Set permissions for the admin roles - Organization Admins, Billing Admins, Network Admins.

SET PERMISSIONS

How to set up organizations

Familiarize yourself with documentation on how to set up your organization. Or delegate setup to someone else with a simple email. [Learn more](#)

DELEGATE SETUP

Admin Console

Manage your organization settings, users, groups, devices, and more through the G Suite Admin Console at admin.google.com.

MANAGE USERS MANAGE GROUPS

Step 2

项目迁移

迁移步骤

- 前3步使用非cloud identity账号操作
- 后3步使用cloud identity账号操作

Migrate projects and billing accounts and set permissions

Important:

- Complete steps 1–3 below from your non-administrator Google Cloud Platform account. This account is typically a personal Gmail account.
- Complete steps 4–6 from your Cloud Identity administrator account.

To migrate content from a previous account, follow these steps:

1. Grant access to billing accounts.
 2. Grant access to projects.
 3. Log in to your Cloud Identity account, and accept the project invitations.
 4. Go to GCP, log in with your Cloud Identity account, and remove access.
 5. Migrate projects.
 6. Set permissions.
-

1. 把cloud identity的admin添加为Billing Account Admin

Google Cloud Platform

Billing

Account management Liuchenggang-Second-BA RENAME BILLING ACCOUNT CLOSE BILLING ACCOUNT HIDE INFO PANEL

Billing account ID: 01BC27-459385-3C0FF5

Credits

\$2,349.81 Credits remaining Out of \$2,349.81

365 Days remaining Ends Nov 5, 2020

Projects linked to this billing account

Project name	Project ID
My First Project	wise-dispatcher-258207

PERMISSIONS

Add members

Search members

Filter by name or role

Billing Account Administrator (1 member) Authorized to see and manage all aspects of billing accounts.

Account management

1.把cloud identity的admin添加为Billing Account Admin

Add members to "Liuchenggang-Second-BA"

Add members and roles for "Liuchenggang-Second-BA" resource

Enter one or more members below. Then select a role for these members to grant them access to your resources. Multiple roles allowed. [Learn more](#)

New members

goodvm@goodvm.club ✕



Role

Billing Account Administr... ▼



Authorized to see and manage all aspects of billing accounts.

[+ ADD ANOTHER ROLE](#)

SAVE

CANCEL

2.把Org Admin添加为项目 owner

Add members to "My First Project"

Add members, roles to "My First Project" project

Enter one or more members below. Then select a role for these members to grant them access to your resources. Multiple roles allowed. [Learn more](#)

New members

goodvm@goodvm.club ✕



Role

Owner ▼



Full access to all resources.

[+ ADD ANOTHER ROLE](#)

SAVE

CANCEL

2.把Org Admin添加为项目 owner

Add members to "My First Project"

Add members, roles to "My First Project" project

Enter one or more members below. Then select a role for these members to grant them access to your resources. Multiple roles allowed. [Learn more](#)

New members

goodvm@goodvm.club ✕



Role

Owner ▼



Full access to all resources.

[+ ADD ANOTHER ROLE](#)

SAVE

CANCEL

3.Org Admin收到邮件后接受项目 Owner邀请

Join my project on Google Developers Console ☆

发件人: **liu chenggang** <noreply-cloud@google.com>

时 间: 2019年11月7日(星期四) 凌晨0:29

收件人: goodvm <goodvm@goodvm.club>

Hello, goodvm@goodvm.club,

I invite you to join the Google Developers Console project "My First Project" (id: wise-dispatcher-258207). Please click this link to accept my invitation:

<https://console.cloud.google.com/invitation?project=wise-dispatcher-258207&account=goodvm@goodvm.club&memberEmail=goodvm@goodvm.club>

Thanks,
liuchenggangsecond@gmail.com



Google Cloud Platform

Build your apps on Google's infrastructure.

4. 登陆Org Admin, 迁移项目

Google Cloud Platform

Manage resources [+ CREATE PROJECT](#) [MIGRATE](#) [DELETE](#)

NO ORGANIZATION Filter tree

<input checked="" type="checkbox"/>	Name	ID	Status	Charges	Labels	Actions
<input checked="" type="checkbox"/>	▼ No organization	0				⋮
<input checked="" type="checkbox"/>	My First Project	wise-dispatcher-258207				⋮

[0 RESOURCES PENDING DELETION](#)

IAM ——» Manage Resource -»

4. 登陆Org Admin, 迁移项目

Migrate project "My First Project"

Organization: ?

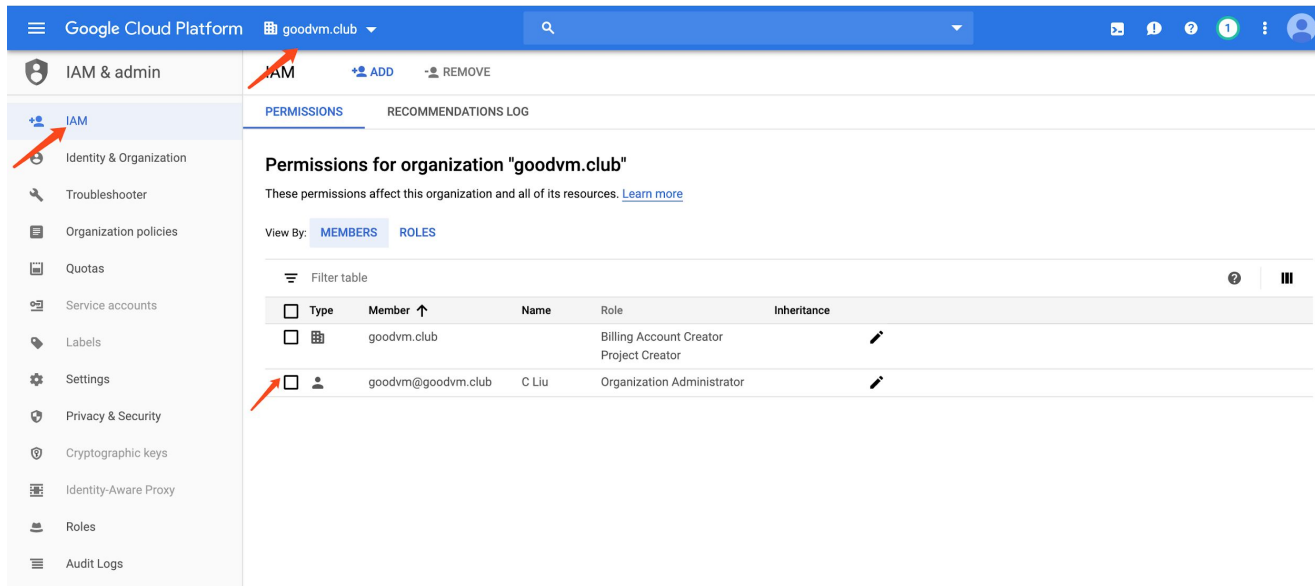
GOODVM.CLUB ▼

 Migrating a project will permanently attach that project to an organization. Projects cannot be detached from an organization once they are migrated.

CANCEL

MIGRATE

5. 登陆IAM, 设置Org内的权限



The screenshot shows the Google Cloud Platform IAM & admin console for the organization 'goodvm.club'. The left sidebar contains a navigation menu with the following items: IAM & admin, IAM, Identity & Organization, Troubleshooter, Organization policies, Quotas, Service accounts, Labels, Settings, Privacy & Security, Cryptographic keys, Identity-Aware Proxy, Roles, and Audit Logs. The 'IAM' item is highlighted with a red arrow. The main content area shows the 'Permissions for organization "goodvm.club"' page. It includes a 'PERMISSIONS' tab and a 'RECOMMENDATIONS LOG' tab. Below the tabs, there is a 'View By:' section with 'MEMBERS' and 'ROLES' options. A table lists the members of the organization. The table has columns for 'Type', 'Member', 'Name', 'Role', and 'Inheritance'. The first row shows 'goodvm.club' as a 'Billing Account Creator' and 'Project Creator'. The second row shows 'goodvm@goodvm.club' as an 'Organization Administrator'. A red arrow points to the 'goodvm@goodvm.club' row.

Type	Member	Name	Role	Inheritance
<input type="checkbox"/>	goodvm.club		Billing Account Creator Project Creator	
<input type="checkbox"/>	goodvm@goodvm.club	C Liu	Organization Administrator	

Tips: domain内的用户默认具有billing account creator和project creator的权限

可选：添加Organization Policy Admin Role,可以控制Org Policy

IAM [+ ADD](#) [- REMOVE](#)

[PERMISSIONS](#) [RECOMMENDATIONS LOG](#)


Permissions for organization "goodvm.club"

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

View By: [MEMBERS](#) [ROLES](#)

Filter table

<input type="checkbox"/>	Type	Member ↑	Name	Role	Inheritance
<input type="checkbox"/>	🏢	goodvm.club		Billing Account Creator Project Creator	✎
<input type="checkbox"/>	👤	goodvm@goodvm.club	C Liu	Organization Administrator	✎



Member: goodvm@goodvm.club Organization: goodvm.club

Role: Organization Administrator ▼

Access to administer all resources belonging to the organization.

Role: Organization policy

Organization Policy

[Organization Policy Administrator](#)

[Organization Policy Viewer](#)

[MANAGE ROLES](#)

