Tab 1

Overview

在AWS上创建Ubuntu虚拟机实例（新注册AWS的用户可以免费试用下面创建的虚拟机，为期十二个月，千万不要错过这白嫖的机会。）

https://docs.google.com/document/d/1l14Tykq97zU8P4rXSvV5c5aqQ5bpL_quvuexHI6_flw/edit?tab=t.0

AWS 是当前规模最大的云计算服务商，拥有广泛的个人与企业用户群体。不论是个人使用或是企业级需求，AWS 都是一个值得深入学习和投资的云计算平台。此文档详细描述了在 AWS 云平台上搭建 Ubuntu 虚拟机实例的步骤。用户将会学习如何注册 AWS 账号、进入 AWS 管理控制台、根据延迟选择距离最近的数据中心，随后利用 EC2 服务启动一台新的虚拟机实例，并生成用于服务器访问的密钥对。最终，为虚拟机创建并配置 postgres 用户。之后，用户便可以自由地编译和设置 PG 数据库。

250618更新：

1. 添加小节 “建立安全组”。描述了在AWS EC2中建立安全组的步骤。首先进入EC2控制台，点击“安全组”，然后点击“创建安全组”，接着添加规则并填写必要的信息，最后点击“创建安全组”完成安全组的创建。
2. 创建虚拟机时，选择相应的安全组，并且配置自定义的子网IP方便以后的管理和维护。
3. 添加小节 “配置安全组允许子网内部远程访问”。描述了如何在AWS EC2中配置安全组以允许子网内部的虚拟机之间进行远程访问。具体步骤包括进入EC2控制台，点击“安全组”，选择创建虚拟机时使用的安全组，编辑入站规则，添加规则以允许同一安全组内的虚拟机之间使用任意协议和端口进行通信，然后保存规则。文档还提到需要检查数据库虚拟机的数据库配置，确保允许远程访问，并在另一台位于同一安全组的虚拟机上尝试远程访问数据库以验证配置是否成功。

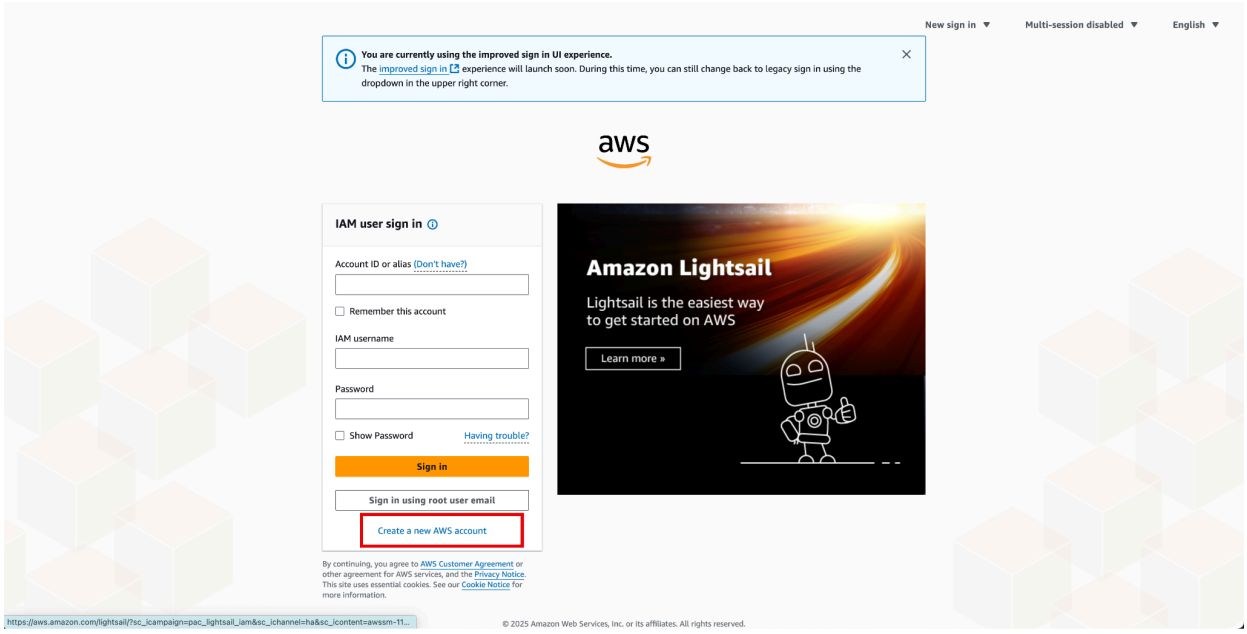
250619更新：

1. 安装和配置Postgres通常情况下有两种。一种是从源码编译安装配置运行Postgres。另外一种是使用apt安装和systemctl管理Postgres。前者更能够理解底层实现和方便学习，后者是生产系统的主要配置方式。本文档重点放在前者，后者我之后会专门写一篇文档讨论。

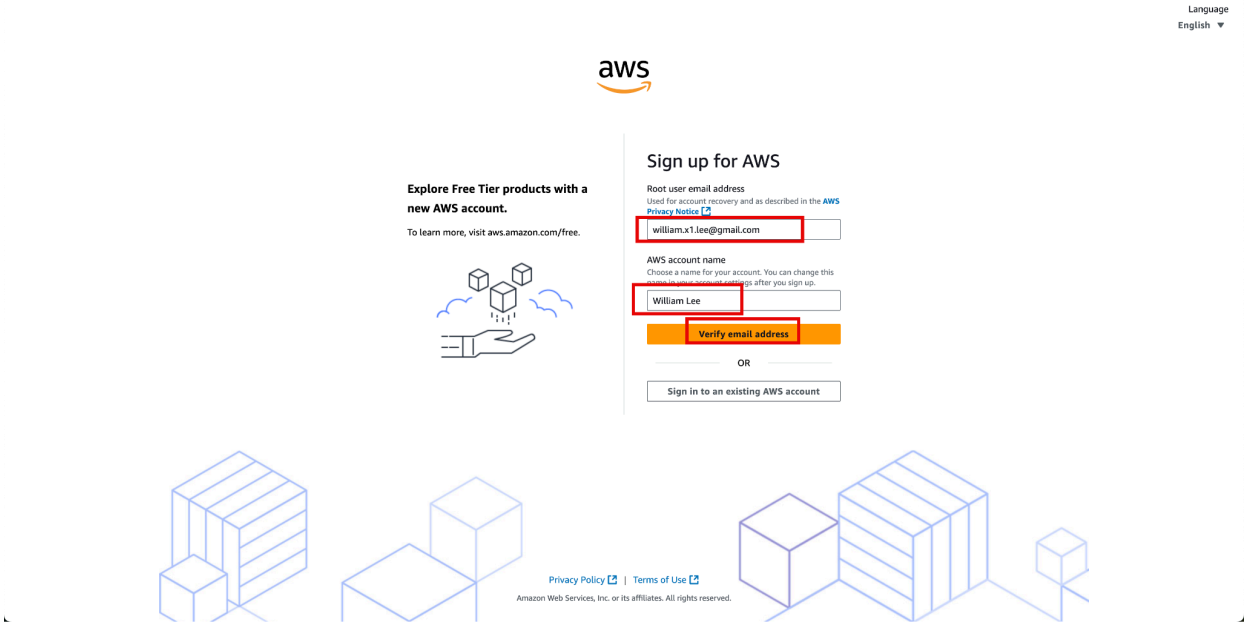
注册AWS账号

登陆AWS主页。
https://aws.amazon.com/

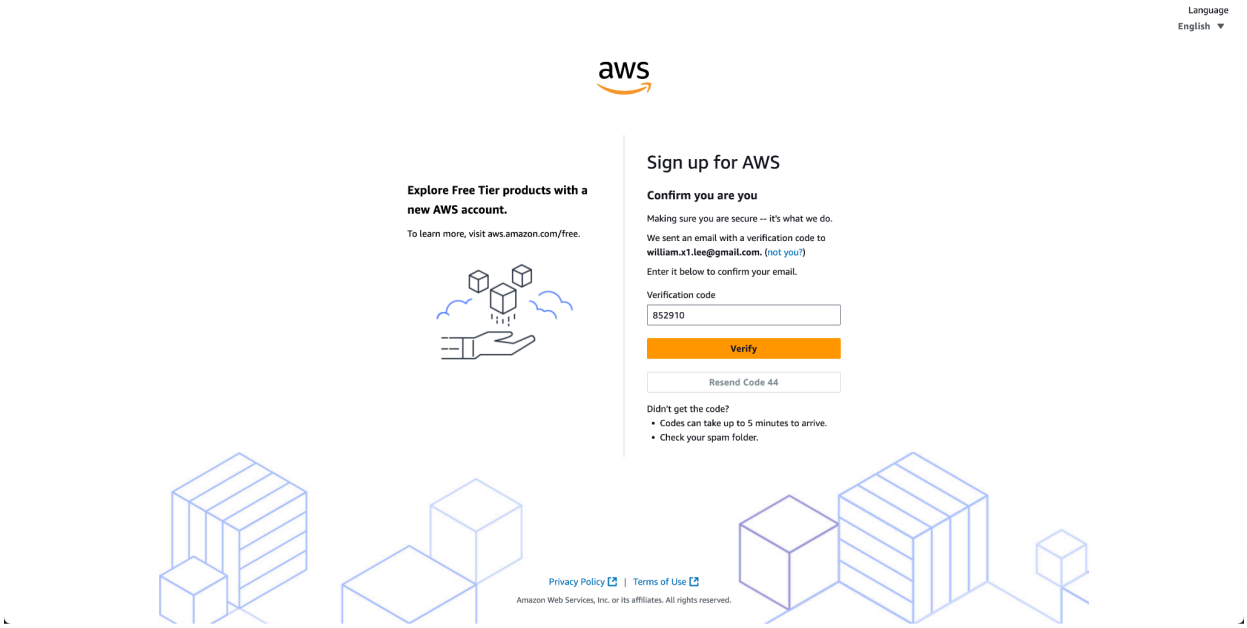
创建新用户。



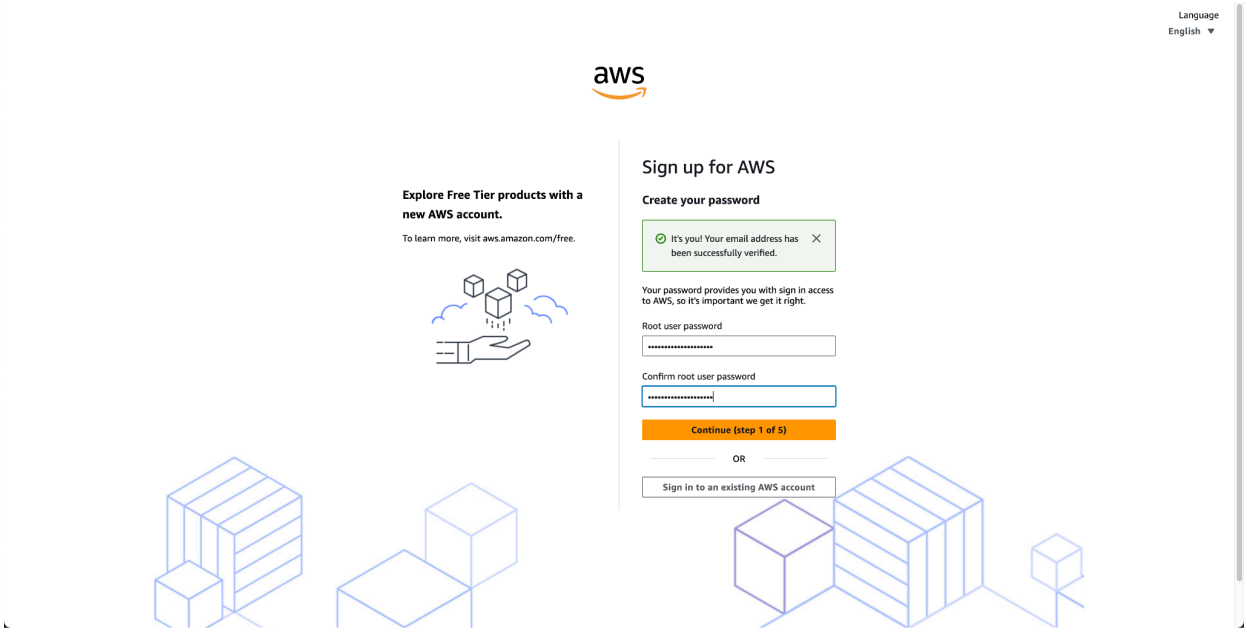
填写邮箱和账户名。



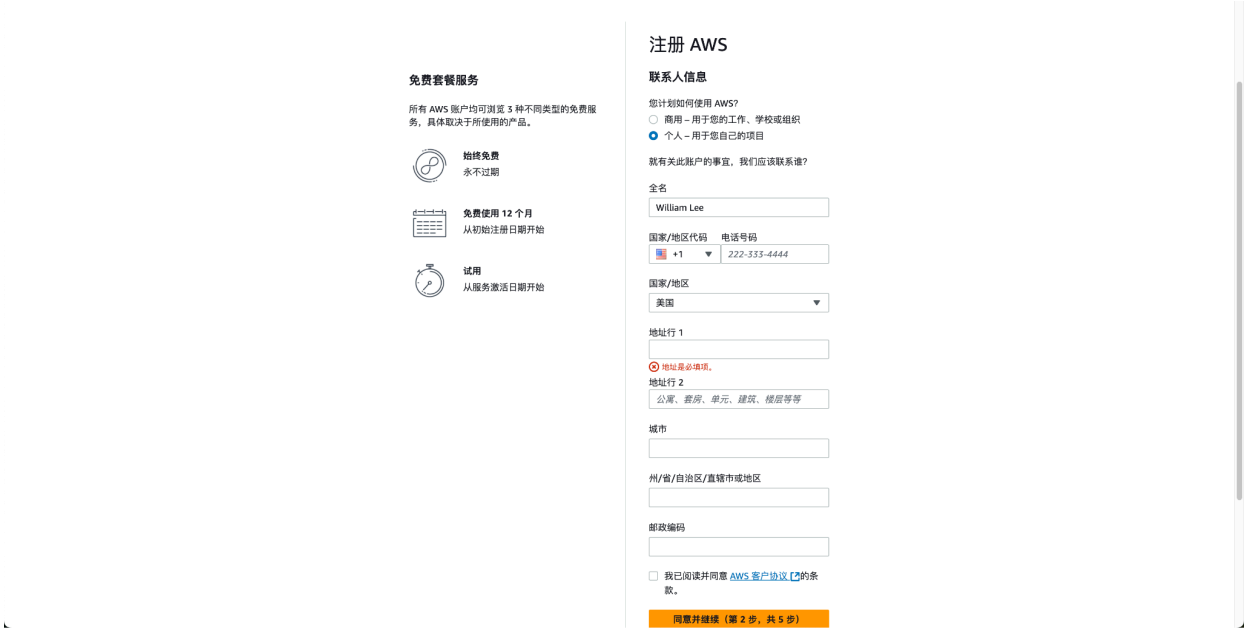
输入验证码，验证。



指定root密码。



输入自己的个人信息。姓名，电话，地址，同意条款，最后点击同意。

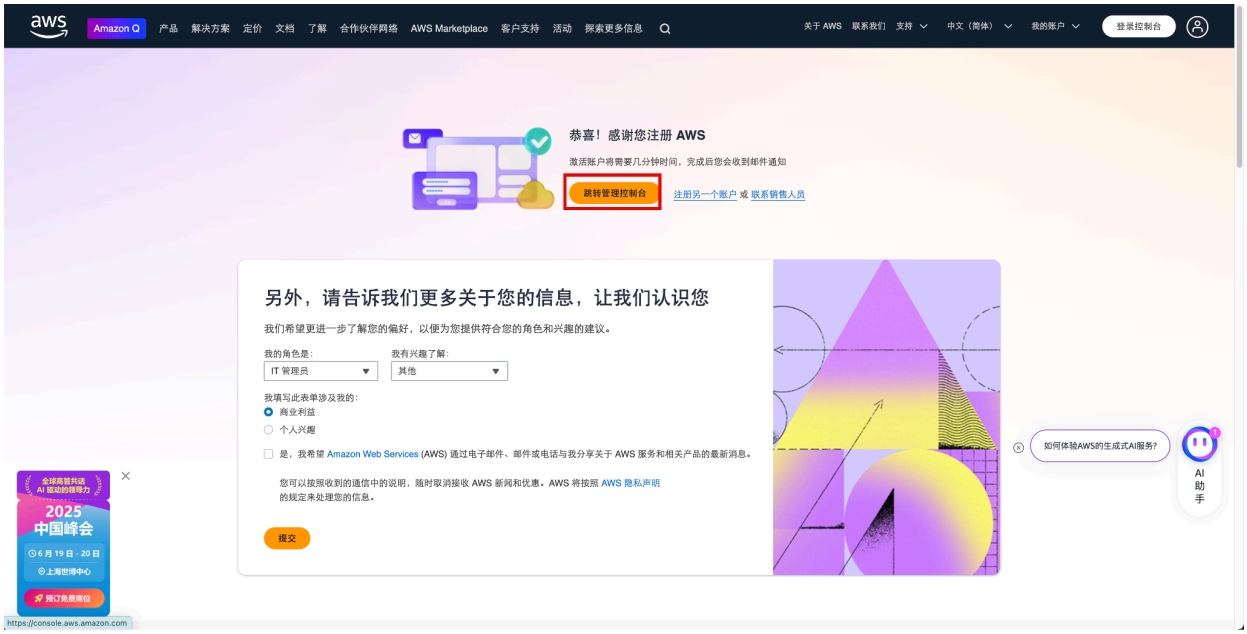


下一步填写信用卡信息。

下一步进行短信验证。确认短信验证码。

选择免费支持，完成注册。

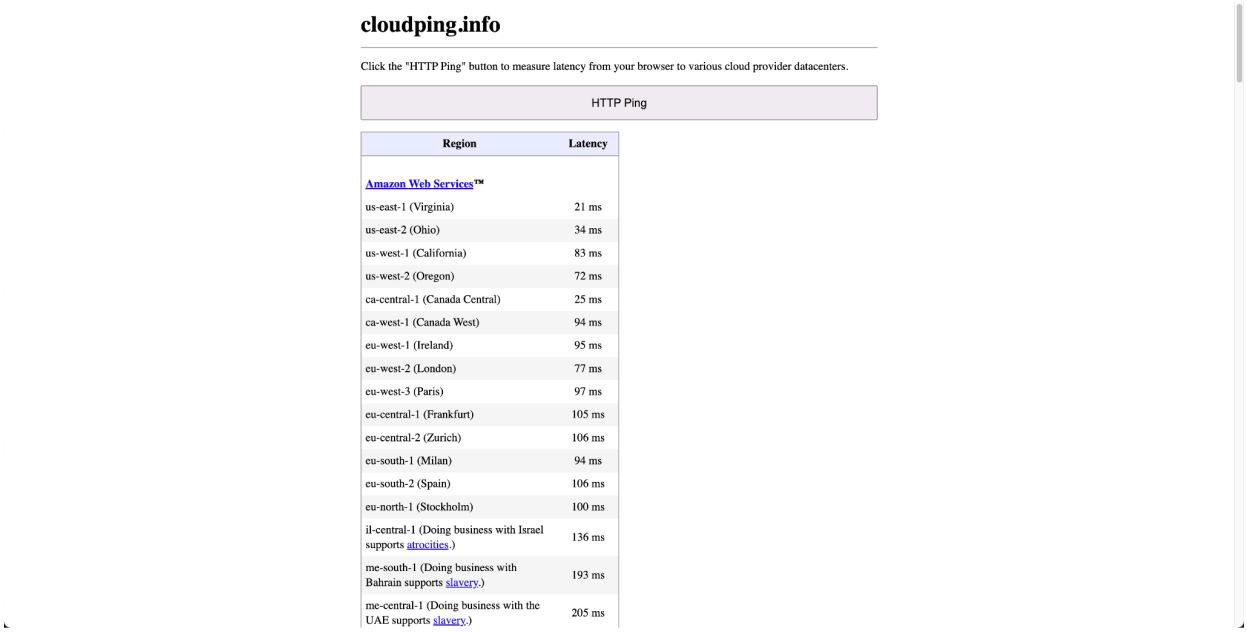
跳转到控制台。



选择数据中心

我们优先选择并使用距离自己最近的数据中心。

使用http ping 查看距离最近的aws数据中心。对于我来说，us-east-1 (Virginia)数据中心距离我最近（Ping Latency最小）。
https://www.cloudping.info/



cloudping.info

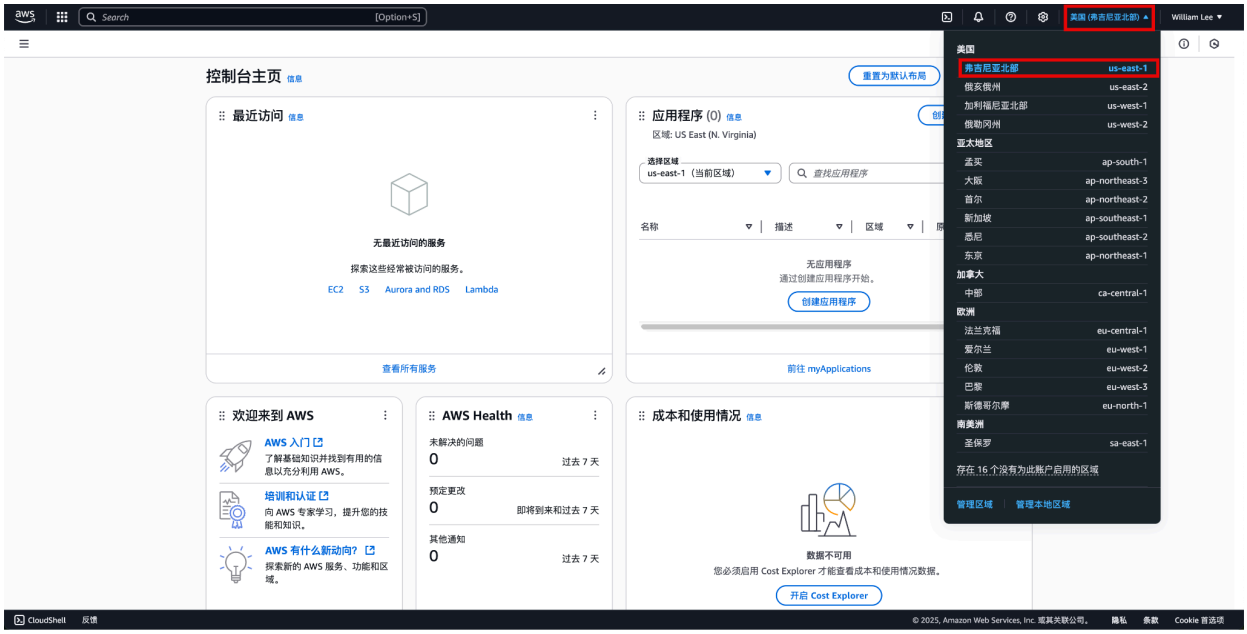
Click the "HTTP Ping" button to measure latency from your browser to various cloud provider datacenters.

HTTP Ping

Region	Latency
Amazon Web Services™	
us-east-1 (Virginia)	21 ms
us-east-2 (Ohio)	34 ms
us-west-1 (California)	83 ms
us-west-2 (Oregon)	72 ms
ca-central-1 (Canada Central)	25 ms
ca-west-1 (Canada West)	94 ms
eu-west-1 (Ireland)	95 ms
eu-west-2 (London)	77 ms
eu-west-3 (Paris)	97 ms
eu-central-1 (Frankfurt)	105 ms
eu-central-2 (Zurich)	106 ms
eu-south-1 (Milan)	94 ms
eu-south-2 (Spain)	106 ms
eu-north-1 (Stockholm)	100 ms
il-central-1 (Doing business with Israel supports atrocities.)	136 ms
me-south-1 (Doing business with Bahrain supports slavery.)	193 ms
me-central-1 (Doing business with the UAE supports slavery.)	205 ms

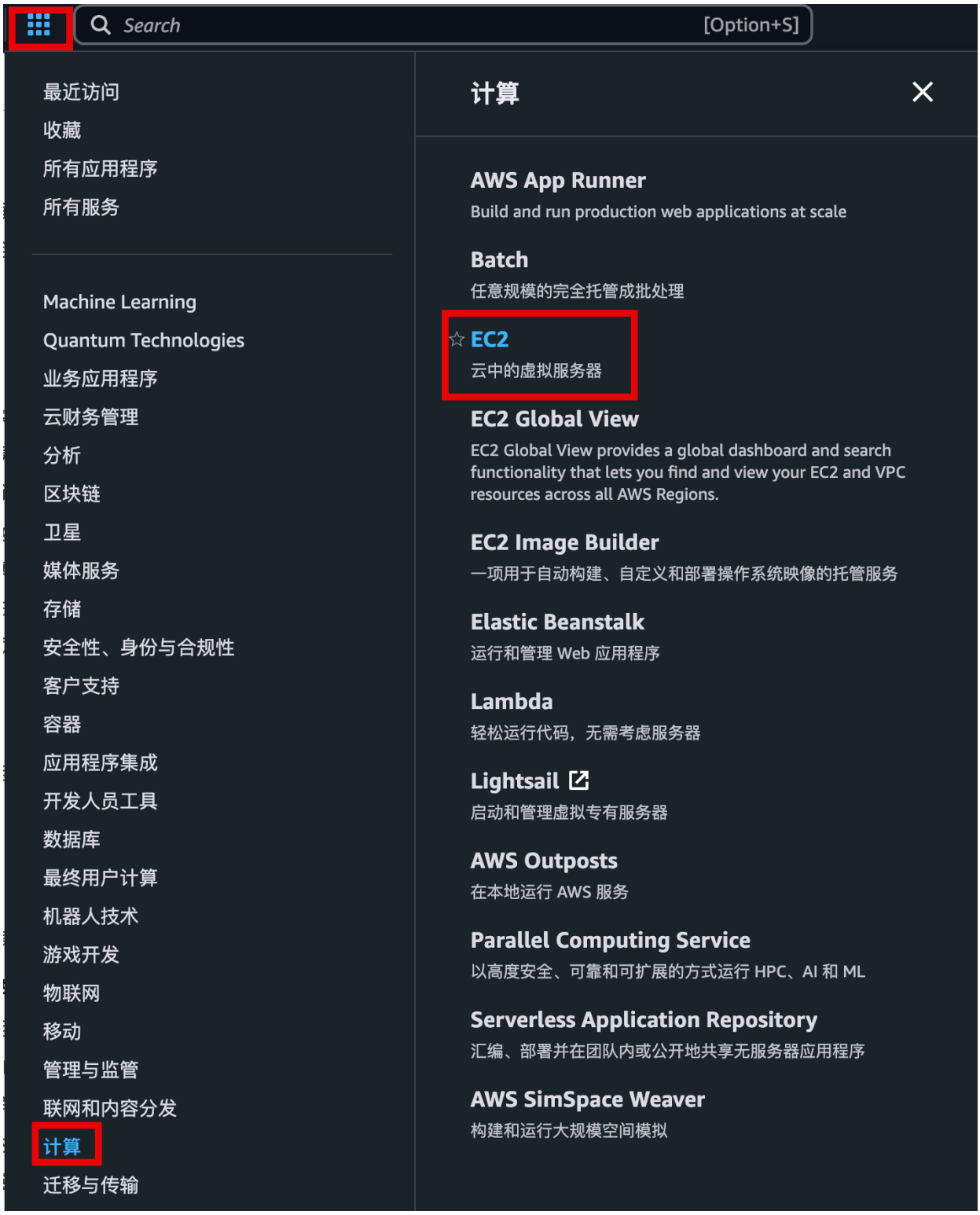
登陆AWS控制台。
https://console.aws.amazon.com/

控制台右上角选择距离最近的数据中心。美国而言通常而言选择 us-east-1 (Virginia)（靠近东部）或者us-west-2 (Oregon)（靠近西部）。

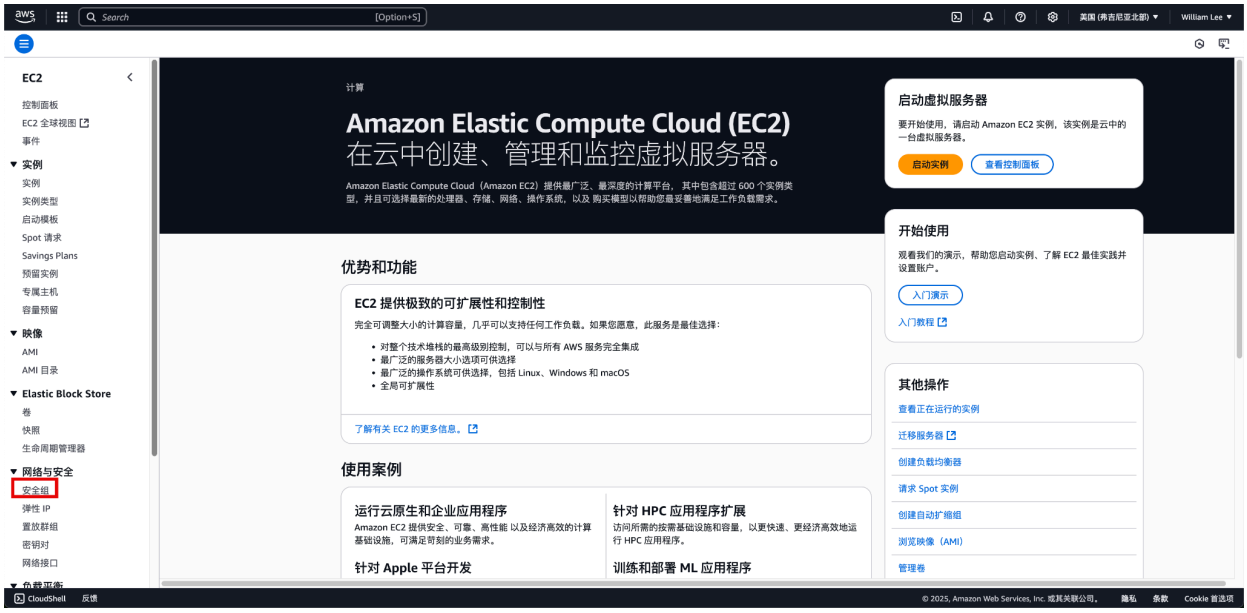


建立安全组

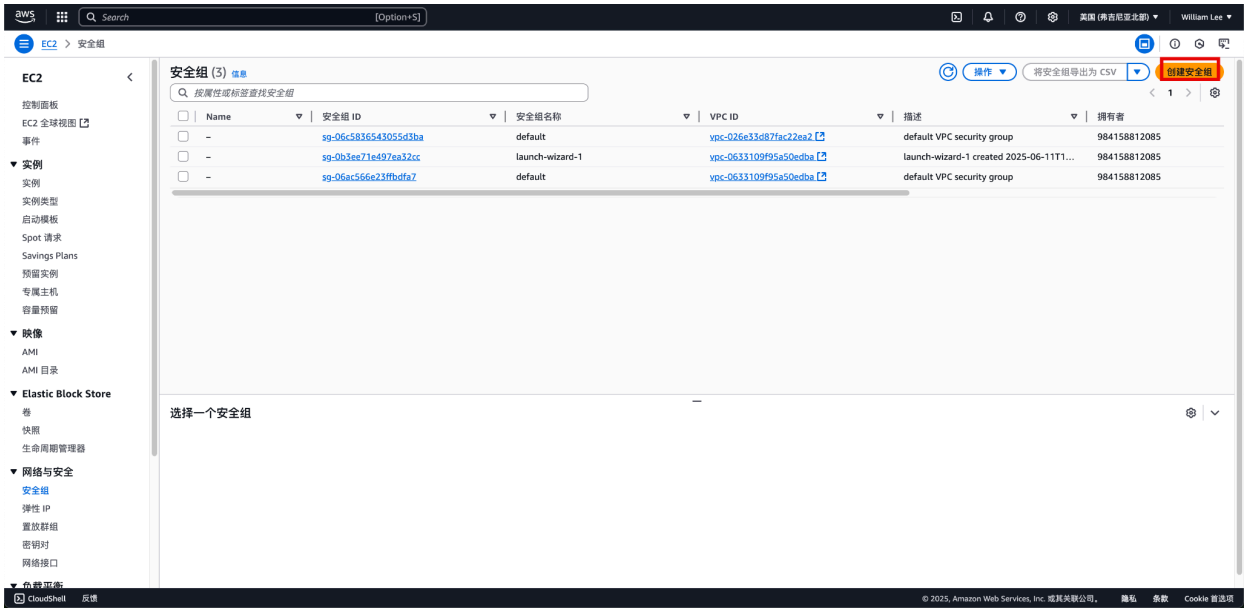
点击菜单，计算，EC2。


Search
[Option+S]
最近访问
收藏
所有应用程序
所有服务
Machine Learning
Quantum Technologies
业务应用程序
云财务管理
分析
区块链
卫星
媒体服务
存储
安全性、身份与合规性
客户支持
容器
应用程序集成
开发人员工具
数据库
最终用户计算
机器人技术
游戏开发
物联网
移动
管理与监管
联网和内容分发
计算
迁移与传输
计算
AWS App Runner
Build and run production web applications at scale
Batch
任意规模的完全托管成批处理
EC2
云中的虚拟服务器
EC2 Global View
EC2 Global View provides a global dashboard and search functionality that lets you find and view your EC2 and VPC resources across all AWS Regions.
EC2 Image Builder
一项用于自动构建、自定义和部署操作系统映像的托管服务
Elastic Beanstalk
运行和管理 Web 应用程序
Lambda
轻松运行代码，无需考虑服务器
Lightsail
启动和管理虚拟专有服务器
AWS Outposts
在本地运行 AWS 服务
Parallel Computing Service
以高度安全、可靠和可扩展的方式运行 HPC、AI 和 ML
Serverless Application Repository
汇编、部署并在团队内或公开地共享无服务器应用程序
AWS SimSpace Weaver
构建和运行大规模空间模拟

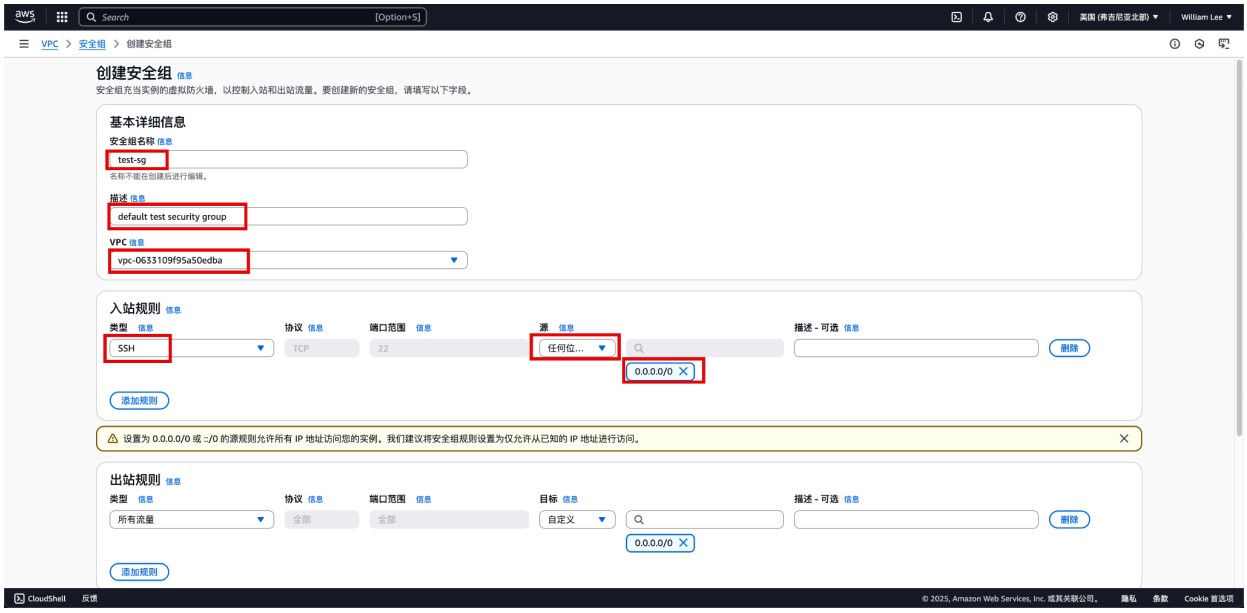
点击安全组。



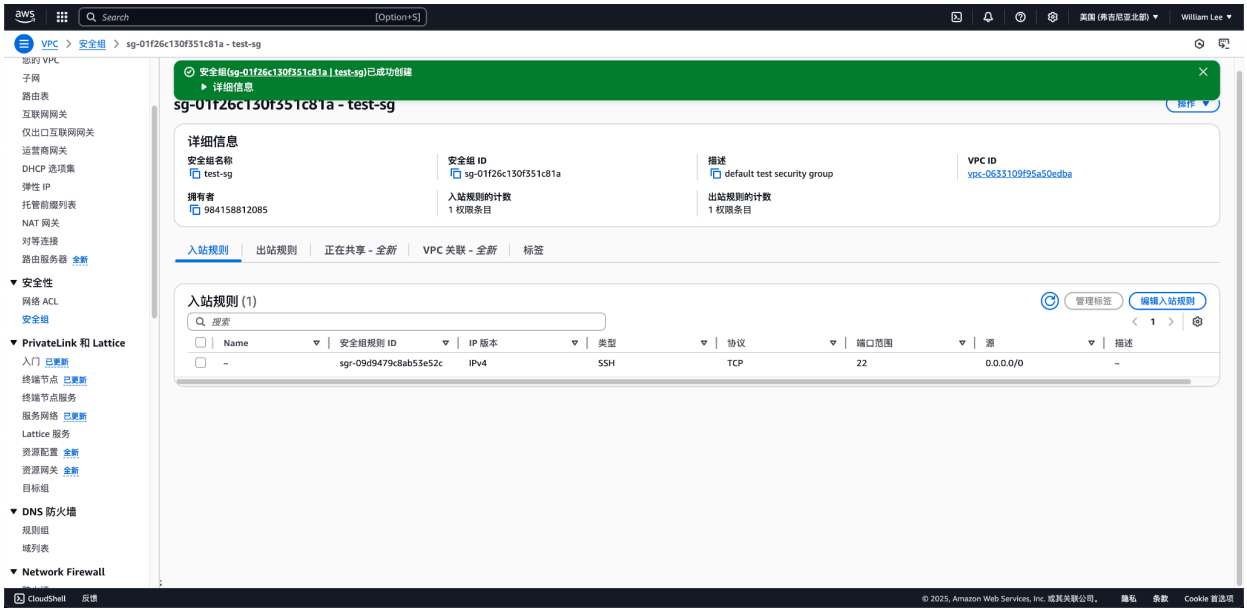
点击创建安全组。



击添加规则，然后填写下面的信息。最后点击右下角的创建安全组。

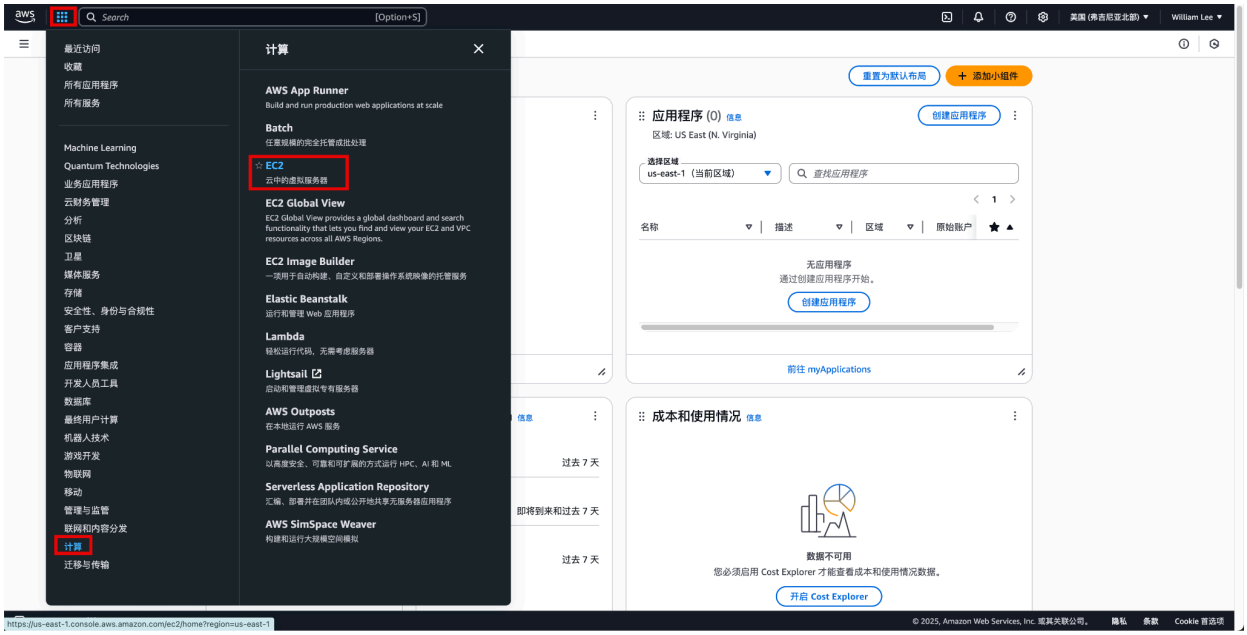

Search
[Option+S]
美国 (弗吉尼亚北部)
William Lee
VPC > 安全组 > 创建安全组
创建安全组 信息
安全组充当实例的虚拟防火墙，以控制入站和出站流量。要创建新的安全组，请填写以下字段。
基本详细信息
安全组名称 信息
test-sg
名称不能在创建后进行编辑。
描述 信息
default test security group
VPC 信息
vpc-0633109f95a50edba
入站规则 信息
类型 信息
协议 信息
端口范围 信息
源 信息
描述 - 可选 信息
SSH
TCP
22
任何位...
0.0.0.0/0
删除
添加规则
设置为 0.0.0.0/0 或 ::/0 的源规则允许所有 IP 地址访问您的实例。我们建议将安全组规则设置为仅允许从已知的 IP 地址进行访问。
出站规则 信息
类型 信息
协议 信息
端口范围 信息
目标 信息
描述 - 可选 信息
所有流量
全部
全部
自定义
0.0.0.0/0
删除
添加规则
CloudShell
反馈
© 2025, Amazon Web Services, Inc. 或其关联公司。
隐私
条款
Cookie 首选项

安全组创建完成。


Search
[Option+S]
美国 (弗吉尼亚北部)
William Lee
VPC > 安全组 > sg-01f26c130f351c81a - test-sg
安全组(sg-01f26c130f351c81a | test-sg)已成功创建
详细信息
sg-01f26c130f351c81a - test-sg
操作
详细信息
安全组名称
test-sg
安全组 ID
sg-01f26c130f351c81a
描述
default test security group
VPC ID
vpc-0633109f95a50edba
拥有者
984158812085
入站规则的计数
1 权限条目
出站规则的计数
1 权限条目
入站规则
出站规则
正在共享 - 全新
VPC 关联 - 全新
标签
入站规则 (1)
管理标签
编辑入站规则
搜索
Name
安全组规则 ID
IP 版本
类型
协议
端口范围
源
描述
sgr-09d9479c8ab53e52c
IPv4
SSH
TCP
22
0.0.0.0/0
子网
路由表
互联网网关
仅出口互联网网关
运营商网关
DHCP 选项集
弹性 IP
托管前缀列表
NAT 网关
对等连接
路由服务器 全新
安全性
网络 ACL
安全组
PrivateLink 和 Lattice
入门 已更新
终端节点 已更新
终端节点服务
服务网络 已更新
Lattice 服务
资源配置 全新
资源网关 全新
目标组
DNS 防火墙
规则组
域列表
Network Firewall
CloudShell
反馈
© 2025, Amazon Web Services, Inc. 或其关联公司。
隐私
条款
Cookie 首选项

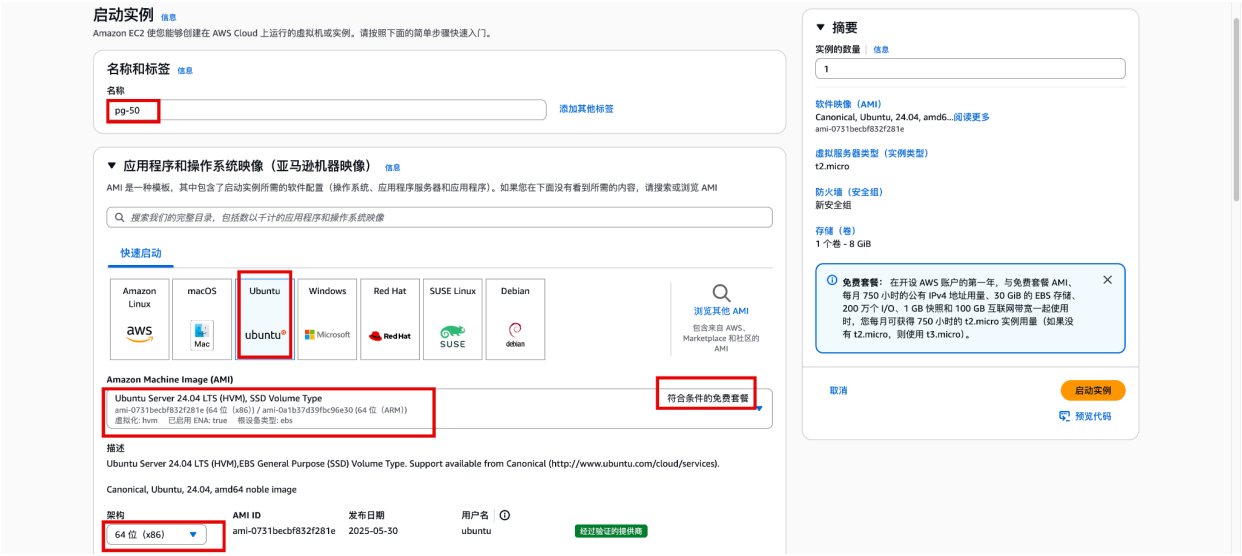
建立虚拟机

依次点击菜单，最后选择EC2。

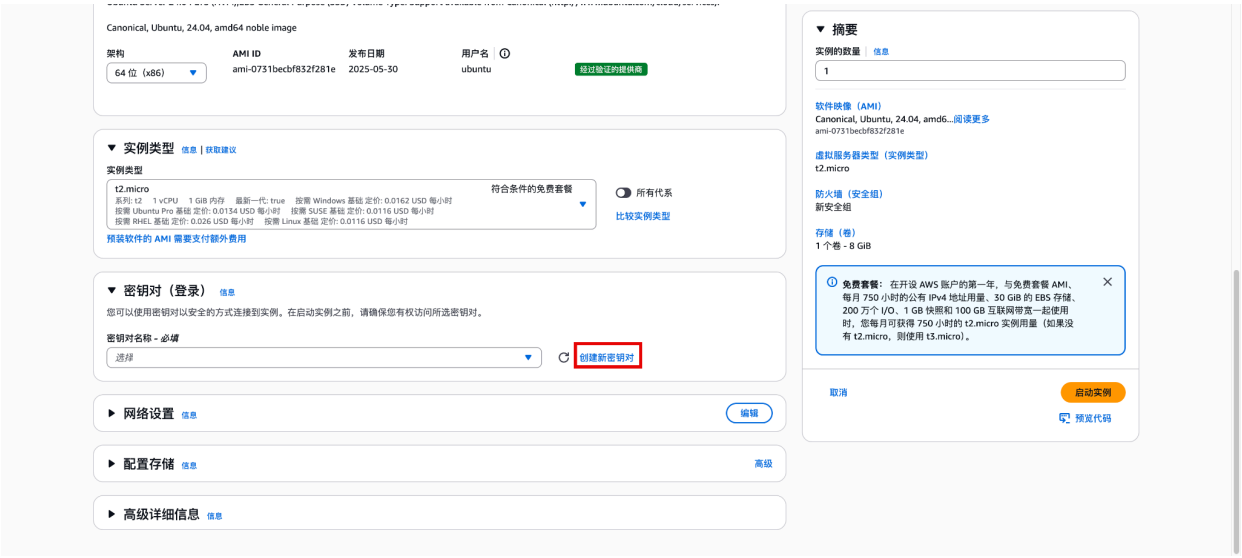


启动实例。

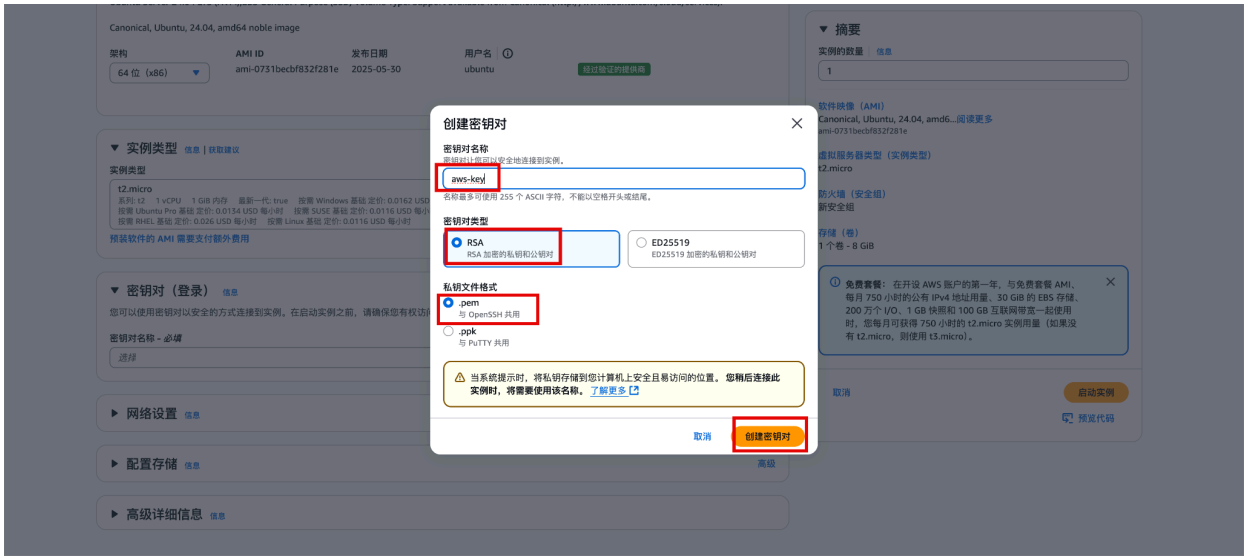
依次输入和选择。注意这里可以首先选择12个月免费的套餐。架构选择64位 x86。



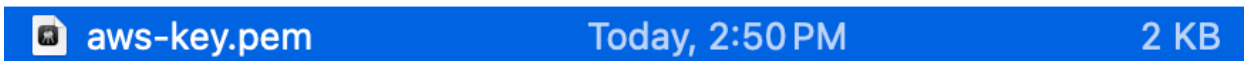
通过公钥和私钥进行AWS服务器访问。点击创建新密钥对。



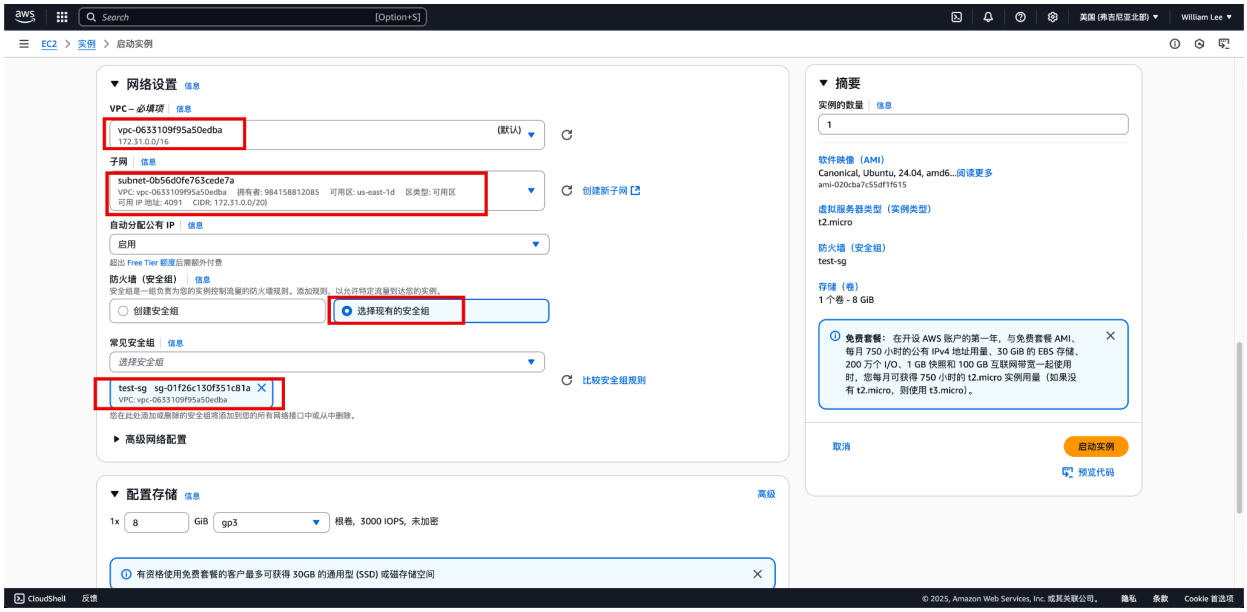
填写密钥对名称。选择最主流的RSA和pem。



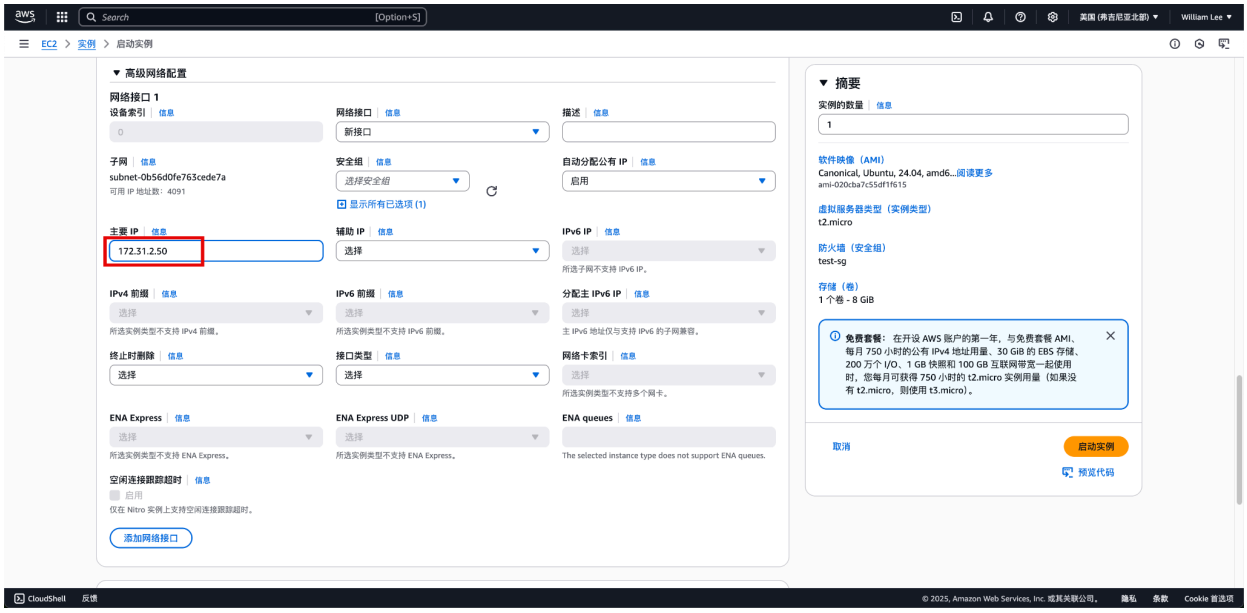
妥善保存生成的密钥。选择刚刚生成的密钥aws-key。



点击网络设置，点击编辑。依次选择下面的选项。

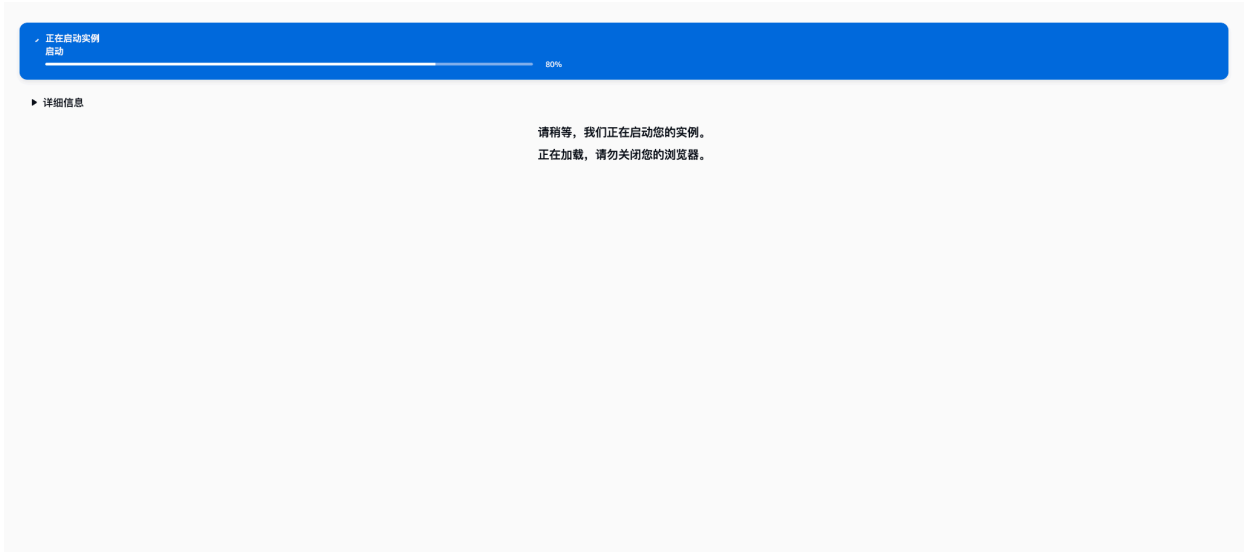


点击高级网络配置。手动指定私有IP。

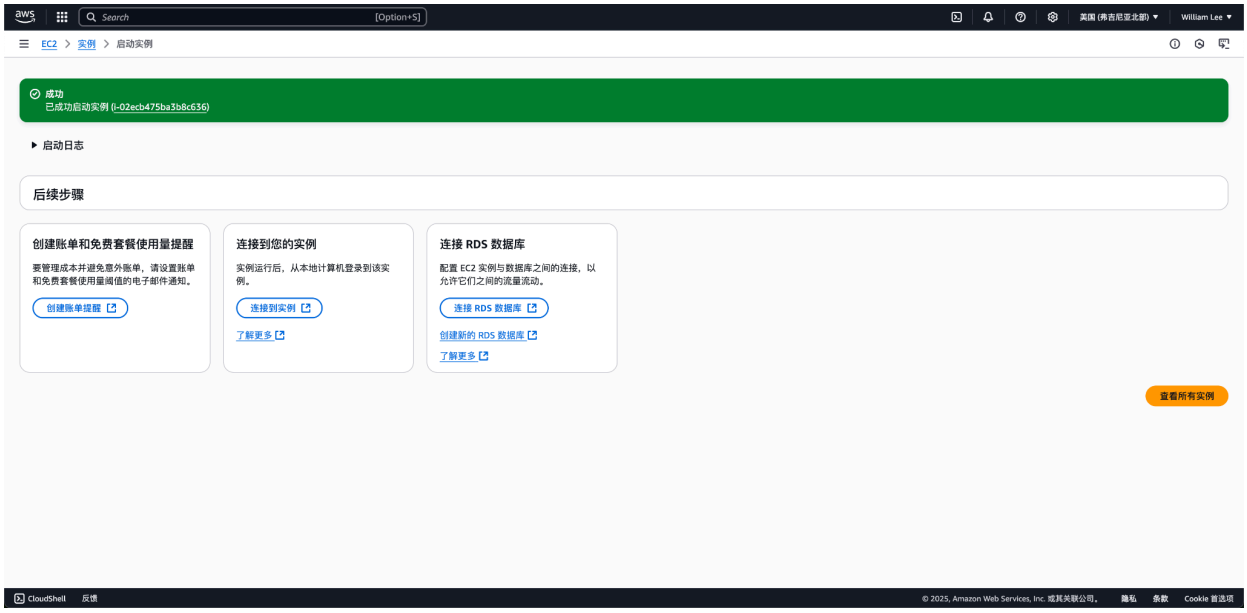


其他选项接受默认。最后点击右下角的启动实例。

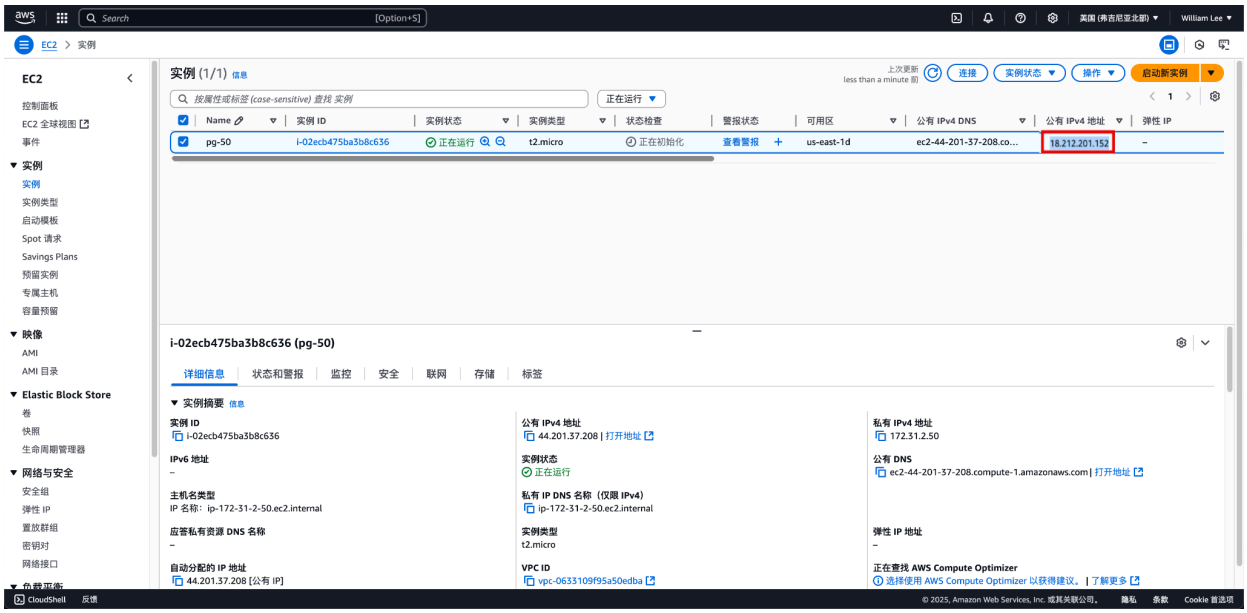
稍等片刻。



实例创建成功，点击查看所有实例。



拷贝并记录刚刚创建的EC2实例的公网IP地址。



使用ssh远程登陆实例。需要设置私钥的访问权限为600，不然会报错。

chmod 600 aws-key.pem

ssh -i aws-key.pem ubuntu@18.212.201.152

```
willi@macbook-pro-m3 ~ % ssh -i aws-key.pem ubuntu@18.212.201.152
The authenticity of host '18.212.201.152 (18.212.201.152)' can't be established.
ED25519 key fingerprint is SHA256:5Zf5j9DiELdbgksP3OJFoCGEitl42XWGaECeIjQnCWQ.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '18.212.201.152' (ED25519) to the list of known hosts.
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@         WARNING: UNPROTECTED PRIVATE KEY FILE!          @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Permissions 0644 for 'aws-key.pem' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
Load key "aws-key.pem": bad permissions
ubuntu@18.212.201.152: Permission denied (publickey).
willi@macbook-pro-m3 ~ % chmod 600 aws-key.pem
willi@macbook-pro-m3 ~ % ssh -i aws-key.pem ubuntu@18.212.201.152
Welcome to Ubuntu 24.04.2 LTS (GNU/Linux 6.8.0-1029-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Wed Jun 11 18:58:37 UTC 2025
```

```
Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-172-31-82-142:~$ hostname
ip-172-31-82-142
ubuntu@ip-172-31-82-142:~$ whoami
ubuntu
ubuntu@ip-172-31-82-142:~$ sudo su -
root@ip-172-31-82-142:~#
```

可以正常切换到root用户，并且执行命令。
sudo su -
apt update && apt upgrade -y

```
root@ip-172-31-82-142:~# apt update && apt upgrade -y
Hit:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble InRelease
Get:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Get:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-backports InRelease [126 kB]
Get:4 http://security.ubuntu.com/ubuntu noble-security InRelease [126 kB]
Get:5 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 Packages [15.0 MB]
0% [5 Packages 0 B/15.0 MB 0%] [4 InRelease 14.2 kB/126 kB 11%]
```

安装和配置Postgres的不同方式

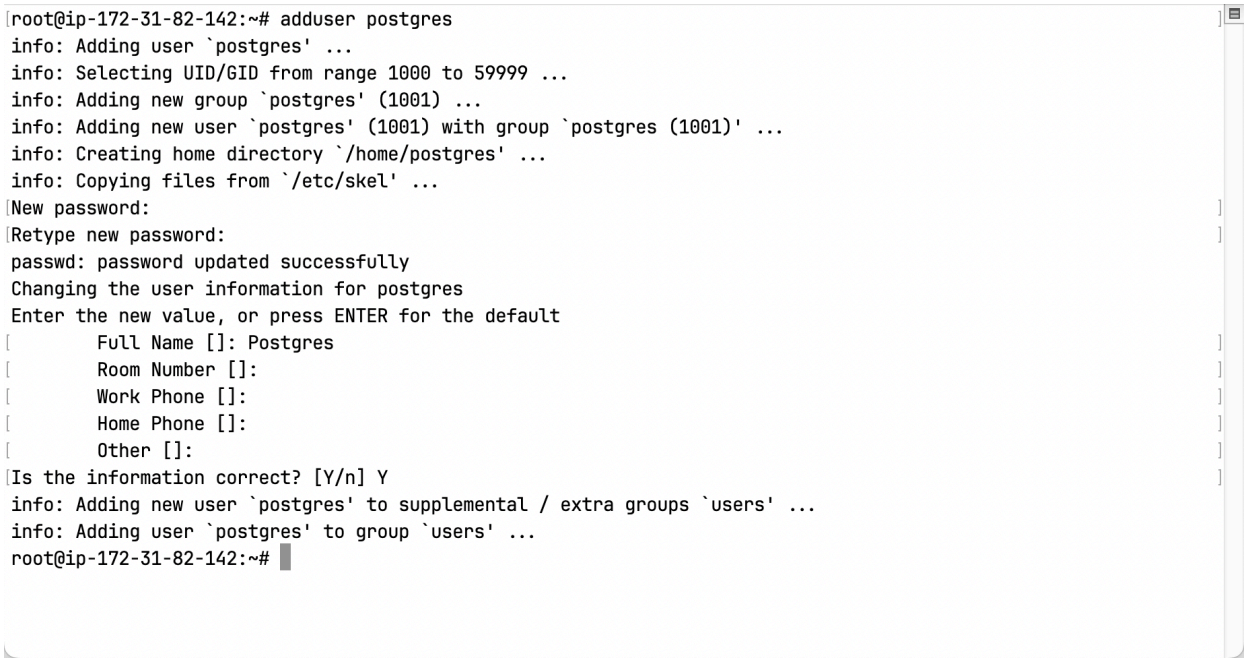
安装和配置Postgres通常情况下有两种。一种是从源码编译安装配置运行Postgres。另外一种是使用apt安装和systemctl管理Postgres。前者更能够理解底层实现和方便学习，后者是生产系统的主要配置方式。本文档重点放在前者，后者我之后会专门写一篇文档讨论。

创建和配置postgres用户

提取之前私钥 aws-key.pem 的公钥。
ssh-keygen -y -f aws-key.pem

```
willi@macbook-pro-m3 ~ % ssh-keygen -y -f aws-key.pem
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCulFbHHpr+5/KMeeLtg+9fTKXZ6E+sTbeJf8bCQv6Bc2Y7T2zP8gP+nauiWAE89M5PJrvsCrtg
/JuPie4i6LJyaC/CrEt+o5NKZjTlNyEGj9i7pwAJ++z1rI+Y+dHH3xnAiyWI1GTnimw3qltvfShcaWGFxPchddaIIh9oCuoymNvDTsjCIODRcPYa
aAqxjwv+6yt8by0/ZmdooVOpy7uY5lf4ZWd8RbDiJ0NP3mPcjYHJ2DWcn+xROEdj27ziblrMHRExVBtCJFToiMMUWav+XvBDVmevkqIgmJ9KuIrS
/k47v5zfw2hTcKJKUTn2J31fb2ae4Vuz4kgtca91/cxz
willi@macbook-pro-m3 ~ %
```

登陆ec2实例，并且切换至root用户。
sudo su -
adduser postgres



切换至postgres用户。执行下面命令，并且添加上面提取的公钥信息到信任文件。信任文件里的每一行代表一个信任的公钥，改行公钥的最后可以加一个空格接一个注释表示该公钥的来源（aws-key）。
su - postgres
cd
mkdir .ssh
touch .ssh/authorized_keys
chmod 700 .ssh
chmod 600 .ssh/authorized_keys
vi .ssh/authorized_keys

```
root@ip-172-31-82-142:~# su - postgres
postgres@ip-172-31-82-142:~$ cd
postgres@ip-172-31-82-142:~$ mkdir .ssh
postgres@ip-172-31-82-142:~$ touch .ssh/authorized_keys
postgres@ip-172-31-82-142:~$ chmod 700 .ssh
postgres@ip-172-31-82-142:~$ chmod 600 .ssh/authorized_keys
postgres@ip-172-31-82-142:~$ vi .ssh/authorized_keys
postgres@ip-172-31-82-142:~$ cat .ssh/authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCulFbHHpr+5/KMeeLtg+9fTKXZ6E+sTbeJf8bCQv6Bc2Y7T2zP8gP+nauiWAE89M5PJrvsCrtg
/JuPie4i6LJyaC/CrEt+o5NKZjTlNyEGj9i7pwAJ++z1rI+Y+dHH3xnAiyWI1GTnimw3qltvfShcaWGFxPchddaIIh9oCuoymNvDTsjCIODRcPYa
aAqxjwv+6yt8by0/ZmdooVOpy7uY5lf4ZWd8RbDiJ0NP3mPcjYHJ2DWcn+xROEdj27ziblrMHRExVBtCJFToiMMUWav+XvBDVmevkqIgmJ9KuIrS
/k47v5zfw2hTcKJKUTn2J31fb2ae4Vuz4kgtca91/cxz aws-key
postgres@ip-172-31-82-142:~$
```

测试使用私钥，远程使用postgres用户登陆。登陆成功。
ssh -i aws-key.pem postgres@18.212.201.152

```
willi@macbook-pro-m3 ~ % ssh -i aws-key.pem postgres@18.212.201.152
Welcome to Ubuntu 24.04.2 LTS (GNU/Linux 6.8.0-1029-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Wed Jun 11 19:39:30 UTC 2025

  System load:  0.0               Processes:             110
  Usage of /:   29.0% of 6.71GB   Users logged in:       1
  Memory usage: 23%               IPv4 address for enX0: 172.31.82.142
  Swap usage:   0%


Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status
```

```
  Usage of /:   29.0% of 6.71GB   Users logged in:       1
  Memory usage: 23%               IPv4 address for enX0: 172.31.82.142
  Swap usage:   0%


Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status



The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

postgres@ip-172-31-82-142:~$ whoami
postgres
postgres@ip-172-31-82-142:~$
```

为postgres用户添加sudo执行权限。

使用root执行下面的命令为postgres添加sudo执行权限。测试sudo命令的执行。
usermod -aG sudo postgres

```
root@ip-172-31-82-142:~# usermod -aG sudo postgres
root@ip-172-31-82-142:~# su - postgres
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

postgres@ip-172-31-82-142:~$ sudo whoami
[sudo] password for postgres:
root
postgres@ip-172-31-82-142:~$
```

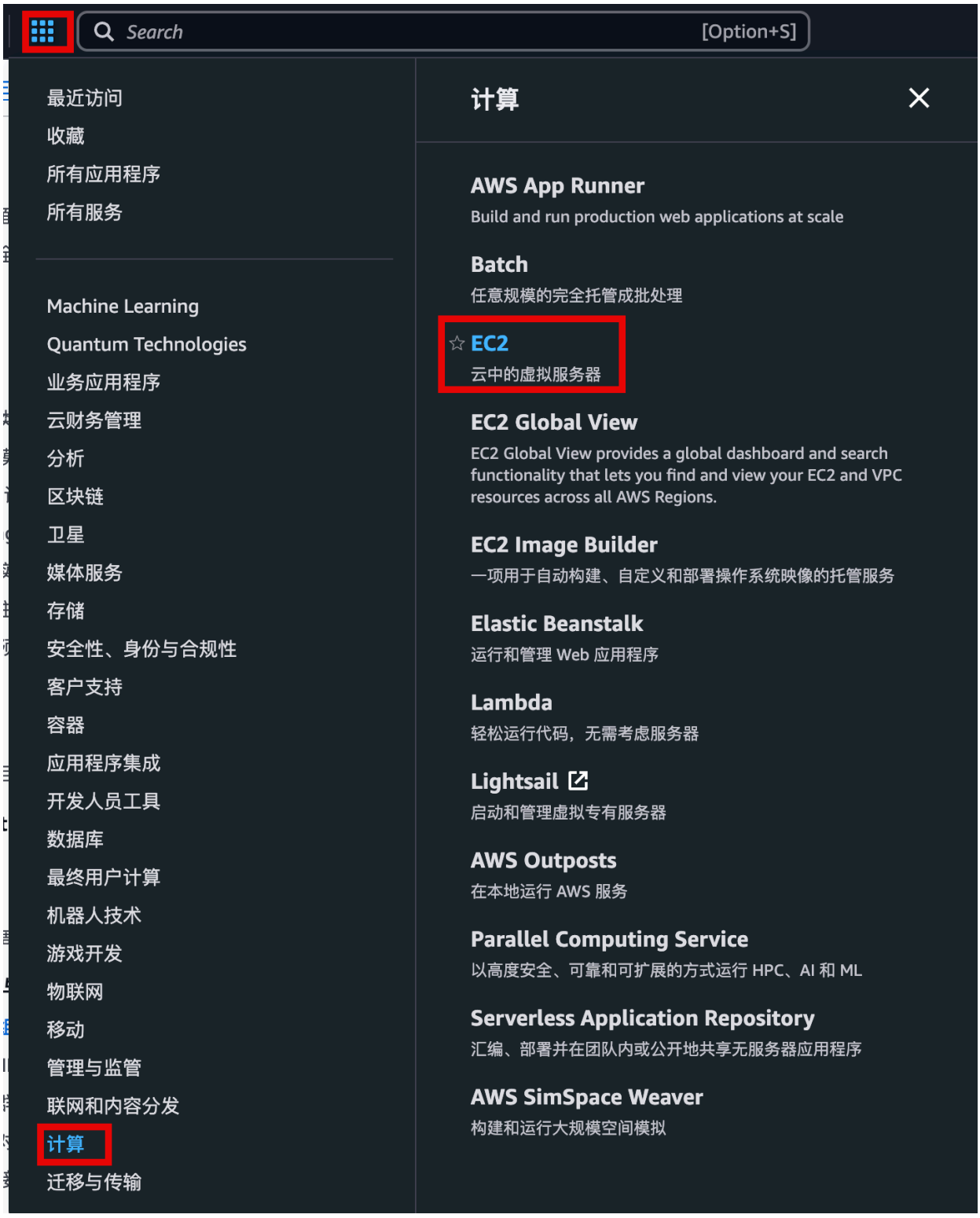
下载编译安装使用PG数据库

参考下面文档，下载编译安装使用PG数据库。

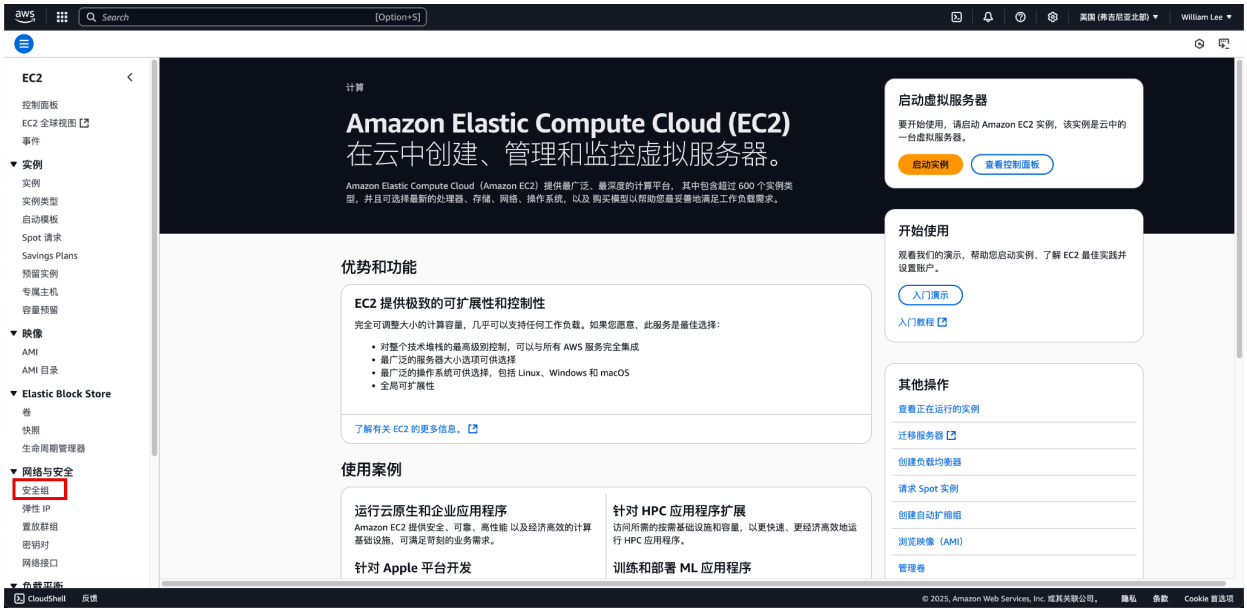
PostgreSQL 17.5 在Ubuntu 24.0.2 x64 上的安装（Windows x64 + VMware Workstation Pro）

配置安全组允许子网内部远程访问

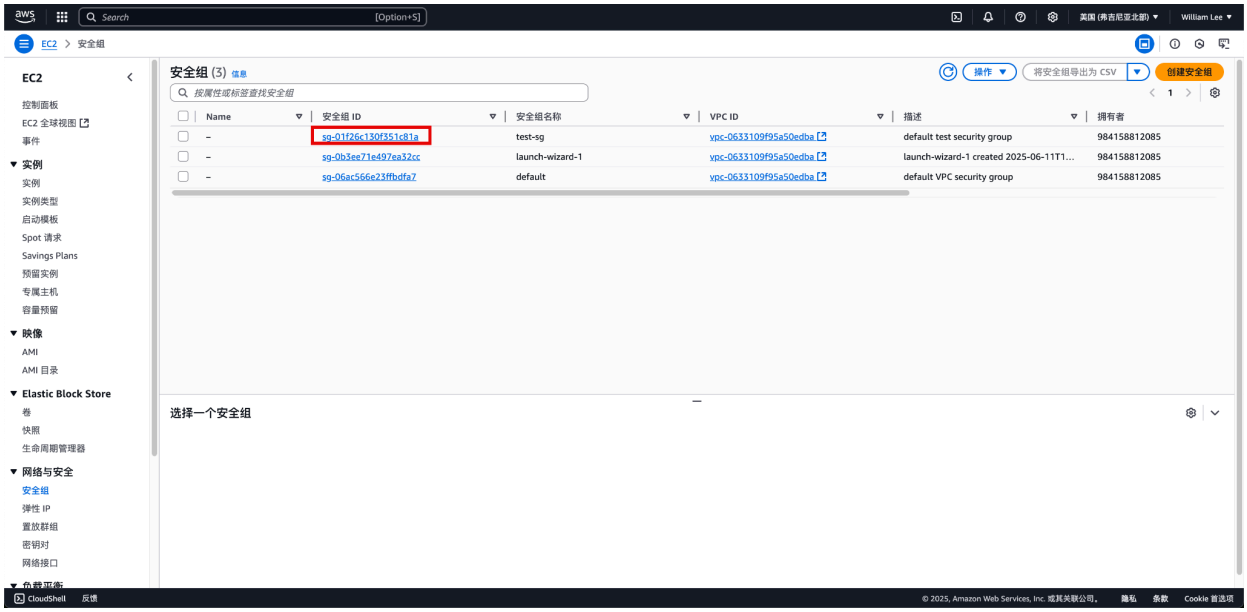
点击菜单，计算，EC2。


Search
[Option+S]
最近访问
收藏
所有应用程序
所有服务
Machine Learning
Quantum Technologies
业务应用程序
云财务管理
分析
区块链
卫星
媒体服务
存储
安全性、身份与合规性
客户支持
容器
应用程序集成
开发人员工具
数据库
最终用户计算
机器人技术
游戏开发
物联网
移动
管理与监管
联网和内容分发
计算
迁移与传输
计算
AWS App Runner
Build and run production web applications at scale
Batch
任意规模的完全托管成批处理
EC2
云中的虚拟服务器
EC2 Global View
EC2 Global View provides a global dashboard and search functionality that lets you find and view your EC2 and VPC resources across all AWS Regions.
EC2 Image Builder
一项用于自动构建、自定义和部署操作系统映像的托管服务
Elastic Beanstalk
运行和管理 Web 应用程序
Lambda
轻松运行代码，无需考虑服务器
Lightsail
启动和管理虚拟专有服务器
AWS Outposts
在本地运行 AWS 服务
Parallel Computing Service
以高度安全、可靠和可扩展的方式运行 HPC、AI 和 ML
Serverless Application Repository
汇编、部署并在团队内或公开地共享无服务器应用程序
AWS SimSpace Weaver
构建和运行大规模空间模拟

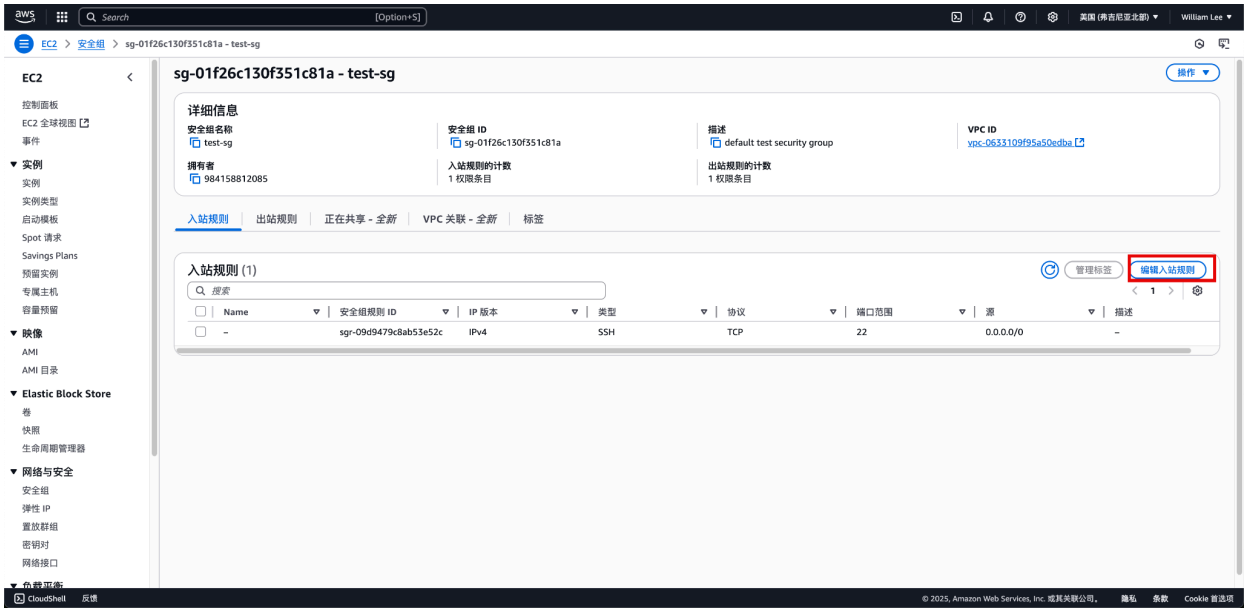
点击安全组。



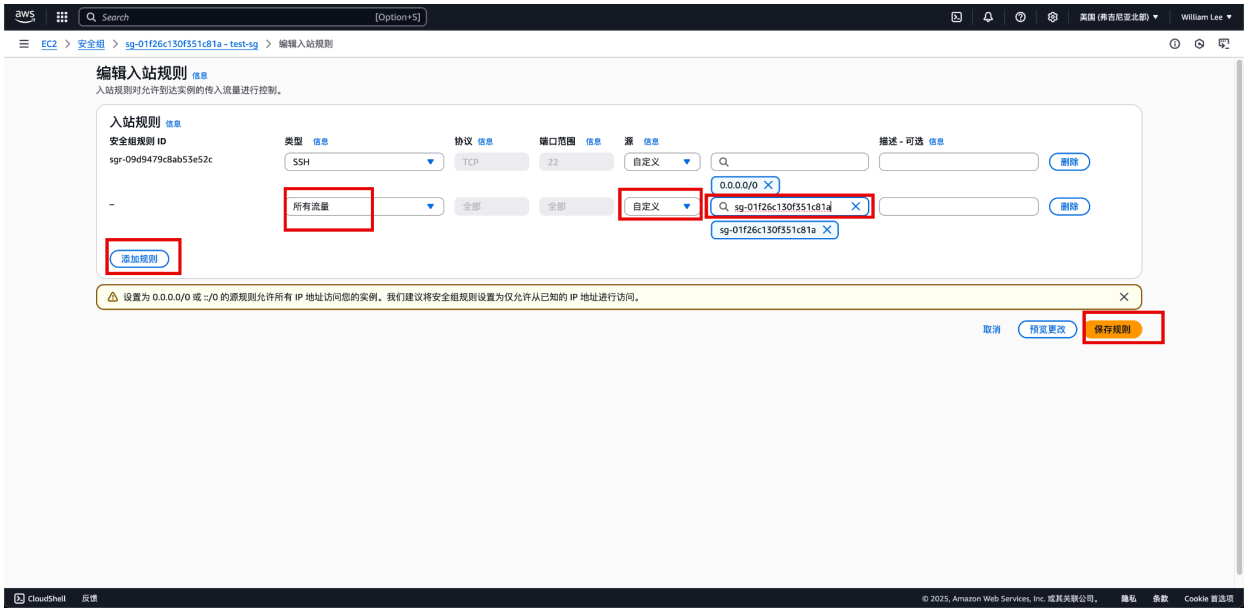
点击创建虚拟机时使用的安全组。



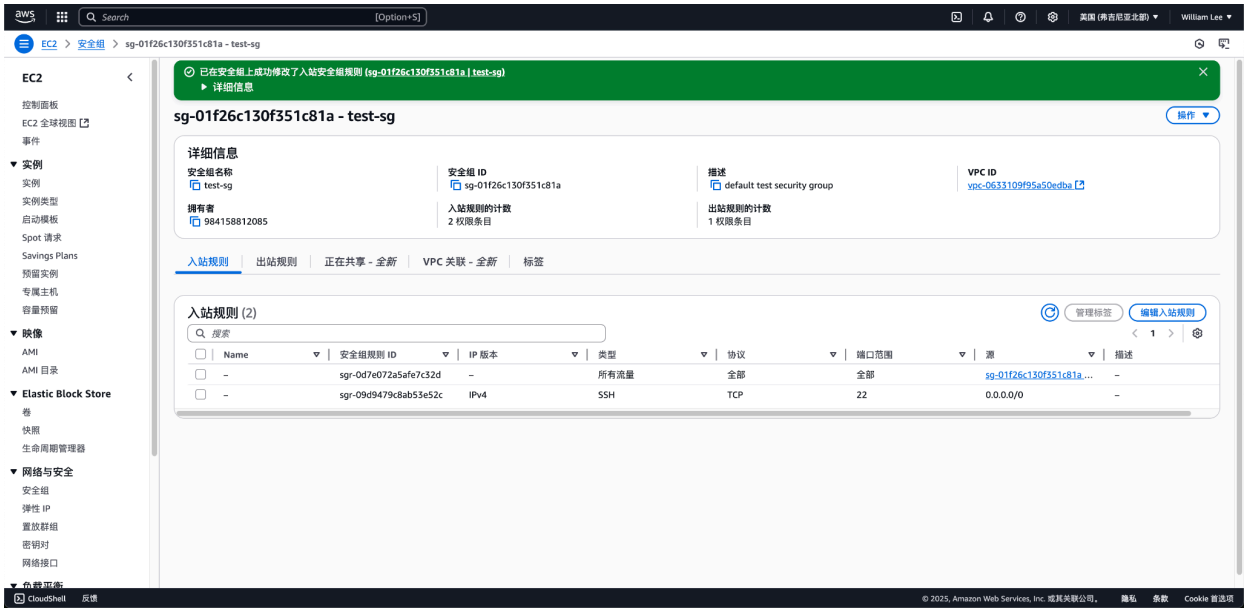
点击编辑入站规则。



点击添加规则，进行下面的选择。这里允许使用自定义安全组(test-sg)的所有虚拟机之间使用任意协议和端口进行通讯。



保存规则成功。



检查数据库虚拟机的数据库配置，确保在数据库层面可以被远程访问。注意由于在安全组层面设置了访问控制，这里的PG数据库层面我设置允许所有远程主机通过libpq和replication的协议访问。

```
[postgres@ip-172-31-2-50:~/data1$ grep listen postgresql.conf
#listen_addresses = 'localhost'         # what IP address(es) to listen on;
listen_addresses = '*'
[postgres@ip-172-31-2-50:~/data1$ grep md5 pg_hba.conf
# METHOD can be "trust", "reject", "md5", "password", "scram-sha-256",
# Note that "password" sends passwords in clear text; "md5" or
host    all             all             0.0.0.0/0               md5
host    replication     all             0.0.0.0/0               md5
postgres@ip-172-31-2-50:~/data1$
```

在使用安全组（test-sg）的另外一台虚拟机尝试psql远程访问上面的数据库。访问成功。

```
postgres@ip-172-31-2-51:~/data1$ psql -h 172.31.2.50 -p 5432 -U postgres -d oracle
Password for user postgres:
psql (17.5)
Type "help" for help.

oracle=# select * from state;
 id |   name
----+----------
 CO | Colorado
 TX | Texas
(2 rows)

oracle=#
```

对于没有使用指定安全组（test-sg）的任何其他访问源，例如我的本地电脑，则无法访问除22端口（SSH）以外的所有端口。

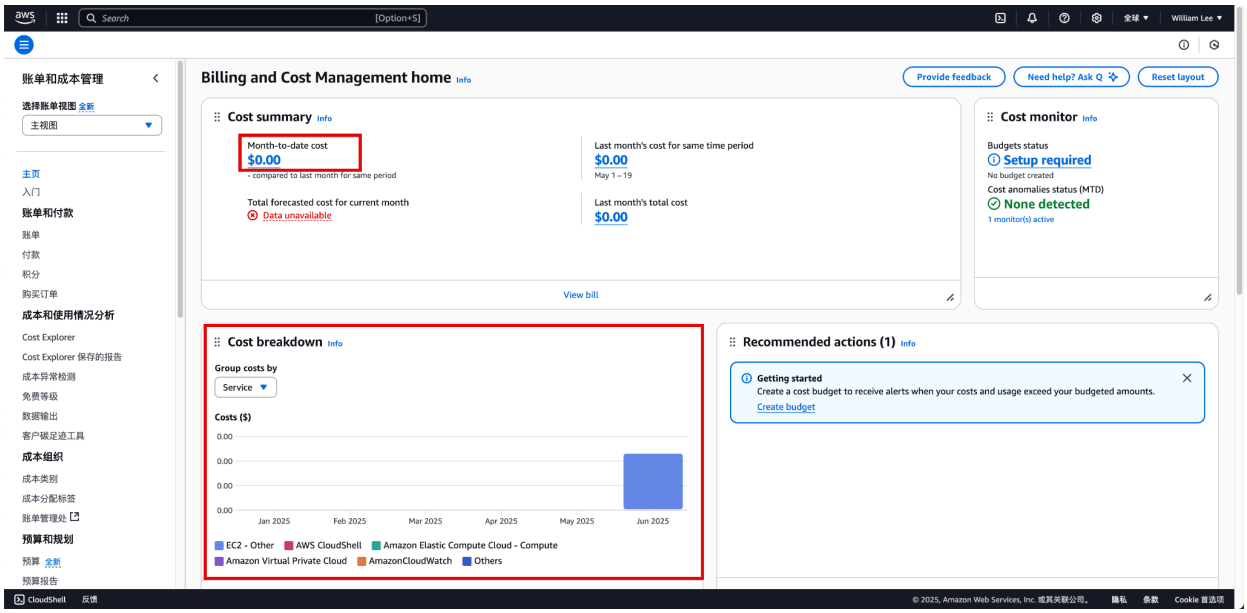
```
willi@macbook-pro-m3 ~ % telnet 44.201.37.208 5432
Trying 44.201.37.208...
^C
willi@macbook-pro-m3 ~ %
```

周期性检查账单

AWS的大多数服务都是收费的。定期检查账单能帮助您及早发现意外配置导致的额外收费服务使用。

选择菜单，云财务管理，账单与成本管理。

这里重点关注month-to=end cost 和cost breakdown。前者是本月截止到目前的花费，后者表示分别在那些aws的服务上分别花费了多少钱。



Reference

AWS EC2设置防火墙规则，允许两台EC2网络互通

End