ssh -i 5120key.pem ubuntu@107.23.164.146

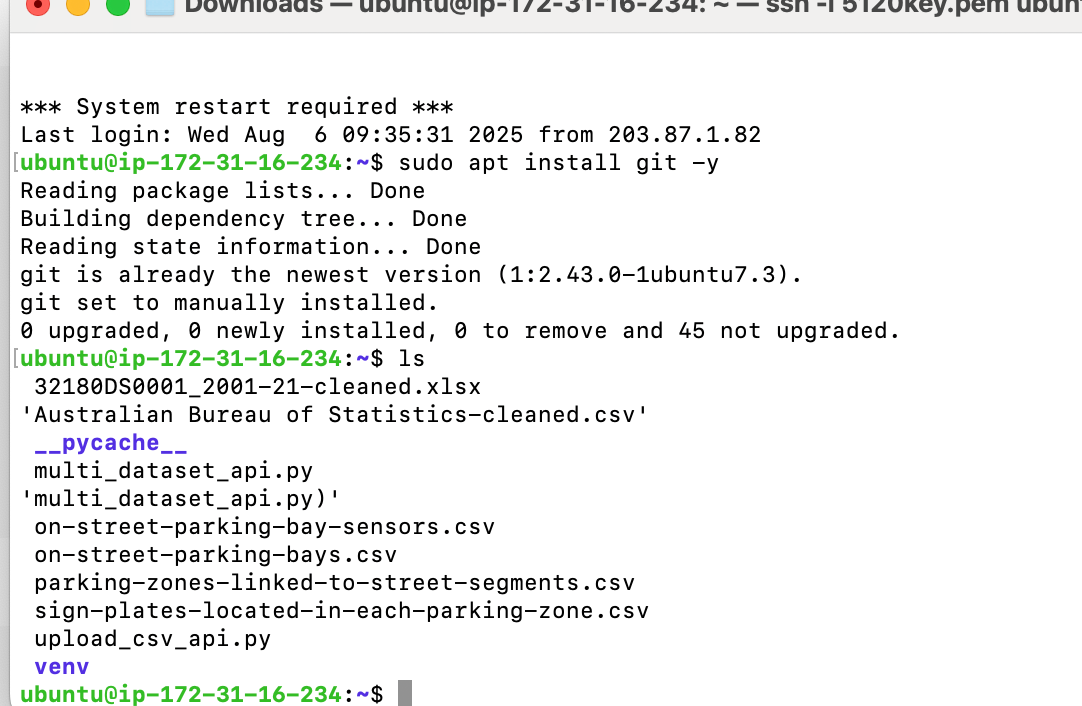
chmod 400 5120key.pem

sudo apt update && sudo apt upgrade -y

sudo apt install python3 python3-pip -y

pip3 install fastapi uvicorn

sudo apt install git -y



依赖

pip install fastapi uvicorn pandas

完整fast Api

from fastapi import FastAPI, HTTPException

import pandas as pd

import os

app = FastAPI()

# Supported file extensions

SUPPORTED\_EXTENSIONS = ['.csv', '.xlsx']

# List all files in the current directory with supported extensions

def list\_supported\_files():

return [

f for f in os.listdir(".")

if os.path.isfile(f) and os.path.splitext(f)[1] in SUPPORTED\_EXTENSIONS

]

# Endpoint to return all available file names

@app.get("/api/files")

def get\_all\_files():

return {"files": list\_supported\_files()}

# Endpoint to return the content of a specific file

@app.get("/api/file/{filename}")

def get\_file\_content(filename: str):

# Prevent directory traversal or invalid file access

if '..' in filename or '/' in filename or '\\' in filename:

raise HTTPException(status\_code=400, detail="Invalid filename")

# Check if the file exists

if not os.path.exists(filename):

raise HTTPException(status\_code=404, detail="File not found")

ext = os.path.splitext(filename)[1]

try:

if ext == '.csv':

df = pd.read\_csv(filename)

elif ext == '.xlsx':

df = pd.read\_excel(filename)

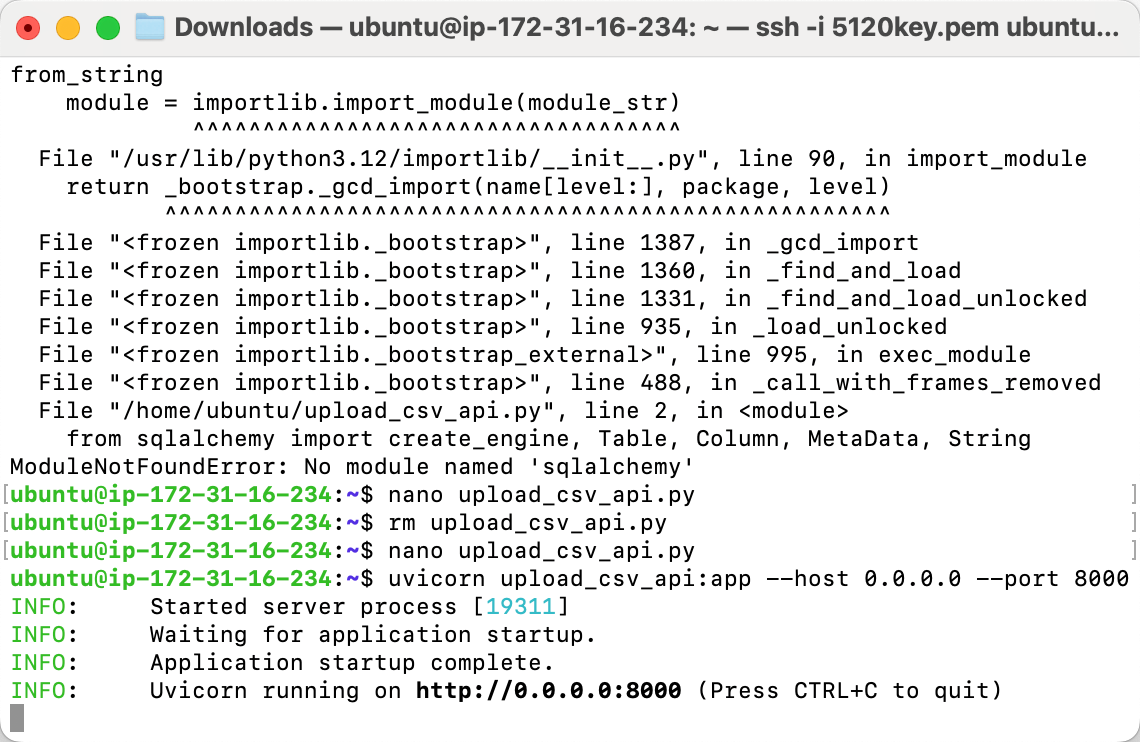
else:

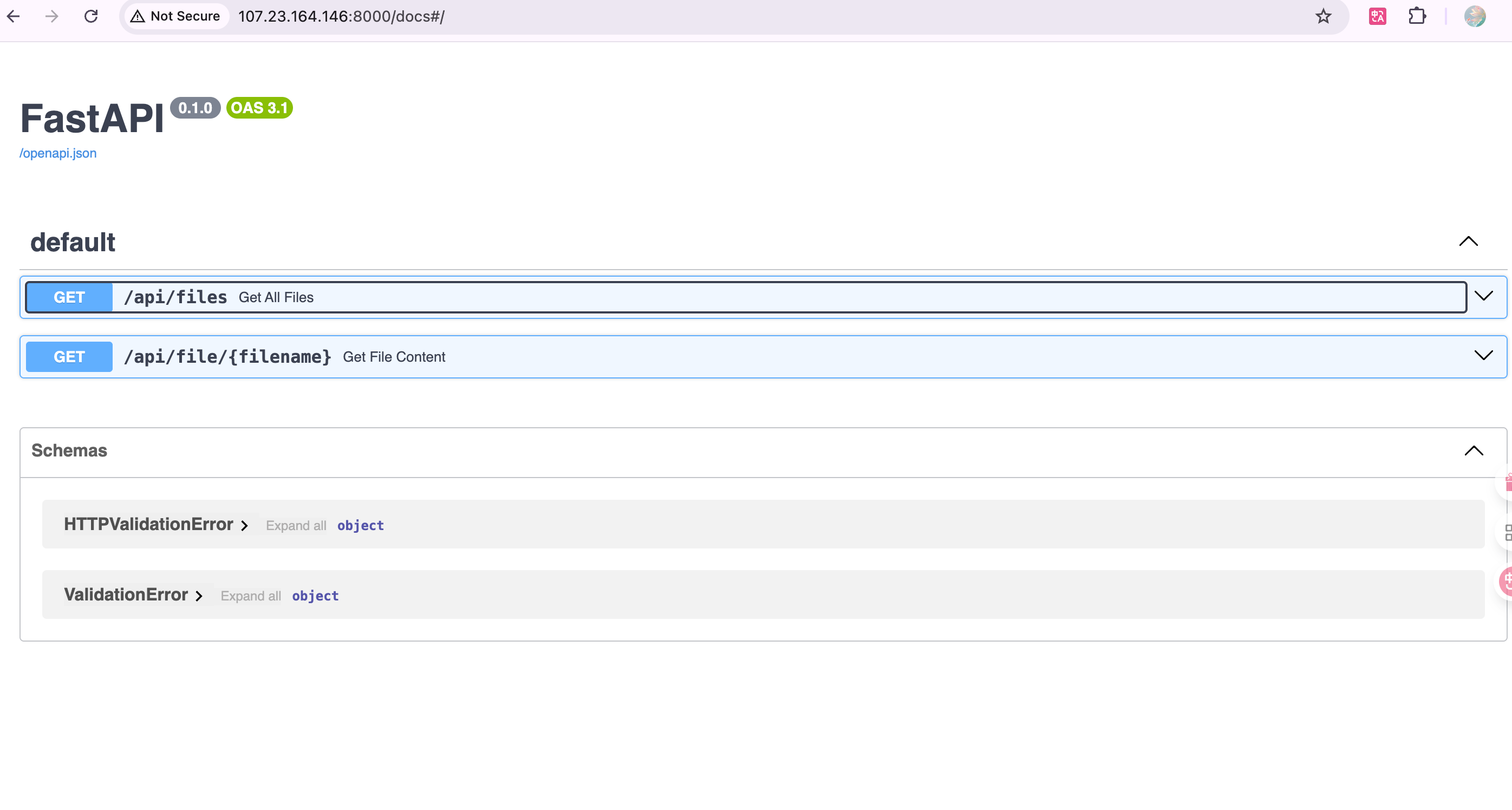
raise HTTPException(status\_code=400, detail="Unsupported file type")

return df.to\_dict(orient="records")

except Exception as e:

raise HTTPException(status\_code=500, detail=f"Failed to read file: {str(e)}")





把所有文件暴露给了前端

使用 FastAPI 暴露了本地目录中的所有 .csv 和 .xlsx 文件，并通过 Swagger 文档页面提供了查看和下载接口

· 云服务器：AWS EC2 Ubuntu 实例（公网 IP：107.23.164.146）

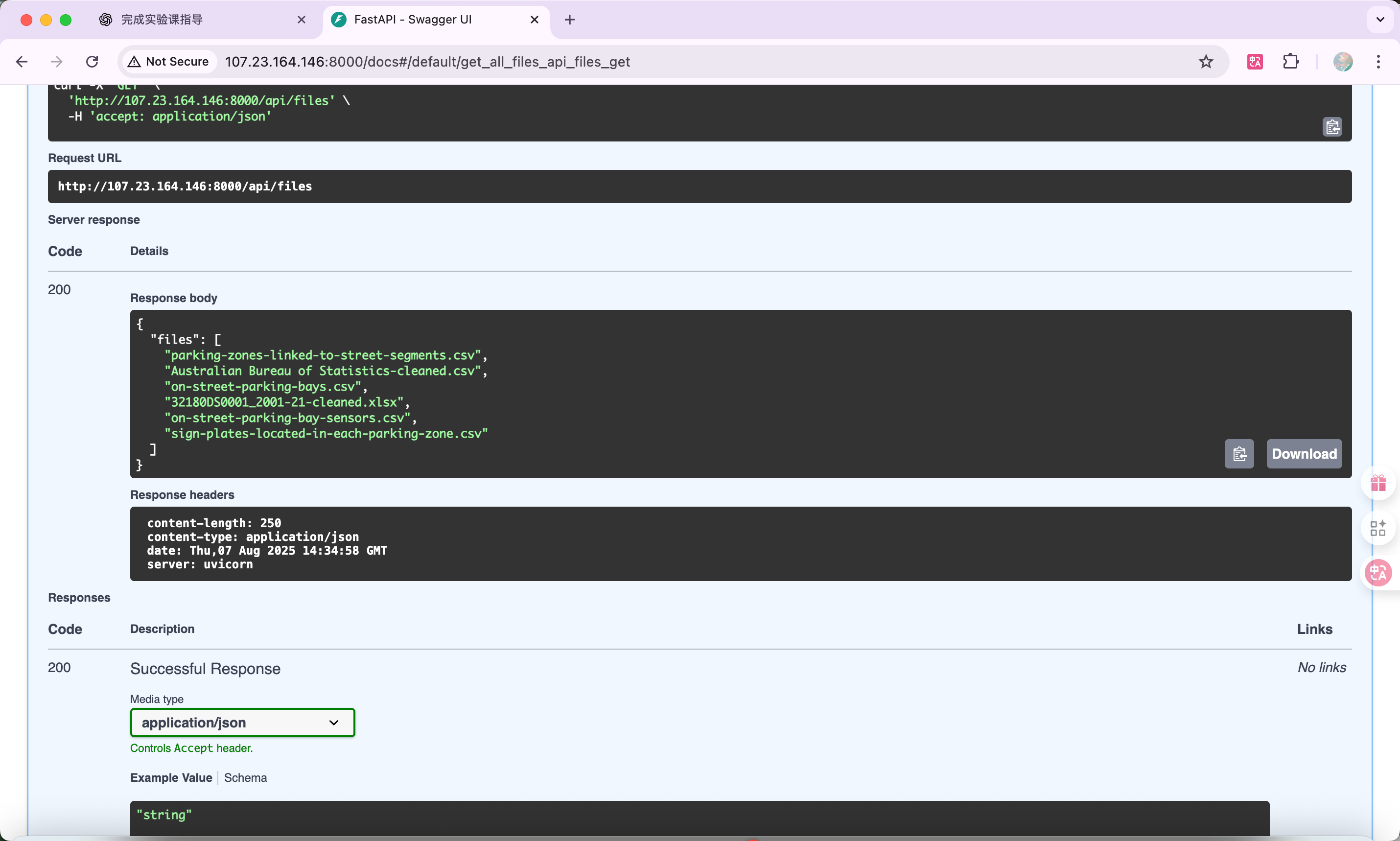
· · Python 3.12

· · FastAPI

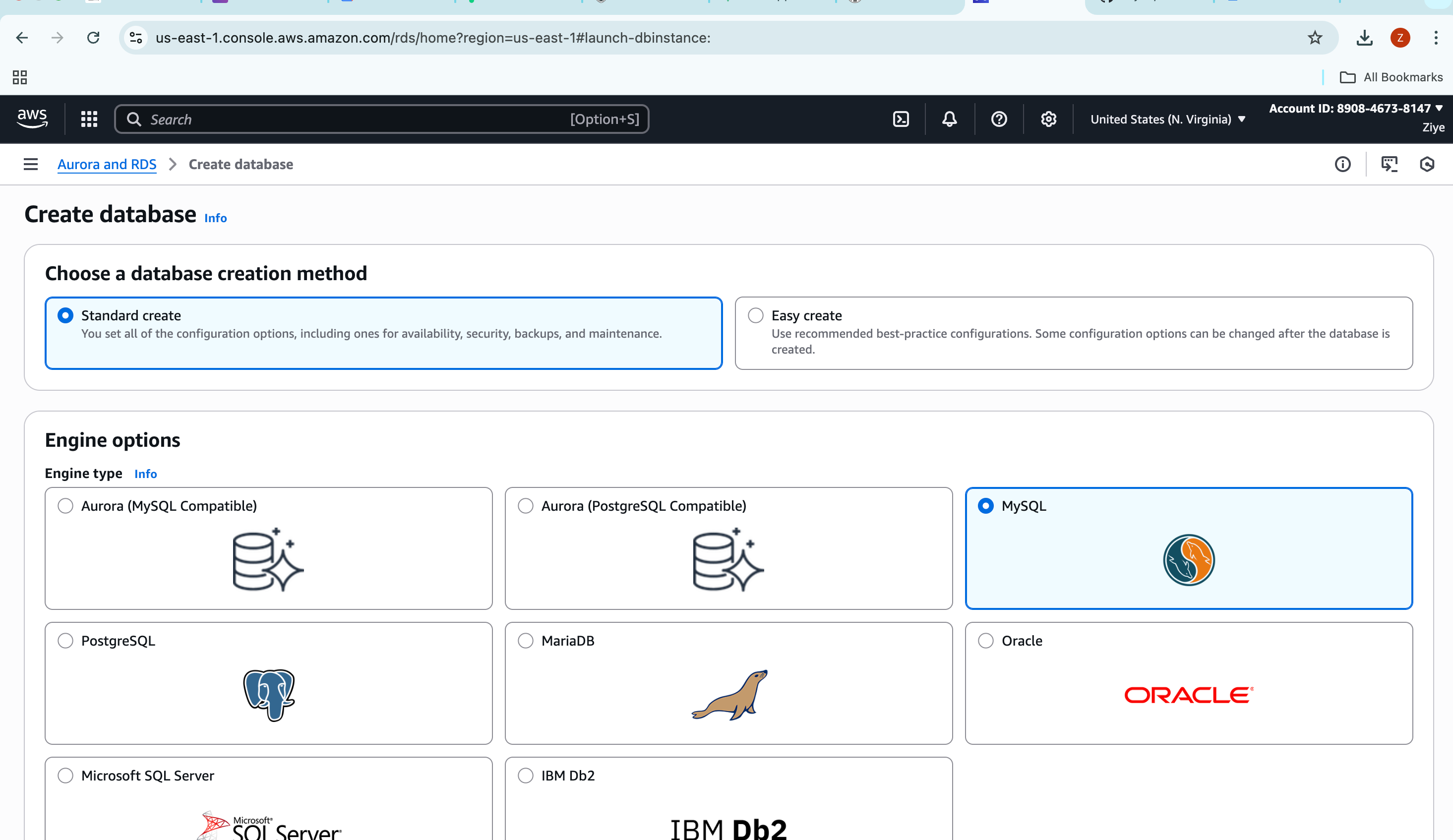
· · Uvicorn（FastAPI 的服务器）

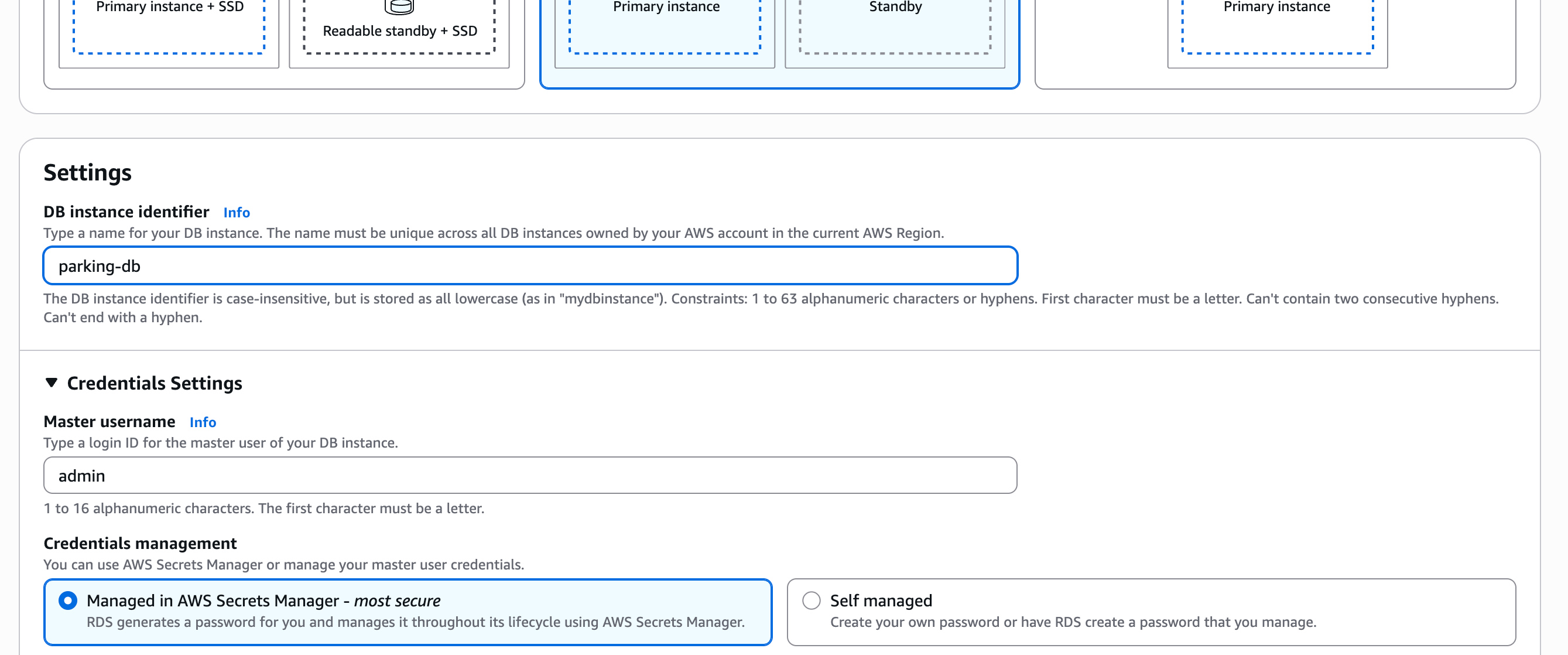
· · 运行文件：upload\_csv\_api.py

·



在云端创建数据库





注意开发端口3306

选择了 default 的 VPC security group，但是要想真正开放端口 3306（MySQL 默认端口），还需要去 EC2 的 Security Groups 设置里添加一条入站规则（Inbound Rule）

步骤：进入 EC2 控制台并修改 Security Group

回到 AWS 控制台主页

在搜索框输入 EC2，点击进入 EC2 Dashboard

在左侧菜单找到 Network & Security → 点进去 Security Groups

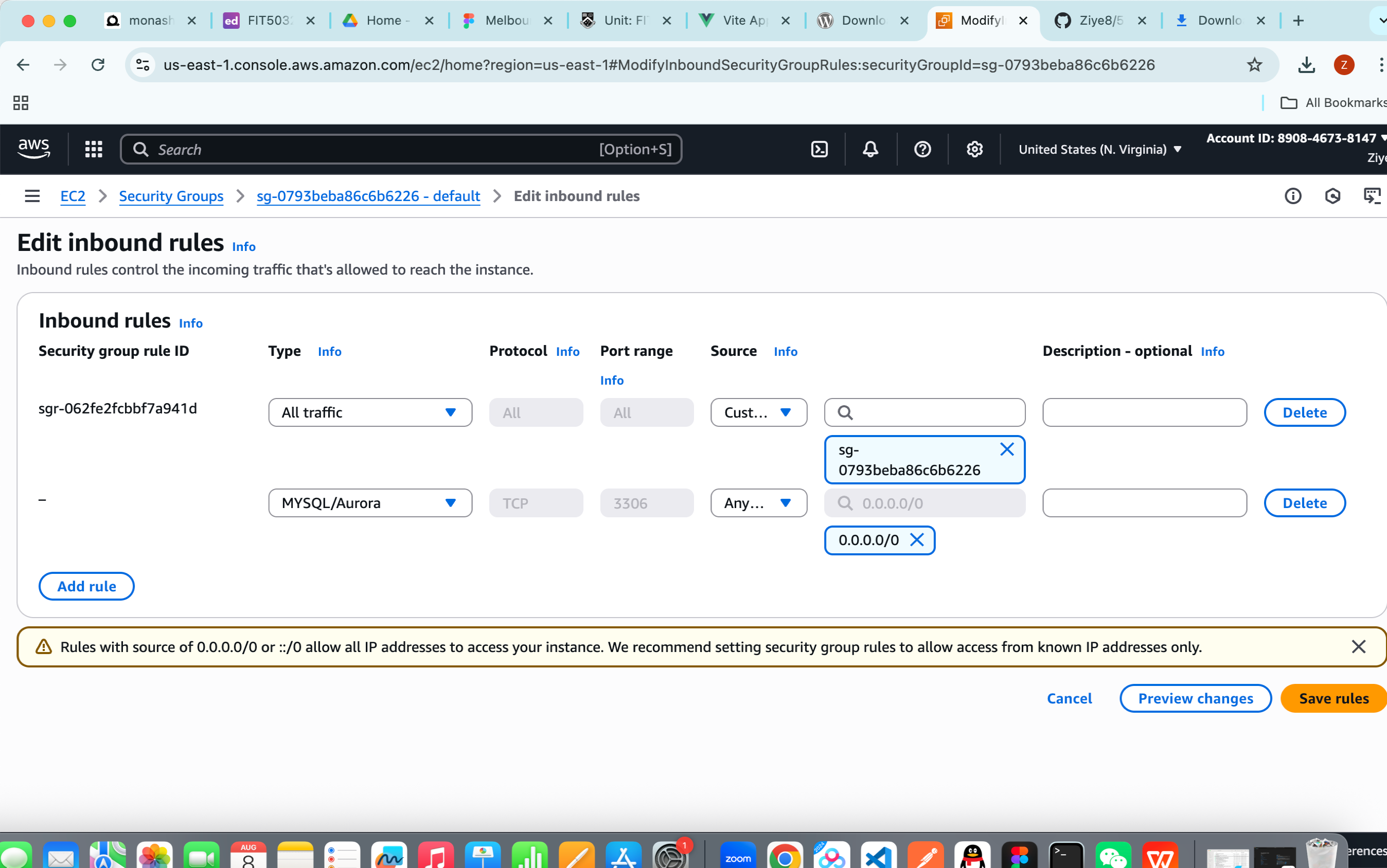
找到你在 RDS 创建中选用的 default Security Group，点击它的名称进入

点击 Inbound rules → 再点击 Edit inbound rules

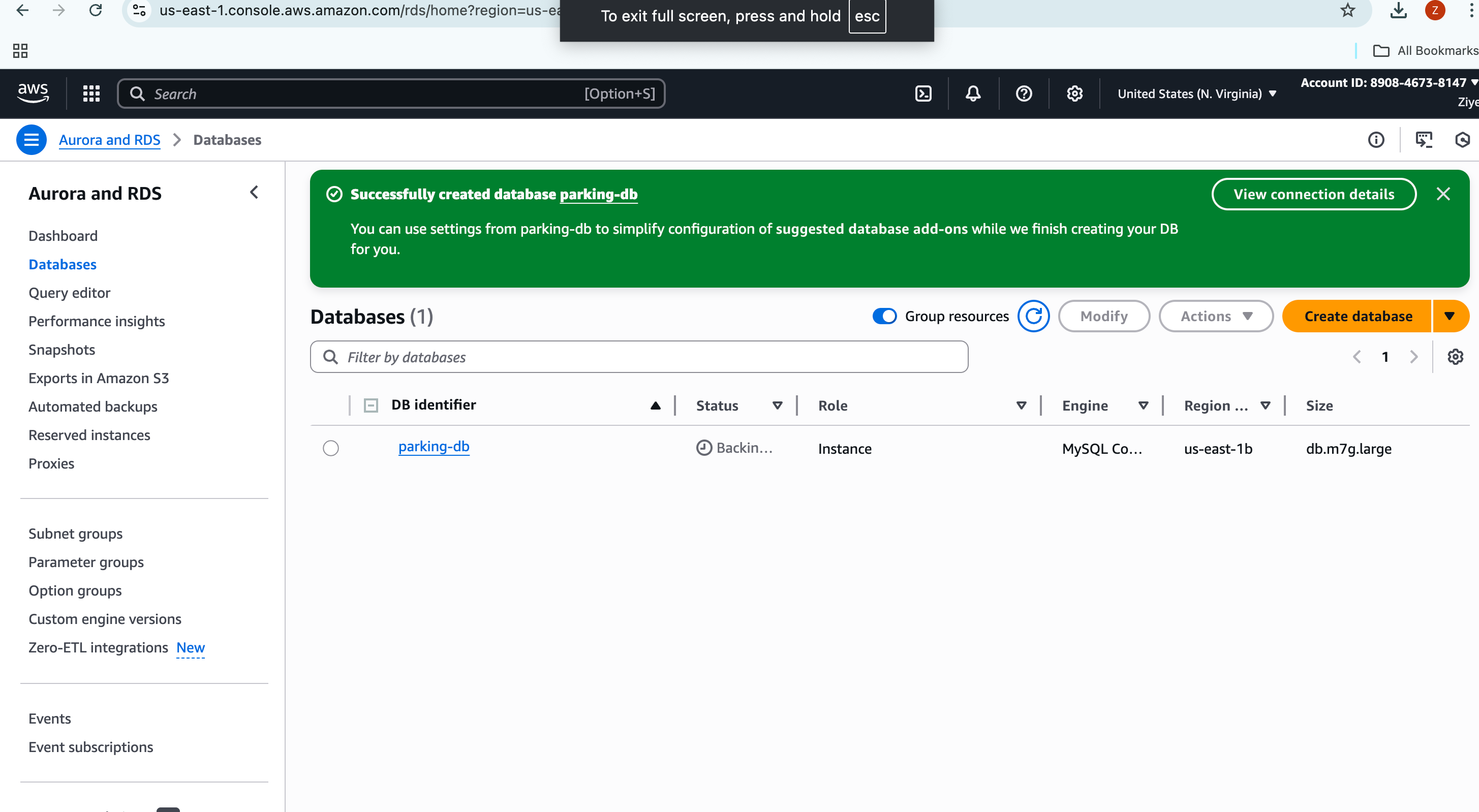
添加如下规则：

Type Protocol Port Range Source

MySQL/Aurora TCP 3306 Anywhere (0.0.0.0/0) ✅ or your EC2 IP only



这是database



使用 DBeaver 连接数据库

