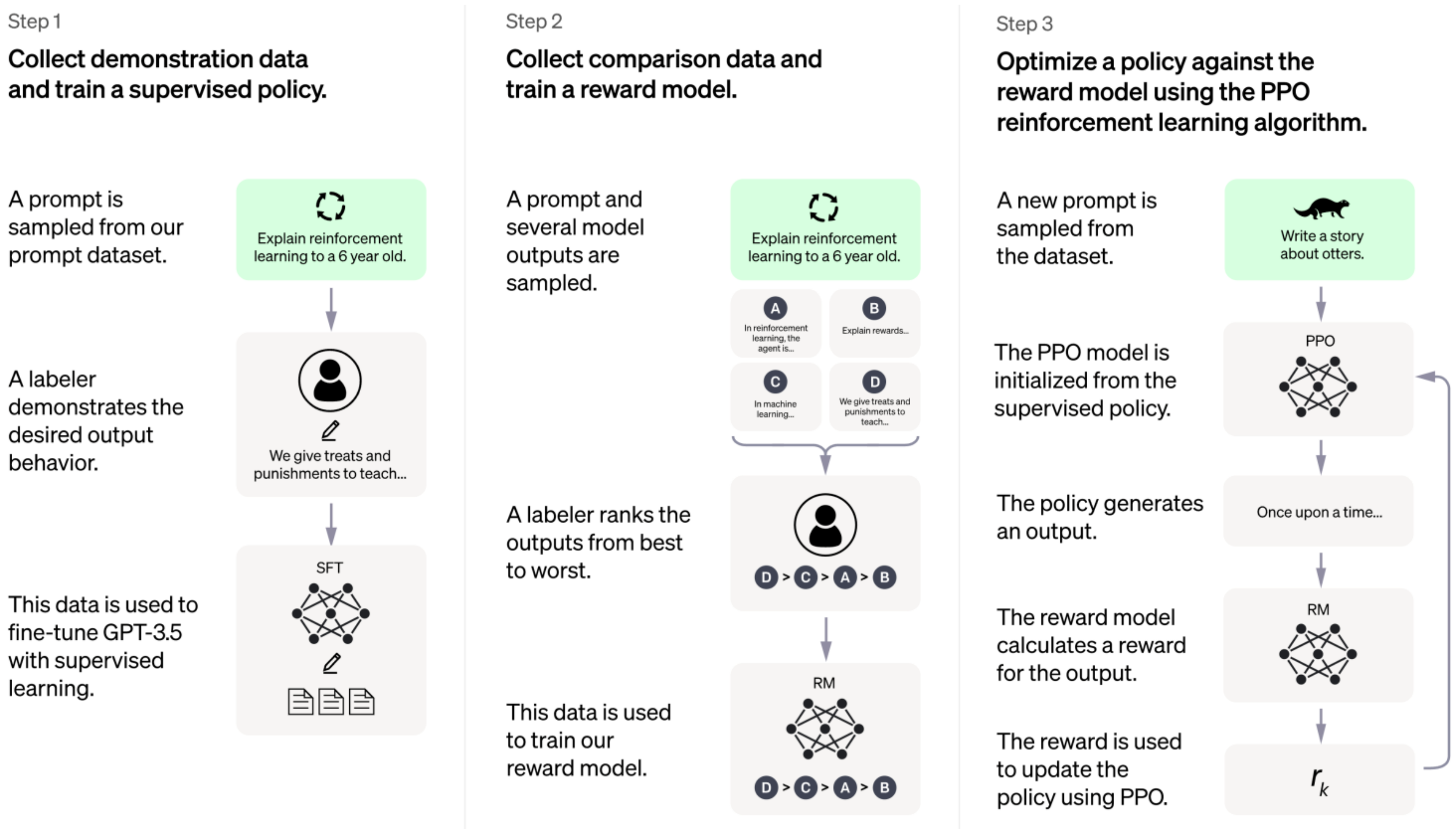
LLM application

Dr. Shuang LIANG

School of Computer Science and Technology
TongJi University

ChatGPT training process



Step 1

Collect demonstration data and train a supervised policy.

A prompt is sampled from our prompt dataset.

A labeler demonstrates the desired output behavior.

This data is used to fine-tune GPT-3.5 with supervised learning.

Step 2

Collect comparison data and train a reward model.

A prompt and several model outputs are sampled.

A labeler ranks the outputs from best to worst.

This data is used to train our reward model.

Step 3

Optimize a policy against the reward model using the PPO reinforcement learning algorithm.

A new prompt is sampled from the dataset.

The PPO model is initialized from the supervised policy.

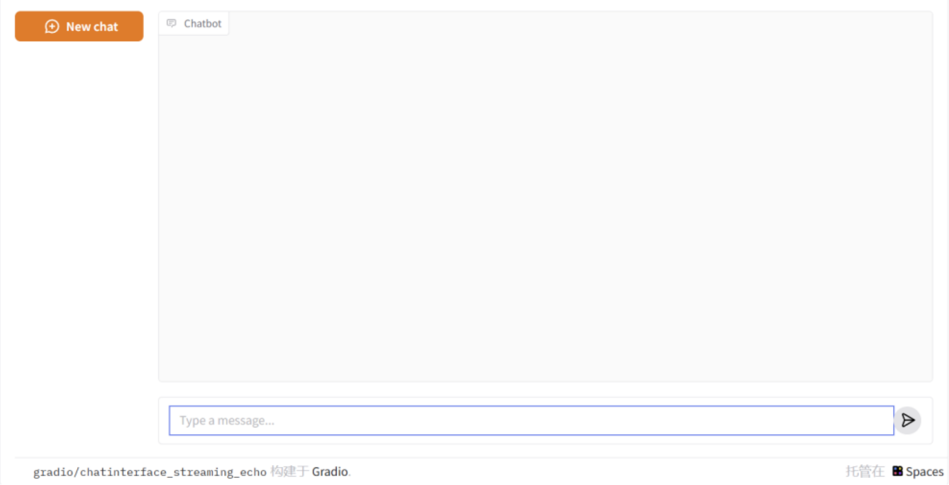
The policy generates an output.

The reward model calculates a reward for the output.

The reward is used to update the policy using PPO.

Explain reinforcement learning to a 6 year old.
We give treats and punishments to teach...
SFT
Explain reinforcement learning to a 6 year old.
A
In reinforcement learning, the agent is...
B
Explain rewards...
C
In machine learning...
D
We give treats and punishments to teach...
D > C > A > B
RM
D > C > A > B
Write a story about otters.
PPO
Once upon a time...
RM
r_k

gradio framework



- A Python library for quickly creating and sharing user interfaces for machine learning models. It simplifies the process of building a user interface (UI).
- Supports multiple types of input and output components, such as text boxes, image uploaders, sliders, and more.

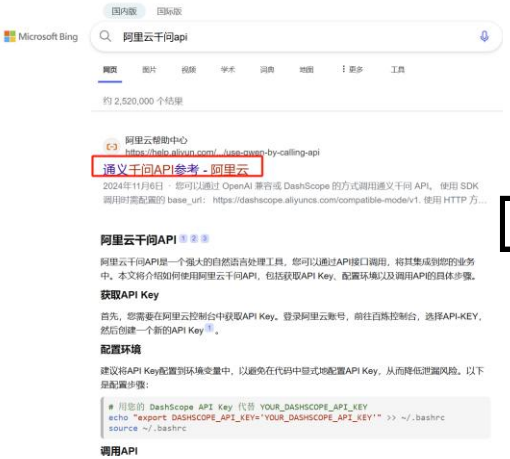
Steps to call LLM API in gradio

You can follow the steps below to use LLM and its API in gradio:

- Acquire llm api key
- install gradio
- Design your gradio app with python
- call&run LLM API in gradio project

Acquire llm api key

可以通过以下方式来获取API key(以Qwen为例):



阿里云千问api

约 2,520,000 个结果

阿里云帮助中心
https://help.aliyun.com/.../use-qwen-by-calling-api

通义千问API参考 - 阿里云

2024年11月6日 · 您可以通过 OpenAI 兼容或 DashScope 的方式调用通义千问 API。使用 SDK 调用时需配置的 base_url：https://dashscope.aliyuncs.com/compatible-mode/v1. 使用 HTTP 方...

阿里云千问API 1 2 3

阿里云千问API是一个强大的自然语言处理工具，您可以通过API接口调用，将其集成到您的业务中。本文将介绍如何使用阿里云千问API，包括获取API Key、配置环境以及调用API的具体步骤。

获取API Key

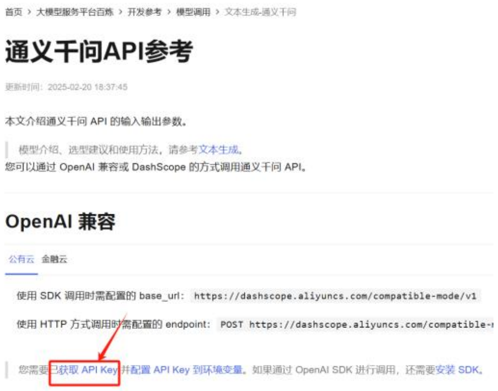
首先，您需要在阿里云控制台中获取API Key。登录阿里云账号，前往百炼控制台，选择API-KEY，然后创建一个新的API Key 1 。

配置环境

建议将API Key配置到环境变量中，以避免在代码中显式地配置API Key，从而降低泄漏风险。以下是配置步骤：

```
# 用您的 DashScope API Key 代替 YOUR_DASHSCOPE_API_KEY
echo "export DASHSCOPE_API_KEY='YOUR_DASHSCOPE_API_KEY'" >> ~/.bashrc
source ~/.bashrc
```

调用API


首页 › 大模型服务平台百炼 › 开发参考 › 模型调用 › 文本生成-通义千问
公有云
金融云

通义千问API参考

更新时间：2025-02-20 18:37:45

本文介绍通义千问 API 的输入输出参数。

> 模型介绍、选型建议和使用方法，请参考文本生成。

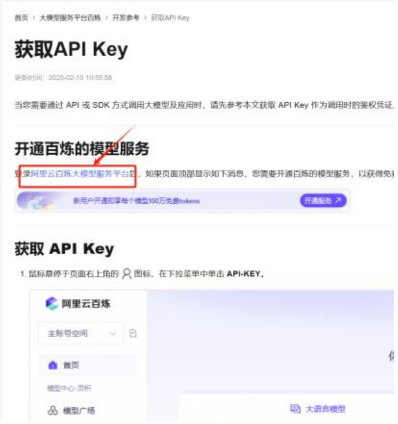
您可以通过 OpenAI 兼容或 DashScope 的方式调用通义千问 API。

OpenAI 兼容

使用 SDK 调用时需配置的 base_url：`https://dashscope.aliyuncs.com/compatible-mode/v1`

使用 HTTP 方式调用时需配置的 endpoint：`POST https://dashscope.aliyuncs.com/compatible-`

> 您需要已获取 API Key并配置 API Key 到环境变量。如果通过 OpenAI SDK 进行调用，还需要安装 SDK。


首页 › 大模型服务平台百炼 › 开发参考 › 获取API Key
新用户开通即享每个模型100万免费tokens
开通服务 ↗
阿里云百炼
主账号空间
首页
模型中心-灵积
模型广场
大语言模型

获取API Key

更新时间：2025-02-10 10:55:56

当您需要通过 API 或 SDK 方式调用大模型及应用时，请先参考本文获取 API Key 作为调用时的鉴权凭证。

开通百炼的模型服务

登录阿里云百炼大模型服务平台后，如果页面顶部显示如下消息，您需要开通百炼的模型服务，以获得免

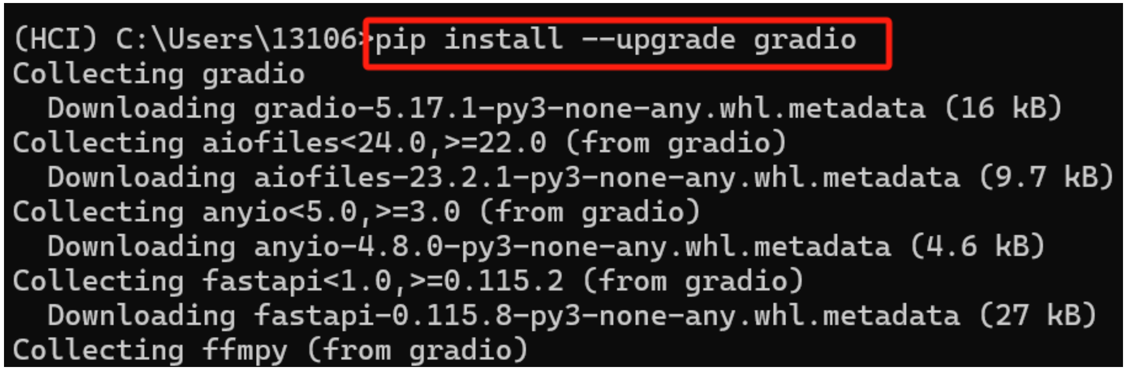
获取 API Key

1. 鼠标悬停于页面右上角的 图标，在下拉菜单中单击 **API-KEY**。

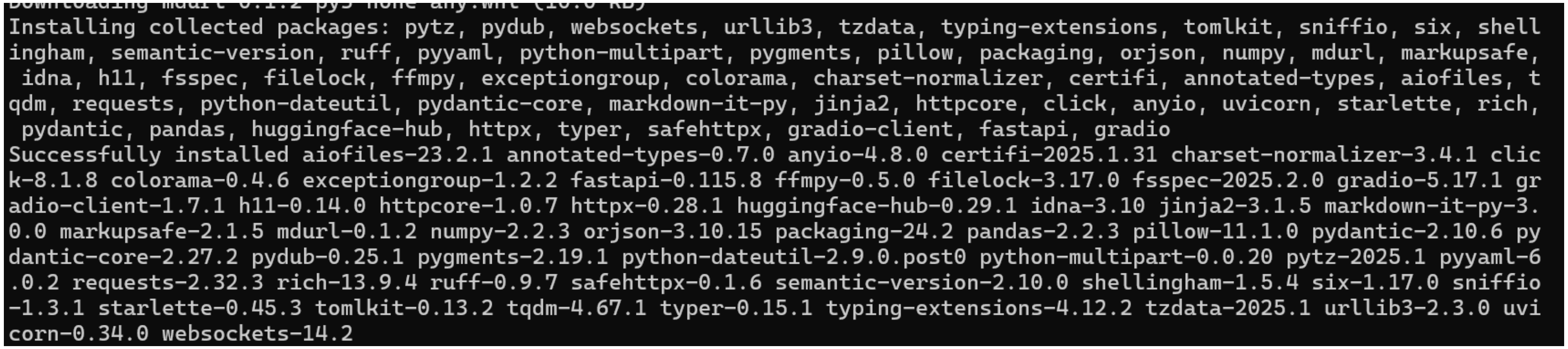
后续跟随该教程继续便可获取到API：
https://help.aliyun.com/zh/model-studio/developer-reference/get-api-key?spm=a2c4g.11186623.0.0.74b04823Yw4aeD

PS：同济大学AI应用创新平台好像也可以获取到API Key，若有兴趣也可以尝试一下

install gradio



```
(HCI) C:\Users\13106>pip install --upgrade gradio
Collecting gradio
  Downloading gradio-5.17.1-py3-none-any.whl.metadata (16 kB)
Collecting aiofiles<24.0,>=22.0 (from gradio)
  Downloading aiofiles-23.2.1-py3-none-any.whl.metadata (9.7 kB)
Collecting anyio<5.0,>=3.0 (from gradio)
  Downloading anyio-4.8.0-py3-none-any.whl.metadata (4.6 kB)
Collecting fastapi<1.0,>=0.115.2 (from gradio)
  Downloading fastapi-0.115.8-py3-none-any.whl.metadata (27 kB)
Collecting ffmpy (from gradio)
```



```
Downloading mdurl-0.1.2-py3-none-any.whl (10.0 kB)
Installing collected packages: pytz, pydub, websockets, urllib3, tzdata, typing-extensions, tomlkit, sniffio, six, shell
ingham, semantic-version, ruff, pyyaml, python-multipart, pygments, pillow, packaging, orjson, numpy, mdurl, markupsafe,
 idna, h11, fsspec, filelock, ffmpy, exceptiongroup, colorama, charset-normalizer, certifi, annotated-types, aiofiles, t
qdm, requests, python-dateutil, pydantic-core, markdown-it-py, jinja2, httpcore, click, anyio, uvicorn, starlette, rich,
 pydantic, pandas, huggingface-hub, httpx, typer, safehttpx, gradio-client, fastapi, gradio
Successfully installed aiofiles-23.2.1 annotated-types-0.7.0 anyio-4.8.0 certifi-2025.1.31 charset-normalizer-3.4.1 clic
k-8.1.8 colorama-0.4.6 exceptiongroup-1.2.2 fastapi-0.115.8 ffmpy-0.5.0 filelock-3.17.0 fsspec-2025.2.0 gradio-5.17.1 gr
adio-client-1.7.1 h11-0.14.0 httpcore-1.0.7 httpx-0.28.1 huggingface-hub-0.29.1 idna-3.10 jinja2-3.1.5 markdown-it-py-3.
0.0 markupsafe-2.1.5 mdurl-0.1.2 numpy-2.2.3 orjson-3.10.15 packaging-24.2 pandas-2.2.3 pillow-11.1.0 pydantic-2.10.6 py
dantic-core-2.27.2 pydub-0.25.1 pygments-2.19.1 python-dateutil-2.9.0.post0 python-multipart-0.0.20 pytz-2025.1 pyyaml-6
.0.2 requests-2.32.3 rich-13.9.4 ruff-0.9.7 safehttpx-0.1.6 semantic-version-2.10.0 shellingham-1.5.4 six-1.17.0 sniffio
-1.3.1 starlette-0.45.3 tomlkit-0.13.2 tqdm-4.67.1 typer-0.15.1 typing-extensions-4.12.2 tzdata-2025.1 urllib3-2.3.0 uvi
corn-0.34.0 websockets-14.2
```

Design your gradio app with python

可以参考的网址：

- https://www.gradio.app/guides/quickstart
- https://github.com/THUDM/ChatGLM2-6B/blob/main/web_demo.py
- https://blog.csdn.net/weixin_42426841/article/details/142128223

Assignment

1. 尝试使用gradio等软件，构建一个LLM的用户可视化页面，并且通过调用API的方式来调用不同的LLM模型（至少两个不同的公司的LLM模型）
2. 构建用户可视化的页面时，需要满足以下内容（总分5分）：

基础对话功能：可以成功的调用LLM模型的API来回答用户的问题，存在基本的输入输出的页面，不要求可以进行多轮对话。（必须）4分

多轮对话功能：在同一个对话下，记录同该用户之前的对话内容，一同输入给大模型，从而实现多轮对话功能。（可选，3选1即可）记1分

历史记录功能：可以记录用户之前同LLM的对话历史记录，并且可以选择之前的历史记录继续聊天（可选，3选1即可）记1分

其他可选的能够提升用户交互体验的内容（可选， 3选1即可）记1分

Report

- The report should answer the following questions (in English)， 总分5分:

1. 不同模型在进行API调用的时候是否有区别，如果有区别，区别在什么地方；1分

2. 自己在设计用户交互页面时的思路，自己为什么要这样子设计自己的页面，页面当中的组件的作用都是什么；1分

3. 大模型当中存在许多可以调整的参数（例如：采样温度、核采样阈值等）这些参数对大模型生成的回答有什么影响；1分

4. 不同的提示词对大模型的输出会产生不同的区别 ，在面对日常使用和专业问题的时候，你会更推荐什么风格的提示词书写方法呢？；1分

5. 至多不超过6页（不含封面等，只算正文部分），in English；1分

- Submit your work (code and report)
  - Prepare a readme file to illustrate how to run your program
  - Compress all the codes and the report into a zip file: ID_name_lab2.zip
  - Submitted to canvas.tongji.edu.cn