OAuth定义了四种角色：

* resource owner（资源所有者）
* resource server（资源服务器）
* client（客户端）：代表资源所有者并且经过所有者授权去访问受保护的资源的应用程序
* authorization server（授权服务器）：在成功验证资源所有者并获得授权后向客户端发出访问令牌

四种授权方式

密码模式（resource owner password credentials）

授权码模式（authorization code）

简化模式（implicit）

客户端模式（client credentials）

密码模式（resource owner password credentials）

这种模式是最不推荐的，因为client可能存了用户密码

这种模式主要用来做遗留项目升级为oauth2的适配方案

当然如果client是自家的应用，也是可以

支持refresh token

授权码模式（authorization code）

这种模式算是正宗的oauth2的授权模式

设计了auth code，通过这个code再获取token

支持refresh token

简化模式（implicit）

这种模式比授权码模式少了code环节，回调url直接携带token

这种模式的使用场景是基于浏览器的应用

这种模式基于安全性考虑，建议把token时效设置短一些

不支持refresh token

客户端模式（client credentials）

这种模式直接根据client的id和密钥即可获取token，无需用户参与

这种模式比较合适消费api的后端服务，比如拉取一组用户信息等

不支持refresh token，主要是没有必要