oauth2 四种授权使用场景

作者：limaoyuan
原文链接：https://ld246.com/article/1520841604473
来源网站：链滴

OAuth 2.0定义了四种授权方式。

- 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

refresh token的初衷主要是为了用户体验不想用户重复输入账号密码来换取新token，因而设计了refresh token用于换取新token

这种模式由于没有用户参与，而且也不需要用户账号密码，仅仅根据自己的id和密钥就可以换取新token，因而没必要refresh token

小结

- 密码模式（resource owner password credentials）（ 为遗留系统设计)(支持refresh token)
- 授权码模式（authorization code）（ 正宗方式)(支持refresh token)
- 简化模式（implicit）（ 为web浏览器应用设计)(不支持refresh token)
- 客户端模式（client credentials）（ 为后台api服务消费者设计)(不支持refresh token)

作者：go4it
链接：https://juejin.im/post/5a2933a96fb9a0452a3c3988
来源：掘金