OAuth 即：Open Authrization(开放授权)， 它是一个开放标准，允许用户让第三方应用访问该用户在某一网站上存储的私密资源，而无需将用户名和密码提供给第三方。比如我们熟知的通过qq/微信/微博等登录第三方平台。OAuth 1.0版本发布后有许多安全漏洞，所以在OAuth2.0里面完全废止了OAuth1.0，它关注客户端开发者的简易性，要么通过组织在资源拥有者和HTTP服务商之间的被批准的交互动作代表用户，要么允许第三方应用代表用户获得访问的权限。读起来有点绕口，其实原理也非常简单，请看下面讲解。

**一、首先我们要了解在OAuth2 认证和授权的过程中有这三个角色：**

1. 服务提供方：顾名思义，提供受保护的服务和资源的，用户在这里面存了很多东西。

2. 用户： 存了东西（照片，资料等）在服务提供方的人。

3. 客户端：服务调用方，它要访问服务提供方的资源，需要在服务提供方进行注册，不然服务提供方不鸟它呀。

**二、OAuth2 认证和授权的过程：**

1）用户想操作存放在服务提供方的资源；

2）用户登录客户端，客户端向服务提供方请求一个临时token;

3）服务提供方验证用户的身份后，给它一个临时token;

4）客户端获得临时token之后，将用户引导至服务提供方的授权页面，并请求用户授权。（在这个过程中会将临时token和客户端的回调链接/接口 发送给服务提供方 ---很明显服务提供方到时会回来call这个接口在用户认证并授权之后）

5）用户输入用户名密码登录，登录成功之后，可以授权客户端访问服务提供方的资源；

6）授权成功后，服务提供方将用户引导至客户端的网页（call第4步里面的回调链接/接口）；

7）客户端根据临时token从服务提供方那里获取正式的access token；

8）服务提供方根据临时token以及用户的授权情况授予客户端access token;

9）客户端使用access token访问用户存放在服务提供方的受保护的资源。

**三、拿access token的方法（Grant Type）有下面四种，每一种都有适用的应用场景：**

1. Authorization Code  
结合普通服务器端应用使用。

2. Implicit  
结合移动应用或 Web App 使用。

3. Resource Owner Password Credentials  
适用于受信任客户端应用，例如同个组织的内部或外部应用。

4. Client Credentials  
适用于客户端调用主服务API型应用（比如百度API Store）

四、使用Azure AD实现OAuth2认证授权 （只距离Client Credentials，这个在微服务项目中用的比较多，适合内部系统之间调用。其他的认证方式可以去Azure Active Directory看看相关文档）

1）申请Azure租户，其实就是用户。目前Azure China主要是世纪互联在代理，去上面申请一个试用账号（试用账号可以享受一个月的免费体验，好好珍惜哦）：<https://www.azure.cn/zh-cn/>

2）申请通过之后，访问 portal.azure.cn，进入到控制面板，找到Azure Active Directory，去里面创建一个应用程序，填写一些简单信息并创建成功之后，你再回到应用列表，会发现这个应用程序有一个application id。点进该应用程序，到设置里面，去为这个应用添加一个秘钥（secret key）。

3）上面两步完成之后，我们就可以获取access token了。打开Postman，请求这个路径：

[https://login.partner.microsoftonline.cn/<](https://login.partner.microsoftonline.cn/%3c)你的租户ID>/oauth2/token

请将URL完善。租户ID很好找，到Active Directory里面去，很容易找到你账号的租户ID，也可以直接鼠标移到你登录之后右上角的个人信息部分，会有一个悬浮框出来，上面一长串的GUID那个就是。

这个请求是POST请求，ContentType是application/www-urlencoded-formdata

详细参数如下：

**grant\_type**:client\_credentials

**client\_id**:这个填你的应用ID，你目前所在的应用，这里填刚才创建的那个application ID。

**client\_secret**: application ID对应的那个秘钥。

**resource**:这个填你要访问的那个应用的ID，可以直接填上面那个application ID（自己访问自己），如果你要访问其他应用就填其他应用的application ID，就要别人给你的client id有授权。

请求之后，就可以拿到access token了。可以根据这个access token访问resource指定的那个应用。

4）你自己还需要在代码里面实现与Azure AD的集成，这个可以查看官方文档，有示例代码。主要需要在代码里面配置一下resourceID，以及Azure的RSA加解密的URL，因为客户端请求你的应用的时候，会传access token，你要根据Azure提供的RSA算法来解密这个token，把它转成json格式的数据，这个json数据里面包含了请求进来的client拥有的权限，以及它的一些其他信息，你可以根据这个来判断给client开放哪些功能。