Spring Authorization Server (1) 认证、授权、oauth2概念和流程初步介绍

爱吃西瓜的胖娃 2023-09-18 1,223 阅读6分钟 关注

认证和授权

认证

可以理解为 **验证账号的合法性** 就称之为认证。

> 例如登录QQ的时候，我们输入【QQ号+密码】进行登录，如果QQ号没有注册企鹅服务器就会返回QQ号未注册；如果QQ密码错误，企鹅服务器就会QQ密码错误；这些都是验证账号合法性的过程，这样一个验证的过程就是认证。

> 【QQ号+密码】登录 ，这个只是认证的一种方式，常见的认证方式：【账号+密码】；【手机号+验证码】；【二维码扫码】等。

授权

授权也是就字面含义，授予权限，我目前理解授权有两种：

- oauth2的 授权给其他系统

> 一个授权操作，【获取你的昵称、头像】如果允许，就授权给掘金有了可以从微信服务器中获取你微信昵称、头像的权限。

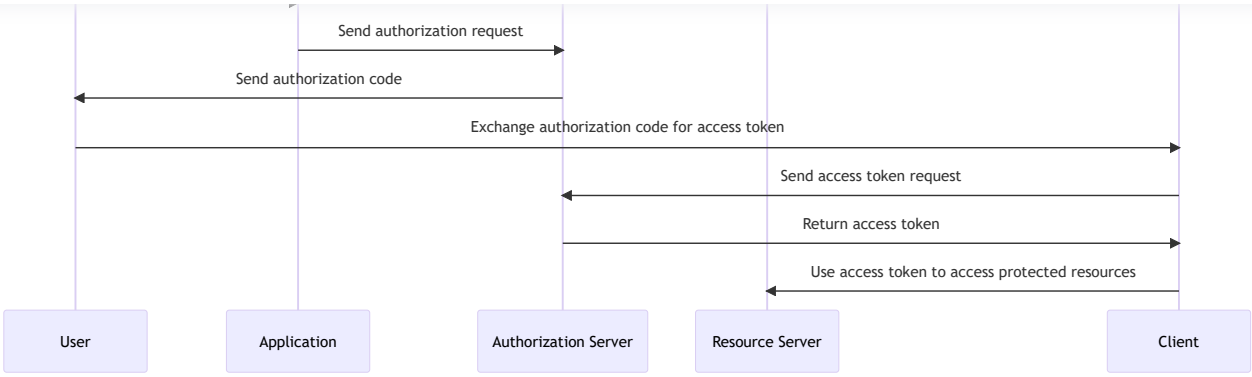
- 角色授权

> 还有一种授权，例如我们自己开发的一个管理系统，管理系统里面有 用户、角色、资源；不同角色下面有不同的资源；我们的赋予用户拥有角色，也就是赋予拥有了系统资源，当我登录成功后对应用户有哪些角色就有哪些资源，哪用户可以操作对应的。

oautrh2

> OAuth 2.0实际是业界定义标准的授权协议，这个协议也就是统一定义的oauth2.0的认证授权的流程，业界都按照这个流程标准去执行。也就是所有大厂都按照以下流程开发的oauth2认证授权流程 。

OAuth 2.0 授权码流程图



OAuth 2.0 的协议流程通常涉及以下角色

> - 资源所有者(Resource Owner)：资源的拥有者，通常是用户
> - 客户端（Client）：第三方应用程序，希望访问资源所有者的资源。客户端通过向授权服务器进行请求来获取访问令牌。
> - 授权服务器（Authorization Server）：负责验证资源所有者的身份，并向客户端颁发访问令牌，前提是资源所有者已经授权。
> - 资源服务器（Resource Server）：存储资源的服务器，可以接受访问令牌并提供资源给客户端。

OAuth 2.0 定义了几种不同的授权流程

> - 授权码授权流程（Authorization Code Flow）
> - 隐式授权流程（Implicit Flow）
> - 密码授权流程（Password Credentials Flow）
> - 客户端凭证授权流程（Client Credentials Flow）
> - 设备授权流程（Device Flow）

> 每种授权流程都有其特定的用例和安全性考虑。OAuth 2.0 主要用于实现用户授权和认证，而 OpenID Connect 则是在 OAuth 2.0 基础上构建的，用于实现身份验证和提供用户信息的协议。这两者一起在构建安全的身份验证和授权系统时发挥重要作用。

OpenID Connect (OIDC) 1.0 的理解

> 辅协议。它允许应用程序验证用户的身份，并获取有关用户的基本信息，同时利用 OAuth 2.0 提供的授权机制来访问受保护的资源。

OAuth 2.1 又是什么呢

> OAuth 2.1 是 OAuth 2.0 协议的更新版本，旨在提供更好的安全性和实用性。OAuth 2.1 修复了 OAuth 2.0 中的一些安全漏洞和缺陷，以使开发人员更容易实现安全的身份验证和授权流程。OAuth 2.1 保留了 OAuth 2.0 的核心概念，但在一些方面进行了细化和改进，以提供更清晰、更安全的授权框架

Spring Authorization Server 是什么?

官方是这样描述的

> `Spring Authorization Server` 是一个框架，提供 `OAuth 2.1` 和 `OpenID Connect 1.0` 规范以及其他相关规范的实现。它构建在 `Spring Security` 之上，为构建OpenID Connect 1.0 Identity Providers和OAuth2 Authorization Server产品提供了一个安全、轻量级和可定制的基础。

总结一下

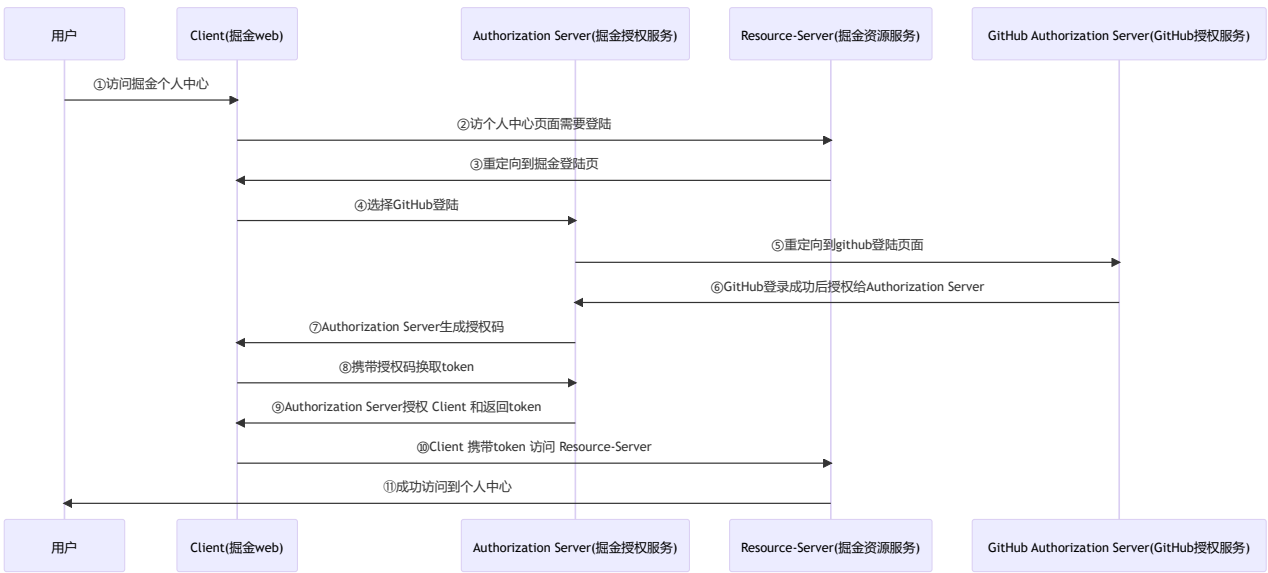
> `Spring Authorization Server` 实际上为了避免大家重复造轮子；每个大厂都要按照 `OAuth 2.1` 和 `OpenID Connect 1.0` 规范去开发，是不是每一个厂都要自己再写这样一套的代码，Spring 大哥就把这个事情代劳了最后写出了 `Spring Authorization Server` 框架给我们用，当然也有 Spring Security的要干的事情，结合二者 就不用重复造轮子了。

主要特点和组成部分

> OIDC 提供的机制进行登录，然后应用程序将收到一个 ID 令牌，证明用户已经通过身份验证。
>
> 2. **ID 令牌（ID Token）**：这是 OIDC 所引入的重要概念。ID 令牌是一个 JSON Web Token（JWT），其中包含有关用户身份的信息，如用户ID、姓名、电子邮件等。应用程序可以使用这个令牌来验证用户身份，避免了需要让用户提供用户名和密码。[到授权服务器获取token时，scope包含有openid是，会有id_token返回里面也包含了用户信息]
> 3. **用户信息端点（UserInfo Endpoint）**：OIDC 规范定义了一个用户信息端点，允许应用程序通过访问令牌获取有关用户的详细信息，如头像、地址等。[授权服务器上也有一个端点-/userinfo,当然每个授权服务器的端点命名都不同，客户端的配置说明]
> 4. **基于标准的扩展（Standard Extensions）**：OIDC 提供了一些扩展，以支持单点登录（Single Sign-On）和其他身份验证场景。例如，通过使用会话状态信息，用户可以在多个应用程序之间进行无缝的身份验证。
> 5. **与 OAuth 2.0 的结合**：OIDC 本质上是在 OAuth 2.0 的框架中添加了身份验证功能。它仍然使用 OAuth 2.0 的授权码、隐式、密码等流程，但添加了 ID 令牌和用户信息端点来支持身份验证和用户信息传递。

> OpenID Connect 1.0 旨在通过在 OAuth 2.0 基础上添加身份验证和用户信息传递的功能，为应用程序提供更安全、更便利的用户身份验证和授权机制。这对于构建安全、可信的身份验证系统以及支持单点登录等功能非常重要。

Spring Authorization Server 和spring Security 中OAuth 2.0 流程图 举一个例示例如下：



我们可以直接下载 spring-authorization-server 最新的源码（当前最新1.1.x），因为源码里面有demo，但是spring-authorization-server是基于gradle构建的，并不是基于maven构建的，如果没有配置gradle环境的，下面也为大家提供maven环境的demo，以便于直接上手

1. 👉 spring-authorization-server官方文档
2. 👉 spring-security官方文档
3. 👉 spring-authorization-server源码(源码里面有demo)
4. 👉 基于maven的构建的spring-authorization-server源码demo

对于 spring-authorization-server 框架完全讲透的太少了，此专栏一定是讲透的，能够让你少走很多弯路！！

标签： Spring Boot Spring Cloud 话题： 日新计划更文活动

本文收录于以下专栏

Spring Authorization Server 精讲 专栏目录

本专栏将深入讲解Spring Authorization Server在实践中的扩展点，希...

56 订阅 · 11 篇文章

订阅

上一篇 Spring Authorization Ser... 下一篇 Spring Authorization Ser...

评论 2

登录 / 注册 即可发布评论！

最热 最新

不错嘞通俗易懂，消化之后还能将自己理解的东西讲出来就很佩服 🤝

2月前 点赞 1 ···

爱吃西瓜的胖娃 作者 ：🤝

2月前 点赞 回复 ···

目录 收起

搜索建议 搜索关键词

Spring Authorization Server 文章说明和目录

Spring Authorization Server入门 (一) 初识SpringAuthorizationServer和OAuth2.1协议

OAuth2.0系列之基本概念和运作流程（一）

OAuth2.0系列之基本概念和运作流程（一）

Spring OAuth2 开发指南（一）：体系架构和开发概览

Spring Authorization Server (2) 授权服务、资源服务、客户端核心配置讲解

OAuth2.0协议入门（一）：OAuth2.0协议的基本概念以及使用授权码模式（authorization code）实现百...

Spring Authorization Server入门 (二) Spring Boot整合Spring Authorization Server

微服务安全Spring Security OAuth2 介绍(1)

SpringSecurity OAuth2 流程分析

精选内容

Spring Cloud Gateway 请求转发源码分析

程序猿秃头之路 · 50阅读 · 1点赞

自从我读透了Spring的事务传播性，用户每次都兑奖成功了！！

掉头发的王富贵 · 237阅读 · 4点赞

从单节点到集群：使用Redis解决负载均衡后WebSocket在线聊天室通信难题

翼飞 · 78阅读 · 1点赞

Spring Event 的幕后故事

不爱总结的麦穗 · 85阅读 · 4点赞

为你推荐

SpringSecurity+OAuth2.0

阿龙不写BUG 2年前 1.3k 15 1 后端

关于 OAuth2.0 详解

蛋黄派万岁 3年前 623 1 评论 前端

OAuth2.0与前端无感知token刷新实现

zhangwinwin 3年前 6.8k 60 8 JavaScript

【揭秘OAuth协议 — Java安全认证框架的核心基石】 从初识到精通，带你领略OAuth协议...

洛神灬殇 6月前 2.6k 15 2 后端 Java 网络协议

OAuth2.0授权码模式实战

码农参上 3年前 894 1 评论 Java

Oauth2.0及五种授权协议

思达帕克 3年前 1.5k 1 1 Spring Boot

微信授权登录移动端流程&多平台确定唯一用户

是江迪呀 8月前 514 3 评论 前端 后端 Java

OAuth2 & OIDC(informal essay)

Turman 3年前 552 5 1 Java

🚀SpringSecurity+OAuth2+JWT认证服务

冰块学融化 9月前 3.4k 20 评论 Java

Web网页应用集成Google API

算法不过是小case啦 7月前 378 点赞 评论 Google JavaScript

OAuth2.0基础及分布式认证管理系统的分析

xxsd 3年前 1.3k 3 评论 安全

关于登录授权的小分享

七彩祥云至尊宝 2年前 1.2k 13 评论 Android Java

最详细的一篇关于Oauth2的认证模式

唐宋xy 3年前 6.9k 14 1 Java

Spring 全家桶之 Spring Security（二）

RiemannHypo 2年前 764 57 评论 Spring