Spring Authorization Server常见问题解答(FAQ)

叹雪飞花 2023-09-17 928 阅读14分钟

关注

常见问题解答

1. 访问授权申请(/oauth2/authorize)接口跳转到默认登录页面，登录成功后响应错误码999

错误示例

```json
{"timestamp":"2023-06-24 01:08:42","status":999,"error":"None"}
```

可能造成该问题的原因：

1. 登录页面的某些静态资源被拦截了，在资源服务器中放行登录页面的所有静态资源
2. 未放行路径 `/error` ，当登录页面的某些静态资源不存在导致404时会跳转到/error处理，未放行该路径会导致请求重定向至登录页面

以上问题排查建议：

> 浏览器打开登录页面(http://127.0.0.1:8080/login)，然后按F12，看一下控制台中有哪些请求是302并且被重定向至登录页面的

2. 访问授权申请(/oauth2/authorize)接口跳转到默认登录页面，登录成功后跳转回来时授权申请(/oauth2/authorize)接口响应400错误

检查数据库中是否存在授权申请使用的客户端信息，因为最终客户端信息是在数据库中存储着的。

现在可能有些是存入redis中的，所以根据客户端存入位置去对应的库检查客户端信息。

3. 访问授权申请(/oauth2/authorize)接口跳转到默认登录页面，登录成功后跳转回来时授权申请(/oauth2/authorize)接口响应404错误

> **在添加认证服务配置与资源服务配置时两个过滤器链不要添加 `Order` 注解，以防认证服务配置被覆盖**
> **如果有网关代理，记得认证服务配置中的签发地址(issue)中需要添加网关的代理路径**

4. 在PKCE流程中通过token(/oauth2/token)接口获取token时，响应invalid_grant

错误示例

```json
{"error":"invalid_grant"}
```

可能造成该问题的原因

> 1. 授权码错误
> 2. 客户端id错误
> 3. 回调地址错误(跟请求/oauth2/authorize时携带的不一致)
> 4. 授权码过期
> 5. 生成code_challenge的算法有问题

5. 在OAuth2流程中通过token(/oauth2/token)接口获取token时，响应invalid_client

错误示例

```
{"error":"invalid_client"}
```

可能造成该问题的原因

> 1. 客户端id错误

6. client 授权登录后 如何退出呢?

Spring Security 提供了退出的端点：/logout

7. 直接配置 @PreAuthorize注解不生效

检查是否添加以下两个注解

java 复制代码

```
@EnableWebSecurity
@EnableMethodSecurity(jsr250Enabled = true, securedEnabled = true)
```

详见本系列的第九篇文章: Spring Authorization Server入门 (九) Spring Boot引入Resource Server对接认证服务

8. 客户端对接认证服务时出现[authorization_request_not_found]异常

认证服务器和客户端在同一个机器上时不能使用同一个ip，例如127.0.0.1，在存储cookie时不会区分端口的，比如127.0.0.1:8000和127.0.0.1:8080这两个，他们的cookie是同一个的，后者会覆盖前者；如果配置认证服务的地址是127.0.0.1:8080然后通过127.0.0.1:8000去访问客户端则会在登录后出现 `[authorization_request_not_found]` 异常，**详见spring-security issues 5946**

如果使用的是域名，可以解析两个子域名，一个解析到认证服务，一个解析到客户端服务

9. 如果不用这个web页面登录，有个接口，然后用安卓界面登录呢，应该用什么处理方式?

移动app和pc的app用的比较多的是PKCE模式，如果不想跳转到web登录页面就用自定义grant_type的方式添加一种认证并获取token的grant，比如系列文章中的自定义grant_type，那种是访问接口就直接响应access token了

10. oidc中的idToken到底有什么用？一路看过来也没看到有用这个token的地方

idToken中包含了用户信息，解析后可以直接获取用户信息，不用再请求服务器了

11. 使用自定义的UserDetailsService登录时出现序列化问题

异常堆栈描述

> java.lang.IllegalArgumentException: The class with com.example.entity.Oauth2BasicUser and name of com.example.entity.Oauth2BasicUser is not in the allowlist. If you believe this class is safe to deserialize, please provide an explicit mapping using Jackson annotations or by providing a Mixin. If the serialization is only done by a trusted source, you can also enable default typing. See github.com for details

解决方案

实体类添加两个注解：@JsonSerialize与@JsonIgnoreProperties(ignoreUnknown = true)

`@JsonSerialize`：添加JsonMixin

`@JsonIgnoreProperties(ignoreUnknown = true)`：序列化时忽略未知字段

12. 按照教程搭建起来，结果登录时一直提示用户名密码不对

可能是注入了一个UserDetailsService，账号密码跟文中不同，但是使用的账号密码却是文章的账号密码

13. 为什么客户端的认证信息要在请求头中添加Authorization这个请求头，header的Authorization 参数值为Basic+空格+base64(clientId:clientSecret)

这是oauth2协议定的标准，客户端的认证方式设置为BasicAuth时认证信息是在header中是这么个格式，以base64编码后加上前缀放入header中，详见本系列的第一章：Spring Authorization Server入门 (一) 初识SpringAuthorizationServer和OAuth2.1协议，里边介绍了客户端的各种认证方式

14. 要怎样继承改写DaoAuthenticationProvider，主要是继承了这个类，项目启动了发现并没有进入自己继承的这个DaoAuthenticationProvider的类操作。是啥问题

自己实现的没加 `@Component` 注解吗？如果加了那可能是在其它地方有provider实现被注入ioc中了；Security在初始化时会有个校验，好像是如果ioc中有多个 `DaoAuthenticationProvider` 的实例就只初始化默认的 `DaoAuthenticationProvider` 而不初始化子类，但是如果只有一个的话就会用ioc中的，所以不能多个实现都注入ioc

15. 使用Oracle数据库在授权申请时会抛出异常堆栈

框架问题，使用Oracle时确实会出现这种问题，如果需要解决可能需要重写AuthorizationService，详见issues 428

16. 如果自定义access_token以后随着权限的增多Jwt格式的access_token越来越长怎么办?

1. 使用匿名token(opaque token)，匿名token的长度都是固定的。
2. 可以自己在响应access_token时包装一层加密算法，减小token的长度，如下。

java 复制代码

```java
authorizationServerConfigurer
    .tokenEndpoint(tokenEndpoint -> tokenEndpoint
        // 自定义access_token响应
        .accessTokenResponseHandler(accessTokenResponseHandler)
    );
```

如果生成/响应token时有自定义操作，则解析时做好对应处理。

17. 客户端登录时跳转到客户端的登录页面并提示错误信息 `Bad Crendentials`

2. 获取用户信息失败
3. yml配置中用户名字段配置错误(用户信息接口响应的数据中没有该字段)

yml 复制代码

```yml
spring:
  security:
    oauth2:
      client:
        # oauth登录提供商
        provider:
          # 这里是oauth2登录提供商，自定义的，但引用时要对应，针对oauth2登录的特殊配置，指定使用该客户端
          github:
            # 这里就是上边说的用户名字段，详见下方说明1
            user-name-attribute: login
```

说明1：如果配置在这里的值在用户信息接口的响应数据中不存在则也会提示 Bad Crendentials，这里之所以需要配置这个字段是因为使用oauth2登录后，客户端会将用acce_token获取的用户信息以map的方式存储，Principal对象调用getName时是以该配置当做key来获取用户名的，并校验是否为空，为空则抛出异常，所以说该配置必须在用户信息响应数据中存在。

18. PKCE模式是什么意思，常用在什么场景下?

PKCE 是 Proof Key for Code Exchange 的缩写，PKCE 是一种用于增强授权码模式安全性的方法，它可以防止恶意应用程序通过截获授权码和重定向 URI 来获得访问令牌。PKCE 通过将随机字符串（code_verifier）和其 SHA-256 哈希值（code_challenge）与授权请求一起发送，确保访问令牌只能由具有相应 code_verifier 的应用程序使用，保障用户的安全性。

【OAuth 2.0 协议扩展】PKCE 扩展协议：**为了解决公开客户端的授权安全问题**

「面向对象」public 客户端，其本身没有能力保存密钥信息（恶意攻击者可以通过反编译等手段查看到客户端的密钥 client_secret， 也就可以通过授权码 code 换取 access_token， 到这一步，恶意应用就可以拿着 token 请求资源服务器了）

「原理」PKCE 协议本身是对 OAuth 2.0 授权码模式 的扩展， 它和之前的授权码流程大体上是一致的， 区别在于在向授权服务器的 authorize endpoint 请求时，需要额外的 code_challenge 和 code_challenge_method 参数；向 token endpoint 请求时， 需要额外

官网How-to: Authenticate using a Single Page Application with PKCE一文中说明了单页面应用如何使用PKCE模式获取认证，从这里可以看出PKCE模式适用于安全系数不高的客户端中，因为单页面应用在浏览器运行时，用户打开F12可以直接看到源码，从而获取客户端id与秘钥，桌面应用同理，反编译之后就能拿到，所以推出了"通过将随机字符串（code_verifier）和其 SHA-256 哈希值（code_challenge）与授权请求一起发送"的方案，因为code_verifier是随机生成的，攻击者无法提前知道code_verifier值，也就无法通过后端的校验。

19. oidc与传统的oauth有啥区别

这里引用一位知乎网友的回答：www.zhihu.com/question/59...

20. 实现 AuthenticationSuccessHandler 和 AuthenticationFailureHandler 这两个接口看代码只是返回给前端了对应成功或失败状态的json，前端拿这个json用在什么地方呢?

在前后端分离的授权码模式中前端与认证服务的交互都应该以json的形式交互，不应该重定向，所以后端实现这两个interface后只是响应个JSON，前端收到登录成功/失败响应后作出对应的处理，成功就获取地址栏参数target(认证服务跳转登录之前处理，获取当前url并拼接至登录页面地址)并进行跳转(由前端跳转)，失败就弹框处理。

21. 如果项目中禁用session，前后端分离的nonceId不用从session获取那改需要怎么处理?

如果项目中禁用session，则需要由前端生成一个uuid当做nonceId的值，然后前端在发起授权申请(/oauth2/authorize)时需要带着这个参数，重定向到登录页面时也需要带着参数，提交登录时也需要带着，授权确认时也是一样的，所以说了这么一大堆核心就一个，**前端在与认证服务交互时，只要是需要认证信息就需要带着这个参数，我说的交互期间指的是oauth2的登录流程中，因为后续走完oauth2流程就有access_token了。**

22. 公司内部有多个业务系统，认证服务器需要为他们都创建一个client吗?

这个看自己选择，如果不想那么麻烦使用一个也是可以的；最好是提供一个管理平台，可以动态管理客户端。

上边第18个问题中有说过，PKCE模式就是为了解决该问题的。

24.使用Spring Authorization Server获取到的token，是不是就是sso了？一个token可以在多个业务系统中使用。

SSO是在多个应用系统中，用户只需要登录一次就可以访问所有相互信任的应用系统；相对于后端来说，只要是认证服务的资源服务器则获取一次access_token以后就都可以使用access_token来访问；但是对于前端来说，如果有两个域名不一样的子业务系统，那么在浏览器中它们之间无法共享token，需要走一遍oauth2的登录流程来获取access_token，但是对于浏览器来说认证服务的域名一致没有变，相对应的它们之间的session也没有变化，所以说当子业务系统走oauth2流程时也是不用登录就能获取到access_token的，这样也是符合SSO的标准的。

25. client中一直没明白scope有什么用，是相当于拥有某个权限吗，那某个客户端N个权限，是不是都可以放到scope里，有的话scope一个字段不会变得超级大吗？

scope 参数是用来约束客户端的权限的，跟用户权限（authorities）是不同的，在OAuth2流程中实际上授权的主体一直都是客户端，例如Spring Security OAuth2 Resource Server默认情况下解析access_token后里边只有客户端的scope而没有用户的权限；但是在日常开发中为了简化开发步骤，直接就使用登录用户的权限来替换客户端的scope，甚至有时会直接忽略客户端的scope，这样在鉴权时可以直接对登录用户鉴权，简化逻辑。

26. 没太明白/login/oauth2/code/messaging-client-oidc这个接口是干嘛的，什么时候用到？

实际上这是使用Spring Security OAuth2 Client提供的一个过滤器，它会固定拦截 `/login/oauth2/code/{registrationId}` ，当请求被拦截后会根据registrationId获取客户端信息，之后获取请求中携带的授权码，然后使用授权码获取token，最后再使用token获取用户信息，获取到用户信息后oauth2的流程也结束了，因为已通过oauth2获取到认证信息了，之后就会跳转到未登录之前的地址。

这个地址一般是在使用Spring Security OAuth2 Client对接认证服务时使用，认证服务回调至客户端，客户端根据授权码获取认证信息这些都是默认提供的，但是在yml中的配置一定要对应上。

```yaml
spring:
  security:
    oauth2:
      client:
        registration:
          # 这个'gitee'就是registrationId
          gitee:
            # 指定oauth登录提供者，该oauth登录由provider中的gitee来处理
            provider: gitee
            # 客户端名字
            client-name: Sign in with Gitee
            # 认证方式
            authorization-grant-type: authorization_code
            # 客户端id，使用自己的gitee的客户端id
            client-id: dd8de6dfa9674cc307e18ca75616a0ded06126ddc4f95098da36e1fbfa141d0a
            # 客户端秘钥，使用自己的gitee的客户端秘钥
            client-secret: 59b069e525b84cac8fcb854148b623743eefd6bbe9d54433c006ec0c2f785c4d
            # 回调地址
            redirect-uri: ${custom.security.issuer-url}/login/oauth2/code/gitee
            # 申请scope列表
            scope:
              - emails
              - projects
```

27. 授权码模式去掉授权确认页面，是不是就相当于oauth2.0的密码模式了?

对于用户来说看起来是这样的，但是实际上多两次重定向。

文章会记录可能遇到的问题，并给出一个解决方案，目前框架异常提示信息不完善，所以出现问题后很难排查，这里给出一些解决方案，让大家少走一些弯路；本篇文章持续更新中，欢迎各位读者指正、补充和完善，谢谢大家

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

本文收录于以下专栏

1 / 2

Spring Authorization Server 专栏目录

上一篇 Spring Authorization Server... 下一篇 Spring Authorization Server...

评论 17

平等表达，友善交流

0 / 1000 发送

最热 最新

端碗吹水

请问在前后端分离的页面中，使用了axios去调用资源服务器的接口，在没有认证的状态下会触发几个重定向，但重定向授权服务器的/oauth2/authorize接口时出现跨域问题，请求头中的Origin为null，请问作者有遇到过这个问题吗。

3月前 点赞 6

叹雪飞花 作者：这一块儿应该添加特殊处理的，针对axios的请求未登录时响应JSON，不应该让他重定向的，重定向的逻辑有问题的

3月前 点赞 回复

端碗吹水 回复 叹雪飞花 作者：那请问在我这个案例里就是对/oauth2/authorization/banbole-client-oidc接口的重定向特殊处理，如果是axios的请求则返回json是吗

3月前 点赞 回复

查看全部 6 条回复

用户9367754597345

请问通过网关向认证服务器获取access_token，再通过网关请求post请求/logout转发到认证服务器，显示注销成功跳转登录页了可是access_token仍然有效，能请求到资源

3月前 点赞 9 ···

叹雪飞花 作者：1. 没有调用撤销token端点
2.调用过撤销token端点，但是access_token是自包含token(jwt)，请求时未调用自省端点查看access_token状态(因为jwt是无状态的)。

3月前 点赞 回复 ···

用户9367754... 回复 叹雪飞花 作者：/logout接口内部有撤销token的操作吗，还是需要通过自定义方法调用对token撤销

3月前 点赞 回复 ···

查看全部 9 条回复

目录 收起

常见问题解答

1. 访问授权申请(/oauth2/authorize)接口跳转到默认登录页面，登录成功后响应错误码999
2. 访问授权申请(/oauth2/authorize)接口跳转到默认登录页面，登录成功后跳转回来时授权申请(...
3. 访问授权申请(/oauth2/authorize)接口跳转到默认登录页面，登录成功后跳转回来时授权申请(...
4. 在PKCE流程中通过token(/oauth2/token)接口获取token时，响应 invalid_grant
5. 在OAuth2流程中通过token(/oauth2/token)接口获取token时，响应 invalid_client
6. client 授权登录后 如何退出呢?
7. 直接配置 @PreAuthorize注解不生效
8. 客户端对接认证服务时出现[authorization_request_not_found]异常
9. 如果不用这个web页面登录，有个接口，然后用安卓界面登录呢，应该用什么处理方式?
10. oidc中的idToken到底有什么用？一路看过来也没看到有用这个token的地方
11. 使用自定义的UserDetailsService登录时出现序列化问题
12. 按照教程搭建起来，结果登录时一直提示用户名密码不对
13. 为什么客户端的认证信息要在请求头中添加Authorization这个请求头，header的Authorizati...
14. 要怎样继承改写DaoAuthenticationProvider，主要是继承了这个类，项目启动了发现并没有...
15. 使用Oracle数据库在授权申请时会抛出异常堆栈
16. 如果自定义access_token以后随着权限的增多Jwt格式的access_token越来越长怎么办?
17. 客户端登录时跳转到客户端的登录页面并提示错误信息Bad Crendentials
18. PKCE模式是什么意思，常用在什么场景下?

21. 如果项目中禁用session，前后端分离的nonceId不用从session获取那改需要怎么处理?
22. 公司内部有多个业务系统，认证服务器需要为他们都创建一个client吗?
23. 在前后端分离中，通过code换取token的时候需要传递客户端的id和密钥，那客户端密钥不是...
24.使用Spring Authorization Server获取到的token，是不是就是sso了？一个token可以在多个...
25. client中一直没明白scope有什么用，是相当于拥有某个权限吗，那某个客户端N个权限，是不...
26. 没太明白/login/oauth2/code/messaging-client-oidc这个接口是干嘛的，什么时候用到?
27. 授权码模式去掉授权确认页面，是不是就相当于oauth2.0的密码模式了?

相关推荐

Spring Data Redis工具类
208阅读 · 3点赞

Spring Authorization Server入门 (十四) 联合身份认证添加微信登录
1.2k阅读 · 5点赞

Spring Authorization Server 入门教程
615阅读 · 1点赞

SpringSecurityOAuth已停更，来看一看进化版本Spring Authorization Server
374阅读 · 0点赞

Spring Authorization Server入门 (十五) 分离授权确认与设备码校验页面
1.6k阅读 · 14点赞

为你推荐

Spring Authorization Server入门 (二) Spring Boot整合Spring Authorization Server
叹雪飞花 9月前 6.8k 31 86 Java

Spring Authorization Server入门 (十二) 实现授权码模式使用前后端分离的登录页面
叹雪飞花 8月前 4.8k 24 65 后端 Spring ... Spring

Spring Authorization Server入门 (十) 添加短信验证码方式登录
叹雪飞花 9月前 3.4k 20 9 Spring Spring ...

Spring Authorization Server入门 (八) Spring Boot引入Security OAuth2 Client对接认...

Spring Authorization Server入门 (十六) Spring Cloud Gateway对接认证服务

叹雪飞花 7月前 2.6k 17 44 Spring … Spring … 安全

Spring Authorization Server入门 (十三) 实现联合身份认证，集成Github与Gitee的OAu…

叹雪飞花 8月前 2.3k 13 51 Spring Spring … 安全

Spring Authorization Server入门 (十一) 自定义grant_type(短信认证登录)获取token

叹雪飞花 9月前 2.5k 15 39 Spring Spring … 安全

Spring Authorization Server入门 (七) 登录添加图形验证码

叹雪飞花 9月前 2.9k 18 4 Spring …

SpringBoot3.x最简集成SpringDoc-OpenApi

叹雪飞花 4月前 2.3k 17 评论 后端 Spring … Java

Spring Authorization Server入门 (九) Spring Boot引入Resource Server对接认证服务

叹雪飞花 9月前 1.8k 13 8 Spring Spring …

Spring Authorization Server优化篇：添加Redis缓存支持和统一响应类

叹雪飞花 8月前 1.7k 6 12 Spring Spring … 安全

Spring Authorization Server入门 (十五) 分离授权确认与设备码校验页面

叹雪飞花 7月前 1.6k 14 8 Spring … Spring Vue.js

Spring Authorization Server入门 (十九) 基于Redis的Token、客户端信息和授权确认信…

叹雪飞花 4月前 1.2k 8 19 Spring … 后端 Redis

Spring Authorization Server入门 (二十) 实现二维码扫码登录

叹雪飞花 2月前 935 16 6 Spring … Spring Java

Spring Authorization Server入门 (十七) Vue项目使用授权码模式对接认证服务

叹雪飞花 6月前 760 9 12 Vue.js 安全 Spring …