埋点平台OAuth2接口设计

# 概述

本文档主要讲解OAuth2表设计及接口设计。

## 接口基本设计

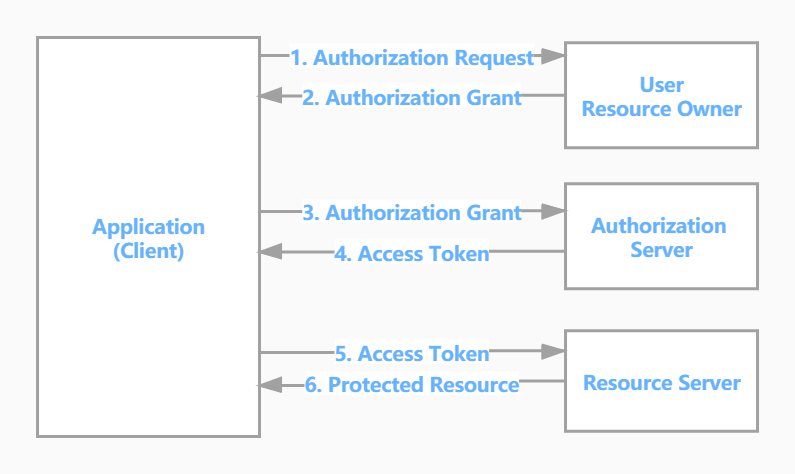
授权服务器和资源服务器都集成到一起，客户端访问接口时需要先请求授权服务器，拿到授权服务器返回的访问令牌access\_token，客户端拿到授权access\_token后就可以到资源服务器获取需要的资源。授权服务器访问令牌缓存到Redis中，下次读取从Redis中读取。

## OAuth2认证流程

**第一步：获取access\_token**

客户端通过客户端模式或密码模式接口获取access\_token

**第二步：获取资源**

客户端拿到授权服务器返回的access\_token去资源服务器访问所需资源

## E-R模型图：

图1（用户权限）



图2（应用）

# 数据字典

用户表sys\_user

|  |  |  |  |
| --- | --- | --- | --- |
| **字段名** | **类型** | **缺省值** | **说明** |
| id | bigint(20) | not null | 主键 |
| username | varchar(30) | not null | 用户名（唯一） |
| password | varchar(50) | not null | 密码 |
| nickname | varchar(50) | null | 昵称 |
| phone | varchar(20) | null | 手机号（唯一） |
| email | varchar(50) | null | 邮箱（唯一） |
| create\_time | timestamp | not null | 创建时间 |
| update\_time | timestamp | not null | 更新时间 |
| create\_user | bigint(20) | not null | 创建人ID |
| update\_user | bigint(20) | null | 更新人ID |
| logic\_delete | tinyint(1) | not null | 是否删除（0-否,1-是） |

角色表sys\_role

|  |  |  |  |
| --- | --- | --- | --- |
| **字段名** | **类型** | **缺省值** | **说明** |
| id | bigint(20) | not null | 主键 |
| parent\_id | bigint(20) | not null | 父ID |
| enname | varchar(50) | not null | 角色英文名称 |
| name | varchar(50) | not null | 角色名称 |
| description | varchar(200) | not null | 备注 |
| create\_time | timestamp | not null | 创建时间 |
| update\_time | timestamp | not null | 更新时间 |
| create\_user | bigint(20) | not null | 创建人ID |
| update\_user | bigint(20) | null | 更新人ID |
| logic\_delete | tinyint(1) | not null | 是否删除（0-否,1-是） |

权限表sys\_permission

|  |  |  |  |
| --- | --- | --- | --- |
| **字段名** | **类型** | **缺省值** | **说明** |
| id | bigint(20) | not null | 主键 |
| parent\_id | bigint(20) | not null | 父ID |
| enname | varchar(50) | not null | 权限英文名称 |
| name | varchar(50) | null | 权限名称 |
| url | varchar(255) | not null | 授权路径 |
| description | varchar(200) | null | 备注 |
| create\_time | timestamp | not null | 创建时间 |
| update\_time | timestamp | not null | 更新时间 |
| create\_user | bigint(20) | not null | 创建人ID |
| update\_user | bigint(20) | null | 更新人ID |
| logic\_delete | tinyint(1) | not null | 是否删除（0-否,1-是） |

用户角色表sys\_permission

|  |  |  |  |
| --- | --- | --- | --- |
| **字段名** | **类型** | **缺省值** | **说明** |
| id | bigint(20) | not null | 主键 |
| user\_id | bigint(20) | not null | 用户ID |
| role\_id | bigint(20) | not null | 角色ID |
| create\_time | timestamp | not null | 创建时间 |
| update\_time | timestamp | not null | 更新时间 |
| create\_user | bigint(20) | not null | 创建人ID |
| update\_user | bigint(20) | null | 更新人ID |
| logic\_delete | tinyint(1) | not null | 是否删除（0-否,1-是） |

角色权限表sys\_role\_permission

|  |  |  |  |
| --- | --- | --- | --- |
| **字段名** | **类型** | **缺省值** | **说明** |
| id | bigint(20) | not null | 主键 |
| permission\_id | bigint(20) | not null | 权限ID |
| role\_id | bigint(20) | not null | 角色ID |
| create\_time | timestamp | not null | 创建时间 |
| update\_time | timestamp | not null | 更新时间 |
| create\_user | bigint(20) | not null | 创建人ID |
| update\_user | bigint(20) | null | 更新人ID |
| logic\_delete | tinyint(1) | not null | 是否删除（0-否,1-是） |

应用表sys\_app

|  |  |  |  |
| --- | --- | --- | --- |
| **字段名** | **类型** | **缺省值** | **说明** |
| id | bigint(20) | not null | 主键 |
| app\_id | varchar(50) | not null | 应用ID |
| app\_secret | varchar(50) | not null | 应用秘钥（明文） |
| app\_name | varchar(50) | null | 应用名称 |
| description | varchar(20) | null | 描述 |
| create\_time | timestamp | not null | 创建时间 |
| update\_time | timestamp | not null | 更新时间 |
| create\_user | bigint(20) | not null | 创建人ID |
| update\_user | bigint(20) | null | 更新人ID |
| logic\_delete | tinyint(1) | not null | 是否删除（0-否,1-是） |

客户端信息（oauth\_client\_details）

|  |  |  |  |
| --- | --- | --- | --- |
| **字段名** | **类型** | **缺省值** | **说明** |
| client\_id | varchar(50) | not null | 客户端ID，主键 |
| resource\_ids | varchar(50) | not null | 应用ID |
| client\_secret | varchar(50) | not null | 客户端秘钥：加密存储 |
| scope | varchar(50) | null | 权限范围 |
| authorized\_grant\_types | varchar(20) | null | 授权类型 |
| web\_server\_redirect\_uri | timestamp | not null | 客户端的重定向URI |
| authorities | timestamp | null | 权限值 |
| access\_token\_validity | int(5) | not null | token有效期：单位（秒） |
| refresh\_token\_validity | int(5) | not null | 刷新token有效期：单位（秒） |
| additional\_information | varchar(4096) | null | 预留字段，格式必须是json |
| autoapprove | varchar(2) | null | 是否自动approve操作 |

# 接口定义（2种授权方式）

1. **密码模式：**

请求地址：/oauth2/token/password

请求方式: POST

请求数据类型：application/json

请求参数：

|  |  |  |  |
| --- | --- | --- | --- |
| 参数名称 | 类型 | 是否必须 | 说明 |
| grant\_type | string | 是 | 授权类型（password/refresh\_token） |
| appId | string | 是 | 应用ID（client\_id） |
| appSecret | string | 是 | 应用秘钥 |
| username | string | 是 | 用户名 |
| password | string | 是 | 密码 |
| refresh\_token | string | 否 | 刷新token(当grant\_type=refresh\_token)时必传 |

返回数据：

|  |  |  |
| --- | --- | --- |
| 属性名称 | 类型 | 说明 |
| access\_token | string | 访问令牌 |
| token\_type | string | 令牌类型：bearer |
| refresh\_token | string | 刷新令牌 |
| expires\_in | int | 有效时间(秒) |
| scope | array | 权限范围 |

返回示例：

|  |
| --- |
| {  "code": "00000",  "data": {  "access\_token": "",  "expires\_in": 0,  "refresh\_token": "",  "scope": [],  "token\_type": "bearer"  },  "msg": ""  } |

1. **客户端模式：**

请求地址：/oauth2/token/client

请求方式：POST

请求数据类型：application/json

请求参数：

|  |  |  |  |
| --- | --- | --- | --- |
| 参数名称 | 类型 | 是否必须 | 说明 |
| appId | string | 是 | 应用ID（client\_id） |
| appSecret | string | 是 | 应用秘钥 |

返回数据：

|  |  |  |
| --- | --- | --- |
| 属性名称 | 类型 | 说明 |
| access\_token | string | 访问令牌 |
| token\_type | string | 令牌类型：bearer |
| expires\_in | int | 有效时间(秒) |
| scope | array | 权限范围 |

返回示例：

|  |
| --- |
| {  "code": "00000",  "data": {  "access\_token": "",  "expires\_in": 0,  "scope": [],  "token\_type": "bearer"  },  "msg": ""  } |

1. **注销登陆：**

请求地址：/oauth2/logout

请求方式：GET

请求数据类型：application/x-www-form-urlencoded

请求参数：

|  |  |  |  |
| --- | --- | --- | --- |
| 参数名称 | 类型 | 是否必须 | 说明 |
| access\_token | string | 是 | 访问令牌 |

返回数据：

|  |  |  |
| --- | --- | --- |
| 属性名称 | 类型 | 说明 |
| access\_token | string | 访问令牌 |
| token\_type | string | 令牌类型：bearer |
| expires\_in | int | 有效时间(秒) |
| scope | array | 权限范围 |

返回示例：

|  |
| --- |
| {  "code": "00000",  "msg": "注销成功"  } |

# 接口状态码说明

|  |  |
| --- | --- |
| 状态码值（code） | 说明 |
| 00000 | 成功 |
| 10005 | 认证失败 |
| 10009 | 注销失败 |
| 10010 | 不支持的授权类型 |
| 10011 | 请授权后访问（需要登陆） |