Token认证实现机制及接口

目录

[Token认证机制 1](#_Toc470512595)

[1 Token认证的好处 2](#_Toc470512596)

[2 Token机制的处理过程概要描述 2](#_Toc470512597)

[3 Token的内容 3](#_Toc470512598)

[4 Token加密算法 4](#_Toc470512599)

[5 Token验证规则 4](#_Toc470512600)

[6 认证中心拓扑图 4](#_Toc470512601)

[7 具体实现方案 5](#_Toc470512602)

[8 Token机制主要接口 6](#_Toc470512603)

[8.1 登录接口 6](#_Toc470512604)

[8.2 登出接口 7](#_Toc470512605)

[8.3 授权接口 7](#_Toc470512606)

[9 权限控制数据接口 8](#_Toc470512607)

[9.1添加权限接口 8](#_Toc470512608)

[9.2修改权限接口 8](#_Toc470512609)

[9.3 查询单个权限接口 9](#_Toc470512610)

[9.4 查询所有权限接口 10](#_Toc470512611)

[9.5 删除权限接口 10](#_Toc470512612)

[9.6 添加角色接口 10](#_Toc470512613)

[9.7 修改角色接口 12](#_Toc470512614)

[9.8 删除角色接口 12](#_Toc470512615)

[9.9获取单个角色接口 13](#_Toc470512616)

[9.10 获取所有角色接口 13](#_Toc470512617)

[9.11 角色绑定权限接口 14](#_Toc470512618)

[9.12 角色解除权限关联接口 14](#_Toc470512619)

[9.13添加用户接口 15](#_Toc470512620)

[9.14修改用户接口 15](#_Toc470512621)

[9.15删除用户接口 16](#_Toc470512622)

[9.16查询用户接口 16](#_Toc470512623)

[9.17根据用户名查找用户接口 18](#_Toc470512624)

[9.18给用户添加角色接口 18](#_Toc470512625)

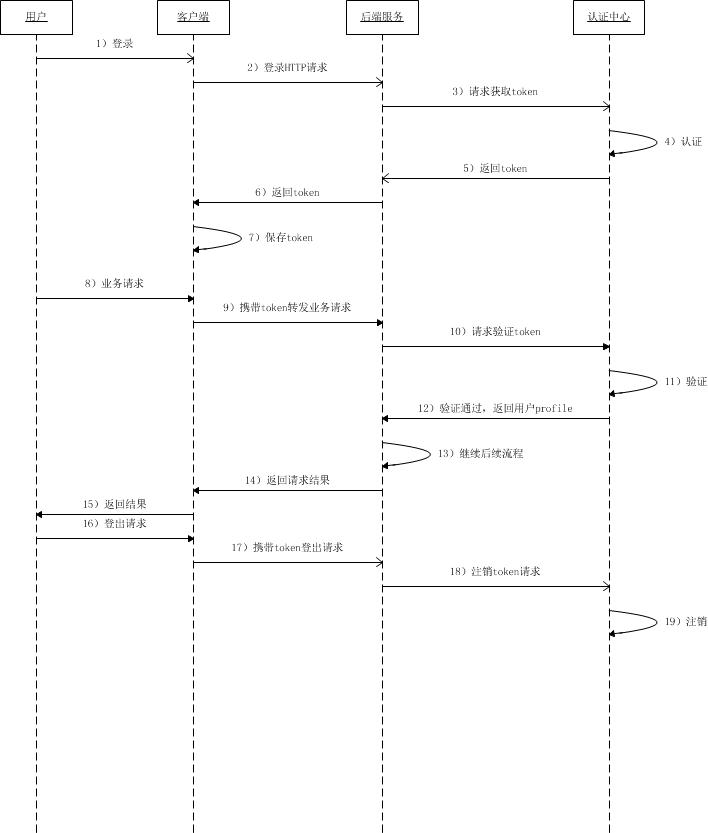
[9.19 解除用户角色关联接口 19](#_Toc470512626)

# 1 Token认证的好处

* **支持跨域访问**: Cookie是不允许垮域访问的，这一点对Token机制是不存在的，前提是传输的用户认证信息通过HTTP头传输.
* **无状态**:Token机制在服务端不需要存储session信息，因为Token 自身包含了所有登录用户的信息，只需要在客户端的cookie或本地介质存储状态信息.
* **更适用CDN**: 可以通过内容分发网络请求你服务端的所有资料（如：javascript，HTML,图片等），而你的服务端只要提供API即可.
* **去耦**: 不需要绑定到一个特定的身份验证方案。Token可以在任何地方生成，只要在你的API被调用的时候，你可以进行Token生成调用即可.
* **更适用于移动应用**: 当你的客户端是一个原生平台（iOS, Android，Windows 8等）时，Cookie是不被支持的（你需要通过Cookie容器进行处理），这时采用Token认证机制就会简单得多。
* **CSRF**:因为不再依赖于Cookie，所以你就不需要考虑对CSRF（跨站请求伪造）的防范。
* **不需要为登录页面做特殊处理**: 如果你使用Protractor 做功能测试的时候，不再需要为登录页面做特殊处理.

# 2 Token机制的处理过程概要描述

1. 用户在客户端输入用户名/密码；
2. 客户端将请求（HTTP）转发给后端服务；
3. 后端服务接收到请求后，解析客户端的IP地址，连同用户名/密码发送给认证中心进行认证；
4. 认证中心负责对用户名/密码进行认证，认证通过后，生成token，并将该token与客户端的IP地址绑定；
5. 认证中心返回token给后端服务；
6. 后端服务将认证中心生成的token返回给客户端；
7. 客户端保存token，以作为后续请求的认证凭据；
8. 客户端发起新的业务请求，同时在请求头部带上token；
9. 后端服务接收业务请求时，首先获取请求头部的token，解析请求的IP地址，向认证中心确认该token是否有效。
10. 如果认证中心验证该token有效，则返回用户profile给后端服务；
11. 后端服务获取认证中心的验证结果，继续执行该业务请求的后续动作。如果验证不通过，则跳转到登录界面，请求新的token。



# 3 Token的内容

{用户名|客户端IP地址|时间戳}

# 4 Token加密算法

对称加密 默认采用DES

Base64

示例：/NQ5ultMnf9deFRuHmyGk68L/nv9fTwa4g+4lpY0pTYOa/q1I5HTxw==

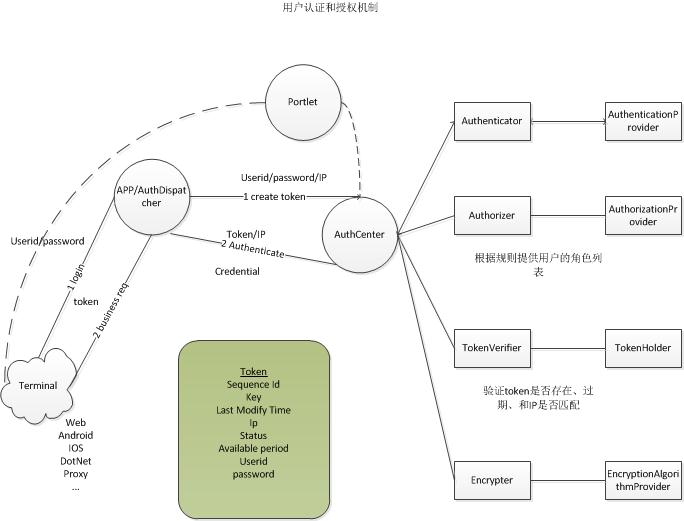
# 5 Token验证规则

1）认证中心接收token后，首先检查是否以前有生成过该token；

2）验证该token是否过期（有效时间可以为30分钟，系统可配）；

3）解密该token，检查其中的IP地址是否与客户端请求的IP地址相匹配。

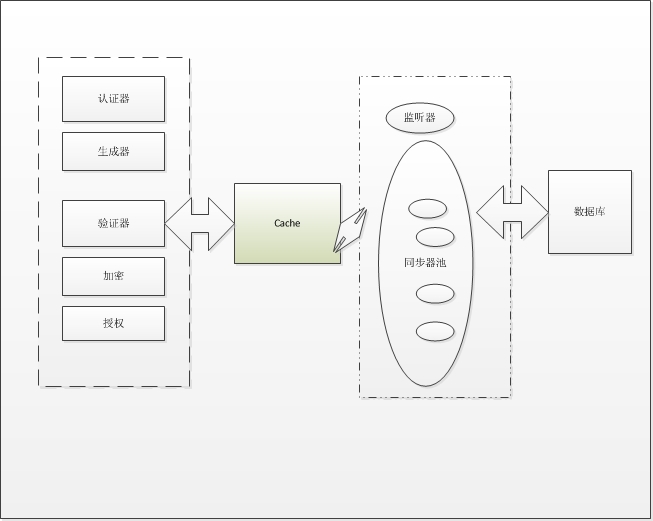
# 6 认证中心拓扑图



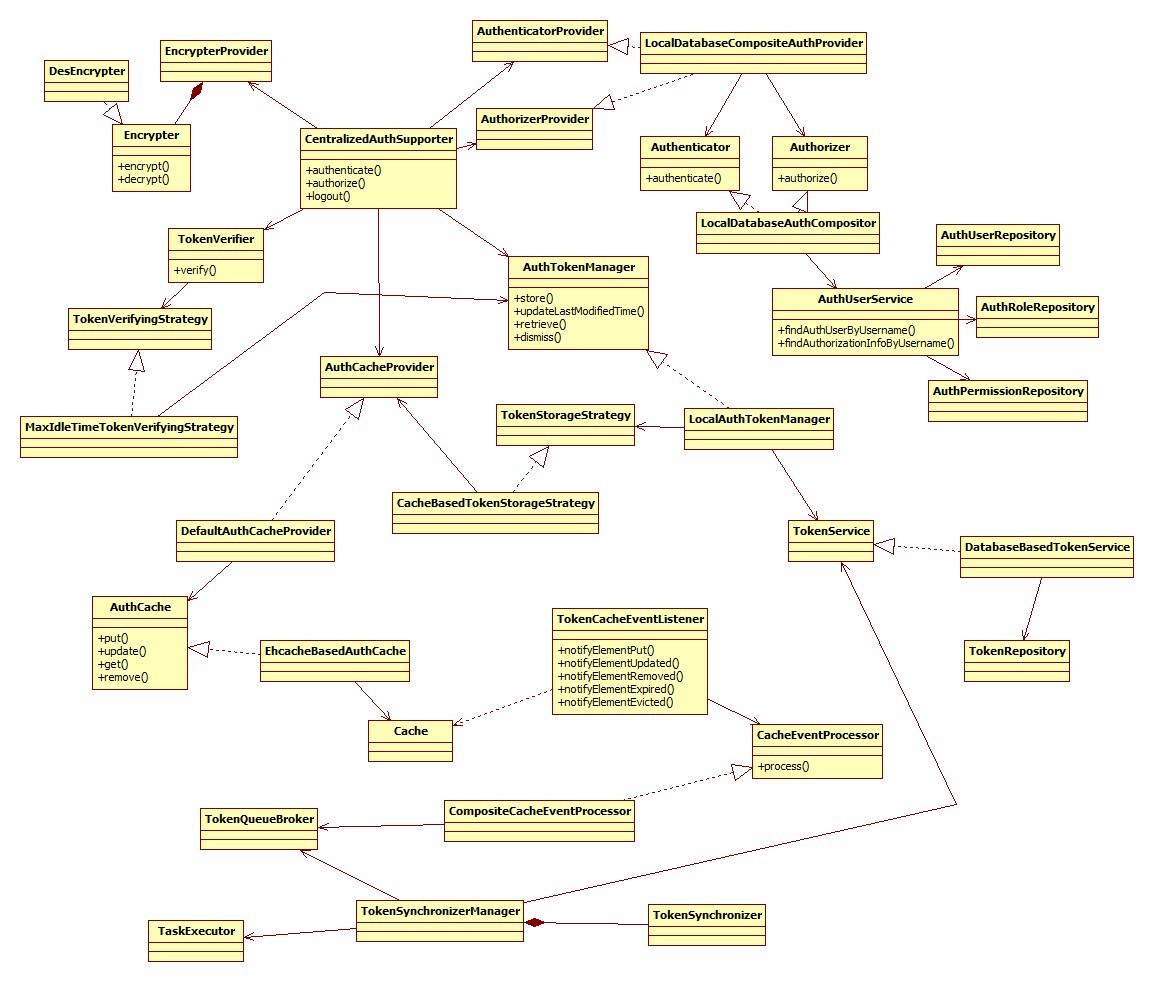
# 7 具体实现方案

目前的实现方案，token的存储和状态更新主要通过cache，考虑到现在的需求，选择EhCache来实现。考虑到可靠性和持续性，对EhCache进行了扩展，加入了各种事件监听，把缓存中的数据异步模式同步到数据库中。

逻辑实现及处理过程



整体实现的核心类图



# 8 Token机制主要接口

## 8.1 登录接口

url：http://{host}:{port}/authc/api/{v1}/tokens

请求方式：POST

入参：

|  |  |  |  |
| --- | --- | --- | --- |
| 参数名 | 类型 | 是否必需 | 备注 |
| Username | String | Y |  |
| Password | String | Y |  |

示例：

{

“username”:”{username}”,

“password”:”{password}”

}

出参：状态码200

|  |  |  |
| --- | --- | --- |
| 参数名 | 类型 | 备注 |
| Token | String | 生成的token串 |
| userID | String | 对应数据库自增长ID |

示例：

{

“token”:”{token}”,

“userId”:”{userId}” //用户OID

}

## 8.2 登出接口

URL：http://{host}:{port}/authc/api/{v1}/tokens/{tokenid}

请求方式：DELETE

入参：

|  |  |  |  |
| --- | --- | --- | --- |
| 参数名 | 类型 | 是否必需 | 备注 |
| Tokenid | String | Y |  |

出参：返回204

无

## 8.3 授权接口

URL：http://{host}:{port}/authc/api/{v1}/authorizations/{tokenid}?ip={terminalIpAddress}

请求方式：GET

入参：

|  |  |  |  |
| --- | --- | --- | --- |
| 参数名 | 类型 | 是否必需 | 备注 |
| Tokenid | String | Y | Token串 |
| terminalIpAddress | String | Y | 客户端的IP地址 |

出参：状态码200

|  |  |  |
| --- | --- | --- |
| 参数名 | 类型 | 备注 |
| Id | String | 用户ID |
| Username | String | 用户名 |
| Roles | List<string> | 角色列表 |
| Permissions | List<string> | 权限列表 |

# 9 权限控制数据接口

## 9.1添加权限接口

url：http://{host}:{port}/authc /api/{version}/permissions

请求方式：post

入参

|  |  |  |  |
| --- | --- | --- | --- |
| 参数名 | 类型 | 是否必需 | 备注 |
| code | String | N | 权限编码，预留 |
| name | String | Y | 权限名称 |
| label | string | N | 可用于前端默认展示 |
| description | string | N | 描述 |

出参 200

|  |  |  |
| --- | --- | --- |
| 参数名 | 类型 | 备注 |
| Id | long |  |
| code | string |  |
| name | string |  |
| label | string |  |
| description | string |  |
| deleted | boolean | 该资源是否标记为删除 |

示例：

{

"id":1,

"code":"PERM\_DEPT\_LIST",

"name":"DEPT:LIST",

"label":"科室员工列表",

"description":"descriptions",

"deleted":false

}

## 9.2修改权限接口

url：http://{host}:{port}/authc /api/{version}/permissions/{id}

请求方式：PUT

入参

|  |  |  |  |
| --- | --- | --- | --- |
| 参数名 | 类型 | 是否必需 | 备注 |
| Id | long | Y |  |
| code | string | N |  |
| name | string | N |  |
| label | string | N |  |
| description | string | N |  |
| deleted | boolean | N |  |

出参

|  |  |  |
| --- | --- | --- |
| 参数名 | 类型 | 备注 |
| Id | long |  |
| code | string |  |
| name | string |  |
| label | string |  |
| description | string |  |
| deleted | boolean | 该资源是否标记为删除 |

## 9.3 查询单个权限接口

url：http://{host}:{port}/authc /api/{version}/permissions/{id}

请求方式：GET

入参

|  |  |  |  |
| --- | --- | --- | --- |
| 参数名 | 类型 | 是否必需 | 备注 |
| id | long | Y |  |
|  |  |  |  |

出参

|  |  |  |
| --- | --- | --- |
| 参数名 | 类型 | 备注 |
| Id | long |  |
| code | string |  |
| name | string |  |
| label | string |  |
| description | string |  |
| deleted | boolean | 该资源是否标记为删除 |

## 9.4 查询所有权限接口

url：http://{host}:{port}/authc /api/{version}/permissions

请求方式：GET

入参

|  |  |  |  |
| --- | --- | --- | --- |
| 参数名 | 类型 | 是否必需 | 备注 |
|  |  |  |  |
|  |  |  |  |

出参

|  |  |  |
| --- | --- | --- |
| 参数名 | 类型 | 备注 |
|  | List<permission> |  |

## 9.5 删除权限接口

url：http://{host}:{port}/authc /api/{version}/permissions/{id}

请求方式：DELETE

入参

|  |  |  |  |
| --- | --- | --- | --- |
| 参数名 | 类型 | 是否必需 | 备注 |
| id | string | Y |  |

出参 204

|  |  |  |
| --- | --- | --- |
| 参数名 | 类型 | 备注 |
|  |  |  |
|  |  |  |

## 9.6 添加角色接口

url：http://{host}:{port}/authc /api/{version}/roles

请求方式：post

入参

|  |  |  |  |
| --- | --- | --- | --- |
| 参数名 | 类型 | 是否必需 | 备注 |
| Code | String | N | 角色编码，预留 |
| Name | String | Y |  |
| label | String | N |  |
| description | string | N |  |

示例：

{

"code":"ROLE\_USER",

"name":"ROLE:USER",

"label":"普通用户",

"description":"普通用户角色"

}

出参 200

|  |  |  |
| --- | --- | --- |
| 参数名 | 类型 | 备注 |
| Id | Long |  |
| Code | String |  |
| Name | String |  |
| Description | String |  |
| deleted | Boolean |  |
| createAt | Date |  |
| updateAt | Date |  |
| createBy | long | 创建者ID |
| updateBy | long | 该记录最后修改者ID |
| dataSource | String |  |
| permissions | List<permission> |  |

示例：

{

"id": 69,

"code": "ROLE\_USER",

"name": "ROLE:USER",

"label": "普通用户",

"description": "普通用户角色",

"deleted": false,

"createAt": 1482387072345,

"updateAt": null,

"createBy": null,

"updateBy": null,

"dataSource": "system",

"permissions":

[

]

}

## 9.7 修改角色接口

url：http://{host}:{port}/authc /api/{version}/roles/{roleId}

请求方式：PUT

入参

|  |  |  |  |
| --- | --- | --- | --- |
| 参数名 | 类型 | 是否必需 | 备注 |
| Code | String | N | 角色编码，预留 |
| Name | String | N |  |
| label | String | N |  |
| description | string | N |  |
| Deleted | boolean | N |  |

出参

|  |  |  |
| --- | --- | --- |
| 参数名 | 类型 | 备注 |
| Id | Long |  |
| Code | String |  |
| Name | String |  |
| Description | String |  |
| deleted | Boolean |  |
| createAt | Date |  |
| updateAt | Date |  |
| createBy | long | 创建者ID |
| updateBy | long | 该记录最后修改者ID |
| dataSource | String |  |
| permissions | List<permission> |  |

## 9.8 删除角色接口

url：http://{host}:{port}/authc /api/{version}/roles/{roleId}

请求方式：DELETE

入参

|  |  |  |  |
| --- | --- | --- | --- |
| 参数名 | 类型 | 是否必需 | 备注 |
| roleId | long | Y |  |
|  |  |  |  |

出参 204

无

## 9.9获取单个角色接口

url：http://{host}:{port}/authc /api/{version}/roles/{roleId}

请求方式：GET

入参

|  |  |  |  |
| --- | --- | --- | --- |
| 参数名 | 类型 | 是否必需 | 备注 |
| roleId | long | Y |  |
|  |  |  |  |

出参 200

|  |  |  |
| --- | --- | --- |
| 参数名 | 类型 | 备注 |
| Id | Long |  |
| Code | String |  |
| Name | String |  |
| Description | String |  |
| deleted | Boolean |  |
| createAt | Date |  |
| updateAt | Date |  |
| createBy | long | 创建者ID |
| updateBy | long | 该记录最后修改者ID |
| dataSource | String |  |
| permissions | List<permission> |  |

## 9.10 获取所有角色接口

url：http://{host}:{port}/authc /api/{version}/roles

请求方式：GET

入参

|  |  |  |  |
| --- | --- | --- | --- |
| 参数名 | 类型 | 是否必需 | 备注 |
|  |  |  |  |
|  |  |  |  |

出参

|  |  |  |
| --- | --- | --- |
| 参数名 | 类型 | 备注 |
|  | List<role> | 角色列表 |
|  |  |  |

## 9.11 角色绑定权限接口

url：http://{host}:{port}/authc /api/{version}/roles/{roleId}/permissions

请求方式：post

入参

|  |  |  |  |
| --- | --- | --- | --- |
| 参数名 | 类型 | 是否必需 | 备注 |
| roleId | long | Y | 角色ID |
| id | long | Y | 权限ID |

出参 200

|  |  |  |
| --- | --- | --- |
| 参数名 | 类型 | 备注 |
| Id | Long |  |
| Code | String |  |
| Name | String |  |
| Description | String |  |
| deleted | Boolean |  |
| createAt | Date |  |
| updateAt | Date |  |
| createBy | long | 创建者ID |
| updateBy | long | 该记录最后修改者ID |
| dataSource | String |  |
| permissions | List<permission> |  |

## 9.12 角色解除权限关联接口

url：http://{host}:{port}/authc /api/{version}/roles/{roleId}/permissions/{permId}

请求方式：delete

入参

|  |  |  |  |
| --- | --- | --- | --- |
| 参数名 | 类型 | 是否必需 | 备注 |
| roleId | long | Y | 角色ID |
| permId | long | Y | 权限ID |

出参 204

|  |  |  |
| --- | --- | --- |
| 参数名 | 类型 | 备注 |
|  |  |  |
|  |  |  |

## 9.13添加用户接口

url：http://{host}:{port}/authc /api/{version}/users

请求方式：post

入参

|  |  |  |  |
| --- | --- | --- | --- |
| 参数名 | 类型 | 是否必需 | 备注 |
| Code | String | N |  |
| username | String | Y |  |
| password | String | Y |  |
| name | String | N |  |
| gender | String | N |  |
| mobilePhone | String | N |  |
| telephone | String | N |  |
| email | string | N |  |

出参

|  |  |  |
| --- | --- | --- |
| 参数名 | 类型 | 备注 |
| Object:user |  |  |
|  |  |  |

## 9.14修改用户接口

url：http://{host}:{port}/authc /api/{version}/users/{id}

请求方式：put

入参

|  |  |  |  |
| --- | --- | --- | --- |
| 参数名 | 类型 | 是否必需 | 备注 |
| id | long | Y |  |
| Code | String | N |  |
| username | String | Y |  |
| password | String | Y |  |
| name | String | N |  |
| gender | String | N |  |
| mobilePhone | String | N |  |
| telephone | String | N |  |
| email | string | N |  |

出参

|  |  |  |
| --- | --- | --- |
| 参数名 | 类型 | 备注 |
| Object:user |  |  |
|  |  |  |

## 9.15删除用户接口

url：http://{host}:{port}/authc /api/{version}/users/{id}

请求方式：delete

入参

|  |  |  |  |
| --- | --- | --- | --- |
| 参数名 | 类型 | 是否必需 | 备注 |
| Id | long | Y |  |
|  |  |  |  |

出参 204

|  |  |  |
| --- | --- | --- |
| 参数名 | 类型 | 备注 |
|  |  |  |
|  |  |  |

## 9.16查询用户接口

url：http://{host}:{port}/authc /api/{version}/users/{id}

请求方式：GET

入参

|  |  |  |  |
| --- | --- | --- | --- |
| 参数名 | 类型 | 是否必需 | 备注 |
| id | long | Y | 用户ID |
|  |  |  |  |

出参

|  |  |  |
| --- | --- | --- |
| 参数名 | 类型 | 备注 |
| Id | Long |  |
| Code | String |  |
| username | String |  |
| password | String |  |
| name | String |  |
| gender | String |  |
| mobilePhone | String |  |
| telephone | String |  |
| email | string |  |
| isDeleted | boolean |  |
| isActive | boolean |  |
| createAt | date |  |
| updateAt | date |  |
| createBy | long |  |
| updateBy | long |  |
| dataSource | string |  |
| roles | List<role> |  |

示例：

{

"id": 80,

"code": "code-test",

"username": "user-test-98742656089847",

"password": "123",

"name": "USER-TEST",

"gender": "M",

"mobilePhone": "189252222211",

"telephone": "0755-89896666",

"email": "abcddd@lachesis.com",

"isDeleted": false,

"isActive": true,

"isLocked": false,

"createAt": 1482204892330,

"updateAt": 1482204892330,

"createBy": 1,

"updateBy": 2,

"dataSource": "SYSTEM",

"roles":

[

{

"id": 31,

"code": "ROLE\_TEST-",

"name": "ROLE-TEST-98742656149251",

"label": null,

"description": null,

"createAt": 1482163200000,

"updateAt": null,

"createBy": null,

"updateBy": null,

"dataSource": null,

"permissions":

[

],

"deleted": false

}

]

}

## 9.17根据用户名查找用户接口

url：http://{host}:{port}/authc /api/{version}/users/user?username={username}

请求方式：GET

入参

|  |  |  |  |
| --- | --- | --- | --- |
| 参数名 | 类型 | 是否必需 | 备注 |
| username | string | Y |  |
|  |  |  |  |

出参 200

|  |  |  |
| --- | --- | --- |
| 参数名 | 类型 | 备注 |
| Refer:9.16 |  |  |

## 9.18给用户添加角色接口

url：http://{host}:{port}/authc /api/{version}/users/{userId}/roles

请求方式：post

入参

|  |  |  |  |
| --- | --- | --- | --- |
| 参数名 | 类型 | 是否必需 | 备注 |
| userId | long | Y | 用户ID |
| roleId | long | Y | 角色ID，放在请求体 |

出参 200

|  |  |  |
| --- | --- | --- |
| 参数名 | 类型 | 备注 |
| User | Object:user |  |
|  |  |  |

## 9.19 解除用户角色关联接口

url：http://{host}:{port}/authc /api/{version}/users/{userId}/roles/{roleId}

请求方式：

入参

|  |  |  |  |
| --- | --- | --- | --- |
| 参数名 | 类型 | 是否必需 | 备注 |
| userId | long | Y | 用户ID |
| roleId | long | Y | 角色ID |

出参 204

|  |  |  |
| --- | --- | --- |
| 参数名 | 类型 | 备注 |
|  |  |  |