**IDM详细设计文档**

**2014.03**

**修订记录**

|  |  |  |  |
| --- | --- | --- | --- |
| **版本** | **修订内容** | **作者** | **日期** |
| 1.0 | 初稿完成 | 袁欢 | 2014/3/26 |
| 1.1 | 去掉黑白名单；  去掉role的概念；  完善数据库设计； | 袁欢 | 2014/4/2 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**目 录**

[1 IDM总体架构 4](#_Toc385504447)

[1.1 概述 4](#_Toc385504448)

[1.2 IDM系统架构 4](#_Toc385504449)

[2 数据模型 4](#_Toc385504450)

[2.1 User 4](#_Toc385504451)

[2.2 Group 5](#_Toc385504452)

[2.3 AccessKey 5](#_Toc385504453)

[2.4 Policy 6](#_Toc385504454)

[3 数据库设计 6](#_Toc385504455)

[3.1 t\_idm\_user 6](#_Toc385504456)

[3.2 t\_idm\_group 6](#_Toc385504457)

[3.3 t\_idm\_user\_group\_map 7](#_Toc385504458)

[3.4 t\_idm\_accesskey 7](#_Toc385504459)

[3.5 t\_idm\_policy 7](#_Toc385504460)

[3.6 t\_idm\_ip\_request\_logs 8](#_Toc385504461)

[3.7 t\_idm\_user\_request\_logs 8](#_Toc385504462)

[4 算法 8](#_Toc385504463)

[4.1 数字签名算法 8](#_Toc385504464)

[5 流程 9](#_Toc385504465)

[5.1 用户管理 9](#_Toc385504466)

[5.2 组管理 11](#_Toc385504467)

[5.3 接口认证 12](#_Toc385504468)

# IDM总体架构

## 概述

本文档旨在对IDM系统进行详细设计和描述，以保障整个云计算平台的安全性。

## IDM系统架构

下面的图片展示了IDM系统的整体框架。



说明如下：

1. IDM对外提供基于数字签名、时间戳、SSL机制的安全API；
2. IDM包括用户和账户管理、组管理、AccessKey管理、Policy管理以及请求限制管理几个部分；
3. IDM基于Mysql保存数据。

# 数据模型

## User

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **字段名称** | **字段含义** | **字段类型** | **取值范围** | **备注** |
| userId | 用户ID | String |  |  |
| userName | 用户名 | String |  |  |
| userType | 用户类型 | String | user/account |  |
| accountId | 所属账户ID | String |  |  |
| createDate | 创建时间 | String |  | 格式：  yyyy-MM-dd'T'HH:mm:ss'Z'，例如：2014-03-28T14:48:31Z |
| password | 密码 | String |  |  |

## Group

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **字段名称** | **字段含义** | **字段类型** | **取值范围** | **备注** |
| groupId | 组ID | String |  |  |
| groupName | 组名 | String |  |  |
| accountId | 所属账户ID | String |  |  |
| description | 描述 | String |  |  |
| createDate | 创建日期 | String |  | 格式：  yyyy-MM-dd'T'HH:mm:ss'Z'，例如：2014-03-28T14:48:31Z |

## AccessKey

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **字段名称** | **字段含义** | **字段类型** | **取值范围** | **备注** |
| accessKeyId | AccessKeyID | String |  |  |
| secretAccessKey | SecretAccessKey | String |  |  |
| status | 状态 | String | active/inactive |  |
| ownerId | 所属的属主ID | String |  | userId/accountId |
| createDate | 创建日期 | String |  | 格式：  yyyy-MM-dd'T'HH:mm:ss'Z'，例如：2014-03-28T14:48:31Z |

## Policy

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **字段名称** | **字段含义** | **字段类型** | **取值范围** | **备注** |
| policyId | 策略名ID | String |  |  |
| policyName | 策略名称 | String |  |  |
| policyDocument | 策略内容 | String |  |  |
| ownerType | 属主类型 | String | user/group |  |
| ownerId | 属主ID | String | 用户ID或者组ID |  |

# 数据库设计

## t\_idm\_user

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **字段名称** | **字段含义** | **字段类型** | **取值范围** | **备注** |
| userId | 用户ID | char(64) |  | 主键 |
| userName | 用户名 | char(128) |  |  |
| userType | 用户类型 | char(16) | user/account |  |
| accountId | 所属账户ID | char(64) |  |  |
| createDate | 创建时间 | char(32) |  | 格式：  yyyy-MM-dd'T'HH:mm:ss'Z'，例如：2014-03-28T14:48:31Z |
| password | 密码 | char(64) |  |  |

## t\_idm\_group

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **字段名称** | **字段含义** | **字段类型** | **取值范围** | **备注** |
| groupId | 组ID | char(64) |  | 主键 |
| groupName | 组名 | char(64) |  |  |
| accountId | 所属账户ID | char(64) |  |  |
| description | 描述 | text |  |  |
| createDate | 创建日期 | char(32) |  | 格式：  yyyy-MM-dd'T'HH:mm:ss'Z'，例如：2014-03-28T14:48:31Z |

## t\_idm\_user\_group\_map

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **字段名称** | **字段含义** | **字段类型** | **取值范围** | **备注** |
| userId | 用户ID | char(64) |  | 联合主键 |
| groupId | 组ID | char(64) |  |

## t\_idm\_accesskey

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **字段名称** | **字段含义** | **字段类型** | **取值范围** | **备注** |
| accessKeyId | AccessKeyID | char(64) |  | 主键 |
| secretAccessKey | SecretAccessKey | char(64) |  |  |
| status | 状态 | char(32) | active/inactive |  |
| ownerId | 所属的属主ID | char(64) |  | userId/accountId |
| createDate | 创建日期 | char(32) |  | 格式：  yyyy-MM-dd'T'HH:mm:ss'Z'，例如：2014-03-28T14:48:31Z |

## t\_idm\_policy

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **字段名称** | **字段含义** | **字段类型** | **取值范围** | **备注** |
| policyId | 策略名ID | char(64) |  | 主键 |
| policyName | 策略名称 | char(128) |  |  |
| policyDocument | 策略内容 | text |  |  |
| ownerType | 属主类型 | char(16) | user/group |  |
| ownerId | 属主ID | char(64) | 用户ID或者组ID |  |

## t\_idm\_ip\_request\_logs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **字段名称** | **字段含义** | **字段类型** | **取值范围** | **备注** |
| ipAddress | IP地址 | char(32) |  | 主键 |
| requestTimes | 当前统计周期内的请求次数 | int(16) | 访问频率限制 |  |
| currentHour | 当前统计周期，计算到小时 | char(32) |  | 格式：  yyyy-MM-dd'T'HH:'00:00Z'，例如：2014-03-28T17:00:00Z |

## t\_idm\_user\_request\_logs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **字段名称** | **字段含义** | **字段类型** | **取值范围** | **备注** |
| userId | 所属的用户ID | char(32) |  | 主键 |
| requestTimes | 当前统计周期内的请求次数 | int(16) | 访问频率限制 |  |
| currentHour | 当前统计周期，计算到小时 | char(32) |  | 格式：  yyyy-MM-dd'T'HH:'00:00Z'，例如：2014-03-28T17:00:00Z |

# 算法

## 数字签名算法

数字签名算法如下：BASE64(HMAC\_SHA256(SignString, SecretAccessKey))。

其中SignString构造方法如下：

|  |
| --- |
| HTTPMethod\n  HOST\n  URI\n  Params |

说明：

1. HOST不包括端口号；

2. HttpMethod为大写；

3. Params在GET请求中为QueryString，在POST请求中为Json格式的PostData。为空时，取值空字符串""

4. 所有字段必须采用UTF-8进行URL解码；

例如，如果一个请求为：

|  |
| --- |
| https://idm.example.com/createUser?userName=Jason&twsAccessKeyId=AKIAIOSFODNN7EXAMPLE&signatureMethod=HmacSHA256&signatureVersion=1&timestamp=20140325232010 |

那么构造的签名字符串为：

|  |
| --- |
| GET\n  idm.example.com\n  /createUser\n |

如果按照签名算法计算出来的签名值为：

i91nKc4PWAt0JJIdXwz9HxZCJDdiy6cf%2FMj6vPxyYIs%3D

那么，最终构造出来的请求URL添加上这个签名字段即可，样例如下：

|  |
| --- |
| https://idm.example.com/createUser?userName=Jason&twsAccessKeyId=AKIAIOSFODNN7EXAMPLE&signatureMethod=HmacSHA256&signatureVersion=1&timestamp=20140325232010&signature=i91nKc4PWAt0JJIdXwz9HxZCJDdiy6cf%2FMj6vPxyYIs%3D |

# 流程

## 用户管理

创建用户、AccessKey以及Policy的序列图如下所示：



说明如下：

1. 首先，客户端程序调用IDM接口创建用户；
2. IDM系统对请求进行鉴权，如果认证失败则直接返回失败信息；
3. IDM将用户信息保存到数据库；
4. IDM系统返回用户信息给客户端；
5. 接下来，客户端调用IDM接口创建AccessKey和SecretAccessKey；
6. IDM系统对请求进行鉴权，如果认证失败则直接返回失败信息；
7. IDM接口认证通过之后，IDM系统创建AKSK；
8. IDM将新产生的AKSK保存入库；
9. IDM系统返回用户AKSK信息给客户端；
10. 最后，客户端调用IDM接口创建用户策略；
11. IDM系统对请求进行鉴权，如果认证失败则直接返回失败信息；
12. IDM认证通过之后，创建用户策略；
13. IDM检查通过之后，将用户策略保存入库；
14. IDM将用户策略信息返回给IDM系统；
15. IDM返回用户策略创建的结果给客户端；

## 组管理

创建组、增加组策略以及为组添加用户的序列图如下所示：

s

说明如下：

1. 首先，客户端程序调用IDM接口创建组；
2. IDM系统对请求进行鉴权，如果认证失败则直接返回失败信息；
3. IDM创建一个新的组；
4. IDM将组信息保存到数据库；
5. IDM系统返回组信息给客户端；
6. 接下来，客户端调用IDM接口创建组策略；
7. IDM系统对请求进行鉴权，如果认证失败则直接返回失败信息；
8. IDM接口认证通过之后，IDM创建组策略；
9. IDM将新产生的组策略保存入库；
10. IDM系统返回组策略信息给客户端；
11. 最后，客户端调用IDM接口将用户添加到组；
12. IDM系统对请求进行鉴权，如果认证失败则直接返回失败信息；
13. IDM认证通过之后，将用户添加到组；
14. 保存入库；
15. sIDM返回结果给客户端；

## 接口认证

接口认证过程如下图所示：



说明如下：

1. 首先，客户端程序向rkit API Server发起一个接口调用；
2. rkit API Server向IDM发起接口调用进行认证；
3. IDM检查客户端IP是否符合IP访问频率限制；
4. IDM在数据库中查询用户信息；
5. 数据库返回用户信息；
6. IDM根据客户端请求构造签名并与客户端传递的签名进行对比；
7. IDM向rkit API Server返回认证结果；
8. rkit API Server根据认证结果进行内部处理；
9. rkit API Server向客户端返回接口调用结果。