**单点登录开发设计文档**

文档管理信息表

|  |  |
| --- | --- |
| **主题** | 单点登录开发设计文档 |
| **版本** | 1.1 |
| **内容** |  |
| **关键字** |  |
| **参考文档** |  |
| **创建时间** | 2019-08-3 |
| **创建人** |  |
| **最新发布日期** | 2019-08-16 |

文档变更记录表

|  |  |  |
| --- | --- | --- |
| **修改人** | **修改时间** | **修改内容** |
| Alger | 2019-08-08 | 初版完成 |
| Alger | 2019-08-15 | 补充Web登陆相关流程，补充QM获取OpenID |
| 王雷 | 2019-11-28 | 服务开发完成后补充说明 |
|  |  |  |
|  |  |  |

**目 录**

[1 引言 1](#_Toc25918957)

[1.1 编写目的 1](#_Toc25918958)

[1.2 背景 1](#_Toc25918959)

[**1.2.1** 项目简述 1](#_Toc25918960)

[1.3 定义 1](#_Toc25918961)

[1.4 参考资料 1](#_Toc25918962)

[2 单点登录架构设计 1](#_Toc25918963)

[2.1 架构图 1](#_Toc25918964)

[2.2 设计说明 2](#_Toc25918965)

[2.3 Web登陆过程 3](#_Toc25918966)

[2.4 QM获取OpenID 3](#_Toc25918967)

[3 接口调用与协议说明 4](#_Toc25918968)

[3.1 接口调用时序图 4](#_Toc25918969)

[3.2 接口协议图 5](#_Toc25918970)

[**3.2.1** 协议说明 6](#_Toc25918971)

[4 接口及参数设计 6](#_Toc25918972)

[4.1 客户端通用接口 6](#_Toc25918973)

[4.2 IAM/Login接口 6](#_Toc25918974)

[4.3 GateWay接口说明 7](#_Toc25918975)

[4.4 DDS接口说明 8](#_Toc25918976)

[5 服务端接口对接说明 9](#_Toc25918977)

[6 单点登录服务配置文件说明 9](#_Toc25918978)

[6.1 配置文件介绍 9](#_Toc25918979)

[6.2 单点登录服务配置项 9](#_Toc25918980)

[**6.2.1** msgbus配置模块 9](#_Toc25918981)

[**6.2.2** lava配置模块 9](#_Toc25918982)

[**6.2.3** http配置模块 10](#_Toc25918983)

[**6.2.4** gateway配置模块 10](#_Toc25918984)

[**6.2.5** DDS配置模块 10](#_Toc25918985)

[**6.2.6** login server配置模块 10](#_Toc25918986)

# 引言

## 编写目的

本文基于单点登录架构设计的讨论，根据新架构提出的开发需求，描述单点登录模块设计的基本原理，主要流程、交互等内容。

本文的主要读者为各个项目开发人员、测试人员等。

## 背景

统一的单点登录方案可以将森浦对外的服务认证过程整合起来，有利于权限的统一管理，减少冗余的开发工作。本次的架构有灵活的扩展与伸缩性，方便公司内部产品的登录使用，也可以直接提供给第三方公司用于其通过认证来获取森浦的API数据。

### 项目简述

|  |  |
| --- | --- |
| 中文名称 | 单点登录开发设计文档 |
| 英文名称 |  |
| 项目简称 |  |
| 项目代号 |  |
| 命名约定 |  |

## 定义

|  |  |
| --- | --- |
| 缩略语 | 解释 |
| GW | GateWay |
| DDS | Data Distribution Service |
| IAM | Identity and Access Management |
|  |  |

## 参考资料

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **编号** | **名称** | **作者** | **日期** | **密级** |
|  |  |  |  |  |

# 单点登录架构设计

## 架构图



## 设计说明

* 异地负载均衡：

1. 在上海和北京两个不同的数据中心，利用F5的GTM模式，实现动态路，由F5选择更优的数据中心给到用户。

* 数据中心内部负载均衡：

1. 采用软件选择（选择特殊网关）和F5相结合模式。
2. 在数据中心内部有三个集群，分别是IAM（Login）集群、GW集群、DDS集群。每个集群分别通过F5的LTM模式实现负载均衡。
3. 用户首先登录到IAM服务，由IAM根据配置选择是登录到GW集群还是登录到特殊网关GWx。

* 登录过程说明：

1. 客户端首先通过账号登录的IAM服务，IAM进行用户的合法性验证。
2. IAM 验证账户通过后会返回Token和GW集群和DDS集群的单一入口域名给到客户端，同时将Token广播到GW集群和DDS集群；IAM验证失败则返回失败信息。
3. 客户端拿到IAM返回的GW地址和DDS地址，根据需要客户端用Token再到这两个服务进行认证登录。
4. GW服务和DDS服务根据Token对链接上来的客户端进行合法性验证。
5. 客户端可以根据实际业务需求，选择只登录DDS或者只登录GW，或者两者都登录。

* 关于Token

1. Token 由IAM/Login 唯一生成， 一个Token 在GW和DDS 上只能用一次验证，即对于某个DDS服务，收到的Toke只能用于对一个TCP链接的验证。 Token有过期时间，默认1分钟。
2. IAM/Login 生成Token后广播推送到总线，所有GW服务和DDS服务接收推送消息，取得Token信息。

## Web登陆过程



Web调用QB.login()时，浏览器请求接收到请求后调用QB的QB.Login()，QB返回Token、UserName通浏览器传递给Web。

Web拿到Token、UserName需要发送给Web后台服务。

在Web后台服务接收到Token后，再携带这Web的APPID（用于区分不同Web应用）、UserName去访问Login/IAM服务，Login/IAM服务会返回UserID(OpenID)，session\_key。

其中：

1. UserID(OpenID)是用户唯一标识。
2. Session\_key是解密用的，也可以用来生产SessionID。如果是外部Web应用，可以对某些调用 API接口数据进行加密，然后用这个Session\_key进行解密。

当Web后台服务器拿到Login/IAM返回的UserID，Session\_key后，会自己生成一个SessionID 。然后把这个SessionID返回给Web前台，并且在服务器的session中存入以SessionID为key，UserID+Session\_key为value的数据。

Web前台收到这个SessionID后，保存起来，后续的Web请求需要带上这个SessionID，作为认证用。

## QM获取OpenID



QM需要和客户端本地总线建立链接。

QM调用GetOpenID方法向总线发请求。

总线把请求传递给QB，QB用户提示用户，是否允许授权QM获取OpenID， 如果允许则将OpenID和Token通过总线返回给QM。QM可以拿着OpenID和Token 向QM的后台进行登陆。

# 接口调用与协议说明

## 接口调用时序图



## 接口协议图



## 协议说明

1. 单点登录服务工作时与多种角色之间产生数据交互，这些角色有QB、QM、Excel等客户端，DDS Server，网关服务，QB Web，数据源服务等。

2. 与各个角色间交互所使用的通信协议也不尽相同，目前涉及的通信协议主要有三种：lava box、msgbus以及http。

3. lava box与msgbus为我司私有协议，http主要使用post方式且以application/json的格式交互数据。

4. 有关lava box的接入方式请参考lava box提供的相关文档。

5. 有关msgbus的接入方式请参考iam项目提供的demo代码。

6. http post接入方式为标准协议，此处不再说明。

# 接口及参数设计

## 客户端通用接口

下面的两个接口是在客户端网络层需要实现的基础API接口，详细见DDS API设计文档或GW 的API。

|  |  |
| --- | --- |
| **SetProxy** | |
| 功能 | 设置代理登录连接TCP的方式 |
| 输入参数 | |
| **proxy** | 指向proxy结构体指针 |
| 输出参数 | |
| **无** |  |
| 返回值 | |
| **void** |  |
| 备注： | |

|  |  |
| --- | --- |
| **Connect** | |
| 功能 | 客户端建立与IAM服务器之间的TCP连接 |
| 输入参数 | |
| **ip\_addr** | 服务器ip |
| **port** | 服务器监听端口号 |
| 输出参数 | |
| **无** |  |
| 返回值 | |
| **bool** | 指示连接是否成功 |
| 备注： | |

## IAM/Login接口

|  |  |  |
| --- | --- | --- |
| **Login** | | |
| 功能 | | 客户端连接IAM服务器进行账号等认证 |
| Topic | |  |
| 请求参数 | | |
| **user\_name** | | 用户账号 |
| **password** | | 账号密码 |
| **mac** | | MAC地址 |
| **version** | | 客户端版本号 |
| **reserve** | | 保留字段 |
|  | |  |
| 应答参数 | | |
| 验证通过 | | |
|  | **user\_id** | 客户唯一标识码 |
| **gw\_ip** | 网关地址 |
| **gw\_port** | 网关端口 |
| **dds\_ip** | DDS地址 |
| **dds\_port** | DDS端口 |
| **token** | Token |
| **time** | 系统时间 |
| **reserve** | 保留字段 |
|  |  |
| 验证失败 | | |
|  | **error\_code** | **错误代码** |
| **error\_msg** | **错误信息** |
|  | | |

|  |  |
| --- | --- |
| **Logout** | |
| 功能 | IAM/Login客户端登出 |
| Topic |  |
| 请求参数 | |
| **user\_name** | 用户名 |
| 应答参数 | |
| **无** |  |

|  |  |
| --- | --- |
| **BroadcastToken** | |
| 功能 | IAM/Login向Gateway 和DDS广播 Token信息 |
| Topic |  |
| 推送参数 | |
| **user\_name** | 用户名 |
| **user\_id** | 用户唯一ID |
| **token** | Token |
| **validate** | 有效期，一般1分钟 |
| 应答参数 | |
|  | |

## GateWay接口说明

|  |  |  |
| --- | --- | --- |
| **Login** | | |
| 功能 | | 客户端连接GateWay服务器进行Token等认证 |
| Topic | |  |
| 请求参数 | | |
| **user\_name** | | 用户账号 |
| **token** | | token |
| **reserve** | | 保留字段 |
|  | |  |
| 应答参数 | | |
| 验证通过 | | |
|  | **time** | 系统时间 |
| **reserve** | 保留字段 |
|  |  |
| 验证失败 | | |
|  | **error\_code** | **错误代码** |
| **error\_msg** | **错误信息** |
|  | | |

|  |  |
| --- | --- |
| **Logout** | |
| 功能 | GateWay客户端登出 |
| Topic |  |
| 请求参数 | |
| **user\_name** | 用户名 |
| 应答参数 | |
| **无** |  |

## DDS接口说明

|  |  |  |
| --- | --- | --- |
| **Login** | | |
| 功能 | | 客户端连接DDS服务器进行Token等认证 |
| Topic | |  |
| 请求参数 | | |
| **user\_name** | | 用户账号 |
| **token** | | token |
| **reserve** | | 保留字段 |
|  | |  |
| 应答参数 | | |
| 验证通过 | | |
|  | **time** | 系统时间 |
| **reserve** | 保留字段 |
|  |  |
| 验证失败 | | |
|  | **error\_code** | **错误代码** |
| **error\_msg** | **错误信息** |
|  | | |

|  |  |
| --- | --- |
| **Logout** | |
| 功能 | DDS客户端登出 |
| Topic |  |
| 请求参数 | |
| **user\_name** | 用户名 |
| 应答参数 | |
| **无** |  |

# 服务端接口对接说明

服务端接口的具体设计与对接方所使用的协议相关，同时以第四节的接口及参数设计为依据，这部分的内容已在《单点登录服务接口文档.docx》中详细说明，具体细节请参照这个文档即可。

# 单点登录服务配置文件说明

## 配置文件介绍

1.log4cxx.properties，这个配置文件是log4cxx模块所使用的标准文件，可以通过调整此配置文件控制单点登录服务输出日志的级别、种类、日志按天归档等，具体使用方法请参考官方文档。

2.setting.ini，这个配置文件是单点登录服务使用的，在下一节将全面说明各个配置项。

## 单点登录服务配置项

### msgbus配置模块

1.msgbus.direct.ip：配置msgbus服务ip与端口，用于直连，例如172.16.8.85

2.msgbus.direct.listen\_queue：配置单点登录服务监听队列，主要用于通过msgbus与gateway server通信，例如gateway\_srv\_token\_verify.req.queue

3.msgbus.fanout.ip：配置msgbus服务ip与端口，用于广播，例如172.16.8.85

4.msgbus.fanout.listen\_queue：配置单点登录服务监听队列，主要用于接收广播消息，例如login\_srv\_fanout\_listen.queue

### lava配置模块

1.lava.server.thread：配置lava消息模块工作线程数，一般为cpu内核数

2.lava.server.addr：内置的lava server地址，即单点登录服务实例地址，例如172.16.73.236

3.lava.server.port：内置的lava server端口号，例如10080

4.lava.server.name：内置的lava server名称，用于接入lava服务的验证，与接入zookeeper集群时使用，例如loginsrv.lava\_server

5.lava.server.pwd：内置的lava server授权码，用于接入lava服务的验证，例如123.com

6.lava.cluster.enable：内置lava server是否开启集群运行，0为不开启，1为开启

7.lava.cluster.type：内置lava server开启集群后，设置集群运行方式，0未知，1全活模式，2主备模式，3负载均衡模式，4消息轮询模式

8.lava.cluster.addr：内置lava server开启集群后，设置zookeeper服务地址，例如172.16.73.169

lava.cluster.port：内置lava server开启集群后，设置zookeeper服务端口号，例如2837

### http配置模块

1.http.server.addr：内置http server地址，即单点登录服务实例地址，例如172.16.73.236

2.http.server.port：内置http server端口号，例如8080

3.http.server.root\_path：内置http server的根目录，例如loginservice

4.http.server.name：内置http server的名称，用于接入http server时验证，例如loginsrv.http\_server

5.http.server.pwd：内置http server的授权码，用于接入http server时验证，例如123.com

### gateway配置模块

1.gateway.server.addr：gateway server地址，当客户端登录成功时发送，例如 172.16.8.85

2.gateway.server.port：gateway server端口号，当客户端登录成功时发送，例如1234

### DDS配置模块

1.dds.server.addr：dds server地址，当客户端登录成功时发送，例如172.16.8.85

2.dds.server.port：dds server端口号，当客户端登录成功时发送，例如1234

### login server配置模块

1.loginsrv.token.ttl：token过期时间，单位为秒，例如3600

2.loginsrv.token.scan\_time：过期token扫描时间间隔，单位为秒，例如60

3.loginsrv.lava\_task\_pool\_size：lava 任务池线程数，推荐最大设置为20

4.loginsrv.lava\_msg\_handle\_limit：lava并发任务数限制，超过此数量时，发过来的消息由于来不及处理，服务将其直接丢弃，建议设置为1500

5.loginsrv.msgbus\_task\_pool\_size：msgbus任务池线程数，推荐最大设置为20