**单点登录服务接口文档**

文档管理信息表

|  |  |
| --- | --- |
| **主题** | 单点登录服务接口文档 |
| **版本** | 1.0 |
| **内容** |  |
| **关键字** |  |
| **参考文档** |  |
| **创建时间** | 2019-11-04 |
| **创建人** | 王雷 |
| **最新发布日期** | 2019-11-06 |

文档变更记录表

|  |  |  |
| --- | --- | --- |
| **修改人** | **修改时间** | **修改内容** |
| 王雷 | 2019-11-05 | 初版完成 |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**目 录**

[1 接口总体介绍 1](#_Toc23784905)

[1.1 单点登录服务简介 1](#_Toc23784906)

[1.2 单点登录服务对接对象 1](#_Toc23784907)

[1.3 消息传播方式 1](#_Toc23784908)

[2 基于qpid的msgbus协议接口 1](#_Toc23784909)

[2.1 Gateway Server请求响应接口 1](#_Toc23784910)

[2.2 数据源服务广播接口(用户账号信息增量) 3](#_Toc23784911)

[2.3 Token信息同步广播接口 4](#_Toc23784912)

[2.4 踢出消息广播接口 4](#_Toc23784913)

[3 基于lavabox的ceda协议接口 4](#_Toc23784914)

[3.1 QB Client登录请求响应接口 4](#_Toc23784915)

[3.2 DDS Server请求响应接口 6](#_Toc23784916)

[3.3 踢出消息的订阅接口 7](#_Toc23784917)

[4 基于http协议的接口 7](#_Toc23784918)

[4.1 QB Web的POST请求响应接口 7](#_Toc23784919)

[4.2 数据源服务HTTP接口(主动拉取用户账号信息全量) 9](#_Toc23784920)

# 接口总体介绍

## 单点登录服务简介

单点登录服务login server是Identity Access and Management(IAM)项目一个部分，负责QB客户端的登录验证，QB网关服务、DDS服务以及QB Web端对其管理的客户端token的有效性验证。

## 单点登录服务对接对象

单点登录服务的对接对象按照功能划分主要有：客户端和服务端两种类型，客户端主要是QB client，服务端主要分为QB Web、QB网关服务、DDS服务以及QB用户账户数据源提供者服务等。

按照消息协议划分，主要分为：基于qpid的msgbus协议、基于lavabox的ceda协议以及http协议等，每种协议对应的对接对象如下表：

|  |  |  |  |
| --- | --- | --- | --- |
| **协议名称** | **msgbus** | **lavabox** | **http** |
| **对接对象** | Gateway Server | QB Client | QB Web |
| 用户账户数据源服务  (增量接口) | DDS Server | 用户账户数据源服务(全量接口) |
| Token同步fanout接口(login server内部使用) | -- | -- |
| 踢出消息 | 踢出消息(需要主动向login server订阅) | -- |

## 消息传播方式

描述各个对接对象的消息传播方式，如下表所示：

|  |  |  |
| --- | --- | --- |
| **对接对象** | **消息协议** | **传播方式** |
| **Gateway Server** | msgbus | direct请求响应 |
| **数据源服务(增量)** | msgbus | fanout广播 |
| **Login Server(token同步)** | msgbus | fanout广播 |
| **踢出消息** | msgbus | fanout广播 |
| **QB Client** | lavabox | request\_asyn或request |
| **DDS Server** | lavabox | request\_asyn或request |
| **踢出消息** | lavabox | subscribe接口，需要向login server主动订阅topic |
| **QB Web** | http | post请求响应(login server作为http server) |
| **数据源服务(全量)** | http | post请求响应(login server作为http client) |

# 基于qpid的msgbus协议接口

## Gateway Server请求响应接口

|  |  |
| --- | --- |
| **Gateway Server请求响应接口** | |
| **功能** | Gateway Server向Login Server请求验证QB用户的token |
| **请求参数** | |
| **消息头(Header)** | |
| Type | 80100(假设) |
| Subject | 项目号，目前为空 |
| MessageID | 消息ID，目前为空 |
| ReplyTo | gateway\_srv\_token\_verify.req.queue.rspa |
| **消息体(Body)** | |
| <Map> | [xGtwTokenVerifyReq] |
| --<LIST> | [List] |
| ----<MAP> | [0] |
| ------<STR> | [userName](sumscope\_user\_00001) |
| ------<STR> | [token](336df8681794f308f244da4532ad07efe73ee39f3f4fd5c42177288914da70e0) |
| ----<MAP> | [1] |
| ------<STR> | [userName](sumscope\_user\_00002) |
| ------<STR> | [token](336df8681794f308f244da4532ad07efe73ee39f3f4fd5c42177288914da70e1) |
| ……略 | |
| **符号说明** | <>表示类型，[]表示类型对应的名称，()表示值，--表示嵌套关系 |
| **响应参数** | |
| **消息头(Header)** | |
| Type | 与请求参数的相同 |
| Subject | 同上 |
| MessageID | 同上 |
| ReplyTo | 空 |
| **消息体(Body)** | |
| **内层消息头(Header)** | |
| <MAP> | [AckMsgHead] |
| --<I16> | [retcode](0) 可能值：  =0，消息响应成功，返回内层消息体，其他情况不返回内层消息体  =1，消息解析失败  =2，login server状态异常 |
| --<STR> | [desc](success)  可能值：  =”verify token handle success.”  =“request message parse failed!”  =”server status error!” |
| **内层消息体(Body)** | |
| <MAP> | [AckMsgBody] |
| --<LIST> | [List] |
| ----<MAP> | [0] |
| ------<I16> | [verifyRet](0)  可能值：  =0，验证通过  =-1,验证不通过  =-2,无效用户名 |
| ------<STR> | [verifyMsg](token passed.)  可能值：  =”token passed.”  =“token not passed!”  =“invalid user name!” |
| ------<STR> | [userName](与请求参数相同) |
| ------<STR> | [userId](E316F453-35D3-4517-A10A-80564B727280)  **注意：仅验证通过时会返回userId信息，否则为空** |
| ------<STR> | [token](与请求参数相同) |
| ------<STR> | [serverTime](2019-10-24 10:00:00))  **注意：仅验证通过时会返回userId信息，否则为空** |
| ----<MAP> | [1] |
| ------<I16> | [verifyRet](-1) |
| ------<STR> | [verifyMsg](token not passed!) |
| ------<STR> | [userName](sumscope\_user\_00001) |
| ------<STR> | [userId](E316F453-35D3-4517-A10A-80564B727280) |
| ------<STR> | [token](336df8681794f308f244da4532ad07efe73ee39f3f4fd5c42177288914da70e0) |
| ------<STR> | [serverTime](2019-10-24 10:00:00) |
| ……略 | |

## 数据源服务广播接口(用户账号信息增量)

|  |  |
| --- | --- |
| **数据源增量数据广播接口** | |
| **功能** | 数据源服务通过msgbus的fanout方式向所有login server实时广播增量的用户账户信息。 |
| **请求参数** | |
| **消息头(Header)** | |
| Type | 80102(假设) |
| Subject | 项目号，目前为空 |
| MessageID | 消息ID，目前为空 |
| ReplyTo | 空 |
| **消息体(Body)** | |
| <Map> | [xUserInfoUpdFanout] |
| --<LIST> | [List] |
| ----<MAP> | [0] |
| ------<I16> | [optFlg](0)  可能值：  =0，更新用户账户信息(update)  =1，新增用户账户信息(insert)  =2，删除用户账户信息(delete) |
| ------<STR> | [userName](sumscope\_user\_00001) |
| ----<MAP> | [userPwd](123456.com) |
| ------<STR> | [userId]( E316F453-35D3-4517-A10A-80564B727280) |
| ------<STR> | [cliMacAddr]() |
| ------<STR> | [cliVersion]() |
| ----<MAP> | [1] |
| ------<I16> | [optFlg](1) |
| ------<STR> | [userName](sumscope\_user\_00002) |
| ----<MAP> | [userPwd](123456.com) |
| ------<STR> | [userId]( E316F453-35D3-4517-A10A-80564B727280) |
| ------<STR> | [cliMacAddr]() |
| ------<STR> | [cliVersion]() |
| ……略 | |
| **符号说明** | <>表示类型，[]表示类型对应的名称，()表示值，--表示嵌套关系 |
| **无响应参数** | |

## Token信息同步广播接口

|  |  |
| --- | --- |
| **Token信息同步广播接口** | |
| **功能** | Login Server各个实例之间同步token信息的广播接口。 |
| **请求参数** | |
| **消息头(Header)** | |
| Type | 80101(假设) |
| Subject | 每个login server实例启动后会生成一个唯一的server id(UUID的形式)，该id用于过滤掉广播给自己的消息。 |
| MessageID | 消息ID，目前为空 |
| ReplyTo | 空 |
| **消息体(Body)** | |
| <Map> | [xTokenInfoSyncFanout] |
| --<LIST> | [List] |
| ----<MAP> | [0] |
| ------<STR> | [token](336df8681794f308f244da4532ad07efe73ee39f3f4fd5c42177288914da70e0) |
| ------<I64> | [tokenTime](1571903962)  说明：int64类型时间戳，为格林威治时间1970年1月1日至今的秒数，该时间戳记录token被创建的时间。 |
| ------<STR> | [userName](sumscope\_user\_00001) |
| ……略 | |
| **符号说明** | <>表示类型，[]表示类型对应的名称，()表示值，--表示嵌套关系 |
| **无响应参数** | |

## 踢出消息广播接口

暂无

# 基于lavabox的ceda协议接口

## QB Client登录请求响应接口

|  |  |  |  |
| --- | --- | --- | --- |
| **QB Client登录请求响应接口** | | | |
| **功能** | QB客户端向Login Server请求账号登录验证。 | | |
| **请求参数** | | | |
| **lava server连接验证** | | | |
| server address | lava server的ip或者zookeeper集群的ip。  说明：当login server内置的lava server运行在非集群模式时，此ip即为login server的ip，否则为zookeeper集群ip。 | | |
| server port | lava server的宽口或zookeeper集群端口。  说明：当login server内置的lava server运行在集群模式时，此端口为zookeeper集群端口，否则为lava server指定端口。 | | |
| server name | lava server的名称，用于连接验证。 | | |
| server password | lava server的授权码，用于连接验证。 | | |
| **QB账号登录验证请求(ceda消息)** | | | |
| **域编号** | **域类型** | | **域值** |
| 1-3 | 保留 | | 保留 |
| 4 | INT | | 身份标识码  =0，身份为DDS Server  **=1，身份为QB Client** |
| 5 | INT | | 功能号  **=1，QB Client登录验证请求**  =2，DDS Server验证token请求 |
| 6 | STRING | | 请求参数。  说明：每个请求参数按先后顺序用逗号连接组成一个string字符串：  user\_name,user\_pwd,cli\_mac\_address,cli\_version。  user\_name：用户账户名  user\_pwd：用户密码  cli\_mac\_address：客户端mac地址  cli\_version：客户端版本号 |
| **响应参数** | | | |
| **lava server连接验证响应** | | | |
| uint\_8 | 可能值：  =1，连接成功  =2，lava server名称错误  =3，lava server授权码错误 | | |
| **QB账号登录验证响应(ceda消息)** | | | |
| **域编号** | **域类型** | **域值** | |
| 1-3 | 保留 | 保留 | |
| 4 | INT | 处理结果code。  可能值：  =0，登录成功  =-1，用户账号错误  =-2，用户账号密码错误  =-3，服务器状态异常 | |
| 5 | STRING | 处理结果message。  可能值：  =”login success.”  =“user name not exist!”  =”password not correct!”  =“login server handle failed!” | |
| 6 | STRING | 响应参数。  说明：每个响应参数按先后顺序用逗号连接组成一个string字符串：  user\_name,user\_id,token,server\_sys\_time,dds\_server\_addr,dds\_server\_port,gtw\_server\_addr,gtw\_server\_port。  user\_name：用户账户名  user\_id：用户账户标识，登录失败为空。  token：用户登录成功的token，登录失败为空。  server\_sys\_time：服务器时间，登录失败为空，格式(yyyy-mm-dd hh:mm::ss)  dds\_server\_addr：dds server地址，登录失败为空。  dds\_server\_port：dds server端口，登录失败为空。  gtw\_server\_addr：gateway server地址，登录失败为空。  gtw\_server\_port：gateway server端口，登录失败为空。 | |

## DDS Server请求响应接口

|  |  |  |  |
| --- | --- | --- | --- |
| **DDS Server请求响应接口** | | | |
| **功能** | QB网关服务向Login Server请求token验证。 | | |
| **请求参数** | | | |
| **lava server连接验证** | | | |
| server address | lava server的ip或者zookeeper集群的ip。  说明：当login server内置的lava server运行在非集群模式时，此ip即为login server的ip，否则为zookeeper集群ip。 | | |
| server port | lava server的宽口或zookeeper集群端口。  说明：当login server内置的lava server运行在集群模式时，此端口为zookeeper集群端口，否则为lava server指定端口。 | | |
| server name | lava server的名称，用于连接验证。 | | |
| server password | lava server的授权码，用于连接验证。 | | |
| **QB账号登录验证请求(ceda消息)** | | | |
| **域编号** | **域类型** | | **域值** |
| 1-3 | 保留 | | 保留 |
| 4 | INT | | 身份标识码  **=0，身份为DDS Server**  =1，身份为QB Client |
| 5 | INT | | 功能号  =1，QB Client登录验证请求  **=2，DDS Server验证token请求** |
| 6 | STRING | | 请求参数。  说明：每个请求参数按先后顺序用逗号连接组成一个string字符串：user\_name,token。  user\_name：用户账户名  token：用户登录成功后的token |
| **响应参数** | | | |
| **lava server连接验证响应** | | | |
| uint\_8 | 可能值：  =1，连接成功  =2，lava server名称错误  =3，lava server授权码错误 | | |
| **QB账号登录验证响应(ceda消息)** | | | |
| **域编号** | **域类型** | **域值** | |
| 1-3 | 保留 | 保留 | |
| 4 | INT | 处理结果code。  可能值：  =0，token验证通过  =-1，token验证不通过  =-2，无效用户名  =-3，服务器状态异常 | |
| 5 | STRING | 处理结果message。  可能值：  =”token passed.”  =“token not passed!”  =“invalid user name!”  =“login server handle failed!” | |
| 6 | STRING | 响应参数。  说明：每个响应参数按先后顺序用逗号连接组成一个string字符串：  user\_name,user\_id,token,server\_sys\_time。  user\_name：用户账户名  user\_id：用户账户标识，登录失败为空。  token：用户登录成功的token。  server\_sys\_time：服务器时间，登录失败为空，格式(yyyy-mm-dd hh:mm::ss) | |

## 踢出消息的订阅接口

暂无

# 基于http协议的接口

## QB Web的POST请求响应接口

|  |  |
| --- | --- |
| **QB Web的POST请求响应接口** | |
| **功能** | QB Web以http client的身份向login server发起post请求，请求验证token，login server以http server的身份处理请求并将处理结果返回给QB Web。 |
| **请求参数** | |
| **登录认证请求接口** | **http://172.16.73.169:8080/loginservice/login-auth** |
| **访问方式** | **POST** |
| **数据格式** | **JSON** |
| **消息头(Header)** | |
| Content-Type | application/json |
| **消息体(Body)** | |
| **JSON格式例子** | {  "http\_server\_name":"loginsrv.http\_server",  "http\_auth\_pwd":"123.com",  "user\_name":"sumscope\_user\_00001",  "token":"336df8681794f308f244da4532ad07efe73ee39f3f4fd5c42177288914da70e0"  } |
| **字段说明** | |
| http\_server\_name | http server的服务名称 |
| http\_auth\_pwd | http server的授权访问码 |
| user\_name | QB用户账号名称 |
| token | token |
| **响应参数** | |
| **消息头(Header)** | |
| Content-Length | http body的长度 |
| Content-Type | application/json |
| **消息体(Body)** | |
| **JSON格式例子** | {  "status":"ok",  "code":200,  "data": {  "ret\_code":0,  "ret\_message":"user token authentication success.",  "user\_name":"sumscope\_user\_00001",  "user\_id":"E316F453-35D3-4517-A10A-80564B727280", "token":"336df8681794f308f244da4532ad07efe73ee39f3f4fd5c42177288914da70e0",  "server\_time":"2019-10-24 10:00:00"  }  } |
| **字段说明** | |
| status | http post调用返回消息，可能值：  =”OK”  =“No Content”  =“No Data”  =”Bad Reauest”  =“Unauthorized”  =“Forbidden”  =”Not Found”  =“Internal Server Error”  =“Not Implemented”  =”Bad Gateway”  =“Service Unavailable” |
| code | http post调用返回状态码，可能值：  = 200，ok  = 204, no content  = 205, no data  = 400, bad request  = 401, unauthorized  = 403, forbidden  = 404, not found  = 500, internal server error  = 501, not implement  = 502, bad gateway  = 503, service unavailable |
| **data部分的字段说明** | |
| ret\_code | Token验证结果code，可能值：  =0，认证通过  =-1，认证不通过  =-2，无效用户名  =-3，解析url失败  =-4，请求类型不正确(如根目录不是loginservice或者接口类型不是login-auth)  **=-**5，请求参数不正确，json参数没有正确填写  **=**-6，http server无权访问 |
| ret\_message | Token验证结果message，可能值：  =”token passed.”  =“token not passed!”  =“invalid user name!”  =“parse url failed!”  =”request type not correct!”  =“request parameters no correct!”  =“have no right to access http server!” |
| user\_name | 用户账户名称，同输入参数 |
| user\_id | 用户账户id，验证失败时为空 |
| token | 用户token，同输入参数 |
| server\_time | 服务器时间，格式(yyyy-mm-dd hh:mm::ss)，验证失败时为空 |

## 数据源服务HTTP接口(主动拉取用户账号信息全量)

暂无