签名验签服务-上线方案

由 王辉创建, 最后修改于大约8小时以前

一、资源申请

1、申请新的数据库实例

在rm-2zevjx295d22n5c91.mysql.rds.aliyuncs.com创建数据库实例，数据库名称：api_gw_authentication, 并初始化以下表结构 @孟江桥 2019-10-12 。

完成后提供用户名、密码给@王辉

表名	建表语句
device	create table device (id bigint(15) auto_increment comment '主键id' primary key, device_id varchar(128) default '' not null comment '设备id', device_name varchar(128) default '' not null comment '设备名称', customer_id varchar(128) default '' not null comment '客户id', customer_name varchar(128) default '' not null comment '客户名称', device_cert varchar(2000) default '' not null comment '公钥', securecode varchar(64) default '' not null comment '公钥', status varchar(32) default '' not null comment '状态：NORMAL 正常; STOP 停用; DELETE 删除', create_time datetime default CURRENT_TIMESTAMP not null comment '创建时间', update_time timestamp default CURRENT_TIMESTAMP not null on update CURRENT_TIMESTAMP comment '修改时间') comment 'device' charset=utf8mb4; create index device_id on device (device_id);
platform	create table platform (id bigint(15) auto_increment comment '主键' primary key, platform_id varchar(128) default '' not null comment '平台id', platform_name varchar(128) default '' not null comment '平台名称', rsa_public_key varchar(2000) default '' not null comment '公钥', sm2_public_key varchar(2000) default '' not null comment '公钥', secure_code varchar(64) default '' not null comment '公钥', status varchar(32) default '' not null comment '状态：NORMAL 正常; STOP 停用; DELETE 删除', create_time datetime default CURRENT_TIMESTAMP not null comment '创建时间', update_time datetime default CURRENT_TIMESTAMP not null on update CURRENT_TIMESTAMP comment '修改时间') comment 'platform' charset=utf8mb4; create index app_id on platform (platform_id);
application	create table application (id bigint(15) auto_increment comment '主键' primary key, app_id varchar(128) default '' not null comment '应用id', app_name varchar(128) default '' not null comment '应用名称', customer_id varchar(128) default '' not null comment '客户id', customer_name varchar(128) default '' not null comment '客户名称', status varchar(32) default '' not null comment '状态：NORMAL 正常; STOP 停用; DELETE 删除', create_time datetime default CURRENT_TIMESTAMP not null comment '创建时间', update_time datetime default CURRENT_TIMESTAMP not null on update CURRENT_TIMESTAMP comment '修改时间', rsa_public_key varchar(2000) default '' null comment '公钥', sm2_public_key varchar(2000) default '' null comment '公钥', secure_code varchar(64) default '' null comment '公钥') comment 'applicaiton' charset=utf8mb4; create index app_id on application (app_id);
app_auth_id	create table app_auth_id (id bigint(15) auto_increment comment '主键' primary key, auth_id int default -1 not null comment '验证这个id是否有权限访问app', app_id varchar(128) default '' not null comment '应用id', type int default -1 not null comment '应用id是平台还是客户 0平台, 1客户', create_time datetime default CURRENT_TIMESTAMP not null comment '创建时间', update_time datetime default CURRENT_TIMESTAMP not null on update CURRENT_TIMESTAMP comment '修改时间', status varchar(32) null, auth_id_type varchar(32) not null comment 'api-version-id表示是网关的api verson id;service-id表示是服务的id', constraint ux_auth_id_auth_type_id_app_id_type unique (auth_id, auth_id_type, app_id, type)) comment 'app_auth_id' charset=utf8mb4;

表结构表更 @孟江桥 2019-10-12

表名	库名	备注
developer	api-manager	去掉developer_name字段的唯一索引 alter table developer drop key idx_developer_developer_name;
developer	api-manager	修改developer_key字段长度到64 alter table developer modify developer_key varchar(64) charset latin1 default '' not null comment 'key';
developer	api-manager	修改develop_name字段的编码： ALTER TABLE developer MODIFY COLUMN developer_name VARCHAR(64) CHARACTER SET utf8mb4 COLLATE utf8mb4_unicode_ci;

申请阿里云生产环境vip server（api-manager-servers使用），网关机器可以访问该vipserver。 @孟江桥 2019-10-12
vipserver后端挂载的机器列表：

ip	port
192.168.29.11	10000
192.168.37.82	10000

ng网关机器列表：

ip	备注
192.168.20.5	外网ng
192.168.38.157	外网ng
192.168.38.161(B区-网关服务内网02)	内网ng
192.168.20.7 (C区-网关服务内网01)	内网ng

申请新的服务器，总共3台机器，旧版本鉴权服务逐步迁移到新机器，用于鉴权服务迁移 @孟江桥 2019-10-12
服务器配置：
cpu：2
内存：4GB
硬盘：100GB

挂载新机器到vipserver
把上述新申请的机器挂载在192.168.29.15:10902 这个vipserver上，配置最低权重，待服务部署完成、数据同步结束、验证通过之后挂载。 @孟江桥

二、应用部署：

名称	备注
MSSM-auth	@王辉 时间：待资源申请结束之后上线。 鉴权服务。 1、增加密钥同步接口； 2、增加授权控制； 3、清理tomcat的access_log日志 通过统一发版平台发版，用户：footstone（旧鉴权服务使用的用户是：msspoper） **部署方案：** 方案一、申请新机器（阿里云短期服务器）部署，待稳定后可释放机器。 配置要求： cpu：2U 内存：4GB 硬盘：100GB 负载均衡要求： 添加到负载均衡器中 方案二、部署在原有机器上，部署时，修改服务的端口号。 目前线上机器部署了3个java应用，其中两个运管的应用需要等开放平台上线之后才能迁移，内存不够。

三、接口发布：

发布同步密钥接口，待ng网关上线后发布授权接口（因为ng网关没有传递id过来，不进行授权校验） @王辉 //mssm-auth应用上线后发布。

注意：同步密钥等接口的内网ip地址为新部署的鉴权服务地址

四、鉴权数据准备：

公钥数据同步 @zhangkexin //待鉴权服务接口发布后进行。
补齐平台数据中的securecode(develop-key) @zhangkexin
公钥数据校对 @王辉 @zhangkexin //数据同步之后进行比对，对比两库的数据条数。
新、旧鉴权服务并行期间，保证新老库数据同步 @zhangkexin //鉴权服务新老并行期间
网关develop-key数据进运管库，方式：手动导出 @王辉 @zhangkexin // 待鉴权服务全量上线之后进行
鉴权服务、ng网关（只增加id）上线后，汇总线上appId列表、api-version-id列表给运管，运管来初始化授权数据 @王辉 @zhangkexin //鉴权、网关上线之后

五：鉴权服务测试脚本

对鉴权服务进行测试 @王辉 //鉴权数据校对完毕后进行

不传递id （测试时，ip:port地址替换为新的鉴权服务）

```
curl -X POST \
  http://192.168.29.20:10902/mssm/v3/auth/api/customerVerify \
  -H 'Content-Type: application/json' \
  -H 'Postman-Token: ff4340fe-f1f1-41f8-9aa5-5324910f0bcc' \
  -H 'cache-control: no-cache' \
  -d '{"signAlgo":"HmacSHA256","signature":"mvF9bWd+KmTmjv/vFiubdVWHWhpNXoetHt7XZQZZVBo=","appId":"APP_1698D243C3D04C46B1D488EBAE2F8348","deviceId":"DEV_37A4DD248CDC4DB7ADE0D3626CAB24CA
```

六、切流量：

通知运维同学切最小权重的流量到新鉴权服务。 @孟江桥

七、回归测试

测试同学进行回归测试，新旧鉴权服务均能正常使用。 @yuqi @王思宇

八、埋点监控

修改告警规则，只在签名不通过时进行告警，参数校验不通过 @王辉 //待鉴权服务整体上线完毕之后