1 引言

1.1 概述

1.2 参考资料

- spring cloud 官网资料;

1.3 名词约定

- 一种服务：一个服务项目，也是一个微服务的服务单元；

2 构架描述

2.1 技术选型

- 服务注册第三方包 Netflix Eureka;
- web 后台服务 spring boot;
- 微服务：spring cloud;
- 前端UI：JSP;

3 需求说明

服务注册时需要使用非对称加密对注册的服务进行校验，每个服务通过服务中心的管理员获得证书公钥，及证书ID；
一种服务可以有多个可用的证书。
一个证书只能注册一种服务。

4 数据库设计

t_server_central_rsa
c_public_key ------------ Varchar-256 --- // 公钥 HEX 编码字符; c_private_key ------------ Varchar-256 --- // 私钥 HEX 编码字符; c_server_name ------------ Varchar-256 --- // 服务名称; c_status ---------------- int-1 --------- // 证书状态; 0-正常；1-禁用; c_del_flag -------------- int-1 --------- // 删除标识; 0-正常；1-删除; c_create_date ------------ DATETIME ------ // 创建时间戳; c_create_user ------------ Varchar-256 --- // 创建用户; c_update_date ------------ DATETIME ------ // 修改时间戳; c_update_user ------------ Varchar-256 --- // 修改用户; c_valid_start_date ------ DATETIME ------ // 生效日期; c_valid_end_date -------- DATETIME ------ // 过期日期;

5 功能模块

服务中心的功能分为两个模块：

1. 一个服务信息功能，提供服务注册信息，及相关证书控制。
2. 另一个是服务功能，服务注册，续约及相关微信服务相关功能。

5.1 服务中心信息

此功能通过 web 拦截器，来管理处理对用户的权限需求。

5.1.1 权限管理-用户信息

通过用户登录发放，用户及密码通过配置文件配置，可以操作服务信息下功能。
令牌 30 分钟过期，可配置。
令牌过期、失效不存在时，跳转到登录页面;

5.1.2 用户登录面

通过JSP实现 WEB 页面；

5.1.3 服务信息[仪表盘]

1. 开始 eureka 提供的仪表盘UI；eureka.dashboard.enabled = false;
2. 自定义 eureka 仪表盘页面，在仪表盘 JSP 中引入 eureka 仪表盘页面。

5.1.4 证书管理

管理服务注册证书，证书字段包含：公钥【hex编码的字符串】、密钥【hex编码的字符串】、服务名称、生效起始日期、到期日期。

证书指定服务注册时服务名称、生效日期区间，服务注册与服务续约时，需校验服务名称及生效日期区间，启用禁用状态。
提供，生成，下载，禁用/启用，删除 四个功能。

1. 生成
   输入证书的服务名称【必输】，生效日期区间【起始时期不输入，立即生效；结束日期不输入，永不失效】
2. 列表
   展示，证书服务名称，有效日期区间，启用/禁用，操作列【删除，下载】
3. 下载
   下载公钥 .cer 文件；
   文件内容格式说明：第1行为证书ID，第二行为证书公钥。
4. 禁用/启用
   启用，禁用；
5. 删除；
   删除证书

5.2 服务中心服务功能

此功能通过多个 web 拦截器，来管理不同服务功能对证书的权限需求。

5.2.1 权限管理-证书令牌

在服务注册时发放，可以使用相关服务功能，如：继约，摘取服务列表等。
证书令牌过期时间为服务续约时间再加3分钟，在服务续约时，令牌会自动更新有效期。
令牌校验：令牌过期、令牌不存在；分别提示：

证书校验：证书不存在、证书禁用、证书已被删除、证书过期、解密失败、注册服务名称不一至；分别提示：

服务注册时进行证书校验；服务续约时进行令牌及证书校验；其他服务中心服务功能只校验令牌是否有效校验，不做证书校验。

5.2.2 服务注册

1. 服务注册程序流程
   通过拦截器实现注册的证书校验，拦截指定的路径：/eureka/apps/*
2. 注册功能
   同 Eureka 原有功能

5.2.3 其他服务中心服务功能

1. 证书信息校验程序流程
   通过拦截器，拦截指定的路径：/eureka/xxx/*
2. 续约功能
   同 Eureka 原有功能

6 错误码

错误码	错误信息
zk.ser.cen.000001	未登录，请登录。
zk.ser.cen.000002	登录过期，请重新登录。
zk.ser.cen.000003	证书令牌不存在，请使用证书注册服务。
zk.ser.cen.000004	证书令牌过期，请重新使用证书注册服务。
zk.ser.cen.000005	证书不存在，请通过管理员获取证书。
zk.ser.cen.000006	证书已被删除，请联系管理员更新证书。
zk.ser.cen.000007	证书已被禁用，请联系管理员更新证书。
zk.ser.cen.000008	证书过期，请联系管理员更新证书。
zk.ser.cen.000009	证书解密失败。
zk.ser.cen.000010	证书与注册服务名称不一至。
zk.ser.cen.000011	证书生成异常。
zk.ser.cen.000012	账号不能为空。
zk.ser.cen.000013	密码错误。
zk.ser.cen.000014	账号不存在。
zk.ser.cen.000015	未知的登录错误。
zk.ser.cen.000016	接口通信错误，请联系管理员。