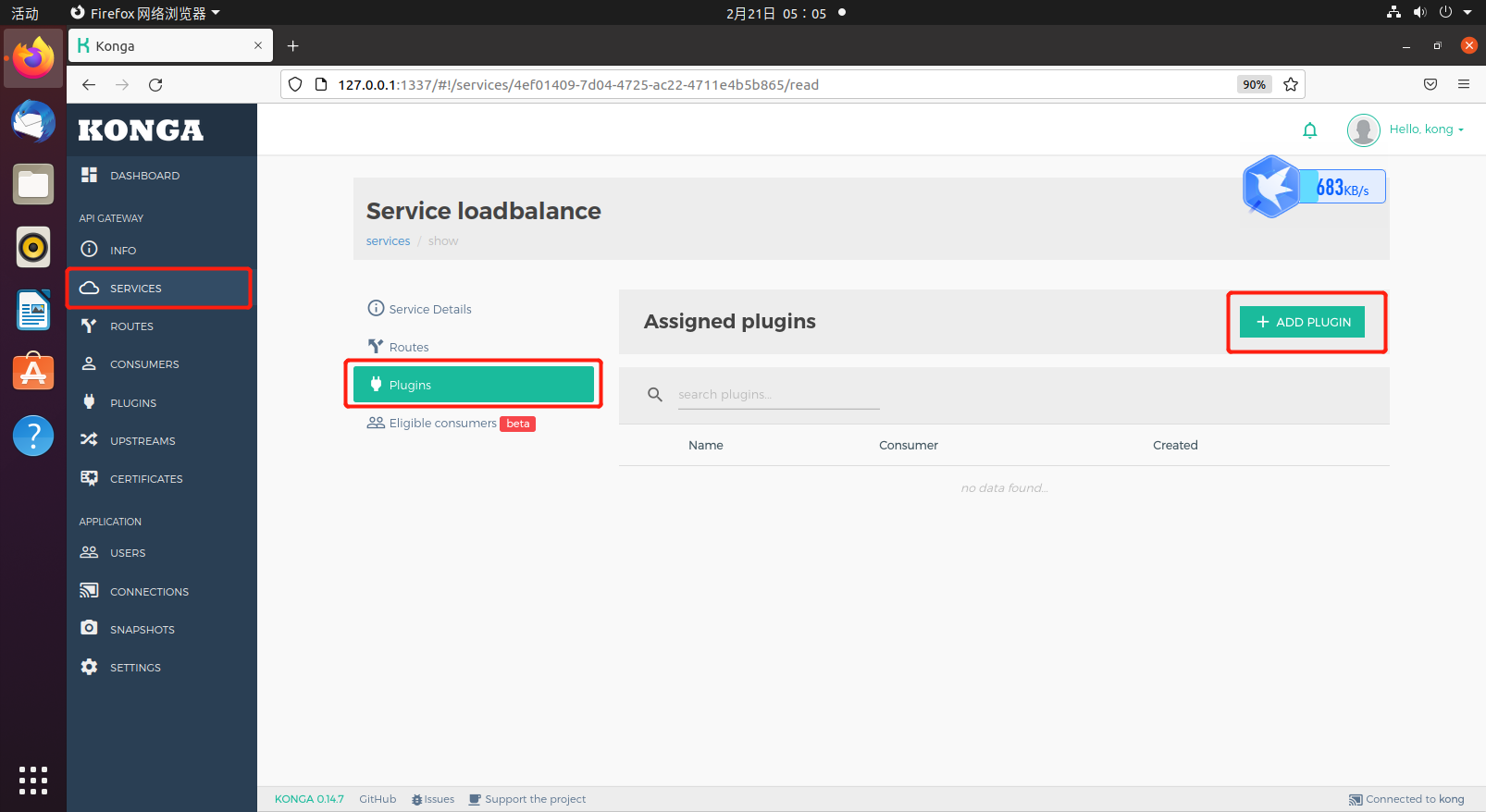
本篇文件介绍Kong内置的一些插件

注：本篇文章纯属鸡肋

**添加插件**

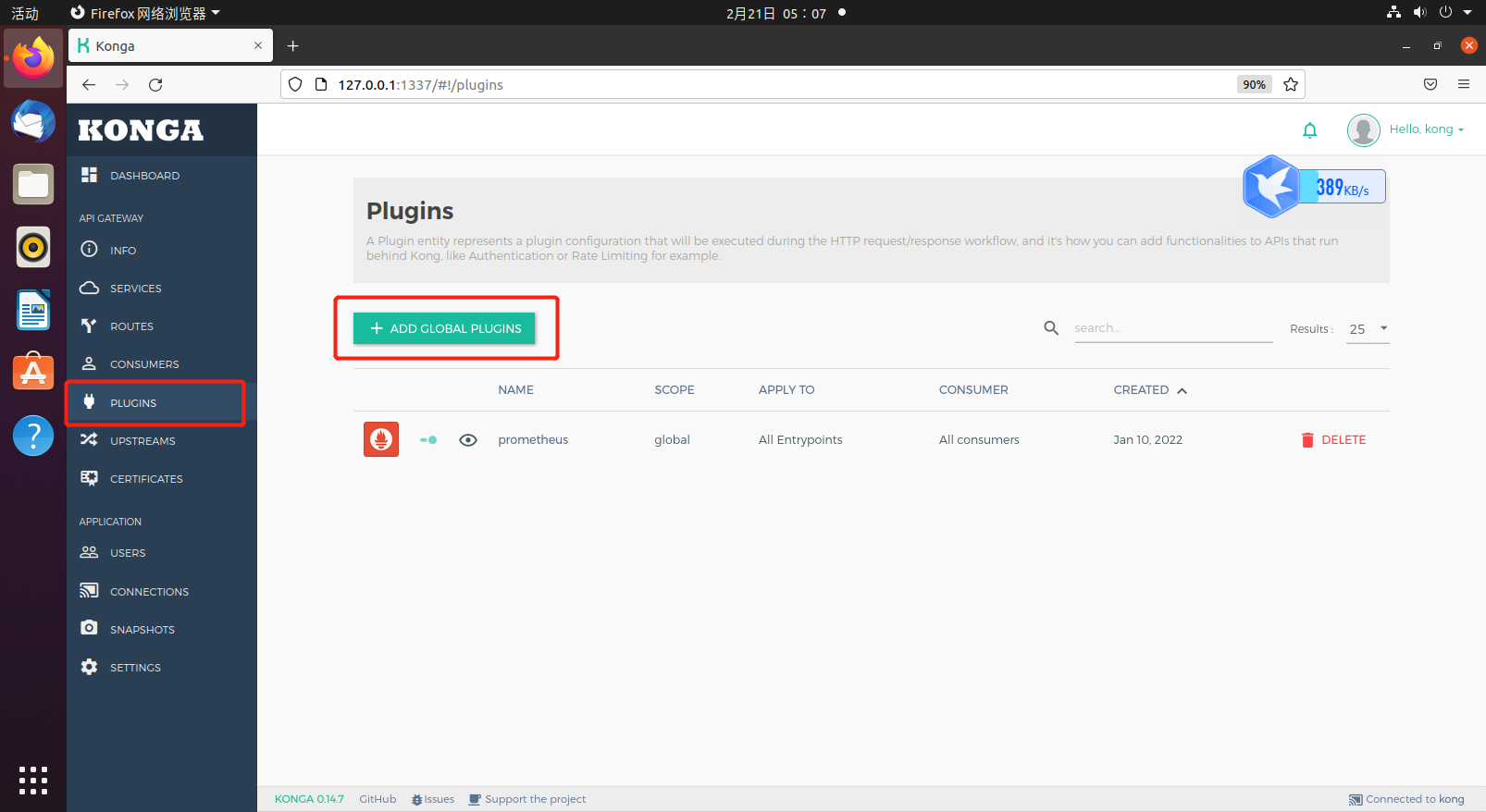
1. 针对某个服务的插件

进入服务详情页面，Plugins标签页下面添加插件



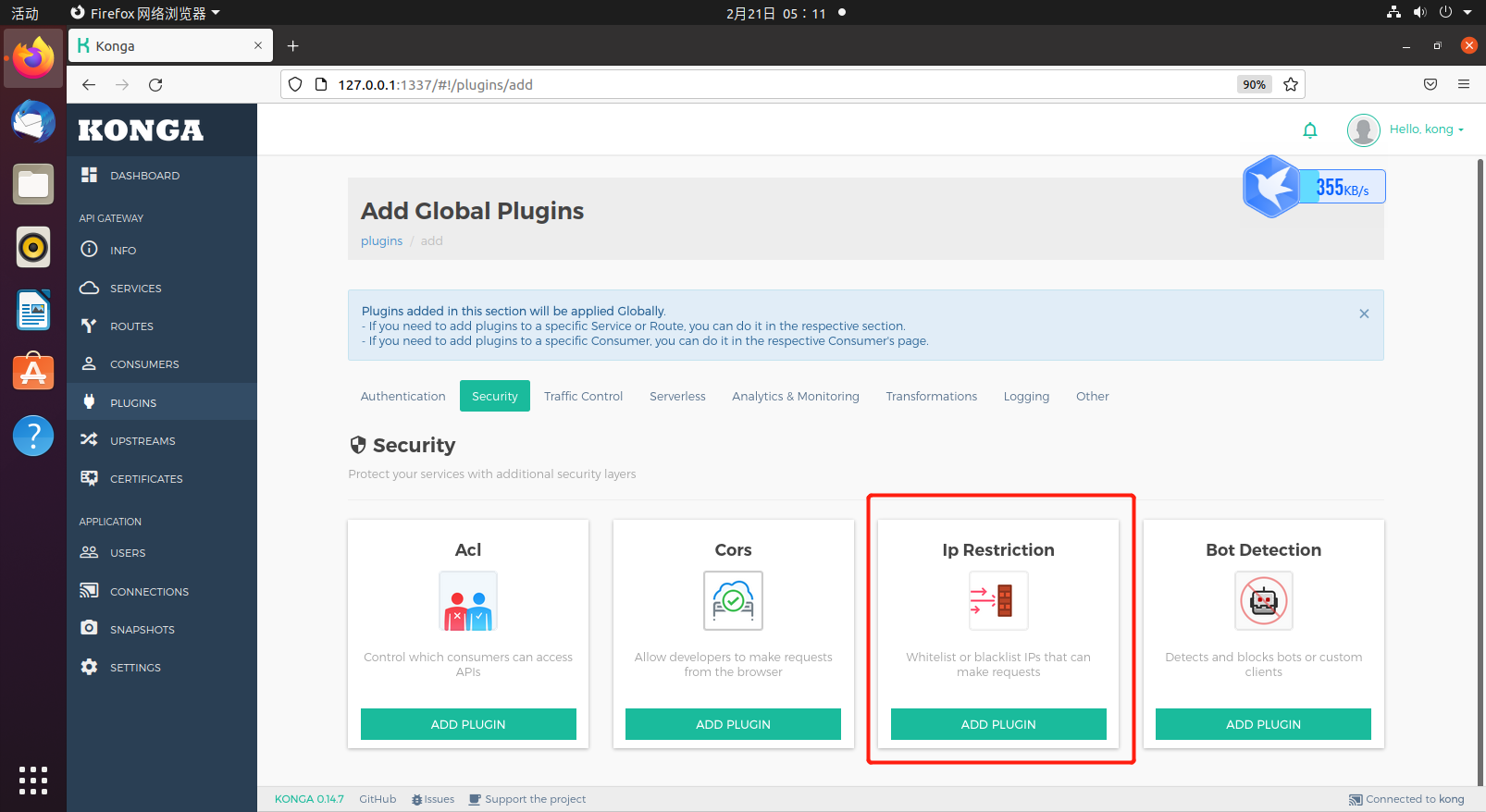
1. 全局插件

在PLUGINS页面可以添加全局插件



**IP限制插件**

Security -> ip restriction 为IP限制插件



其包含字段如下：

consumer：要应用的消费者，为空为应用到所用消费者

whitelist：IP白名单列表，不在白名单内的不运允许访问

blacklist：IP黑名单列表，在黑名单内的不允许访问

注：whitelist和blacklist只能填写一个

**机器人检测插件**

Security -> bot detection 为机器人检测插件

其包含字段如下：

consumer：要应用的消费者，为空为应用到所用消费者

whitelist：白名单正则表达式列表，不在白名单内的不运允许访问

blacklist：黑名单正则表达式列表，在黑名单内的不允许访问

注：whitelist和blacklist只能填写一个，将根据Http头的User-Agent字段进行匹配

**CORS跨域插件**

Security -> Cors 为跨越插件

其包含的字段如下：

consumer：要应用的消费者，为空为应用到所用消费者

origins：允许的跨域源列表，\*为允许所有

其他字段：不做介绍，不认识

**关于Kong的认证授权**

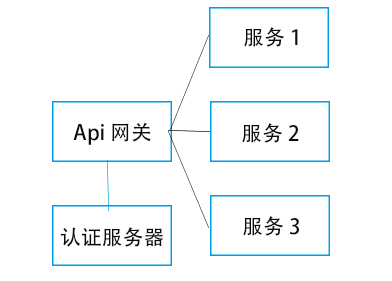
1. 关于微服务授权的2种方式

方式1）

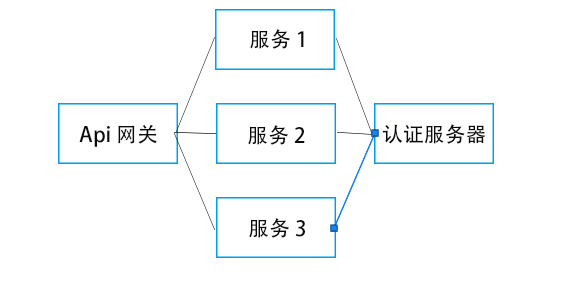
这种方式网关与认证服务器相连，由网关统一管理API的认证

优点：服务不在关心认证

缺点：服务无法控制权限



方式2）



优点：每个服务可以控制自己的权限

缺点：每个服务都需要引入认证代码

1. 基于网关的同一认证

没有教程 ======

本来想做一个基于OIDC的教程，但是官方的OIDC插件需要企业版才能安装，github上面的插件安装了又报错，一直每解决，索性就不写了

1. 基于各自服务的认证

没有教程 ======

基于各自服务的认证与kong教程无关，百度搜索OIDC可以给你一个解决方案