## 鉴权系统设计

目前是单一系统使用shiro+jwt进行用户鉴权

未来如果系统水平扩展只需要把session在公共redis中存储就可以了

如果拆分成多个系统使用sso架构模式

如果对外提供服务，涉及到跨域问题，需要使用oauth2系统设计。

为什么使用jwt？

Jwt是json web token的意思，提供了现有的实现，已经定义好请求的格式和解析类，直接使用就可以了，使用json方便前后台开发。

为什么使用jwt和shiro结合？

Jwt提供了前台友好的支持，但是没有session验证等功能，所以需要shiro权限系统来弥补。

开发方法？

资源和鉴权服务进行分离。鉴权使用aop前面和filter方式进行开发，对资源访问没有侵入。可以独立开发。

Sso和oauth2.0的区别？——使用场景不同。实现技术不同。

分布式鉴权sso，单点登录，一处登录到处运行。

参与者是：单点登录和子系统。实现技术主要是session共享。

分布式授权oauth2.0，使用场景是对第三方授权，但是第三方还是从服务提供方获得数据。

参与者是：第三方和服务提供方还有服务提供方的授权服务。实现技术主要是token。

Jwt格式？

客户端：

fetch('api/user/1', {

headers: {

'Authorization': 'Bearer ' + token

}

})

服务端token生成格式：

三部分