<https://blog.csdn.net/qq_24127857/article/details/80818742>

原

# 关于token和refresh token

2018年06月26日 18:00:27 [米粒人生](https://me.csdn.net/qq_24127857) 阅读数：2370 标签： [认证](http://so.csdn.net/so/search/s.do?q=%E8%AE%A4%E8%AF%81&t=blog)[token](http://so.csdn.net/so/search/s.do?q=token&t=blog)[refresh token](http://so.csdn.net/so/search/s.do?q=refresh%20token&t=blog) 更多

个人分类： [架构](https://blog.csdn.net/qq_24127857/article/category/7759221)

版权声明：本文为博主原创文章，未经博主允许不得转载。 https://blog.csdn.net/qq\_24127857/article/details/80818742

最近在做公司的认证系统，总结了如下一番心得。

传统的认证方式一般采用cookie/session来实现，这是我们的出发点。

~~1.为什么选用token而不选用cookie/session？  
本质上token和cookie/session都是字符串，然而token是自带加密算法和用户信息(比如用户id)，；而cookie本身不包含用户信息，它指向的是服务器上用户的 session，而由session保存用户信息。这点差别，决定token可以很容易的跨服务器，只要不同服务器实现相同解密算法即可；而cookie/session是存在于某一台服务器上，~~

~~要实现跨服务器比较困难，这是任何基于cookie/session应用天生的短板。~~

李孟军：第一点作者的理解狭隘了，或者说有很大偏差，不予采纳。应用的场景和解决的问题压根就不一样。

2.token需要过期时间吗？  
token即是获取受保护资源的凭证，当然必须有过期时间。否则一次登录便可永久使用，认证功能就失去了其意义。非但必须有个过期时间，而且过期时间还不能太长，

参考各个主流网站的token过期时间，一般不超过1h.

3.token过期该怎么办？  
token过期，就要重新获取。那么重新获取有两种方式，一是重复第一次获取token的过程(比如登录，扫描授权等)，这样做的缺点是用户体验不好，每一小时强制登录一次几乎是无法忍受的。那么还剩第二种方法，那就是主动去刷新token. 主动刷新token的凭证是refresh token，也是加密字符串，并且和token是相关联的。相比获取各种资源的token，refresh token的作用仅仅是获取新的token，因此其作用和安全性要求都大为降低，所以其过期时间也可以设置得长一些。

4.refresh token需要过期时间么？  
客户端需要保存token和refresh token，以便下一次访问能继续。如果客户端是浏览器，那么两个token都需要设置过期时间；但是可以设置得长一点，可以以天为单位（例如7天、15天）；如果客户端是一个服务器，那么refresh token可以永久有效，直到下一次登录，refresh token本身被更新为止。

李孟军：个人认为refresh token时间可以设置长一点，要根据业务需要。

通常情况下，可以设置为几倍于accessToken的有效期，但是refresh token最好到期后就失效，不再续期，

每次使用refresh token换取新的accessToken的时候，也会返回新的refresh token，但是refresh token不续期。

以上几个问题是层层递进的，虽说如此，也无法从逻辑上/理论上保证认证系统的绝对安全。但是，我觉得任何一种认证方式，都不能做到逻辑上的绝对安全和毫无漏洞。但是如果给攻击者造成了足够的麻烦，使其破解成本大大提升，那么我们就认为认证系统足够安全了。认证功能最后的落地实现，总是和现实想妥协的结果。