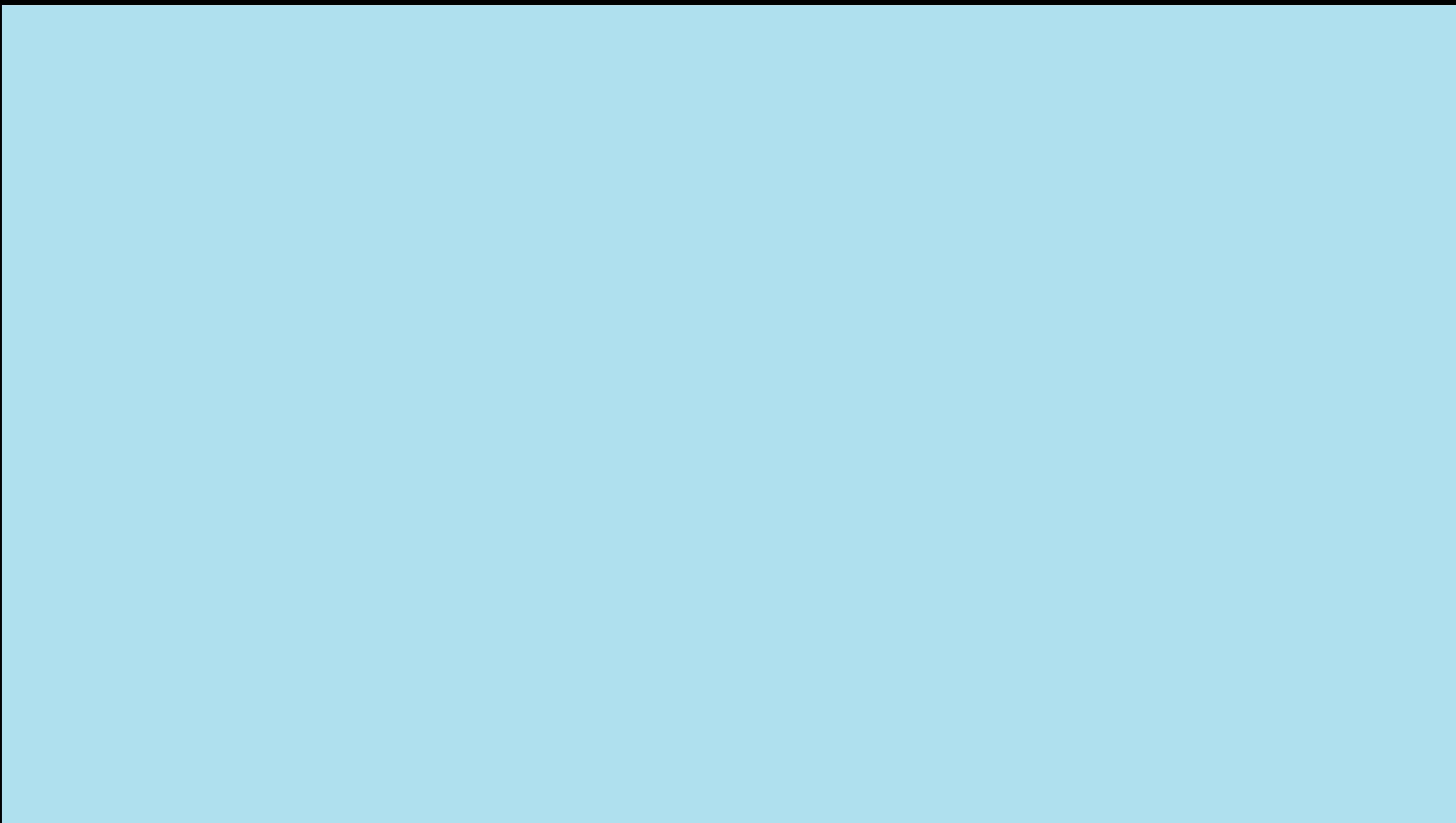


Tnc OssService 实现和解读

tnc 公共库里面 oss 交互的实现
怎么通过前端和服务端协作完成 oss 文件鉴权
公司内部使用 oss 的几种产品实践

王先淦 2020.4.27

- 什么是 Oss
- tnc OssService
- fenbi-oss-server
- 举几个🍑
- 参考资料
- Q & A



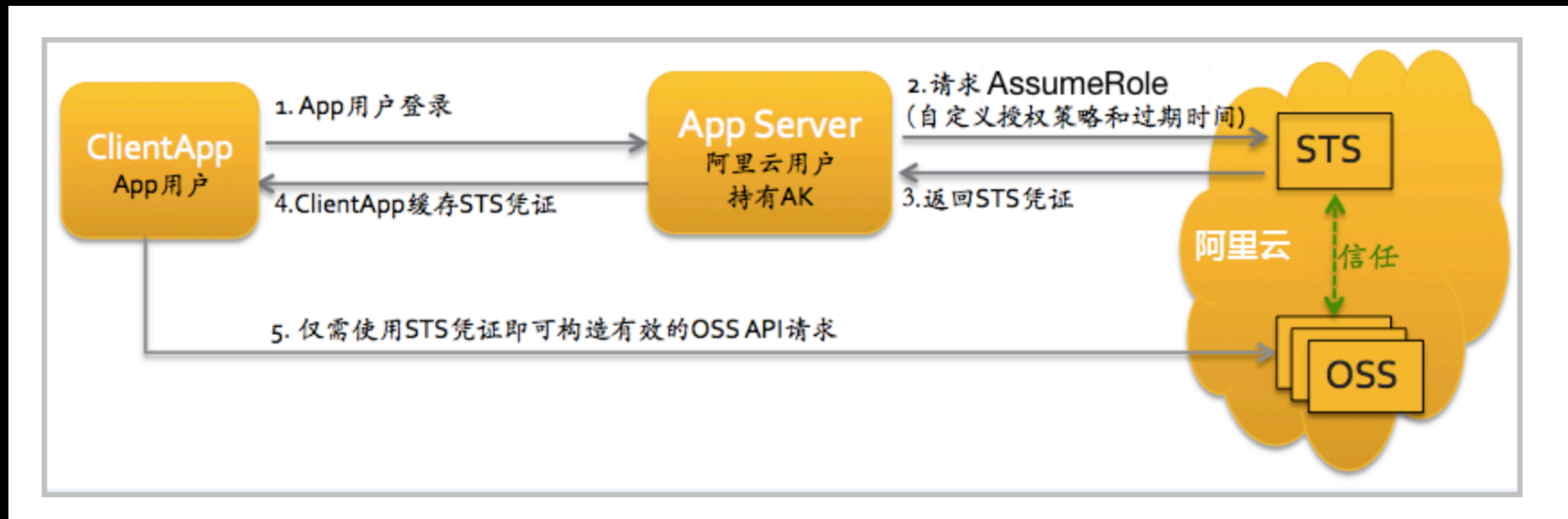
阿里云对象存储服务（Object Storage Service, 简称 OSS）

- 存储空间（Bucket）
 - 存储空间是您用于存储对象（Object）的容器，所有的对象都必须隶属于某个存储空间。存储空间具有各种配置属性，包括地域、访问权限、存储类型等。您可以根据实际需求，创建不同类型的存储空间来存储不同的数据。
- 对象/文件（Object）
 - 对象是 OSS 存储数据的基本单元，也被称为 OSS 的文件。对象由元信息（Object Meta）、用户数据（Data）和文件名（Key）组成。对象由存储空间内部唯一的 Key 来标识。
- 地域（Region）
 - 地域表示 OSS 的数据中心所在物理位置。
- 访问域名（Endpoint）
 - Endpoint 表示 OSS 对外服务的访问域名
- 访问密钥（AccessKey）
 - AccessKey（简称 AK）指的是访问身份验证中用到的 AccessKeyId 和 AccessKeySecret。OSS 通过使用 AccessKeyId 和 AccessKeySecret 对称加密的方法来验证某个请求的发送者身份。AccessKeyId 用于标识用户；AccessKeySecret 是用户用于加密签名字符串和 OSS 用来验证签名字符串的密钥，必须保密。

API 文档

- <https://www.alibabacloud.com/help/zh/doc-detail/31965.htm?spm=a2c63.p38356.b99.910.5dfe1833TCT4C9>

阿里云STS (Security Token Service) 临时授权访问



tnc OssService 干了什么


- 根据传参获取 sts
- 根据 sts 设置 Put 方法所需要的 headers
 - Content-md5
 - Security-Token
 - OSS-Date
- 计算签名
- 处理返回数据

Authorization字段计算的方法

```
Authorization = "OSS " + AccessKeyId + ":" + Signature
Signature = base64(hmac-sha1(AccessKeySecret,
    VERB + "\n"
    + Content-MD5 + "\n"
    + Content-Type + "\n"
    + Date + "\n"
    + CanonicalizedOSSHeaders
    + CanonicalizedResource))
```

细节分析如下：

- `AccessKeySecret` 表示签名所需的密钥。
- `VERB` 表示HTTP请求的Method，主要有PUT、GET、POST、HEAD、DELETE等。
- `\n` 表示换行符。
- `Content-MD5` 表示请求内容数据的MD5值，对消息内容（不包括头部）计算MD5值获得128比特位数字，对该数字进行base64编码得出。该请求头可用于消息合法性的检查（消息内容是否与发送时一致），例如”eB5eJF1ptWaXm4bijSPyxw==”，也可以为空。详情请参见[RFC2616 Content-MD5](#)。
- `Content-Type` 表示请求内容的类型，例如”application/octet-stream”，也可以为空。
- `Date` 表示此次操作的时间，且必须为GMT格式，例如”Sun, 22 Nov 2015 08:16:38 GMT”。
- `CanonicalizedOSSHeaders` 表示以x-oss- 为前缀的HTTP Header的字典序排列。
- `CanonicalizedResource` 表示用户想要访问的OSS资源。

 **说明** 其中，Date和CanonicalizedResource不能为空。如果请求中的Date时间和OSS服务器的当前时间差15分钟以上，OSS服务器将拒绝该请求，并返回HTTP 403错误。

Fenbi-oss-server

- 数据库存储 AK 通过通过 sts 提供临时鉴权服务
- fos 通过数据库配置权限限制用户获取临时鉴权
- 上传文件重名覆盖校验

应用

- 纯网盘 =_=||
 - 前端项目代码目前放到 bucket static-nginx-test
- 数据备份
 - 课件编辑器生成的 pdf 课件 / 互动题播放器 js 代码 （每个版本）
- 服务端异步生成文件
 - 教研下载错题 / Guten 生成图书
- to C 用户个人空间

参考资料

- <https://www.alibabacloud.com/help/zh/doc-detail/31817.htm?spm=a2c63.p38356.b99.4.12bd276d35eqyR>

Q & A

Thanks