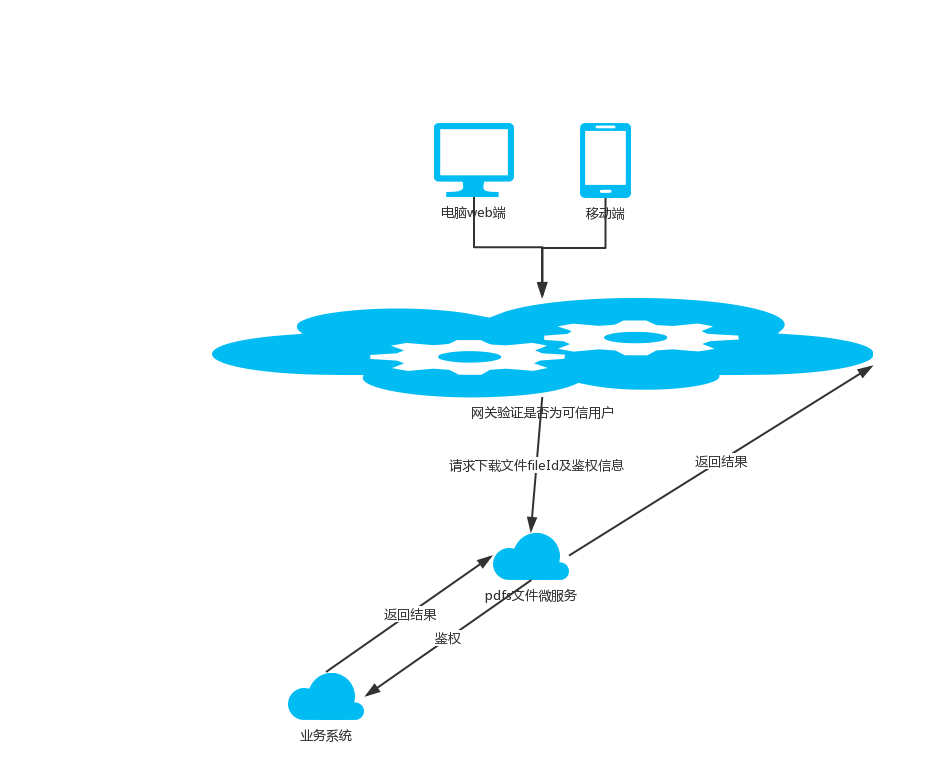
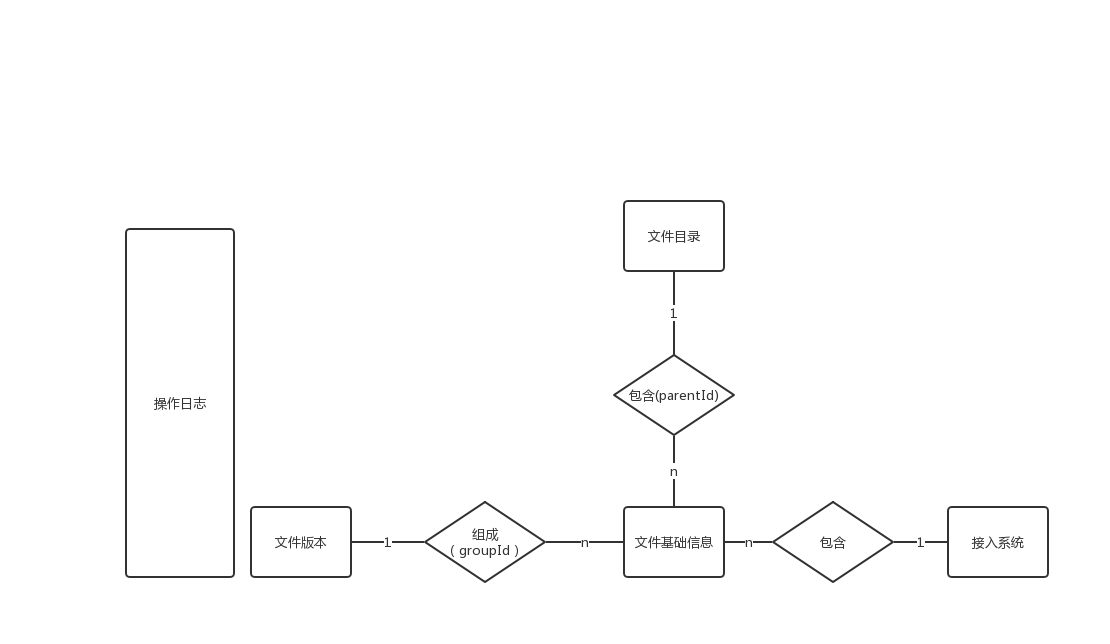
# 整体设计思路

文件系统是放在内网中的一个微服务，文件系统是不带用户的，用户权限等应有业务方鉴权接gsso或者其他。

前端首先应该经过网关，网关验证用户是否为可信用户，如果通过，则可调用文件系统。



## 数据库设计



## 文件基本操作

上传、下载、批量上传、批量下载、预览、秒传、删除、断点续传

## 批量上传、批量下载

限制最大大小及数量（可配置式）

批量限制最大200M

数量100个文件

个人用户限制500M大小

## 预览

设置返回给浏览器的消息头Content-Disposition去掉attachment;

## 断点续传

设置切片大小上传

## 秒传

通过文件指纹识别服务器中是否已经上传过，如已经有上传过相同文件，则实现秒传。

## 删除

彻底删除判断是否有秒传数据，如有，只删除数据库数据，服务器文件不能删除。

## 文件目录

类似于菜单的形式，通过parentId指定上级菜单。带有文件目录的上传、批量上传。

**文件重命名**

文件重命名，记操作日志。

## 版本

可查看该文件的所有版本列表

带文件版本上传

## 权限的设计

所有文件、文件夹权限均可分为私有权限---只有创建人自己可以操作，其他人读、写都需要鉴权、可读（读不需要鉴权、写需要鉴权）、可读写（读写都不需要鉴权）权限、关闭鉴权。

技术实现：

AOP拦截所有方法，码表（配置中心）定义哪些方法是读操作、哪些方法是写操作，再进行权限认证。逻辑流程见[权限设计流程图](#_权限设计流程图)

### 系统级权限的设计

当系统级权限开启鉴权（authstate为私有权限、可读、可写）时，

文件上设置了权限，则以文件上的为准；

当文件上没有设置权限时，文件夹有权限，以文件夹的权限为准；

当文件及文件夹都没有权限时，以系统级权限为准。

当系统级权限关闭鉴权（authstate为关闭鉴权）时，

文件上设置了权限，则以文件上的为准；

当文件上没有设置权限时，文件夹有权限，以文件夹的权限为准；

### 文件夹级权限设计

设置文件夹级的权限只对该下层的文件生效可读、可读写权限，不对该下层的文件夹或者下下层的文件生效。

设置了文件夹级权限，则该文件夹下的文件都具有该文件夹级的权限，也可对该文件夹下的文件设置单独的权限。

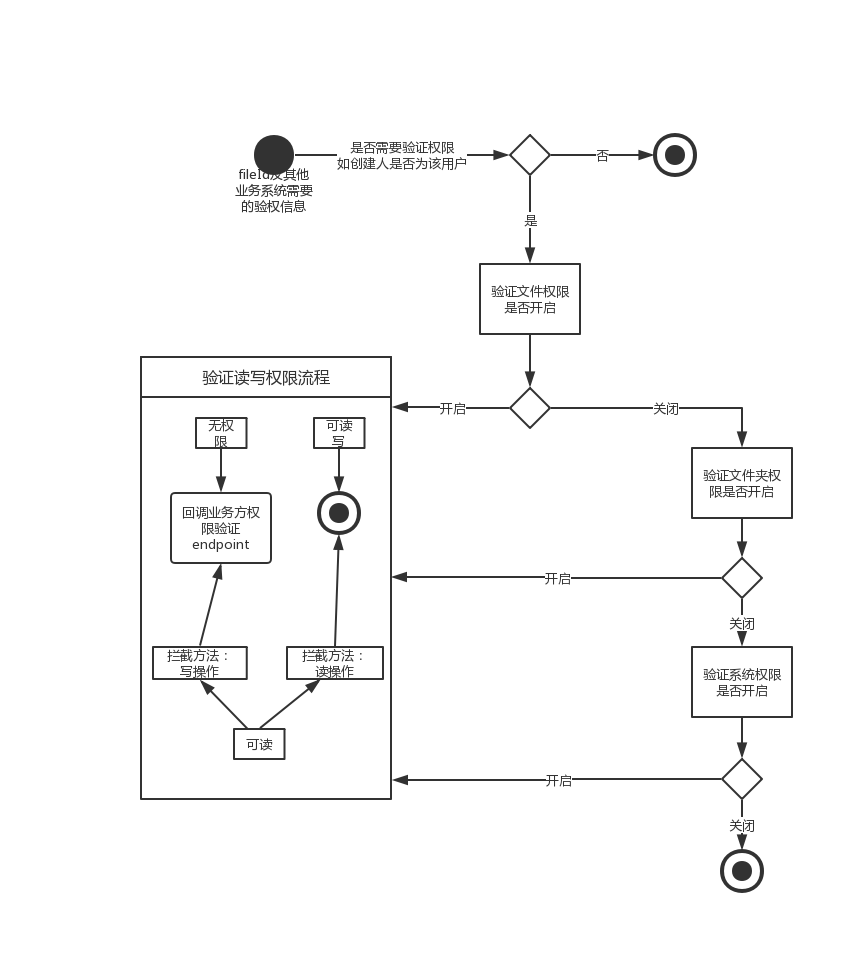
系统实现：

对文件夹设置权限时，不会对下层文件设置权限，防止移动文件、新建文件产生额外的操作。只会对文件夹进行权限操作。只是判断权限的时候需要查询文件夹级的权限。

当文件夹和文件都有权限时，以文件权限为准。

文件权限优先级：文件>文件夹>系统级

### 权限设计流程图



## 租户概念

每张表设计appid来隔离每个业务系统

## 数据权限

通过appid or appid+userid进行隔离

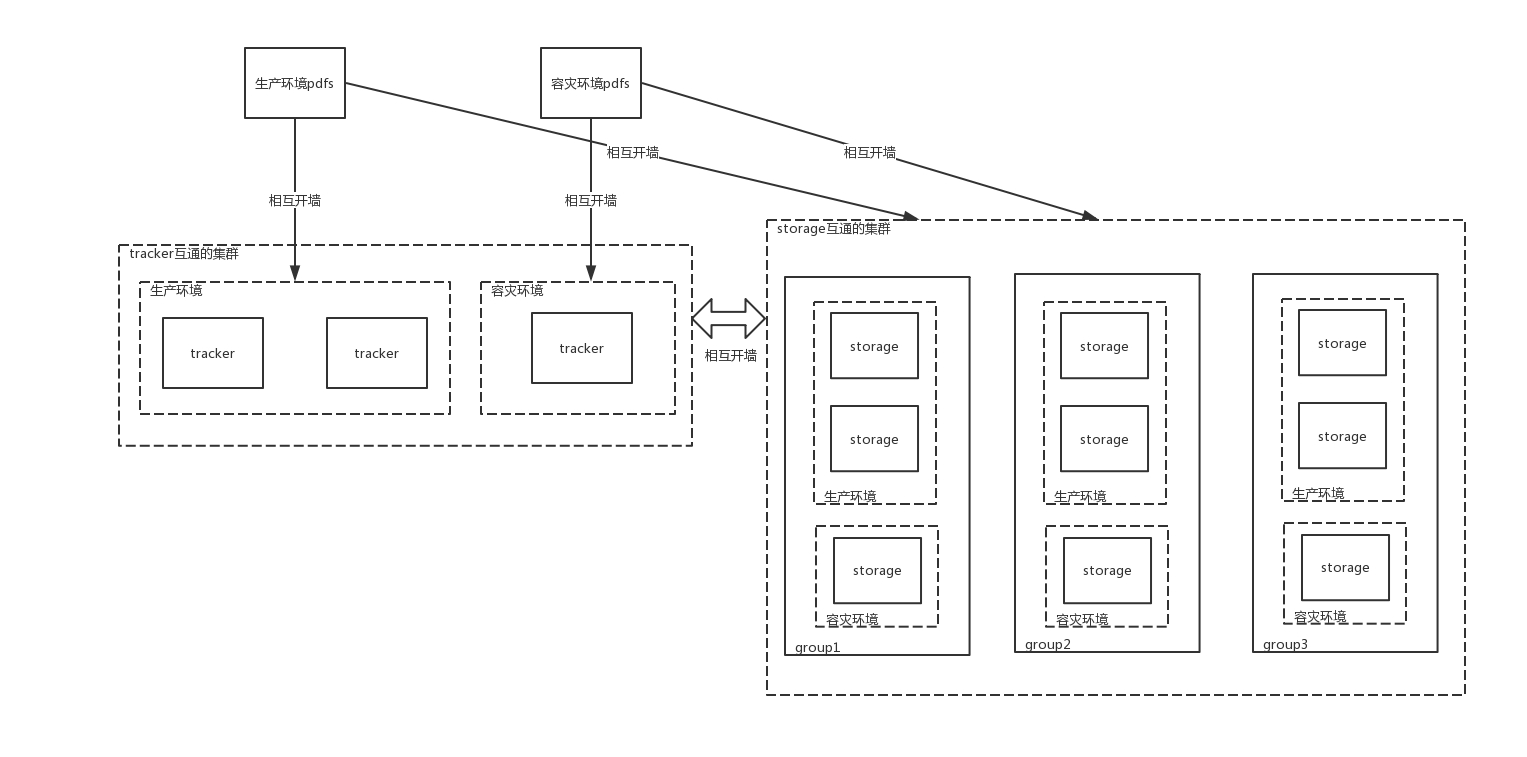
## 容灾备份

容灾环境中的tracker放入tracker集群中，容灾环境中的storage分别加入相应的group卷中

生产环境正常运行时，设置生产环境的tracker访问，容灾环境中的tracker不访问，同时生产环境中的group卷中的storage优先访问，设置store\_server为2,download\_server设置为1, storage.conf设置upload\_priority为9，默认10，越小优先级越高

容灾切换演练时，设置容灾环境的tracker访问，生产环境的tracker不访问，store\_server为0,download\_server设置0（都是默认值）

这样，生产环境中只会访问生产环境中的机器；容灾做备份，同时容灾环境也能使用。



## 切换存储介质

底层可切换为NAS等其他存储

使用策略模式替换存储介质

## 部署

fastdfs部署脚本