WPS 云文档产品技术白皮书

北京金山办公软件有限公司

2018 年 02 月

商标声明

和其他金山商标均为北京金山办公软件有限公司的商标。

本文档提及的其它所有的商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受北京金山办公软件有限公司商业合同和条款的约束，本文档中描述的全部或者部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，北京金山办公软件有限公司对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或者暗示的担保。

目 录

一、 产品介绍 .....
二、 系统架构图 .....
三、 主要功能技术要点.....
（一） 文档存储管理.....
1. 多中心存储.....
2. 内外网分享.....
3. 全文检索.....
4. 按策略的文档分类 .....
（二） 文档在线预览.....
1. 至臻至强的排版引擎 .....
2. 预览分页传输.....
3. 文档预转机制.....
4. 前端安全防护（水印、防复制、防打印） .....
（三） 不落地编辑.....
1. 云端文件自动下载、回传 .....
2. 单点登录.....
3. 修订和清稿编辑模式 .....
（四） 安全文档.....
1. 加解密文档.....
2. 细粒度权限管理.....
3. 权限申请与审批.....

4. 离线使用.....
5. 文档外发.....
6. 日志审计.....
7. 溯源追踪.....
（五） 协作文档..... 错误!未定义书签。
1. 多人在线编辑..... 错误!未定义书签。
2. 普通文档转为协作文档 ..... 错误!未定义书签。
（六） 历史版本管理.....
四、 产品部署方案 .....
（一） 部署拓扑.....
（二） 容器技术.....
（三） 高可用 .....
1. 网络层面（接入层）： .....
2. 应用层面：.....
3. 缓存层面.....
4. 数据设计层面：.....
（四） 分布式存储.....
（五） 数据备份.....
1. 存储文件备份.....
2. 数据库备份.....
3. 定时备份机制.....
（六） 配置需求.....

1. 操作系统.....
2. 网络.....
3. 数据库.....
4. 配置列表.....
五、 云文档安全架构设计.....
（一） 数据安全架构设计.....
1. 文件存储机制.....
2. 数据分块存储机制.....
3. 数据库架构.....
4. 安全机制.....
（1） 数据持久化安全.....
（2） 链路信道安全.....
（3） 终端缓存加密.....
（4） 系统访问安全.....
（二） 业务逻辑安全设计.....
1. 文件夹授权机制.....
（1） 利用团队文件夹共享实现文档协同共享.....
（2） 团队文件夹支持多层嵌套授权管理机制.....
（3） 满足海量文档的多类文档管理服务.....
2. 统一安全访问.....
（1） 统一身份认证.....
（2） 文档全生命周期的安全审计.....

（3）三员后台管控.....
3. 文档预览安全防护.....
（三） 文档内容安全架构设计.....
1. 文档权限概述.....
2. 文件权限框架设计.....
3. 加解密方式.....
六、云文档服务组件.....

一、产品介绍

WPS 云文档产品是一款围绕文档处理工具的全平台文档管理系统，包括云文档储存服务、文档权限管理服务、在线文档处理服务、配合文档协同沟通的即时通讯服务及供第三方业务系统调用的文档组件 API 服务。

作为国内近 30 来一直致力于办公软件的公司，在文档格式、文档内容、文档安全等方面实现在产品内核级的保障与支持。另外金山公司从 2009 年开启了云技术的探索，从金山快盘到金山云，在云技术领域也有了 8 年之久的经验积累。

二、系统架构图

WPS 云文档系统架构图如下：

WPS 云协作系统架构

三、主要功能技术要点

（一）文档存储管理

1. 多中心存储

WPS 云文档支持文件实体按照策略存储在合适的存储中心，适应云文档元数据统一管控、企业分部专线网络带宽有限等情况。云文档系统通过判断用户的特征信息，如分公司、部门等，计算出最近的存储节点进行存储，降低对跨区域网络的依赖和提高文档的上传和下载的速度。

2. 内外网分享

利用 WPS 云文档服务的开放 API，企业可根据其需求结合其 OA 的审批业务流程将分享文档同步到企业部署于中立区或者外网的云文档服务器，提供外网访问，以达到内外网分享文档的需求，也保证文档分享在受控和安全的基础上提高了分享文档的外网访问速度和体验，不影响企业内外网的专线带宽。

3. 全文检索

利用 WPS Office 对办公文档全格式的支持和分布式检索引擎索引的优势，WPS 云文档支持快速和准确的全文内容检索体验。文档上传到 WPS 云文档后，会通过 WPS Office 导出文档内容工具将文档中所有的内容，包括各个子文档内容、隐藏内容，导到分布式索引引擎中，建立索引仓库。索引仓库的数据是多维度的，实现各种场景组合的全文检索需求。

4. 按策略的文档分类

WPS 云文档通过文档标签实现文档的分类索引和管理，WPS 云文档分类管理根据企业的分类策略，建立文档的标签，也利用分布式索引引擎的能力，实现快速查找文档。而文档的标签属性支持企业层次和用户层次的，以实现企业和用户个人有专属的分类数据，实现不同层次的文档管理需求。

（二）文档在线预览

1. 至臻至强的排版引擎

office 文档的在线预览，采用 WPS Office 原创内核架构在服务端运行作为文档预览转换的排版引擎，进而完全按照排版结果形成的文字所属行段页锚点位置的相对位置进行切分渲染输出 html 显示内容，29 年的 office 软件自主核心技术沉淀保证了文档的内容显示效果符合不跑版的预期。

2. 预览分页传输

在线预览内容查看时运用了数据分页渲染输出的技术，针对不同文档格式分别应用不同的数据分块计算和渲染规则，形成可查阅的分页的数据，客户端按查看进度实时分段管理数据缓存，加快内容显示速度的同时，大大减轻服务端、客户端和网络的开销 。

3. 文档预转机制

在提升预览查看速度上， 文档预览采用了预转机制，根据上传来源、时间、使用频率等不同维度，配置高效的预转队列和分布式节点的执行策略，让文预览结果提前准备好，让大部分文档在用户使用在线预览时感受到秒开的速度，减少无谓的加载等待时间从而提高工作效率。

4. 前端安全防护（水印、防复制、防打印）

为适应内容安全防护的需求，在线预览内容还同时具备安全水印信息、禁止内容复制、禁止内容打印三个层面的能力，此三项安全防护表现是在内容输出源上进行管控的，在全平台加载显示均生效，无需外部程序配合做附加的处理机制，从而保护内容无法轻易操作泄露，守护数据安全。

（三）不落地编辑

1. 云端文件自动下载、回传

WPS Office 与 WPS 云文档采用一致的身份认证体系，支持使用云文档 ID 打开文件的模式，当 WPS Office 接收到云文档时，会自动去云端请求下载对应的文件，云端校验身份通过，并验证有权限时，文件会被成功下载到本地。WPS Office 本地编辑后保存时，向云端提交获取上传地址的请求，云端身份验证有编辑权限时，则会成功上传，产生新的版本，反之则失败。

2. 单点登录

因为打开云端文档需要身份认证，在 WPS 云文档产品体系中调起 WPS Office 打开云端文件时，会尝试使 WPS Office 客户端保持与云端当前用户身份一致，具体实现如下：云文档功能模块向服务器申请当前用户身份标识随机码，这个随机码是有时效的，将它传递给 WPS

Office，WPS Office 使用随机码从服务器获取用户 Session 及身份信息，使自己处于登录状态。

3．修订和清稿编辑模式

WPS 云文档在调起 WPS Offie 打开文件时，可以通过注册到系统的私有协议传递参数给 WPS Office，达到控制 WPS Office 状态的目的。目前实现了控制 WPS Office 进入修订模式和清稿，不需要调用 Office 的 COM API，适用任意浏览器框架加载 WPS 云文档服务使用生效。

（四）安全文档

WPS 安全文档是通过 WPS Office 客户端和安全服务器提供加解密文档、细粒度权限管理、权限申请与审批、离线使用、外发、日志审计以及溯源追踪等功能的文档安全管理服务的；使企业机密文档（如财务报表、营销数据、产品规格、研发流程等）在产生、流转、版本修改、存储、外发整个生命周期都能安全无忧，独特的泄密追溯技术能够在泄密后追究责任人，起到警示作用。

1．加解密文档

在保证一文档一密钥的同时，客户端和服务器对文档信息、密钥等数据进行双重加密。

WPS 原生支持加解密机制，无需通过驱动、hook 等技术手段，从而增加系统稳定性。

此外，加密流程深度整合到 WPS 处理文档过程，加快文档数据的处理效率并且无明文落地。

还可由第三方提供加密算法，扩展程序已规范化的接口接入 WPS 安全系统。

2. 细粒度权限管理

打开安全文档和对文档进行操作都会受到权限限制，拥有阅读权限的用户在登录后通过服务器鉴权才可以打开安全文档进行浏览，其他编辑、复制、打印、另存、离线、授权操作都会受到相应的权限管控，只有有权限的用户才能进行这些操作，没有权限的用户无法进行该操作。目前 Windows、iOS、Android 系统的 Office 客户端都可以做到权限控制。

3. 权限申请与审批

用户在对安全文档操作时，可以将向其他有审批权限的用户或管理员申请权限。拥有审批权限的用户和管理员可以对其他用户的权限申请进行审批，审批同意后，申请人获得新权限。

4. 离线使用

离线权限是安全文档的权限之一，拥有离线权限的用户，可以离线使用安全文档，但只能继承阅读、编辑和复制权限，所有的操作日志均会记录本地，连线后自动上传，离线有时效限制，每一个文档累

计离线时长到达上限时，无法再离线打开，需要在线通讯后才恢复最大时效，管理员可以自行配置离线时效。

在线安全文档在通讯中断后会引导用户切换到离线登录，无需关闭文档；离线状态过程中检测到服务器可通讯时，会静默切换到在线状态， 不影响文档阅读和保存。

5. 文档外发

企业需要与合作伙伴进行文档交流时，企业用户可以对安全文档提起外发申请流程，管理员审批之后可以制作外发文档。

企业用户可以在 WPS Office 客户端制作外发文档，发送给外发收件人。

6. 日志审计

企业内用户对安全文档进行的所有操作都会被服务器记录下来，包括创建、阅读、编辑、复制、另存、打印、授权，管理员可以定期对安全文档进行审计工作，通过日志时间、文档名称、操作者名称等条件进行筛选，某一个文档被某个用户做过何种操作都可以随时查出来，支持导出日志。

系统记录的管理员在后台的操作行为信息，包括外发收件人维护、权限模板维护、导出日志、同步用户等，管理员可以定期对安全文档进行审计工作，通过日志时间、文档名称、操作者名称等条件进行筛选，某一个文档被某个用户做过何种操作都可以随时查出来，支持导

出日志。

7．溯源追踪

WPS 文档的溯源模块提供 Office 文档水印信息隐写、水印信息提取、打印分发插件、编码库管理等功能，为企业提供有效的文档泄密溯源能力，一旦截获泄密文件、图片，能够快速定位到泄密责任人。

WPS 安全文档，会自带仿宋、宋体、楷体、方正仿宋等特殊字体，在打开文件、打印文件时，均会对字体进行绘制，可将用户的登录身份基本信息（或者硬件 ID 设备信息）形成隐藏的数字水印分布在文字排版中。此过程不影响原文件，仅影响 WPS 呈现出来的效果，且通过肉眼识别不出来，客户无差异感知。这样达致原生支持水印隐写机制，支持打印、截屏、拍摄多种泄密渠道溯源；同时智能化提取权限控制，提供集中追溯提取、分级追溯提取多种方式，确保溯源信息安全可控。

当用户通过打印、复印、拍照等方式造成文档泄密，单位管理者仅需要获取到文档的复印件、或相关的拍照图片，即可通过 WPS 溯源解析系统，寻找到泄密的原始人，从而方便追责工作。

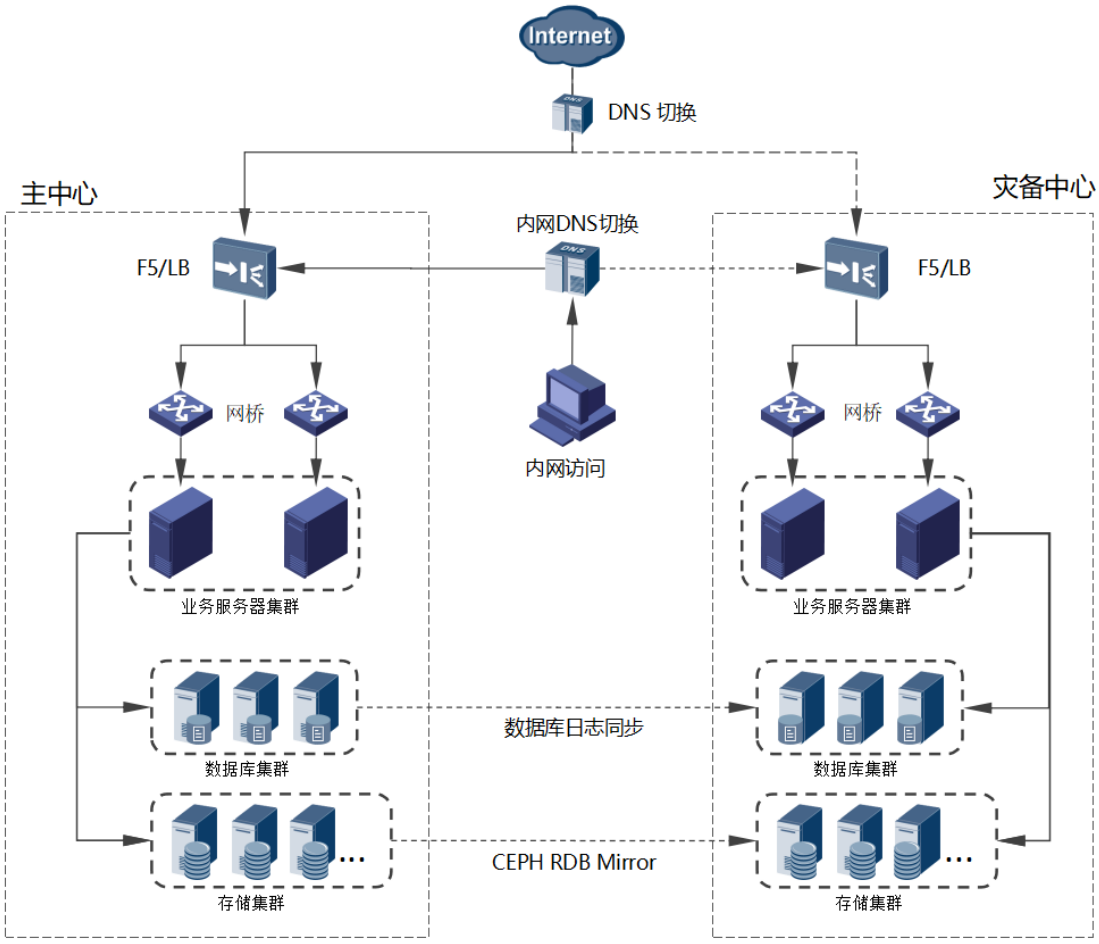
（五）历史版本管理

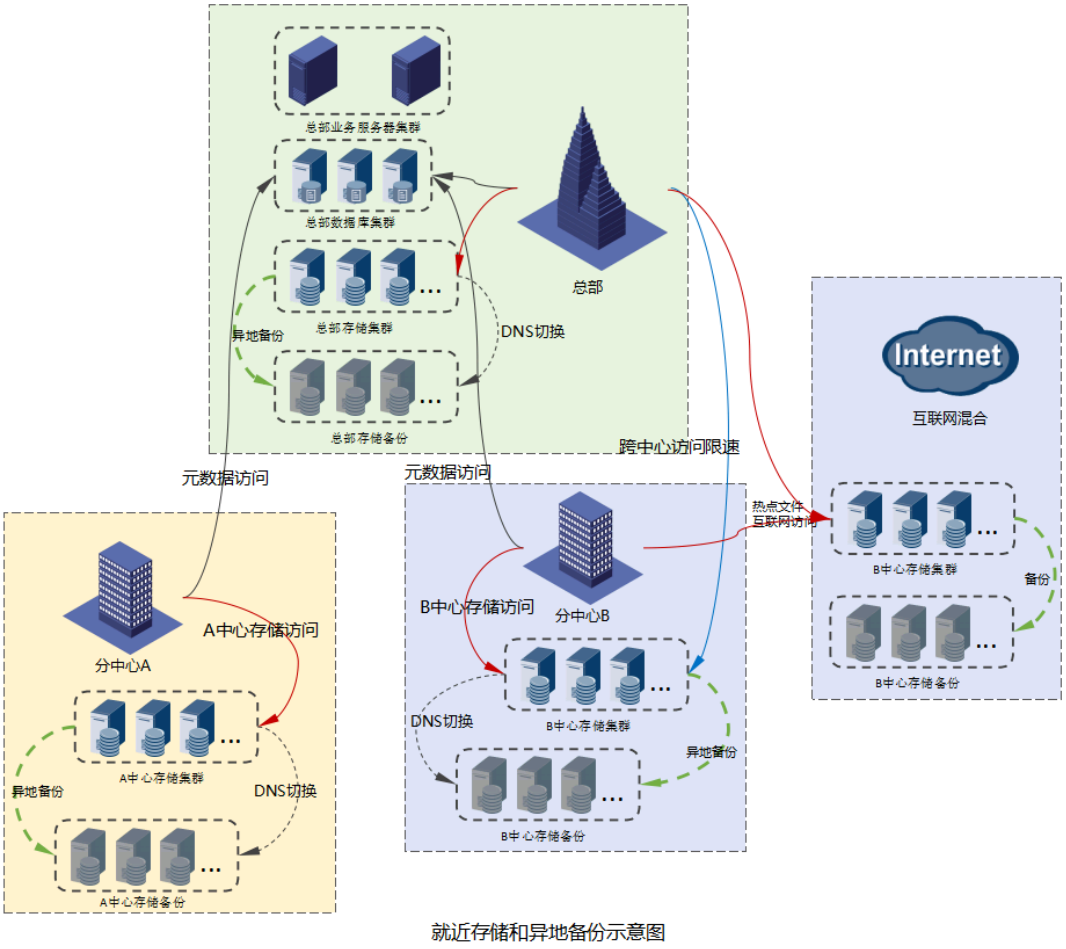
云端的每一个在线文档都会有历史版本体系，且都是通过对应唯一文档 ID 维系不同版本集，进而对每个独立的文档 ID 维护一个版本序号关系表，这样两个维度的关系管理可保证文档在大量存储下仍然

是可以绝对正常准确匹配访问的，且可满足随时按需恢复特定版本，保证数据不错乱。

四、产品部署方案

（一）部署拓扑





就近存储和异地备份示意图

（二）容器技术

容器技术保证开发、交付和运维的一致性、提供管理自动化，提升系统利用率、降低日常运维成本、松耦合应用架构，提升系统的敏捷性和可维护性。

使用容器进行部署，相关服务都已经封装成镜像的形式，通过微服务架构方法将应用逻辑分解为一组松耦合的服务，使得每个服务可以独立开发、部署、演进和伸缩。

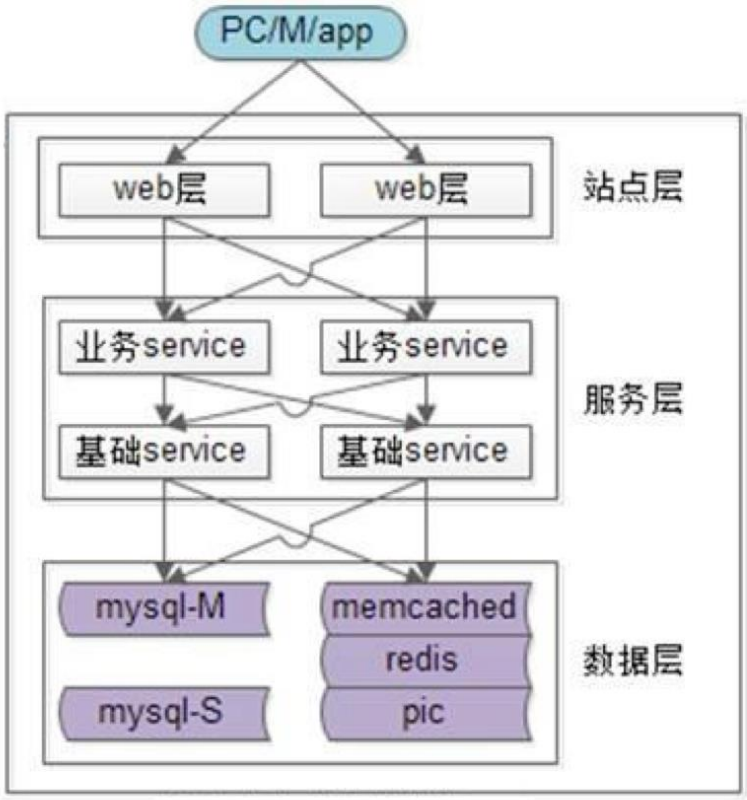
（三）高可用

单点是系统高可用的大敌，单点往往是系统高可用最大的风险和敌人，应该尽量在系统设计的过程中避免单点。方法论上，高可用保证的原则是“集群化”，或者叫“冗余”：只有一个单点，挂了服务会受影响；如果有冗余备份，挂了还有其他 backup 能够顶上。

保证系统高可用，架构设计的核心准则是：冗余。

有了冗余之后，还不够，每次出现故障需要人工介入恢复势必会增加系统的不可服务实践。所以，又往往是通过“自动故障转移”来实现系统的高可用。

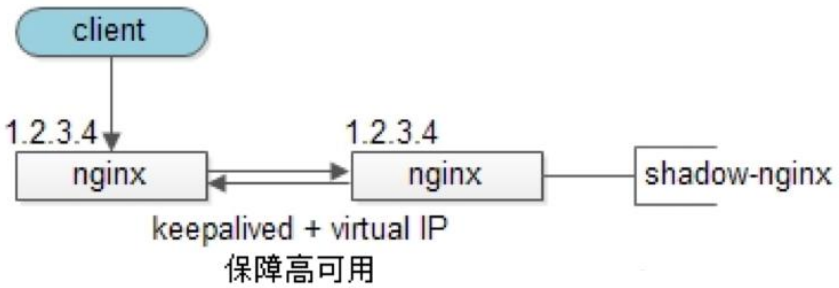
接下来我们看下典型互联网架构中，如何通过冗余+自动故障转移来保证系统的高可用特性。



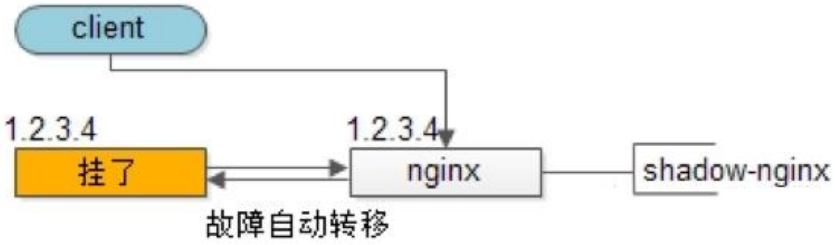
1. 网络层面（接入层）：

利用 Nginx Upstream ，提供 4 层和 7 层上的负载均衡方案，4 层（TCP、UDP 协议）监听器支持设置源 IP 转发规则实现会话保持；7 层监听器（HTTP、HTTPS）通过植入/重写 cookie 实现会话保持。

以 nginx 为例：有两台 nginx，一台对线上提供服务，另一台冗余以保证高可用，常见的实践是 keepalived 存活探测，相同 virtual IP 提供服务。



自动故障转移：当 nginx 挂了的时候，keepalived 能够探测到，会自动的进行故障转移，将流量自动迁移到 shadow-nginx，由于使用的是相同的 virtual IP，这个切换过程对调用方是透明的。



2．应用层面：

在应用部署时，通过 Docker 的集群管理和资源调度能力，将位于同一地域的多台服务器资源虚拟成一个高性能、高可用的应用服务池；根据应用指定的方式，将来自客户端的网络请求分发到服务池中。

3．缓存层面

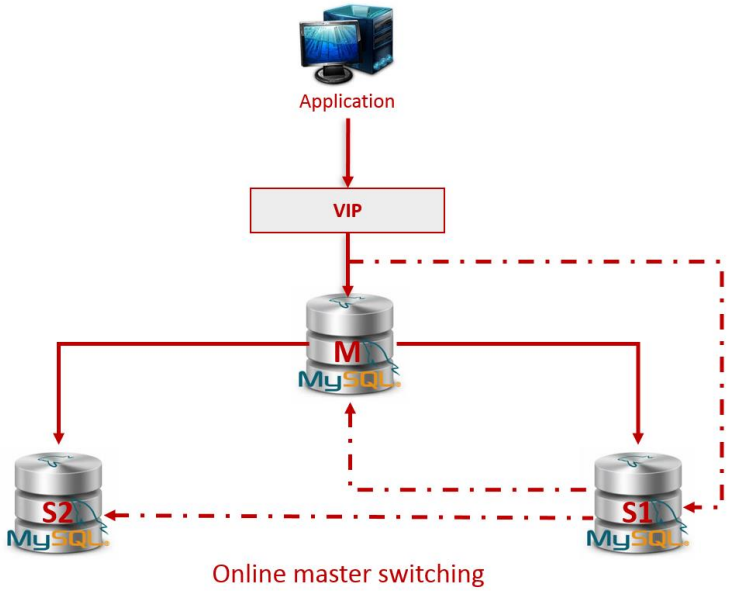
为了提高应用响应的速度，降低数据库的压力，缓存层起了很重要的作用。缓存层使用了缓存服务的集群和分布式能力，保证了缓存数据的一致性和高可用。

4．数据设计层面：

应用层和数据层的分离。一方面它可以使得应用逻辑变成无状态的，支持水平扩展；另一方面区分无状态和有状态服务，可以针对不同工作负载实现性能优化和扩展

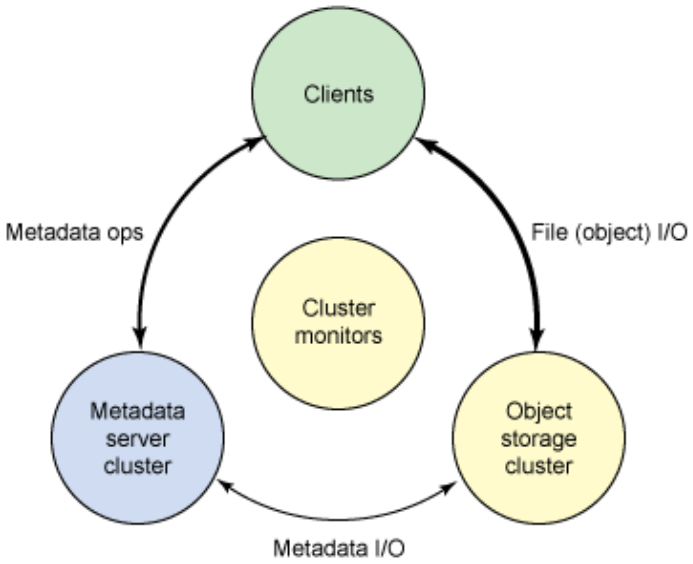
应用通过 VIP(虚拟路由，由 MHA manager 使用 Keepalived 创建)

访问 MySQL 集群。一主(图 M)二从(图 S1 和 S2)，S2 作备用主库。一旦原 Master 节点出现故障，MHA 自动将主库切换到 S1，并且 S2 随之连接到新的 Master。MHA 同时通过 master_ip_failover_script 脚本停止原 Master 节点上的 Keepalived，路由自动切换到 新 Master。这时候外部应用实际访问的是 S1 了，不会出现 MySQL 突然无法使用的问题。



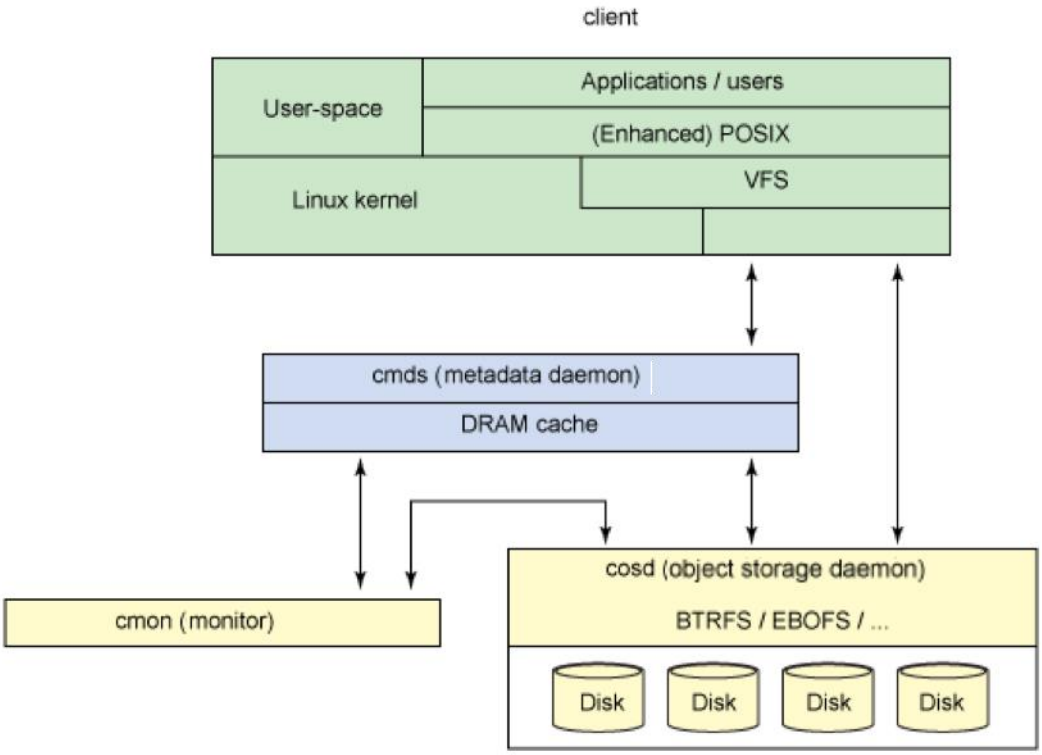
（四）分布式存储

WPS 云文档分布式存储生态系统可以大致划分为四部分（见图 1）：客户端（数据用户），元数据服务器（缓存和同步分布式元数据），一个对象存储集群（将数据和元数据作为对象存储，执行其他关键职能），以及最后的集群监视器（执行监视功能）。



如图上图所示，客户使用元数据服务器，执行元数据操作（来确定数据位置）。元数据服务器管理数据位置，以及在何处存储新数据。值得注意的是，元数据存储在一个存储集群（标为 “元数据 I/O”）。实际的文件 I/O 发生在客户和对象存储集群之间。这样一来，更高层次的 POSIX 功能（例如，打开、关闭、重命名）就由元数据服务器管理，不过 POSIX 功能（例如读和写）则直接由对象存储集群管理。

下图显示了 WPS 云文档分布式存储生态系统。Client 是文件系统的用户。Metadata Daemon 提供了元数据服务器，而 Object Storage Daemon 提供了实际存储（对数据和元数据两者）。最后，Monitor 提供了集群管理。要注意的是，分部署存储客户，对象存储端点，元数据服务器（根据文件系统的容量）可以有许多，而且至少有一对冗余的监视器。



（五）数据备份

1. 存储文件备份

多机热备：分布式储存是三备机制，保证服务的可用性和数据的安全。采用强一致性同步模型，即必须所有副本都完成写操作才算一次写入成功。数据是以三副本的形式分散在数十上百个存储磁盘集群进行存储的，凭借三副本机制以及后台校验等机制，可以提升集群数据的可靠性保护，在单个磁盘发生故障时，节点可以做到动态的负载均衡，并且可以凭借分布在不同的机器上的

副本及算法完成数据的恢复，实现高可用性。

冷备：定时将存储文件数据到备份存储中；

2. 数据库备份

多机热备:采用 Mysql 数据库的 MHA 高可用三备方案;MHA Manager 会定时探测集群中的 master 节点，当 master 出现故障时，它可以自动将最新数据的 slave 提升为新的 master，然后将所有其他的 slave 重新指向新的 master。整个故障转移过程对应用程序完全透明。在 MHA 自动故障切换过程中，MHA 试图从宕机的主服务器上保存二进制日志，最大程度的保证数据的不丢失.

冷备：定时备份到备份数据库中；

3. 定时备份机制

（六）配置需求

1. 操作系统

操作系统	版本
SUSE	64 位，SUES 12.x 或以上
CentOS	64 位，CentOS 7 或以上
RedHat	64 位，RHEL 7.2 或以上
Ubuntu	64 位，14.04 或以上

2. 网络

服务内部通过域名的方式进行沟通，所以需要指定三个域名如下：

服务器	类别	域名
云文档服务器	云文档主功能	yun.xxx.xx
文档协同服务器	文档协同	yiqixie.xxx.xx
云文档服务器	文档存储	storage.xxx.xx

其中存储服务依据部署需要，可以申请多个（eg:storage-beijing.xxx.xx，storage-zhuhai.xxx.xx。。。）供多地访问使用。

3. 数据库

WPS 云文档解决方案使用了 3 种常见的数据库存储数据，包括：

数据库	版本	应用场景
Mysql	5.7.17 或以上	数据主要的储存方式，对关系型数据进行储存
MongoDB	3.4.4 或以上	对非结构型数据进行储存
Redis	0.1.3 或以上，single 和 trib 版本	记录登录等热点信息

针对写操作频繁的表（用户表，文件表），进行了分表的设计。用户表和文件表都按 1024 进行分表，按照用户 id 或者团队（部门）

将数据存在对应的子表里。

4. 配置列表

环境	类别	cpu	内存	硬盘	个数	需求总数	总用户数	并发用户数
测试环境	业务服务器	16 核	32G	200G	1	3	1 万	250
	消息平台、协作文档	8 核	16G	200G	1			
	数据库	8 核	16G	200G	1			
生产环境	业务服务器	16 核	32G	200G	2	14	10 万	1 千
	消息平台、协作文档	16 核	32G	500G	3			
	数据库	16 核	32G	1T	3			
	公共服务器	16 核	32G	500G	3			
	存储服务器	8 核	16G	100G（按需分配）	3			
生产环境	业务服务器	16 核	32G	200G	4	14	50 万	5 千
	消息平台、协作文档	16 核	64G	500G	3			
	数据库	16 核	32G	5T	3			
	公共服务器	16 核	32G	2T	6			
	存储服务器	8 核	16G	100G（按需分配）	3			

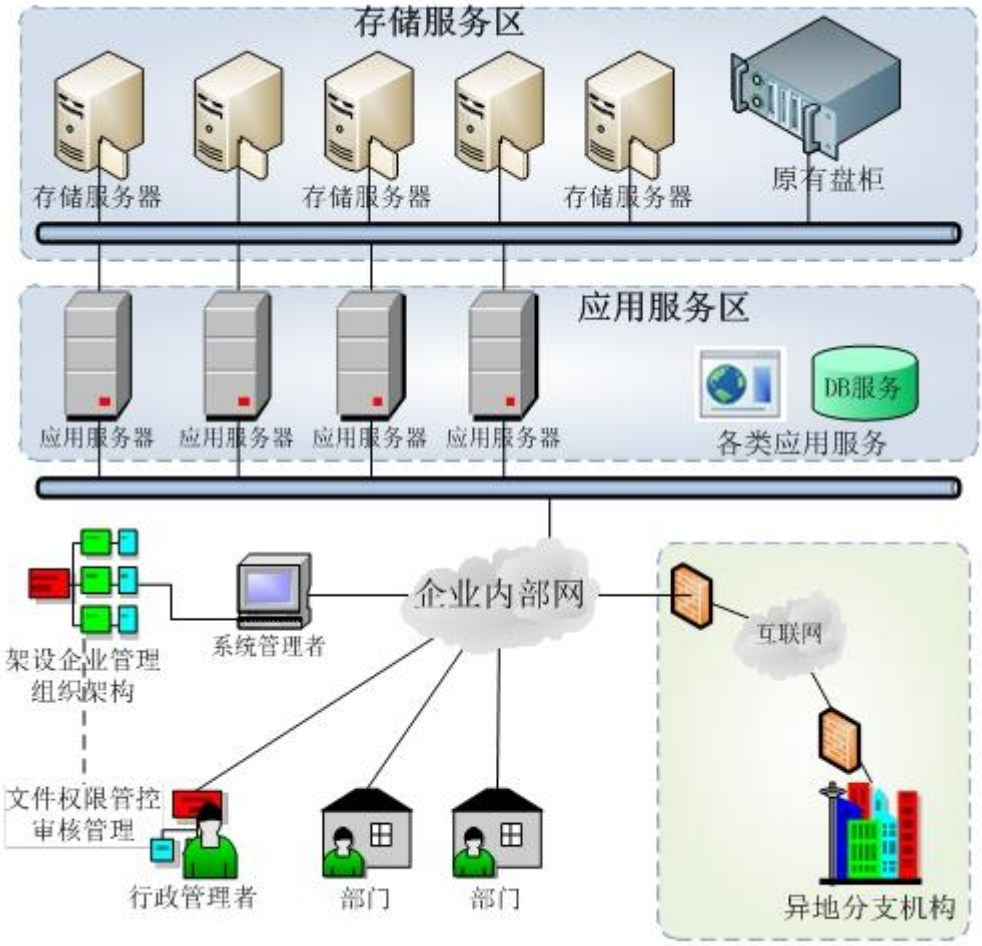
五、云文档安全架构设计

（一）数据安全架构设计

1. 文件存储机制

为了满足企业内部海量数据文件的存储，需要部署足够的磁盘存

储空间；为了确保文档数据存储的安全，又需要具备足够的冗余和可靠性；从企业的扩展需求看，文件数据存储需要满足多部分、多分支机构的状况；从企业 IT 设备运维角度看，也需要足够的运维方便性；从企业的运营成本角度看，同时也需要最经济的设备成本方案。云文档产品能充分满足上述要求。云文档服务器端的部署框架如下图所示。



上图展示了利用云文档架设在企业内部私有云存储平台的结构。

产品支持多服务器集群方式部署，通过负载均衡，实现高效的集群存储，确保数据的多倍冗余存储，提升数据安全性和可靠性。系统的服务器部署分应用服务层和数据存储服务层两层，文件存储服务器专门负责提供存储服务，并可以动态进行无限扩展，实现海量服务。

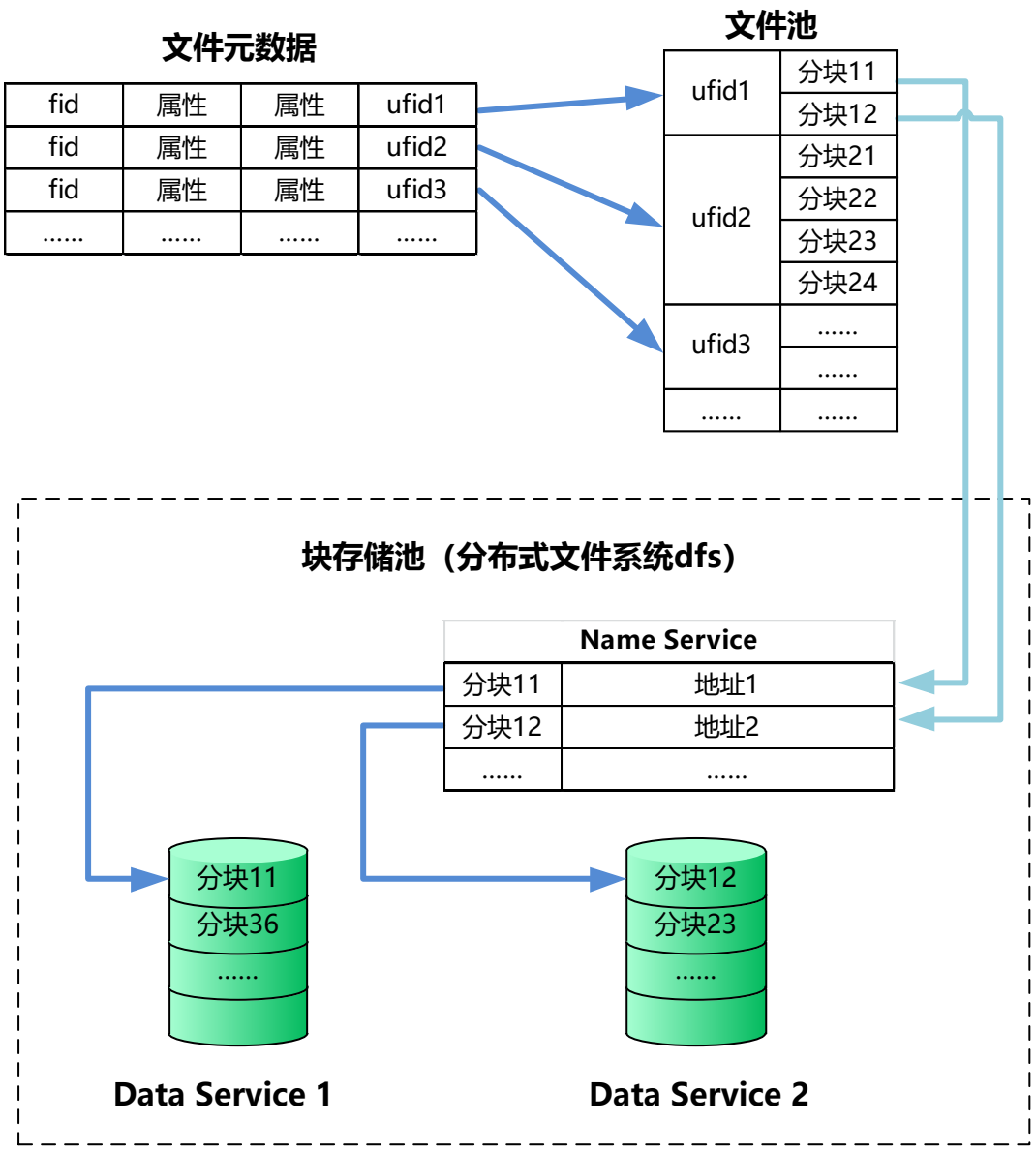
2．数据分块存储机制

WPS 云文档客户端对文件进行分块，上传下载是以数据块为单元，云端存储文件数据也按此分块存储。

文件分块会进行压缩加密，分块加密保证了文件上传下载过程及存储在云端时的安全性，分块压缩则大大增加了存储系统的可用容量。

分块机制使处理数据单元比整个文件方式来说相对固定，上传下载及云端处理的效率与稳定性都有大幅提升，且可以支持断点续传。

分块机制同时使得大文档修改后的上传速度加快。如一个 1M 以上的文件，在末尾追加内容，那么仅最末尾的文件块需要重新上传，而不必全文重新上传，提高了同步效率。对在文件中间某些内容进行修改而没有产生数据移位的，也仅上传被修改的文件块。



文件切片机制

3. 数据库架构

WPS 云文档后台数据库为 MySQL，采用 MHA 高可用设计，最低要求一主两从架构。该设计由两部分组成：MHA Manager（管理节点）和 MHA Node（数据节点）。MHA Manager 会定时探测集群中的 master 节点，当 master 出现故障时，它可以自动将最新数据的 slave 提升为新的 master，然后将所有其他的 slave 重新指向新的 master。整

个故障转移过程对应用程序完全透明。在 MHA 自动故障切换过程中，MHA 试图从宕机的主服务器上保存二进制日志，最大程度的保证数据的不丢失.

WPS 云文档使用过程中，随着时间积累，文件数据会越来越多，单数据表会导致数据记录插入、检索性能大幅降低，WPS 云文档数据表分库分表设计：文件数据表拆分为 1024 个表，按用户 ID 将数据记录平均分配到各表中，这 1024 个表可以位于一个数据库中，也可以分布在多个数据库中，可以依据负载情况调节数据库集群机器数量，实现动态扩容。

4. 安全机制

（1）数据持久化安全

WPS 云文档系统采用块数据存储机制，每个文件按分块原则分成等尺寸的多个数据块，每个数据块独立加密，分散形式的存储在服务器端的磁盘空间中，因此磁盘中的文件存储形式不同普通操作系统看到的明文文件存储方式。

WPS 云文档系统的服务端所有存储的数据都经过 AES256 位加密。加密数据所使用的密钥有完整的密钥策略，以及配套的密钥管理制度。

存于服务端的文件分割成数据块，每个数据块有独立的密钥，即使通过某种途径获取到某个数据块密钥，也无法解密其他数据块，不会危及其他用户的数据安全。

数据块密钥的运算过程为：数据块密钥 =SHA1【SHA1（数据）+原钥】。SHA1（数据块）的计算可以保证数据块密钥的独立性，绝密的原钥可以保证数据块密钥的安全性。

原钥是恒定（每个系统不同，生成之后不变）的密钥，加密存放在服务端，原钥的明文不存在于任何持久存储设备，也不会进行传输，原钥通过严谨的过程进行解密，并仅存放在内存。

WPS 云文档系统为了最大的安全性考虑，设计有几种密钥管理制度，分别对应几种原钥解密过程如下，推荐使用的是密钥分片管理制度。

几种原钥解密过程，企业可以按需选择：

1)原钥 = 解密（原钥片密码 1，原钥片密码 2，原钥片密码 3），同时输入三个原钥片密钥，才能解密原钥，三个片密码可以由不同管理人员分别保管。

2)原钥 = 解密（数字证书），使用不可复制的硬件数字证书作为原钥的加解密密钥。

3)原钥直接明文存放，在服务器机房管理完善、服务器操作系统权限管理良好、可以保证安全的情况下可以采取这个方案。

WPS 云文档系统把服务端的所有数据都放在严格的加密策略保护下，保证了数据的安全性。

（2）链路信道安全

WPS 云文档系统使用业界标准的 Https/SSL 安全连接来保证会话

过程不被窃听。

SSL 过程分为 3 阶段，可抵御网络传输过程中的数据窃听：

1)服务端配置有 RSA 非对称加密算法的私钥，连接建立时，向客户端传递其对应公钥。公钥是公共数据，被截获不影响数据安全。

2)客户端随机生成对称加密算法的密钥，使用公钥加密后传到服务端。此数据只有拥有对应私钥的服务端才能解密，若被截获无法被解密。

3)此时服务端与客户端拥有共同的对称密钥，之后的通信数据都通过此密钥加密后再传输，若被截获无法被解密。

（3）终端缓存加密

WPS 云文档系统提供的无缓存虚拟磁盘客户端应用方案，在进行服务端文档访问操作时，平时只显示文件列表，不会将数据调取至本地，有文件请求时，所有数据均来源于服务器，退出客户端后本地没有任何数据缓存，包括文件编辑时产生的缓存文件同样不会存在于本地，且无法从本地磁盘中恢复出来。若用户选择将数据离线缓存，本地存储数据同样经过 AES256 加密，选择缓存后，会提示用户输入密码，将本地密码以多次不可逆运算后的结果保留在本地以便本地认证，如果用户忘记密码，将无法访问离线缓存，只能卸载重装，原有缓存数据不可破解。

（4）系统访问安全

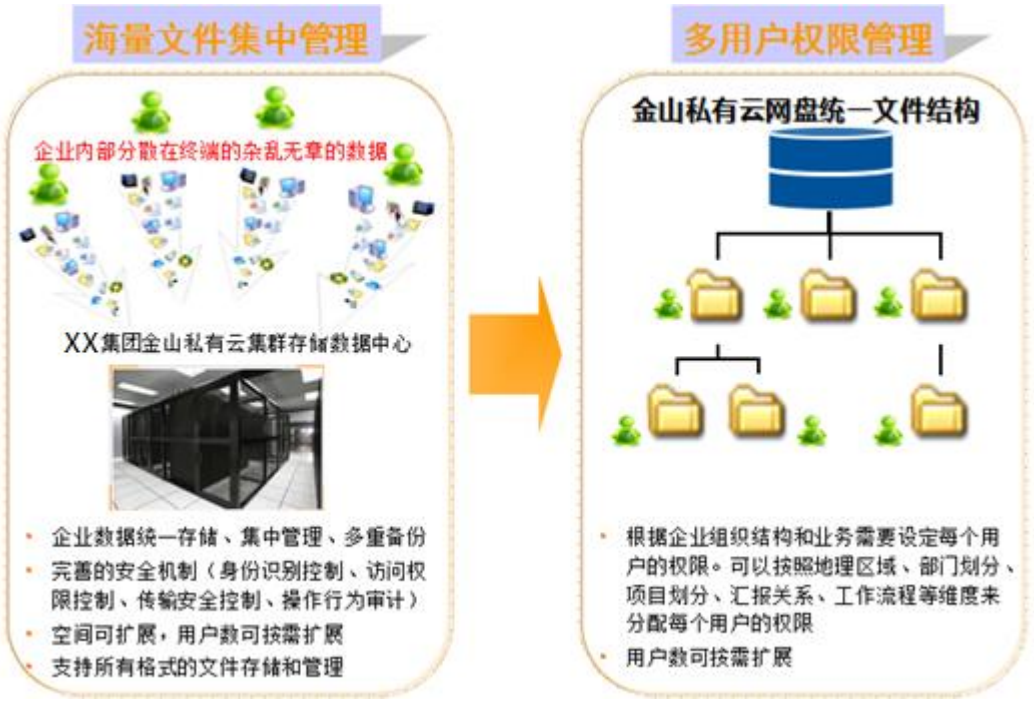
1. 登录：用户通过帐号密码进行登录验证后，服务器端返回一个唯一的 Token 给客户端，在该 Token 的有效时间内，客户端均可使用该 Token 与服务间进行接口交互。当用户输入密码错误次数超过 3 次以上，需要输入验证码，防止帐号遭到暴力破解。
2. 文件权限控制：xServer 目前有个人文件和团队文件。个人文件只能用户自己才可以访问，团队文件视管理员配置的权限，可设定参加群组的用户，还可以对每个用户进行 “读写”，“只读”等权限的控制。
3. 访问审计：xServer 所有的 API 调用均会存入审计数据库，并提供审计查询界面供管理员对审请信息进行查询。

（二）业务逻辑安全设计

1. 文件夹授权机制

（1）利用团队文件夹共享实现文档协同共享

WPS 云文档作为面向企业的云存储产品，与个人云存储产品的最大区别就是具有与企业“组织机构”集成，提供团队文件夹共享机制，WPS 云文档系统能有效地替代企业现有的 FTP、Window 共享文件夹，能解决文档集中存储后的安全管理问题，能有效地提升企业内部员工文档协作的工作效率。



WPS 云文档的“团队文件夹”功能具有如下一些特点：

- 团队文件夹的访问权限既可授权给某些用户，也可以授权给某个部门。
- 团队文件夹的授权访问用户，可授予可编辑、只读、可删除、可再管理等组合权限，可满足企业员工对文档的日常共享需求
- 同一团队文件夹可设置多个管理人员，以便在单个管理者外出时的状况
- 团队文件夹的创建者不必是企业 IT 管理人员，任何用户都可以创建团队文件夹，方便企业实际工作的空间授权管理。
- 团队文件夹的创建者通常就是企业各部门的业务管理者，无需 IT 管理部门参与，可节省部门间沟通的环节。
- 利用团队文件夹共享机制，可将原先 IT 部门对企业文档共享

的集中管理权限，下放到各业务部门，即减轻了 IT 部门文档管理的压力，也增大了业务部门管理文档的灵活性。

- 团队文件夹的创建者可根据当前业务的需要随时创建，无需预先制定长远的目录规划。可即刻开始工作，并可以随时修改目录结构。
- 群组创建者可确定群组文档的生命周期，对于到期的群组文档可通过归档操作将群组转入云端访问，每个群组授权用户的桌面端将自动删除，不会长期占用用户的桌面存储空间
- 团队文件夹直接就是云端文件的影像，能对所有授权访问者提供一致最新版本
- 用户可以在团队文件夹中直接编辑文档，编辑结束后的文档即时显示到团队文件夹共享的所有用户终端，大家保持一致的最新版本
- 团队文件夹中的用户可以对文件进行“锁定”处理，被锁定的文件不会被其他用户窜改，因此能实现文档的统一维护更新。并且也可以防止文档多人编辑时的冲突问题。
- 团队文件夹中的每一个用户，在每次编辑完成后，都会自动形成一份历史版本文件，群组的每个用户都可以追溯到该文档之前的所有历史版本，即能查看到文档形成历史过程
- 团队文件夹中的文档，支持 Excel 电子表格文件的“共享工作簿”编辑应用，直接支持在虚拟磁盘上进行多人协同表格工作。

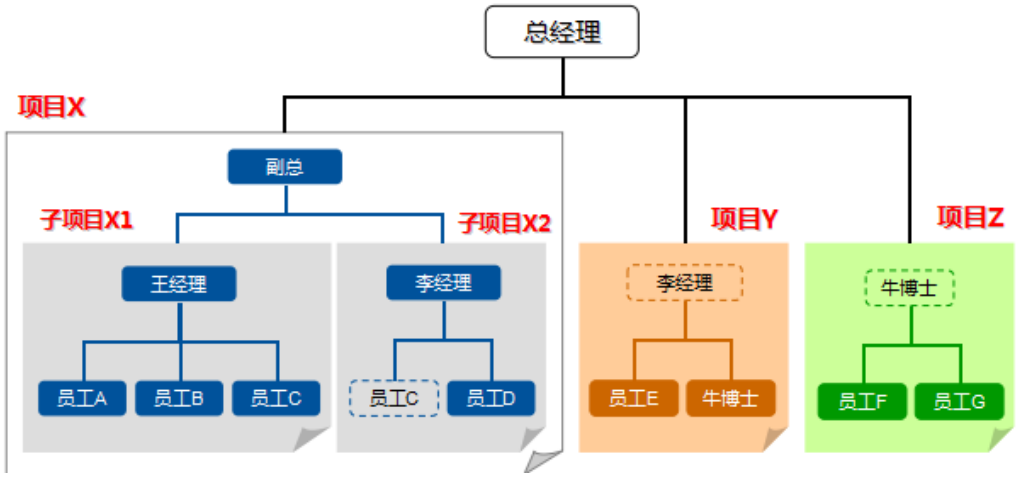
- 文档的历史版本记录功能满足各类文档，与文档格式无关。

（2）团队文件夹支持多层嵌套授权管理机制

利用“团队文件夹”上述的一些特点，能快速实现统一文档共享及协同工作规范，具体举例如下：

- 实现企业公共文件快速分发到桌面。
- 企业管理者可将“企业制度”、“工作规范”等公共类型的文档通过公共访问授权的群组，直接下发到员工桌面端。
- 企业部门的主管可将“工作模板”等规范化模板文档下发给部门人员
- 对同一任务多个人分工进行的情况下，保持统一的、最新的工作版本
- 一个企业项目，需要 5、6 个人分工协作，每人负责一部分，大家实时保持最新的、一致的版本
- 企业管理者利用群组收集分散用户终端的资料，形成有序的文档集合
- 企业部门管理者利用群组监督员工的工作进度

利用 WPS 云文档文件共享实现的一种典型应用案例如下：



总经理可以监管所有项目组织、人员安排、工作进度的情况

- 复杂项目可以分级管理（“项目 X”分解为相互独立的 X1、X2）
- 一个员工可以参加多个项目（“员工 C”同时参与项目 X2、项目 Y）
- 一个经理可以管理多个项目（“李经理”同时管理项目 X2、项目 Y）
- 一个员工可以同时作为项目普通成员和项目管理者(“牛博士”参与项目 Y，同时管理项目 Z）

（3）满足海量文档的多类文档管理服务

- 企业所有人员都可以共享、分布式、并行使用的海量文件资源管理系统
- 用户账户数目可动态扩展
- 存储空间可动态扩展

- 存储管理的文件类型、数量不限
- 使用 WPS 云文档能实现文件服务基础功能统一（更专业、更可靠、更低成本）
- 所有文件数据在物理上集中、统一存储和安全备份
- 完善的安全管理机制（身份安全控制、访问权限控制、传输安全控制、操作行为审计）
- 统一的访问接口（Client 端）和使用模式（读、写）
- 应用功能按需配置(通过文件夹的授权管理保持与业务流程一致）
- 按用户角色配置应用功能（权限）
- 按业务流程配置文件存储模式（域目录）
- 按组织架构配置用户账户
- 使用过程采用网络服务方式（部署和使用更为灵活）
- 可以部署在 DMZ 中（为分支机构、移动办公、客户、合作伙伴服务）
- 可以完全部署在内网中（内部数据文件管理）

2. 统一安全访问

（1）统一身份认证

WPS 云文档支持以下帐号创建验证机制：

1. 使用云盘标准版的帐号系统；
2. LDAP、AD 域导入帐号，导入帐号后，与原 LDAP、AD 域中帐号无关联；
3. 使用 LDAP、AD 域验证用户帐号信息，账户信息修改同步生效；
4. 使用企业自研发的用户帐号系统验证身份，账户信息修改同步生效，支持硬件认证。

WPS 云文档 API 访问授权协议使用 OAUTH，OAUTH 的授权没有涉及到用户密钥等信息，确保安全。

（2）文档全生命周期的安全审计

WPS 云文档的审计信息包含 44 类不同行为，包括：错误、读取文件、新建/上传文件、编辑文件、创建文件夹、移动、删除文件/文件夹、恢复文件/文件夹、彻底删除、创建部门、删除部门、编辑部门、移动部门、创建用户、删除用户、恢复用户、编辑用户、移动用户、修改密码、添加第三方账号、修改第三方账号、删除第三方账号、设置用户状态、创建外链、关闭外链、加锁文件、解锁文件、命名、系统设置、锁定用户、解锁用户、导出日志、登录、退出登录、设置空间、修改空间、取消空间限制、禁用空间等，随着版本更新还在继续

增加。

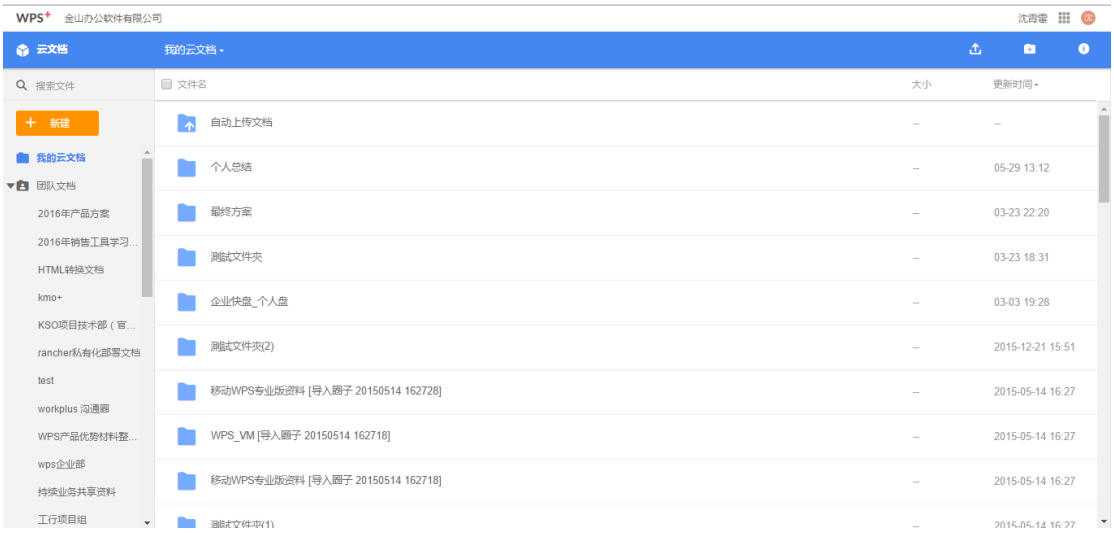
每条审计信息会记录以下内容，包括：操作人员、行为、文件路径、时间、IP、平台、结果等。

审计查询可根据以下信息：人员、行为、日期（时间范围）、IP、平台、结果等进行单项或多项查询，支持查询结果导出。

审计记录可以 csv 文件格式导出。

支持与其他审计系统对接。

支持独立审计账号。



（3）三员后台管控

WPS 云文档在系统安全管理方面，除了统一管理员的版本，还有支持三员标准的版本，分为系统管理员、安全员和审计员，各成员独立账号密码。管理员可以重置其他用户的密码，系统会有记录，可审计。通过三员分离的管控模式，更贴近大型企业的安全管理需求。

3. 文档预览安全防护

文档预览过程中存在复制、拍照、打印、越权预览等等泄密风险。WPS 云文档支持后台配置自定义水印，水印可以包含用户信息、设备信息。WPS 云文档在生成预览页面的过程中，可以跟据设置生成防复制、打印的逻辑。

前端请求预览页面时，需要传入用户份标识，验证用户是否对目录、文件内容有权限。

（三）文档内容安全架构设计

1. 文档权限概述

文档数据安全除了存储与管理过程的安全以外，内容编辑期过程中的安全也非常重要，为了解决办公文档内容的安全，WPS 云文档结合 WPS Office 客户端设计了 WPS 文档权限系统。

WPS 文档权限在设计上突破传统 DRM 在保护粒度上的弱势，以“用户中心”设计概念来直接保护文档本身，实现对使用者影响最小；与 WPS Office 客户端深度结合来保障防泄密的目标；构架文档的全生命周期保护，实现企业文档应用中的细粒度安全。在整体设计上，产品突出以下的几点设计原则：

注重产品的稳定性与安全性

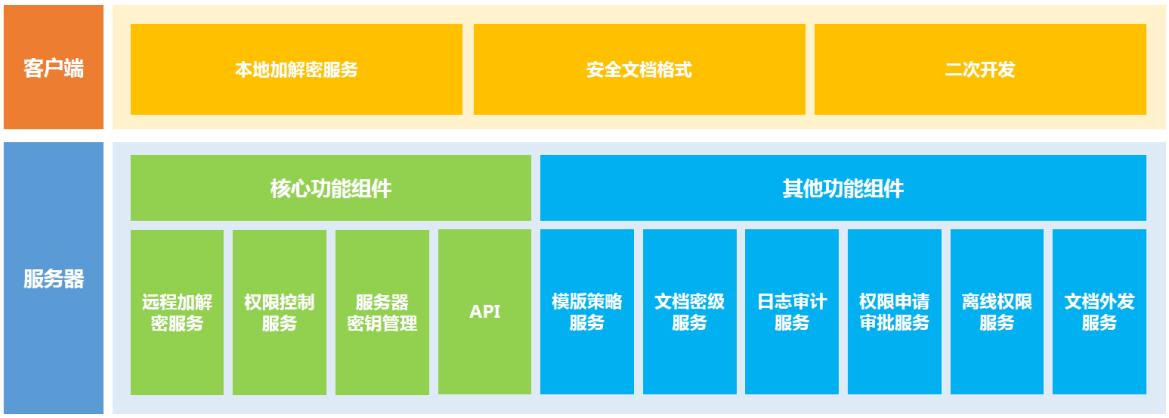
稳定性是 WPS 文档权限产品的重要目标。与其它电子文档安全管理软件不同，WPS 文档权限产品追求安全性与稳定性的完美结合，在

设计开发中对安全性与稳定性有影响的因素都会被排除在体系之外，在保障稳定的情况下实现系统的更深层次安全。产品的技术使用以稳定为优先，只有确定稳定的技术才会被纳入到产品中。

注重产品的易用性

信息安全产品通常会出现一个矛盾：提升了安全性，易用性就会降低。提升了易用性，安全性就会降低。这两者的平衡相当重要，一开始不先决定好，就会导致目标不清晰，功能过多，使用者无法很好的使用系统。安全软件必定会带来效率上的损失。WPS 文档权限的设计充分考量这一点，在技术运用上，尽可能在透明使用和安全架构及算法上做文章，力保对用户的使用改变上影响最小。保障安全与效率的统一。

2. 文件权限框架设计

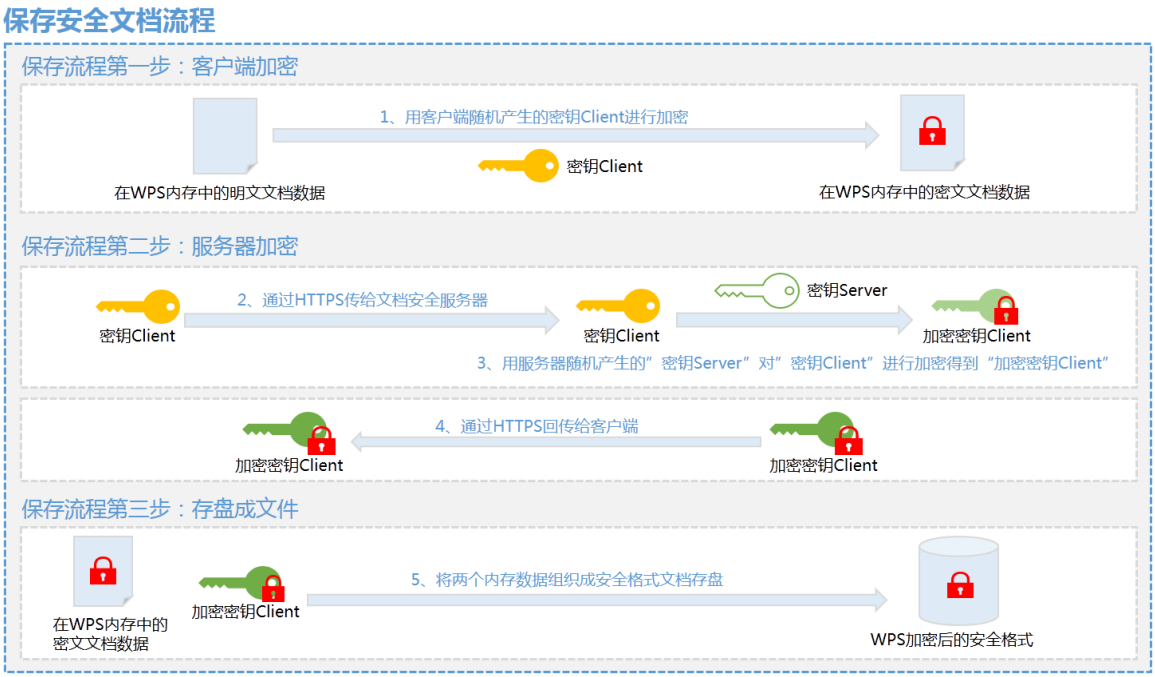


上图为 WPS Office 文档权限系统架构图，在 WPS 文档权限体系中，客户端和服务器共同参与保障数据的安全性。WPS 客户端本地负责安全文档格式的产生，而服务器所提供的远程加解密服务也参与安全文档格式的产生过程，让敏感数据分布在文档格式与服务器数据库

中，从而保证敏感数据的安全性。

3. 加解密方式

WPS 安全文档与传统电子文档安全软件不同，安全文档采用一文一密钥的机制，密钥本身会二次加密，二次加密密钥由服务器产生并保存，每次打开安全文档需要到服务器利用二次密钥解开文档密钥，才能打开安全文档，多重防护确保文档安全。



加解密方式特性：

- 客户端密钥 Client 每次保存都会重新产生以保证其安全性。
- 服务端密钥 Server 不传输到任何地方。
- 权限信息不写入安全文档中，而是保存在服务器。
- 客户端和服务器均使用标准 AES 进行加解密，支持接入第三方算法。

六、云文档服务组件

WPS 云文档服务组件是 WPS 云文档面向业务系统应用提供的一种云服务能力，通过提供文档组件页面、API 接口等方式，支持全平台业务系统应用的调用，让业务应用可以直接有如下功能体现：

- 文档存储管理
- 文档在线预览
- 文档安全控制
- 文档历史版本
- WPS Office 不落地编辑
- 在线协作文档

让业务应用产生的文档上云并流转，减去常见的中间件逻辑处理，大大提升业务流转时程序间的处理效率，给予用户更好的使用体验。

接口列表

Operations

Resource Path	Operation	Description
/sys_api/v1/spaces/{space_id}/files	POST	创建文件
/sys_api/v1/spaces	POST	创建空间
/sys_api/v1/spaces/{space_id}/upload_request	POST	请求文件上传地址
/sys_api/v1/spaces/{space_id}/files/{file_id}/preview_address	GET	请求文件预览地址
/sys_api/v1/spaces/{space_id}/files/{file_id}/download_address	GET	请求文件下载地址
/sys_api/v1/spaces/{space_id}/files/{file_id}/permissions	PUT	修改文件权限
/sys_api/v1/spaces/{space_id}/files/{file_id}/permissions	GET	获取文件权限列表
/sys_api/v1/spaces/{space_id}/files/{file_id}/versions	GET	获取文件历史版本列表
/sys_api/v1/spaces/{space_id}/files/{file_id}/histories/{version_id}/download_address	GET	获取文件历史版本下载地址
/sys_api/v1/spaces/{space_id}/files/{file_id}/revert	POST	回滚历史版本
/sys_api/v1/spaces/{space_id}/search_files	POST	搜索文件
/sys_api/v1/spaces/{space_id}/files/{file_id}/name	POST	重命名文件
/sys_api/v1/spaces/{space_id}/files/{file_id}	DELETE	删除文件
/sys_api/v1/spaces/{space_id}/files/{file_id}/outwarddoc	POST	创建外带文档