KODBOX 企业网盘

文档云存储与协同办公平台

架构与产品安全性设计

kodcloud.com

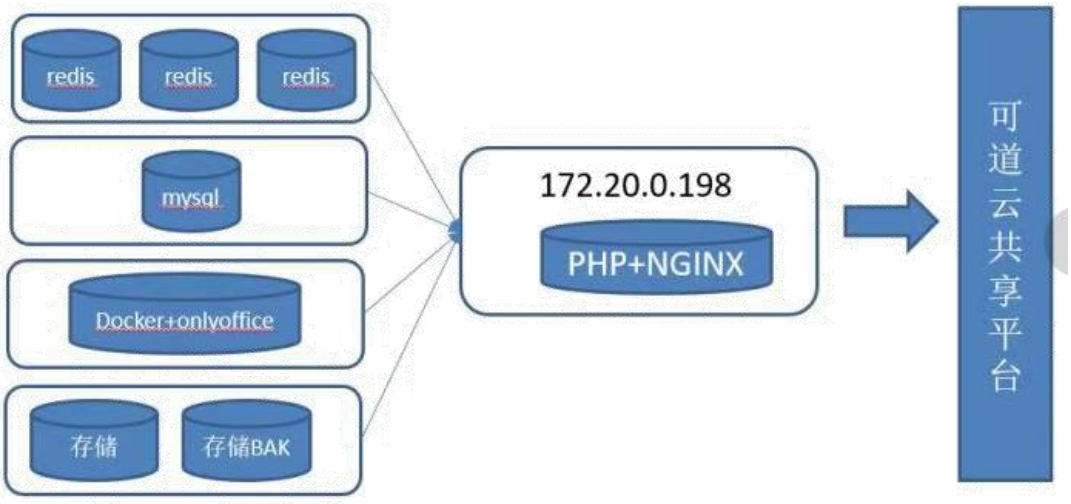
01

1 产品架构设计

基于文档集中存储和管控、办公协作需求，企业网盘系统属于日常办公的高频重度应用，具有访问频繁，IO 吞吐量大，带宽要求高的特点。为了确保系统在大用户、高并发状态下的性能，可道云平台支持采用高可用集群架构部署。

1.1 私有化部署/内外网隔离/集群架构

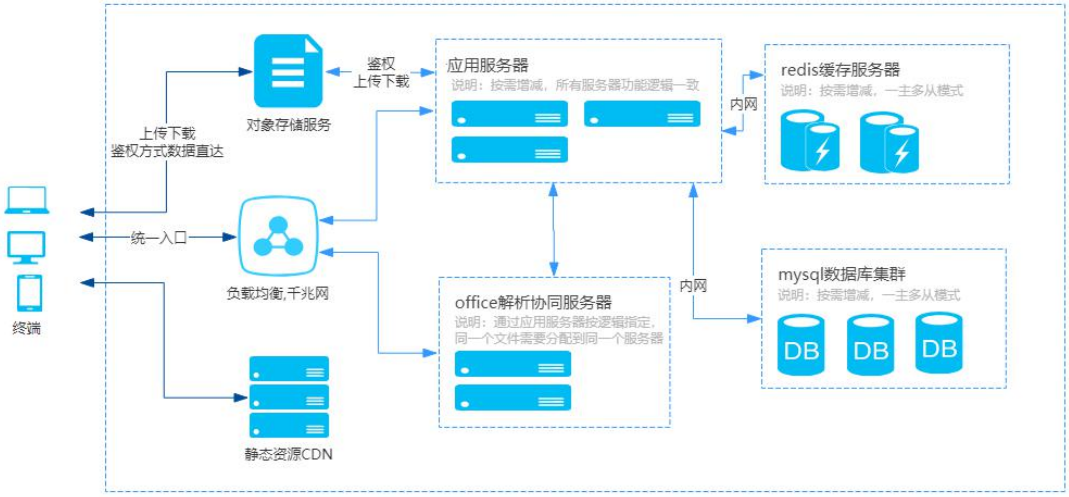
可道云系统采用 B/S（+C/S）架构，具有轻量、全平台兼容性和适应性，在 Linux / Windows / Mac(Apache、Nginx、IIS)环境中均可安装部署。B/S 架构下，用户界面完全通过浏览器实现，仅需浏览器即可轻松实现文档上传下载、访问管理和分享。应用程序的升级和维护都可以在服务器端完成，升级更加维护方便。系统分为服务器、客户端两大部分，形成了 B/S+C/S 的混合架构，同时提供了 PC 客户端、移动端 APP 应用（Android+iOS），客户端、APP 可以方便用户快速实现本地和云端数据的同步、适应用户本地化的操作习惯。



可道云 KODBOX 私有化部署按企业数据管理需求可选择多种方案，从普通的单台服务器系统到服务器集群，超融合系统，甚至混合云方案。

针对用户规模较小的使用场景，可道云提供了数据增量备份功能，可以定时将数据增量备份到指定的磁盘或网盘存储挂载。

用户多、业务规模较大时（一般 1000 用户以上时），可道云企业网盘推荐采用集群部署方案。集群部署方案是将系统中不同的应用服务分离部署到多台服务器中，共同实现完整的企业网盘服务，通过提高单位时间内执行的任务数来提升效率，实现高可用和负载均衡。

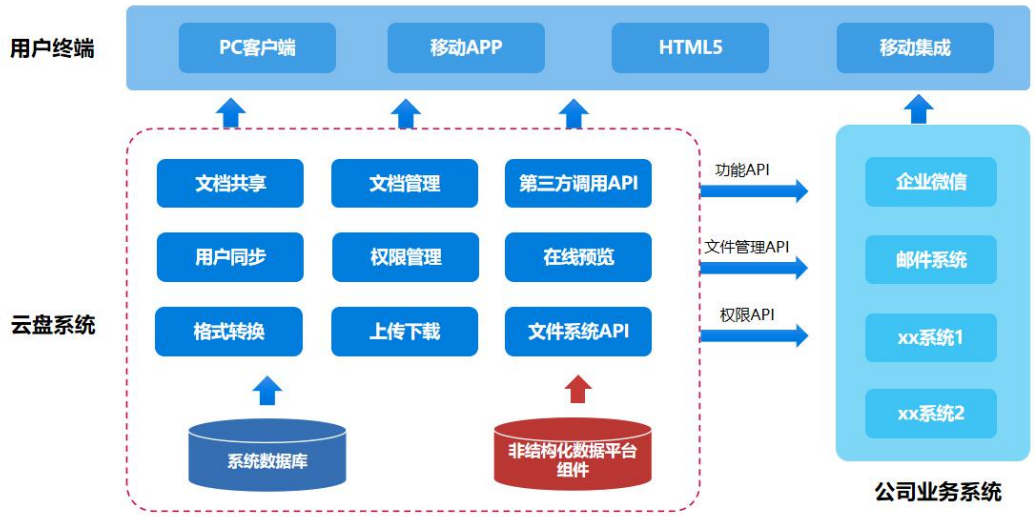


根据平台各功能负载的特点，主要分为应用、数据、存储、缓存、解析等多个服务单元，协同完成复杂的文档协作功能。集群部署时，可采用负载均衡 LVS + 应用服务器*N + 数据库服务器*N + 缓存服务器*N + 存储服务器*N。

可道云系统支持多种存储方式并行挂载：磁盘、FTP、主流对象存储等，极大提高了系统存储的可扩展性。可最大程度满足业务增长提供弹性扩展能力，无论是在用户数、文件数、计算性能、存储空间等各方面，均支持无限制的后期线性扩展能力，能在不停机服务的情况下实现弹性扩容。

1.2 应用架构

可道云通过云盘应用接口、插件接口、文件预览组件接口及通用 API 接口实现与 PC、手机客户端及第三方业务系统的互通互联。



1.3 技术架构

可道云系统分为 4 层架构，由显示层，逻辑层，持久层，存储层。自下而上，由低层为高层提供服务。

- 存储层包含存储于数据库的结构化数据和存储于文件系统非结构化数据；
- 持久层确保事务的完整性，将数据优化后写入数据库，包含数据访问组件和事物管理组件；
- 逻辑层负责实现所有的业务逻辑，主要包含用户组织架构、角色权限管理、文档权限管理、业务逻辑组件、业务接口组件、插件服务组件等；
- 显示层为不同平台客户端呈现系统 UI，完成系统功能交互，主要包含多端显示支持。

可道云由存储储存于数据库中的结构化数据，以及存储于文件系统系统中经加密处理的非结构性数据两部分组成，二者通过唯一的 ID 标识相关联。外部接口利用可道云中的控制数据实现业务逻辑，最终索引至相应的文档，实现跨平台的访问。

02

2 系统安全性说明

2.1 系统安全设计

可道云系统针对每种攻击方式都制定了一套完整防御方案，可有效抵制恶意用户对系统进行的攻击，有力提高系统的安全性，保证系统能够相对安全的部署、运营、维护、升级、发展。同时，在局域网环境下私有化部署，可以确保软件、硬件、网络三位一体，物理隔绝，系统防范数据安全风险，确保数据安全。

2.1.1 账号及登录安全

密码保护 用户密码加严及 32 位 MD5 加密

登录验证码 自定义设置启用登录验证码防止利用工具破解密码，方便进行人机验证

密码强度 支持普通、中等、高强度不同密码强度组合供管理员选择和设置，可有效杜绝弱口令

密码锁定 连续 5 次密码输入错误后，账号会进入锁定阶段，防止暴力破解

IP 白名单 仅允许指定 IP 或 ip 区段用户访问，防止数据异地访问、泄露

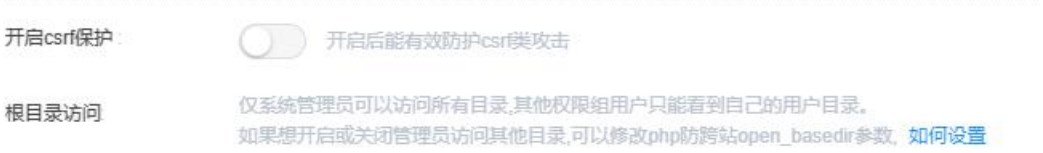
2.1.2 注入漏洞攻击防范

- 查询参数使用严格的过滤函数进行过滤；
- 限定 URL 的传递参数类型、数量、范围等来防止通过构造 URL 进行恶意攻击

2.1.3 跨站脚本攻击防范

CRFS 保护 可选择开启，以防护 CSRF 类攻击

根目录访问限制 可限制服务器目录访问权限



- 对于不支持 HTML 标记的内容使用 HTMLEncode 进行编码；
- 对于支持 HTML 标记的内容使用脚本过滤函数来过滤绝大部分可运行的脚本代码，作为防范的辅助措施；

2.1.4 其他安全措施

●对程序业务逻辑代码进行加密和混淆，避免恶意用户通过反射程序集利用代码漏洞攻击；

●建议和协助项目方配备有关防病毒及木马软件来处理系统病毒及木马问题；

●建议和协助项目方配备具有快照功能的存储设备对用户文件进行实时备份；

●建议和协助项目方配备分级存储管理软件系统，以提高存储空间利用率；

2.2 传输/存储安全

2.2.1 传输链路加密

传输加密 可道云系统支持文件上传下载 HTTPS 加密，传输过程中对文件本身进行了二次 AES CTR 256 算法流式分块加密，确保最终保存在云存储系统的文件均为密文，在传输以及存储过程中杜绝被窃取可能 。

2.2.2 数据存储安全

加密存储 可道云对上传文件进行去后缀元数据加密存储，以避免被上传木马文件攻击，同时可以有效防范勒索病毒破坏；对上传文件进行加密后统一存储，以避免恶意用户根据目录或文件名获取文件。

管理员也可以基于后台数据可见性需求可选不加密模式。

文件校验 存储文件在服务器端均进行 MD5 哈希校验，确保文件独一无二，防止篡改。
分布式存储/混合存储 支持将数据存储在百度云 BOS、阿里云 OSS、AmazonS3 等对象存储，数据存储节点多，自动实现异地容灾，可以最大程度确保数据安全性。
分布式数据库 分布式数据库保证数据库的稳定安全及读写速率，可在数据库受损的情况下快速还原。

2.3 权限管控与操作审计

可道云采用**角色权限**和**文档权限**双轨制的权限体系，最大程度上保证内容安全。

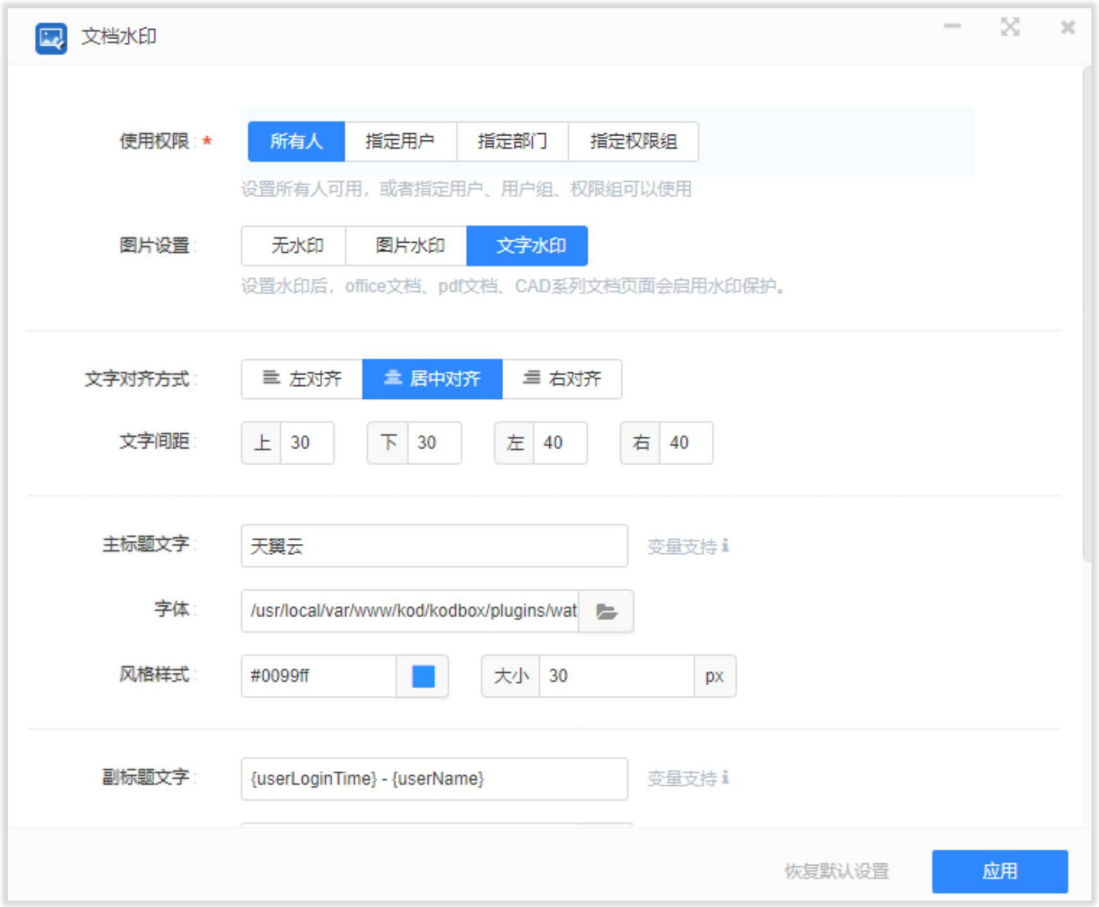
2.3.1 权限体系

- 权限角色、部门权限、文档权限三维权限管控，覆盖多场景权限设置需求
- 按需设定不同角色，文件管理、上传下载、数据配置、用户管理、群组管理、插件管理等 30 余种项目灵活配置权限。
- 按需灵活设置文档权限组合，列表查看，预览，编辑，下载，上传，删除，分享，文档评论，查看动态，管理权限，满足不同场景下的文档权限赋能。
- 文档管理员可以对任意数量的任意部门、任意用户进行权限指定，按需配置文档权限。
- 支持多层文件夹嵌套不同级别的文件权限，按人、按组织、按文档、按事件灵活授权。

2.3.2 文件安全策略

文件分享 分享文件可以进行相关设置，条件不满足则不能对文件进行访问和操作

文件水印 可对文档添加图片或文字动态水印，防止未经授权对文件进行截屏、拍照，保护知识产权。



文档历史记录 对同名文件进行操作，产生历史记录，可以进行文件版本回退；文件重命名或移动，版本记录自动跟随。

2.3.3 行为审计

可道云详细记录了整个企业网盘的登录日志、操作日志，可导出作为凭据。可以筛选查看特定成员的访问情况。确保文档有迹可循。