GallopWave

郑州市骏澜咨询服务有限公司

PRIVATE DEPLOYMENT · WHITE PAPER

私有化部署白皮书

架构 · 数据安全 · 运维建议 | 供 IT 评估参考

技术方案 · 公开资料

版本：V1.0 | 发布：2026 年 11 月

郑州市骏澜咨询服务有限公司 · 服务热线 150-9336-3914 · junlanzixun.cn

摘要

本白皮书面向客户 IT、信息化与采购评估人员，说明 GallopWave 系列业务管理系统在**私有化部署**形态下的总体架构、多租户隔离、账号与访问策略、数据安全、客户端形态与运维保障，供技术选型与内部评审参考。

> 产品定位：以「体系文件搭建 → 软件系统 → 软件相关硬件服务」三条互为闭环的线为交付主线，一套账号打通，一个口子交付到底；所有软件系统均支持免费体验。

本文适用读者与边界

读者	关注点
IT / 信息化负责人	架构、集成方式、数据归属、权限与运维交接
安全与合规	传输与存储加密、账号策略、备份、审计与最小权限
业务与采购	交付范围、上线节奏、验收方式、后续服务

> 本白皮书描述的是**通用的技术方案与工程实践**。具体服务器规格、域名规划、系统清单、性能指标、服务等级与商务条款，以双方确认的正式实施方案与合同为准；本文不含报价与量化 SLA 承诺。

一、总体架构

系统采用分层设计，各层职责清晰、可独立扩展；对外通过统一域名与反向代理收敛入口，减少暴露面并简化证书与运维管理。

层次	主要组件	职责
接入层	Nginx 虚拟主机、HTTPS 证书、反向代理	统一入口、TLS 终止、路径/子域路由、静态资源与下载分发、缓存策略
鉴权层	统一鉴权服务（GW-Auth）	登录、会话与令牌、企业代码与租户识别、角色与权限校验
应用层	各业务系统服务、进程管理（PM2 等）	按系统独立部署、独立启停与重启、故障隔离
数据层	每租户独立数据库 / 数据文件	数据隔离、按租户备份与恢复、权限分库
运维层	备份与回滚、日志与监控、发布脚本	原子上线、变更可回退、运行可观测、定期巡检

对外访问可按阶段收敛为**单端口整合**：官网与云应用合并在同一服务端口下以路径区分，子域名逐步退役，从而降低证书、端口与防火墙策略的维护成本。

二、多租户与隔离

- **一租户一库：**每个企业租户拥有独立数据库或数据目录，账号、业务数据与配置互不共享。
- **企业代码：**以企业代码作为租户标识，登录时与账号一并校验，确保账号只落在所属租户内。
- **独立域名 / 子路径：**每套系统可对应独立子域名，亦可收敛到统一域名下的子路径，便于统一品牌与证书管理。
- **配置隔离：**各租户的鉴权配置、界面文案与业务参数独立维护，互不影响。
- **按租户运维：**账号开通、数据备份、版本升级均可按租户粒度执行与回滚。

三、统一账号与访问策略

按系统属性划分三类访问策略，既保证公开资料的可达性，又保证企业数据的受控访问：

类型	适用系统	开通方式
免登录访问	官网、门户 / 云入口	公开访问，无需账号
自助注册	个人版系统	用户自助注册后即可使用
管理员开通	企业版系统	由企业管理员提交信息、后台审核开通，绑定企业代码

登录与凭据

- 统一采用**手机号 + 密码 + 图形验证码**方式登录，界面口径全站一致；第三方登录与短信验证码不作为登录入口。
- 密码在服务端以**加盐哈希**方式存储（按系统采用 scrypt / bcrypt / PBKDF2 / HMAC-SHA256 等不可逆算法），不保存明文口令。
- 角色分级：系统管理员 / 企业管理员 / 普通用户，权限按角色最小化授予。
- 企业管理员可在所属企业代码下维护本企业用户（姓名、电话、部门、邮箱等信息）。

四、数据安全

方面	措施
传输	

方面	措施
	全站 HTTPS / TLS，证书由自动化工具签发与续期；管理入口与下载分发同样受 TLS 保护
存储	口令不可逆哈希；敏感配置与密钥不落前端；租户数据分库隔离
权限	按角色与租户双重校验；后台管理操作限定管理员；最小权限原则
备份	变更前完整备份、周期性数据备份、可验证的恢复流程
变更	发布遵循「只读勘察 → 备份 / 回滚预案 → 最小改动 → 原子上线 → 复核」流程
审计	关键操作与登录留有记录，便于追溯与问题定位

五、客户端形态

形态	获取方式	适用场景
Web	浏览器直接访问	全功能、日常办公主入口
PWA	浏览器添加到桌面	轻安装、离线可用、自动更新
Android APK	官网下载中心	移动端快捷入口、现场作业

移动端与桌面端共用同一账号体系与后端服务，数据实时一致。

六、部署与运维保障

1. **环境准备：**Linux 服务器（如 Ubuntu LTS）、域名解析、证书、反向代理与运行时环境。
2. **安装部署：**按系统清单逐个部署服务，配置独立数据库与租户参数。
3. **账号初始化：**开通企业代码与管理员账号，按角色分配权限。
4. **联调验证：**配置校验、磁盘落盘、HTTP 拉取、浏览器真实渲染三重复核。
5. **上线与交付：**提供访问地址、账号清单、操作手册与培训。
6. **持续运维：**版本升级、监控告警、备份巡检、故障响应与定期复核。

> 工程实践要点：任何生产变更均保留可执行的回滚预案；变更后以 fresh 实时复核确认，不以历史结论代替现实验证。

七、交付与验收清单（参考）

序号	交付项	验收要点
1	系统访问地址与域名总表	逐系统可访问、命名与清单一致
2	管理员账号清单	账号可登录、角色正确、口令独立交付
3	企业代码与租户配置	租户隔离生效、数据不串库
4	操作手册 / 培训	覆盖登录、通用操作、移动端与常见问题
5	备份与回滚说明	备份可恢复、回滚步骤可执行
6	证书与安全配置	HTTPS 有效、证书续期可用

八、声明与联系

本白皮书为技术方案说明，属于公开参考材料。文中架构、组件与流程为通用工程实践描述，具体规格、系统范围、性能指标、服务等级与商务条款以双方确认并签署的正式方案 / 合同为准，本文不构成报价或承诺。

获取定制部署方案：服务热线 / 微信同号 **150-9336-3914** · 官网 **junlanzixun.cn** · 郑州市骏澜咨询服务有限公司