

汉土私有云平台

汉土私有云系统功能介绍

产品功能介绍 · 售前与交付对齐

文档类型：系统功能介绍

编写日期：2026-07-16

适用范围：产品对外介绍、售前培训、交付说明、内部对齐

1. 产品定位

汉土私有云面向机房/专网/无公网环境的私有云交付与运维，提供从物理资产纳管、Ceph 存储、OpenStack 离线安装，到虚拟机与自动运维的一体化平台。

一句话定位：

无网可装、装完可验、运行可审计、故障可 Playbook 处置 —— 尽量少 SSH、少改库、少手拼配置。

核心价值：

价值点	说明
纯离线交付	OpenStack / Ceph 等安装一律走离线包，禁止公网回退与代理绕过
黄金安装路径	四段式流水线：选方案 → 准备专属包 → 确认就绪 → 部署入库
存储铁律	OpenStack 块/镜像存储对接平台已纳管的外部 Ceph，并强制选池
减轻运维	Install Guard（装前）+ Runtime Auditor（运行）+ Playbook（处置）
资产可审计	裸金属上架/下架台账、配件流转、运维事件与交付凭证留痕
多租户 RBAC	租户隔离、平台/租户角色、权限键校验前后端一致

2. 总体能力地图

汉土私有云管理平台			
资产管理	基础设施	自动运维	应用平台
裸金属节点	存储(Ceph)	运维中心	数据库 / CDN
配件管理	节点群集	巡检与预检	安全编排 / HPC
BMC/PXE/KVM	虚拟机管理	审计与自愈	AI 算力 / 对象存储
	网络 / 镜像		
用户与租户 · 系统配置 · AI 运维辅助(Copilot) · SSH/合规门户			

导航结构（产品壳层）：

- **侧栏主链：**资产管理 → 存储管理 → 节点群集管理 → 虚拟机管理 → 网络规则 → 自动运维 → 镜像管理 → 用户管理（平台管理员）
- **顶栏入口：**应用平台、系统配置（管理员）
- **独立能力页：**裸金属 KVM 控制台、SSH Web 终端、系统初始化安装向导、法务材料门户

3. 资产管理

3.1 裸金属节点

不依赖 OpenStack IroniC，平台直连 BMC，实现物理机全生命周期管理。

能力	说明
纳管与扫描	网段扫描落库；Redfish / IPMI 适配；凭据探测与可编辑台账
电源管控	开机 / 关机 / 重启 / 状态查询（双协议）
远程控制台	优先 HTML5 KVM 流代理；老旧机走 IPMI KVM
重装系统	Redfish 虚拟介质、PXE/Kickstart；支持批量 PXE
PXE 发现	探活 MAC、多网口登记、控制节点 PXE 栈与装机包联动
上架/下架	运单、合同/视频凭证、业务 IP/带宽等交付字段台账
运维事件	按节点记录处理方案、时间、结果与附件；可联动 AI 生成建议

3.2 配件管理

物理配件入库、库存、装机、拆机、报废；与裸金属节点关联，支撑交付清单与资产盘点。

4. 存储管理（Ceph）

以外部 Ceph 为 OpenStack 唯一块/镜像后端，平台负责集群纳管与日常运维。

能力	说明
集群向导	创建集群记录、SSH 预检、cephadm 环境、bootstrap（门禁）
节点纳管	存储节点登记、探测、加入集群
OSD 运维	状态同步、out / in / reweight、创建 OSD
存储池	远端创建/删除/调参；RBD 预检；数据面健康（对齐/降级）可见

OpenStack 对接	集群密钥与池供四段式部署强制选用
异步任务	部署与运维任务可追踪；容量/IOPS 概览来自状态同步

5. 节点群集管理（OpenStack 离线部署）

资源池页是 OpenStack 控制面/计算面交付的主战场，核心是 **四段式离线部署**。

5.1 四段式主路径

1. **选定方案（Ansible 模板）** —— 组件、Neutron 插件、规模与角色契约
2. **准备专属离线包** —— 模板与固化包 1:1；支持增量构建 / 本地超集裁剪重打包
3. **确认就绪** —— 选包校验、组件三处一致（模板 / 包 manifest / 部署 options）
4. **安装部署** —— 填 SSH、外部 Ceph 池、业务网等现场参数 → 预检 → prepare → deploy → **节点自动入库**

硬性约束：

- install_mode 固定 **offline**，必填安装包 ID
- 禁止公网 apt/pip/拉镜像，禁止 SSR/SOCKS5 等代理绕过
- OpenStack **必须**对接平台 Ceph 并选池
- 取消「手工随意加节点」作为主路径

5.2 配套能力

模块	说明
OpenStack 节点	部署成功后入库的控制/计算节点树表与详情
Ansible 配置模板	按类别管理生产/实验方案；组件只读来自契约
固化安装包	installpage 离线包台账与元数据
构建专属包	按模板生成/重打包专属离线制品
SSH 管理	主机台账、凭据、Web 终端入口；高危命令门禁可配置
部署任务与日志	长跑任务心跳、SSH 重连、预检与部署日志可观测

网络侧配套：公网 SSH 保活、业务 VLAN 分离、VIP/business_ip 预检，避免部署后误断管理通道。

6. 虚拟机管理

对接 OpenStack Nova 等计算能力，提供日常 IaaS 操作：

- 虚拟机列表、创建、启停、重启、调整规格、修改管理员密码
- 批量操作与控制台（noVNC）
- 与镜像、网络、外部 Ceph 卷联动
- 裸金属已迁出至「资产管理」，计算页专注虚拟机

7. 网络规则与镜像管理

模块	说明
网络规则	业务/管理网络规划与策略视图，支撑部署前网络预检与运行审计
镜像管理	云主机镜像台账与分发；与 Glance（Ceph 后端）及裸金属装机介质协同

8. 自动运维

以 **减轻人工 SSH** 为北极星，值班入口统一到「自动运维」。

8.1 运维中心

值班主界面，聚合：

- 运行期告警与平台监控告警
- 告警渠道健康、日志与任务时间线
- Playbook 一键处置（高危操作需确认 + 审计）
- 与部署/裸金属事件同一观测语境

8.2 巡检与预检

- **Install Guard**：部署前提条件硬校验（网络、Ceph、组件、SSH 等）
- Day-0 冒烟验收思路：装完可验，失败可追溯

8.3 审计与自愈

- **Runtime Auditor**：运行期周期检查配置双轨、幽灵卷、服务健康等痛点
- 自愈与 Playbook 闭环：优先准确处置脚本，危险操作默认告警确认

- SSH 凭据审计、配置单一真相（平台渲染，避免目标机与平台配置分叉）

9. 应用平台

上层应用能力统一卡片入口（按权限显隐）：

应用	能力概要
数据库集群	MySQL / PostgreSQL / ClickHouse / Redis / MongoDB 等部署与运维（含备份就绪视图）
CDN 管理	加速域名、缓存策略、边缘节点与统计
安全编排	安全组件部署、策略编排与合规材料
超算模块	Job/节点调度与算力相关能力（如 Slurm）
AI 算力管理	GPU 资源、训练/推理等算力台账（独立产品线）
对象存储	S3 兼容桶与密钥等（占位/演进中）

监控能力已并入运维中心 Tab，不再作为侧栏重复入口。

10. 用户、租户与权限

能力	说明
登录与会话	认证、刷新令牌、工作租户切换
租户空间	组织/客户隔离边界；配额与成员管理
账号体系	平台管理员 / 租户管理员 / 普通用户；可建平台预置角色与租户自定义角色
权限模型	资源域 + 动作键（前后端校验一致）；侧栏与应用卡片按权限裁剪
API 审计	平台写操作审计记录（用户管理页签）

11. 系统配置与生产就绪

面向平台管理员：

- 系统参数 / 数据库连接与初始化相关配置
- 生产就绪（Ops Readiness）门禁与导出
- SSH 密码轮换策略与高危命令规则指向
- 告警 Webhook、附件/S3、备份就绪等运维配套

- 固化安装包等与交付相关的系统级入口聚合

另提供 **系统安装向导**（首次初始化库与管理员）及 **法务材料门户**（已发布合规文档下载）。

12. AI 运维辅助（Copilot）

定位为 **只读建议层**，不替代 Install Guard / Playbook 执行闭环。

能力	说明
统一 LLM 网关	多模型路由、按场景选型与降级；可对接内网推理
RAG 环境记忆	成功/失败经验、运维事件等入库向量检索，回答时注入环境上下文
落地场景	裸金属 KVM 侧栏问答、运维事件「生成处理方案」、资源池模板只读建议
安全约束	脱敏、审计、租户隔离； 禁止 默认自动执行高危命令；开关关闭时前端优雅降级

13. 典型使用场景

场景	路径摘要
新机房无网装 OpenStack	存储纳管 Ceph → 选四段式方案 → 构建专属包 → 预检部署 → Day-0 验收
物理机上架交付	扫描/纳管 BMC → 上架台账与凭证 → PXE 或 ISO 装机 → 控制台验收
日常值班	运维中心看告警 → Playbook 处置 → 审计留痕；少登目标机
多租户运营	建租户与角色 → 配额隔离 → 租户内自助使用 VM/应用能力
配件与资产盘点	配件入库/装机关联节点 → 与上架清单一致可追溯

14. 技术架构概览

层次	选型与说明
前端	Vue 3 + 现代响应式壳层；业务页组件化（资产管理、资源池、运维中心等）
后端	Go（Gin）REST API；权限中间件与异步任务模型
数据	PostgreSQL（含 AI 场景 pgvector）；业务台账与运维事件

	落库
基础设施对接	OpenStack API、Kolla-Ansible 离线部署、cephadm / Ceph、BMC（Redfish/IPMI）、SSH
观测	Agent 指标上报、告警渠道、WebSocket 任务/告警推送

15. 产品原则（交付与排期标尺）

- 1. **一条安装主路径**：四段式 + 仅 offline，减少「每人一套装法」
- 2. **三处一致**：构建 manifest = 包元数据 = 部署组件契约
- 3. **防御切面**：装前预检、运行审计、Playbook 处置
- 4. **危险操作门禁**：默认告警 + 人工确认 + 审计表留痕
- 5. **配置单一真相**：网络、SSH、Ceph 参数从平台渲染，避免双轨
- 6. **运维中心唯一值班入口**：部署、告警、裸金属事件汇聚同一语境
- 7. **AI 后于 Playbook**：先准确处置，再增强建议；建议默认只读

16. 文档与演进说明

本介绍归纳自现网导航、路由与中期需求体系（离线安装、资产管理、自动运维、AI Copilot 等）。部分应用子模块（如对象存储）仍在占位或分阶段完善；详细实施与验收以 doc/ 目录下中期需求、四段式方案、裸金属总方案、AI 实施计划等工程文档为准。