

汉土私有云平台

汉土私有云系统操作手册

交付与值班操作指南

文档类型：操作手册

编写日期：2026-07-16

适用角色：平台管理员、机房交付工程师、值班运维

配套文档：汉土私有云系统功能介绍系统.md

1. 使用前须知

1.1 浏览器与网络

- 推荐使用桌面浏览器，宽度 $\geq 1280\text{px}$ （四段式装机、批量 PXE、复杂表单）
- 手机/窄屏仅适合查看进度、日志与告警，不适合发起完整离线部署
- 管理端需能访问平台 Web 与各目标机 BMC/SSH（按现场网络规划）

1.2 账号与权限

角色	典型权限
平台管理员	全菜单；用户/租户；系统配置；危险操作开关相关能力
租户管理员	本租户资源与成员；可见资产管理、存储、群集、运维等（按权限键）
普通用户	按角色权限矩阵裁剪菜单与写操作

未加入任何租户的账号，业务菜单可能不可用。工作租户以登录后会话为准，可在个人能力中切换租户（若账号属于多租户）。

1.3 操作铁律（务必遵守）

1. OpenStack / Ceph **仅离线**安装，禁止指望目标机访问公网拉包
2. OpenStack 部署前，**必须**已有平台纳管的 Ceph，并在部署向导中选池
3. 部署节点请走 **四段式**，不要以「手工随意加节点」替代主路径
4. 高危操作（OSD out、Playbook 高危项、幽灵卷删除等）默认需 **确认 + 留痕**
5. 配置以平台台账为准，避免在目标机手改 `globals.yml` 等与平台分叉

2. 首次初始化与登录

2.1 系统安装向导（全新环境）

访问路径：`/install`

步骤	操作
1	填写数据库主机、端口、库名、用户名与密码 → 测试连接
2	开始初始化 ，导入表结构（已有表时可能失败，需换空

	库或人工处理)
3	创建默认 管理员账号
4	安装完成 → 进入登录页

已初始化且非平台管理员会话下，高危初始化步骤可能被隐藏，避免误重置。

2.2 日常登录

1. 打开平台登录页，输入用户名与密码
2. 登录成功后默认进入 **应用平台**（或按权限可见首页）
3. 顶栏右侧可进入 **应用平台 / 系统配置**（管理员） / 退出

密码遗失请联系平台管理员在「用户管理」侧重置（以现网流程为准）。

3. 界面导航一览

入口位置	名称	做什么
侧栏	资产管理 → 裸金属节点	BMC 纳管、电源、控制台、上架/重装、运维事件
侧栏	资产管理 → 配件管理	配件入库、装机关联、报废
侧栏	存储管理	Ceph 集群、节点、OSD、存储池
侧栏	节点群集管理	四段式 OpenStack、SSH 台账、模板与离线包
侧栏	虚拟机管理	云主机生命周期与 noVNC
侧栏	网络规则	网络规划与相关策略视图
侧栏	自动运维 → 运维中心	值班主界面：告警、Playbook、时间线
侧栏	自动运维 → 巡检与预检	装前/运行巡检相关
侧栏	自动运维 → 审计与自愈	运行审计、自愈与 SSH 凭据审计入口
侧栏	镜像管理	云主机镜像
侧栏	用户管理	租户、角色、API 审计（平台管理员）
顶栏	应用平台	数据库/CDN/安全/超算/AI/对象存储
顶栏	系统配置	生产就绪、SSH 轮换、系统参数等

小屏用左上角汉堡打开侧栏；部分次要入口收入顶栏「更多」菜单。

4. 推荐交付顺序（新机房）

按下列顺序执行，可显著降低「装到一半缺存储 / 缺 SSH / 装完断管理网」的失败率：

- ① 规划网络与主机清单（管理 IP、BMC、业务 VLAN、VIP）
↓
- ② 登记 SSH 台账（节点群集管理 → SSH 管理）
↓
- ③ 存储管理：纳管/部署 Ceph → 建池 → 状态同步 → OpenStack 密钥就绪
↓
- ④ 四段式：选方案 → 准备专属包 → 确认就绪 → 填写现场参数并部署
↓
- ⑤ 自动运维：查看部署任务与 Install Guard 结果 → Day-0 冒烟/验收
↓
- ⑥ （可选）裸金属上架交付、虚拟机开户、应用平台业务

5. SSH 台账操作

路径：侧栏「节点群集管理」→ Tab「SSH 管理」

用途：安装与运维统一凭据来源；四段式部署、Ceph 远端操作、巡检从此选择，避免每次手输密码。

建议操作：

1. 为每台将要装机或运维的主机新增 SSH 目标（主机地址、端口、用户、密码/密钥按现场策略）
2. 保存后先做连通性验证（页内提供的探测/预检能力，以界面按钮为准）
3. 后续部署与存储远端操作一律选已保存台账

高危命令规则、双人审批等：在 SSH 相关配置区或「系统配置」中维护（见第 12 章）。

6. 存储管理（Ceph）操作

路径：侧栏「存储管理」

6.1 新建与 bootstrap（示意）

1. 使用 **部署向导** 创建集群记录（名称、版本等）
2. 选择「当前操作集群」
3. 按页内顺序：**SSH 预检** → **cephadm 环境** → **bootstrap**（需危险权限且服务端开关允许）
4. 在「存储节点」登记节点（先编辑保存 SSH 凭据）→ **纳管探测** → 加入集群
5. 「OSD」扫盘/创建 OSD；「状态同步」刷新健康、容量、池与 OSD 列表

6.2 存储池

- 1. 确认已选当前集群并选好管理节点 SSH 台账
- 2. **新建存储池**：勾选「远端执行」才会真正在 Ceph 上建池，否则只写平台记录（降级）
- 3. 删除池前可做 **RBD 预检**；远端删除会同步删库记录
- 4. OpenStack 安装前，在「Ceph 集群」页对该集群完成 **OpenStack 密钥** 相关就绪操作（见页内说明）

6.3 日常运维

操作	说明
状态同步	刷新 health、池用量、OSD、IOPS 采样
OSD out/in/reweight	维护窗口执行；需确认权限与二次确认
概览数据面	关注「对齐 / 降级 / 仅控制面」摘要，连续同步失败会进告警中心

7. 四段式 OpenStack 离线部署

路径：侧栏「节点群集管理」顶部「四段式 OpenStack 离线部署」

口号：**选定方案** → **为该方案准备专属包** → **用该包安装**。

7.1 步骤 ① 选定方案

- 1. 打开 Tab 「Ansible 配置模板」
- 2. 按分类浏览（控制面、计算最小包等）
- 3. 将目标模板设为 **当前方案**（星标/选中按钮）
- 4. 确认组件清单、网络插件等符合现场契约（组件只读，勿指望部署阶段随意扩大）

7.2 步骤 ② 准备专属包

- 1. 进入「构建专属包」或按页内引导为当前模板生成/重打包
- 2. 也可在「固化安装包」中确认该模板 1:1 专属包已存在且制品完整
- 3. 构建体积大、耗时长，请在有制品源/基础层的环境执行；避免半成品包直接上线

7.3 步骤 ③ 确认就绪

- 1. 查看专属包各制品分层是否全部就绪（页内 ✓ 指示）
- 2. 全部通过后再进入安装部署

7.4 步骤 ④ 安装部署

在部署对话框中重点填写：

字段类别	说明
方案与包	由四段式上下文锁定；换方案需返回步骤 ①
SSH 台账 / 连接 IP	目标机管理通道；可选 management_ip
Ceph 集群与池	必选 ；对接平台已纳管外部 Ceph
业务网等现场参数	VIP、业务 IP、网卡角色等按模板与预检矩阵

提交后：

- 1. 先过 **Install Guard / 安装预检**（失败则按提示修网络/SSH/存储后再试）
- 2. 观察页面底部 **最近部署任务** 与日志
- 3. 成功后 **OpenStack 节点自动入库**，在「OpenStack 节点」Tab 可见

失败常见原因：包组件与模板不一致、Ceph 未选池、公网 SSH 被 OVS 误占、SSH 台账错误。优先看预检矩阵与任务日志。

8. 虚拟机管理

路径：侧栏「虚拟机管理」

常见操作：

- 1. 列表筛选目标租户下的实例
- 2. **创建**：按向导选镜像、规格、网络与存储（依赖已部署 OpenStack + Ceph）
- 3. 启停 / 重启 / 调整规格 / 改管理员密码
- 4. **控制台**：打开 noVNC
- 5. **批量操作**：对多选实例执行允许的批量动作

若页面报 OpenStack API 不可用，先到「节点群集管理」确认控制节点健康与部署状态。

9. 网络与镜像

9.1 网络规则

路径：侧栏「网络规则」

用于查看/维护与业务、管理相关的网络规划信息，支撑部署前网络预检。物理交换机改配需机房侧配合，平台以检测与告警为主。

9.2 镜像管理

路径：侧栏「镜像管理」

上传或登记云主机镜像，供虚拟机创建使用。裸金属装机介质另见裸金属重装/PXE 流程。

10. 资产管理操作

10.1 裸金属纳管

路径：资产管理 → 裸金属节点

1. **扫描：**按网段探测 BMC（623/相关端口），结果落库
2. **添加/编辑：**填写 BMC 地址、协议（Redfish/IPMI）、凭据；可顺带勾选上架信息
3. **电源：**开机 / 关机 / 重启 / 刷新状态
4. **控制台：**进入 HTML5 KVM 或 IPMI KVM 页（独立控制台路由）

10.2 上架 / 下架

在节点详情「上架」相关面板：

1. **上架登记：**上架时间（必填）、运单、业务 IP/网关/带宽、MAC、合同与视频等凭证 → 提交
2. **下架：**须已有在服上架记录；填写下架信息与凭证后提交

未纳管 BMC 也可先台账，但不建议跳过电源与控制台验收。

10.3 重装与批量 PXE

1. 单机：**重装/部署**对话框，按机型选择 VirtualMedia 或 PXE/Kickstart
2. **批量 PXE：**列表入口打开批量对话框；缺 MAC 时建议先走 **PXE 发现** 回填，再正式装机
3. 需预先配置 PXE 服务地址或上传 kickstart（见系统配置 / 安装包说明）

10.4 运维事件

在节点「运维事件」面板：

1. 新增事件：现象、处理方案、结果、附件
2. 若已启用 AI 辅助，可用「生成处理方案」草稿，**人工确认后再保存**
3. 保存结果会进入运维审计/RAG 记忆（视开关而定）

10.5 配件管理

路径：资产管理 → 配件管理

登记配件入库 → 装机关联到裸金属节点 → 拆机/报废流转，保持与交付清单一致。

11. 自动运维值班

11.1 运维中心（主界面）

路径：自动运维 → 运维中心

建议值班节奏：

1. 看摘要卡：未确认告警、严重告警数量
2. 进入 **告警** Tab：筛选未确认 / 分类 / 处置类型
3. 可处理项：先 **确认**，再视情况点 **执行 Playbook**（弹出确认框，高危必二次确认）
4. 用时间线追溯部署、裸金属、Playbook 事件；深链可跳转节点上架/运维事件页
5. **可观测 / 日志 / 渠道** 等 Tab：看监控与告警通道健康

11.2 巡检与预检

路径：自动运维 → 巡检与预检

发起或回顾与部署相关的预检、巡检结果；失败项按提示回到资源池或存储侧修复后重跑。

11.3 审计与自愈

路径：自动运维 → 审计与自愈

查看运行期审计发现项、自愈执行记录；SSH 凭据审计可从本页或系统配置交叉进入。

12. 用户与系统配置

12.1 用户管理（平台管理员）

路径：侧栏「用户管理」

Tab	操作要点
租户列表	创建新租户 = 资源隔离空间；创建用户 = 登录账号。二者分开。先建租户再拉成员，或先建用户再加入租户
角色管理	维护平台角色权限键；按租户维护自定义角色
API 审计	查看平台写操作审计

12.2 系统配置

路径：顶栏「系统配置」

常见区块：

- 生产就绪检查与导出
- SSH 密码轮换策略与批次
- 系统键值配置、数据库相关说明
- 与固化安装包、告警 Webhook、备份就绪的跳转

修改危险开关前确认影响范围；生产变更建议留变更单。

13. 应用平台操作

路径：顶栏「应用平台」

点击卡片进入对应模块（数据库、CDN、安全编排、超算、AI 算力、对象存储）。无权限的卡片不显示。对象存储若标记「占位」，以页内说明为准，勿当生产能力承诺。

各子模块内操作按其页面向导执行（集群创建、策略配置、作业提交等）。

14. AI 辅助（若已开启）

前提：llm_assist（或等价开关）已启用，且账号有场景权限。

场景	操作
裸金属 KVM 侧栏	提问排障建议；若回复含命令，须人工点「执行」才写入 KVM

运维事件	「AI 生成处理方案」写入表单草稿 → 人工改完再保存
资源池模板	只读建议， 不会 自动改当前模板

原则：AI 是建议，不是放行；高危一律人工确认。

15. 日常运维速查

场景	去哪	做什么
半夜告警	运维中心 → 告警	确认 → Playbook 或按处置类型转现场
部署失败	节点群集 → 任务日志；巡检与预检	按 Install Guard 项修 SSH/网络/Ceph 后重试
Ceph 容量告警	存储管理 → 状态同步 / 池 / OSD	扩盘、调权；勿盲目删卷
客户机器上架	裸金属节点 → 上架登记	填 IP/带宽/凭证 → 可选装机验收
虚拟机卡死	虚拟机管理；必要时运维中心	走 OpenStack API 复位，禁止直接改库
忘记租户配额	用户管理 → 租户	调整配额后再开资源
无法登录菜单	用户/租户关系	确认已加入租户且角色有资源权限

16. 故障排查提示

- 1. **先看任务/告警，不要先 SSH 改机器** —— 平台日志往往已有预检失败原因
 - 2. **四段式中间失败**：核对模板、专属包、Ceph 池、SSH 台账四者是否同一套现场参数
 - 3. **装完断 SSH**：关注公网/管理口恢复相关提示与网络架构约定（管理面与业务面分离）
 - 4. **权限 403**：对照角色权限键；租户管理员不能操作仅平台管理员入口
 - 5. **控制台黑屏**：检查 BMC 协议选择、证书/端口、HTML5 vs IPMI 路径是否匹配机型
- 仍无法定位时，收集：时间点、任务 ID、节点 IP、告警 ID、浏览器控制台错误（脱敏后）交研发。

17. 附录：关键术语

术语	含义
四段式	选方案 → 专属包 → 就绪确认 → 离线部署
专属包	与某一 Ansible 模板 1:1 对应的离线安装制品
Install Guard	部署前硬性预检门禁

Runtime Auditor	运行期配置与健康审计
Playbook	平台固化的自动处置剧本
SSH 台账	平台内统一维护的主机凭据记录
上架台账	裸金属交付生命周期记录（非 BMC 电源状态）

汉土私有云系统操作手册 — 请与现场变更单、网络拓扑图一并使用