

汉土私有云私域组网 Linux 客户端操作手册

项目	说明
产品名称	汉土私有云-异地组网（Linux 终端）
适用对象	服务器 / 云主机 / 运维工作站上的现场工程师与运维人员
文档版本	1.0
对应客户端能力	凭组网 Token 入网、本机 Web 管理、systemd 常驻、自动重连、自动升级
对照文档	DOC/ADS/汉土私有云私域组网windows客户端操作手册.md

1. 产品简介

Linux 客户端是汉土私有云私域组网在服务器与工作站上的接入端。它通过管控面完成身份校验与地址分配，在本机创建虚拟网卡 `hantu0`（产品文案称 **Hantu SD-WAN**），与同一组网空间内的 Windows / Linux / 其它设备建立加密通道。

核心特点：

- **无需管控运维账号登录**：入网只需填写管控地址与组网 Token；账号体系保留在管控面管理端。
- **本机 Web 管理**：日常操作在浏览器中完成，页面布局与用词对齐 Windows 客户端。
- **智能链路**：优先局域网 / P2P 直连；必要时自动走「汉土中继」或「汉土保障线路」。
- **systemd 常驻**：首次以 root 前台启动时，会自动安装为系统服务并交由服务接管。
- **自动升级与重连**：管控面发布新版本后可自动替换；组网意外掉线时按策略重连。

本客户端定位为单节点接入终端，不要当作多设备流量中转路由器使用。
Linux **没有**系统托盘；断开组网在 Web 里操作，停守护进程用 `systemctl`。

2. 运行环境与组件

2.1 系统要求

- 操作系统：Ubuntu / Debian / CentOS / Rocky / Alma 等 **64 位 Linux** (amd64)
- 权限：安装网卡、装系统服务需要 **root**（或具备 `CAP_NET_ADMIN`）
- 工具：系统需有 `ip` (`iproute2`)；Web 测 Ping 依赖系统 `ping`
- 网络：能访问管控面 API 地址（形如 `http://管控域名或IP:8080`）

- 浏览器：任意现代浏览器即可打开本机管理页

2.2 主要组件

组件	作用
<code>hantu-client-linux</code>	单二进制：数据面 + 控制面 + 内嵌 Web 管理
systemd 服务 <code>hantu-client</code>	开机自启、异常重启、常驻运行
<code>/etc/hantu/client.yaml</code>	本地配置（管控地址、Token、MTU、Web 监听、管理密码密文等）
<code>/etc/hantu/client.env</code>	可选环境变量（可单独放 Token 等敏感项）
<code>/etc/hantu/log/</code>	客户端日志（按日滚动，默认保留约 3 天）
虚拟网卡 <code>hantu0</code>	组网数据面（Hantu SD-WAN）

与 Windows 的差异：Linux **不需要** 桌面端多文件组合，一个二进制即可。

3. 安装与启动

3.1 安装二进制

1. 从管理员处获取正式发布的 `hantu-client-linux` 。
2. 放到固定路径（建议 `/usr/local/bin/hantu-client-linux` ），并赋予执行权限：

```
sudo install -m 0755 hantu-client-linux /usr/local/bin/hantu-client-linux
```

3. 准备配置目录：

```
sudo mkdir -p /etc/hantu
```

可将样例配置复制为 `/etc/hantu/client.yaml`（Token 也可写在 `/etc/hantu/client.env` ）。即使暂不写配置，也可以先启动，再在 Web 设置页填写。

3.2 首次启动（推荐）

以 **root** 执行：

```
sudo /usr/local/bin/hantu-client-linux run
```

若本机是 systemd 发行版，客户端会：

1. 写入 `/etc/systemd/system/hantu-client.service`
2. 执行 `systemctl enable --now hantu-client`
3. **当前前台进程退出**，改由系统服务接管

之后请用服务命令管理，不要再长期前台跑第二份进程。

无 `systemd`、或非 `root`、或配置了 `auto_install_service: false` 时：跳过自动装服务，当前进程继续前台运行。

3.3 确认服务已起来

```
sudo systemctl status hantu-client
ss -lntp | grep 17890
```

看到服务 `active`，且 `17890` 在监听，即可打开管理页。

4. 打开 Web 管理页

4.1 访问地址

默认监听 `0.0.0.0:17890`（本机与局域网均可访问）。

- 本机浏览器：`http://127.0.0.1:17890/`
- 同网段其它电脑：`http://该Linux的管理网IP:17890/`

仅希望本机访问时，在设置页把「Web 管理监听地址」改为 `127.0.0.1:17890`，保存后 **重启服务** 生效。

远程服务器建议：不要把 `17890` 直接暴露到公网。可用 SSH 隧道在本机打开：

```
ssh -L 17890:127.0.0.1:17890 user@服务器地址
```

然后访问 `http://127.0.0.1:17890/`。

将 `ui_listen` 设为 `off` 可关闭 Web（仅保留 CLI / 自动连接）。

4.2 本机管理密码（与管控账号无关）

打开管理页后，标题为「汉土私有云-异地组网终端管理」。

情况	操作
第一次打开	设置管理密码（至少 6 位），确认后进入
已设置过	输入管理密码登录

说明：

- 这是保护 **本机管理页** 的密码，**不是** 管控面运维账号，也 **不是** 组网 Token。
- 密文写入 `client.yaml` 的 `ui_password_enc`，不会保存明文。
- 会话 Cookie 默认约 24 小时。
- 忘记密码时，在服务器上重置：

```
sudo hantu-client-linux set-ui-password 新密码
```

5. 首次配置（入网必做）

登录后，左侧底部 **齿轮图标** → **客户端常规设置**，按管理员提供的信息填写：

配置项	说明	建议
控制面 REST API 地址	管控面的 HTTP(S) 地址	例： <code>http://ipc.ipv4.me:8080</code> （以实际环境为准）
组网空间 Token	加入哪个虚拟组网空间的凭证	格式一般为 <code>NET_TOKEN_</code> + 32 位字符
虚拟网卡 MTU	隧道 MTU	默认常用 <code>1380</code>
开机自动连接组网网络	启动后自动连；意外掉线也会自动重连	服务器场景建议开启
Web 管理监听地址	管理页绑定地址	默认 <code>0.0.0.0:17890</code> ；仅本机改为 <code>127.0.0.1:17890</code>

操作步骤：

1. 填好地址与 Token。
2. 点击 **保存配置**（写入 `/etc/hantu/client.yaml`）。
3. 点击左侧栏 **链路图标** 发起连接（见下一章）。

说明：

- Linux 端 **没有** 管控运维登录页，也 **没有** 多空间管理；换空间请改 Token 后重新连接。
- Token 必须以 `NET_TOKEN_` 开头，否则无法入网。
- 修改监听地址后，页面会提示需要重启服务，请到本页「系统服务」点 **重启服务**。

6. 连接与断开

6.1 一键连接

1. 确认设置已保存。
2. 点击左侧栏下方的 **链路图标**（未连接时为断开样式）。
3. 连接过程中按钮会转圈并禁用，请勿重复点击。
4. 成功后：
 - 按钮变为已连接样式；
 - 侧栏可看到实时上下行速率；
 - 节点列表出现本机与同空间设备；
 - 本机出现网卡 `hantu0`，并获得虚拟内网 IP。

可用命令确认网卡：

```
ip addr show hantu0
```

6.2 断开连接

再次点击同一链路按钮即可断开。断开后会向管控面宣告离线，并拆除 `hantu0`。

注意：

- **手动断开** 后，本会话内不会自动重连（即使开了自动连接）。
- 若因网络抖动、服务重启等意外掉线，在自动连接开启时会按退避策略自动重连。
- 版本被管控面封禁、或连续鉴权失败等情况，可能关闭自动连接并提示升级/联系管理员。
- 断开后界面应立即恢复为未连接；若偶发卡住，刷新浏览器即可（客户端也会用状态轮询对齐）。

6.3 连接失败常见原因

现象	可能原因	处理建议
浏览器打不开管理页	服务未运行、端口未监听、热更后进程未拉起	<code>systemctl status hantu-client ; ss -lntp grep 17890</code>
401 / 鉴权失败	Token 错误、管控地址不对、本机与服务器时差过大	核对 Token/地址；校准系统时间；重启服务后再连
一直转圈或失败	配置未保存、服务异常	保存设置；看 <code>/etc/hantu/log/</code> ；重启服务
能连上但列表为空	空间内暂无其他在线设备，或策略隔离	确认对端已上线；联系管理员检查空间与 ACL
列表有人但互 ping 不通	对端防火墙拦 ICMP、对端未更新	先看通道状态与握手；业务端口仍可能正常

7. 界面功能说明

主界面与 Windows 客户端同构：标题区、左侧导航、节点列表、详情区。Linux 无窗口最小化/托盘，关闭浏览器标签 **不会** 停止组网。

7.1 左侧导航

图标	功能
服务器图标	节点管理 ：查看组网内设备列表与详情
盾牌图标	服务端配置 ：查看当前 Token 空间、带宽、网段、流量模式与保障/中继状态
链路图标	连接 / 断开 组网
齿轮图标	客户端设置 （含系统服务、Web 管理密码）

连接成功后，链路上方会显示当前实时速率。

7.2 节点管理

- 标题显示 **组网节点（在线数 / 总数）**。
- 支持按内网 IP 或名称搜索。
- 列表每页 10 条，底部分页翻页。
- 节点角标含义：
- **绿点**：管控侧判定在线
- **红点**：离线 / 未连通

- **灰点**：探测中
- 延迟数字（如 `35ms`）仅表示 ICMP 探测结果，**不会**因为 ping 失败就把在线节点改成红点。
- **本机** 节点带 `[本机]` 标识。设备 SN 一般为 `linux-...`。

设备备注

- 在节点上 **右键** → 「设置备注名称」；也可在详情页点「改备注」。
- 备注保存在本机，列表优先显示备注；原名仍可在副标题看到。
- 「清除备注」可恢复只显示管控原名。

节点详情

选中某节点后，右侧可查看：

- 在线状态、设备类型、标识信息
- 虚拟内网 IP、物理端点（Endpoint）
- **通道状态**（见 7.4）
- 延迟与「测 Ping」
- 收发流量（Rx/Tx）、最新握手时间
- 本机节点可看实时上下行速率折线

阻断入网 / 移除节点：Linux Web **暂不支持**（请到管控台操作）。界面上若仍有按钮，操作会提示不支持。

不走加密通道网段（Bypass）：当前版本 Linux **尚未开放**，详情页该列表为空，添加不会生效。需要直通本地网段时请联系管理员另作规划。

7.3 系统服务（设置页）

设置页中部为 **系统服务**：

操作	效果
以服务方式运行	打开：安装并启用 <code>hantu-client</code> ；关闭：停止并取消开机自启
重启服务	<code>systemctl restart</code> ，用于改监听地址、热更后异常、配置未生效等
刷新状态	重新读取 <code>installed / enabled / active</code>

无 `systemd` 的环境会提示无法以服务方式托管，请保持前台运行或自行编写 `init`。

7.4 服务端页与流量模式

进入「服务端配置」页可看到：

- 当前组网 Token 空间、QoS 带宽、组网 CIDR、隔离策略摘要
- **当前网络流量模式**：根据各对端实际通道汇总
- **汉土保障线路**：保活与兜底转发通道状态（ACTIVE / STANDBY / ERROR）
- **汉土中继**：中继能力状态（ACTIVE / ERROR / OFF）
- **P2P 公网映射**：是否已探测到公网映射及 NAT 类型

节点通道状态用语对照：

界面显示	含义
L1 局域网直连	同公网出口，走局域网直连，延迟通常最低
L2 IPv6 直连	原生 IPv6 端到端
P2P 网络	公网 UDP 点对点
汉土中继	经中继转发
汉土保障线路	经保障线路转发（弱网兜底）

7.5 Web 管理密码（设置页）

可修改本机管理密码，或点击 **退出登录** 回到登录页。修改后密文立即写入配置。

7.6 自动升级提示

检测到需升级时，会弹出全屏进度条，自动下载、替换并重启服务，一般无需手工干预。

策略要点：

- **正在组网时**会跳过普通热更，避免业务中断。
- 管控面标记 **强制更新** 时才会在组网中静默替换；替换前会先离开组网，新进程起来后按标记自动重连。
- 升级过程中请勿强制 `kill -9`；完成后服务会重新拉起。
- 若版本被封禁，界面可能出现不可关闭的拦截提示，请按提示完成升级或联系管理员。

8. systemd 与命令行运维

日常图形操作走 Web；下列命令给 SSH 登录后的运维使用。

8.1 服务生命周期

```
sudo systemctl start hantu-client      # 启动
sudo systemctl stop hantu-client       # 停止 (会 disconnect 并拆除 hantu0)
sudo systemctl restart hantu-client    # 重启
sudo systemctl enable hantu-client     # 开机自启
sudo systemctl disable hantu-client    # 取消开机自启
sudo systemctl status hantu-client     # 查看服务状态
sudo journalctl -u hantu-client -f    # 跟踪服务日志
```

8.2 客户端子命令

```
hantu-client-linux run                 # 连接并常驻 (Web + 自动重连 + 热更)
hantu-client-linux connect             # 同 run
hantu-client-linux disconnect          # 宣告离线并拆除 hantu0 (本会话不重连)
hantu-client-linux status              # 查看连接、虚拟 IP、Web 监听等
hantu-client-linux set-ui-password PWD # 设置/重置 Web 管理密码
hantu-client-linux help                # 查看用法
```

注意：服务已经在跑时，不要再另开一个 `run`，以免抢同一张网卡、同一监听端口。需要断开组网时优先用 Web「断开」，或：

```
sudo hantu-client-linux disconnect
```

`stop` 服务也会走 `disconnect`。

8.3 配置与环境变量

项	说明
HANTU_CONFIG	配置文件路径，默认 <code>/etc/hantu/client.yaml</code>
HANTU_CONFIG_DIR	密钥与运行时目录，默认 <code>/etc/hantu</code>
HANTU_SERVER_URL	覆盖 yaml 中的管控地址
HANTU_NETWORK_TOKEN	覆盖 yaml 中的 Token

`client.yaml` 常用字段：

字段	含义
server_url	管控面地址
network_token	组网 Token
mtu	默认 1380
auto_connect	默认 true
ui_listen	默认 0.0.0.0:17890 ; off 关闭 Web
auto_install_service	默认 true; false 关闭首次自动装服务
ui_password_enc	管理密码密文（禁止改成明文）
sn	留空则首次启动自动生成并回写

8.4 日志位置

- 文件日志： `/etc/hantu/log/` （配置目录不可写时才会落到其它路径）
- systemd 日志： `journalctl -u hantu-client`

排查问题时请同时保留近期文件日志与 journal。

9. 日常使用建议

1. **固定路径安装** (`/usr/local/bin` + `/etc/hantu`) , 便于自动升级与日志落盘。
2. **Token 仅从管理员处获取**, 不要使用来路不明的 Token。
3. 服务器建议开启 **开机自动连接**, 并用 systemd 托管。
4. 访问对端前, 先看节点是否绿点在线, 再看通道是直连还是保障/中继。
5. 互访业务优先用 **虚拟内网 IP** (列表中的组网 IP) 。
6. 更换管控地址或 Token 后: 保存 → 断开 (如已连接) → 再连接。
7. 修改 Web 监听地址后必须 **重启服务**。
8. 管理页默认全网卡监听时, 务必设好管理密码, 并用防火墙限制 `17890` 来源。
9. **不要** 在同一台机器上用其它组网工具同时占用 `hantu0` 或同一虚拟 IP。

10. 常见问题 (FAQ)

Q1: 为什么没有管控用户名密码? 登录页那个密码是什么?

入网不需要运维账号, 只用组网 Token。登录页密码只保护本机 Web 管理, 与管控面账号无关。

Q2: 关掉浏览器后组网还在吗?

在。浏览器只是管理入口。真正常驻的是 `hantu-client` 服务。要停组网请在 Web 点断开; 要停进程请 `systemctl stop`。

Q3: 连接成功但 ping 对端虚拟 IP 不通?

先确认两端都在线、握手有更新、通道状态不是异常。对端防火墙可能拦截 ICMP; 业务端口 (SSH、HTTP 等) 仍可能正常。两端建议使用同版本客户端。

Q4: 管理页打不开, 提示连接被拒绝?

先确认服务在跑、`17890` 在听。常见原因是热更把旧进程换掉后未再拉起, 执行 `systemctl restart hantu-client` 后再打开。

Q5: 点了断开, 页面一直转圈?

刷新浏览器。当前版本会用状态轮询把按钮恢复为未连接; 若仍异常, 执行 `hantu-client-linux status` 核对真实状态。

Q6: 设备列表从哪里来? 要不要自己添加?

由当前 Token 对应空间内实际上线设备自动同步, **不需要** 手工添加。同空间设备上线/离线会推送刷新。

Q7: 本机 SN 是什么?

按平台与硬件信息生成, 前缀一般为 `linux-`, 用于管控面识别设备, 一般无需手工修改。

Q8: 升级后服务没起来?

查看 `systemctl status hantu-client` 与日志。可手动再执行一次二进制; 残留的 `.old` 文件下次启动通常会自动清理。

Q9: 能否和 Windows 电脑互访?

可以。只要加入 **同一个组网 Token 空间**, Linux 与 Windows 使用同一套控制面/数据面协议, 用各自虚拟 IP 互访即可。

Q10: 忘记 Web 管理密码怎么办?

SSH 登录该机器后执行 `sudo hantu-client-linux set-ui-password 新密码`, 再用新密码打开管理页。

11. 运维侧简要对照（给管理员）

事项	说明
发放 Token	在管控面管理端创建空间 Token，格式建议 <code>NET_TOKEN_</code> + 32 位
管控地址	告知客户端填写的 API 根地址（含端口）
发布二进制	将 <code>hantu-client-linux</code> 放到服务器 <code>update/linux-amd64/</code> ，服务自动识别并推送升级
设备类型	上报 <code>linux_node</code> ；SN 前缀 <code>linux-</code>
设备清理	管理端可删除设备；删除后会回收地址并通知同空间刷新
封禁 / 踢人	请在管控台操作；Linux Web 暂不提供阻断/移除
客户端不做	管控运维登录、多空间管理 UI、系统托盘

12. 安全与合规提示

- Token 等同入网密钥，勿截图发到公开渠道，勿提交到代码仓库。
- Web 管理密码与 Token 都不要写进聊天记录或公开工单附件。
- 默认 `0.0.0.0:17890` 可被局域网访问：务必设置管理密码，生产环境建议防火墙只放行运维来源，或改为 `127.0.0.1` + SSH 隧道。
- 不要在不受信任的机器上长期保存正式环境 Token。
- 客户端仅服务授权私有云/私域场景，请遵守公司网络安全管理制度。

附录 A：推荐操作路径（最短上手）

1. 将 `hantu-client-linux` 安装到 `/usr/local/bin/`
2. `sudo hantu-client-linux run`（自动装服务后前台退出）
3. 浏览器打开 `http://127.0.0.1:17890/`
4. 首次设置本机管理密码并登录
5. 设置 → 填 API 地址与 Token → 保存
6. 打开「开机自动连接」（可选）
7. 点左侧链路图标连接
8. 在节点列表确认本机绿点、记下虚拟 IP
9. 用虚拟 IP 访问同空间设备
10. 不用组网时在 Web 点断开；停机维护时 `systemctl stop hantu-client`

附录 B：界面词汇对照

界面用语	含义
组网 Token / Network Token	加入某个虚拟组网空间的凭证
Hantu SD-WAN / <code>hantu0</code>	本机虚拟网卡 / 组网数据面
本机管理密码	保护 Linux Web 管理页，与管控账号无关
P2P 网络	点对点直连通道
汉土保障线路	保活与弱网兜底转发
汉土中继	中继转发通道
不走加密通道网段	指定流量绕过隧道（Linux 当前版本未开放）

附录 C：与 Windows 客户端差异速查

项目	Windows	Linux
日常入口	<code>hantu-admin.exe</code> 窗口 + 托盘	浏览器打开本机 Web
后台进程	HantuDaemon 服务	<code>systemd hantu-client</code>
虚拟网卡	Hantu SD-WAN	<code>hantu0</code>
关闭窗口	进托盘，程序仍在	关浏览器不影响组网
正式退出	托盘「退出应用」	<code>systemctl stop</code> 或 Web 断开 + 停服务
本机管理密码	无（本机 GUI 直开）	有（登录页）
阻断 / 移除节点	界面可操作	请用管控台
Bypass 直通网段	可用	当前版本未开放

如本手册与现场版本界面略有差异，以实际客户端界面与管理员最新通知为准。