

智眸现场接入指南

接入盒、云托管控制面、多盒互备：架构、部署、运维与接口

沅虹科技

版本 0.10 · 2026-10-07

目录

第 1 章 概述与架构	4
1.1 读者对象与范围	4
1.2 部署形态	4
1.3 系统组件	5
1.4 接入流程	6
1.5 安全边界	6
1.6 故障域	7
第 2 章 部署场景	8
2.1 形态选择	8
2.2 宽带要求	8
2.3 硬件配置	9
2.4 相机要求	9
2.5 多盒现场	9
第 3 章 部署全景	11
3.1 三层职责	11
3.2 平台的三类角色	11
3.3 租户开通的内容	12
3.4 现场开通的内容	12
3.5 本地化盒子的组成	12
第 4 章 安装与配置	14
4.1 租户开通	14
4.2 接入盒安装	14
4.3 预绑定	16
4.4 升级、回滚与卸载	16
4.5 安装包构建与发布	17
4.6 控制面部署	17
4.7 处理节点与中心部署	17
第 5 章 运维与排障	18
5.1 日志与状态位置	18
5.2 相机状态与原因	18
5.3 常见故障与根因	19
5.4 多盒现场运维	20
5.5 控制面版本更新	20
5.6 接入盒版本更新	20
第 6 章 接口与数据参考	22
6.1 鉴权方式	22

6.2 数据表 (sqlite, WAL)	22
6.3 配置版本与长轮询	23
6.4 运营侧 /v1/admin/	23
6.5 盒子侧 /v1/box/{id}/	23
6.6 租户侧 /v1/t/{tenant}/	23
6.7 节点侧 /v1/hub/{hub_id}/	24
6.8 密封格式 sealed_v1	24
6.9 中心接入页接口	25
附录 A 参数表	26
附录 B 容量与带宽	27
附录 C 勘查单	28
附录 D 相机调参 (海康)	29
附录 E 接入盒装机说明 (安装员)	30
附录 F 版本记录	31

第 1 章

概述与架构

1.1 读者对象与范围

智眸（UanVision）是智觉（UanSense）下的视觉神经，将现场相机画面转换为带证据的结构化事件。画面从相机到识别引擎之间的传输、鉴权、配置下发与故障处理，统称现场接入。本章说明现场接入的部署形态、系统组件、接入流程、安全边界与故障域；后续各章分别说明部署场景、部署全景、安装配置、运维排障与接口数据。

读者为沅虹交付与运维工程师，以及合作集成商的技术人员。客户管理员的日常操作见文档中心的智眸产品文档，不在本指南范围内。

本指南按部署与运维的顺序组织，内容以对应的软件版本为准，版本变化见附录 F。

1.2 部署形态

现场接入支持三种部署形态，按识别引擎所在位置区分。

形态	现场设备	检测位置	判定位置	画面是否离开场站
远程（云托管）	接入盒：双网口小型主机，仅负责拉流与推流	沅虹处理中心	沅虹处理中心（智悟与蓝精灵）	经加密通道传出
本地轻	带独立显卡的小型主机，内存 64 GB 起	现场本机	现场本机（蓝精灵放内存）或云端智悟	不离开
本地重	DGX Spark（64 GB 或 128 GB）	现场本机	现场本机	不离开

本版主要描述远程形态。远程形态涉及接入盒、控制面与处理节点三方协作，组件最多。本地两种形态的安装程序正在开发，完成后补充相应章节。

智眸的识别分两层。处理节点上的小模型完成检测、跟踪、区域与时序规则，直接给出入侵、烟火、安全帽、反光衣、车辆、异常光源等科目的结果；打架、倒地、攀爬等行为科目以及规则判断不清的事件，节点只组装候选（多帧蒙太奇、时间线、姿态），以“待判定”事件经虹元送到智悟，由智悟调用蓝精灵（沅虹在自有现场数据上微调的判定模型）给出最终结论与处置建议，结论回流后告警才成为正式科目。判定能力的位置决定部署形态：云托管由处理中心的智悟统一判定；本地形态要么在本机运行蓝精灵（硬件要求见第 2 章），要么在合同允许时把候选送云端智悟判定；完全断网的现场必须在本机运行蓝精灵。

候选在上行之前先经过处理节点上的行为时序门控。视频行为模型对攒帧窗口内的每个人框给出打架、倒下、攀登三类分数，三类分数都低于门限时该窗口不上行；其余情况一律上行，分数附在事件时间线上供智悟与复核人员参考。门限取真值集上三类全部召回的位置，缓冲

帧不足或模型不可用时门控放行。门控的作用是把大量正常走动的窗口挡在节点，判定本身仍由智悟完成。

1.3 系统组件

远程形态由接入控制面、接入盒代理、处理节点代理、智眸中心接入页四个服务组件和一个公共库构成。

接入控制面 uanlink 运行在公网入口主机上，由 nginx 反向代理为 link.uanhon.cn，负责接入码签发、盒子入网与心跳、相机清单下发、推流账号管理、口令密文中转、计量台账与审计。公网入口主机的资源有限，控制面的常驻内存控制在 100 MB 以内。

接入盒代理 uanbox-agent 运行在客户现场的接入盒上，完成入网、自检、相机发现、口令解密、本机 mediamtx 配置渲染、心跳上报与失败退避。

处理节点代理 uanhub-agent 运行在处理节点上，将推流账号同步到节点的 mediamtx，上报每路收到的字节数，并处理上行拥塞卸路与公网地址跟随。

智眸中心接入页由租户的中心实例提供，路径 /api/link/*，代客户管理员调用控制面的租户侧接口，管理员本人不接触租户钥匙。

智悟（UanMind）与蓝精灵不属于现场接入组件，但识别链路依赖它们：智眸中心把事件送入虹元，智悟取出待判定事件，用蓝精灵判定后把结论与处置写回虹元并回流智眸中心。

公共库 common 为上述组件提供签名、接入码、推流口令、密封格式与接口数据结构的统一实现，接口的字段定义以公共库为准。

组件之间的关系如下图所示。

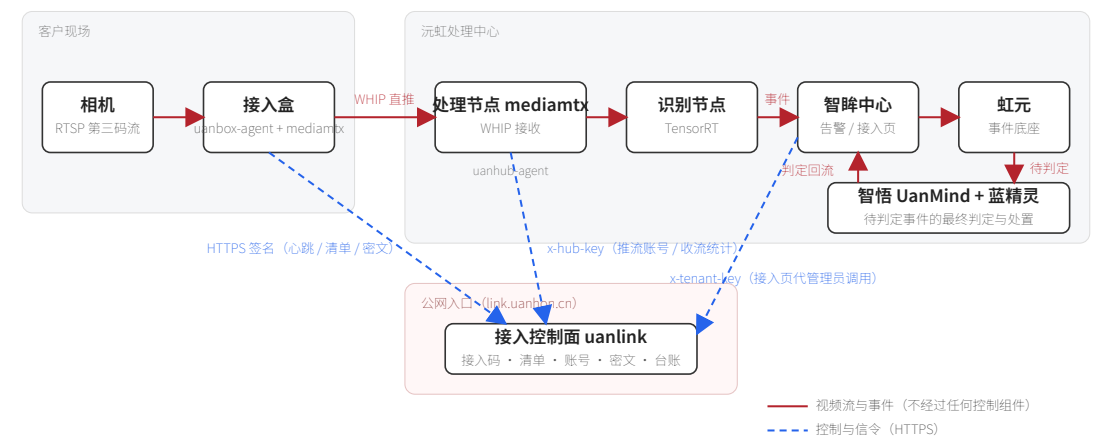


图 1-1 远程形态的组件关系：实线为视频流与事件，虚线为控制与信令，判定由智悟调用蓝精灵完成后回流

视频流不经过任何控制组件。接入盒上的 mediamtx 通过 WHIP 将每路画面直接推送到处理节点的 mediamtx，控制面只下发推送地址与账号。由此得到两条性质：控制面不可用时，正在推送的画面不受影响；控制面上不保存任何口令明文与画面。证据短片的回放同样不经过公网入口：中心返回处理节点上的按需路径，节点将短片转为一路临时流，浏览器以 WHIP 直连播放。

1.4 接入流程

步骤	执行者	位置	操作	系统行为
0	沅虹运营	运维主机	sense-tenant add <租户> <序号> 开通租户	处理节点建立网络命名空间与节点实例，中心实例生效并登记到入口网关；控制面建立租户，租户钥匙写入中心环境
1	沅虹运营	预绑定场所	盒子安装系统，接入页建立现场并生成接入码，uanbox-prebind <接入码> 入网，贴标签	盒子生成身份密钥（Ed25519）与密封密钥（P-256），绑定现场
2	安装员	现场	蓝口接宽带，黄口接相机交换机，通电	盒子联网、自检，每 60 秒在黄口发现相机，结果上报控制面
3	客户管理员	接入页	确认盒子在线、网络合格，发现的相机默认全选	中心每 10 秒从控制面拉取状态
4	客户管理员	接入页	填写账号口令并保存	浏览器用盒子公钥加密，控制面只存密文；盒子 1 秒内拉取、解密，每台相机以 RTSP 探测一次
5	客户管理员	接入页	点击”全部接入（n 台）”	控制面分配 cam01 至 camNN 并生成推流账号；盒子开始推送，节点接收；中心写入相机配置，节点 20 秒内建立通道
6	系统		每路转为在线并显示缩略图；异常的路显示原因	盒子心跳携带每路状态与原因

从设备到货到 30 路上线，现场操作仅为接线通电，管理员操作约 10 分钟。

1.5 安全边界

接入盒只主动出站：HTTPS 到 link.uanhon.cn，WHIP 到处理节点。盒子不向公网开放任何端口；黄口仅开放本地诊断页 8080、DHCP、对时以及相机发现的回包。

盒子身份在入网时由盒子自行生成 Ed25519 密钥对，此后每个请求携带 x-box-id、x-ts、x-sig，签名覆盖方法、路径、时间戳与请求体哈希。时间差超过 300 秒、同一时间戳同一签名重放、盒子状态非 active 的请求一律返回 401。

相机口令只在管理员浏览器内加密（P-256 ECDH、HKDF-SHA256、AES-256-GCM，格式 sealed_v1），密钥推导与附加数据均绑定 box_id|ip，密文更换盒子或 IP 后均无法解开。控制面、中心、日志与备份中只有密文。盒子本地 /etc/uanbox/cameras.secret（权限 600）中手工填写的条目优先于下发的条目。

推流账号按相机签发，账号为 p_<租户>_<相机>，口令为 32 字节随机值，数据库仅保存 mediamtx 可直接使用的 sha256 哈希，明文只在下发给盒子时出现一次。

租户隔离在处理节点上以系统用户、网络命名空间与独立存储实现，nftables 仅放行该租户需要到达的端口。智眸的入口域名是 vision.uanhon.cn，原入口 sense.uanhon.cn/app 并行保留，两者共用同一套租户路由，不为租户设子域；用户经门户（portal.uanhon.cn）登录，门户签票时确定租户，入口网关按租户码把页面与接口转到该租户的中心实例，中心兑换票据后种路由 cookie；控制面租户侧接口按 x-tenant-key 鉴权，其他租户的现场、盒子与相机一律按不存在返回 404。运营侧钥匙 x-admin-key 仅接受来自本机回环或 nginx / v1/admin/ 前缀（来源 IP 白名单）的请求。

1.6 故障域

一路画面从相机到事件经过五个环节。各环节的故障表现与应对方式如下，多盒互备的设计以此为出发点。

环节	故障表现	单盒现场	双盒现场
相机与相机交换机	相机掉电、交换机故障	无法应对，属客户设备	同左。交换机为单点，勘查时向客户说明
接入盒	掉电、硬盘故障	该盒全部相机停止	另一台盒子在失联判定后接管其相机
现场上行	断网、带宽占满	占满时节点卸路；断网全部停止	两台盒子各接一条宽带，一条中断由另一条承担
处理节点	宕机、机房断网	全部云托管租户停止	同左，节点级互备在后续阶段
控制面	服务不可用	盒子按最后配置继续推送，配置不可更改	同左

第 2 章

部署场景

2.1 形态选择

现场具备商业宽带或专线，且客户不限制画面离开场站时，采用远程形态。接入盒成本最低，安装最简单，故障时整机更换。合同约定画面不得离开场站，或现场仅有家庭宽带时，采用本地形态：30 路以内为本地轻，超过 30 路为本地重。条件不明确时，先按勘查单确认宽带与相机情况再做选择。

三种形态共用的部分：相机均按第三码流 H.264、1280×720、8 帧配置；客户管理员均在接入页操作；告警、视频墙与统计功能无差别。

判定能力的位置随形态变化：云托管由处理中心的智悟统一判定，现场不承担判定算力；本地形态需要在本机运行蓝精灵，或在合同允许候选数据（蒙太奇、姿态，不含连续画面）出场站时送云端智悟判定。本地轻的内存要求（64 GB 起）即来自在本机运行蓝精灵。

2.2 宽带要求

上行带宽按每路约 1 Mbps 计算（第三码流定码率 768 Kbps 加传输开销），30 路需要 40 Mbps 以上，并且需要持续可用。家庭宽带的上行通常为 20 至 30 Mbps，可接 15 路以内；更多路数需要商业宽带。

控制面能够判断两项网络条件：盒子自检上报的公网出口类型（锥形 NAT 可直连，对称 NAT 需依赖节点宣告的固定端口），以及同一现场两台盒子是否共用同一出口（出口相同时不构成冗余）。电源条件无法远程判断，依赖勘查登记。

自检项	检测方法	判定
时钟偏差	与 HTTPS 响应头的 Date 比较	超过 300 秒时签名被拒；安装 chrony 后不会出现
HTTPS 连通	连接 link.uanhon.cn	不通则无法入网
UDP 与 NAT 类型	同一 socket 向两个 STUN 服务器各探测一次，映射端口一致记为 eim（锥形）	锥形可直连；对称 NAT 依赖节点的固定端口宣告
IPv6	是否有全球单播地址、能否连接 2400:3200::1 的 53 端口	具备 IPv6 的现场直连成功率最高
相机网段	黄口是否有链路、能否发现设备	未接相机时记”尚未配置相机”

运营商级 NAT 的现场需要注意：地址池中每条映射可能分到不同的公网 IP。盒子连续两次读到同一个新地址才判定为出口变更，避免每个心跳周期误判一次。

2.3 硬件配置

接入盒：x86 小型主机（N100 级别），两个千兆网口，8 GB 内存，64 GB 以上硬盘（盒子不存储视频），Debian 12，功耗约 10 W。arm64 主机同样支持（安装包提供 aarch64 版本），出厂预装仅提供 x86。安装位置为弱电箱或机柜，环境温度 0 至 40 °C，防雨。

本地轻：NVIDIA 桌面显卡，显存 8 GB 起；内存 64 GB 起（判定模型与摘要模型各 20 GB 以上，专家权重放内存、注意力层放显卡）；2 TB NVMe；Ubuntu 24.04；20 至 30 路；安装于值班室或机房。

本地重：DGX Spark 64 GB 或 128 GB，2 TB 以上存储，出厂 DGX OS，50 路以上。

本地两种形态均为桌面级设备，不是宽温工控机。户外机柜或高温车间需要另选工控整机。

2.4 相机要求

支持海康、大华等主流品牌，相机需提供 H.264 的第三码流或子码流。配置要点如下，详细步骤见附录 D。

- 地址固定为 192.168.88.11 至 .99，网关与对时地址 192.168.88.1，一台一个地址。
- 预览账号单独创建，仅授予”远程预览”权限，口令全站统一并交给客户管理员。管理员口令不交给沅虹。
- 第三码流 H.264、1280×720、定码率 768 Kbps、8 帧、I 帧间隔 16、关闭 H.264+ 与 SVC。没有第三码流的型号改用子码流，主码流保持不变。
- 相机接入同一台相机交换机，不接在录像机的供电口上；使用录像机时，录像机同样接入该交换机。

接入盒的码流核对规则：ffprobe 抽取 4 秒，判定 H.264、是否含 B 帧（按帧类型判定，不依赖 has_b_frames 标志）、分辨率 640×360 至 1280×720、帧率 6 至 15。选流规则：有第三码流（通道 103）用第三码流，否则用子码流（通道 102），不自动选择主码流；NVR 通道默认取 x02。不合格的路不推送，原因上报并在接入页显示。

2.5 多盒现场

多盒现场指同一现场两台接入盒接入同一台相机交换机，分别使用两条宽带，电源为两个独立回路或配备 UPS。

- 相机登记在首选盒子，实际由哪台盒子推送由控制面决定。盒子失联达到在线判定时限后，其名下相机交给同现场中能够发现该相机（发现清单含该 IP）且已持有其口令密文的在线盒子，名下路数少的优先。首选盒子恢复并稳定 10 分钟后，相机交还首选盒子；现场可关闭自动回切。
- 两台盒子的黄口分别为 192.168.88.2 与 .3，仅 1 号盒子给相机分配地址；192.168.88.1 由 keepalived 在两台之间浮动，相机的网关与对时地址仍为 .1，相机侧无需改动。
- 管理员保存口令时，同一台相机的口令为现场内每台盒子各封一份密文。后加入的盒子需要再保存一次口令；控制面在盒子取得密文之前不会向其分配相机。
- 接入页提供”演练切换”：将一台盒子按离线对待 10 分钟，相机当场交给另一台，演练结束当场切回。验收时建议当着客户执行一次。
- 单台盒子承担全部相机时上行可能不足，节点侧的卸路逻辑会自动生效。双盒现场勘查时要求单条宽带至少能承载一半以上的路数。

切换时间指标：失联判定 90 秒加巡检周期 30 秒以内完成接管；接管后约 5 秒恢复推送；首选盒子恢复后 10 分钟稳定期结束回切；演练切换与结束均即时生效。

处理节点级互备（双处理节点，租户在两个节点各开实例）属后续阶段，前提是处理中心的电源与出网独立。

第3章

部署全景

本章说明云托管形态下智眸由哪些部分组成、各部分承担什么职责，并区分三类工作：平台的一次性工作、每开通一个租户的工作、每个现场的工作。租户与现场两层的工作均已压缩为一条命令。

3.1 三层职责

层	频次	执行方式
平台	一次，长期运维	沅虹运营负责，交付人员无需操作
租户（一个客户单位）	每个客户一次	sense-tenant add <租户> <序号> 一条命令，外加门户登记
现场（一个工地或场站）	每个现场一次	接入盒一条命令，相机在接入页点击”全部接入”
本地化盒子（客户自有机器）	每台一次	一条命令加一个激活码

3.2 平台的三类角色

平台按职责分为公网入口、处理节点与中心三类角色。三类角色的组件如下。

公网入口

组件	职责
网关	全部公网域名的入口：vision.uanhon.cn 与 sense.uanhon.cn/app（按租户将请求转到对应中心实例）、link.uanhon.cn（接入控制面）、ingest.uanhon.cn（推流信令）
uanlink	接入控制面：接入码、盒子入网与心跳、相机清单、推流账号、口令密文中转、计量与审计
身份服务	用户身份与单点登录，各产品共用

公网入口只承载信令与读取类数据。视频推流与短片回放均在浏览器、接入盒与处理节点之间直连，公网入口只交换连接参数。

处理节点

组件	职责	说明
GPU 推理运行时	推理	节点启动时按模型构建 TensorRT FP16 引擎并缓存；更换显卡后重建

组件	职责	说明
mediamtx	接收接入盒推流；视频墙与回放路径	按来源地址限制每个租户只能读取自己的流
uanhub-agent	同步推流账号、上报收流字节、拥塞时卸路、公网地址跟随	规格见第 6 章
uansense-node@<租户>	每个租户一个识别节点实例	独立系统用户、网络命名空间与存储，由 sense-tenant 创建
共享环境 /opt/uansense	Python 环境与模型	各租户实例只读引用
nftables	租户之间、租户与宿主之间的网络隔离	按租户目录重建

中心

组件	职责
uansense@<租户>	每个租户一个中心实例：告警、工作台、接入页；独立端口、会话密钥、随机管理员口令、租户钥匙，只接受本租户的门户票
数据目录挂载	读取处理节点上该租户的证据与短片
虹元、智悟	中心把事件送虹元，智悟取事件判定并回写

门户：租户、应用开通、成员与授权。智眸单点登录依赖门户签票。

3.3 租户开通的内容

sense-tenant add <租户> <序号> 在三类角色上执行十余步，明细见第 4 章”租户开通”一节。处理节点上建立独立的用户、命名空间、存储、节点实例、防火墙规则、数据目录导出、mediamtx 读权限与回放地址表；中心上建立中心实例；网关的三张路由表各增加一行；控制面建立租户并取得租户钥匙。序号决定全部端口与网段，分配后不再复用。

门户登记（登记租户、开通智眸应用、绑定管理员账号）目前单独执行，计划并入开通脚本。

3.4 现场开通的内容

接入盒执行 `curl -fsSL https://dl.uanhon.cn/box/get.sh | sudo bash -s -- --router`，重启后执行 `uanbox-prebind <接入码>`。此后盒子自动发现相机，管理员在接入页填写一次相机口令并点击”全部接入”。双盒互备在安装时增加 `--ha 1` 或 `--ha 2`。

3.5 本地化盒子的组成

客户自有机器上运行智眸时，平台中的多数组件不再需要：

不需要的组件	原因
公网会合与转发	盒子在客户内网，浏览器直接访问其地址
网关路由表、推流信令中转	单租户，没有多实例路由；相机以 RTSP 直接拉取
网络命名空间、数据目录挂载、按租户的 nftables	单租户

不需要的组件	原因
回放直连	浏览器与盒子在同一内网，直接传输文件
门户单点登录	可选，以本地账号为主

本地化盒子由识别节点、中心、mediamtx、nginx 四个容器加一个数据卷组成。首次启动按显卡构建 TensorRT 引擎并缓存，激活码换取许可文件。需要本地判定的现场另加智悟与蓝精灵推理两个容器，蓝精灵权重（量化后约 22 GB）随安装介质预装，不经公网下载。安装程序负责识别硬件、生成环境配置、启动容器与执行自检。

第 4 章

安装与配置

4.1 租户开通

租户开通由沅虹运营执行 `sense-tenant`，脚本编排处理节点、中心与公网入口三类角色：

```
sense-tenant add <租户> <序号n> [--name 名称] [--workers 2] [--disk 500G] [--rotate-link-key] [--dry-run]
sense-tenant status <租户> <序号n>
sense-tenant remove <租户> <序号n> --yes
```

序号 n (1 至 19) 决定全部编号：uid=2000+n，网段 10.90.n.0/30（节点在 .2），中心端口 8090+n，视频墙端口 5060+n。序号分配后不再复用。每台机器上的动作先判断再执行，同一租户重复执行结果一致。

脚本在各角色上的动作：

角色	动作
处理节点	系统用户 <code>sense-<租户></code> 、网络命名空间（一对 veth）、XFS 存储镜像、模板单元 <code>uansense-node@<租户></code> 、NFS 导出给中心、mediamtx 按来源地址限制该租户只读自己的流、nftables 仅放行必要端口、回放地址表 <code>/etc/uansense/centers.map</code> 增加一行
中心	同名同 uid 用户、模板单元 <code>uansense@<租户></code> （独立端口、会话密钥、只认本租户门户票、随机管理员口令）、NFS 挂载节点数据目录、公网入口到该实例的转发
公网入口	在入口网关的三张 map（接口上游、视频墙路径、前端目录， <code>vision.uanhon.cn</code> 与 <code>sense.uanhon.cn</code> 共用）各登记一行；不建子域、不签证书
控制面	执行环境中存在 <code>UANLINK_ADMIN_KEY</code> 时建立租户、取得租户钥匙并写入中心环境（ <code>UANLINK_TENANT_KEY</code> ）；不存在时提示并跳过

控制面地址分为两个变量：脚本自身调用控制面使用 `UANLINK_URL`；写入中心环境的地址必须是中心可达的地址（`SENSE_LINK_URL_CENTER`，缺省 `https://link.uanhon.cn`），给出回环地址时脚本拒绝执行。

节点共享目录 `/opt/uansense`（Python 环境与模型）为只读共享，租户代码树中的 `models` 以软链指向它。脚本先移走代码树中原有的 `models` 目录再建立软链，避免软链建到目录内部导致模型无法加载。

4.2 接入盒安装

安装包发布在下载站 <https://dl.uanhon.cn/box/>：get.sh 引导脚本、latest 当前版本号、<版本>/ 目录下两个架构的安装包、install.sh、SHA256SUMS。

双网口盒子（蓝口宽带、黄口相机），安装后需重启

```
curl -fsSL https://dl.uanhon.cn/box/get.sh | sudo bash -s -- --router  
sudo reboot  
sudo uanbox-prebind <接入码>
```

单网口主机，安装后直接入网

```
curl -fsSL https://dl.uanhon.cn/box/get.sh | sudo bash -s -- --code <接入码>
```

两台盒子接同一台相机交换机互备：另一台使用 --ha 2

```
curl -fsSL https://dl.uanhon.cn/box/get.sh | sudo bash -s -- --router --ha 1
```

get.sh 按机器架构获取 latest 与 SHA256SUMS，核对 install.sh 与安装包的哈希后交给 install.sh。除 --code 与 --base（更换下载站）外的参数原样透传。

install.sh 参数：

参数	用途	
--bundle <目录或 tar.gz> / --url <地址> --sha256 <值>	包来源；均未指定时，脚本所在目录若为解开的安装包则直接使用	
--link <地址>	控制面地址，缺省 link.uanhon.cn；已有 agent.env 时不改	
--router	双网口：WAN 口自动获取地址，LAN 口固定 192.168.88.1/24 并给相机分配地址，不转发。重启后生效	
--wan / --lan	网口名不是 enp1s0 / enp2s0 时指定	
--ha 1 2	两盒互备：黄口 .2 / .3，仅 1 号分配地址，.1 由 keepalived 浮动（VRRP 组 88，1 号优先级 150，回抢延迟 30 秒），防火墙放行 VRRP	
--pppoe <账号>	光猫桥接需要拨号。口令按提示输入或经环境变量 UANBOX_PPP0E_PASS 传入，不进入命令行	
--ssh-wan / --ssh-lan	防火墙缺省不放行 SSH；远程维护加前者，技术员现场接黄口维护加后者	
--no-apt	离线镜像已装 chrony、ffmpeg 时跳过系统包安装	
--reset-machine-id	制作出厂镜像克隆前必须指定（见下）	
--any-distro	发行版不在 Debian 12+ / Ubuntu 22.04+ 范围时仍安装，仅用于测试机，通常与 --no-apt 同用	
--dry-run / --uninstall / --purge / --root <假根>	演示、卸载、连身份一起删除、测试用假根	

安装内容：

路径	说明
/opt/uanbox/versions/<版本>/ 与 current 软链	两个二进制、install.sh、prebind.sh、MANIFEST；升级进入新目录后原子切换，旧版本保留
/usr/local/sbin/uanbox-prebind	指向 current/prebind.sh
/etc/uanbox/agent.env (600)	UANBOX_LINK、UANBOX_STATE、UANBOX_CAMERA_SECRETS、UANBOX_MEDIAMTX_YML、UANBOX_MEDIAMTX_API、RUST_LOG
/etc/uanbox/cameras.secret (600)	相机口令，每行 IP 账号 口令；手工填写的优先于接入页下发的
/etc/uanbox/mediamtx.yml (600)	首次为空配置，之后由代理整份覆盖
/var/lib/uanbox/ (700)	身份 (box.key、seal.key、state.json)、下发配置、记账、标签、备份
uanbox-mediatrix.service、 uanbox-agent.service	Restart=always，代理在 mediamtx 之后启动
/etc/chrony/conf.d/ uanbox.conf	国内公共 NTP；--router 时允许黄口网段对时

--router 另外写入 systemd-networkd 的两个 .network、/etc/sysctl.d/90-uanbox.conf (关闭转发)、/etc/uanbox/firewall.nft (仅管理 inet uanbox 一张表) 以及拨号时的 ppp 配置。修改前的原文件备份到 /var/lib/uanbox/backup-<时间>/。

制作出厂镜像必须指定 --reset-machine-id。硬件指纹为 machine-id 与物理网卡 MAC 的哈希，克隆镜像的盒子指纹相同，第二台入网会被控制面拒绝（“这台机器已有在用的盒子”）。母机清除后不再执行预绑定。

4.3 预绑定

预绑定在沅虹办公场所完成。前提：盒子已安装（双网口带 --router 并已重启），蓝口可上网。接入码在接入页”生成接入码”获取，24 小时有效、仅可使用一次。

```
sudo uanbox-prebind ABCD-EFGH-JKLM      # 入网、显示自检判定、启动两个单元、打印标签
sudo uanbox-prebind --label              # 重印标签
```

预绑定场所的自检结论不代表现场，盒子到现场更换宽带后会重新自检。已入网的盒子会被拒绝：先在控制面吊销，待盒子收到吊销并自行标记后，再预绑定。不要直接删除 /var/lib/uanbox：控制面旧记录仍在，相同硬件指纹会被拒绝（409），旧记录也无法正常停用。

4.4 升级、回滚与卸载

升级：再次执行安装命令（或 install.sh --bundle <新包>）。回滚：

```
ls /opt/uanbox/versions/
sudo ln -sf versions/<旧版本> /opt/uanbox/.current.new && sudo mv -T /opt/
uanbox/.current.new /opt/uanbox/current
sudo systemctl restart uanbox-mediatrix uanbox-agent
```

身份与口令文件不随版本变动，回滚无需重新入网。卸载 `install.sh --uninstall` 保留身份与口令，`--purge` 连身份一起删除（控制面上的记录由运营吊销）。网口配置在卸载时保留，避免卸载过程中断开自身网络。

4.5 安装包构建与发布

```
# 构建主机上执行；mediamtx 使用官方 v1.21.1 发布包
MEDIAMTX_TAR=<x86_64 包路径> MEDIAMTX_TAR_AARCH64=<aarch64 包路径> deploy/box/make-
bundle.sh --arch all
deploy/box/publish.sh # 上传到公网入口，切换 latest，从公网回读 Content-
Length 核对
```

版本号 <Cargo 版本>-g<提交号>，工作区有未提交改动时带 `.dirty`，`publish.sh` 拒绝发布 `dirty` 版本。下载站的 `nginx` 配置不得引入扫描器拦截片段，该片段会拦截全部 `.tar.gz` 请求。

4.6 控制面部署

二进制 `/opt/uanlink/uanlink` (`musl` 静态链接，`cargo build --release --target x86_64-unknown-linux-musl -p uanlink`)，环境文件 `/etc/uanlink.env` (`UANLINK_ADMIN_KEY`、`UANLINK_INGEST_HOST`、`UANLINK_DB`、`UANLINK_BIND`)，数据库 `/var/lib/uanlink/uanlink.db` (`sqlite WAL`，权限 600，含推流口令明文)，单元 `uanlink.service`。

版本更新：备份二进制与数据库，新二进制先复制到 `/tmp` 再 `mv` 替换，`systemctl restart uanlink`，检查 `GET /v1/admin/hubs` 返回 200 且盒子心跳正常。数据库在启动时自动补列建表，旧版本不读取新列，回滚无需处理数据库。

`nginx conf.d/link.conf`：`/v1/box/` 与 `/v1/t/` 的 `client_max_body_size 2m`，`/v1/t/` 仅放行中心主机的出口 IP（出口变更时同步修改），`/v1/admin/` 按来源白名单放行。

4.7 处理节点与中心部署

节点代理 `uanhub-agent` 在处理节点本机编译，`x-hub-key` 每个节点一把。它将 `p_` 开头的推流账号整段替换进 `/opt/mediamtx/mediamtx.yml` 的 `authInternalUsers`（本机与视频墙固定条目不动），先写临时文件再改名，两次写入至少间隔 1.2 秒，写入后通过 `/v3/config/global/get` 核对。

节点侧三项自动机制：公网地址跟随（每 15 秒 STUN，连续两次得到同一新地址即更新 `webrtcAdditionalHosts`，`UANHUB_PUBLIC_HOSTS=off` 关闭）；上行拥塞卸路（每 10 秒按现场汇总丢包，连续 3 个窗口不低于 5% 判定拥塞，卸载到测得容量的一半，恢复需连续 3 个窗口低于 1%，`UANHUB_SHED=off` 关闭）；配置检查（出现 `turn:` 或非中国大陆地址时拒绝写入）。

回放直连依赖处理节点上的两项配置：`/opt/uansense/bin/clip-stream`（按需转码脚本）与 `/etc/uansense/centers.map`（租户到中心地址的映射，每行 <租户> `http://<中心地址>:<端口>`）；`mediamtx` 的路径模板与匿名读权限由 `deploy/cloud/mediamtx-clip-path.py` 幂等写入。

中心接入页的后端为 `console/link_api.py`，环境变量位于 `env.d/center`：`UANLINK_URL`、`UANLINK_TENANT_KEY`、`UANLINK_TENANT`、`SENSE_INGEST_RTSP`、`UANLINK_HUB_NAME`。未配置租户钥匙时接入页不开通，`/api/link/*` 一律返回 503。

第 5 章

运维与排障

5.1 日志与状态位置

位置	内容
接入盒	journalctl -u uanbox-agent -u uanbox-mediatrix -f; /opt/uanbox/current/uanbox-agent probe 执行一次自检; 黄口接电脑访问 http://192.168.88.1:8080 本地诊断页 (只读: 状态、相机、自检逐项、日志尾部, 口令遮蔽)
控制面	journalctl -u uanlink; 数据库 sqlite3 /var/lib/uanlink/uanlink.db (权限 600, root); nginx 访问日志中 link.uanhon.cn 的记录
处理节点	journalctl -u uanhub-agent、journalctl -u uansense-node@<租户>; mediatrix API /v3/paths/list、/v3/webtrcsessions/list
中心	journalctl -u uansense@<租户>; 中心审计表 audit_log 中 link_* 动作。中心管理员账号为 admin, 口令在开通时随机生成, 保存于中心主机 /srv/sense/<租户>/env.d/admin.pass (root 可读)
接入页	页面顶部红色提示表示中心无法连接控制面; 相机行黄色提示可展开查看原因; “上送记录”显示每路本月字节数以及口令填写与暂停操作记录

控制面审计 (租户侧 GET audit) 记录每一笔写操作, 操作人为中心登录名; 指纹、来源 IP 与密文一律不记录。接管与回切的操作人记为 system:failover。

5.2 相机状态与原因

盒子心跳对每路携带 state (online / checking / connecting / shed / backoff / paused / failed)、cred (ok / bad / none / untested)、err、codec、bframes、chosen_stream、fps。接入页按下表显示:

原因	页面提示	处理方法
黄口未发现设备	黄口那边没有找到相机	确认相机交换机通电、网线接在黄口、相机指示灯亮; 20 秒后自动重新发现
相机 RTSP 不通	相机能看到但连不上视频口	等待数分钟; 持续不通时重启该相机
同 IP 多个 MAC	有两台相机用了同一个地址	由相机安装方修改其中一台的地址
未激活	有几台相机还没设过密码	先激活

原因	页面提示	处理方法
cred none	还没有这台相机的口令	在口令框填写一次
cred bad	口令和填的不一样	单独为该相机填写。盒子只尝试一次，避免相机因多次口令错误锁定；填写正确后点击”重新检查”
H.265	视频格式是 H.265	第三码流改为 H.264
B 帧 / H.264+	开了 B 帧或 H.264+	关闭 H.264+
no_third	第三码流没开	相机网页 系统维护 > 系统服务 启用第三码流后重启；或点击”改用子码流”
res_out / fps_out	分辨率或帧率不合适	设为 1280×720、8 帧
shed	这条宽带暂时带不动这么多路	无需处理，带宽空闲后自动恢复；频繁出现时增加上行带宽
backoff	断线重连中	超过 15 分钟仍未恢复时检查现场网络
paused	已暂停上送	由操作者暂停，需要时恢复
指纹冲突	盒子的身份在两台机器上出现	已自动挂起，联系沅虹（常见原因是克隆镜像未清除 machine-id）

5.3 常见故障与根因

盒子在线但没有任何一路推送。 查看盒子日志是否出现”拉口令密文 HTTP 401”：盒子状态不是 active（已挂起或吊销）。再检查 `cameras.secret` 是否包含该相机：手工填写的条目优先，接入页下发的只补充缺失项。

盒子在推送但节点收不到。 查看 `uanhub-agent` 日志中的候选对类型：出现 relay 时立即记录 error（系统不使用 TURN）。对称 NAT 后的盒子只能连接节点宣告的固定端口 公网 IP:8189，检查节点的公网地址跟随是否正常（`webrtcAdditionalHosts`）。推流地址必须将账号口令写入 URL 以 Basic 方式鉴权，`mediamtx` 的 `whipBearerToken` 与内置账号鉴权不兼容。

签名被拒。 盒子时间偏差超过 300 秒：`chrony` 未运行（安装脚本结尾会提示）。同一秒内同一请求的签名相同会被判为重放，自动化脚本需间隔 1.1 秒以上。

出口 IP 变更后盒子不重连。 自检中的 STUN 与 HTTPS 一旦恢复即清零全部退避；出口 IP 变更同样清零，但需要连续两次读到同一新地址（运营商级 NAT 的地址池）。

第二台盒子入网被拒：“这台机器已有在用的盒子”。 硬件指纹相同：克隆镜像时未指定 `--reset-machine-id`。同一台主机运行第二个盒子实例做测试时，用 `UANBOX_MACHINE_ID_FILE` 指向另一份 `machine-id`。

保存口令后相机从”在线”变为”口令不对”并停止推送。 接入页口令框填写的是相机的预览账号，不是中心登录账号；盒子对新口令只尝试一次，不正确即停止推送并报 `cred_bad`，重新保存正确口令后恢复。

无法进入某个租户的中心。 入口是 `vision.uanhon.cn`（`sense.uanhon.cn/app` 并行保留），租户由门户签票决定；门户主库中需要存在该租户、已开通智眸应用、用户为成员且已授权，缺一项门户不签票。运维排障时可访问 `https://vision.uanhon.cn/app/t/<租户>` 种下路由由 cookie 后用本地 admin 登录，`/app/t/-` 清除。

中心接入页整页 503。中心环境缺少 UANLINK_TENANT_KEY, 或写入中心环境的控制面地址是中心不可达的地址 (应为 `https://link.uanhon.cn`)。

租户钥匙错误 5 次锁定 15 分钟。按 (来源 IP, 租户码) 计数, 一个中心配错钥匙不会锁住经同一出口的其他租户。钥匙正确即放行, 不受锁定影响。

节点未加载任何模型。models 软链建到了目录内部 (models/models)。执行 `ls -la /srv/sense/<租户>/app/models` 确认软链指向 `/opt/uansense/models`。

下载站安装包无法下载, 其他文件正常。nginx 配置引入了扫描器拦截片段, 该片段对 .tar.gz 请求一律返回 444; 下载站配置不得引入。

回放显示”文件回放 (经服务器)“。直连未在 20 秒内建立, 前端已退回 HTTP 文件方式。查看处理节点 mediamtx 日志中 `clip_<租户>_<告警号>` 路径: 无 `runOnDemand command started` 表示 WHEP 请求未到达节点 (检查入口网关 /whep/ 转发); 有启动但无 `stream is available` 表示节点无法从中心取得短片 (检查 `centers.map` 与中心 `/api/clip/<id>?t=` 可达性); 有 `peer connection established` 但立即关闭表示浏览器侧超时或页面切换。

5.4 多盒现场运维

- 接入页现场卡片的”冗余”状态: 有效 (两台以上在线且出口不同)、同一条宽带、仅 n 台在线、单盒、待自检。出口取控制面看到的来源地址, 缺失时取自检中 STUN 测得的地址。
- 失联达到在线判定时限后接管, 首选盒子恢复并稳定 600 秒后回切, 巡检每 30 秒一轮。接管需同时满足三个条件: 同现场在线、发现清单含该相机 IP、持有该相机 IP 的密文。未接管的常见原因是后加入的盒子未保存过口令, 由管理员再保存一次即可。
- 两台盒子不会同时推送同一路: 推流账号按相机签发, 节点 mediamtx 只接受先到的发布者, 旧盒子在取得新清单之前会被拒绝, 取得清单后停止。
- --ha 现场: `ip addr show <黄口>` 查看 .1 当前所在的盒子, `journalctl -u keepalived` 查看切换记录; 1 号恢复 30 秒后收回 .1。
- 演练切换 10 分钟到期自动切回; 人工”结束演练”当场切回, 不等待稳定期也不受回切开关影响。
- 吊销正在代推的盒子时, 其代推的相机退回各自的首选盒子; 该盒子自己首选的相机口令作废, 需要重新登记。

5.5 控制面版本更新

1. 构建 musl 静态二进制, 备份 `/opt/uanlink/uanlink` 与 `/var/lib/uanlink/uanlink.db`。
2. 新二进制复制到 /tmp 后 mv 替换, `systemctl restart uanlink`, 日志出现”已监听”。
3. `GET /v1/admin/hubs` 返回 200; 数据库中 `box.last_seen_at` 在 90 秒内刷新 (盒子心跳正常)。
4. 数据库自动补列, 旧版本不读新列, 回滚只需替换二进制。
5. 在运维台账记录发版: 每一步的操作、回滚方法、未在线上验证的项。

5.6 接入盒版本更新

1. `make-bundle.sh --arch all` 构建, `publish.sh` 发布 (dirty 工作区拒绝发布, 发布后回读大小核对)。

2. 现场再次执行安装命令，或 `install.sh --bundle <新包>`；新版本进入独立目录后原子切换。
3. 盒子心跳携带 `agent_version`，接入页盒子卡片可见；旧版本保留，回滚时改软链并重启两个单元。

第 6 章

接口与数据参考

接口与数据表的完整定义见 [uanlink/SPEC.md](#)，本章为其摘要与说明。名字与格式：租户码 `^[a-z][a-z0-9]{1,30}$`；相机名 `camNN`（两位补零，过 99 三位）；推流路径 `t_<租户>/<相机>`；推流账号 `p_<租户>_<相机>`；盒子 id `bx_` 加 26 位 ULID；时间 RFC3339 UTC。

6.1 鉴权方式

主体	凭据	说明
运营	x-admin-key	等于 UANLINK_ADMIN_KEY，只从 127.0.0.1 或 nginx 白名单进
盒子	x-box-id、x-ts、x-sig	Ed25519 对 METHOD\PATH_AND_QUERY\nts\nhex(sha256(body)) 签名；时间差 300 秒内；同 ts 同签名 300 秒内重放 401
租户	x-tenant-key	sha256 后与租户 key_hash 常数时间比较；错 5 次按（IP，租户码）锁 15 分钟；别的租户的钥匙 403；中心代调带 x-uanlink-actor-user 进审计
节点	x-hub-key	每个节点一把，库存哈希

6.2 数据表 (sqlite, WAL)

```
tenant(code PK, name, hub_id, state, cfg_rev, key_hash, created_at)
hub(hub_id PK, key_hash, signal_port, public_v4, public_v6, capacity_streams,
udp_open, shed_json, cfg_rev, updated_at)
site(site_id PK, tenant, name, failback, created_at)
join_code(code_hash PK, site_id, expires_at, used_at, used_by_box, fail_count,
locked_until, created_by, created_at)
box(box_id PK, tenant, site_id, pubkey_b64, hw_fingerprint, state[active|
suspended|revoked], cfg_rev, last_seen_at, last_ip,
    agent_version, probe_json, name, paused, seal_pub, secrets_rev,
secrets_rev_applied, discovery_at, up_since, drill_until, created_at)
camera(tenant, cam, box_id, assigned_box, site_id, source_kind[rtsp_url|
nvr_channel], source_ref, stream_role, publish_user, publish_hash,
    state[enabled|paused|removed], name, created_at, updated_at, PK(tenant,
cam))
camera_secret(tenant, cam, secret) -- 推流口令明文，只在这里
discovery(box_id, ip, mac, json, seen_at, PK(box_id, ip, mac))
box_secret(box_id, ip, sealed, rev, updated_at, PK(box_id, ip))
box_action(box_id, kind, created_at, PK(box_id, kind))
ledger_hour(tenant, cam, hour, hub_bytes, box_bytes, sessions, reconnects,
pair_kind, PK(tenant, cam, hour))
audit(id PK, at, actor, action, object, detail_json)
```

字段说明：box_id 是登记时的首选盒子，assigned_box 是当前实际推送的盒子；source_ref 只是 ip 或 ip/通道，带 @ 的一律拒；box.paused 是租户按的”停止上送”；up_since 只在心跳从离线变在线时写；老库启动时 add_column 幂等补列。

6.3 配置版本与长轮询

db::bump(tenant, boxes, hubs): 租户版本加一，受影响的盒子取这个版本，受影响的节点各自加一，回要唤醒的键 b:<盒子> / h:<节点>。提交事务后 App::notify 用 tokio::sync::watch 叫醒挂着的长轮询（最多 25 秒，停机时立刻回 304）。盒子 GET config?rev= 与节点 GET publishers?rev= 版本没变就挂着等。

6.4 运营侧 /v1/admin/

建改节点 PUT hubs/{h} (回 hub_key 一次)、建改租户 PUT tenants/{t} (新建回 tenant_key 一次, ?rotate_key=1 轮换)、建现场、发接入码、登记相机、吊销盒子 POST boxes/{b}/revoke、台账 GET ledger、nginx 映射渲染。

6.5 盒子侧 /v1/box/{id}/

方法与路径	要点
POST /v1/join	接入码、公钥、硬件指纹、可选 seal_pub_b64；接入码一次性、24 小时、错 5 次按 IP 锁 15 分钟
POST probe	自检结果：时钟、HTTPS、UDP 与 NAT 类型、IPv6、相机网段；返回判定 (ready_v4 / ready_v6 / blocked 等) 与面向网络负责人的说明文字
POST heartbeat	30 秒一次；每路 state / cred / err / codec / bframes / chosen_stream / fps；seal_pub_b64 每次都带；secrets_rev 已应用版本；hw_fingerprint 90 秒内换了就挂起。回 cfg_rev 与 actions (reload、discover、probe、recheck、revoke)
GET config?rev=	BoxConfig {cfg_rev, cameras[{cam, path, publish_url, source_kind, source_ref, stream_role, state}], paused, secrets_rev}; state 取 enabled / paused / shed / removed；租户停用时全部 paused
POST discovery	整份覆盖，最多 256 台，同 ip 不同 mac 两条都留
GET secrets	只回本盒子的 {rev, items[{ip, sealed}]}
POST ledger	每路发出的字节，小时差分

盒子收到配置后的动作：state=paused/shed 不推不重试；removed 从配置里拿掉；某路连续 60 秒没建连退避 60 / 300 / 900 秒；收到 revoke 删令牌与 box.key、清空推流、退出不再自启。

6.6 租户侧 /v1/t/{tenant}/

方法与路径	要点		
GET sites / POST sites / POST sites/{s}/join-codes	现场与接入码；GET sites 带 fallback		
PUT sites/{s}/fallback {enabled}	现场回切开关		

方法与路径	要点		
PUT sites/{s}/secrets {items[{box_id, ip, sealed}]}	同一 IP 给现场内每台盒子各一份密文，单个事务写入；任一盒子不属于该现场时整批拒绝		
GET boxes?site=	不回硬件指纹；online = 90 秒内有心跳；streams/sys 取内存里最近一次心跳；带 up_since、drill_until		
PUT boxes/{b} {name} / POST boxes/{b}/pause resume	改名、停止上送		
POST boxes/{b}/actions {type}	discover / probe / recheck，落库排队，下一次心跳带走；recheck 5 分钟一次		
POST boxes/{b}/drill {minutes}	演练切换；minutes=0 结束演练；最长 60 分钟		
GET boxes/{b}/discovery / PUT boxes/{b}/secrets	发现清单；单盒的密文写入		
POST cameras/bulk	1 到 256 项，整批校验；同现场同 source_ref 回原来的相机；名字缺省取发现清单的自报名		
GET cameras	含已移除的；带 assigned_box		
PUT cameras/{cam} / stream-role / pause resume remove	改名、改码流意图（auto / third / sub / main）、单路状态		
POST pause-all / resume-all	总闸		
GET ledger / GET audit	台账；审计不回指纹与来源 IP		

6.7 节点侧 /v1/hub/{hub_id}/

GET publishers?rev=: 该放行的推流账号（租户 active 且挂在这个节点、相机 enabled、代推盒子 active 且没按停止上送），按现场分组带 rank（卸路时后加的先让）。POST status: 每路收到字节、就绪、候选对类型、卸路名单；卸路名单有变，受影响盒子的配置版本加一。

6.8 密封格式 sealed_v1

盒子公钥 P-256 未压缩点 65 字节，标准 base64
 共享秘密 ECDH(临时私钥，盒子公钥) 取 256 位
 AES 钥 HKDF-SHA256, salt 32 个 0, info "uanbox-camsecret-v1|<box_id>|<ip>", 32 字节
 IV 12 字节随机；AAD "<box_id>|<ip>"
 明文 JSON {"user": "...", "pass": "..."}
 密文串 JSON {"v": 1, "epk": "<临时公钥 base64>", "iv": "<base64>", "ct": "<含 16 字节 tag>"}

浏览器只用 WebCrypto，不引第三方库；frontend/scripts/seal_selftest.mjs 和盒子的 uanbox-agent seal-selftest 做互通测试。crypto.subtle 只在 https 或 localhost 下有，页面走 http 时拿不到会报 no_webcrypto。

6.9 中心接入页接口

中心代登录用户调上面的租户侧接口，读接口对非超级管理员按园区过滤，写接口只给超级管理员并进中心审计。回包 {ok: true, result}，控制面连不上或回错一律 502 带中文原因。overview 把现场、盒子（带发现清单）、相机三表合一，并上本中心的相机配置与在线状态。

附录 A

参数表

项	值	定义位置
盒子心跳间隔	30 秒	uanbox-agent
在线判定	最后心跳在 90 秒内	ONLINE_S
签名时间差上限 / 防重放窗口	300 秒	MAX_SKEW_S
接入码	24 小时有效、一次性、错 5 次锁定 15 分钟	JOIN_MAX_FAILS、JOIN_LOCK_S
租户钥匙错误锁定	5 次 15 分钟，按（IP，租户码）	同上
硬件指纹冲突窗口	90 秒	FP_CONFLICT_S
长轮询	25 秒	Config.long_poll
相机发现周期	60 秒	uanbox-agent
退避	60 / 300 / 900 秒	uanbox-agent
重新检查限频	5 分钟	ActionGap
失联巡检	30 秒一轮	FAILOVER_TICK_S
回切稳定期	600 秒	FAILBACK_S
演练上限	60 分钟，缺省 10 分钟	DRILL_MAX_MIN
卸路判定	连续 3 个窗口（10 秒）丢包不低于 5%；恢复需连续 3 个窗口低于 1%	uanhub-agent shed.rs
中心拉取控制面	10 秒	link_api 同步线程
缩略图缓存	55 秒	link_api
回放直连等待	20 秒，建连后再延长 10 秒	ClipPlayer
回放路径空闲关闭	5 秒	mediamtx 路径模板
黄口地址	192.168.88.1/24；互备为 .2 / .3，浮动 .1	install.sh
相机静态地址	.11 至 .99；DHCP 池 .100 至 .199	相机调参 / install.sh

附录 B

容量与带宽

条件	数值
每路上行	约 1 Mbps（第三码流 768 Kbps 定码率加传输开销）
30 路	40 Mbps 上行以上
单处理节点长期运行参考	13 路持续 22.5 小时会话重建 0 次，合计约 23.6 Mbps，节点温度最高 69 °C
处理节点推理（TensorRT FP16）	单模型 yolox_s 1.4 ms；8 路生产负载 GPU 占用 5% 至 6%；30 路每路 0.5 帧约 30%
双盒现场	单条宽带至少承载一半以上路数
双盒切换	停机到接管不超过 120 秒（失联判定 90 秒加巡检周期）；接管到恢复推送约 5 秒；恢复到回切 10 分钟稳定期
回放直连	点击到出画约 5 秒（节点按需转码约 3 秒，候选收集兜底 3 秒）

附录 C

勘查单

宽带：地址类型（固定 / 商业 / 家庭 / 专线）、是否有 IPv6、上行速度（30 路需 40 Mbps）、光猫接法（直接联网 / 需拨号）、拨号账号（口令另行传递）、宽带归属。

盒子位置：安装位置、插座、温度与通风、与光猫的距离。双盒现场另问：第二条宽带的运营商、两台盒子的电源是否独立回路或有无 UPS。

相机：数量、品牌型号、已装或新装、安装与调试责任方、有无录像机、是否同一台交换机、交换机空口数、现有地址是否被其他系统占用。

其他：能否远程维护、期望启用日期、客户管理员（姓名、手机）、合同是否允许画面离开场站。

勘查后的工作：上行不足时先说明可接路数；画面不得离开场站时改报本地方案；需拨号时将账号记入预绑定任务；相机需新装或未调参时将相机调参说明发给设备方；家庭宽带且无固定地址与 IPv6 时先评估能否云托管。

附录 D

相机调参（海康）

1. 激活：首次打开网页设置管理员口令。
2. 地址：关闭自动获取；IPv4 192.168.88.11 至 .99；掩码 255.255.255.0；网关 192.168.88.1。
3. 预览账号：用户名 view，口令全站统一，权限仅”远程预览”。
4. 启用第三码流：系统 > 系统维护 > 系统服务，启用后重启。
5. 第三码流：H.264、1280×720、定码率、8 帧、768 Kbps、I 帧间隔 16、关闭 H.264+ 与 SVC。旧型号最高 704×576 的按其最大分辨率设置。没有第三码流的改用子码流。
6. 对时：NTP，服务器 192.168.88.1，间隔 60 分钟。
7. 交付：参数页截图（文件名用相机地址）加登记表一行。

常见遗漏：H.264+ 未关闭（画面可见但无法上云）、两台相机同地址（均时断时续）、修改后未保存。

附录 E

接入盒装机说明（安装员）

接三根线：宽带线接蓝口，相机线接黄口（相机交换机任意空口），电源线接不易被误拔的插座。蓝口与黄口不可接反，接反后交换即可。通电后等待两分钟，期间不拔线、不反复开关。查看指示灯：电源灯常亮，网口灯亮或闪烁。不需要接显示器、不需要输入密码、不需要修改相机与光猫。安装于弱电箱或机柜，远离发热设备，防雨。出现问题时拍两张照片（正面指示灯与标签、背面网线接口）发给沅虹客服。不要拆开盒子、不要按压盒上小孔、不要接入办公网络。

附录 F

版本记录

版本	日期	内容
0.10	2026-10-01	命名与入口：智眸英文名改为 UanVision，归入智觉（UanSense）之下作为视觉神经；入口域名改为 vision.uanhon.cn，sense.uanhon.cn/app 并行保留
0.9	2026-10-01	章节编号改为技术手册格式（第 N 章、N.N 节、附录 A 至 F、图按章编号、页码）；部署全景章删去平台内部运维细节，只保留三类角色的职责
0.8	2026-10-01	识别分层补行为时序门控
0.7	2026-10-01	识别的两层结构与对智悟、蓝精灵的依赖：部署形态表加判定位置，架构图加智悟与判定回流，本地化需预装蓝精灵
0.6	2026-10-01	全书按技术手册语域重写：去除口语表述、内部机器名、工单编号与开发测试过程叙述；切换时间改为指标表述；组件关系改为插图
0.5	2026-10-01	新增”部署全景”章；回放直连
0.4	2026-10-01	入口改为 sense.uanhon.cn 单域名
0.3	2026-10-01	补充双盒切换指标；安装脚本 --any-distro
0.2	2026-10-01	标题改名词短语，系统组件改为段落说明
0.1	2026-10-01	初稿