

智眸现场接入

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 0.2 · 2026-10-05

目录

概述与架构	2
读者对象与范围	2
部署形态	2
系统组件	2
接入流程	4
安全边界	6
故障域	6
部署场景	7
形态选择	7
宽带要求	7
硬件配置	7
相机要求	8
多盒现场	8
安装与配置	8
租户开通	8
接入盒安装	9
预绑定	11
升级、回滚与卸载	11
安装包构建与发布	12
控制面部署	12
处理节点与中心部署	12
运维与排障	13
日志与状态位置	13
相机状态与原因	13
常见故障与根因	14
多盒现场运维	15
控制面版本更新	15
接入盒版本更新	15
接口与数据参考	16
鉴权方式	16
数据表 (sqlite, WAL)	16
配置版本与长轮询	17
运营侧 /v1/admin/	17

盒子侧 /v1/box/{id}/	17
租户侧 /v1/t/{tenant}/	18
节点侧 /v1/hub/{hub_id}/	18
密封格式 sealed_v1	18
中心接入页接口	19
附录	19
附录 A 参数表	19
附录 B 容量与带宽	20
附录 C 勘查单	20
附录 D 相机调参（海康）	20
附录 E 接入盒装机说明（安装员）	20
附录 F 版本记录	21

概述与架构

读者对象与范围

智眸（UanSense）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、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。客户管理员使用的操作说明发布在文档中心（docs.uanhon.cn），不在这本书的范围内。

技术正本分布在三处：接入控制面仓库 uanlink 的 SPEC.md（接口与数据表）、台账仓库的各期方案与发版记录、智眸仓库 uansense 的 deploy/ 目录。这本书按部署与运维的顺序组织这些内容，代码变更后随版本更新。

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	识别位置	画面是否离开场站
远程（云托管）	接入盒：N100 小主机，双网口，仅负责拉流与推流	沅虹处理中心（北京 B101）	经加密通道传出
本地轻	带独立显卡的小主机（铭凡 G1 Pro 一类，内存 64 GB 起）	现场本机	不离开
本地重	DGX Spark（64 GB 或 128 GB）	现场本机	不离开

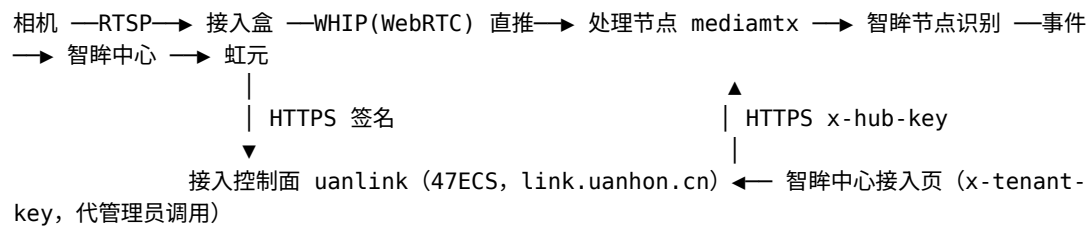
本版主要描述远程形态。远程形态涉及接入盒、控制面与处理节点三方协作，组件最多。本地两种形态的安装程序属于 D-69 第二阶段，完成后补充相应章节。

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 47ECS 上，监听 127.0.0.1:9800，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; ECS 仅有 2 核 1.9 GB 内存, 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 (B101) 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 (base) 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。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。



视频流不经过以上任何组件。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。

接入流程

步骤	执行者	位置	操作	系统行为
0	沅虹运营	运维机	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, 中心实例与子域生效; 控制面建立租户, 租户钥匙写入中心环境
1	沅虹运营	办公室	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。

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；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 127.0.0.1 或 nginx /v1/admin/ 前缀（来源 IP 白名单）的请求。

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，D-70 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（D-70 第一阶段）
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 90 秒内接管其相机
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、办公室断网	全部云托管租户停止	同左，节点级互备在第二阶段
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

部署场景

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。

宽带要求

上行每路约 1 Mbps（第三码流定码率 768 Kbps 加开销），30 路要 40 Mbps 以上，并且要能一直跑满。家庭宽带的上行通常 20 到 30 Mbps，接 15 路以内可以，再多要换商业宽带。

控制面能看出两样：盒子自检上报的公网出口类型（锥形 NAT 能直连，对称 NAT 要靠节点宣告固定端口），和同一现场两台盒子是不是同一个出口（出口相同就不是真冗余）。看得出来的是电源，只能靠勘查登记。

自检项	检测方法	判定
时钟偏差	和 HTTPS 响应头的 Date 比	超过 300 秒签名会被拒，装 chrony 就不会
HTTPS 通	连 link.uanhon.cn	不通一切免谈
UDP 与 NAT 类型	同一个 socket 向两个 STUN 服务器各问一次，映射端口一致记 eim（锥形）	锥形可直连，对称要靠节点的固定端口宣告
IPv6	有没有全球单播地址、能不能连 2400::1 的 53	具备 IPv6 的现场打洞成功率最高
相机网段	黄口有没有链路、能不能发现设备	没相机时记”还没配相机”

运营商级 NAT 的现场要注意：地址池里每条映射可能分到不同的公网 IP，盒子要连续两次读到同一个新地址才算换了 IP（10-01 贵州联通实测），否则每 30 秒误判一次。

硬件配置

接入盒：x86 N100 一类小主机，两个千兆口，8G 内存，64G 以上硬盘（盒子不存视频），Debian 12，10 瓦上下。arm64 小主机也能装（安装包有 aarch64 版），出厂预装只做 x86。放弱电箱或机柜，0 到 40 度，不淋雨。

本地轻：NVIDIA 桌面显卡 8G 显存起，内存 64G 起（判定模型蓝精灵与摘要模型各 20G 多，专家放内存、注意力放显卡，实测 243 机器可行），2T NVMe，Ubuntu 24.04，20 到 30 路，值班室或机房。

本地重：DGX Spark 64G 或 128G，2T 以上，出厂 DGX OS，50 路以上。

本地两档都是桌面机，不是宽温工控机。要放户外机柜或高温车间的另选工控整机。

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 192.168.88.11 到 .99，网关与对时 192.168.88.1，一台一个地址。
- 预览账号单独建，只勾“远程预览”，口令全站统一交给客户管理员。管理员口令不给沅虹。
- 第三码流 H.264、1280×720、定码率 768 Kbps、8 帧、I 帧间隔 16、H.264+ 关、SVC 关。没有第三码流的型号改子码流，主码流永远不动。
- 相机接同一台相机交换机，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 到 1280×720、帧率 6 到 15。选流：有第三码流 103 用 103，否则子码流 102，永不自动选主码流；NVR 通道默认拼 x02。不合格的路不推，报原因，管理员在接入页能看到一句话。

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。该能力于 D-70 第一阶段实现。

- 相机登记在首选盒子，实际由谁推由控制面定。盒子失联 90 秒，它名下的相机交给同现场里看得见这台相机（发现清单里有它）且拿到了它口令密文的在线盒子，路数少的先。首选盒子回来并稳定 10 分钟后把相机还回去，现场可以关掉自动回切。
- 两台盒子的黄口分别 192.168.88.2 和 .3，只有 1 号给相机发地址，192.168.88.1 由 keepalived 在两台间浮动，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，同一台相机的口令给现场里每台盒子各封一份密文。后加的盒子要再保存一次口令，控制面在它没拿到密文之前不把相机分给它。
- 接入页”演练切换”按钮：把一台盒子按离线对待 10 分钟，相机当场交给另一台，结束时当场切回。验收时当着客户做一遍。
- 一台顶两台时上行如果带不动，节点侧的卸路逻辑自动起作用，所以双盒现场勘查时要求单条宽带至少带得动一半以上的路数。

处理节点级互备（双 Spark，租户在两个节点各开实例）属第二阶段，前提是办公室的电源与出网分开，目前 B101 与 B102 共用同一条宽带与同一台 UPS。

安装与配置

租户开通

租户开通由沅虹运营在运维机上执行 uansense/deploy/cloud/sense-tenant，脚本经 ssh 编排处理节点、中心与入口三台机器：

```
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 到 19）决定一切编号：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，frp 远端端口 27060+n。n 分出去就不再复用。每台机器上的动作都先判断再做，同一个租户连跑两次不出错。

它在三台机上做的事：

机器	动作
处理节点 (B101)	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 按来源地址只让它读自己租户的流、nftables 只放它该到的端口
中心 (base)	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)、NFS 挂节点上的数据目录、frpc 加一条到 ECS 的代理
入口 (47ECS)	<code><租户>.sense.uanhon.cn</code> 解析、证书、nginx 站点
控制面	运维机环境里有 <code>UANLINK_ADMIN_KEY</code> 时建租户、拿租户钥匙写进中心 <code>env (UANLINK_TENANT_KEY)</code> ；没有就提示一句跳过

控制面地址分两个变量：运维机自身调用控制面可以经隧道 (`UANLINK_URL=http://127.0.0.1:19800`)；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 (S-58)。

节点共享目录 `/opt/uansense` (Python 环境与模型) 是只读共享，租户代码树里的 `models` 软链指向它。代码树中原有 `models` 目录，`ln -sf` 会把软链建到该目录内部形成 `models/models`，脚本改为先挪开目录再执行 `ln -sf` (zt 节点 2026-10-01 至 10-04 火焰烟雾模型未加载即由此引起)。

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、`<版本>` 下两个架构的包、`install.sh`、`SHA256SUMS`。

双网口盒子 (蓝口宽带、黄口相机)，装完要重启

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

单网口机器，装完直接入网

```
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 (D-70)：另一台 `--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` 与包的哈希，交给 `install.sh`。除 `--code` 与 `--base` (换下载站) 外的参数原样透传。

`install.sh` 的参数：

参数	用途
--bundle <目录或 tar.gz> / --url <地址> --sha256 <值>	包来源, 不给时脚本所在目录是解开的包就用它
--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 并给相机发地址, 不转发。要重启才生效
--wan / --lan	网口名不是 enp1s0 / enp2s0 时指定
--ha 1 2	两盒互备: 黄口 .2 / .3, 只有 1 号发地址, .1 由 keepalived 浮动 (VRRP 组 88, 1 号优先级 150, 回抢延迟 30 秒), 防火墙放 VRRP
--pppoe <账号>	光猫桥接要拨号。口令按提示输入或环境变量 UANBOX_PPPOE_PASS, 不进命令行
--ssh-wan / --ssh-lan	防火墙缺省不放 SSH; 要远程维护加前者, 技术员带笔记本接黄口兜底加后者
--no-apt	离线镜像已装 chrony、ffmpeg 时跳过装系统包
--reset-machine-id	做出厂镜像克隆前必须带 (见下)
--dry-run / --uninstall / --purge / --root <假根>	演示、卸载、连身份一起删、测试用假根

装了什么:

路径	说明
/opt/uanbox/versions/<版本>/ 与 current 软链	两个二进制、install.sh、prebind.sh、MANIFEST; 升级进新目录原子切换, 旧版本不删
/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; 手填的优先于接入页下发的
/etc/uanbox/mediamtx.yml (600)	首次空配置, 之后 agent 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、 agent.service	uanbox- Restart=always, agent 在 mediamtx 之后
/etc/chrony/conf.d/uanbox.conf	阿里、腾讯对时; --router 时允许黄口网段来对时

--router 另外写 systemd-networkd 的两个 .network、/etc/sysctl.d/90-uanbox.conf (转发全关)、/etc/uanbox/firewall.nft (只管 inet uanbox 一张表)、拨号时的 ppp 配置。改之前原文件备份到 /var/lib/uanbox/backup-<时间>/。

出厂镜像必须带 --reset-machine-id: 硬件指纹是 machine-id 加物理网卡 MAC 的哈希, 克隆出来的盒子指纹一样, 第二台入网会撞(控制面回”这台机器已有在用的盒子”)。母机清完别再预绑。

预绑定

预绑定在沅虹办公室完成。前提: 盒子已装(双网口带 --router 并重启过), 蓝口能上网。接入码在接入页”生成接入码”拿, 24 小时有效、只能用一次。

```
sudo uanbox-prebind ABCD-EFGH-JKLM # 入网、显示自检判定、拉起两个单元、打印标签
sudo uanbox-prebind --label # 重印标签
```

办公室宽带的自检结论不代表现场, 到现场换了宽带盒子会重测。已入网的盒子会被拒: 先在控制面吊销, 等盒子收到吊销(它会自己标记), 再预绑。**不要自己删 /var/lib/uanbox:** 控制面旧记录还在, 同一硬件指纹会被拒(409), 旧记录也没法正常停。

升级、回滚与卸载

升级: 再跑一遍那条命令(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走，回滚不用重新入网。卸载 `install.sh --uninstall` 留身份与口令，`--purge` 连身份一起删（控制面上的记录要运营吊销）。网口配置在卸载时保留，避免卸载过程中断开自身网络。

安装包构建与发布

```
# 168 上, mediamtx 用官方 v1.21.1 包 (贵州盒子在用的就是官方版)
MEDIAMTX_TAR=~/.smurf-xfer/mtx/mediamtx_v1.21.1_linux_amd64.tar.gz \
MEDIAMTX_TAR_AARCH64=~/.smurf-xfer/mtx/mediamtx_v1.21.1_linux_arm64.tar.gz \
deploy/box/make-bundle.sh --arch all
deploy/box/publish.sh                # scp 到 ECS, 切 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带 `.dirty`, `publish.sh` 拒发 `dirty`。下载站 `nginx` 不能套 ECS 的 `block-scanners` 片段, 那个片段把所有 `.tar.gz` 请求掐断。

控制面部署

二进制 `/opt/uanlink/uanlink` (musl 静态, 168 上 `cargo build --release --target x86_64-unknown-linux-musl -p uanlink`), 环境 `/etc/uanlink.env` (`UANLINK_ADMIN_KEY`、`UANLINK_INGEST_HOST`、`UANLINK_DB`、`UANLINK_BIND`), 库 `/var/lib/uanlink/uanlink.db` (sqlite WAL, 600, 里面有推流口令明文), 单元 `uanlink.service`。

换版: 留底二进制与库, `cp` 到 `/tmp` 再 `mv`, `systemctl restart uanlink`, 看 `GET /v1/admin/hubs 200`、盒子心跳照常。库在启动时自动补列建表, 老版本不读新列, 回滚不用动库。

`nginx conf.d/link.conf`: `/v1/box/` 与 `/v1/t/` 的 `client_max_body_size 2m`, `/v1/t/` 只放中心的出口 IP (现在是 base 的办公室宽带出口, 变了要改), `/v1/admin/` 按来源白名单。

处理节点与中心部署

节点代理 `uanhub-agent` (B101 本机编译, 168 交叉编不了 ring), `x-hub-key` 每个节点一把。它把 `p_` 开头的推流账号整段替换进 `/opt/mediamtx/mediamtx.yml` 的 `authInternalUsers` (本机、看墙两条固定条目不动), 写临时文件再改名, 两次写至少隔 1.2 秒, 写完用 `/v3/config/global/get` 核对。

节点侧三件自动的事: 公网地址跟随 (每 15 秒 STUN, 连续两次同一个新地址就改 `webRTCAdditionalHosts`, `UANHUB_PUBLIC_HOSTS=off` 关)、上行拥塞卸路 (每 10 秒按现场汇总丢包, 连续 3 窗口不低于 5% 判挤满, 卸到实测容量一半, 放回要连续 3 窗口干净, `UANHUB_SHED=off` 关)、配置 lint (turn: 或非中国大陆地址直接拒写)。

中心接入页的后端是 `console/link_api.py`, 环境变量在 `env.d/center`: `UANLINK_URL`、`UANLINK_TENANT_KEY`、`UANLINK_TENANT`、`SENSE_INGEST_RTSP`、`UANLINK_HUB_NAME`。没配钥匙整个接入页不开通, `/api/link/*` 一律 503。

运维与排障

日志与状态位置

位置	内容
盒子	<code>journalctl -u uanbox-agent -u uanbox-mediatrix -f; /opt/uanbox/current/uanbox-agent probe</code> 只跑一次自检; 黄口上接电脑开 <code>http://192.168.88.1:8080</code> 本地诊断页 (只读: 状态、相机、自检逐项、日志尾, 口令遮掉)
控制面	47ECS <code>journalctl -u uanlink;</code> 库 <code>sqlite3 /var/lib/uanlink/uanlink.db (600, root); nginx access.log</code> 里 <code>link.uanhon.cn</code> 那些行
处理节点	B101 <code>journalctl -u uanhub-agent、uansense-node@<租户>; mediatrix API /v3/paths/list、/v3/webrtcsessions/list</code>
中心	base <code>journalctl -u uansense@<租户>;</code> 中心审计表 <code>audit_log</code> 里 <code>link_*</code> 动作
接入页	页面顶部报红是中心连不上控制面; 相机行黄色点开有一句原因; “上送记录”看每路本月字节、谁在什么时候填过口令或暂停过

控制面审计 (租户看 `GET audit`) 记每一笔写操作, 操作人是中心登录名; 指纹、来源 IP、密文一律剥掉。接管与回切记 `system:failover`。

相机状态与原因

盒子心跳每路带 `state` (`online / checking / connecting / shed / backoff / paused / failed`)、`cred` (`ok / bad / none / untested`)、`err`、`codec`、`bframes`、`chosen_stream`、`fps`。
接入页按下表翻成一句话:

原因	页面提示	处理方法
黄口没发现设备	黄口那边没有找到相机	相机交换机通电、网线在黄口、相机灯亮；20 秒后自动再找
相机 RTSP 不通	相机能看到但连不上视频口	等几分钟，不行重启那台相机
同 IP 两个 MAC 没激活	有两台相机用了同一个地址 有几台相机还没设过密码	装相机的人改掉一台 先激活
cred none	还没有这台相机的口令	在口令框填一次
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，避免海康相机因多次口令错误锁定 30 分钟；填写正确后点”重新检查”
H.265	视频格式是 H.265	第三码流改 H.264
B 帧 / H.264+	开了 B 帧或 H.264+	关 H.264+
no_third	第三码流没开	相机网页 系统维护 > 系统服务 勾”启用第三码流”后重启；或点”改用子码流”
res_out / fps_out	分辨率或帧率不合适	设成 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 分钟还这样看现场网络
paused	已暂停上送	有人点了暂停，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 machine-id）

常见故障与根因

盒子在线但一路都不推。 看盒子日志里有没有”拉口令密文 HTTP 401”：盒子状态不是 active（被挂起或吊销）。再看 `cameras.secret` 有没有这台相机：本地手填的优先，接入页下发的只补缺。

推了但节点收不到。 节点 `uanhub-agent` 日志看候选对类型：出现 relay 立即 error（我们不走 TURN）。对称 NAT 的盒子只能打节点宣告的固定端口 公网 IP:8189，节点的公网地址跟随有没有在跑（`webrtcAdditionalHosts`）。mediamtx 的 `whipBearerToken` 和内置账号鉴权对不上（401），推流地址必须把账号口令写进 URL 用 Basic（10-01 实测）。

签名被拒。 盒子时间差超过 300 秒：chrony 没起来（安装脚本结尾会提示）。同一秒同一请求签名一样会被当重放，测试脚本要隔 1.1 秒。

办公室换了 IP 盒子不重连。退避里自检的 STUN 与 HTTPS 一恢复就清零所有退避；盒子公网 IP 变了也清零，但要连续两次读到同一个新地址（运营商级 NAT 地址池）。

第二台盒子入网被拒”这台机器已有在用的盒子”。硬件指纹一样：克隆镜像没带 `--reset-machine-id`。同一台开发机起第二个盒子做测试用 `UANBOX_MACHINE_ID_FILE` 指一份别的 `machine-id`。

中心接入页整页 503。中心 env 没有 `UANLINK_TENANT_KEY`，或 `UANLINK_URL` 写成了运维机的隧道地址（S-58）。

租户钥匙错 5 次锁 15 分钟。按（来源 IP，租户码）这一对计数，所以一个中心配错钥匙不会锁住走同一出口的别的租户。钥匙对就放行，不看锁。

节点上一个模型都没加载。`models` 软链建进了 `models/models`（sense-tenant 老版本），`ls -la /srv/sense/<租户>/app/models` 看是不是软链指向 `/opt/uansense/models`。

下载站包下不了，别的文件能下。`nginx` 套了 `block-scanners` 片段，它把 `.tar.gz` 一律 444；下载站单独不套。

多盒现场运维

- 接入页现场卡片的”冗余”：有效（两台以上在线且出口不同）、同一条宽带、只 `n` 台在线、单盒、待自检。出口取控制面看到的来源地址，没有再看自检里 STUN 测到的。
- 盒子失联 90 秒接管，首选回来稳定 600 秒回切，巡检 30 秒一轮。接管条件三个都要满足：同现场在线、发现清单里有这台相机的 ip、有这台相机 ip 的密文。常见的”没接管”就是后加的盒子没保存过口令，让管理员再保存一次。
- 两台盒子不会同时推同一路：推流账号按相机发，节点 `mediamtx` 只认先到的，旧盒子没拉到新清单时被拒，拉到清单就停。
- `--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，不等稳定期也不看回切开关。
- 吊销正在代推的盒子，它代推的相机退回各自首选；它自己首选的相机口令作废要重新登记。

控制面版本更新

1. 168 编 `musl` 静态包，留底 `/opt/uanlink/uanlink.bak-<期号>` 与 `/var/lib/uanlink/uanlink.db.bak-<期号>`。
2. `cp` 到 `/tmp` 再 `mv`，`systemctl restart uanlink`，看日志”已监听”。
3. `GET /v1/admin/hubs 200`；库里 `box.last_seen_at` 在 90 秒内刷新（盒子心跳照常）。
4. 库自动补列，老版本不读新列，回滚只换二进制。
5. 在台账仓写发版记录：每一步的操作、回滚方法、未在线上验证的项。

接入盒版本更新

1. `make-bundle.sh --arch all`，`publish.sh`（工作区 `dirty` 拒发，回读大小核对）。
2. 现场再跑一遍一条命令，或者 `install.sh --bundle <新包>`；新版本进自己的目录原子切换。
3. 盒子心跳带 `agent_version`，接入页盒子卡片能看到；旧版本不删，回滚改软链重启两个单元。

接口与数据参考

接口与数据表的正本为 uanlink/SPEC.md，本章为其摘要与说明。名字与格式：租户码 $^{\wedge}[a-z][a-z0-9]\{1,30\}\$$ ；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。

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、Ed25519 签名	Ed25519 签名 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

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 是当前实际在推的（D-70）；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。

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。

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。

盒子侧 /v1/box/{id}/

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

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 failback
PUT sites/{s}/failback {enabled}	D-70 回切开关
PUT sites/{s}/secrets {items[{box_id, ip, sealed}]}	D-70 同一 ip 给现场每台盒子各一份密文, 一个事务, 有一台不在现场整批拒
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}	D-70 演练切换, 0 结束, 最多 60
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

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。

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>"}
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。

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

附录 A 参数表

项	值	在哪定
盒子心跳间隔	30 秒	uanbox-agent
在线判定	最后心跳 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、一次性、错 5 次锁 15 分钟	JOIN_MAX_FAILS、JOIN_LOCK_S
租户钥匙错码锁	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	DRILL_MAX_MIN
卸路判定	连续 3 窗口（10 秒）丢包不 低于 5%；放回要连续 3 窗 口低于 1%	uanhub-agent shed.rs
中心拉控制面	10 秒	link_api 同步线程
缩略图缓存	55 秒	link_api
黄口地址	192.168.88.1/24；互 备 .2 / .3，浮动 .1	install.sh
相机静态地址	.11 到 .99；DHCP 池 .100 到 .199	调参页 / install.sh

附录 B 容量与带宽

条件	数
每路上行	约 1 Mbps (第三码流 768 Kbps 定码率加开销)
30 路	40 Mbps 上行以上
贵州长稳 (D-55)	13 路 22.5 小时会话重建 0 次, 合计约 23.6 Mbps, B101 温度最高 69 度
处理节点 B101 (TensorRT FP16)	单模型 yolo_x_s 1.4 ms; 8 路生产负载 GPU 5 到 6%; 30 路回环压测 (每路 0.5 帧) 约 30%
双盒现场	单条宽带至少带得动一半以上路数

附录 C 勘查单

宽带: 地址类型 (固定 / 商业 / 家庭 / 专线)、有没有 IPv6、上传速度 (30 路要 40 兆)、光猫怎么接 (插上就能上网 / 要拨号)、拨号账号 (口令另传)、宽带归谁。

盒子放哪: 位置、插座、温度与通风、离光猫多远。双盒现场另问: 第二条宽带是哪家、两台盒子的电源是不是独立回路或有没有 UPS。

相机: 台数、品牌型号、已装还是新装、谁装谁调、有没有录像机、是不是同一台交换机、空口数、现有地址是否被别的系统在用。

其它: 能不能远程维护、希望哪天开始、客户管理员是谁、合同允不允许画面出场站。

勘查完要做的: 上行不够先说清能接多少路; 画面不能出场站改本地方案; 要拨号把账号记进预绑任务; 相机要新装或没调参把调参页发给设备方; 家庭宽带两样都没有的先评估能不能上云。

附录 D 相机调参 (海康)

1. 激活: 第一次打开网页设管理员口令。
2. 地址: 自动获取关; IPv4 192.168.88.11 到 .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, 权限只勾“远程预览”。
4. 启用第三码流: 系统 > 系统维护 > 系统服务, 勾后重启。
5. 第三码流: H.264、1280×720、定码率、8 帧、768 Kbps、I 帧间隔 16、H.264+ 关、SVC 关。旧型号最高 704×576 的按它能给的最大设。没有第三码流的改子码流。
6. 对时: NTP, 服务器 192.168.88.1, 60 分钟。
7. 交回: 参数页截图 (文件名用地址) 加登记表一行。

容易漏: H.264+ 没关 (能出画面但上不了云)、两台同地址 (都时好时坏)、改完没点保存。

附录 E 接入盒装机说明 (安装员)

接三根线: 宽带线插蓝口, 相机线插黄口 (相机交换机任意空口), 电源线插不会被随手拔的插座。蓝黄不能插反, 插反了换回来就好。插电后等两分钟, 不要拔线反复开关。看灯: 电源灯常亮, 网口灯亮或闪。不用接显示器、不用输密码、不用改相机和光猫。放弱电箱或机柜, 别和发热设备挤、别淋雨。出问题拍两张照片 (正面看灯和贴纸、背面看网线插哪) 发沅虹客服。别拆盒子、别按小孔、别接进办公室的网。

附录 F 版本记录

版本	日期	内容
0.2	2026-10-05	文风改为技术手册语域：标题改名词短语，系统组件改为段落说明，去掉口语化表述
0.1	2026-10-04	初稿。收 D-55（云托管接入）、D-68（接入程序与向导）、D-69（一条命令安装与文档中心）、D-70 第一期（多盒互备）。本地两档的安装章等 D-69 第二步