侯军

IT 运维工程师 / 信息安全工程师

手机：17680146825（微信同号）｜邮箱：17680146825@163.com

期望城市：广州 / 深圳｜期望薪资：面议｜到岗：月内

个人优势

- **技术闭环：**具备 5 年企业 IT 运维与信息安全经验，拥有企业 IT 架构从 0 到 1 的规划、建设和运营经历，能够从现状调研、架构设计、设备选型推进到上线验收、故障恢复和持续优化，持有 HCIP 认证。
- **综合落地：**覆盖企业级三层网络、服务器与 VMware 虚拟化、AD / GPO、NAS 与监控存储、终端标准化、零信任、DLP、企微高级安全和自动化运维，能够将业务与甲方安全要求转化为技术控制、制度流程及检查证据，兼顾业务连续性与数据安全。

核心技能

- **网络与边界安全：**企业级三层网络规划，VLAN、Trunk、Eth-Trunk、PVID、DHCP、ACL、路由与链路排障；华为防火墙、深信服 AC 上网行为管理和最小权限访问策略。
- **Windows 与终端治理：**Windows Server、AD DS、OU、GPO、DNS、域账号与计算机对象管理，标准镜像、批量部署、软件限制、公共设备权限和终端交付回收。
- **虚拟化、存储与恢复：**VMware ESXi、NAS / SMB、CVR 存储、备份恢复、虚拟机快照回滚、跨盘迁移、阵列热备、故障切换及 UPS 断电保障测试。
- **信息安全与数据治理：**深信服 aTrust 零信任、XDLP 数据防泄密、aES 终端安全、AC 上网行为管理，IP-guard 透明加密、企微高级安全、飞书 SSO 与安全管控（AD FS/SAML、OAuth2、可信设备、IP 围栏）、敏感信息识别、文件外发审批和日志审计。
- **自动化与运维开发：**PowerShell、WMI/CIM、WinRM、RSAT ActiveDirectory、Windows Event Log、IIS、Node.js、HTML/JavaScript、DataTables、ECharts、飞书开放平台 API。

工作经历

广东云云律师事务所｜IT 运维与信息安全工程师｜2025.06 - 2026.11

- **企业网络从 0 到 1 建设：**主导将原有家用设备及小型二层网络重构为企业级三层网络，完成“防火墙-上网行为管理-核心交换-汇聚-接入”全链路部署；按办公区域、用户类型和设备用途规划 20+ VLAN，配置 Trunk、Eth-Trunk、PVID、DHCP、ACL 及路由策略，实现终端、服务器与 IoT 设备分区隔离和访问控制。
- **运行保障与机房巡检：**负责网络、服务器、VMware、NAS/CVR 存储、华为防火墙、深信服 AC、UPS 及机房环境的日常运行，维护 8 台虚拟服务器、约 30TB NAS 和约 300TB 海康 CVR 存储；建立机房与平台巡检清单，检查设备状态、资源容量、链路、备份、供电和安全日志。服务器与存储设备投产前均按方案完成备份恢复、快照回滚、阵列热备、故障切换或 UPS 断电保障等对应验收测试；完成 AD 误删 OU 与用户对象的墓碑恢复，保留用户原 SID 并验证原账号登录与桌面恢复；修复备用域控启动故障，验证 AD 服务、双向复制、SYSVOL/NETLOGON 及 DNS 正常，支撑身份服务与业务连续运行。
- **身份与终端运维：**负责 AD 域账号、计算机对象、OU 和 GPO 的日常管理，处理人员入离调转、终端加域与回收、账号权限调整、软件部署、公共设备登录及扫描归档访问等需求；结合合规要求与业务场景开发、测试和迭代域控策略，将浏览器限制、离席锁屏、软件安装控制、工具开机自启等需求转化为可下发、可回退、可验证的终端策略，提升业务响应效率与终端管控一致性。
- **安全运营与甲方审查：**负责深信服 aTrust、XDLP、aES、AC 及 IP-guard 等平台的日常运营、告警跟进和策略优化；结合业务与甲方要求完善终端安全、权限管理、文件外发及应急处置制度，配合甲方现场安全审查，开展审前自查、技术措施说明及制度台账、配置和日志举证，协同相关部门跟进问题整改。

- **文档、知识库与自动化：**输出网络拓扑、设备台账、系统配置、变更回滚、故障处置、终端交付、权限申请和平台操作等运维文档，建立常见问题知识库及 SOP；通过标准镜像、Netcopy 网络克隆、批量脚本和远程 GPO 刷新优化终端交付与策略执行，将终端标准化交付由约 60 分钟缩短至 15 分钟内，批量终端 GPO 刷新在 1 分钟内完成。
- **项目与团队协同：**统筹网络、安防、安全平台、设备租赁和文印设备等 6 类供应商售前、实施及售后资源，涉及项目金额 300 万元以上；协同 4 人推进需求确认、设备选型、变更排期和验收交付，安排下属跟进现场事项并对处理结果进行复核闭环。
- **飞书平台与身份运营：**负责飞书统一认证、可信设备及访问策略维护，处理账号匹配、登录异常和 XDLP 审批回传问题，支撑全所电脑端内部沟通及配套协作应用运行。

广州观己景观设计有限公司 | IT 运维工程师 | 2022.07 - 2025.05

- **IT 运维整体负责：**独立负责约 500 人规模公司的 IT 运维，覆盖办公网络、服务器、虚拟化、存储、终端、账号权限和办公设备，承担运行保障、故障处理和资源调配。
- **多工区网络互联：**独立负责总部与 3 个异地工区的网络建设和互通，采用站点到站点 IPSec VPN 建立跨区域安全通道，完成地址规划、路由策略、访问控制及隧道状态检查，处理线路波动、隧道中断和跨网段访问异常。
- **服务器与存储管理：**管理 20+ 台服务器及 PB 级存储环境，维护邮件、文件共享和虚拟化平台，开展容量检查、权限调整、备份恢复及关键服务异常处理。
- **终端规划与工作站交付：**根据行政办公、平面设计、三维建模和模型渲染需求，制定“高配设备新增、存量设备梯度下沉、老旧设备循环汰换”的更新方案；完成 CPU、GPU、内存、存储选型，以及图形工作站组装、系统部署和稳定性测试，整机成本较供应商方案降低约 25%。
- **设计业务支撑：**围绕图纸和模型大文件传输、共享存储、打印出图及跨团队协作，处理终端性能、网络连接、存储权限、办公软件和外设问题，保障设计项目交付。

广州中望龙腾软件股份有限公司 | IT 运维工程师 | 2021.07 - 2022.06

- **全球 IT 支持：**面向集团全球子公司及业务团队提供远程技术支持，覆盖桌面终端、账号权限、办公网络、办公设备及 OA / CRM / Eteams 等业务系统接入。
- **全球网络协同：**参与国内外分支和子公司的网络接入、连通性排障及访问权限协同，配合用户、业务团队和上级网络团队定位跨区域访问及链路异常。
- **规模化服务交付：**面向 2000+ 员工和 1000+ 终端提供技术支持，依托 ITSM 完成问题受理、分类、分级响应、升级协同和闭环反馈，年均处理 2500+ 起问题，常规事项平均响应时间控制在 15 分钟内。
- **终端与办公设施保障：**维护打印机、会议系统等办公设备，处理终端系统、软件安装、网络接入和外设故障，并沉淀常见问题处理文档。
- **团队协作：**对复杂网络、权限和业务系统问题完成信息采集、初步诊断和分级转交，协同国内外用户及专业团队推进问题闭环。

项目经历

广东云云律师事务所信息安全治理体系建设 | 核心推进 / 技术统筹 | 2025.06 - 2026.06

- **项目背景：**内部业务系统承载近 40 万起诉讼案件相关数据，办公过程同时涉及本地终端、异地接入、共享存储、打印扫描、材料出件和物理安防；原有网络、终端版本及权限管理较为分散，需要在不中断业务的前提下，逐步建立覆盖身份、终端、访问、数据和物理空间的信息安全治理体系。
- **身份与终端治理：**以 AD、OU 和 GPO 为统一管控底座，结合深信服 aES 建立人员、域账号、计算机对象和终端安全策略的管理关系；根据合规要求与业务需求配置密码、锁屏、软件安装、浏览器、公共设备登录及扫描归档访问等策略，并建立策略下发、验证和回退机制。
- **访问边界治理：**基于深信服 aTrust 和 AC 完成异地办公可信接入、高敏部门准内网访问及内部系统审计；分析 20 万+ 条网页访问日志，梳理 TOP100 域名、URL 和业务程序依赖，形成满足最小办公需求的访问白名单。

- **数据防泄密与安全运营：**基于深信服 XDLP，根据材料外发、图片与视频传输、压缩包和异常打印等业务场景评估泄密风险，制定敏感内容识别与风险分级规则；围绕审批、拒绝和风险事件建立处置台账，持续开展事件核查、误判复核和规则调整，推动策略从初始拦截转向按风险分级、按业务场景放行。
- **文件与物理空间管控：**将 NAS / SMB 目录权限接入域账号体系，按岗位和业务场景划分访问边界；建设封闭式打印中心，将员工打印、扫描和材料邮寄集中在受控空间完成，结合手机禁入、人员进出、门禁、监控和扫描归档记录降低纸质材料流转风险。
- **项目结果：**建立覆盖身份、终端、异地访问、电子文件、共享存储、纸质材料及物理空间的安全治理链路，使账号权限、访问策略、文件外发和材料出件具备统一管控与审计依据。在职期间累计审计 157 万+ 次文件外发行为，覆盖 5726 次审批和 1255 次拒绝记录，识别并跟进 1100+ 起风险事件，其中包含 76 起高风险事件，形成规则配置、事件核查、误判复核和策略调整闭环；在保障业务连续运行的前提下，实现高敏办公、异地接入和敏感信息流转可控制、可审批、可追溯，任职期间未发生经确认的数据泄露事件或重大信息安全事故。

飞书统一认证与安全管控建设｜独立负责｜2026.09 - 2026.10

- **项目背景：**原有办公 IM 依赖手机登录，私人设备和对外沟通难以统一管理；部分账号缺少文档创建与会议室预约能力，需要兼顾内部安全与协作需求。
- **实施内容：**接入域账号统一登录，将使用范围限定为公司可信电脑和指定内网；按内部沟通场景收紧外部联系、会议、云文档及第三方账号使用权限，并联通受控文件发送审批。
- **应用补齐：**开发文档创建、会议室预约两个应用，由同租户旗舰版服务账号代办，补充其他版本员工的使用入口；完成内网部署、授权维护及重启恢复验证。
- **项目成果：**实现飞书登录与日常协作脱离手机依赖，沟通及文档协作限于内部，受控文件发送纳入审批与留痕；通过 1 个旗舰版服务账号补充专业一线版员工的文档与会议室预约能力，减少不必要的全员升级需求。

AD 终端运维与安全巡检平台｜独立开发｜2026.06

- **建设背景：**设备配置、账号归属及策略执行信息分散在不同工具和人工台账中，资产盘点、策略核查与故障排查依赖逐台查询，异常设备难以集中识别。
- **平台建设：**独立开发域内终端巡检平台，定期汇总设备配置、在线状态、最近登录用户、策略执行及磁盘容量等信息，支持按部门、设备和异常筛选，并展示检查时间与采集状态。
- **项目成果：**将设备、账号与策略信息关联到统一页面，管理员可先筛选异常，再定位需要核查的终端及具体问题，减少多处取数、重复查表和逐台查询，为资产盘点、策略覆盖检查与故障定位提供依据。

观已设计数据加密项目｜项目负责人｜2024.07 - 2024.09

- **方案建设：**针对图纸和模型文件类型相对统一、无需区分敏感等级的特点，设计并部署基于 IP-guard 的透明加密方案，完成 AD 权限集成、文件外发审批、权限分级和操作审计。
- **项目结果：**完成 5 万+ 存量历史文件批量加密迁移，核心数据在 24 小时内完成切换，提升设计资料防护、权限控制和外发审计能力。

教育背景与资格证书

广州现代信息工程职业技术学院｜计算机网络技术｜专科｜2019.09 - 2022.06

HCIP（华为数通高级认证）｜局域网管理中级证书