物流配送管理系统 Windows 上线部署文档

Table of Contents

## 1 物流配送管理系统 Windows 上线部署文档

### 1.1 1. 背景与目标

* 将后端 API（Nest，端口 3000）与管理后台（Next，端口 3001）部署在老板的 Windows 电脑上。
* 对外提供 HTTPS 域名，供微信小程序和管理后台访问。
* 统一通过反向代理暴露 443 端口；关闭直连 3000、3001 的外网访问。

### 1.2 2. 架构与端口约定

* 后端 API：http://127.0.0.1:3000，全局前缀 /api，Swagger 也挂在 /api。
* 管理后台：http://127.0.0.1:3001。
* 静态上传：后端以 /receipts/uploads/... 暴露。
* 对外域名：https://yourdomain.com（必须 HTTPS，供小程序与后台共用）。
* 反向代理：将 /api 转到 3000，将 /admin 转到 3001，将 /receipts/uploads 透传到后端。

### 1.3 3. 前置准备清单

* 域名 1 个（如 yourdomain.com），解析到公网 IP。
* 路由器端口映射：外网 80、443 → Windows 电脑 80、443。
* Windows 电脑具有固定公网 IP，或通过 DDNS 稳定解析。
* 安装清单：
  + Node.js LTS（推荐 v20）
  + MySQL 8.0（本机实例）
  + 反向代理（推荐 Caddy，或 Nginx + win-acme）
  + NSSM 或 PM2 Windows Service（进程守护）
* 数据盘与目录（建议）：
  + 代码目录：D:\apps\dswl1
  + 上传目录：D:\logistics\uploads（通过环境变量指定）

### 1.4 4. 域名与 HTTPS（必须）

* DNS：把 yourdomain.com A 记录指向公网 IP。
* 路由器：映射外网 80、443 到 Windows 电脑 80、443。
* 反向代理选择：
  + 方案 A（推荐）：Caddy for Windows（自动签证书与续期）。
  + 方案 B：Nginx for Windows + win-acme（wacs.exe 一键签证书与续期）。
* 微信小程序后台“业务域名”配置（发布必需）：
  + request 合法域名：https://yourdomain.com
  + uploadFile 合法域名：https://yourdomain.com
  + downloadFile 合法域名：https://yourdomain.com
  + 注意：不能使用 IP、不能带端口、必须 443 且证书有效。

### 1.5 5. 反向代理配置（示例）

* Caddyfile（推荐）

yourdomain.com {  
 encode gzip  
  
 # API -> 3000  
 reverse\_proxy /api/\* 127.0.0.1:3000  
  
 # 管理后台 -> 3001（可使用二级路径 /admin）  
 reverse\_proxy /admin/\* 127.0.0.1:3001  
  
 # 静态上传透传给后端  
 reverse\_proxy /receipts/uploads/\* 127.0.0.1:3000  
}

* Nginx（Windows）

server {  
 listen 80;  
 server\_name yourdomain.com;  
 return 301 https://$host$request\_uri;  
}  
server {  
 listen 443 ssl http2;  
 server\_name yourdomain.com;  
 ssl\_certificate C:/path/to/fullchain.pem;  
 ssl\_certificate\_key C:/path/to/privkey.pem;  
  
 location /api/ {  
 proxy\_pass http://127.0.0.1:3000/;  
 proxy\_set\_header Host $host;  
 proxy\_set\_header X-Real-IP $remote\_addr;  
 proxy\_set\_header X-Forwarded-Proto $scheme;  
 }  
  
 location /admin/ {  
 proxy\_pass http://127.0.0.1:3001/;  
 proxy\_set\_header Host $host;  
 }  
  
 location /receipts/uploads/ {  
 proxy\_pass http://127.0.0.1:3000/receipts/uploads/;  
 }  
}

### 1.6 6. 数据库（MySQL 8.0）

* 安装 MySQL for Windows。
* 初始化
  + 创建数据库：logistics\_db（utf8mb4）。
  + 创建业务用户：logistics\_user（限制本机访问），授予数据库权限。
  + 导入项目根目录 init.sql。
* 推荐配置（my.ini）
  + character-set-server=utf8mb4，collation-server=utf8mb4\_unicode\_ci
  + default-time-zone=+08:00
  + 慢查询日志开启，合理设置 innodb\_buffer\_pool\_size

### 1.7 7. 后端部署（Nest，端口 3000）

* 进入 D:\apps\dswl1\backend-node
* 安装依赖与构建

npm install  
npm run build

* 生产环境变量（创建 .env）

PORT=3000  
NODE\_ENV=production  
DATABASE\_HOST=localhost  
DATABASE\_PORT=3306  
DATABASE\_USERNAME=logistics\_user  
DATABASE\_PASSWORD=强口令  
DATABASE\_NAME=logistics\_db  
JWT\_SECRET=强随机的JWT密钥  
MINIPROGRAM\_SIGNATURE\_KEY=生产签名密钥  
# 上传根目录（强烈建议显式指定到数据盘）  
UPLOAD\_ROOT\_PATH=D:\logistics\uploads

* 手动启动验证

node dist/main.js

* 注意：
  + 生产请通过反向代理访问，不要暴露 3000 给外网。
  + 走反代后可禁用 CORS 或保持默认（当前 main.ts 已开启 CORS 白名单；同域经反代不触发 CORS）。

### 1.8 8. 管理后台部署（Next，端口 3001）

* 进入 D:\apps\dswl1\admin-frontend
* 安装与构建

npm install  
npm run build  
npm run start # 端口 3001

* 重要提醒（必须确认再上线）：
  + 当前 admin-frontend/src/config/api.ts 在浏览器端会把 API 指向 protocol//hostname:3000，这在生产（仅开放 443）会失败。
  + 建议改为使用相对路径 /api 或读取 NEXT\_PUBLIC\_API\_BASE\_URL=https://yourdomain.com。若来不及改代码，请务必按建议调整后再上线，避免跨端口直连问题。

### 1.9 9. 文件上传与静态访问

* 通过 UPLOAD\_ROOT\_PATH 指定上传根目录，建议：D:\logistics\uploads。
* 后端将该目录通过 /receipts/uploads 暴露。
* 反向代理将 /receipts/uploads 透传给后端，无需单独映射物理目录。

### 1.10 10. 开机自启与进程守护

* 方案 A：NSSM（简单稳定）
  + 后端
    - Path: C:\Program Files\nodejs\node.exe
    - Startup directory: D:\apps\dswl1\backend-node
    - Arguments: dist/main.js
  + 管理后台
    - Path: C:\Program Files\nodejs\npm.cmd
    - Startup directory: D:\apps\dswl1\admin-frontend
    - Arguments: start
  + 设置自动重启、日志输出、依赖 MySQL 服务。
* 方案 B：PM2 Windows Service

npm install -g pm2 pm2-windows-service  
pm2-service-install -n "logistics-pm2"  
# 启动应用  
cd D:\apps\dswl1\backend-node && pm2 start dist/main.js --name logistics-backend  
cd D:\apps\dswl1\admin-frontend && pm2 start npm --name logistics-admin -- start  
pm2 save

### 1.11 11. 日志与监控

* 后端日志目录：工作目录上一级的 logs（确保以 backend-node 为工作目录启动）。
* 反向代理访问日志：Caddy/Nginx 默认开启。
* 健康检查：
  + 后端：GET https://yourdomain.com/api/health（如有调整）
  + API 文档：建议生产限制访问或关闭。

### 1.12 12. 备份与恢复（必须）

* 每日数据库备份（Windows 计划任务，示例 bat）

@echo off  
set BACKUP\_DIR=D:\backup\db  
if not exist %BACKUP\_DIR% mkdir %BACKUP\_DIR%  
for /f "tokens=1-3 delims=/- " %%a in ("%date%") do (set TS=%%a-%%b-%%c)  
"C:\Program Files\MySQL\MySQL Server 8.0\bin\mysqldump.exe" -ulogistics\_user -pYourPwd logistics\_db > %BACKUP\_DIR%\logistics\_db-%TS%.sql  
powershell -Command "Get-ChildItem %BACKUP\_DIR%\\*.sql | Where-Object {$\_.CreationTime -lt (Get-Date).AddDays(-14)} | Remove-Item"

* 每日上传目录备份（PowerShell 压缩）

$src="D:\logistics\uploads"  
$dst="D:\backup\uploads"  
$ts=Get-Date -Format yyyyMMdd  
if(!(Test-Path $dst)){New-Item -ItemType Directory -Path $dst | Out-Null}  
Compress-Archive -Path "$src\\*" -DestinationPath "$dst\uploads-$ts.zip" -Force  
Get-ChildItem $dst -Filter \*.zip | Where-Object {$\_.CreationTime -lt (Get-Date).AddDays(-30)} | Remove-Item

* 恢复演练：每次上线后抽样恢复一次，确保可用。

### 1.13 13. 小程序联调与发布配置

* 后端与反向代理必须已启用有效 HTTPS。
* 微信小程序后台设置三项“合法域名”为 https://yourdomain.com。
* 开发版可用内网/HTTP 调试，但发布版必须用 HTTPS 域名，不可用 IP/端口。

### 1.14 14. 安全加固

* 修改所有默认口令（MySQL、JWT、系统账号）。
* 对外仅开放 80/443；3000/3001 仅本机或内网。
* Swagger 文档对外关闭或加 IP 白名单/基本认证。
* Windows 防火墙仅放行 80/443；MySQL 限制本机访问。
* 备份加密与异地容灾；日志至少保留 90 天。

### 1.15 15. 上线验收清单

* 域名 80/443 可访问，证书有效。
* 小程序后台合法域名校验通过。
* https://yourdomain.com/api/health 返回 200。
* 管理后台登录与各页面接口请求成功。
* 上传/下载文件成功，/receipts/uploads/... 可访问。
* 数据库字符集/时区正确；慢查询日志生效。
* 日志持续写入；计划任务备份正常生成。
* 重启电脑后服务自动拉起。

### 1.16 16. 故障排查速查

* 端口占用：netstat -ano | findstr :3000、:3001、:80、:443
* 反代 502：检查本地服务是否启动、服务工作目录、证书是否有效。
* 小程序 403/跨域：确认走同域的 https://yourdomain.com，不要直连 3000/3001。
* 上传失败：确认 UPLOAD\_ROOT\_PATH 写权限与磁盘空间。
* 数据库连不上：检查 MySQL 服务、账号口令、my.ini 绑定地址。

### 1.17 17. 仅内网试运行（可选对比）

* 不做 HTTPS/域名与端口映射；同一内网通过 http://电脑IP:3001（后台）和 http://电脑IP:3000/api（接口）。
* 小程序只能开发版调试，不能发布上线。

### 1.18 18. 变更建议（上线前建议落实）

* 管理后台 admin-frontend/src/config/api.ts 改用相对路径 /api 或读取 NEXT\_PUBLIC\_API\_BASE\_URL=https://yourdomain.com，避免浏览器直连 :3000。
* 生产限制或关闭 Swagger UI。
* 后端 CORS 最终可精简/关闭（统一同域访问）。