Hệ Thống Nha Khoa
Nụ Cười Việt

NCV DCIMS

Vận hành, cài đặt và cập nhật

BẢN 0.2.30-r2

Tài liệu bàn giao • 30/09/2026

NAS hiện đã chạy ứng dụng 0.2.30. Bộ cài revision r2 và tài liệu bàn giao cho cấu trúc Volume 2. Chọn đúng hướng dẫn vận hành, cập nhật hoặc khởi động sau reboot; không nâng cấp lại chỉ để nhận tài liệu.

NCV DCIMS - NCV Dental Clinical Image Management System

Mục lục

Sao chép lệnh 4

Vận hành và bàn giao NCV DCIMS 0.2.30-r2 4

Chọn đúng hướng dẫn 4

Trạng thái đã xác nhận 4

Sơ đồ lưu trữ hiện tại 5

Database và công cụ vận hành của 0.2.30 5

Kiểm vận hành thường ngày 5

Thay đổi 0.2.30 cần bàn giao 6

Những điểm cần biết trong 0.2.30-r2 6

Kiểm chứng và phần còn phải nghiệm thu 7

Danh sách công việc mở 7

Cách đọc bộ bàn giao 7

Cài mới NCV DCIMS 0.2.30-r2 trên NAS riêng 8

Phạm vi, hiện trạng và điều kiện 8

Nhận source r2 và tạo cấu hình riêng 9

Ba credential DB, secret và quyền storage 10

Build, generator và preflight 10

DB trống → role → migrate 11

Seed/bootstrap Admin một lần, rồi provision lại 12

Activate, smoke và nghiệm thu owner 13

Nguồn kỹ thuật đi kèm 14

Phạm vi và những thứ giữ nguyên 15

Upload và đăng nhập đúng nơi 16

Kiểm ZIP và hiện trạng trước giải nén 17

Sao lưu rồi chép source r2 17

Tạo credential và tự cập nhật năm khóa .env 18

Cài revision adapter rồi update một lần 20

Kiểm sau cập nhật và UI 20

Các lỗi đã gặp và cách xử lý đúng 21

Sao chép lệnh

PDF có xuống dòng khi trình bày mã lệnh dài. Khi thực hiện, sao chép nguyên khối từ Markdown tương ứng trong 05_NGUON_TAI_LIEU; không ghép các dòng từ PDF.

Vận hành và bàn giao NCV DCIMS 0.2.30-r2

NCV DCIMS - NCV Dental Clinical Image Management System. Chốt tài liệu: 30/09/2026.

Chọn đúng hướng dẫn

Tình huống	Tài liệu / hành động
NAS hiện tại đang chạy bình thường	Bàn giao PDF theo vai trò, kiểm vận hành; không nâng cấp lại
NAS reboot bình thường / sau mất điện	07-KHOI-DONG-SAU-REBOOT-NAS.md và PDF Khởi động lại NAS
NAS còn 0.2.29, đúng topology V2	02-CAP-NHAT-NAS-VOLUME2.md; dùng đúng ZIP r2 và 5 khối NAS
NAS khác / cài mới	01-CAI-MOI-NAS-RIENG.md; không áp dụng adapter site V2 theo phỏng đoán
Cập nhật dang dở / image lỗi quyền	Đối chiếu stage và nhật ký xử lý quyền; không chạy lại toàn updater

Trạng thái đã xác nhận

Ứng dụng hiện tại **0.2.30**. Revision bộ cài **r2** sửa quyền đọc program workspace bên trong image để UID/GID NAS dùng pnpm/Prisma được. Bản r2 không đổi thêm TypeScript, giao diện hoặc SQL so với 0.2.30 trước hotfix quyền.

Operator ngày 30/09/2026 xác nhận: migration và provision role sau migration đạt; API/Web/Gateway healthy, đúng image; DSM Compose đồng bộ Volume 2; HTTPS smoke đạt; Dockerfile sửa quyền đã lưu trong source NAS; đăng nhập và giao diện bình thường. Đây là kết quả đã có trước đợt tạo tài liệu này. Không chạy lại updater, tạo credential hay overlay ZIP chỉ để nhận bộ bàn giao.

Sơ đồ lưu trữ hiện tại

Thành phần	Vị trí / giá trị đã chốt
Source project	/volume2/docker-v2/ncv-dcims-production
Công cụ vận hành site	/volume2/docker-v2/ncv-tools/dcims-v1
Project Compose	ncv-dcims-production
PostgreSQL	PostgreSQL 17; external volume ncv-dcims-postgres-data-v2
Device của volume database	/volume2/docker-v2/ncv-dcims-postgres-data-v2
Media mã hóa	/volume2/ncv-dcims/media
Ledger WriteOnce / WORM	/volume2/ncv-dcims-ledger-v2
Backup repository / receipts	/volume2/ncv-dcims/backup/repository và /volume2/ncv-dcims/backup/receipts
Backup khi cập nhật	/volume2/migration-backup
UID / GID ứng dụng	1044 / 65549
Docker Root / Container Manager	Giữ trên Volume 1, Docker Root /volume1/@docker

Gateway, tunnel, hostname và TLS tiếp tục dùng cấu hình riêng của site. Mẫu env dùng host/IP giả; không thay toàn bộ .env thật bằng mẫu. Docker mountpoint dưới Volume 1 không chứng minh dữ liệu DB ở Volume 1: phải kiểm Options.device của external volume.

Database và công cụ vận hành của 0.2.30

• Runtime: credential DML riêng cho API.

• Migration: credential owner riêng cho migration/bootstrap được kiểm soát.

• Backup: credential đọc riêng cho job backup.

• Administrator: file credential cũ được giữ riêng, chỉ mount vào maintenance job được gọi rõ ràng.

Không dùng chung URL quản trị làm runtime. Không in hay gửi các file credential. Giữ đúng quyền được updater thiết lập; hotfix r2 sửa quyền mã chương trình trong image, không chmod toàn shared folder hoặc secrets.

Adapter dcims-security-update và installer install-dcims-security-update.sh cung cấp guard cho layout credential mới cùng DSM sync. Payload công cụ Volume 2 cũ vẫn được giữ để đối chiếu nguồn; không chạy lại installer Volume 2 gốc trên site đã nâng cấp. NAS hiện tại đã cài revision adapter phù hợp.

Kiểm vận hành thường ngày

1. Mở website HTTPS do quản trị cung cấp, đăng nhập bằng tài khoản riêng.

2. Kiểm đúng phạm vi dữ liệu; tìm hồ sơ, đổi trang và mở ảnh/hợp đồng theo quyền.

3. Người vận hành đối chiếu PostgreSQL/API/Web/Gateway healthy; tunnel running.

4. Khi có lỗi, ghi thời điểm, service, request ID và bước đã làm. Chỉ gửi log đã che thông tin nhạy cảm.

5. Dùng PDF riêng sau reboot. Nếu share mã hóa chưa mount, mở khóa trong DSM trước khi start ứng dụng.

Thay đổi 0.2.30 cần bàn giao

Những điểm cần biết trong 0.2.30-r2

Ứng dụng là **0.2.30**; **r2** là revision bộ cài sửa quyền đọc mã chương trình trong image NAS. Tài liệu chốt ngày **30/09/2026**. NAS hiện tại đã cập nhật và đăng nhập bình thường; nhận tài liệu này không cần chạy cập nhật lại.

• Danh sách bệnh nhân lấy dữ liệu từ server, **25 hồ sơ mỗi trang**. Xem tổng số hồ sơ, dùng nút trang trước/trang sau; không kết luận bệnh nhân không tồn tại chỉ vì chưa thấy ở trang hiện tại. Tìm kiếm, lọc và sắp xếp áp dụng trên toàn bộ phạm vi được phép. Các số ca/cần bổ sung trong trang phản ánh trang hiện tại; tổng hồ sơ phản ánh kết quả tìm/lọc.

• Khi chọn đồng thời Bác sĩ và Dịch vụ, kết quả phải có **cùng một ca điều trị** thỏa cả hai điều kiện. Muốn tìm ca khác, điều chỉnh bộ lọc thay vì mở rộng quyền tài khoản.

• Back/Forward khôi phục hồ sơ đã mở kể cả khi hồ sơ không ở trang danh sách hiện tại; quyền truy cập vẫn được kiểm lại.

• Xóa ca điều trị sẽ thu hồi các link chia sẻ của ca. **Khôi phục ca không phục hồi link cũ**; người có quyền phải tạo link mới và gửi lại cho người nhận được phép.

• Nếu đăng nhập báo quá nhiều yêu cầu, chờ rồi thử lại; không bấm liên tục hoặc mở nhiều phiên đăng nhập cùng lúc.

• Trong Cài đặt, tiêu đề các khối không còn icon đứng trước. Icon trên menu và các nút vẫn được giữ. Các quyền nghiệp vụ của ADMIN, DOCTOR, LABO không đổi.

Ảnh trong PDF được chụp lại từ frontend build 0.2.30 ngày 30/09/2026, API mô phỏng và dữ liệu giả. Ảnh minh họa cách thao tác; không chứng nhận ghi dữ liệu, authorization hay UAT trên NAS.

Kiểm chứng và phần còn phải nghiệm thu

Phạm vi	Kết quả / giới hạn
Kiểm sản phẩm trước hotfix quyền, ngày 30/09	Lint, type-check, build, unit: 688 pass / 0 fail / 1 skip; PostgreSQL 17.10 DB trống 47 migration và seed, integration và kiểm responsive 390/768/1440 đạt theo evidence
Hướng dẫn r2 và ZIP	5 khối NAS kiểm syntax; 12 fixture source/env; 15 contract test; CRC/checksum/source receipt đạt
NAS đang dùng	Migration, role, health, image, DSM sync, HTTPS smoke, source Dockerfile hash và đăng nhập/giao diện được operator xác nhận
Full Docker build local sau hotfix quyền	Chưa chạy lại từ đầu: Docker engine unavailable / WSL access denied; NAS đã kiểm image candidate với cùng logic sửa quyền
Reboot, auto-mount, scheduler enabled	Chưa có diễn tập / xác nhận mới trong đợt này
Offsite, NAS full restore / DR	Chưa chứng nhận; dump parse và restore test DB không thay diễn tập khôi phục toàn bộ NAS
UAT nghiệp vụ trên NAS	Đăng nhập/giao diện bình thường chưa chứng minh toàn bộ role/scope/share/upload/confirm/reopen

Xem KET_QUA_KIEM_CHUNG.md và BIEN_BAN_NGHIEM_THU.md trong 04_KIEM_CHUNG. Các phiếu nghiệm thu là biểu mẫu trống, không phải biên bản đã ký.

Danh sách công việc mở

Công việc	Owner	Ưu tiên	Điều kiện đóng
Diễn tập reboot và xác nhận auto-mount	Quản trị NAS	P1	Ghi kết quả theo PDF reboot, khóa được lưu theo chính sách được duyệt
UAT mọi vai trò và scope trên NAS	Chủ hệ thống / quản trị ứng dụng	P1	Dữ liệu giả, tài khoản được phép, ghi từng luồng và kết quả
Offsite / full restore / DR	Chủ hệ thống / phụ trách backup	P1	Chính sách được duyệt, recovery key và diễn tập có bằng chứng
Fresh Docker build r2 từ đầu	Phụ trách kỹ thuật	P2	Engine sẵn sàng, build sạch và probe UID thực đạt

Bộ bàn giao này không thay retention, legal hold, data scope, auto-mount hoặc cấu hình đang chạy. Không cần làm các công việc mở chỉ để mở PDF.

Cách đọc bộ bàn giao

Mở MO_DANH_MUC.html hoặc index.html. Bộ cài ở 01_BO_CAI, PDF vận hành ở 02_HUONG_DAN_CAP_NHAT, ba PDF người dùng ở 03_PDF_THEO_VAI_TRO; kiểm chứng, nguồn tài liệu và ảnh nằm ở ba thư mục còn lại. Mọi liên kết danh mục mở tab mới. Trang dùng logo/font cục bộ, có thể mở offline.

Nếu đưa lên hosting, giữ nguyên đường dẫn tương đối giữa HTML và các thư mục. Danh mục đầy đủ chứa bộ cài/source và thông tin vận hành NAS: chỉ cấp truy cập cho người được phép. Trang tài liệu công khai chỉ nên chứa PDF người dùng và tài sản giao diện đã chọn. Chưa thực hiện upload hoặc đổi hosting trong đợt này.

Cài mới NCV DCIMS 0.2.30-r2 trên NAS riêng

NCV DCIMS - NCV Dental Clinical Image Management System. Tài liệu kỹ thuật cập nhật ngày 30/09/2026. `r2` là revision **bộ cài**; phiên bản ứng dụng/tag image là `0.2.30`.

Phạm vi, hiện trạng và điều kiện

Chỉ áp dụng cho NAS riêng chưa có NCV DCIMS, storage mới và **database trống**. Đây là hướng dẫn cho operator, không phải biên bản đã triển khai.

NAS hiện tại đã chạy 0.2.30, migration/role/activation/DSM sync/HTTPS smoke và đăng nhập/giao diện đã được operator xác nhận ngày 30/09. **Không cài mới hoặc chạy lại updater trên NAS đó để nhận r2.** Đối chiếu README, guide cập nhật r2 và phần chốt cuối evidence. Một số đoạn trước đó trong nguồn là lịch sử trước khi NAS cập nhật xong.

Evidence ghi 47 migration và seed đạt trên PostgreSQL 17.10 trống bằng migration role; role denial/IDOR và dump bằng backup role đã kiểm trong môi trường giả lập. **Chưa có bằng chứng cài trắng/full rebuild Dockerfile r2 trên NAS mới**; NAS hiện hữu đã kiểm image ứng viên sửa quyền, không tương đương full rebuild. DR/offsite/reboot và UAT NAS mới còn phải nghiệm thu.

Operator chuẩn bị Container Manager/Docker Engine/Compose, CPU tương thích base images, DNS/NTP, dung lượng build/dữ liệu và truy cập registry/package registry. ZIP chứa source/Compose, không kèm image offline, credential hoặc database.

Owner NAS/chủ hệ thống chốt root storage, UID/GID, ACL/mã hóa, hostname/TLS/ingress và người nhận Admin. Policy retention/legal hold, offsite/custody khóa, quyền ngoài hệ thống hoặc restore cần owner xác nhận **khi triển khai thực**, theo assumptions. Viết tài liệu không phê duyệt hoặc thực hiện các quyết định đó.

Dùng placeholder `<project-root>`, `<media-root>`, `<ledger-root>`, `<repository-root>`, `<receipts-root>`, `<runtime-uid>`, `<runtime-gid>` và tham số mạng của NAS đích. Thay trước khi chạy. Roots là đường dẫn tuyệt đối, không PII; source, media, ledger, repository, receipts không chồng lấn. Ledger tách khỏi DB/media; WORM/WriteOnce do owner storage xác nhận.

Topology cần hiểu đúng: Compose certified dùng named volume PostgreSQL `ncv-dcims-postgres-data`; vị trí phụ thuộc Docker Root, không tự nằm trên Volume 2. `.env` không có biến host path DB. Nếu cần mount DB khác, owner thiết kế/kiểm override trước init; lệnh base dưới đây không đáp ứng yêu cầu đó tự động. Container/network/volume có tên cố định; đổi project name không đủ cô lập chúng.

Trước lần up đầu tiên, kiểm chỉ đọc:

```
docker ps -a --filter name=ncv-dcims --format 'table {{.Names}}\t{{.Image}}\t{{.Status}}'
docker volume ls --filter name=ncv-dcims
docker network ls --filter name=ncv-dcims
```

Nếu đã có tên trùng hoặc dữ liệu chưa rõ nguồn gốc, dừng đối chiếu; không xóa để tiếp tục. Không dùng adapter `deploy/site/nas-volume2`, `dcims.sh update`, override/DSM helper của site hiện hữu làm

installer NAS bất kỳ, hoặc thay hash/UUID để vượt guard.

Nhận source r2 và tạo cấu hình riêng

Trên Windows, đối chiếu hash ZIP với sidecar:

```
Get-FileHash -Algorithm SHA256 .\ncv-dcims-production-0.2.30-complete-synology-r2.zip
Get-Content .\ncv-dcims-production-0.2.30-complete-synology-r2.zip.sha256.txt
```

Upload staging riêng tư; giải nén bằng File Station nếu NAS không có `unzip`. Đặt source vào `<project-root>` mới, không đè project hiện hữu. Root phải có trực tiếp `package.json`, `apps`, `deploy`, `scripts`, Compose và mẫu env. Manifest root/API/Web cùng ghi `0.2.30`. Dockerfile r2 sửa quyền đọc/traverse **program trong image**, không sửa quyền host data.

Sao chép mẫu production root thành `.env` tại project mới. Mẫu còn có path Volume 2 và host/IP minh họa: phải thay theo NAS đích. Không dùng env thật của NAS hiện tại hoặc guide credential một URL của 0.2.29. Những khóa chính cần đối chiếu:

```
NCV_DCIMS_APP_VERSION=0.2.30
NCV_DCIMS_PUBLIC_HOST=<public-host>
NCV_DCIMS_ALLOWED_HOSTS=<danh-sach-host-chinh-xac-co-public-host>
NCV_DCIMS_CLOUDFLARED_TRUSTED_IP=<mot-ipv4-peer-ingress-duoc-tin>
NCV_DCIMS_CORS_ORIGINS=<danh-sach-origin-https-chinh-xac>
NCV_DCIMS_GATEWAY_BIND_IP=<bind-ip-da-duyet>
NCV_DCIMS_HTTP_PORT=<http-port>
NCV_DCIMS_HTTPS_PORT=<https-port>
NCV_DCIMS_POSTGRES_DB=ncv_dcims
NCV_DCIMS_POSTGRES_USER=ncv_dcims_app
NCV_DCIMS_RUNTIME_UID=<runtime-uid>
NCV_DCIMS_RUNTIME_GID=<runtime-gid>
NCV_DCIMS_DB_ADMIN_URL_FILE=./secrets/database-url.txt
NCV_DCIMS_DATABASE_URL_FILE=./secrets/runtime-database-url.txt
NCV_DCIMS_MIGRATION_DATABASE_URL_FILE=./secrets/migration-database-url.txt
NCV_DCIMS_BACKUP_DATABASE_URL_FILE=./secrets/backup-database-url.txt
NCV_DCIMS_NAS_MEDIA_ROOT=<media-root>
NCV_DCIMS_NAS_LEDGER_ROOT=<ledger-root>
NCV_DCIMS_NAS_BACKUP_REPOSITORY_ROOT=<repository-root>
NCV_DCIMS_NAS_BACKUP_RECEIPTS_ROOT=<receipts-root>
NCV_DCIMS_BACKUP_ENCRYPTION_KEY_ID=<id-khoa-khong-phai-secret>
```

Giữ các khóa đường dẫn password/TLS/share secret/receipt key từ mẫu; chuẩn bị file tương ứng ở mục 3. Mỗi khóa xuất hiện một lần. Giữ **false** cho ba cờ `BACKUP_OFFSITE_CONFIGURED`, `BACKUP_POLICY_APPROVED`, `BACKUP_RECOVERY_KEY_TESTED`, ba cờ `MEDIA_PURGE_SCHEDULER_ENABLED`, `MEDIA_PURGE_EXECUTION_ENABLED`, `MEDIA_PURGE_LEGAL_HOLD_CLEAR_CONFIRMED` và `EXTERNAL_API_ENABLED` cho tới khi owner thực sự hoàn thành/xác nhận điều kiện tương ứng (tên đầy đủ có prefix `NCV_DCIMS_`).

Init user `ncv_dcims_app` trong mẫu là **quản trị PostgreSQL của DB mới**, không phải role runtime dù tên có chữ `app`. Có thể chọn tên khác trước init nhưng phải khớp admin URL/password; sửa env sau khi volume có dữ liệu không tự đổi user/password DB.

Host không có scheme/port; CORS dùng origin đầy đủ, có port nếu cần, không path/slash cuối. Renderer Gateway bắt buộc đúng một trusted IPv4 ngay cả khi không dùng Cloudflare; owner mạng đối chiếu renderer, không điền IP giả để qua validation. Compose không tạo tunnel hoặc reverse proxy DSM.

Ba credential DB, secret và quyền storage

Tạo `secrets/` riêng tư tại project. Không ghi giá trị secret vào env, command line, log, screenshot, source hoặc PDF. Các file theo mẫu root:

File trong `secrets/`	Consumer / yêu cầu
`postgres-password.txt`	Password init user, nguyên văn
`database-url.txt`	Admin URL, khớp init user/password/database
`runtime-database-url.txt`	Role `ncv_dcims_runtime`: DML, API
`migration-database-url.txt`	Role `ncv_dcims_migration`: owner schema/objects, migrate/seed/bootstrap
`backup-database-url.txt`	Role `ncv_dcims_backup`: đọc DB cho dump
`media-share-token-secret.txt`	Secret độc lập, ngẫu nhiên mạnh, tối thiểu 32 byte
`tls-certificate.pem`, `tls-private-key.pem`	Cặp TLS hợp lệ cho hostname đích
`backup-receipt-private-key.pem`, `backup-receipt-public-key.pem`	Ed25519 ký/xác minh receipt, không mã hóa dữ liệu
`bootstrap-admin-password.txt`	Password Admin tạm, chỉ cho bootstrap một lần

Cấu trúc admin URL, chỉ là placeholder:

```
postgresql://<init-user>:<password-percent-encode>@ncv-dcims-
postgres:5432/ncv_dcims?schema=ncv_dcims
```

Ba role URL cùng host/port/database/schema, username đúng bảng trên; password khác nhau và khác admin. Password trong URL percent-encode; file PostgreSQL password vẫn nguyên văn. Generator mục 4 tạo ba URL từ admin URL, chưa tạo role trong DB.

Receipt keys: trên máy tin cậy có Node, tại root source, chọn thư mục tuyệt đối mới/rỗng:

```
$env:NCV_DCIMS_BACKUP_KEY_OUTPUT_ROOT='<thu-muc-tuyet-doi-moi-hoac-rong>'
node scripts/generate-backup-receipt-keys.mjs --generate
```

Công cụ tạo `receipt-private.pem`/`receipt-public.pem`; chuyển an toàn và đặt đúng tên trong bảng. Private signing key chỉ mount vào backup, API chỉ nhận public key. Mã hóa backup/offsite/recovery key vẫn phải cấu hình riêng. Password Admin: 12-128 ký tự, không chỉ khoảng trắng hoặc ký tự điều khiển.

Owner storage xác nhận share thật đang mount/mở khóa và quyền UID/GID. API ghi media; backup đọc media/ledger, ghi repository/receipts. Gateway chạy `101:101`, cần đọc TLS. Secret-init chỉ chỉnh bảy file được chỉ định trong Compose, không xử lý TLS, PostgreSQL password hoặc bootstrap password. Operator chuẩn bị quyền đọc tối thiểu cho các consumer này; bootstrap password không có group/other write. Không chmod 777 hoặc chown/chmod đệ quy ledger WORM.

Build, generator và preflight

SSH vào **NAS đích**, dùng shell có quyền Docker (`sudo sh` nếu cần). Khai báo trong cùng shell; mất SSH thì khai báo lại và kiểm bước đã đạt trước tiếp tục:

```
set -eu
umask 077
```

```
DCIMS_PROJECT='<project-root>'
cd "$DCIMS_PROJECT"
dcims_compose() {
  docker compose --project-name ncv-dcims-production \
    --project-directory "$DCIMS_PROJECT" --env-file "$DCIMS_PROJECT/.env" \
    -f "$DCIMS_PROJECT/compose.production.certified.yml" "$@"
}
dcims_compose --profile maintenance build ncv-dcims-api ncv-dcims-web ncv-dcims-migrate
dcims_compose --profile backup build ncv-dcims-backup
```

Đây là lệnh theo build target/service của source; chưa chứng nhận full build NAS mới. Giữ Dockerfile r2/pnpm/lockfile. Nếu build lỗi, dừng, không build song song hoặc đổi API sang root để sửa EACCES.

Khi admin URL đã có và cả ba role file **chưa tồn tại**, dùng generator từ guide r2 đã tham số hóa đường dẫn:

```
DCIMS_ADMIN_FILE="$DCIMS_PROJECT/secrets/database-url.txt"
docker run --rm --network none --user 0:0 --entrypoint node \
  --mount "type=bind,src=$DCIMS_ADMIN_FILE,dst=/old-admin-url,readonly" \
  --mount "type=bind,src=$DCIMS_PROJECT/secrets,dst=/role-secrets" \
  ncv-dcims-api-migration:0.2.30 dist/scripts/generate-database-role-secrets.js \
  --admin-url-file /old-admin-url --output-directory /role-secrets </dev/null
```

Đạt `DB_ROLE_SECRET_FILES_CREATED`; generator không kết nối DB, không in giá trị, từ chối ghi đè. Lỗi/partial files: giữ trạng thái, không xóa/sinh lại theo phỏng đoán.

```
dcims_compose config --quiet
dcims_compose run --rm -T --no-deps ncv-dcims-secret-init </dev/null
```

Cả hai phải exit 0. `config` không xác minh nội dung secret/TLS/quyền mount. Nếu media/ledger đều mới/rỗng, chưa khóa WORM và owner chấp nhận cơ chế quyền của job, có thể chạy:

```
dcims_compose run --rm -T --no-deps ncv-dcims-storage-init </dev/null
```

Job đổi owner/quyền thư mục media/ledger; không chạy trên ledger WORM hiện hữu. Nếu site dùng ACL riêng, owner chuẩn bị/kiểm quyền thay cho job. Repository/receipts phải chuẩn bị riêng, storage-init không xử lý hai root đó.

DB trống → role → migrate

Theo deployment hiện hành, không bật API/Web/Gateway trước khi hoàn tất bootstrap và provision lần hai. Sau khi xác minh volume mới và không xung đột tên:

```
dcims_compose up -d ncv-dcims-postgres
docker inspect --format '{{.State.Running}}|{{.State.Health.Status}}' ncv-dcims-postgres
```

Chờ `true|healthy`; health không chứng minh credential role đúng. Chạy từng lệnh, chỉ tiếp tục khi lệnh trước exit 0:

```
dcims_compose run --rm -T --no-deps ncv-dcims-db-roles </dev/null
dcims_compose run --rm -T --no-deps ncv-dcims-migrate </dev/null
```

Role job phải có `DB_ROLES_PROVISIONED`; migration phải `migrate deploy` thành công. Provisioning dùng admin URL trong **job maintenance riêng**, tạo ba role hạn quyền và schema `ncv_dcims`. API không dùng admin; migrate chỉ dùng migration URL; backup chỉ dùng backup URL. Secret-init có bind admin file để đổi quyền, không có network và không quản trị DB.

Source có 47 migration, gồm bootstrap nguồn checklist còn thiếu trên DB trống; không bỏ/sửa migration lịch sử. Lỗi thì giữ trạng thái và dừng; không reset/resolve thủ công hoặc seed để che lỗi. Sau migrate vẫn chưa có Admin ứng dụng. Admin ứng dụng khác admin PostgreSQL.

Seed/bootstrap Admin một lần, rồi provision lại

Vướng mắc source: Compose bootstrap đặt production nhưng thiếu share secret/CORS/quarantine; bootstrap-admin.ts gọi config yêu cầu cả ba. Job cũng chưa đặt UID/GID site. **Compose bootstrap gốc chưa được chứng nhận chạy đạt trên NAS mới.** Không chạy nguyên trạng hoặc đổi sang development để bỏ validation.

Tại NAS đích, tạo `.env.bootstrap-admin` riêng tư; không thay `.env` production. Mẫu root có path Volume 2 cần thay. Nội dung đối chiếu:

```
NCV_DCIMS_APP_VERSION=0.2.30
NCV_DCIMS_RUNTIME_UID=<runtime-uid>
NCV_DCIMS_RUNTIME_GID=<runtime-gid>
NCV_DCIMS_BOOTSTRAP_ADMIN_USERNAME=admin
NCV_DCIMS_BOOTSTRAP_ADMIN_FULL_NAME=<ten-admin-owner-chon>
NCV_DCIMS_DATABASE_URL_FILE=./secrets/migration-database-url.txt
NCV_DCIMS_BOOTSTRAP_ADMIN_PASSWORD_FILE=./secrets/bootstrap-admin-password.txt
NCV_DCIMS_MEDIA_SHARE_TOKEN_SECRET_FILE=./secrets/media-share-token-secret.txt
NCV_DCIMS_CORS_ORIGINS=<cung-origin-https-trong-env-production>
```

Trong env bootstrap, `DATABASE_URL_FILE` **trỏ migration; trong env production, khóa này trỏ runtime.** Không dùng admin URL cho bootstrap. Chuẩn bị bootstrap password file đọc được bởi UID/GID đích; secret-init không sửa nó.

Tạo `compose.bootstrap-admin.local.yml` tại NAS, cạnh Compose gốc. Mẫu bổ sung suy ra từ source, đã kiểm cấu trúc merge, **chưa chạy bootstrap trên NAS mới**:

```
services:
  ncv-dcims-bootstrap-admin:
    user: "${NCV_DCIMS_RUNTIME_UID:?Set UID}:${NCV_DCIMS_RUNTIME_GID:?Set GID}"
    environment:
      NCV_DCIMS_CORS_ORIGINS: ${NCV_DCIMS_CORS_ORIGINS:?Set CORS}
      NCV_DCIMS_MEDIA_SHARE_TOKEN_SECRET_FILE:
/run/secrets/ncv_dcims_media_share_token_secret
      NCV_DCIMS_MEDIA_QUARANTINE_ROOT: /var/lib/ncv-dcims/media/quarantine
    secrets:
      - ncv_dcims_media_share_token_secret
secrets:
  ncv_dcims_media_share_token_secret:
    file: ${NCV_DCIMS_MEDIA_SHARE_TOKEN_SECRET_FILE:?Set share secret file}
```

Quarantine ở đây là tham số validation, bootstrap không upload/mount media. Entrypoint đọc DB/share secret vào process. Trong cùng shell NAS:

```
dcims_bootstrap() {
  docker compose --project-name ncv-dcims-bootstrap-admin \
    --project-directory "$DCIMS_PROJECT" \
    --env-file "$DCIMS_PROJECT/.env.bootstrap-admin" \
    -f "$DCIMS_PROJECT/compose.bootstrap-admin.synology.yml" \
    -f "$DCIMS_PROJECT/compose.bootstrap-admin.local.yml" "$@"
}
dcims_bootstrap config --quiet
dcims_bootstrap run --rm -T --no-deps ncv-dcims-bootstrap-admin </dev/null
```

Job chạy `pnpm db:seed` rồi `pnpm db:bootstrap-admin`, bằng migration credential. Seed tạo permission/ba system role/checklist, mặc định không tạo user/bệnh nhân demo. Bootstrap chỉ tạo Admin khi chưa có user, ghi audit và bắt đổi password lần đầu. Đạt: exit 0 và thông báo tạo Admin.

Nếu seed đạt/bootstrap lỗi, kiểm config/password và trạng thái user trước chọn thao tác tiếp; không lặp theo phỏng đoán. Không chạy seed/bootstrap hoặc bootstrap-test-accounts trên DB vận hành.

Bắt buộc provision lần hai sau seed/bootstrap, trước API:

```
dcims_compose run --rm -T --no-deps ncv-dcims-db-roles </dev/null
```

Phải có `DB_ROLES_PROVISIONED`. Khi các bảng đã có, bước này chặn runtime đọc `_prisma_migrations` và UPDATE/DELETE `audit_logs`; runtime giữ DML nghiệp vụ, migration sở hữu objects, backup chỉ đọc.

Activate, smoke và nghiệm thu owner

Sau PostgreSQL healthy, migration/bootstrap/provision lần hai đạt, mount/quyền đúng:

```
dcims_compose up -d --no-build --pull never --no-deps ncv-dcims-api ncv-dcims-web ncv-dcims-
gateway
dcims_compose ps
sh scripts/synology/ncv-dcims-post-update-smoke-test.sh 'https://<host>[:<port-neu-can>]'
0.2.30 </dev/null
```

Thay URL placeholder toàn bộ. Bốn service PostgreSQL/API/Web/Gateway phải healthy, API/Web đúng tag `:0.2.30`. Owner cấu hình DNS/TLS/ingress; chỉ Gateway public. Internal healthcheck bỏ kiểm certificate, không thay smoke HTTPS có kiểm TLS. Smoke phải có `NCV_DCIMS_POST_UPDATE_SMOKE_OK`; kiểm health/header/title/auth boundary/Swagger-version bị chặn, không so phiên bản public hoặc chứng minh image đúng.

Đăng nhập Admin và đổi password. Owner UAT nghiệm thu bằng dữ liệu giả: ba vai trò, scope/IDOR chéo user/branch/patient/case, upload đúng/sai định dạng, private ảnh/PDF, confirm/reopen, chia sẻ/thu hồi, phân trang/tìm/lọc/Back-Forward và responsive 390/768/1440. Không dùng bệnh nhân thật hoặc xóa ca thật để thử. Runtime không có antivirus scanner; vẫn có quarantine/MIME/signature/decode/PDF validation.

Backup: theo backup/restore, lịch hiện có 02:00 `Asia/Ho_Chi_Minh`, retention 60 ngày; không tự đổi policy. Compose backup là job một lượt, không tự tạo lịch. Owner phải cấu hình lịch/mã hóa/offsite/custody và kiểm recovery, rồi mới xác nhận các cờ backup tương ứng. Lệnh dưới chỉ dùng khi các điều kiện đã được owner xác nhận:

```
dcims_compose --profile backup run --rm -T --no-deps ncv-dcims-backup </dev/null
```

Lệnh thực sự tạo backup/receipt và có thể rotation; không phải preflight chỉ đọc. Dump parse/checksum không thay restore DB **cùng media** cô lập. Purge/External API giữ tắt trong quy trình này; bật là quyết định riêng.

Owner storage kiểm ACL/WORM, mount share mã hóa, startup guard và reboot có kiểm soát trước dùng dữ liệu thật. Không coi helper site cũ đã cài trên NAS mới; `restart: unless-stopped` có thể chạy trước khi share mount. Startup guard có path/số container lịch sử cần đối chiếu, không chép mù hoặc tạo marker trên fallback folder để vượt lỗi.

Việc cần owner đóng	Owner / ưu tiên / bằng chứng
NAS/storage/volume/UID/GID/build/guard	Owner NAS + storage / P0: full build r2, mount/quyền, vị trí DB và reboot trên NAS đích
TLS/ingress/private endpoints	Owner mạng / P0: HTTPS smoke, trusted peer và firewall đúng topology
Backup/retention/hold/offsite/recovery/restore	Chủ hệ thống + owner backup / P0 trước dữ liệu thật: policy xác nhận và restore DB-media cô lập

Việc cần owner đóng	Owner / ưu tiên / bằng chứng
UAT vai trò/scope/responsive	Owner UAT / P0: biên bản dữ liệu giả, 390/768/1440 và nghiệp vụ

Bất kỳ bước lỗi: dừng phụ thuộc, giữ bước cuối/output đã loại secret. Không `down -v`, Delete/Clean, prune, reset DB hoặc chmod/chown hàng loạt. Rollback/restore sau thay role/schema cần chủ hệ thống duyệt phương án khi triển khai thực.

Kiểm lượt viết guide: Compose certified và merge bootstrap `config --quiet` đạt với tham số giả; nguồn có 47 migration. **Chưa chạy** lint/type-check/unit/integration/build/E2E hay cài NAS mới: chỉ sửa tài liệu. Evidence release là kết quả lượt kiểm trước, không chứng nhận cài mới. Tài liệu bàn giao không thay biên bản nghiệm thu triển khai.

Nguồn kỹ thuật đi kèm

Guide có ở 02_HUONG_DAN_CAP_NHAT và 05_NGUON_TAI_LIEU. Các nguồn trực tiếp đã được kèm trong `05_NGUON_TAI_LIEU/technical/`, giữ đường dẫn từ root. Bảng dưới chỉ ra các nguồn chính; `04_KIEM_CHUNG/NGUON_THAM_CHIEU.json` ghi đầy đủ file, SHA-256 và nguồn lấy từ installer r2 hoặc snapshot tài liệu kỹ thuật ngày 30/09/2026.

Source từ root repository	Mục đích
`README.md`	Hiện trạng NAS
`docs/assumptions.md`	Policy/owner/giới hạn
`docs/production-deployment.md`	Thứ tự cài mới hiện hành; không có `docs/operations/deployment-production.md` trong nguồn đã đọc
`docs/operations/synology-update-0.2.30.md`	Guide r2/generator/site boundary
`docs/evidence/release-0.2.30-verification-2026-09-30.md`	DB trống/role/NAS/giới hạn
`docs/backup-restore.md`	Backup/retention/restore
`docs/operations/synology-storage-startup-guard.md`	Guard cần đối chiếu site
`.env.production.example`	Mẫu root, không secret thật
`.env.bootstrap-admin.example`	Bootstrap root, thay path
`compose.production.certified.yml`	Service/job/secret/volume
`compose.bootstrap-admin.synology.yml`	Seed/bootstrap gốc
`deploy/docker/api.Dockerfile`	Image API/migration r2
`deploy/docker/load-database-secret.sh`	Entrypoint DB/share secret
`deploy/gateway/render-nginx-config.sh`	Host/trusted IPv4
`apps/api/scripts/generate-database-role-secrets.ts`	Sinh ba credential
`apps/api/scripts/provision-database-roles.ts`	Role/grants/revokes

Source từ root repository	Mục đích
`apps/api/prisma/seed.ts`	Seed hệ thống
`apps/api/prisma/bootstrap-admin.ts`	Admin một lần
`apps/api/src/config.ts`	Production validation
`scripts/generate-backup-receipt-keys.mjs`	Ed25519 receipt keys
`scripts/synology/ncv-dcims-post-update-smoke-test.sh`	HTTPS smoke
`apps/api/src/auth/password-policy.ts`	Password policy
`scripts/run-backup-scheduler.mjs`	Scheduler riêng
`deploy/docker/backup.Dockerfile`	Backup một lượt

Đã kèm các nguồn tham chiếu theo cấu trúc trên. Source tham chiếu không thay installer đầy đủ để build/chạy; liên kết phụ bên trong source có thể cần checkout đầy đủ. Giữ nguyên các tài liệu 0.2.29/lịch sử.

NCV DCIMS - NCV Dental Clinical Image Management System: cập nhật 0.2.29 → 0.2.30 bằng bộ r2

Ngày 30/09/2026 - hướng dẫn chính của bộ r2. r2 giữ phiên bản ứng dụng 0.2.30, sửa quyền đọc mã chương trình trong image API/migration và tổng hợp kinh nghiệm cập nhật NAS thực tế. Không đổi TypeScript/UI/SQL/Compose hoặc payload Volume 2 lịch sử so với r1.

NAS hiện tại của chủ hệ thống đã xong: migration, provision lại role, API/Web/Gateway healthy, DSM sync Volume 2, HTTPS smoke, Dockerfile source sửa quyền và đăng nhập/giao diện bình thường đều đã được xác nhận. **Không chạy các bước nâng cấp dưới đây lại trên NAS này.** Giữ bộ r2 cho lần build sau và bàn giao. Đây là hướng dẫn cập nhật site còn ở 0.2.29, không phải cài trắng hoặc chuyển volume.

Phạm vi và những thứ giữ nguyên

Theo task **Di chuyển share folder sang Volume 2** chốt 15/09 và hướng dẫn 0.2.25/0.2.27/0.2.28/0.2.29, dùng đúng topology sau. Nếu khác, dừng đối chiếu; không tự sửa hash/layout/UUID để vượt guard.

Thành phần	Giữ nguyên
Project Container Manager	`ncv-dcims-production`, không tạo project mới
Source project	`/volume2/docker-v2/ncv-dcims-production`
Công cụ site/DSM sync	`/volume2/docker-v2/ncv-tools/dcims-v1`
PostgreSQL	17; volume ngoài `ncv-dcims-postgres-data-v2`; device `/volume2/docker-v2/ncv-dcims-postgres-data-v2`
Media	`/volume2/ncv-dcims/media`
Ledger WORM	`/volume2/ncv-dcims-ledger-v2`

Thành phần	Giữ nguyên
Backup ứng dụng	`/volume2/ncv-dcims/backup/repository`, receipts `/volume2/ncv-dcims/backup/receipts`
Sao lưu trước nâng cấp	Shared folder riêng tư `/volume2/migration-backup`
Docker Root / Container Manager	Volume 1; không move `/volume1/@docker` hoặc package
Domain/TLS/Cloudflare/IMS	Không đổi domain, TLS, trusted IP, tunnel hoặc IMS
Quyền/chính sách dữ liệu	Giữ UID/GID, secret chia sẻ/khóa backup, retention/purge/legal hold/scheduler

Khác bản cũ: thêm migration và ba credential runtime/migration/backup; giữ file quản trị cũ. API không dùng credential quản trị. r2 sửa quyền **mã chương trình bên trong image**, không chmod/chown secrets/media/ledger/database trên host.

Trước cửa sổ bảo trì, owner vận hành xác nhận share mã hóa đã mở/mount, backup **database cùng media** và restore point dùng được theo chính sách đang duyệt. Dump của updater chỉ là database và kiểm parse, không thay backup media/offsite/restore drill. Không chạy đồng thời DSM Build/Update hoặc một phiên updater khác.

Upload và đăng nhập đúng nơi

File / thư mục	Vị trí
ZIP	`ncv-dcims-production-0.2.30-complete-synology-r2.zip`
Checksum	`ncv-dcims-production-0.2.30-complete-synology-r2.zip.sha256.txt`
Upload trong File Station	Shared folder **docker-v2**, Location **Volume 2**, tạo thư mục **ncv-dcims-release-0.2.30-r2**
Đường dẫn SSH của thư mục upload	`/volume2/docker-v2/ncv-dcims-release-0.2.30-r2`
Source sau giải nén	`/volume2/docker-v2/ncv-dcims-release-0.2.30-r2/source`

Không upload vào database/media/ledger/backup repository hoặc source project đang chạy. Không giải nén đè project. ZIP chứa source để build, không có image offline/credential/database; NAS cần registry/package registry.

Trong **Windows PowerShell**, mở thư mục chứa hai file, so sánh hash:

```
Get-FileHash -Algorithm SHA256 .\ncv-dcims-production-0.2.30-complete-synology-r2.zip
Get-Content .\ncv-dcims-production-0.2.30-complete-synology-r2.zip.sha256.txt
```

Hai hash phải giống hệt nhau. Upload cả hai file vào đúng thư mục trong bảng.

Trong PowerShell, thay hai phần `<...>` bằng tài khoản quản trị và địa chỉ NAS thực tế:

```
ssh '<tai-khoan-quan-tri-nas>@<dia-chi-nas>'
```

Sau đăng nhập, dấu nhắc phải là `admin@NAS...:~$`, không phải `PS C:\...>`. Tất cả khối `sh` sau đây chạy trên NAS. **Dán nguyên khối từ `sudo sh` đến dòng kết thúc `DCIMS_...`; không bỏ dòng cuối.** Dấu `>` trong lúc dán là shell đang chờ đủ khối. Sudo có thể hỏi password; nhập tại prompt, không viết

password vào lệnh.

Mỗi khối tự khai báo đường dẫn và chạy trong shell sudo riêng, không phụ thuộc biến của khối trước. Không cần `sudo -i`. Khi khối lỗi, shell con dừng nhưng bạn vẫn ở NAS admin; **không chạy bước tiếp theo hoặc lặp bước vừa lỗi theo phỏng đoán**. Mất SSH: đăng nhập lại NAS, kiểm bước đã đạt trước khi tiếp tục.

Kiểm ZIP và hiện trạng trước giải nén

Khối này kiểm site còn ở 0.2.29; nếu NAS đang ở 0.2.30, không chạy quy trình nâng cấp.

```
sudo sh <<'DCIMS_PRECHECK_R2'
set -eu
export PATH=/var/packages/ContainerManager/target/usr/bin:/usr/local/bin:/usr/bin:/bin:/usr/
sbin:/sbin:$PATH
DCIMS_PROJECT=/volume2/docker-v2/ncv-dcims-production
DCIMS_STAGE=/volume2/docker-v2/ncv-dcims-release-0.2.30-r2
DCIMS_TOOLS=/volume2/docker-v2/ncv-tools/dcims-v1
cd "$DCIMS_PROJECT"
test -f .env
test ! -L .env
test "$(sed -n 's/^NCV_DCIMS_APP_VERSION=//p' .env | tr -d '\r')" = 0.2.29
test -d secrets
test -d /volume2/migration-backup
test "$(cat /volume2/docker-v2/ncv-dcims-postgres-data-v2/PG_VERSION)" = 17
sh "$DCIMS_TOOLS/dcims.sh" check </dev/null
docker ps -a --filter name=ncv-dcims --format 'table {{.Names}}\t{{.Image}}\t{{.Status}}'
cd "$DCIMS_STAGE"
test ! -e source
test ! -e operator-state
tr -d '\r' < ncv-dcims-production-0.2.30-complete-synology-r2.zip.sha256.txt | sha256sum -c
-
printf 'PRECHECK_R2_OK\n'
DCIMS_PRECHECK_R2
```

Đạt: checksum `OK`, `NCV_VOLUME2_READY version=0.2.29`, PostgreSQL/API/Web/Gateway healthy, `PRECHECK_R2_OK`. Tunnel có thể xuất hiện thêm. Adapter check có probe nhỏ ở media/backup và helper lưu cấu hình riêng tư; không gọi nó là hoàn toàn không ghi.

Trong **File Station**, chọn ZIP → **Extract/Giải nén** vào **source** bên trong thư mục upload. Nếu DSM tạo thư mục tên ZIP, đổi tên thành `source`. Phải có trực tiếp `source/package.json`, `source/apps/api/package.json`, `source/deploy`; không lồng thêm thư mục tên ZIP và không để source nằm ngay ở gốc staging. **Không dùng** `unzip` **trong SSH: NAS này không có lệnh đó.**

Sao lưu rồi chép source r2

App vẫn chạy. Khối tự lưu source/config/secrets/tools cũ, kiểm version/hash source và bảo đảm `.env`, `volume2.override.yml`, `docker-compose.yml` không bị thay. Đường dẫn backup được lưu trong `operator-state/source-backup.path`; bước sau đọc và kiểm lại, không phải gõ suffix từ ảnh.

```
sudo sh <<'DCIMS_SOURCE_R2'
set -eu
umask 077
export PATH=/var/packages/ContainerManager/target/usr/bin:/usr/local/bin:/usr/bin:/bin:/usr/
sbin:/sbin:$PATH
DCIMS_PROJECT=/volume2/docker-v2/ncv-dcims-production
DCIMS_STAGE=/volume2/docker-v2/ncv-dcims-release-0.2.30-r2
DCIMS_TOOLS=/volume2/docker-v2/ncv-tools/dcims-v1
cd "$DCIMS_PROJECT"
test -f .env
test ! -L .env
```

```
test "$(sed -n 's/^NCV_DCIMS_APP_VERSION=//p' .env | tr -d '\r')" = 0.2.29
test ! -e "$DCIMS_STAGE/operator-state"
for dcims_manifest in package.json apps/api/package.json apps/web/package.json; do
  test -s "$DCIMS_STAGE/source/$dcims_manifest"
  grep -Eq '"version"[[:space:]]*:[[:space:]]*"0[.]2[.]30"'
"$DCIMS_STAGE/source/$dcims_manifest"
done
test -s "$DCIMS_STAGE/source/deploy/site/nas-volume2/install-dcims-security-update.sh"
for dcims_private in .env secrets volume2.override.yml docker-compose.yml; do
  test ! -e "$DCIMS_STAGE/source/$dcims_private"
  test ! -L "$DCIMS_STAGE/source/$dcims_private"
done
test "$(tr -d '\r' < "$DCIMS_STAGE/source/deploy/docker/api.Dockerfile" | sha256sum | cut -d
 ' ' -f 1)" = 43f6cc05d3a78f6da7bd726a01eeb5a6e5328a99973e6ec4cafa6886b90d98a1
mkdir "$DCIMS_STAGE/operator-state"
DCIMS_SAVE=$(mktemp -d /volume2/migration-backup/dcims-source-before-0230-XXXXXX)
printf 'SOURCE_BACKUP=%s\n' "$DCIMS_SAVE"
mkdir "$DCIMS_SAVE/config"
cp -p .env compose.production.certified.yml volume2.override.yml docker-compose.yml
"$DCIMS_SAVE/config/"
cp -a secrets "$DCIMS_SAVE/secrets"
cp -a "$DCIMS_TOOLS" "$DCIMS_SAVE/site-tools"
tar -cf "$DCIMS_SAVE/source-before.tar" \
  --exclude=node_modules --exclude=dist --exclude=generated \
  --exclude=.next --exclude=.wrangler --exclude=coverage \
  apps packages patches deploy scripts \
  package.json pnpm-lock.yaml pnpm-workspace.yaml tsconfig.base.json README.md .dockerignore
for dcims_file in compose.*.yml .env.*.example .gitignore AGENTS.md; do
  if test -f "$dcims_file"; then cp -p "$dcims_file" "$DCIMS_SAVE/config/"; fi
done
test -s "$DCIMS_SAVE/source-before.tar"
tar -tf "$DCIMS_SAVE/source-before.tar" >/dev/null
cp -a "$DCIMS_STAGE/source/." "$DCIMS_PROJECT/"
for dcims_config in .env volume2.override.yml docker-compose.yml; do
  cmp "$DCIMS_PROJECT/$dcims_config" "$DCIMS_SAVE/config/$dcims_config"
done
printf '%s\n' "$DCIMS_SAVE" > "$DCIMS_STAGE/operator-state/source-backup.path"
printf 'SOURCE_R2_READY_PRIVATE_CONFIG_UNCHANGED\n'
DCIMS_SOURCE_R2
```

Đạt: `SOURCE_R2_READY_PRIVATE_CONFIG_UNCHANGED`. Lưu `SOURCE_BACKUP`; thư mục có secrets thật, không gửi cả thư mục. `operator-state` đã có mà khối lỗi: giữ trạng thái, kiểm backup/copy; không xóa marker rồi lặp bước. Không `rsync --delete`, không quét Docker Root, không chép payload site đè `ncv-tools/dcims-v1`. Mẫu `.env.production.example` không thay `.env` thật. Source mới chưa làm container đang chạy restart.

Tạo credential và tự cập nhật năm khóa `.env`

Không dùng `vi`, không in URL/password, không gõ đường dẫn file quản trị theo phỏng đoán. Khối dò file cũ từ `.env`, yêu cầu chưa có ba file mới, build migration image rồi kiểm pnpm/Prisma bằng UID thật **trước downtime**. Nó tạo ba credential khác nhau, giữ file quản trị cũ và thay đúng năm khóa `.env` bằng file tạm sau khi đã sao lưu.

```
sudo sh <<'DCIMS_ENV_R2'
set -eu
umask 077
export PATH=/var/packages/ContainerManager/target/usr/bin:/usr/local/bin:/usr/bin:/bin:/usr/
sbin:/sbin:$PATH
DCIMS_PROJECT=/volume2/docker-v2/ncv-dcims-production
DCIMS_STAGE=/volume2/docker-v2/ncv-dcims-release-0.2.30-r2
cd "$DCIMS_PROJECT"
test -f .env
test ! -L .env
DCIMS_SAVE=$(cat "$DCIMS_STAGE/operator-state/source-backup.path")
case "$DCIMS_SAVE" in /volume2/migration-backup/dcims-source-before-0230-*) ;; *) exit 1;;
```

```
esac
test -s "$DCIMS_SAVE/source-before.tar"
test -d "$DCIMS_SAVE/secrets"
for dcims_config in .env volume2.override.yml docker-compose.yml; do
  cmp "$dcims_config" "$DCIMS_SAVE/config/$dcims_config"
done
read_setting() {
  test "$(awk -F= -v key="$1" '$1==key {n++} END {print n+0}' .env)" = 1 || { printf "STOP:
MISSING_OR_DUPLICATE_KEY %s\n" "$1" >&2; return 1; }
  sed -n "s/^$1=//p" .env | tr -d '\r'
}
test "$(read_setting NCV_DCIMS_APP_VERSION)" = 0.2.29
DCIMS_OLD_DB_FILE=$(read_setting NCV_DCIMS_DATABASE_URL_FILE)
test -n "$DCIMS_OLD_DB_FILE"
case "$DCIMS_OLD_DB_FILE" in
  /*) DCIMS_ADMIN_FILE="$DCIMS_OLD_DB_FILE";;
  ./*) DCIMS_ADMIN_FILE="$DCIMS_PROJECT/${DCIMS_OLD_DB_FILE#./}";;
  *) DCIMS_ADMIN_FILE="$DCIMS_PROJECT/$DCIMS_OLD_DB_FILE";;
esac
test -s "$DCIMS_ADMIN_FILE"
DCIMS_RUNTIME_USER="$(read_setting NCV_DCIMS_RUNTIME_UID):$(read_setting
NCV_DCIMS_RUNTIME_GID)"
test "$DCIMS_RUNTIME_USER" = 1044:65549
for dcims_role in runtime migration backup; do
  test ! -e "secrets/$dcims_role-database-url.txt"
  test ! -L "secrets/$dcims_role-database-url.txt"
done
docker build -f deploy/docker/api.Dockerfile --target migration -t ncv-dcims-api-
migration:0.2.30 . </dev/null
docker run --rm --network none --read-only --user "$DCIMS_RUNTIME_USER" \
  --cap-drop ALL --security-opt no-new-privileges:true \
  --tmpfs /tmp:rw,noexec,nosuid,size=64m \
  -e COREPACK_ENABLE_NETWORK=0 -e CHECKPOINT_DISABLE=1 \
  -e DATABASE_URL=postgresql://127.0.0.1:5432/ncv_dcims_permission_check \
  --entrypoint /bin/sh ncv-dcims-api-migration:0.2.30 \
  -ec 'test -r package.json; pnpm --version; pnpm exec prisma --version' </dev/null
printf 'MIGRATION_TOOLCHAIN_READ_OK_BEFORE_DOWNTIME\n'
docker run --rm --network none --user 0:0 --entrypoint node \
  --mount "type=bind,src=$DCIMS_ADMIN_FILE,dst=/old-admin-url,readonly" \
  --mount "type=bind,src=$DCIMS_PROJECT/secrets,dst=/role-secrets" \
  ncv-dcims-api-migration:0.2.30 dist/scripts/generate-database-role-secrets.js \
  --admin-url-file /old-admin-url --output-directory /role-secrets </dev/null
for dcims_role in runtime migration backup; do test -s "secrets/$dcims_role-database-
url.txt"; done
for dcims_key in NCV_DCIMS_DB_ADMIN_URL_FILE NCV_DCIMS_MIGRATION_DATABASE_URL_FILE
NCV_DCIMS_BACKUP_DATABASE_URL_FILE; do
  test "$(grep -c "^$dcims_key=" .env || true)" -le 1
done
DCIMS_ENV_TMP=$(mktemp "$DCIMS_PROJECT/.env.update-r2.XXXXXX")
trap 'rm -f "$DCIMS_ENV_TMP"' 0
trap 'exit 130' INT
trap 'exit 143' HUP TERM
cp -p .env "$DCIMS_ENV_TMP"
sed \
  -e '/^NCV_DCIMS_APP_VERSION=/d' \
  -e '/^NCV_DCIMS_DB_ADMIN_URL_FILE=/d' \
  -e '/^NCV_DCIMS_DATABASE_URL_FILE=/d' \
  -e '/^NCV_DCIMS_MIGRATION_DATABASE_URL_FILE=/d' \
  -e '/^NCV_DCIMS_BACKUP_DATABASE_URL_FILE=/d' \
  .env > "$DCIMS_ENV_TMP"
printf '\n%s\n' 'NCV_DCIMS_APP_VERSION=0.2.30' >> "$DCIMS_ENV_TMP"
printf 'NCV_DCIMS_DB_ADMIN_URL_FILE=%s\n' "$DCIMS_OLD_DB_FILE" >> "$DCIMS_ENV_TMP"
printf '%s\n' \
  'NCV_DCIMS_DATABASE_URL_FILE=./secrets/runtime-database-url.txt' \
  'NCV_DCIMS_MIGRATION_DATABASE_URL_FILE=./secrets/migration-database-url.txt' \
  'NCV_DCIMS_BACKUP_DATABASE_URL_FILE=./secrets/backup-database-url.txt' >> "$DCIMS_ENV_TMP"
for dcims_key in NCV_DCIMS_APP_VERSION NCV_DCIMS_DB_ADMIN_URL_FILE
NCV_DCIMS_DATABASE_URL_FILE NCV_DCIMS_MIGRATION_DATABASE_URL_FILE
NCV_DCIMS_BACKUP_DATABASE_URL_FILE; do
  test "$(grep -c "^$dcims_key=" "$DCIMS_ENV_TMP")" = 1
done
```

```
mv -f "$DCIMS_ENV_TMP" .env
printf 'ENV_R2_READY\n'
DCIMS_ENV_R2
```

Đạt: `MIGRATION_TOOLCHAIN_READ_OK_BEFORE_DOWNTIME`, `DB_ROLE_SECRET_FILES_CREATED`, `ENV_R2_READY`. Toolchain probe không kết nối DB. Tạo file không đổi password administrator hay provision role. File credential mới có quyền ban đầu 0600; updater chuẩn hóa quyền các file được chỉ định.

Nếu ba file mới đã có hoặc khối lỗi giữa chừng, không xóa/sinh lại và không sửa `.env` bằng mẫu; dừng đối chiếu bước đã đạt. Mọi khóa khác được giữ, bao gồm domain/TLS, storage, UID/GID, khóa chia sẻ/backup và chính sách dữ liệu.

Cài revision adapter rồi update một lần

Chỉ chạy khi bước 3-5 đạt, có cửa sổ bảo trì và backup theo mục 1. Installer có guard riêng cho topology/layout/helper/UID/DSM; nó chỉ cài revision cần cho credential mới, không phải installer Volume 2 gốc. Không stop toàn project trước khối này.

```
sudo sh <<'DCIMS_UPDATE_R2'
set -eu
umask 077
export PATH=/var/packages/ContainerManager/target/usr/bin:/usr/local/bin:/usr/bin:/bin:/usr/
sbin:/sbin:$PATH
cd /volume2/docker-v2/ncv-dcims-production
sh deploy/site/nas-volume2/install-dcims-security-update.sh </dev/null
sh /volume2/docker-v2/ncv-tools/dcims-v1/dcims.sh check </dev/null
sh /volume2/docker-v2/ncv-tools/dcims-v1/dcims.sh update 0.2.30 </dev/null
DCIMS_UPDATE_R2
```

Đạt: adapter ready và `NCV_VOLUME2_UPDATE_OK version=0.2.30 backup=...`. Lưu backup path. `NCV_VOLUME2_READY` riêng lẻ chỉ là kiểm sẵn sàng, không phải đã cập nhật.

Updater build khi app cũ vẫn chạy → kiểm secret/quyền/storage/role input → dừng đúng Gateway/API/Web, giữ PostgreSQL → dump/parse → provision role → migration → provision lại để chặn runtime đọc metadata migration/sửa xóa audit → recreate ba app, kiểm healthy/image → đồng bộ DSM. PostgreSQL và tunnel không được nâng/recreate trong bước này. Build có thể lâu ở download/export layers; không mở phiên build thứ hai.

Kiểm sau cập nhật và UI

```
sudo sh <<'DCIMS_VERIFY_R2'
set -eu
export PATH=/var/packages/ContainerManager/target/usr/bin:/usr/local/bin:/usr/bin:/bin:/usr/
sbin:/sbin:$PATH
cd /volume2/docker-v2/ncv-dcims-production
sh /volume2/docker-v2/ncv-tools/dcims-v1/dcims.sh check </dev/null
sh /volume2/docker-v2/ncv-tools/dcims-v1/sync-dsm-compose.sh check </dev/null
docker ps -a --filter name=ncv-dcims --format 'table {{.Names}}\t{{.Image}}\t{{.Status}}'
test "$(tr -d '\r' < deploy/docker/api.Dockerfile | sha256sum | cut -d ' ' -f 1)" =
43f6cc05d3a78f6da7bd726a01eeb5a6e5328a99973e6ec4cafa6886b90d98a1
DCIMS_HOST=$(sed -n 's/^NCV_DCIMS_PUBLIC_HOST=//p' .env | tr -d '\r')
test -n "$DCIMS_HOST"
sh scripts/synology/ncv-dcims-post-update-smoke-test.sh "https://$DCIMS_HOST" 0.2.30
</dev/null
DCIMS_VERIFY_R2
```

Đạt: `NCV_VOLUME2_READY version=0.2.30`, `DSM_COMPOSE_SYNC_CHECK_OK`, bốn service healthy và `NCV_DCIMS_POST_UPDATE_SMOKE_OK`. Adapter kiểm image pins/volume/UID/layout; HTTPS smoke kiểm health/auth boundary/header, không đọc phiên bản public. Không gửi `.env`, credential hoặc log có dữ liệu thật.

Mở web, **Ctrl+F5**, đăng nhập; kiểm Cài đặt không icon trước tiêu đề, menu/nút vẫn dùng được, paging/tìm/lọc bệnh nhân và Back/Forward. Nghiệm thu role/scope/share/upload/confirm/reopen chỉ dùng tài khoản và dữ liệu thử được phép; không xóa ca thật để thử thu hồi link. Kiểm responsive 390/768/1440 và thiết bị Back/Forward thực khi nghiệm thu UI đầy đủ. Đăng nhập/giao diện bình thường không thay DR/offsite/reboot/restore UAT.

Các lỗi đã gặp và cách xử lý đúng

Hiện tượng	Nguyên nhân / xử lý
Sudo disabled trong Windows	SSH đã đóng và đang ở `PS>`. SSH lại NAS; không bật sudo Windows để sửa
Biến rỗng, lệnh tìm `/source/...`	Biến mất khi đổi root/admin/SSH. Các khối r2 tự khai báo đầy đủ; không tiếp tục dán đoạn cũ
Không tìm thấy ZIP hoặc sidecar	Upload sai folder/tên hoặc đang đứng sai thư mục. Kiểm hai file đúng bảng mục 2, checksum OK trước giải nén
`UNZIP_NOT_AVAILABLE`	Dùng File Station, không cài thêm unzip hoặc lặp lệnh lỗi
Có package.json ngay staging root	Giải nén sai đích. Cần `.../source/package.json`; chưa copy vào project
SOURCE_READY được in dù test trước lỗi	In một marker riêng không chứng minh đạt. Chỉ dùng marker cuối của nguyên khối đã dừng khi lỗi
Backup suffix từ ảnh bị đọc sai	r2 lưu đường dẫn từ mktemp vào operator-state và so config, không gõ tên ngẫu nhiên từ ảnh
Pnpm báo bản mới hoặc request chậm	Không tự nâng package manager; giữ pnpm 11.9.0/lockfile. Chờ và kiểm tiến trình; không build song song
Corepack EACCES đọc package.json	Source giải nén giữ 0600/0700, UID site khác node. r2 sửa quyền program workspace; toolchain probe trước downtime. Không chmod toàn shared folder, không chạy API root
Update lỗi stage=migration/activation	Role/schema có thể đã đổi. Không bật container/image cũ, restore hoặc chạy full updater lại theo phỏng đoán
App healthy nhưng DSM sync lỗi	Kiểm riêng helper/DSM/default Compose; không rebuild/migrate lại chỉ để sửa sync
`update.lock` đã tồn tại	Kiểm tiến trình/trạng thái; không xóa lock để ép chạy

Nếu lỗi: giữ nguyên output và backup path, ghi bước/marker cuối; không thực hiện bước sau. Trước migration, kiểm trạng thái thực rồi mới quyết định tiếp tục. Sau role/migration, phương án rollback/restore theo schema phải được chủ hệ thống duyệt; **Không tự động trả image cũ hoặc restore database** vì có thể không tương thích/mất dữ liệu. Không purge, `down -v`, Clean/Delete project, prune, migrate reset/resolve thủ công hoặc seed DB vận hành. Không chạy Docker system df/quét Docker Root nặng từng gây treo NAS.

Nhật ký và khối xử lý sự cố ZIP gốc/r1 nằm ở hướng xử lý lỗi quyền image, chỉ dùng khi trạng thái khớp và được đối chiếu; không phải phần bắt buộc của upgrade r2. Bằng chứng kiểm phân biệt chuẩn bị local, NAS thực và phần chưa kiểm. Fresh full Docker build từ source sửa chưa được chạy lại local vì engine unavailable/WSL bị từ chối; NAS đã kiểm candidate images với cùng logic chmod, migration/runtime/smoke và source checksum.