Gaps of Phase 1/2/3

Gaps to polish and finalize (MVP: Meta + LinkedIn)

- Security & configuration
  - Secrets management: move env vars to AWS Secrets Manager/Vault; rotate keys.
  - JWT and API key hygiene: expiration, rotation, and scoped API keys.
  - Input validation and schema validation for all POST bodies.
- OAuth & account selection
  - Unify callback/state validation; CSRF/state verification and nonce storage.
  - Multi-account selection UX: allow selecting which page/company (and IG account) to connect/target.
  - Token scope checks and re-consent flow if scopes missing.
- Token lifecycle
  - Expand token audit logging and surface in admin UI/logs.
  - Retry/backoff on refresh failures; alert on repeated failures.
  - Cache invalidation on manual disconnect.
- Content workflow
  - Guardrails: prevent scheduling when missing required media (e.g., IG photo).
  - Permissions: enforce role-based actions (editor vs admin) beyond current guard.
  - Richer IG presets (story/reel/carousel options) and validation hints.
- Scheduling & jobs
  - Reschedule/cancel endpoints and UI semantics.
  - Idempotency keys per schedule publish; dedupe on worker side.

    - Provider-aware retry/backoff policies; exponential with jitter and max cap.
- Publishing robustness
    - Target account selection: persist which page/company to publish to.
    - Media handling: large image/video handling, mime detection, size limits.
    - Error normalization (rate limits, invalid media, auth) with actionable messages.
- Webhooks processing
    - Implement processors for actionable events (comments, messages, status updates).
    - Dead-letter queue dashboards; reprocessing pipeline; alerting on DLQ growth.
    - Signature failure telemetry; idempotency collision monitoring.
- Analytics & insights
    - Wire Meta/LinkedIn insights into API; store snapshots for time series.
    - Basic dashboards (reach, engagement) per account and per post.
    - Pagination and rate-limit friendly batching for analytics fetch.
- Observability
    - Structured logging (JSON) and correlation IDs across API/Worker.
    - Prometheus metrics: queue sizes, job durations, success/failure, publish latency.
    - Grafana dashboards + alerts (token refresh failures, 429 spikes, job fail rate).
- Performance & data
    - DB indexes verification for schedules, tokens, webhook events.
    - Content and schedule queries: pagination and filters.
    - Background image processing concurrency limits.
- Multi-tenancy & tenancy safety

    - Remove hardcoded `org_chauncey`; propagate `organizationId` from auth context.
    - Enforce tenant isolation in queries.
- Rate limiting & abuse prevention
    - Per-route, per-tenant limits; separate limits for webhooks and publish endpoints.
    - Circuit breakers for provider APIs on sustained 429/5xx.
- CI/CD & quality
    - CI: lint/test/build gates; secret scanning; type checks.
    - E2E tests: OAuth, publish flows (mock providers); webhook signature tests.
    - Load testing for publish bursts and webhook storms.
- Documentation & runbooks
    - Step-by-step connect → approve → schedule → publish guide.
    - On-call runbook for token issues, rate limits, DLQ handling.
    - Postman collection updates with envs and examples.
- Compliance & privacy (lightweight)
    - Log redaction for tokens/signatures; PII handling in webhook payloads.
    - Data retention policies for webhook events and logs.
- Nice-to-haves (if time permits)
    - Admin tools: token health page, queue inspector, DLQ replayer.
    - Backfill publish history import from platforms.