

PrismManifest - PILOT DEPLOY

PrismManifest Pilot Deploy (minimal ops)

Field Value
Audience Operator standing up a pilot
Scope Not SOC 2 - pilot hardening only

Required env

Variable Purpose
PRISMMANIFEST_GATE_ENFORCE Path to C++ enforce binary (optional but
PRISMMANIFEST_CANONICALIZE Path to C++ canonicalize binary
PRISMMANIFEST_GEMINI_API_KEY Gemini key for bench-llm only
PRISMMANIFEST_AZURE_KEY_ID Azure Key Vault key URL for KMS envelope

Pilot checklist

1. Generate keys (gen-keys / gen-kms-key --mode azure)
2. Run pytest + prismmanifest-gate compliance
3. Point audit store at an append-only volume
4. Run review UI bound to localhost only
5. Enable RBAC at the API edge (prismmanifest.ops.rbac.authorize)
6. Use IdempotencyStore for enforce retries
7. Scrape MetricsRegistry.to_prometheus() or JSON export

Cost control (LLM)

- * Default model: gemini-2.5-flash-lite
- * Hard abort at \$20 estimated paid-tier cost
- * Prefer ephemeral API keys; delete after benches

API versioning

- * Manifest schema version is carried in FlatBuffer / JSON schema fields
- * gRPC service: treat breaking changes as new package major version