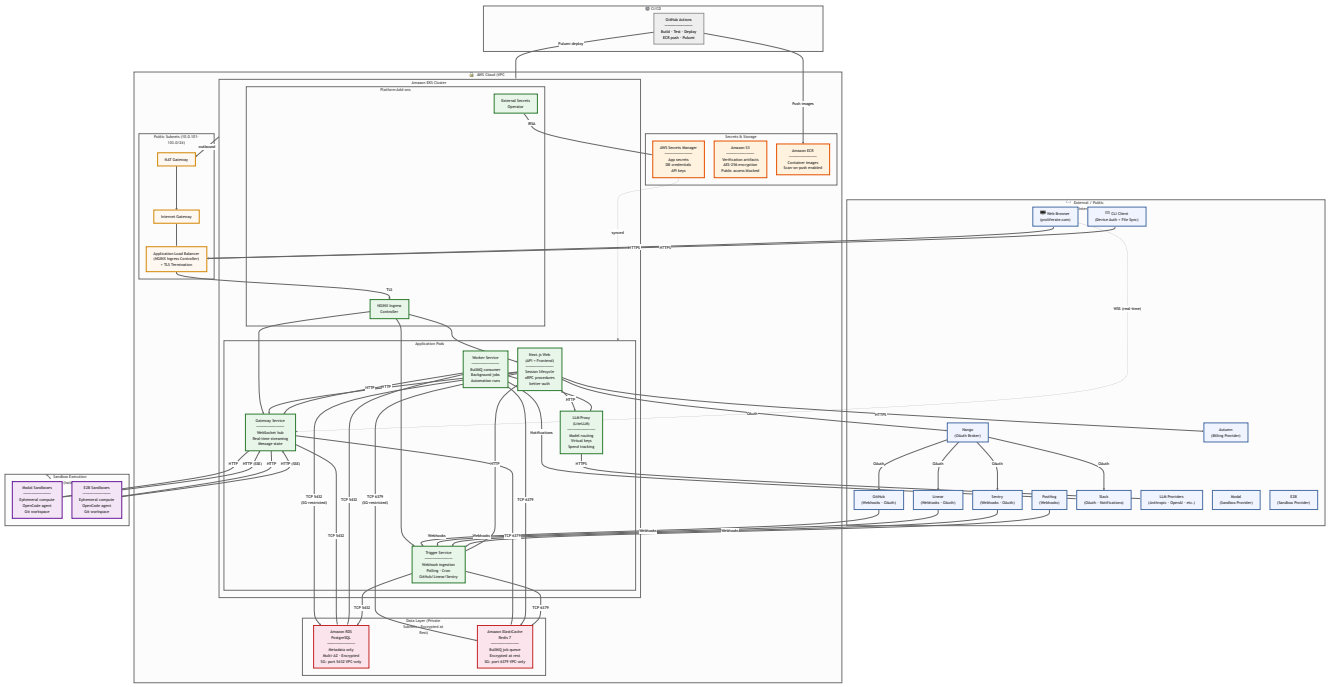
Proliferate — Network Architecture

Production environment · AWS EKS · Last updated February 2026



Legend & Security Controls

Network Boundaries

- **External / Public Internet** — end-user browsers, CLI clients, third-party SaaS integrations
- **AWS VPC (10.0.0.0/16)** — isolated virtual network containing all production infrastructure
- **Public Subnets (10.0.101–103.0/24)** — Internet Gateway, ALB/Load Balancer, NAT Gateway only
- **Private Subnets (10.0.1–3.0/24)** — EKS worker nodes, RDS, ElastiCache (no direct internet access)
- **Sandbox Zone** — ephemeral, isolated compute environments (Modal / E2B) with no direct DB access

Security Controls

- **TLS everywhere** — all external traffic encrypted via TLS termination at NGINX Ingress
- **Security Groups** — DB SG allows TCP 5432 from VPC CIDR only; Redis SG allows TCP 6379 from VPC CIDR only
- **NAT Gateway** — private subnet outbound traffic routes through NAT (no inbound from internet)
- **AWS Secrets Manager + External Secrets Operator** — secrets synced into K8s via IRSA (no static credentials)
- **ECR image scanning** — vulnerability scan on every push

- **S3** — AES-256 server-side encryption, all public access blocked
- **RDS** — storage encrypted at rest, Multi-AZ, private subnet only
- **ElastiCache** — encryption at rest enabled, private subnet only
- **Authentication** — better-auth for user auth; OAuth via Nango for third-party integrations; IRSA for AWS service access
- **NGINX Ingress Controller** — single entry point, rate limiting, request filtering

Data Flows & PII Separation

- **PostgreSQL (RDS)** — stores org/user metadata, session records, billing data. Customer PII is scoped per-org with row-level ownership.
- **Redis (ElastiCache)** — transient job queues (BullMQ) and session state. No persistent PII storage.
- **Sandboxes (Modal/E2B)** — ephemeral, isolated per-session. No direct database access. Communicate only with the Gateway via HTTP/SSE.
- **LLM Proxy** — routes model requests to providers (Anthropic, OpenAI). Per-org virtual keys for spend isolation.
- **S3** — verification artifacts only, encrypted, no public access.
- **No PII in logs** — structured logging (Pino) with sensitive field redaction. Tokens, credentials, and prompt content are never logged.

Solid lines

- Solid arrows (→) = synchronous HTTP/TCP connections
- Dashed arrows (⇢) = WebSocket / async / synced data