Overview

Overview

What this replaces

Previously, backend Spring Boot servers used a long-lived self-signed certificate. nginx pinned that exact cert file via `proxy_ssl_trusted_certificate` and used `proxy_ssl_name` to match its CN. Every cert rotation required touching nginx on every front-end machine, so rotation effectively never happened.

What this system does

Each backend machine issues and renews its own Let's Encrypt certificates using certbot (DNS-01 challenges via Route53), running entirely in Docker alongside the Spring app. Certificates hot-reload into the running JVM with no restart. nginx trusts the public CA root and verifies a shared "pool alias" name, so **nginx configuration never changes again** — adding backends, rotating certs, and promoting environments require zero nginx cert changes.

Revision #1
Created 2026-11-24 16:00:11 UTC by Dennis Underwood
Updated 2026-11-24 16:00:11 UTC by Dennis Underwood