# Root Cause Analysis (RCA) — Nexus (Spectra Systems)

Analysis based on performance and technical debt findings for Backend (Spring Boot, 5,000 users JMeter test) and Frontend (Lighthouse audit).

## 1. Backend (Spring Boot) — 5,000 Users Load Test

During load testing at 1,000 users, ~18–20% of /auth/login requests returned HTTP 400. Projecting to 5,000 users suggests growing error rates (400/429) and throughput instability.

### *1.1 Root Causes*

| # | Cause | Description |
|---|---|---|
| 1 | Thread & Connection Pool Saturation | Tomcat maxThreads (~200) and HikariCP default (10) limit concurrent logins. Under load, threads queue, causing incomplete validation and 400 responses. |
| 2 | Authentication Hotspot (BCrypt/JWT) | Password hashing and token signing are CPU-heavy. At scale, hashing delays cause thread blocking. |
| 3 | Unindexed User Queries | Missing database index on 'email' or 'username' causes full scans during authentication. |
| 4 | Invalid Test Configuration | JMeter missing Content-Type header or shared variables across threads leading to invalid JSON bodies (false 400s). |
| 5 | JVM Resource Pressure | Default G1GC tuning without MaxRAMPercentage may trigger short GC pauses affecting throughput. |

### *1.2 Corrective Actions*

- Increase Tomcat max-threads and HikariCP pool size (e.g., 400 threads, 40 connections).
- Add index on 'users(email)'. Verify EXPLAIN PLAN for login query.
- Tune hashing algorithm (BCrypt 10–11) and JWT signing (prefer HS256 or cached RSA).
- Adjust JVM options (-XX:MaxRAMPercentage=75, -XX:+UseG1GC).
- Include Content-Type and ramp-up in JMeter; test 1k→5k progressive ramp.

## 2. Frontend (Svelte/Vite + GCLB) — Lighthouse Audit

Frontend shows excellent performance (LCP ~2.0s, Speed Index 0.7s), but lacks HTTPS, HSTS, and caching headers, causing lower SEO scores and minor performance losses.

### *2.1 Root Causes*

| # | Cause | Description |
|---|---|---|
| 1 | No HTTPS | Without TLS, HTTP/2 and HTTP/3 are disabled, increasing round trips and blocking modern browser optimizations. |
| 2 | Missing Cache and Compression | Ingress lacks Cache-Control, Brotli/Gzip compression, leading to unnecessary downloads. |
| 3 | Suboptimal LCP Optimization | LCP image not preloaded, and fonts lack 'font-display: swap'. |

### *2.2 Corrective Actions*

- Enable HTTPS via GKE Managed Certificate and force redirect (308).
- Add Strict-Transport-Security header and enable Brotli compression.
- Add Cache-Control: public, max-age=31536000, immutable for static assets.
- Preload LCP images and fonts with font-display: swap.

## 3. Executive Summary

Backend degradation under load is primarily caused by resource saturation (threads, DB pool) and CPU-intensive authentication routines. Frontend impact is tied to lack of HTTPS and caching, reducing protocol efficiency. Mitigations include scaling backend pools, tuning hashing algorithms, enabling TLS + caching on frontend, and validating load test configurations.