

Auth Service Degradation

INTERNAL — Helix Engineering / CS Operations

SCOPE

This runbook covers degradation of the auth-service — the service that issues and validates user sessions and API tokens. Auth-service downtime locks all users out of the platform.

DETECTION

Auth-service exposes /health and /ready endpoints. Synthetic probes alert on degradation. Customer-reported login failures are also a strong signal.

STEP 1 — Confirm scope

Test login from an internal account. If you cannot log in, the impact is total. If you can log in but specific users cannot, the issue may be data-side (corrupted user record, IdP misconfiguration on customer side).

STEP 2 — Check downstream

Auth-service depends on Postgres (user store) and Redis (session cache). Check both. If Postgres is degraded, see database-failover. If Redis is degraded, restart redis-auth pods one by one.

STEP 3 — Roll back recent deploys

If a deploy in the last 30 minutes correlates with the issue, roll back: ``helix deploy rollback auth-service``. Confirm the rollback completed.

STEP 4 — Engage IdP support

For SSO-only failures (password login works, SSO fails): contact the customer's IdP admin if it appears IdP-side. Helix supports SAML 2.0 and the issue may be metadata expiration on their side.

STEP 5 — Emergency bypass

If you must restore service before root cause is found, you may temporarily disable SAML 2.0 enforcement workspace-by-workspace. This requires director approval and must be re-enabled within 24 hours.