Verify a platform release and isolate regressions

Compare the public route, version, role-scoped behavior, and persistence after deployment.

https://docs.qintoravacloud.com/guides/verify-release/

Establish a baseline

Record the currently serving revision, image digest, schema state and expected tenant scope. Capture representative expected outcomes for portal access, a shared workspace list, a representative saved record, configuration preview and any integration changed by the release. Use approved synthetic records when exercising writes.

Verify a candidate

1. Check DNS and TLS, then confirm the application's health endpoint responds. Test both a public route and an authenticated user journey.
2. Use a role permitted to read and change the feature and a role expected to be denied. Inspect final persisted values and downstream links, rather than relying on a toast or HTTP success alone.
3. Review browser and server evidence for errors. Compare failures across tenants, roles, browsers, or provider scope to locate the regression.
4. Before promoting, confirm rollback compatibility with the applied schema. After promotion, verify the live revision and repeat the critical checks on the live hostname.

Triage a regression

If the old revision is healthy and the new one fails with the same context, compare changed route contracts, assets, configuration and migrations. If both fail, check shared dependencies, DNS, authentication, and provider health. Preserve evidence before rolling traffic back. Follow platform release procedures when data recovery is involved.