Configure discovery and reconciliation

Set provider scope, preview ingestion, and diagnose missing resources or unexpected duplicates.

https://docs.qintoravacloud.com/guides/discovery/

Prepare the source

Open **Discovery & reconciliation → Discovery sources**. Choose the provider and discovery type. Use the required read-only provider identity and the approved credential reference for that integration. Set the narrowest project, subscription, account, network range, or asset family that meets the requirement. See Google Cloud discovery profile for an example.

Preview and run

1. Validate connectivity and provider permissions. Run a preview against a known resource.
2. Check identifiers, class mapping, relationship direction, scope, proposed reconciliation outcome, and rejected rows. Confirm that IRE rules match the intended class and authoritative source.
3. Schedule discovery only after the preview is correct. Confirm the configured schedule, timezone, target scope and enabled source.
4. Inspect the run record and a sample ingested CI. Compare processed, matched, inserted, updated and rejected records with the provider inventory.

Diagnose common failures

A provider 401 or 403 generally points to identity, scope, role or expired credentials. Timeouts can reflect DNS, egress, endpoint or range size. A clean run with zero CIs warrants checking filters, region, asset type and discovery scope. A duplicate warrants comparing the provider identifier and normalization before adjusting IRE policy. Capture the run ID, stage and sanitized provider error.