Discovery provider · Amazon Web Services

Discover AWS Organizations accounts and regional resources by assuming a governed IAM role.

https://docs.qintoravacloud.com/integrations/discovery-provider/aws/

Prerequisites

- IAM role with a Qintorava trust policy
- Read-only resource permissions in each account
- Organizations read access for multi-account discovery

Configuration steps

1. Create or select the cross-account role
2. Set the trust-policy external ID
3. Select accounts, regions, and resource families
4. Test AssumeRole and preview inventory

Provider fields

Field	Type	Requirement and options
AWS partition `partition`	select	Required `aws`, `aws-us-gov`, `aws-cn`
Organizations ID `organizationId`	text	Optional
AWS account IDs `accountIds`	tag_list	Required
Cross-account role ARN `roleArn`	text	Required
Trust-policy external ID `externalId`	text	Required
Regions `regions`	tag_list	Required
Resource types `resourceTypes`	tag_list	Optional

Field	Type	Requirement and options
Enumerate AWS Organizations `useOrganizations`	boolean	Optional

Verify and troubleshoot

Test with the narrowest supported non-production scope. Confirm that the connection test reaches the expected provider and that the preview or receipt matches the intended scope. Check identity, credential references, network access and provider permissions before retrying. Record the failure stage and redact sensitive payloads when escalating.