🔔 Incident Notification – Deployments failing due to IAM trust policy change

Status: resolved / mitigated => Need customer action, see below
Impact window (CEST): 01 Sep 2025 ~14:00 → ~16:00
Impact: Qovery operations blocked at pre-check (“Impossible to check that your credentials are valid”), inability to save changes / deploy.
Scope: AWS accounts where the IAM role used by Qovery has a **drifted trust policy**, whether the role was created via our CloudFormation or manually.

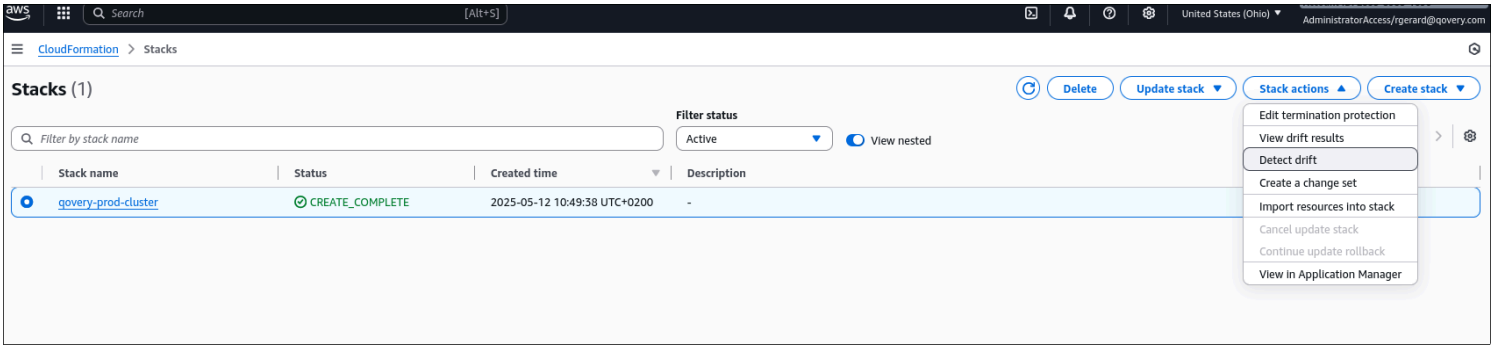
🎯 Executive summary

Several customers encountered pre-check and save errors. Investigation shows a **drift** in the **trust relationship** of the IAM roles used by Qovery. The change removed or replaced the expected trusted entities, preventing our services from assuming the role via STS.
Restoring the expected trust policy immediately re-enabled deployments (a short propagation delay can affect log visibility).

🧭 How to quickly detect if you’re affected

1. **In Qovery:** pre-check fails with
   `Impossible to check that your credentials are valid`.

2. **In AWS CloudFormation** (if you used our stack):
   CloudFormation → Stacks → (your Qovery role stack) → Actions → Detect drift → **Drift detected** on the *AWS::IAM::Role* resource.



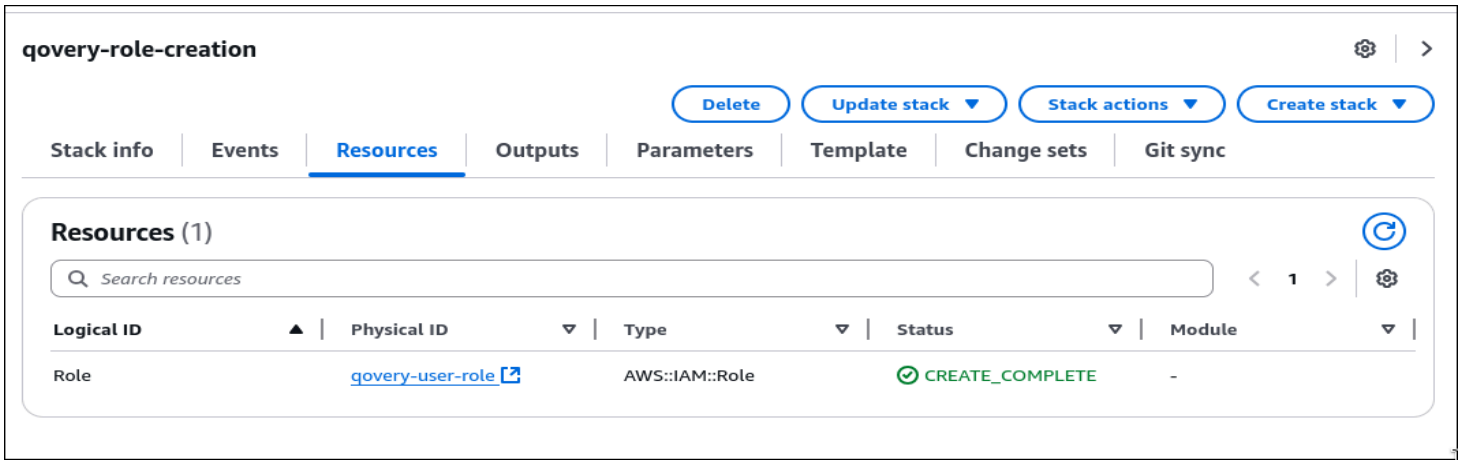
3. **In AWS IAM:**
   IAM → Roles → (qovery-user-role / qovery-user-access-role) → Trust relationships
   If the principals **no longer** reference the Qovery account `283389881690`, you're affected.

📍 Region: check **the region where you created the stack** (often `us-east-1`, but use your actual region).

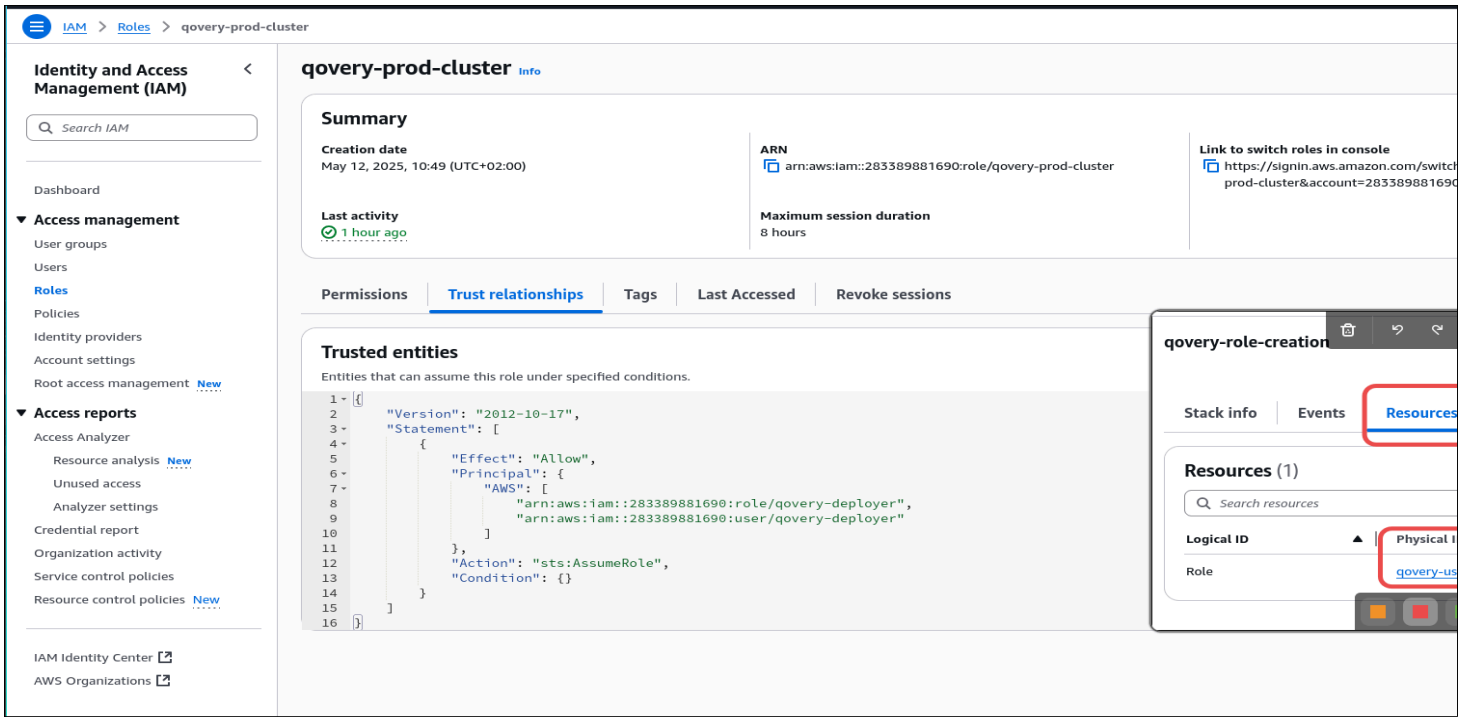
🛠️ Immediate fix (step by step)

For **each AWS account** tied to your clusters (dev, staging, prod, etc.):

1. Go to **IAM** → **Roles** and locate the role used in Qovery (check your cloudformation resources to confirm)



2. Open **Trust relationships → Edit trust policy**.



3. Replace the document with **exactly**:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::283389881690:role/qovery-deployer",
          "arn:aws:iam::283389881690:user/qovery-deployer"
        ]
      },
      "Action": "sts:AssumeRole",
      "Condition": {}
    }
  ]
}
```

4. **Save**, then retry your deployment in Qovery.
   ⚠️ Allow 1–5 minutes for IAM **propagation**; **service logs** may resume with a slight delay once sessions re-establish.

ℹ️ You **do not** need to create anything on your side: the referenced *user/role* exists in **our** AWS account (`283389881690`).

✅ Validation

- **Pre-check** succeeds; **deployments** proceed.
- In CloudFormation (if used), **Detect drift** returns **In sync** for the Role.
- **Service logs** are visible again once the STS session refreshes.

⏱️ Timeline (CEST)

- 14:55 : First customer error reports (pre-check failures).
- 15:05 : Initial triage: reproduction confirmed; scope appears limited to some AWS accounts.
- 15:15 : CloudFormation “Detect drift” shows drift on AWS::IAM::Role resources; IAM trust policies show unexpected principals.
- 15:25 : Hypothesis formed: trusted principal mismatch → STS AssumeRole fails.
- 15:40 : Starting Remediation applied with customers: trust policy updated to the current Qovery principal (role & user).
- 16:10 : Incident declared resolved; RCA ongoing.

- Day +2 : AWS confirms behavior: deletion/recreation of the trusted principal causes internal ID remapping visible in customers’ trust policies.

🪓 Root cause

- Primary cause: During an internal migration, the Qovery deployer identity was rotated (deleted/recreated).

- AWS behavior (by design): Customers' trust policies reference principals that AWS maps to internal IDs. If a principal is deleted/recreated, the mapping changes; the old internal ID may appear in trust policies instead of the ARN, effectively pointing at a non-existent principal.
- Effect: STS AssumeRole calls from Qovery to customer accounts failed, causing pre-check and deployment failures until trust policies were corrected.

🛠️ Corrective & Preventive Actions (CAPA)

Completed

- ✅ Trust policy restoration for affected customers => Action made by customers
- ✅ Runbook update: incident playbook now includes rapid IAM drift triage and a standard trust-policy template.
- ✅Apply a new IAM policy on Qovery AWS organisation to block any suppression or update of critical assets (Qovery deployer role, user and policies).

🤝 Assistance

We can review the affected accounts/roles with you
If you see new symptoms, please share the **Role ARN** and **region** involved.

— Qovery Support Team