Deployment-Repo mit der CI-Component

> Zielgruppe: Anwender und Betreuer · Stand: 06.11.2026

Alle Terraform/OpenTofu-Deployments laufen über dieselbe GitLab-CI-Component. Ein Deployment-Repo bindet sie ein und bekommt damit Stages, Promotion, Freigaben, Destroy und die Ansible-Umgebung, ohne eigene Pipeline-Logik.

Voraussetzungen

- Das Repo liegt in der GitLab-Gruppe deiner Abteilung.
- Du hast mindestens die Rolle Reporter im Projekt `cloud-core-infrastructure/ci-components/deployment`. Die Component ist privat.
- Die vier Stage-Branches existieren und sind geschützt (siehe Stages und Branches).

Vorgehen

1. `.gitlab-ci.yml` auf das `include` der Component reduzieren:

   ```
   include:
     - component: $CI_SERVER_FQDN/cloud-core-infrastructure/ci-
   components/deployment/terraform@<version>
       inputs:
         enabled-stages: "development,staging"
         root-config: proxmox
   ```

   - `<version>`: immer eine feste Version bzw. einen SHA, nie einen Branch
2. Keine eigenen `stages:` und keinen `workflow:` definieren. Eigene Jobs nutzen `extends: .deployment:base`.
3. Projekt einrichten: `scripts/setup-project.sh <projekt>` aus dem Component-Repo legt Trigger-Token, Push-Rechte und den Default-Branch `pre-development` an.
4. Bei `root-config: proxmox` gehört die erzeugte `deployment.generated.tf` in die `.gitignore`. Backend und Standard-Provider bringt die Component dann mit.

5. Braucht das Repo Secrets aus OpenBao: `openbao-jwt-role` und `openbao-addr` setzen (siehe Pipeline per GitLab-JWT anmelden).

Prüfen

> Die Pipeline auf `pre-development` zeigt die Jobs `plan`, `apply-freigeben` und `deploy`. Der Plan ist im Job-Log lesbar.

Stolperfallen

- Neue Component-Versionen können Inputs entfernen (z. B. `promote-development`). Beim Anheben des Pins die Inputs gegen die README prüfen.
- Ansible läuft immer aus Terraform heraus (`terraform_data` mit `local-exec`), nie als eigener Job.
- Den SSH-Schlüssel für Ansible liefert eine geschützte Gruppenvariable. Deshalb müssen alle Stage-Branches geschützt sein.

Weiterführend

- README der CI-Component
- Merge heißt Deploy

Revision #1
Created 2026-11-06 18:10:27 UTC by Alexander Golembek
Updated 2026-11-06 18:10:27 UTC by Alexander Golembek