Pipeline per GitLab-JWT anmelden

> Zielgruppe: Betreuer · Stand: 06.11.2026

Pipelines melden sich mit ihrem GitLab-JWT bei OpenBao an. Sie brauchen dafür kein gespeichertes Token. Den Login übernimmt die CI-Component `ci-components/deployment`. Das Deployment-Repo setzt nur zwei Inputs. Eine Anleitung für Anwender folgt mit DEV.

> **Lab-PoC:** Bisher gibt es nur das Lab-OpenBao. Die JWT-Rollen legen Betreuer an.

Voraussetzungen

- Das Repo nutzt die CI-Component `cloud-core-infrastructure/ci-components/deployment`.
- In OpenBao gibt es eine JWT-Rolle für das Projekt. Sie ist an Projekt, Branch und geschützten Branch gebunden.
- Der Branch ist geschützt. Alle vier Stage-Branches sollten es ohnehin sein.
- Der Runner erreicht OpenBao direkt auf Port 8200.

Vorgehen

1. Inputs im `include` setzen:

   ```
   include:
     - component: $CI_SERVER_FQDN/cloud-core-infrastructure/ci-
   components/deployment/terraform@<version>
       inputs:
         openbao-jwt-role: <rolle>
         openbao-addr: https://openbao-lab-bre1.dexpro.parts:8200
   ```

   - `<version>`: Version bzw. SHA der Component, auf die das Repo pinnt
   - `<rolle>`: JWT-Rolle des Projekts in OpenBao
2. Im Terraform-Code den Vault-Provider ohne Zugangsdaten konfigurieren. Er liest Adresse und Token aus der Umgebung:

```
provider "vault" {}
```

3. Pipeline auf dem Stage-Branch starten.

Was dann passiert: Die Jobs `plan`, `deploy` und `destroy` holen sich vor `tofu` das JWT, prüfen die Erreichbarkeit von OpenBao und tauschen das JWT gegen ein kurzlebiges Token (15 Minuten, höchstens 1 Stunde). Es steht nur in der Shell des Jobs als `BAO_TOKEN`/`BAO_ADDR` und `VAULT_TOKEN`/`VAULT_ADDR` bereit und wird nie ausgegeben.

Prüfen

> Der Job meldet den erfolgreichen Login, und `plan` liest die erwarteten Secrets. Ein Zugriff auf fremde Pfade oder eine andere Stage endet mit 403.

Stolperfallen

- **MR-Pipelines und ungeschützte Branches** melden sich nie an. OpenBao lehnt den Login ab. Mit gesetzter Rolle entfällt `plan` in MR-Pipelines.
- `openbao-addr` hat bewusst keinen Default. Ist die Rolle gesetzt und die Adresse leer, bricht der Job ab.
- Die Adresse ist zugleich die Audience des JWT. Sie muss exakt so lauten wie in der Rolle hinterlegt.
- Module und Jobs melden sich nie selbst an. Sie lesen nur das bereitgestellte Token.
- Ist der Runner nicht freigeschaltet (Firewall auf Port 8200), scheitert schon die Erreichbarkeitsprüfung.

Weiterführend

- README der CI-Component, Abschnitt „OpenBao-Login“
- Pfadschema und Teamtrennung
- OpenBao: JWT/OIDC-Anmeldung

Revision #1
Created 2026-11-06 17:36:28 UTC by Alexander Golembek
Updated 2026-11-06 17:36:28 UTC by Alexander Golembek