Secret anlegen

> Zielgruppe: Betreuer · Stand: 06.11.2026

Secrets entstehen auf genau zwei Wegen: Menschen legen sie nach dem Login per OIDC in der OpenBao-Oberfläche an, Pipelines schreiben sie mit ihrem GitLab-JWT. Andere Wege wie Admin-Token oder lokale Skripte sind nicht vorgesehen. Eine Anleitung für Anwender folgt, sobald es OpenBao in DEV gibt.

> **Lab-PoC:** Der OIDC-Login (Entra ID) kommt erst mit DEV. Bis dahin entstehen Secrets im Lab nur über Pipelines.

Voraussetzungen

- Du kennst Abteilung, Team bzw. Standort und Projekt sowie die Stage (siehe Pfadschema und Teamtrennung).
- **Oberfläche:** Du bist Mitglied der Entra-Gruppe deines Teams und im internen Netz. OpenBao ist nie über den Edge erreichbar.
- **Pipeline:** Das Projekt nutzt die CI-Component `ci-components/deployment`. Für das Projekt gibt es eine JWT-Rolle, die an Projekt, Branch und geschützten Branch gebunden ist.

Vorgehen: Oberfläche (OIDC)

1. OpenBao-Oberfläche öffnen und als Methode **OIDC** wählen, dann mit dem DEXPRO-Konto anmelden.
2. Den Mount deiner Abteilung öffnen, z. B. `cpds/`.
3. **Create secret** wählen und als Pfad den Pfad ohne Mount eintragen, z. B. `<team>/<stage>/<name>`.
4. Schlüssel und Werte eintragen und speichern.

Vorgehen: Pipeline (GitLab-JWT)

1. Die CI-Component meldet die Pipeline per GitLab-JWT an OpenBao an und stellt das Token als `BAO_TOKEN` bereit. Module und Jobs melden sich nicht selbst an.

2. Terraform schreibt das Secret mit dem Vault-Provider (Ressource `vault_kv_secret_v2`) in den eigenen Pfad, z. B. ein von `random_password` erzeugtes Passwort.
3. Die Pipeline darf nur in ihren eigenen Pfad schreiben (bei CCI auch in die `shared`-Ebenen), `production` nur von geschützten Branches.

Prüfen

In der Oberfläche zeigt das Secret unter **Version History** die neue Version mit Zeitstempel. In der Pipeline zeigt der Terraform-Plan bzw. das Apply die Ressource, aber nie den Wert.

> Erscheint die neue Version mit dem erwarteten Zeitpunkt, ist das Secret angelegt.

Stolperfallen

> Die Stage im Pfad muss exakt der Branch-Name sein (`pre-development`, nicht `lab` oder `dev`). Sonst findet die Pipeline das Secret nicht.

- Speichern in der Oberfläche legt eine neue Version an, die **alle** Felder ersetzt. Felder, die fehlen, sind in der neuen Version weg.
- Werte, die Terraform schreibt, stehen wie heute im Terraform-State.
- Für CCI gilt die Gliederung nach Standort und Projekt, nicht nach Team.

Weiterführend

- Pfadschema und Teamtrennung
- Secret-Versionen und Löschen
- OpenBao: KV Secrets Engine Version 2

Revision #1
Created 2026-11-06 17:27:40 UTC by Alexander Golembek
Updated 2026-11-06 17:27:40 UTC by Alexander Golembek