VMs per AppRole anmelden

> Zielgruppe: Betreuer · Stand: 06.11.2026

VMs, die selbst Zertifikate oder Secrets aus OpenBao holen (heute die Lab-Consul-Server), melden sich per AppRole an. Ihre Secret-ID gilt nur von der IP-Adresse des jeweiligen Hosts aus.

> **Lab-PoC:** Bisher nutzen nur die Lab-Consul-Server diesen Weg.

Wie es funktioniert

- Je Dienst gibt es **eine** AppRole, z. B. eine für alle Consul-Server.
- Für jeden Host erzeugt der Terraform-Lauf eine eigene Secret-ID. Sie ist an die Host-IP gebunden und entsteht im selben Lauf, nachdem die IP feststeht und bevor Ansible läuft.
- Die Secret-ID landet nie im Terraform-State. Sie geht über eine temporäre Datei des Runners direkt auf den Host.
- Auf dem Host liegt sie dauerhaft (nur root lesbar), damit sich der `bao agent` nach einem Neustart wieder anmelden kann. Bei Consul ist das `/etc/consul.d/openbao/secret-id`.
- Der `bao agent` holt damit die Zertifikate und lädt den Dienst bei Erneuerung neu.

Vorgehen

Die Anmeldung richten Modul und Rolle ein, es gibt keine Handarbeit. Für einen neuen Dienst:

1. Im Modul die AppRole-Anbindung nach dem Muster des Consul-Moduls übernehmen.
2. Die AppRole und ihre Policies als Konfiguration in OpenBao anlegen.
3. Deploy über die Pipeline. Die Pipeline braucht dafür eine JWT-Rolle, die Secret-IDs erzeugen darf.

Prüfen

> Die Rolle bricht im Preflight ab, wenn die Secret-ID-Datei fehlt. Läuft sie durch und hat der `bao agent` die Zertifikate geschrieben, funktioniert die Anmeldung.

Stolperfallen

> Die IP-Bindung prüft die Adresse, die OpenBao sieht. Hinter NAT (z. B. WSL) ist das eine andere als die Host-IP, und der Login scheitert.

- Bei einem Neuaufbau mit neuer IP braucht der Host eine neue Secret-ID. Die Pipeline erzeugt sie im selben Lauf.

Weiterführend

- Consul-Zertifikate aus OpenBao
- OpenBao: AppRole

Revision #1
Created 2026-11-06 17:36:32 UTC by Alexander Golembek
Updated 2026-11-06 17:36:32 UTC by Alexander Golembek