Erreichbarkeit

> Zielgruppe: Anwender und Betreuer · Stand: 06.11.2026

OpenBao ist nur im internen Netz erreichbar und nie über den Edge. Wer OpenBao nutzen will, braucht deshalb einen direkten Netzweg zu Port 8200.

Regeln

- Erreichbar ist nur der **interne Listener auf Port 8200**, über `openbao-lab-bre1.dexpro.parts:8200`.
- Port **8201** nutzen nur die Knoten untereinander. Er wird nie freigegeben.
- Der Edge leitet nichts zu OpenBao. Das ist im Lab per Negativtest belegt.
- Ohne Token liefert OpenBao nur die öffentlichen CA-Daten (CA-Zertifikat, Kette, Sperrliste).

> OpenBao nie über den Edge veröffentlichen, auch nicht vorübergehend. Oberflächen für Menschen laufen über den Edge, interne Dienste und OpenBao nie.

Zugriff für Pipelines

GitLab-Runner brauchen eine Firewall-Freigabe zu den Knoten auf Port 8200, und nur auf diesem Port. Die Freigabe richtet das Netzteam ein. Für die bestehenden Runner ist sie offen.

Prüfen vom Runner aus:

```
curl -s -o /dev/null -w '%{http_code}\n' https://openbao-lab-bre1.dexpro.parts:8200/v1/sys/health
```

> `200` (aktiver Knoten) oder `429` (Standby-Knoten) bedeutet: erreichbar.

Umgekehrt ruft OpenBao die Signaturschlüssel von GitLab (JWKS) ab, um die JWTs der Pipelines zu prüfen. Dieser Weg ist von allen Knoten aus offen.

Weiterführend

- Pipeline per GitLab-JWT anmelden
- OpenBao: sys/health

Revision #1
Created 2026-11-06 17:49:46 UTC by Alexander Golembek
Updated 2026-11-06 17:49:46 UTC by Alexander Golembek