PKI

- Offline-Root-CA und Intermediates
- Consul-Zertifikate aus OpenBao

Offline-Root-CA und Intermediates

> Zielgruppe: Betreuer · Stand: 06.11.2026

OpenBao ist die zentrale Zertifizierungsstelle (CA) der Plattform. Die Root-CA bleibt offline. In OpenBao arbeiten nur Intermediate-CAs, und zwar eine je Zweck. Diese Seite erklärt den Aufbau und warum er so gewählt ist.

> **Lab-PoC:** Bisher gibt es die Root-CA des Labs und ein Intermediate für Consul.

Aufbau

Ebene	Wo	Laufzeit	Eigenschaften
Root-CA	offline, nie auf einer VM, nie im Terraform-State, nie in OpenBao	10 Jahre	ECDSA P-384, darf nur eine Ebene Intermediates signieren
Intermediate je Zweck	eigener PKI-Mount in OpenBao, z. B. `pki-consul`	3–5 Jahre	Schlüssel verlässt OpenBao nie, Namen per Name Constraints begrenzt
Zertifikate (Leaf)	auf den Hosts	kurz, z. B. Consul 30 Tage	werden automatisch erneuert

Geplante weitere Intermediates: Nomad-TLS und Consul-Connect.

Wie ein Intermediate entsteht

1. OpenBao erzeugt im neuen PKI-Mount Schlüssel und CSR. Der Schlüssel bleibt in OpenBao.
2. Die Root-CA signiert die CSR offline auf einem abgeschotteten Rechner, in einem Speicher, der beim Ausschalten verschwindet.
3. Das signierte Zertifikat wird in OpenBao importiert.
4. Rollen im Mount legen fest, welche Namen und IPs Zertifikate bekommen dürfen.

Der Root-Schlüssel ist verschlüsselt in Bitwarden gesichert und wird nur zum Signieren kurz geladen.

Öffentliche CA-Daten

CA-Zertifikat, Kette und Sperrliste eines Mounts sind ohne Token abrufbar, z. B. für Clients, die der CA vertrauen sollen:

```
curl -s https://openbao-lab-bre1.dexpro.parts:8200/v1/pki-consul/ca_chain
```

Stolperfallen

> IP-Adressen in Rollen begrenzt nur das Feld `allowed_ip_sans_cidr`. Ein Feld `allowed_ip_sans` wird still ignoriert, und `allow_ip_sans=true` allein erlaubt beliebige IPs. Nach jeder Rollenänderung mit einer unerlaubten IP gegenprüfen (Erwartung: HTTP 400).

- Läuft ein Intermediate ab, sind alle Zertifikate darunter wertlos. Die Restlaufzeit braucht deshalb eine Überwachung.
- Leaf-Zertifikate sollen alarmieren, wenn sie weniger als 14 Tage gelten.

Weiterführend

- Consul-Zertifikate aus OpenBao
- OpenBao: PKI Secrets Engine

Consul-Zertifikate aus OpenBao

> Zielgruppe: Betreuer · Stand: 06.11.2026

Die Lab-Consul-Server holen ihre TLS-Zertifikate aus OpenBao und erneuern sie selbst. Die Consul-Clients bekommen ihre Zertifikate von den Servern. Diese Seite beschreibt den Ablauf. Das spätere Consul-Buch verlinkt hierher.

> **Lab-PoC:** Die Lab-Consul-Server sind auf diesem Weg neu aufgebaut. Die ACL-Einrichtung ist noch nicht abgeschlossen, weil sie an der abgebauten Lab-Nomad-Anmeldung hängt.

Ablauf

1. Das Terraform-Modul `proxmox/consul` legt je Server eine an die Host-IP gebundene AppRole-Secret-ID an (siehe VMs per AppRole anmelden).
2. Die Ansible-Rolle `consul` installiert `bao` und richtet den `bao agent` ein.
3. Der Agent holt aus dem Mount `pki-consul` Zertifikat und Schlüssel (Server-Zertifikat für `server.<dc>.consul` und den FQDN des Hosts, Laufzeit 90 Tage) und lädt Consul bei jeder Erneuerung neu.
4. Clients holen ihre Zertifikate per `auto_encrypt` vom Server und brauchen nur die CA-Kette. Die Kette liest das Modul ohne Token aus OpenBao.
5. Gossip-Key und ACL-Bootstrap-Token spiegelt das Modul zusätzlich nach OpenBao (KV-Mount `consul/`). Im Lab bleibt Bitwarden dafür führend, in DEV soll OpenBao allein die Quelle sein.

Versionen

- Modul `proxmox/consul`: Linie 0.3 nur mit dem OpenBao-Weg, ab 0.3.1. Version 0.3.0 nicht verwenden, sie enthält noch den alten Stand. Die Linie 0.2 bleibt für den Bestand.
- Die Pipeline des Stacks braucht `BAO_TOKEN` per GitLab-JWT (siehe Pipeline per GitLab-JWT anmelden) sowie `curl` und `jq` im Runner-Image.

Prüfen

> Der `bao agent` schreibt nach jedem Rendern eine Statusdatei unter `/etc/consul.d/openbao/`. Consul antwortet auf Port 8501 mit einem Zertifikat aus `pki-consul`.

Stolperfallen

> Für Zertifikat, Schlüssel und CA nur **eine** `template`-Stanza mit `pkiCert` verwenden. Drei Stanzas stellen drei verschiedene Zertifikate aus, und Schlüssel und Zertifikat passen nicht zusammen.

- `.CAChain` gibt es im Template nicht. `ca.pem` ist das Intermediate, den Root-Anteil bringt das Modul-Bundle zu den Clients.
- Lokale Verbindungen laufen über `127.0.0.1`, nie über `localhost`. Das Zertifikat enthält keinen `localhost`-Namen.
- Connect-CA über OpenBao ist noch offen. Ob der Vault-Provider von Consul mit OpenBao funktioniert, ist nicht belegt.

Weiterführend

- Offline-Root-CA und Intermediates
- OpenBao Agent