Admin-, Break-glass- und Root-Token

> Zielgruppe: Betreuer · Stand: 06.11.2026

Ohne Root-Token braucht OpenBao zwei Notfall-Zugänge: ein Admin-Token für die Administration und ein Reserve-Token (Break-glass) für den Fall, dass das Admin-Token verloren geht. Diese Seite erklärt, wozu die beiden da sind und was bei ihrer Pflege wichtig ist.

> Ohne gültiges Admin- oder Reserve-Token gibt es nach dem Widerruf des Root-Tokens keinen normalen Rückweg mehr. Im schlimmsten Fall muss OpenBao neu aufgebaut werden. Beide Token müssen deshalb immer gültig sein.

Die drei Token

Token	Zweck	Rechte
Root-Token	nur bei der Erstinstallation	alles; im Lab nach der Einrichtung widerrufen
Admin-Token	Administration und Konfiguration	Administration, ohne Zugriff auf Raw-Daten und ohne Versiegeln
Reserve-Token (Break-glass)	Notfall: neues Root-Token erzeugen	nur das Erzeugen eines Root-Tokens und die Pflege des eigenen Tokens

Admin- und Reserve-Token sind periodische Token ohne Elterntoken mit 90 Tagen Periode. Sie laufen nur dann nicht ab, wenn sie rechtzeitig erneuert werden.

Pflege

1. Beide Token spätestens alle 90 Tage erneuern, empfohlen alle 60 Tage. Eine Prüfung warnt unter 30 Tagen Restlaufzeit.
2. Token nur bei Bedarf und nur verdeckt einsetzen, nie in Dateien, Logs oder Tickets schreiben.

Stolperfallen

> Die Obergrenze für Token-Laufzeiten am Token-Mount (`max_lease_ttl`) kappt die Periode still. Mit dem Standardwert läuft ein „90-Tage“-Token nach etwa 32 Tagen ab. Die Obergrenze ist deshalb auf 90 Tage angehoben. Nebenwirkung: Auch andere Token aus diesem Mount dürfen bis 90 Tage laufen.

- Auch das Erzeugen eines neuen Root-Tokens braucht ein Token mit passendem Recht, also das Reserve-Token. Fehlt es, bleibt nur ein Notweg über eine Listener-Option auf einem Knoten. Dieser Weg ist nur im Lab erprobt und darf nur kurz und mit Freigabe genutzt werden.

Weiterführend

- Menschen-Login
- OpenBao: Token
- OpenBao: Root-Token erzeugen

Revision #1
Created 2026-11-06 17:36:39 UTC by Alexander Golembek
Updated 2026-11-06 17:36:39 UTC by Alexander Golembek