Secrets Vault

Inhaltsverzeichnis

Ein Secrets Vault speichert Zugangsdaten, Keys und Zertifikate zentral und kontrolliert. Anwendungen und Admins holen Secrets bedarfsgerecht statt sie in Configs und Repos zu hardcoden.

1 Funktionsweise

Secrets liegen verschlüsselt im Vault; Policies steuern, wer oder welcher Service was lesen darf. Oft inkl. Rotation, Audit-Log und dynamischer Credentials.

- **Central Store:** ein sicherer Quellort
- **Policy/ACL:** Least Privilege auf Secrets
- **Audit & Rotation:** Nachvollziehbarkeit und Erneuerung

2 Typische Einsatzbereiche

- CI/CD, Container und Plattform-Teams
- Datenbank- und API-Credentials
- Ersatz für Klartext in Env-Files und Wikis

3 Wichtige Hinweise

- Vault selbst ist kritischer SPOF – HA und Backup planen.
- Bootstrapping (unseal/auth) hart absichern.
- App-Integration braucht Disziplin, sonst entstehen Schatten-Secrets.

4 Fazit

Secrets Vaults beenden Passwort-Wildwuchs in Dateien – Voraussetzung für skalierbare, auditierbare Geheimnisverwaltung.