12
03/2026

Meet-up Community Days

Dynamische Secrets in der Praxis: Sicherer Zugriff auf Datenbanken via HashiCorp Vault

Leon Krass

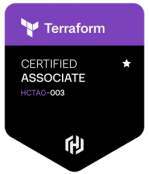
Technical Leader
HashiCorp Vault

/ Über mich

Vorstellung

Begeistert von Secrets Management und bekannt dafür, IT-Automatisierung gerne mal etwas zu overengineeren – typischerweise mit einer Portion Kubernetes-, Terraform- und Ansible-Magie.

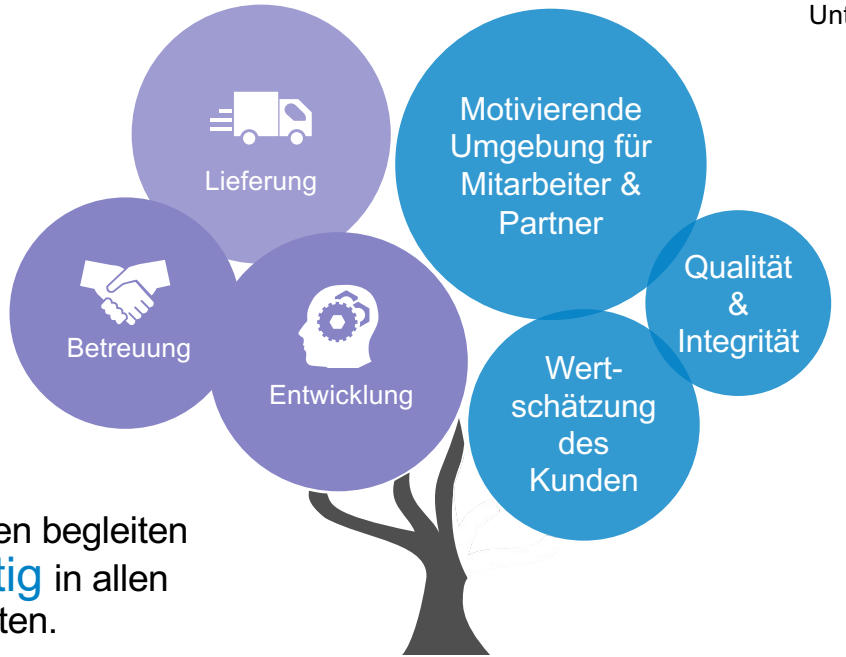
HashiCorp Vault, Kubernetes, Ansible, Terraform



Profil und Unternehmensziel

Größter inhabergeführter System-Integrator Deutschlands

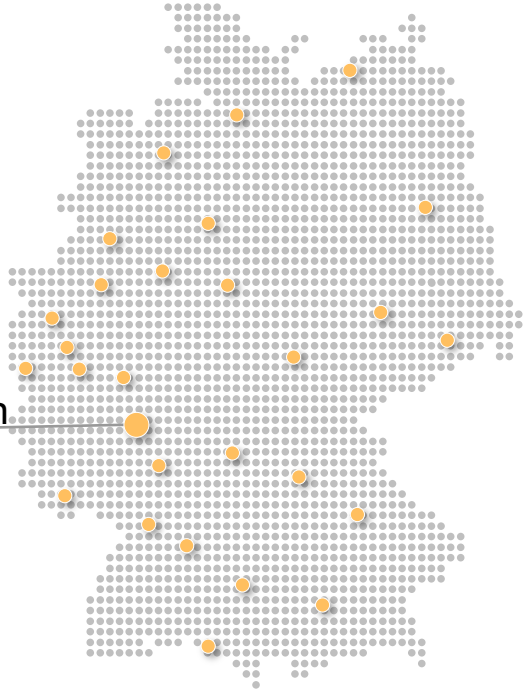
Starkes Wachstum mit mehr als 3.800 Mitarbeitern in Deutschland



Unsere Kunden begleiten wir langfristig in allen Prozessschritten.

Unternehmen

28
Standorte



BRANCHEN

wie

AUTOMOTIVE

RETAIL

PUBLIC

MASCHINEN & ANLAGENBAU

HEALTH CARE

TELEKOMMUNI-KATION

FINANCE & INSURANCE

/ Was macht uns einzigartig?

SVA …

Inhabergeführt

Hohe Mitarbeiterzufriedenheit
und Loyalität

Langfristige technische Betreuung
unserer gelieferten Lösungen

Überdurchschnittliche Kundenzufriedenheit und
Weiterempfehlungsrate

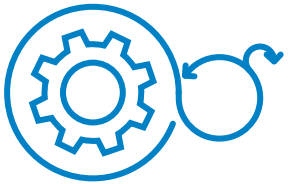
Dynamische Secrets in der Praxis: Sicherer Zugriff auf Datenbanken via HashiCorp Vault

1 Grundlagen

2 Secrets für DBs

3 Demo

4 Wrap-Up



Grundlagen

Identität, Authentifizierung & Autorisierung

- **Identität** beschreibt die eindeutig zuordenbaren Merkmale, die ein Benutzer, ein System oder ein Dienst besitzt, damit es von anderen unterschieden werden kann

- **Authentifizierung** ist der Prozess der Überprüfung, dass eine angegebene Identität echt ist

- **Autorisierung** definiert, welche Aktionen oder Zugriffe einer erfolgreich verifizierten Identität erlaubt sind

Was ist ein Secret?

- **Information**, die absichtlich **vertraulich** gehalten wird
  - → auch personenbezogene Daten
- Repräsentiert häufig ein Merkmal, das eine **Identität** beschreibt
- Werden genutzt, um Legitimität in digitalen Systemen nachzuweisen (**Authentifizierung**) und privilegierten Zugriff zu erhalten (**Autorisierung**)
- Technische Sichtweise:
  - → Passwörter, Passkeys, API-Keys, Tokens, Zertifikate, kryptografisches Schlüsselmaterial

Wo tauchen Secrets auf?

Einige Beispiele:

- ⇢ Konfigurationsdateien
- ⇢ Anwendungscode
- ⇢ Log- & Monitoring-Daten
- ⇢ Container Images
- ⇢ CI/CD Pipelines
- ⇢ Cloud Provider Metadaten
- ⇢ Betriebssystem / Dateisystem
- ⇢ Backups

… und genau dort sollten sie NICHT auftauchen!

Statische vs. Dynamische Secrets

Statische Secrets

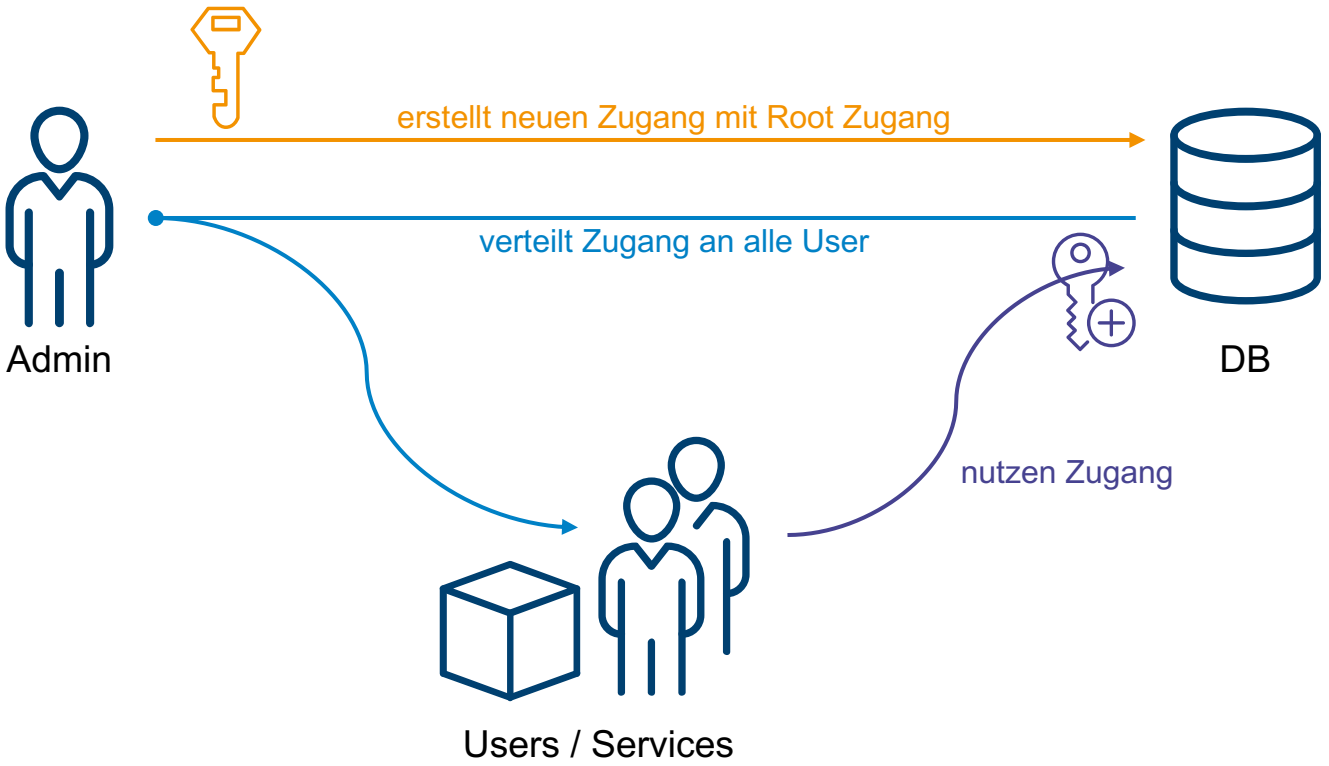
- ⇢ durch Menschen verwaltet
- ⇢ Keine automatische Rotation oder Ablaufdaten
- ⇢ Eher langlebig, häufig geteilt

Dynamische Secrets

- ⇢ Maschinell verwaltet
- ⇢ automatische Rotation und Ablaufdaten
- ⇢ An einen (kurzlebigen) personalisierten Lease gebunden


Secrets für DBs

Workflow mit statischen Secrets



Workflow mit statischen Secrets

Keine Authentizität

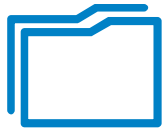
- Mehrere Nutzer teilen sich Zugang
- Zugänge sind keiner Identität zugeordnet

Langlebige Zugänge

- Zugänge nach Erlangung auch in ferner Zukunft nutzbar

Admin als Vermittler

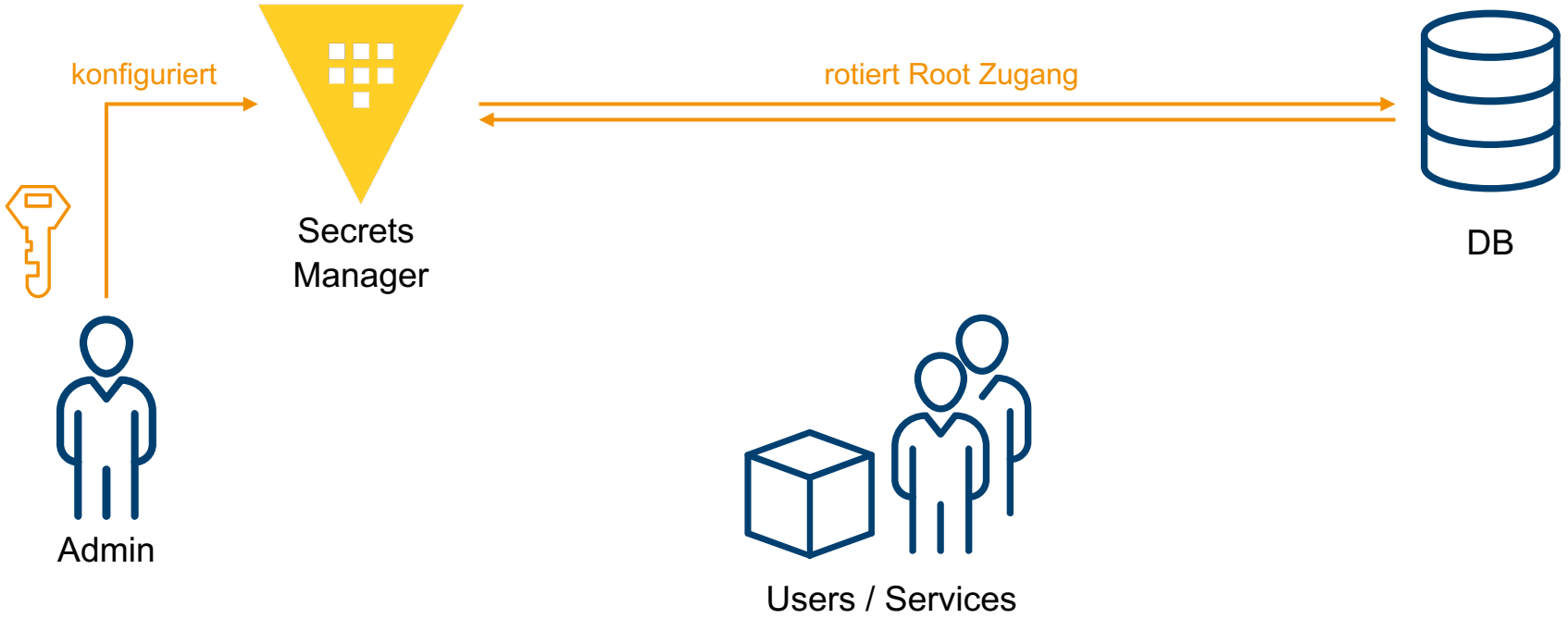
- Zugänge können abgegriffen werden



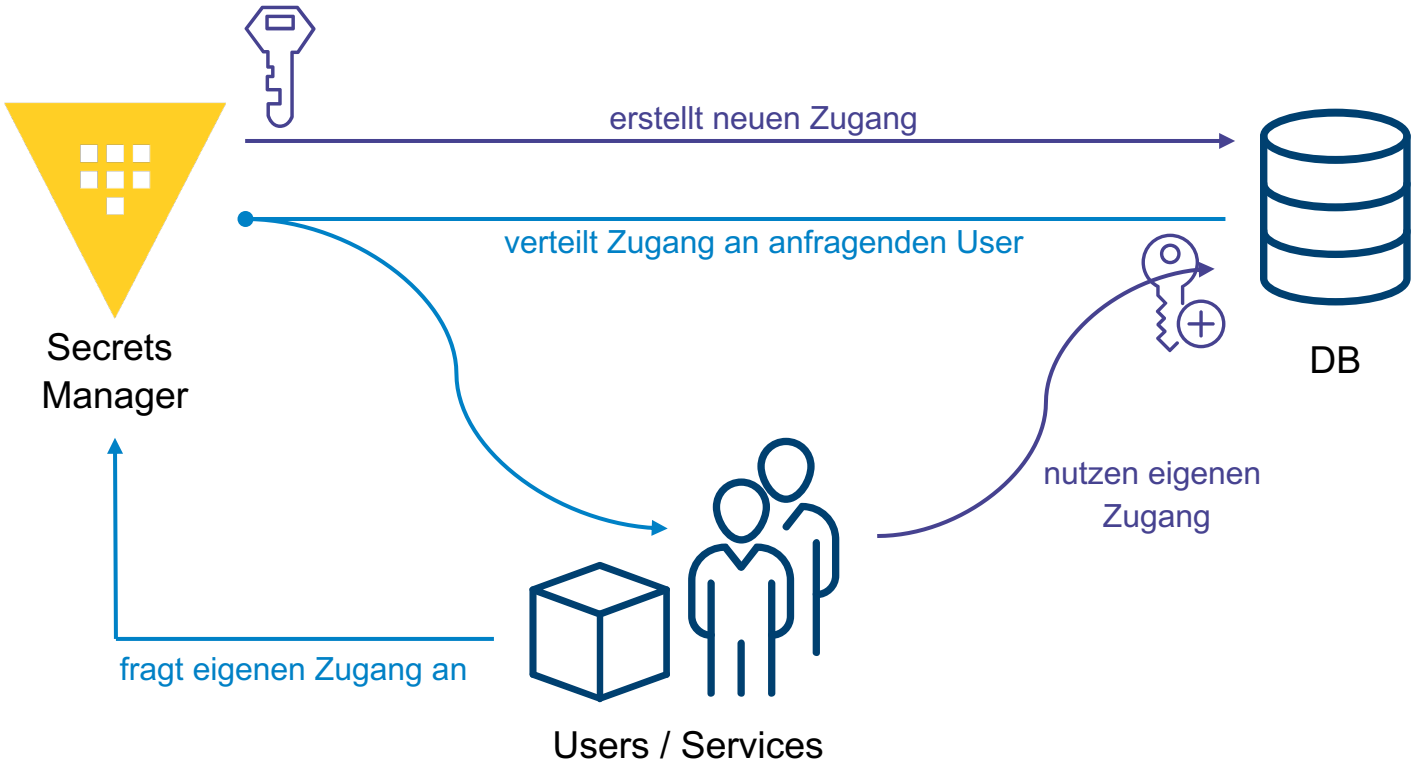
Kopien von Secrets

- Bei Übertragung der Zugänge z. B. per Mail entstehen Kopien

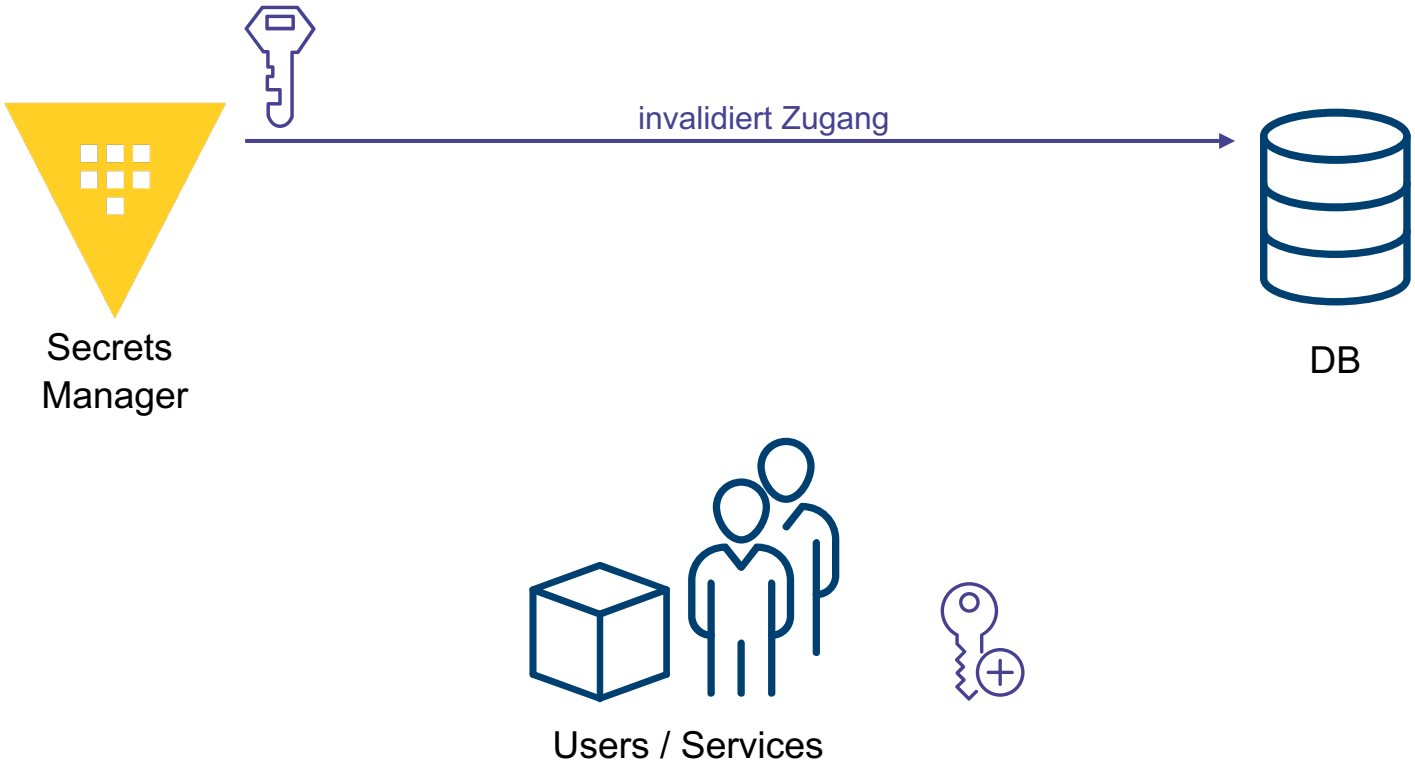
Workflow mit dynamischen Secrets



Workflow mit dynamischen Secrets



Workflow mit dynamischen Secrets



Workflow mit statischen Secrets

Authentizität

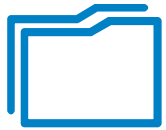
- Jeder Nutzer erhält eigene Zugänge
- Zugänge sind einer Identität zugeordnet

Kurzlebige Zugänge

- Zugänge werden nach Ablauf von TTL oder aktiv invalidiert

Sicherer Vermittler

- Steuerung durch RBAC
- Root Zugang ist gesichert



Keine Kopien

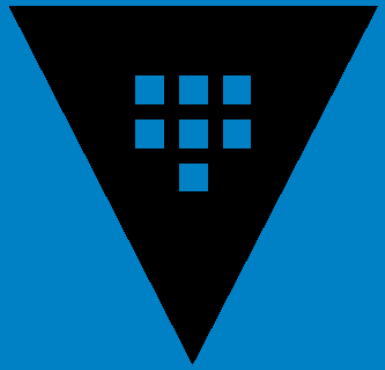
- Kein zusätzliches Medium zur Übertragung als Secrets Manager

Demo

/ Demo Tech Stack

Identity: Keycloak

- Identity und Access Management (IAM) Plattform
- Zentralisierte Authentifizierung und Autorisierung
- Nutzer Management, Identity Brokering und Föderation



Secrets: HashiCorp Vault

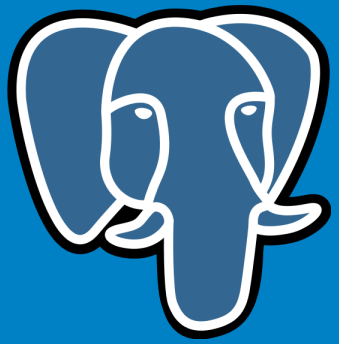
- ⇢ Sicherer Speicher und Zugang zu Secrets
- ⇢ Identitätsbasierter Zugriff auf verteilte Systeme
- ⇢ Dynamische, kurzlebige Secrets

/ Demo Tech Stack

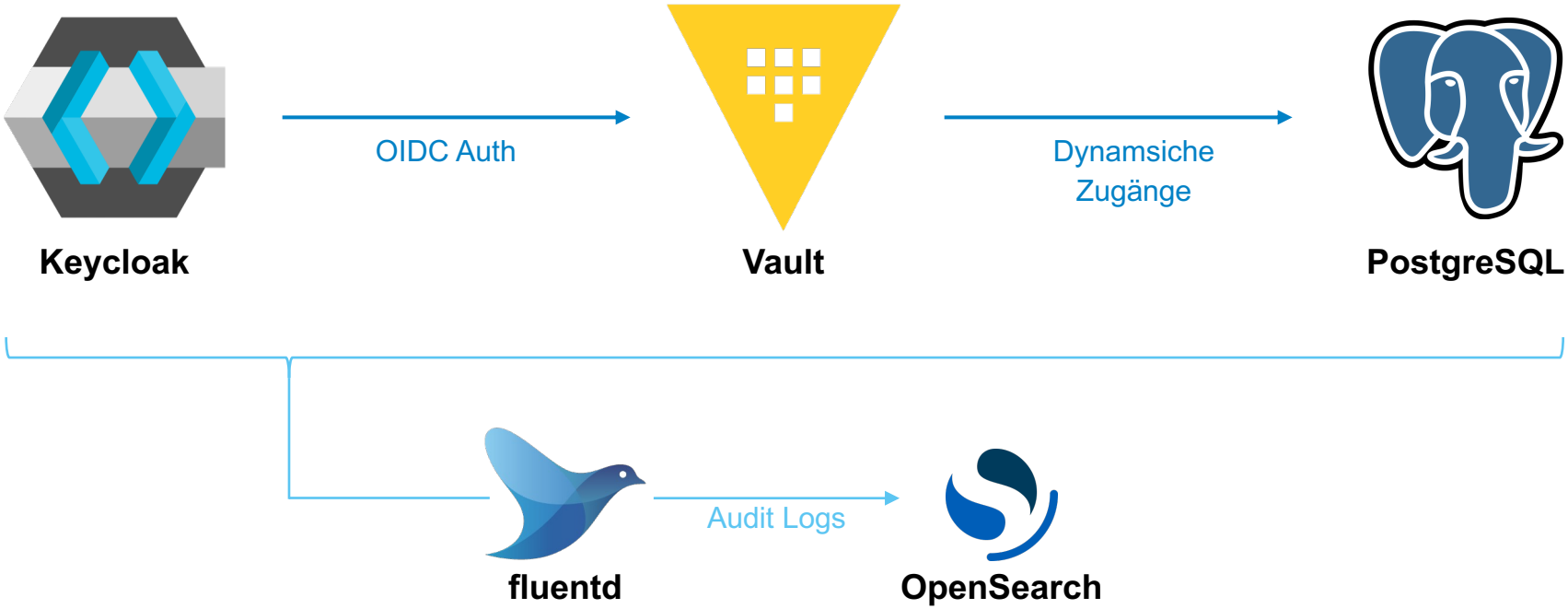
PostgreSQL

⇢ Objektrelationales Datenbanksystem

⇢ Kostenfrei & Open-Source



Architektur



Wrap-Up

Sind dynamische Secrets die Lösung aller Probleme?

Nein, aber sie verbessern unsere Cyber Security!

Weitere Herausforderungen:

- Secret Zero
  - → Wie greifen nicht-menschliche Clients auf Systeme zu?
- Timing
  - → Wie lang sollten Leases sein?
- Nutzerverhalten
  - → Wie kann verhindert werden, dass User ihre Zugänge teilen?

/ Zum Download…

Ressourcen

/ Noch Fragen?

Kontakt

Leon Krass

Technical Leader HashiCorp Vault

+49 151 53882677
leon.krass@sva.de
www.sva.de

SVA System Vertrieb Alexander GmbH
Lokation Hamburg
Große Elbstraße 273
22767 Hamburg