Keycloak – FAQ zu Ausfallsicherheit und Absicherung

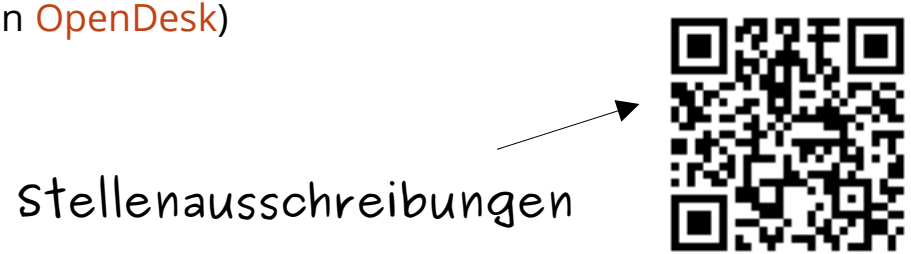
Chemnitzer Linuxtage 2025
22. März 2025

Silke Meyer
silke.meyer@univention.de
@smeyer@univention.social / @freiefunken@mastodon.social

univention

Über Univention

- Bremer Firma, spezialisiert auf Identity und Access Management (IAM) rund um OpenLDAP
- Zusammenarbeit mit öffentlichen Verwaltungen, Bildungsträgern und Firmen
- Unser Produkt „Nubus“:
  - Bündelung der Kernkomponenten OpenLDAP, Rechtemanagement, API, Keycloak, Web-GUI zur Administration, User Self-Service u.a.
  - Betrieb auf Debian-basiertem Betriebssystem (UCS)
  - Betrieb in Kubernetes-Cluster (z.B. als Bestandteil von OpenDesk)



Agenda

- Ganz kurz: Was ist Keycloak?
- Absicherung von Keycloak
  - Nutzerkonten
  - Keycloak-Installation und -Konfiguration
  - von Keycloak genutzte Dienste (IdM, DB, Cache)
  - nicht Teil des Vortrags: angebundene Dienste
- Hochverfügbarkeit von Keycloak
- Fragen und Erfahrungsaustausch

Was ist Keycloak?

Keycloak in a Nutshell I

- Identity Provider für Web Single Sign-on

  → mit einem Login in der Browsersession auf mehrere Webanwendungen zugreifen
- Zusammenziehen der Login-Vorgänge für diverse Webanwendungen an einer zentralen Stelle
- Authentifizierung gegen vorhandenes Identity Management System (z.B. OpenLDAP, AD)
- Kontrolle über Nutzerattribute, die an die Dienste herausgegeben werden

Keycloak in a Nutshell II

- Freie Software aus dem Hause RedHat (Apache 2.0-Lizenz), Java, Datenbank
- mehrere Protokolle (SAML 2.0, Oauth 2.0, OIDC 1.0)
- Webinterface und/oder API zur Konfiguration
- ausgelegt auf Betrieb in Cloud-Infrastrukturen: Skalierbarkeit, Clusterfähigkeit
- Plugin-Ökosystem
- Betrieb in Container oder aus entpacktem Archiv mit Startskript
- Freie Alternativen: Shibboleth IdP (SAML/OIDC), Authentik (SAML/OIDC/SCIM), SimpleSAMLphp (SAML)

Absicherung von Keycloak

Absicherung der Nutzerkonten

- Passwort-Richtlinien (Authentication → Policies für lokale Nutzerkonten)
- Brute-Force-Schutz (Bordmittel und/oder fail2ban)
- Datensparsamkeit:
  - Beschränkung auf das Vorhalten der nötigsten Attribute in Keycloak
  - feingranulare Regeln zu Herausgabe von Attributen an angebundene Dienste, ggf. eigene Scopes[1] definieren
- Zwei- oder Mehrfaktor-Authentifizierung am Identity Provider

[1] In OIDC ist ein Scope ein „thematisch gebündeltes Päckchen“ mit mehreren Nutzerattributen

Mehrfaktor-Authentisierung

- Identity Provider als potentielles Angriffsziel besser von unbefugten Zugriffen auf Nutzerkonten schützen
- Idee der Zwei-(Mehr-)Faktor-Authentisierung:
  - (1) Wissen (Usernamen und Passwort)
  - (2) Besitz (Gerät, Smartphone, Hardware-Token, TAN-Generator)
  - (3) Biometrie
- möglichst: Eingabe der 2 Faktoren über zwei unterschiedliche Geräte und mit expliziter Nutzerinteraktion
- Schutzbedarf eruieren → geeignete Faktoren auswählen

Design-Entscheidung

- Integration der Token-Verwaltung in eigener Infrastruktur betrachten
- Nutzung der folgenden Features bedeutet eine Verlagerung der 2FA-Verwaltung in Keycloak hinein
- Keycloak bietet Schnittstelle zur Selbstverwaltung der Faktoren durch Nutzer*innen
- Wiederherstellung durch Endnutzer*innen, z.B. bei Geräteverlust:
  - wenn mehrere verschiedene Faktoren hinterlegt sind, die von verschiedenen Geräten eingeben werden
  - über das Preview Feature „Recovery Codes“

MFA: Überblick über mögliche Faktoren

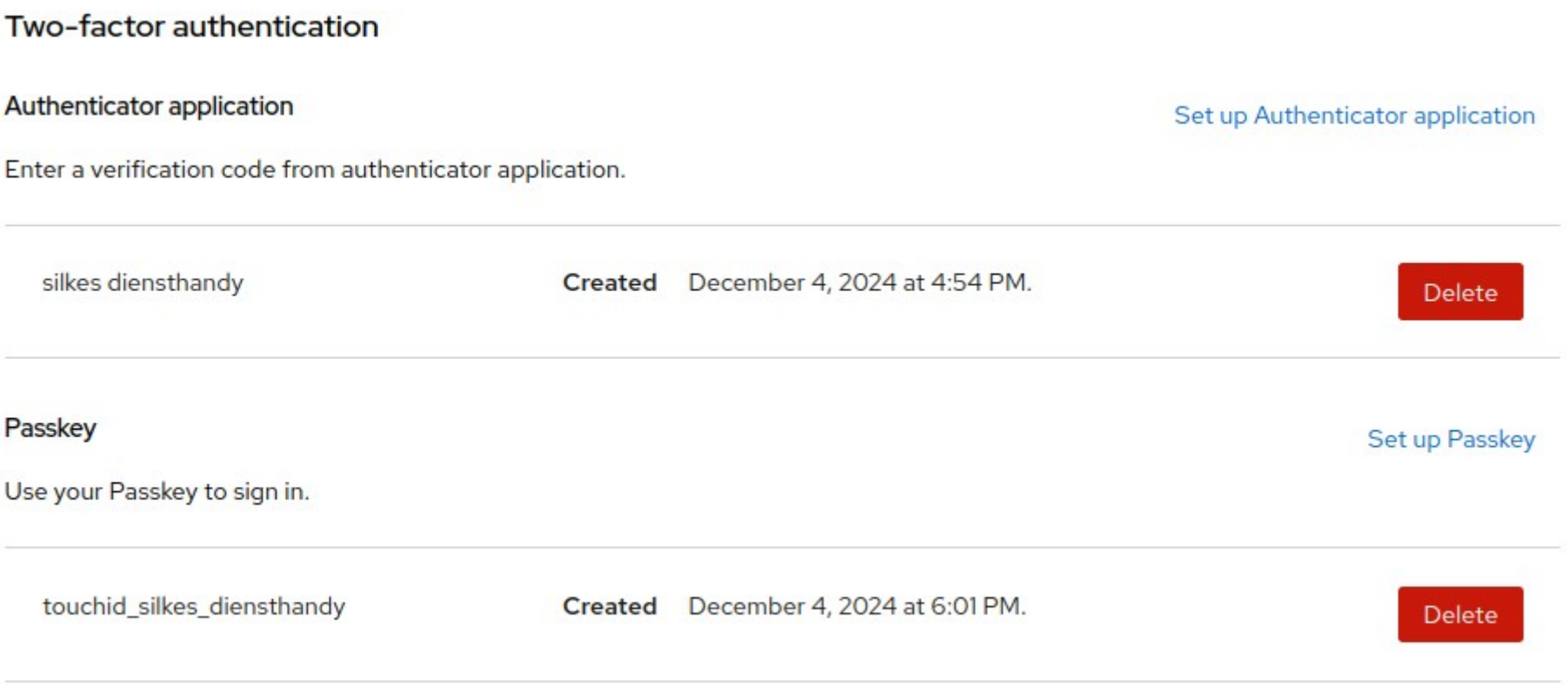
- Doku
- ohne Berücksichtigung von Plugins
- Einmalpasswörter mit Smartphone-App (TOTP)
- Webauthn / FIDO 2 (oder Vorgänger U2F) mit USB-Tokens oder Lesegeräten für biometrische Credentials (siehe Vortrag S. Schumacher zu „Passkeys“ morgen)
- der Vollständigkeit halber: x509-Zertifikate (siehe Keycloak-Dokumentation)
- Einrichtung eines zweiten Faktors beim nächsten Login verpflichtend machen: möglich über Gestaltung des Authentication Flows

MFA durch Nutzer*innen verwalten lassen

» Realm-Einstellungen: User-Managed Access

» Aktiviert das Account Management durch die Nutzer*innen unter `https://login.example.org/realms/myrealm/account`

MFA in den Kontoeinstellungen



Keycloak: Absicherung der Installation

- Quellen: Abschnitt „Mitigating Security Threats“ in der Keycloak-Dokumentation, Buch „Keycloak – Identity and Access Management for Modern Applications“
- Keycloak aktuell halten (keine LTS-Version bei frei erhältlicher Version)
- Erreichbarkeit (nur) über HTTPS (heute mind. TLS 1.2, besser TLS 1.3)
- bei Loadbalancing mit SSL-Terminierung: Neuverschlüsselung des Traffics LB → KC
- Keycloaks Hostname in Realm-Einstellungen explizit setzen
  - KC verwendet sonst Host Header aus eingehenden Requests
  - Angriffsvektor bei Links zum Passwort-Reset

Keycloak: Absicherung der Installation

- Abschnitt „Rotating Keys“ in der Keycloak-Dokumentation
- regelmäßige Rotation des Schlüsselmaterials bei Signierung und Verschlüsselung der SAML-/OIDC-Kommunikation
  - Keycloak ermöglicht unterbrechungsfreien Tausch
  - Ablauf älterer, unbenutzter Tokens

Keycloak-Absicherung über Firewall / WAF

- Absicherung bestimmter Endpunkte
  - Keycloak Admin Console
  - REST API
- Notwendig sind:
  - eingehender Traffic auf Port 443
  - ausgehender Traffic zum Identity Management System (z.B. OpenLDAP)
  - ausgehender Traffics zur Keycloak-Datenbank
  - ausgehende Requests über HTTPS zu angebundenen Anwendungen (z.B. für Logout Requests) oder zu anderen Identity Providern (z.B. für Token Requests)

Keycloak-Datenbank

- enthält die gesamte IdP-Konfiguration inkl. angebundenen Anwendungen
- bei lokalen Nutzerkonten: Konten und gehashte Passwörter
- ggf. LDAP Bind-Credentials, private Schlüssel für Signaturen, SMTP-Credentials

  → hierfür bei entsprechendem Schutzbedarf: Vault verwenden
- Firewall vor die DB
- nur authentifizierte Zugriffe auf DB erlauben, wenn über Netzwerk, dann über TLS
- Datenbank-Backups an einem sicheren Ort aufheben

Infinispan: Keycloaks Session Cache

- enthält keine Informationen über die Nutzerkonten oder Signing Keys, nur Sessions
- keine Verwendung der Session-Information ohne signierten Token oder Cookie
- Cluster-Traffic kann, wenn gewünscht, verschlüsselt werden
- verschiedene Wege → der einfachste mit symmetrischer Verschlüsselung
  - Shared Secret im Java Keystore auf jedem Node ablegen
  - Cache-Konfiguration conf/cache-ispn.xml bearbeiten (Beispiel für verschlüsselte udp-Kommunikation in Keycloak-Doku)

Hochverfügbarkeit von Keycloak

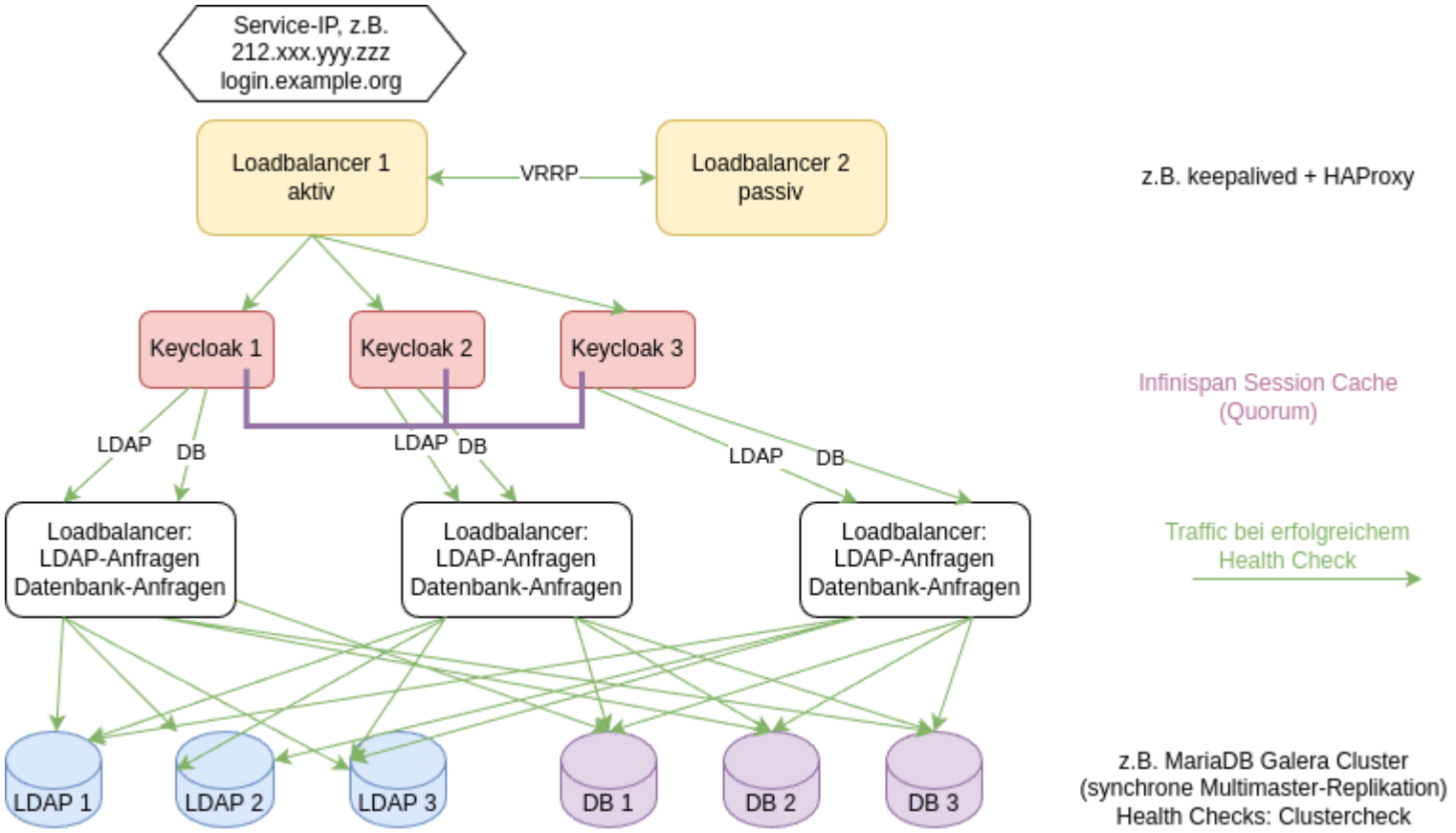
Hochverfügbarkeit von Keycloak

- Je mehr Anwendungen nur über den IdP / Keycloak zugänglich sind, desto wichtiger ist seine Ausfallsicherheit,
  - damit die Leute arbeiten können.
  - damit die Admin*s mitten am Tag Wartungsarbeiten durchführen können.
- Zusammenspiel vieler Ebenen
- hier Fokus auf die involvierten Dienste, keine Betrachtung der Komponenten tiefer im Stack (ggf. Virtualisierung, Storage etc.)
- keine Betrachtung vom Betrieb im Kubernetes-Cluster

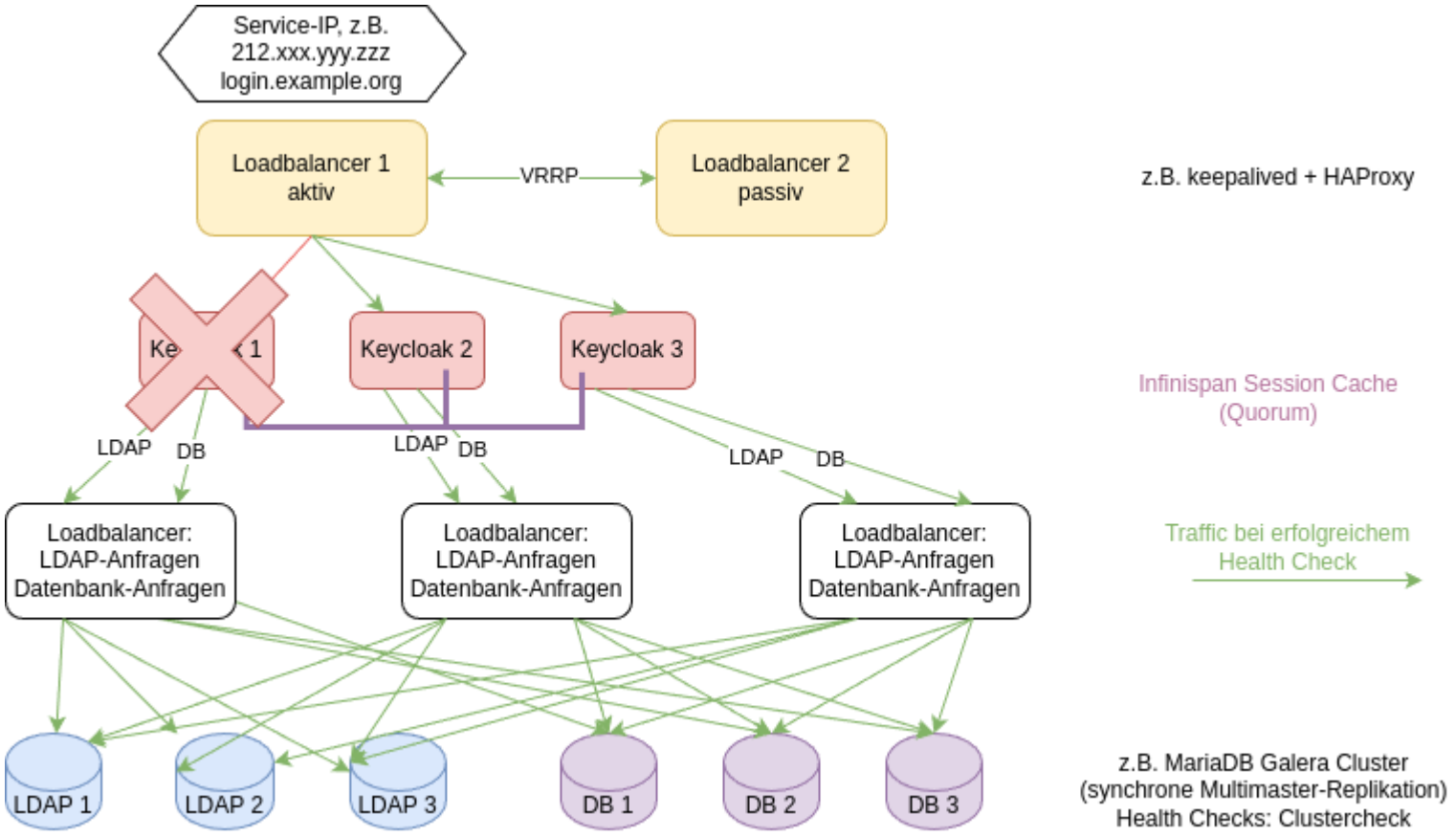
Umsetzungsbeispiel

- zwei Loadbalancer (z.B. keepalived / HAProxy), Service-IP für IdP am aktiven LB
- drei Keycloak-Instanzen mit Austausch der Session-Informationen über Infinispan
- Identity Management System über Service-IP / virtuellen Hostname
- Datenbank-Cluster (z.B. MariaDB Galera Cluster mit drei Datenbankservern) ebenfalls über Service-IP / virtuellen Hostname ansprechen

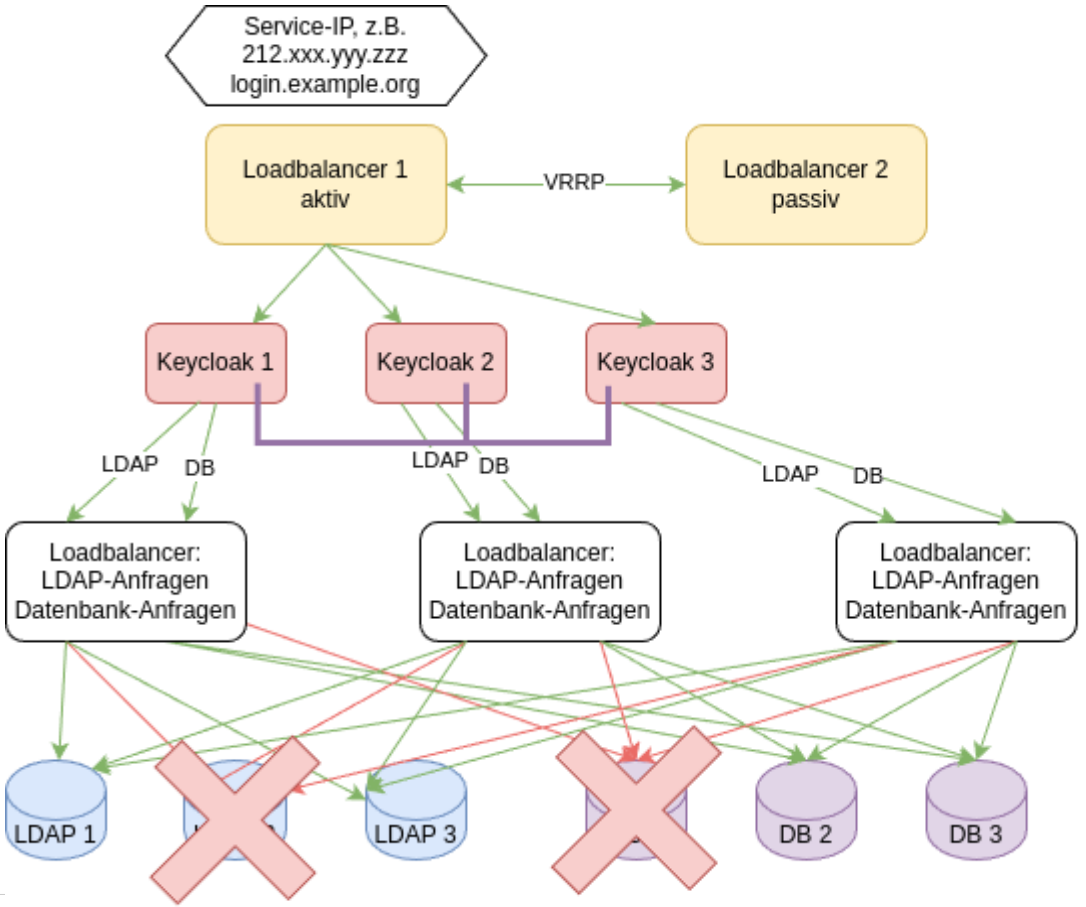
Beispielszenario



Beispielszenario



Beispielszenario



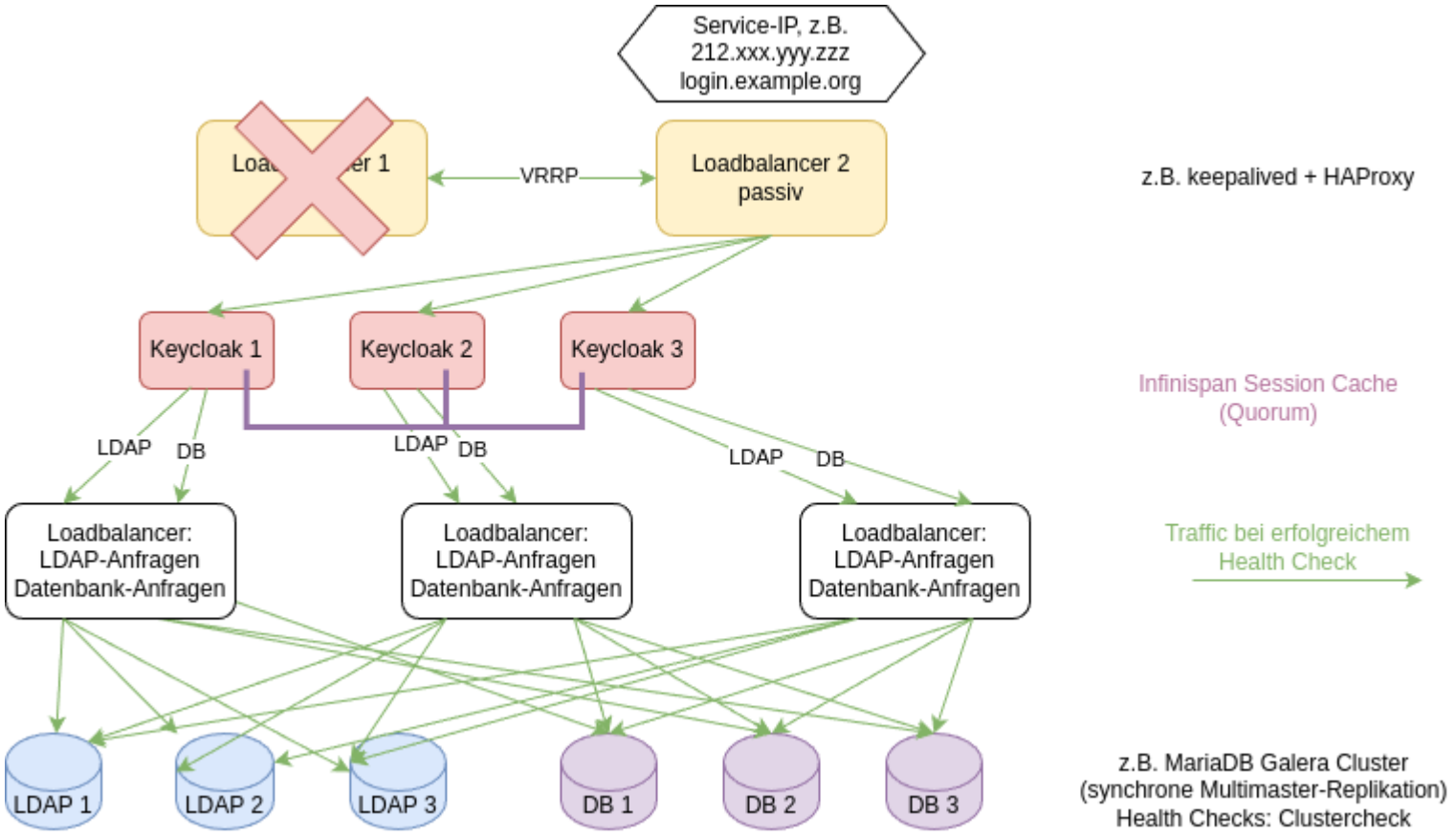
z.B. keepalived + HAProxy

Infinispan Session Cache
(Quorum)

Traffic bei erfolgreichem
Health Check

z.B. MariaDB Galera Cluster
(synchrone Multimaster-Replikation)
Health Checks: Clustercheck

Beispielszenario



Links

- Keycloak Dokumentation und Guides
- Buch: Stian Thorgersen, Pedro Igor Silva: Keycloak – Identity and Access Management for Modern Applications, Packt Publishing, Birmingham/Mumbai 2023 (2. Aufl.)
- HAProxy Configuration Manual
- BSI: Technische Betrachtung: Sicherheit bei 2FA-Verfahren
- eher für Entwickler*innen: Vortrag von Matthijs Melissen „Single Sign-on: A Hacker's Perspective“

Kontaktdaten

Silke Meyer
IT Consultant
<silke.meyer@univention.de>
+49 421 22232-106

Univention GmbH
Mary-Somerville-Str. 1
28359 Bremen

Univention GmbH Berlin
Mariannenstr. 9-10
10999 Berlin

Univention North America Inc.
7241 185th AVE NE #3206
Redmond, WA 98073-3206