Proxmox Virtual Environment (PVE) - tokoeka.netzwissen.de

Die Architektur lehnt sich an die three tier Architektur professioneller Rechenzentren an. Applikations-Server sind **nicht "internet-facing"**, sondern werden über den SSL Accelerator/Load Balancer adressiert. ssh Zugriff ist nur aus dem internen Netz des Root Servers möglich.

Ein zentraler haproxy Container dient als SSL Accelerator (optional für Load Balancing). Applikationen laufen in lxc Containern. die, wo immer möglich, *Unprivileged* laufen. Wo es sinnvoll ist, werden mehrere Services in einem gemeinsamen Container zusammengefasst. Leistungs-hungrigere virtuelle Maschinen unter KVM werden nur genutzt, wenn Anwendungen selbst als Container in einem Docker-Host laufen (docker1, docker2, docker3).

Datenbanken laufen in getrennten Datenbank-Containern für mariadb und postgresql, getrennt vom Applikations-Container. Persistente Daten werden in eigenen *.raw oder *.qcow Images geführt. Backups landen über PVE auf einer separaten Hetzner storagebox. PVE nutzt zur Zeit noch kein Clustering und keine Object-Storage (CEPH, AWS S3), kann aber umgestellt werden.

112 Load Balancer lb1 - devel.netzwissen.de

- extern **138.201.52.38** , intern **10.10.10.21**
- DNS: Hosts/Services gehen per CNAME auf devel.netzwissen.de
- Haproxy nimmt https Request an, agiert als ssl Accelerator und verteilt Web-Services auf die app Server
- optional: Load Balancing
- der lokale sshd ist verlegt auf 222.

108 Identity Provider kc1 - login.netzwissen.de

- 10.10.10.20
- keycloak 20.x
- haproxy reverse proxy » 8080
- https://www.keycloak.org/documentation
- https://www.keycloak.org/getting-started/getting-started-zip
- https://www.keycloak.org/docs/latest/server_installation/index.html

Daten

123 db1b - 10.10.10.16

- ubuntu 20.04 focal (upd. 7.5.23)
- mariadb 10.4
- Web Administration https://netzwissen.de/phpmyadmin/ (» app1)

124 db2b - 10.10.10.18

- Zentrale postgresql Datenbank
- Web Administration https://netzwissen.de/phppgadmin/ (» app1)

103 db3b - 10.10.10.35

- Zentrale mongodb Datenbank
- V 4.4.4
- turnkeylinux

Applikationsserver Docker KVM

120 docker1 10.10.10.14

Ubuntu 22.04 LTS jammy

Portainer: p. 8000

OpenSlides: under construction

drone.netzwissen.de

- DRONE: p. 8010

hedgedoc.netzwissen.de

- Hedgedoc: p. 8004

116 docker2 10.10.10.33

forum.netzwissen.de

- Discourse
- p. 10.10.10.33:84
- Container local_discourse/data
- Container local_discourse/web_only

talk.netzwissen.de

- Rocket Chat 5.x
- p. 10.10.10.33:3000
- https://talk.netzwissen.de
- Container rocket.chat
- Container bitnami/mongodb:4.4

104 docker3 10.10.10.35

* ubuntu 22.04 LTS jammy * docker CE

Applikationen

- portainer: 0.0.0.0:8000→8000/tcp, :::8000→8000/tcp, 0.0.0.0:9000→9000/tcp, :::9000→9000/tcp, 9443/tcp
- ocis: 0.0.0.0:9200→9200/tcp, :::9200→9200/tcp
- passbolt:0.0.0.0:80→80/tcp, :::80→80/tcp, 0.0.0.0:443→443/tcp, :::443→443/tcp

Applikationsserver LXC

111 app1 - devel.netzwissen.de

- 10.10.10.22
- 10.10.10.22:82 hugo
- https://www.netzwissen.de/phpmyadmin nach db1
- https://www.netzwissen.de/phppgpadmin nach db2
- Ubuntu 22 LTS jammy
- php 8
- APACHE

113 app2 - 10.10.10.25

- https://passbolt.netzwissen.de » 10.10.10.25:81 - cake php
- https://cryptpad.netzwissen.de » 10.10.10.25:3020 - nodejs
- Ubuntu 20 LTS focal
- NGINX

121 app3old - 10.10.10.26 INACTIVE

- https://cloud.netzwissen.de ~~(ownCloud Enterprise) » 10.10.10.26:83~~
- https://wiki.netzwissen.de ~~» 10.10.10.26:82~~
- ~~Ubuntu 22 LTS jammy~~
- ~~APACHE~~
- ~~php 7.4 + 8~~

127 app3 - cloud.netzwissen.de

- 10.10.10.26:83 ownCloud Enterprise
- Ubuntu 20 LTS focal
- APACHE
- php 7.4

- recovered from snapshot 04.03.23

117 app4 - 10.10.10.27

- https://solardenkmaeler.de (p.81)
- https://freifunk-esslingen.de (p.82)
- https://netzwissen.eu (p.83)
- Ubuntu 20 LTS focal
- NGINX

118 app5 - 10.10.10.28 INACTIVE

- Python 3.8 environment, python-venv
- https://mv.netzwissen.de openslides 3.3 mit DB Backend postgresql (db2)
- Ubuntu 20 LTS focal

100 app6 - netzwissen.de

- 10.10.10.30
- https://netzwissen.de » /var/www/netzwissen.de
- https://netzwissen.de/matomo/ » /var/www/matomo
- https://netzwissen.de/webmail/ » roundcube /var/www/roundcube
- ubuntu 22.04 LTS jammy, php 8
- APACHE

125 app7 - 10.10.10.37

pixelfed

122 app8 - matrix.netzwissen.de

- 10.10.10.36
- Dendrite (Go)

115 app9 - 10.10.10.23 INACTIVE

- ~~10.10.10.23 port 80 (nginx)~~
- ~~OCIS Prod~~

110 app10 - wiki.netzwissen.de

- 10.10.10.19 port 82 (apache2)
- ubuntu 22.04 LTS
- php 8

126 app11 - 10.10.10.17

- 10.10.10.19 port 82 (apache2)
- ubuntu 22.04 LTS
- php 8

109 app12 - 10.10.10.38

- ubuntu 20.04 LTS

128 app14 - 10.10.10.38 INACTIVE

- ubuntu 20.04 LTS

114 mail - Mail Server - mail.netzwissen.de

- lxc, externe IP 136.243.85.153
- dovecot imaps pops
- postfix smtp
- ubuntu 22.04 LTS jammy
- http://mghadam.blogspot.com/2019/11/how-to-proxy-ssl-imappop3smtp-using.html
- https://wiki.dovecot.org/HAProxy
- https://www.haproxy.com/de/blog/efficient-smtp-relay-infrastructure-with-postfix-and-load-balancers/

119 gitea1 - gitea.netzwissen.de

gitea.netzwissen.de geht wg. der ssh port 22 Verwaltung über gitea NICHT über den load balancer lb1. Der normale ssh Port wird nur für git genutzt, Shell Zugang nur vom Host aus über pct enter.

- 10.10.10.29, extern 136.243.85.155
- https://gitea.netzwissen.de
- letsencrypt lokal
- gitea horcht auf localhost:3010 - golang, systemd
- NGINX reverse proxy

102 idp5 - 10.10.10.17 KVM INACTIVE

Univention UCS - nur temporär (138.201.52.53)