netzwissen.de Server-Landschaft

Server und Dienste werden bei Hetzner und ausgelagert betrieben. Server bei Hetzner laufen virtualisiert über Proxmox PVE in lxc Containern oder als Docker Container in KVM VMs. Ergänzend gibt es Hetzner Cloud Instanzen. Dazu kommt das Hausnetz Urbanstrasse.

- PVE tokoeka Doku
- Öffentliche Dokumentation Proxmox
- Lokales Netz Urbanstrasse

Hetzner AG

Primäre Domäne @netzwissen.de, Backup-Domäne @netzwissen.eu

- EX42 #1011951, FSN1-DC8, RZ Falkenstein
- tokoeka.netzwissen.de 138.201.52.41
- PVE single node Setup
- Subnetz **ipv4 public 1** an vmbr0: 138.201.52.1/26
- Subnetz **ipv4 public 2** an vmbr0: 136.243.85.128/27
- Subnetz **ipv4 privat** an vmbr1: 10.10.10.1
- Subnetz **ipv6**: 2a01:4f8:172:d22:: / 64

DNS Rekursive Server

```
185.12.64.1
185.12.64.2
2a01:4ff:ff00::add:1
2a01:4ff:ff00::add:2
```

Kosten Server

- Server 39,00 €/mtl. netto, 46,41 € brutto
- BX30 Storage, 1 TB, 7,90 €/mtl. netto, 9,40 € brutto
- Zusatz IPs x 4, 12,12 €/mtl brutto, Setup pro neuer IP einmalig 22,61 €

Netzwerk tokoeka

Auf der physischen eth0 existieren zwei virtual bridges, vmbr0 für das öffentliche Netz und vmbr1 für ein privates Netzsegment, das nur zwischen den Containern/VMs existiert. Bridge vmbr0 arbeitet mit einer großen Netzmaske, um beide von Hetzner zugewiesenen Subnetze zu erlauben.

Physical Interface	IP/route/port	Bridge	Network/Mask	Mask	Gateways	Info
enp0s31f6	138.201.52.41	vmbr0	138.201.52.1/26	255.255.255.192	138.201.52.1	public network

Physical Interface	IP/route/port	Bridge	Network/Mask	Mask	Gateways	Info
		vmbr0	136.243.85.128/27	255.255.255.224	136.243.85.129	public network
		vmbr1	10.10.10.1	255.255.255.0	10.10.10.1	internal network

Das interne Netz auf vmbr1 ist nur für Kommunikation zwischen Containern/VMs gedacht. Die interne Bridge arbeitet mit NAT Masquerading, damit interne VMs/Container aktualisiert werden können. Ausgehende Pakete werden per iptables auf die IP des root Servers umgeschrieben und Antwortpakete wieder zurück geroutet (siehe https://pve.proxmox.com/wiki/Network_Configuration#_masquerading_nat_with_tt_span_class_monospaced_iptables_span_tt)

```
auto vmbr1 \\ iface vmbr1 inet static \\ address 10.10.10.1 \\ netmask
255.255.255.0 \\ bridge-ports none \\ bridge-stp off \\ bridge-fd 0''

post-up iptables -t nat -A POSTROUTING -s '138.201.52.41/26' -o enp0s31f6 -j
MASQUERADE \\ post-down iptables -t nat -D POSTROUTING -s '138.201.52.41/26'
-o enp0s31f6 -j MASQUERADE

**DNS (ipV4 + ipV6)**

<code>
213.133.98.98
213.133.99.99
213.133.100.100

2a01:4f8:0:1::add:1010
2a01:4f8:0:1::add:9999
2a01:4f8:0:1::add:9898
```

Samba

Auf tokoeka läuft ein Samba mit einem Gast Share, um Daten von den Containern/VMs zeivintral weg zu sichern. Der Samba horcht nur auf der internen Schnittstelle (vmbr1, 10.10.10.1) und ist von allen Containern, die "privileged" sind, beschreibbar:

```
smbclient -U smbguest //10.10.10.1/guests
```

mit put werden Dateien hochkopiert

Port Weiterleitungen von außen

Für Admin Zwecke gibt es Port Weiterleitungen, die vom Host ausgehen:

* tokoeka.netzwissen.de:**8442** nach 10.10.10.16:22 - ssh auf Datenbank Container db1 (mariadb) *
tokoeka.netzwissen.de:**8452** nach 10.10.10.18:22 - ssh auf Datenbank Container db2 (postgresql) *
tokoeka.netzwissen.de:**8422** nach 10.10.10.17:22 - ssh auf UCS VM IDP *
tokoeka.netzwissen.de:**8443** nach 10.10.10.17:443 - https auf UCS VM IDP *
tokoeka.netzwissen.de:**8462** nach 10.10.10.15:22 - ssh auf Mail Container mail3

```
## Port forwarding from host
        # db1: ssh port forwarding from proxmox host to db1 container
        post-up iptables -t nat -A PREROUTING -i vmbr0 -p tcp --dport 8442 -
j DNAT --to-destination 10.10.10.16:22
        post-up iptables -t nat -A POSTROUTING -p tcp --sport 22 -s
10.10.10.16 -j SNAT --to-source 138.201.52.41:8442

        # db2: ssh port forwarding from proxmox host to db2 container
        post-up iptables -t nat -A PREROUTING -i vmbr0 -p tcp --dport 8452 -
j DNAT --to-destination 10.10.10.18:22
        post-up iptables -t nat -A POSTROUTING -p tcp --sport 22 -s
10.10.10.18 -j SNAT --to-source 138.201.52.41:8452

        # idp4: ssh port forwarding from proxmox host to idp server
        post-up iptables -t nat -A PREROUTING -i vmbr0 -p tcp --dport 8422 -
j DNAT --to-destination 10.10.10.17:22
        post-up iptables -t nat -A POSTROUTING -p tcp --sport 22 -s
10.10.10.17 -j SNAT --to-source 138.201.52.41:8422

        # idp4: http port forwarding from proxmox host to idp server
        post-up iptables -t nat -A PREROUTING -i vmbr0 -p tcp --dport 8443 -
j DNAT --to-destination 10.10.10.17:443
        post-up iptables -t nat -A POSTROUTING -p tcp --sport 443 -s
10.10.10.17 -j SNAT --to-source 138.201.52.41:8443

       # mail3: ssh port forwarding from proxmox host to mail3 container
        post-up iptables -t nat -A PREROUTING -i vmbr0 -p tcp --dport 8462 -
j DNAT --to-destination 10.10.10.15:22
        post-up iptables -t nat -A POSTROUTING -p tcp --sport 22 -s
10.10.10.15 -j SNAT --to-source 138.201.52.41:8462
```

PVE: Masquerading von intern

Damit VMs, die nur eine interne 10.x Adresse haben, auch raus können, gibt es masquerading Regeln: https://pve.proxmox.com/wiki/Network_Configuration#_masquerading_nat_with_tt_span_class_monospaced_iptables_span_tt

```
# internal private network with NAT masquerading to allow internet access
from "private only" VMs
# https://pve.proxmox.com/wiki/Network_Configuration
post-up echo 1 > /proc/sys/net/ipv4/ip_forward
post-up iptables -t nat -A POSTROUTING -s '10.10.10.0/24' -o enp0s31f6 -j
MASQUERADE
post-down iptables -t nat -D POSTROUTING -s '10.10.10.0/24' -o enp0s31f6 -j
MASQUERADE
```

IP Adressen

- Hetzner forciert den Wechsel auf IPv6. Bei Bedarf wird für einmalig 15 € ein zusätzliches IPv6

/56 Netz angelegt.

Externe IPs

Subdomains und Domains werden über DNS cname nach HAPROXY zentralisiert und auf App Server weitergeleitet.

- 138.201.52.41 tokoeka.netzwissen.de **PVE Server**
- 136.243.85.153 mail.netzwissen.de Mail Server (lxc)
- 136.243.85.155 gitea.netzwissen.de
- 138.201.52.38 devel.netzwissen.de **Zentraler SSL Accelerator/Load Balancer (HAPROXY)**
- 138.201.52.53 tmp.netzwissen.de nur für **temporär** betriebene VMs
- ~~136.243.85.156 old.netzwissen.de~~ gekündigt 28.5
- ~~138.201.52.27 mail.netzwissen.de Mail Server ALT (kvm)~~ gekündigt 28.5

Interne IPs

HAPROXY hat zwei Schnittstellen und leitet externe Requests (vmbr0) auf interne IPs und Ports (vmbr1) weiter. Applikations-Server haben nur eine interne Schnittstelle (vmbr1).

- 102 idp5 10.10.10.17
- 108 kc1 10.10.10.20
- 112 lb1 10.10.10.21
- 111 app1 10.10.10.22
- 113 app2 10.10.10.25
- 121 app3 10.10.10.26
- 117 app4 10.10.10.27
- 118 app5 10.10.10.28
- 118 app6 10.10.10.30
- 114 mail 10.10.10.24
- 115 doc1 10.10.10.23
- 119 gitea1 10.10.10.29
- 123 db1b 10.10.10.16
- 124 db2b 10.10.10.18

Temporäre IP extern

Wird nur für jeweils **eine** temporär betriebene VM benutzt.

- 138.201.52.53, Gateway 138.201.52.1
- Externer A Record tmp.netzwissen.de

Cloud Server Helsinki

- CX11 # 12757836 (1 vcpi, 2 GB RAM, 20 GB Disk)
- cloud3.netzwissen.de
- IPv4 95.217.188.165

- IPv6 2a01:4f9:c011:28bc::/64

Kosten

* Server 2,96 €/mtl. brutto (**Neuanlage ab 1.9.21** 4,15 €/mtl.) * zusätzliche Floating IP ab 1.8.21, 3,57 €/mtl. brutto

Ausgelagertes

URL	IP	Service	Anmerkung
meet.netzwissen.de	5.1.71.69	SAAS auf Mars Services	
zammad.netzwissen.de	138.201.252.143	SAAS zammad.com	

Hausnetz in der Urbanstrasse

urbanstrasse