Hetzner-Server

Auf dem Weg weg von Knipp wurde im August 2022 ein Server bei Hetzner gemietet. Der Server vom Modell AX51 steht im deutschen Rechenzentrum und wir über den Robot-User office@ping.de verwaltet.

Der Server heißt `laboratory.ping.de` (CNAME `lab.ping.de`) und ist über die IP-Adressen `167.235.0.46` und `2a01:4f8:262:445e::2` zu erreicht.

Technische Daten

- CPU: Octa-Core AMD Ryzen™ 7 3700X
- RAM: 128 GB DDR4 ECC
- HDD: 2 x 12 TB
- SSD: 512 GB NVME SSD
- Netzwerk: 1 Gbit/s
- Primäre IPv4-Adresse und /64-IPv6-Netz

Software

Das System läuft aktuell mit einem Proxmox 8.14 Image. Dies ist eine auf Debian 12 (Bookworm) basierte Virtualisierungslösung, die eine Web-Oberfläche bietet. Proxmox kann VMs (auf Basis von KVM) und Container (lxc) verwalten. Die Konfiguration richtet sich an der Doku von Proxmox. Verwendete Bridge-Namen und IP-Netze entsprechend (soweit möglich) den Beispielen der Doku.

Das Webinterface von Proxmox kann über https://laboratory.ping.de:8006/ erreicht werden.

Zum Login können die Nutzer des Systems über `pam` genutzt werden. Diese müssen aber wie folgt für Proxmox aktiviert werden:

```
pveum user add <login>@pam
pveum acl modify / --roles PVEAdmin --users <login>@pam
```

Storage

Bei der Installation des Systems wurde ein RAID-1 über beide HDDs gebildet und in einer LVM-Volumegroup verwendet. Die NVMe-SSD wurde nicht eingebunden und wird später über LVM als Cache für bestimme LVs genutzt (z.B. Mailqueue).

Netzwerk

Da aktuell nur eine öffentliche IPv4-Adresse verfügbar ist, wird diese an keine VM gebunden, sonder die benötigten Ports werden an die VMs weitergeleitet. Die VMs (und Container) sind an die interne Bridge `vmbr0` gebunden. Hier wird das interne IPv4-Netz `10.10.10.0/24` verwendet. Für IPv6 wird das Netz `2a01:4f8:262:445e:100::0/72` auf die Bridge geroutet.

haProxy

Für viele VMs/Container ist das Teilen einer IPv4-Adresse relativ problemlos. Da z.B. der Container für DNS andere Ports verwendet als die Mail-VM können diese einfach aufgeteilt werden. Problematischer wird dies mit Port 80 und 443. Diese Ports werden sowohl von der Mail-VM genutzt als auch von einem Webserver-Container. Aus diesem Grund werden Port 80 und 443 nicht an eine VM weitergeleitet, sondern auf dem Host selbst über haProxy als Reverse-Proxy weitergeleitet. Dabei nutzt haProxy für Port 80 den im HTTP-Request angegeben Host und auf 443 wird SNI zur Unterscheidung genutzt. Dies hat den Vorteil, dass haProxy eine Verbindung auf Port 443 an die Ziel-VM weiterleitet, ohne die Verschlüsselung aufzutrennen. Somit bleiben auch sämtliche Daten bis in die VM verschlüsselt und andere VMs können nicht durch Sniffen an der Bridge die Kommunikation einsehen.

Konfiguriert wird haProxy auf dem Basissystem über das Config-File `/etc/haproxy/haproxy.cfg`. Neue VMs oder Namen werden dabei als `backend` konfiguriert. Dies geschieht für Port `80` und `443` getrennt. Für eine Test-VM mit der internen IPv4-Adresse `10.10.10.2` sieht dies wie folgt aus:

```
backend testvm_https
        mode tcp
        option ssl-hello-chk
        source 0.0.0.0 usesrc clientip
        server testvm:443 10.10.10.2:443 weight 100

backend testvm_http
        mode http
        source 0.0.0.0 usesrc clientip
        server testvm:80 10.10.10.2:80 weight 100
```

Speziell ist dabei das Keyword `usesrc`, wodurch die `tproxy`-Funktion haProxy aktiviert wird. Dies bedeutet, dass die VMs die ursprüngliche IP des Clients sehen und diese auch entsprechend loggen oder filtern können.

Um die Backends zu nutzen, müssen diese in den entsprechenden Frontends für http und https hinzugefügt werden:

```
frontend http
        bind 167.235.0.46:80 transparent
        mode http

        ## exact matches
        use_backend testvm_http if { hdr(Host) -i testvm.ping.de } !{ ssl_fc }

frontend https
        option tcplog
        bind 167.235.0.46:443 transparent
        mode tcp
        tcp-request inspect-delay 5s
        tcp-request content accept if { req_ssl_hello_type 1 }

        ## exact matches
        use_backend testvm_https if { req.ssl_sni -i testvm.ping.de }
```

Über den Teil in den Klammern hinter dem `if` wird der Hostname geprüft.

Aktuelle VMs/Container

Folgende VMs und Container sind aktuell konfiguriert:

TestVM

Eine kleine Debian 11 VM mit einem Webserver zum Testen des haProxy. Abgeschaltet wenn nicht benötigt.

e.ns.ping.de

Container mit konfiguriertem Bind. Dient als Nameserver für `ping.de`, `prima.de`, `ping.ruhr` und `prima.ruhr`, um auch noch dann von Nutzen zu sein, wenn Knipp mal wieder vollständig ausfällt. Die Zonen werden aktuell von den Servern bei Knipp über `AXFR` gezogen sobald diese sich dort ändern.

Im Falle eines Ausfalls von Knipp könnte hier angesetzt werden, um z.B. `www.ping.de` auf einen anderen Webserver umzubiegen.

mail.ping.ruhr

Debian 11 (Bullseye) VM mit Docker und den Mailcow-Docker-Containern für unseren Test mit den `*.ping.ruhr`- und `*.prima.ruhr`-Domains. Das Mailcow hat alle PING- und Prima-Sites konfiguriert (nur halt mit der `.ruhr`-Endung) und kann entsprechend für Tests genutzt werden.

lilly

Debian 12 (Bookworm)

lucy

Debian 10 Buster

News-Server mit architektur-abhängigem Storage 32bit

hafen

Debian 12.

Docker Container Server:

- portainer,
- Keycloak (auth),
- Nextcloud (cloud),
- mastodon, Derzeit mit Patch beim Starten der etwas längere Nachrichten erlaubt:

  ```
  sed -ie 's/MAX_CHARS = 500/MAX_CHARS = 1500/' app/validators/status_length_validator.rb
  ```

- Matrix (Synapse Port 8448),
- Jabber (ejabberd),
- bookstack

vserver

VM für Mitglieder VPS

conf

Big Blue Button BBB Videokonferenz

zooey

u.a. wiki.ping.de (ehemals techdoc und aktiv wikis)

Revision #3
Created 2026-01-31 11:32:10 UTC by Daniel Hess
Updated 2026-04-19 20:53:22 UTC by Sven Neuhaus