Einrichtung eines Proxmox-Hostsystem

In diesem Artikel wird beschrieben, wie du einen Server mit Proxmox installierst und einrichtest. Je nach genutztem Hoster weicht die Anleitung natürlich ab. Das wir hier als Hoster Hetzner nutzen, sollte nicht als eine Bewertung unsererseits betrachtet werden. Wir empfehlen auf verschiedene Hoster zu setzen, die jedoch im Idealfall aufeinander abgestimmt sind.

Die Anleitung ist exemplarisch für eines der gerade installierten "Bleche". Falls du diese Anleitung für dein eigenes System benutzt, dann musst du Variablen wie Hostname natürlich anpassen.

FIXME Muss hier noch ein rechtlicher Hinweis à la "Keine Gewähr" hin?

Installation Proxmox-ISO auf einem Hetzner-Server

- LARA-Konsole bei Hetzner beantragen. Diese ist für 3 Stunden kostenlos.
- Upload des Proxmox-ISOs auf einen im Internet erreichbaren SMB-Share. Dieses Share wird später mit der LARA-Konsole verbunden. Alternativ kann auch ein lokales Medium über die Konsole angebunden werden. Durch den meist geringen Upload ist dies nur bedingt zu empfehlen.
- Mit LARA-Konsole verbinden und das Proxmox-ISO vom SMB-Share verbinden. Infos hierzu befinden sich im Hetzner-Wiki: http://wiki.hetzner.de/index.php/LARA
- Den Server von CD starten und Proxmox-Installation durchführen
    - Optionen -> Raid-1 (Nicht RaidZ-1)
    - Hostname: ffhost01.yadn.de
    - root-Kennwort vergeben. (Liegt bei Sebastian im Passwort-Safe) Das Passwort sollte nach der erfolgreichen Einrichtung nicht mehr genutzt werden. Zugriff nur über neu erstellte Benutzer im Webinterface oder per SSH-Key.
- Neustart bei Abschluss der Installation
- SSH-Login mit dem gerade vergebenem root-Kennwort
- SSH-Keys der Admins in ~/.ssh/authorized_keys eingetragen

Konfiguration Netzwerk

Die Netzwerkkonfiguration von Hetzner ist durch das nicht änderbare Routing über die MAC des Hostsystems etwas kompliziert.

⚠️ Achtung. Die Konfiguration hier ist nur bei der Nutzung eines kostenpflichtig bestellten IPv4-Bereichs notwendig. Anleitungen für Einzel-IPs mit NAT oder ähnlichen Lösungen findet man im Netz. Vielen Dank geht auch an diese tolle Informationsquelle: https://www.sysorchestra.com/2014/11/08/hetzner-root-server-with-kvm-ipv4-and-ipv6-networking/

eth0 und virtuelle Bridge

<code| /etc/network/interfaces>
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static

```
        address  144.76.30.226    # Hauptadresse des Servers
        netmask  255.255.255.224  # Hier wird in vielen Anleitungen 255.255.255.255 empfohlen. Leider ist der
Server damit nicht mehr erreichbar.
        gateway  144.76.30.225    # Gateway der Hauptadresse des Servers
        pointopoint 144.76.30.225 # Achtung nur 1 t in der Mitte (Hat mich eine Stunde gekostet)
```

iface eth0 inet6 static

```
        address  2a01:4f8:191:21e1::2 # Eine beliebige IP aus dem von Hetzner zugewiesene Bereich
        netmask  128                  # Nicht 64, da die Bridge den 64er Bereich bekommt
        gateway  fe80::1              # Default bei Hetzner-systemen
```

auto vmbr0
iface vmbr0 inet static

```
        address  144.76.30.226    # Erneut Hauptadresse des Servers
        netmask  255.255.255.224  # Gateway der Hauptadresse des Servers
        bridge_ports none
        bridge_stp off
        bridge_fd 0
```

1. Alle IPs aus dem bestellten /29er Netz

```
        up route add -host 148.251.208.168 dev vmbr0
        up route add -host 148.251.208.169 dev vmbr0
        up route add -host 148.251.208.170 dev vmbr0
        up route add -host 148.251.208.171 dev vmbr0
        up route add -host 148.251.208.172 dev vmbr0
        up route add -host 148.251.208.173 dev vmbr0
        up route add -host 148.251.208.174 dev vmbr0
        up route add -host 148.251.208.175 dev vmbr0
```

iface vmbr0 inet6 static

```
        address  2a01:4f8:191:21e1::2   # Erneut die für eth0 gewählte Adresse
        netmask  64                     # Achtung. Hier jetzt wirklich 64er
```

</code>

IP-Forwarding aktivieren

<code| /etc/sysctl.d/99-networking.conf>
net.ipv4.ip_forward=1
net.ipv4.conf.eth0.send_redirects=0
net.ipv6.conf.all.forwarding=1
</code>

Einrichtung Client-Netzwerk

Am Client wird später folgende Konfiguration genutzt
<code| /etc/network/interfaces>
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static

```
    address 148.251.208.169        # Beliebige noch nicht genutzte IPv4 aus dem bestellten IP-Subnetz
    netmask 255.255.255.255
    gateway 144.76.30.226          # Die Haupt-IP des Host-Systems
    pointopoint 144.76.30.226      # Die Haupt-IP des Host-Systems
```

iface eth0 inet6 static

```
    address 2a01:4f8:191:21e1::169 # Beliebige noch nicht genutzte IPv6 aus dem bestellten IP-Subnetz
    netmask 64
    gateway 2a01:4f8:191:21e1::2   # IPv4 des Hauptsystems
```

</code>

SSL-Zertifikat für die Weboberfläche einbinden

Wir haben für diesen Server ein kostenloses Zertifikat von StartSSL genutzt. Die Domain muss bei StartSSL vorab validiert werden. Hierzu gibt es ausreichende Anleitungen im Netz.

- SSH-Verbindung zum Server aufbauen
- mkdir certs && cd certs
- openssl genrsa -out private.key 4096
- openssl req -new -key private.key -out certrequest.csr -sha512
- Zertifikat mit Hilfe des Requests certrequest.csr bei StartSSL erstellen
- Fertig signiertes Zertifikat speichern in einer neuen Datei mit dem Namen public.pem
- wget http://www.startssl.com/certs/sub.class1.server.ca.pem
- wget https://www.startssl.com/certs/ca.pem
- Backup der vorhandenen Zertifikate
    - cp /etc/pve/pve-root-ca.pem /etc/pve/pve-root-ca.pem.orig
    - cp /etc/pve/local/pve-ssl.key /etc/pve/local/pve-ssl.key.orig
    - cp /etc/pve/local/pve-ssl.pem /etc/pve/local/pve-ssl.pem.orig
- Ersetzen der Zertifikate

        - cp private.key /etc/pve/local/pve-ssl.key
        - cp public.pem /etc/pve/local/pve-ssl.pem
        - openssl rsa -in /etc/pve/local/pve-ssl.key >> /etc/pve/local/pve-ssl.pem
        - cat sub.class1.server.ca.pem >> /etc/pve/local/pve-ssl.pem
        - cat sub.class1.server.ca.pem ca.pem > /etc/pve/pve-root-ca.pem
- Dienste neu starten
    - service pveproxy restart
    - service pvedaemon restart
- Ab sofort müsste ein gültiges Zertifikat auf der Web-GUI angezeigt werden

Konfiguration Proxmox

Sicherheit erhöhen

- Erweiterung von /etc/apt/source.list um die beiden folgenden Zeilen
  `# Proxmox VE No-Subscription Repository`
  `deb http://download.proxmox.com/debian jessie pve-no-subscription`
- /etc/apt/sources.list.d/pve-enterprise.list bearbeiten um die Meldung für das kostenpflichtige Repo zu entfernen (Mit # auskommentieren)
- In der GUI im Tab *Updates* nacheinander Refresh und Upgrade durchführen. Im Hintergrund wird dadurch ein apt-get dist-upgrade durchgeführt.

Email-Benachrichtigung

- Über die GUI unter Datacenter -> Options -> Email from address eine passende Adresse eintragen
- /etc/zfs/zed.d/zed.rc berbeiten (Dateisystem und Software-Raid)
    - `ZED_EMAIL_ADDR="empfaenger-der-emails@domain.de"` aktivieren und mit gültiger Mailadresse füllen
    - `ZED_NOTIFY_INTERVAL_SECS=3600` aktivieren, damit wir bei Fehlern keine Email-Welle bekommen
    - FIXME Todo: Test der Benachrichtigung

Sonstiges

- Neuen Backup-Space unter /var/lib/vz/backup angelegt (Maximal 10 Backup-Sätze pro VM)
- Pools erstellt für die verschiedenen Communitys
- Den Pools unter Member alle verfügbaren Storages hinzufügen
- ISO-Images hochgeladen.
    - Über GUI
    - Oder per SCP bzw. wget direkt in /var/lib/vz/template/iso/
- FIXME Weitere Schritte müssen noch dokumentiert werden.

Zu beachten

- Alle Festplatten müssen auf Cache "Write Trough" eingestellt sein. Sonst startet die VM nicht. Dies liegt an dem von Proxmox genutztem Dateisystem.