# Netzplan

## bestehende Netze

- 213.144.137.160/27
- 213.144.137.32/29
- 2001:1620:2001::/48

## aktuelle Netztabelle

| | | | |
|---|---|---|---|
| 213.144.137.33 | r1zlz1.core.init7.net. | Default Router Init7 | |
| 213.144.137.34 | knox.trash.net. | 22/TCP 443/TCP<br>25/TCP<br>53/TCP 53/UDP | SSH<br>Postfix<br>DNS |
| 213.144.137.35 | dnssec2.trash.net. | 53/TCP 53/UDP | DNS |
| 213.144.137.36 | dnssec3.trash.net. | 53/TCP 53/UDP 953/TCP | DNS rekursiv |
| 213.144.137.37 | | aktiv | |
| 213.144.137.38 | | aktiv | |
| 213.144.137.39 | Broadcast | | |

| | | | |
|---|---|---|---|
| 213.144.137.161 | inetgw.trash.net. | Default Router Init7 | |
| 213.144.137.162 | stinky.trash.net. | 21/TCP<br>22/TCP 443/TCP<br>25/TCP 465/TCP 587/TCP<br>993/TCP 995/TCP<br>5223/TCP 5269/TCP<br>6667/TCP | FTP<br>SSH<br>Postfix<br>Dovecot<br>Jabber<br>IRCD |
| 213.144.137.163 | bge1-6.stinky.trash.net. | 443/TCP | STunnel |
| 213.144.137.164 | | frei | |
| 213.144.137.165 | | frei | |
| 213.144.137.166 | | frei | |
| 213.144.137.167 | | frei | |
| 213.144.137.168 | cloud.trash.net. | 443/TCP 80/TCP | Owncloud |
| 213.144.137.169 | cloud2.trash.net. | | cloud2.trash.net. |
| 213.144.137.170 | dnssec1.trash.net. | 53/TCP 53/UDP 953/TCP | DNS |
| 213.144.137.171 | t.trash.net. | 53/UDP | DNS-Tunnel |
| 213.144.137.172 | bge1-3.stinky.trash.net. | aktiv | |
| 213.144.137.173 | bge1-4.stinky.trash.net. | aktiv | |
| 213.144.137.174 | bge1-5.stinky.trash.net. | aktiv | |
| 213.144.137.175 | | frei | |
| 213.144.137.176 | | frei | |
| 213.144.137.177 | | frei | |
| 213.144.137.178 | | frei | |
| 213.144.137.179 | | frei | |
| 213.144.137.180 | www.trash.net. | 443/TCP 80/TCP | verschiedene Trash-Sites |
| 213.144.137.181 | spam.trash.net. | 443/TCP 80/TCP | User-Sites |

| | | | |
|---|---|---|---|
| 213.144.137.182 | bge1-10.stinky.trash.net. | 443/TCP 80/TCP | verschiedene Project-Sites |
| 213.144.137.183 | bge1-11.stinky.trash.net. | 443/TCP 80/TCP | Apache frei |
| 213.144.137.184 | bge1-12.stinky.trash.net. | 443/TCP 80/TCP | Allmend-Sites |
| 213.144.137.185 | | frei | |
| 213.144.137.186 | | frei | |
| 213.144.137.187 | | frei | |
| 213.144.137.188 | | frei | |
| 213.144.137.189 | | frei | |
| 213.144.137.190 | | frei | |
| 213.144.137.191 | Broadcast | | |

| | | | |
|---|---|---|---|
| 2001:1620:2001::1 | | Router Init7 | |
| 2001:1620:2001::10 | stinky.trash.net. | 21/TCP<br>22/TCP<br>25/TCP 465/TCP 587/TCP<br>993/TCP 995/TCP<br>53/TCP 53/UDP | FTP<br>SSH<br>Postfix<br>Dovecot<br>DNS |
| 2001:1620:2001::11 | dnssec1.trash.net. | 53/TCP 53/UDP<br>443/TCP | DNS<br>Stunnel |
| 2001:1620:2001::12 | cloud2.trash.net. | | |
| 2001:1620:2001::13 | www.trash.net. | 443/TCP 80/TCP | verschiedene Trash-Sites |
| 2001:1620:2001::14 | cloud.trash.net. | 443/TCP 80/TCP | Owncloud |
| 2001:1620:2001::15 | virtserv.trash.net. | 443/TCP 80/TCP | User-Sites |
| 2001:1620:2001::20 | knox.trash.net | 22/TCP<br>25/TCP<br>53/TCP | SSH<br>Postfix<br>DNS |
| 2001:1620:2001::21 | dnssec3.trash.net. | 53/TCP 53/UDP | DNS rekursiv |
| 2001:1620:2001::22 | dnssec2.trash.net. | 53/TCP 53/UDP | DNS |

# Vorschlag neuer Netzplan

## Überlegungen

- die DNS Server sind samt IP Adressen bei den verschiedenen Registrars eingetragen. Eine Anpassung der IP-Adressen muss sorgfältig geplant werden. Daher macht es wohl Sinn die alten Adressen zu übernehmen. Allerdings ist es fraglich ob es zweckmässig ist knox weiterhin im zweiten IPv4 Netz zu betreiben.
- Der Verweis von Webservernamen via CNAME auf virthost.trash.net klappt nur bei FQDN-Hostnamen, nicht aber bei Domainnamen. So kann z.B. allend.ch nicht mittels CNAME operieren. Deshalb müsste ein DNS-Failover direkt im Zonenfile von allmend.ch gemacht werden. *(Anmerkung: dann wäre es einfacher, beim Ausfall eines Webservers seine IP-Adresse einfach auf die andere VM zu übernehmen. Wenn die Apache-Konfigurationen identisch sind, geht dies ohne Konfigurationsänderungen)*
- Die Proxyserver sollen weiterhin nur über das grüne Interface zugänglich sein und via SSH-Tunnel genutzt werden. Daher könnte man den Proxyservice gleich auf dem Shellserver betreiben statt in einer eigenen VM *(Anmerkung: Man muss hier unterscheiden zwischen dem internen Proxy und demjenigen für die User. Der interne Proxy (auf web1/web2) dient lediglich als Cache für die VM. Bei mehreren VM wäre es schade, wenn bei Updates x-mal die gleichen Inhalte vom Mirror geladen werden.*

- Stunnel und DNS-Tunnel dienen als alternativer Zugang zu SSH für den Zugriff auf den Shellserver
- Der bisherige DB-Zugriff via Unix-Socket muss überall auf Netz-Socket umdefiniert werden
- es ist noch zu klären ob die NTP-Server nicht nur Privat sondern auch Public angeboten werden
- die NTP-Server sind auf den beiden DNS-Server platziert, da dort möglichst gleichmässiger Load sein sollte. Wenn eine VM zeitweise keinen Load hat (was beim Shell- oder Web-Server der Fall ist), bezieht sie beim Hypervisor auch keine CPU-Zeit und dann beginnt die Uhr ungenau zu gehen. Dies bewegt sich im Bereich von 10 bis 40ms, ist für einen NTP-Server aber ungünstig.
- die Namensauflösung für die grüne Zone local soll im hosts-File gemacht werden, welches auf jede VM verteilt wird.

## Service-IPs

- Service-IPs werden in der grünen Zone eingesetzt, damit mehrere Dienste auf einer Maschine unterschiedlich adressiert werden. Der Use-Case dafür sind VM, die mehrere Funktionen haben.
    - Falls ein einzelner Service auf einer VM nicht mehr in Betrieb genommen werden kann, dann kann die jeweilige Service-IP auf ihre Partner-Maschine umgezogen werden. Dies würde nicht gehen, wenn mehrere Services über dieselbe IP adressiert werden.
    - Es wird keine Service-IP verwendet, falls eine VM nur eine einzelne Funktion übernimmt.
    - Der dnssec3 ist ein rekursiver DNS und hat zur Zeit nach innen und aussen die gleiche Funktion. Zukünftig könnte sich das aber ändern, deshalb wird die interne Namensauflösung über eine Service-IP angesprochen.
    - NTP ist auf ns1/ns2 und nutzt eine Service-IP, damit er später einmal einfach umgezogen werden könnte.
- Es gibt einen Typ Service-IP - transient, bei der ein Dienst auf einer Maschine eine IP hat und diese zwischen Hosts verschoben werden kann. Der Failover hängt dabei vom Admin ab, der die IP umziehen muss.
- Es gibt einen zweiten Typ Service-IP - persistent, bei der ein Dienst auf zwei Maschinen zwei IP hat und die nicht verschoben wird. Der Failover hängt dann davon ab, dass die Clients beide IPs kennen und selber bemerken, dass sie wechseln müssen.

## Tabelle

| Service | Host | Interface | Adresse | Bemerkungen |
|---|---|---|---|---|
| **Hypervisor** | box1.local | eth0 | - | Crosslink box2 |
| | | eth2 | - | Crosslink box2 |
| | | bond0 | - | Portchannel eth0/eth2 |
| | | bond0.5 | fdd9:35eb:9824:5::1/126 | DRBD-Replikation |
| | | bond0.5 | 172.31.4.129/30 | DRBD-Replikation |
| | | br1 | fdd9:35eb:9824:6::1 | - |
| | | br1 | fdd9:35eb:9824:6::3 | Service-IP NFS |
| | | eth1 | 172.31.4.1/30 | Crosslink IPMI box2 |
| | | IPMI | 172.31.4.6/30 | lokales IPMI |
| | box2.local | eth0 | - | Crosslink box1 |
| | | eth2 | - | Crosslink box1 |
| | | bond0 | - | Portchannel eth0/eth2 |
| | | bond0.5 | fdd9:35eb:9824:5::2 | DRBD-Replikation |
| | | bond0.5 | 172.31.4.130/30 | DRBD-Replikation |
| | | br1 | fdd9:35eb:9824:6::2 | - |
| | | eth1 | 172.31.4.5/30 | Crosslink IPMI box1 |
| | | IPMI | 172.31.4.2/30 | lokales IPMI |
| **Shellserver** | access1.trash.net | eth1 | 213.144.137.164 | zus. Stunnel DNS-Tunnel |
| | | eth1 | 2001:1620:2001::164 | - |
| | access1.local | eth0 | fdd9:35eb:9824:6::164 | - |
| | access2.trash.net | eth1 | 213.144.137.165 | zus. Stunnel DNS-Tunnel |
| | | eth1 | 2001:1620:2001::165 | - |
| | access2.local | eth0 | fdd9:35eb:9824:6::165 | - |
| **DNS-Server** | ns1.trash.net | eth1 | 213.144.137.186 | DNS authoritativ |
| | | eth1 | 213.144.137.187 | dnssec3 |
| | | eth1 | 2001:1620:2001::186 | DNS authoritativ |
| | | eth1 | 2001:1620:2001::187 | dnssec3 |
| | ns1.local | eth0 | fdd9:35eb:9824:6::186 | - |
| | | eth0 | fdd9:35eb:9824:6::187 | - |
| | | eth0 | fdd9:35eb:9824:6::e53 | interner DNS-Resolver |
| | | eth0 | fdd9:35eb:9824:6::e123 | interner NTP |
| | ns2.trash.net | eth1 | 213.144.137.188 | DNS authoritativ |
| | | eth1 | 213.144.137.189 | dnssec3 |
| | | eth1 | 2001:1620:2001::188 | - |
| | | eth1 | 2001:1620:2001::189 | - |
| | ns2.local | eth0 | fdd9:35eb:9824:6::188 | - |
| | | eth0 | fdd9:35eb:9824:6::189 | - |
| | | eth0 | fdd9:35eb:9824:6::f53 | interner DNS-Resolver |
| | | eth0 | fdd9:35eb:9824:6::f123 | interner NTP |
| **DB Server** | db1.local | eth0 | fdd9:35eb:9824:6::500 | - |
| | | eth0 | fdd9:35eb:9824:6::e389 | Service-IP LDAP |
| | | eth0 | fdd9:35eb:9824:6::e336 | Service-IP MySQL |
| | db2.local | eth0 | fdd9:35eb:9824:6::501 | - |
| | | eth0 | fdd9:35eb:9824:6::f389 | Service-IP LDAP |
| | | eth0 | fdd9:35eb:9824:6::f336 | Service-IP MySQL |

| Service | Host | Interface | Adresse | Bemerkungen |
|---|---|---|---|---|
| **Web trash.net** | web1.trash.net | eth1 | 213.144.137.178 | www.trash.net u.a. |
| | | eth1 | 2001:1620:2001::178 | www.trash.net u.a. |
| | web1.local | eth0 | fdd9:35eb:9824:6::178 | - |
| | | eth0 | fdd9:35eb:9824:6::e80 | interner Proxy |
| | web2.trash.net | eth1 | 213.144.137.179 | www.trash.net u.a. |
| | | eth1 | 2001:1620:2001::179 | www.trash.net u.a. |
| | web2.local | eth0 | fdd9:35eb:9824:6::179 | - |
| | | eth0 | fdd9:35eb:9824:6::f80 | interner Proxy |
| **Web Sites** | web11.trash.net | eth1 | 213.144.137.176 | Projet Home Pages |
| | | eth1 | 2001:1620:2001::176 | Projet Home Pages |
| | web11.local | eth0 | fdd9:35eb:9824:6::176 | - |
| | web12.trash.net | eth1 | 213.144.137.177 | Projet Home Pages |
| | | eth1 | 2001:1620:2001::177 | Projet Home Pages |
| | web12.local | eth0 | fdd9:35eb:9824:6::177 | - |
| **Monitoring** | mon1.local | eth0 | fdd9:35eb:9824:6::502 | - |
| | | eth0 | fdd9:35eb:9824:6::e514 | interner Syslog |
| **knox VM** | knox.trash.net | eth1 | 213.144.137.34 | DNS/Postfix |
| | | eth1 | 213.144.137.35 | DNS dnssec2.trash.net. |
| | | eth1 | 213.144.137.36 | DNS dnssec3.trash.net. |
| | | eth1 | 2001:1620:2001::20 | DNS/Postfix |
| | | eth1 | 2001:1620:2001::21 | DNS dnssec3.trash.net. |
| | | eth1 | 2001:1620:2001::22 | DNS dnssec2.trash.net. |
| | knox.local | eth0 | fdd9:35eb:9824:6::34 | - |
| **stinky VM** | stiny.trash.net | eth1 | 213.144.137.162 | DNS/Postfix |
| | | eth1 | 213.144.137.170 | DNS dnssec1.trash.net. |
| | | eth1 | 2001:1620:2001::10 | DNS/Postfix |
| | | eth1 | 2001:1620:2001::11 | DNS dnssec1.trash.net. |
| | stinky.local | eth0 | fdd9:35eb:9824:6::162 | - |

unfertig:

| Service | Host | Interface | Adresse | Bemerkungen |
|---|---|---|---|---|
| Mailserver mail.trash.net | mail1.local ULA::166 | mail1.trash.net 213.144.137.166 x::166 | zus. Submission IMAPS POPS | |
| | mail2.local ULA::167 | mail2.trash.net 213.144.137.167 x::167 | zus. Submission IMAPS POPS | |
| | vhost2.local ULA::175 | vhost2.trash.net 213.144.137.175 x::175 | Userspace | |
| DB Server db.local LDAP Server | db1.local ULA::4 | | zus. LDAP | |
| | db2.local ULA::5 | | zus. LDAP | |
| Proxyserver proxy.local | proxy1.local ULA::6 | | ev. auf Shellserver | |
| | proxy2.local ULA::7 | | ev. auf Shellserver | |
| Messaging | msg.local ULA::178 | msg.trash.net 213.144.137.178 | Jabber zus. ev. IRCD, Messaging | |

From:
https://wiki.trash.net/ - **Trash.Net Wiki**

Permanent link:
**https://wiki.trash.net/plattform-migration:netzplan?rev=1462393380**

Last update: **2016/05/04 20:23**