

---

# **Eulenkunk Documentation**

*Release 0.1*

**JJX, Adorfer, Benedikt Wildenhain, tuennes, PetaByteBoy**

**Jan 15, 2018**



---

# Contents

---

<b>1</b>	<b>Communities</b>	<b>3</b>
1.1	Organigramm . . . . .	3
1.2	Fichtenfunk . . . . .	4
1.3	Siegerland . . . . .	6
1.4	Neanderfunk . . . . .	8
1.5	Düsseldorf-Flingern . . . . .	10
1.6	GL.Eulenfunk . . . . .	11
<b>2</b>	<b>Infrastruktur</b>	<b>13</b>
2.1	gemietete Hosts . . . . .	13
2.2	Virtuelle Hosts . . . . .	14
<b>3</b>	<b>Public Keys (people)</b>	<b>15</b>
3.1	ssh . . . . .	15
3.2	firmware . . . . .	16
<b>4</b>	<b>Firmware</b>	<b>19</b>
4.1	Flingern . . . . .	19
<b>5</b>	<b>Server Kochbuch</b>	<b>21</b>
5.1	Das Blech . . . . .	24
5.2	Proxmox . . . . .	25
5.3	BGP Konzentrador einrichten . . . . .	34
5.4	Supernode einrichten . . . . .	66
5.5	Nützliches . . . . .	99
<b>6</b>	<b>Map</b>	<b>101</b>



### Was ist Eulenfunk nicht?

- keine Community
- keine schlüsselfertige Lösung
- es gibt nichts umsonst

### Was leistet Eulenfunk nicht?

- Eulenfunk administriert keine Server für euch
- Eulenfunk ist kein 24/7 Support-Dienstleister
- Eulenfunk hilft euch nicht beim Kleinreden machbarer Projekte
- Eulenfunk brät dir nicht deine Extrawurst
- Eulenfunk stellt keine Router in deiner Stadt auf

Wer sollte hier nicht mitmachen?

### Du wirst beim eulenfunk vermutlich nicht glücklich wenn Du

- Deine Arbeit nicht öffentlich und zeitnah dokumentierst
- nicht kritikfähig bist
- wenn Du schon alles ganz genau weisst
- nicht regelmäßig im Mumble bist
- nicht nachtaktiv bist
- keine Zeit in das Teilen von Wissen investieren magst
- kein Vertrauen wagst in die Fähigkeiten von anderen
- Tooldiskussionen liebst
- lieber Lösungswege diskutierst als sie praktisch evaluierst.
- die Welt erklären kannst, insbesondere wenn alle anderen böse sind.
- es Dir wichtig ist, besser als eine andere Person oder Gruppe zu sein.

Willst Du immernoch? ( [Ja](#) / [Nein](#) / [Vielleicht](#) )

Wenn Du also bereit bist, Dir mit uns gemeinsam in totaler Frustration die Nächte um die Ohren zu schlagen.

- Und am nächsten Tag dann hören darfst “Alles(tm) funktioniert nicht”.
- Und dann eine informative, freundliche Erklärung präsentieren kannst.
- Und wenn Du zum gemeinsamen Kochen auch noch was mitbringst,

**Dann komm doch mal ins allabendliche Eulenmumble:** [mumble.eulenfunk.de:64738](https://mumble.eulenfunk.de:64738) (mumble vom Freifunk Rheinland)

^\_^  
{o, o}  
|)\_\_\_\_)  
-m-m-



### 1.1 Organigramm

- Flingern
- **Fichtenfunk**
  - Altena (al)
  - Halver (hv)
  - Hemer (he)
  - Herscheid (he)
  - Iserlohn (is)
  - Lüdenscheid (ls)
  - Meinerzhagen (mz)
  - Menden (md)
  - Neuenrade
  - Plettenberg
  - Schalksmühle (sm)
  - Werdohl
- **GL.Eulenkunk**
  - Leichlingen (lln)
  - Bergisch-Gladbach (bgl)
- **Neanderfunk**
  - Erkrath (erk)
  - Haan (han)

- Hilden (hld)
- Heiligenhaus (hlg)
- Langenfeld (lgf)
- Mettmann (met)
- Monheim (mon)
- Ratingen (rat)
- Velbert (vel)
- Wülfrath (wlf)
- **Siegerland**
  - Bad Berleburg (bb)
  - Bad Laasphe (la)
  - Burbach (bu)
  - Erntebrück (eb)
  - Freudenberg (fb)
  - Hilchenbach (hb)
  - Kreuztal (kt)
  - Netphen (np)
  - Neunkirchen (nk)
  - Siegen (si)
  - Wilnsdorf (wd)

## 1.2 Fichtenfunk

Fichtenfunk ist Freifunk im Märkischen Kreis von Iserlohn bis Meinerzhagen.

AS	65410
IPv6	2a03:2260:120::/48

### 1.2.1 Websites

Karte	<a href="http://map.freifunk-mk.de">http://map.freifunk-mk.de</a>
Firmware	<a href="http://firmware.freifunk-mk.de">http://firmware.freifunk-mk.de</a>
Webseiten	<a href="http://freifunk-mk.de">http://freifunk-mk.de</a>
	<a href="http://freifunk-iserlohn.de">http://freifunk-iserlohn.de</a>
	<a href="http://freifunk-hemer.de">http://freifunk-hemer.de</a>
	<a href="http://freifunk-altena.de">http://freifunk-altena.de</a>
	<a href="http://freifunk-meinerzhagen.de">http://freifunk-meinerzhagen.de</a>

## 1.2.2 Team

Nick	Name	Kontakt	Was
domfi			
ling		<a href="mailto:linn@freifunk-mk.de">linn@freifunk-mk.de</a>	
jjx		<a href="mailto:julian.bog@freifunk-mk.de">julian.bog@freifunk-mk.de</a>	

## 1.2.3 Bleche

Community/Blech	1	2	3	4
Altena		x		
Halver				
Hemer	x			
Herscheid				
Iserlohn	x			
Lüdenscheid	x			
Meinerzhagen		x		
Menden				
Neuenrade				
Plettenberg				
Schalksmühle				
Werdohl				

### 1.2.4 BGP-Server

Name		IP	NAT IP	GRE	Berlin A	Berlin B	Düsseldorf A	Düsseldorf B
Fichtenbackbone 1	IPv4	164.132.13.11	185.66.195.56	re-mote	100.64.4.40	100.64.4.44	100.64.4.42	100.64.4.46
				lokal	100.64.4.41	100.64.4.45	100.64.4.43	100.64.4.47
	IPv6			re-mote	2a03:2260:0:212a03:2260:0:212a03:2260:0:212a03:2260:0:21f::1			
				lokal	2a03:2260:0:212a03:2260:0:212a03:2260:0:212a03:2260:0:21f::2			
Fichtenbackbone 2	IPv4	51.255.115.97	185.66.195.52	re-mote	100.64.2.125	100.64.2.126	100.64.2.128	100.64.2.131
				lokal	100.64.2.124	100.64.2.127	100.64.2.129	100.64.2.130
	IPv6			re-mote	2a03:2260:0:142a03:2260:0:142a03:2260:0:149a03:2260:0:14a::1			
				lokal	2a03:2260:0:142a03:2260:0:142a03:2260:0:149a03:2260:0:14a::2			
Fichtenbackbone 3	IPv4	164.132.83.63	185.66.195.53	re-mote	100.64.	100.64.	100.64.	100.64.
				lokal	100.64.	100.64.	100.64.	100.64.
	IPv6			re-mote	2a03:2260:0:	2a03:2260:0:	2a03:2260:0:	2a03:2260:0:
				lokal	2a03:2260:0:	2a03:2260:0:	2a03:2260:0:	2a03:2260:0:
Fichtenbackbone 4	IPv4		185.66.195.54	re-mote	100.64.	100.64.	100.64.	100.64.
				lokal	100.64.	100.64.	100.64.	100.64.
	IPv6			re-mote	2a03:2260:0:	2a03:2260:0:	2a03:2260:0:	2a03:2260:0:
				lokal	2a03:2260:0:	2a03:2260:0:	2a03:2260:0:	2a03:2260:0:

### 1.2.5 Subdomänen

Server	IPv4	IPv4 eth1	IPv6	IPv4 Range	IPv6 Range	Bssid 2.4	Bssid 5
Altena-1	51.255.115.97		2001:41d0:2:b54672:17.0.1/128	172.17.0.1/24	2a03:2260:120:100025ff:13:37:fe:02	02:ff:13:37:fe:05	
Iserlohn-1	5.196.239.99	172.31.254.10	2001:41d0:2:b54672:16.0.1/128	172.16.0.1/24	2a03:2260:120::/56	02:ff:13:37:fe:02	
Meinerzhagen 1	164.132.13.111			172.18.0.1/24	2a03:2260:120:200025ff:13:37:fe:02	02:ff:13:37:fe:06	
Hemer-1	164.132.13.114	172.31.254.1		172.19.0.1/24	2a03:2260:120:300025ff:13:37:fe:02	02:ff:13:37:fe:07	
Lüdenscheid 1	164.132.153.247	172.31.254.5		172.20.0.1/24	2a03:2260:120:400::/56		
Neuenrade-1	51.254.4.237	172.31.254.15		172.21.0.1/24	2a03:2260:120:500::/56		
MK-1	164.132.239.117	172.31.254.200		172.30.0.1/24	2a03:2260:120:990027ff:13:37:fe:99		

## 1.3 Siegerland

Freifunk im Siegerland

AS	65411
IPv6	2a03:2260:100c::/48

### 1.3.1 Websites

Karte	<a href="http://siegerland.map.eulenfunk.de">http://siegerland.map.eulenfunk.de</a>
Firmware	<a href="http://images.ff-si.ovh">http://images.ff-si.ovh</a>
Webseiten	<a href="http://freifunk-siegen.de">http://freifunk-siegen.de</a>
	<a href="http://freifunk-siegerland.de">http://freifunk-siegerland.de</a>

### 1.3.2 Team

Nick	Name	Kontakt	Was
OETiger	Flo	<a href="mailto:ffflo@posteo.de">ffflo@posteo.de</a>	Hilchenbach
TroTLF	Klaus	<a href="mailto:dev0@mailbox.org">dev0@mailbox.org</a>	Freudenberg
pvitt	Peter	<a href="mailto:peter@humulon.de">peter@humulon.de</a>	Firmware

### 1.3.3 Bleche

Community/Blech	1	2
Freudenberg		x
Hilchenbach	x	

### 1.3.4 BGP-Server

Name	IP	NAT IP	GRE	Berlin A	Berlin B	Düsseldorf A	Düsseldorf B	
siegerland	IPv4	176.31.125.14	185.66.194.16	re-	100.64.4.124	100.64.4.128	100.64.4.126	
				mote	100.64.4.125	100.64.4.129	100.64.4.127	100.64.4.131
	IPv6			re-	2a03:2260:0:2482a::1	2a03:2260:0:2482a::2	2a03:2260:0:2482a::3	2a03:2260:0:2482a::4
				mote	2a03:2260:0:2482a::1	2a03:2260:0:2482a::2	2a03:2260:0:2482a::3	2a03:2260:0:2482a::4
siegerland	IPv4	188.165.231.8	185.66.194.17	re-	100.64.4.132	100.64.4.136	100.64.4.134	
				mote	100.64.4.133	100.64.4.137	100.64.4.135	100.64.4.139
	IPv6			re-	2a03:2260:0:2482a::1	2a03:2260:0:2482a::2	2a03:2260:0:2482a::3	2a03:2260:0:2482a::4
				mote	2a03:2260:0:2482a::1	2a03:2260:0:2482a::2	2a03:2260:0:2482a::3	2a03:2260:0:2482a::4

### 1.3.5 Konzentratoren

Name	IPv4	IPv6
ff-si-konz-1.ff-si.ovh	51.254.244.185	
ff-si-konz-2.ff-si.ovh	188.165.115.76	

### 1.3.6 Subdomänen

Server	IPv4	IPv6	IPv4 Range	IPv6 Range	Bssid 2.4	Bssid 5
freudenberg-1.ff-si.ovh	178.33.39.219		172.17.0.1/16	2a03:2260:100c:200::/56		
hilchenbach-1.ff-si.ovh	51.254.244.186		172.16.0.1/16	2a03:2260:100c:100::/56		

## 1.4 Neanderfunk

### 1.4.1 Übersicht

Freifunk im Neanderland (Kreis Mettmann).

AS	64863
IPv6	2a03:2260:300e::/48

### 1.4.2 Websites

Karte	<a href="https://karte.neanderfunk.de/">https://karte.neanderfunk.de/</a>
Firmware	<a href="https://download.ffnef.de/firmware/">https://download.ffnef.de/firmware/</a>
Webseiten	<a href="http://www.neanderfunk.de/">http://www.neanderfunk.de/</a>
	<a href="http://www.freifunk-mettmann.de/">http://www.freifunk-mettmann.de/</a>
	<a href="http://freifunk-ratingen.de/">http://freifunk-ratingen.de/</a>
	<a href="http://www.freifunk-velbert.de">http://www.freifunk-velbert.de</a>

### 1.4.3 Team

Nick	Name	Kontakt	Was
Lutz	Lutz Wulfestieg	<a href="mailto:Lutz@forum">Lutz@forum</a>	Community, Organisation
Benedikt_Wi	Benedikt	<a href="mailto:Benedikt_Wi@forum">Benedikt_Wi@forum</a>	Firmware, Supernodes
plaste	Stephan	<a href="mailto:plaste@forum">plaste@forum</a>	Dokumentation, Supernodes

## 1.4.4 Bleche

Community/Blech	1	2	3
Erkrath (erk)	x	x	
Haan (han)	x	x	
Hilden (hld)	x	x	
Heiligenhaus (hlg)	x	x	
Langenfeld (lgf)	x	x	
Mettmann (met)	x	x	
Monheim (mon)	x	x	
Ratingen (rat)	x	x	
Velbert (vel)	x	x	
Wülfrath (wlf)	x	x	

Stand: 29.05.2016; Blech 1/2 sind VM's beim FFRL, keine dezidierten VM's. Blech 3 (FF-ME-Blech1) befindet sich aktuell im Aufbau.

## 1.4.5 BGP-Server

Name		IP	NAT IP	GRE	Berlin A	Berlin B	Düsseldorf A	Düsseldorf B
neander-1	IPv4	151.80.11.200	185.66.193.11	rd- mote	100.64.3.86	100.64.3.90	100.64.3.88	100.64.3.92
				lokal	100.64.3.87	100.64.3.91	100.64.3.89	100.64.3.93
	IPv6			re- mote	2a03:2260:0:1b2a03:2260:0:1b2a03:2260:0:1b2a03:2260:0:1b8::1	2a03:2260:0:1b2a03:2260:0:1b2a03:2260:0:1b2a03:2260:0:1b8::1	2a03:2260:0:1b2a03:2260:0:1b2a03:2260:0:1b8::1	2a03:2260:0:1b2a03:2260:0:1b2a03:2260:0:1b8::1
				lokal	2a03:2260:0:1b2a03:2260:0:1b2a03:2260:0:1b2a03:2260:0:1b8::2	2a03:2260:0:1b2a03:2260:0:1b2a03:2260:0:1b2a03:2260:0:1b8::2	2a03:2260:0:1b2a03:2260:0:1b2a03:2260:0:1b8::2	2a03:2260:0:1b2a03:2260:0:1b2a03:2260:0:1b8::2
neander-3	IPv4	151.80.11.200	185.66.193.11	rd- mote	100.64.3.102	100.64.3.106	100.64.3.104	100.64.3.108
				lokal	100.64.3.103	100.64.3.107	100.64.3.105	100.64.3.109
	IPv6			re- mote	2a03:2260:0:1b2a03:2260:0:1b2a03:2260:0:1b2a03:2260:0:1c0::1	2a03:2260:0:1b2a03:2260:0:1b2a03:2260:0:1b2a03:2260:0:1c0::1	2a03:2260:0:1b2a03:2260:0:1b2a03:2260:0:1c0::1	2a03:2260:0:1b2a03:2260:0:1b2a03:2260:0:1c0::1
				lokal	2a03:2260:0:1b2a03:2260:0:1b2a03:2260:0:1b2a03:2260:0:1c0::2	2a03:2260:0:1b2a03:2260:0:1b2a03:2260:0:1b2a03:2260:0:1c0::2	2a03:2260:0:1b2a03:2260:0:1b2a03:2260:0:1c0::2	2a03:2260:0:1b2a03:2260:0:1b2a03:2260:0:1c0::2
FF-ME-Blech1	IPv4	37.59.64.72	185.66.193.78	re- mote	100.64.3.94	100.64.3.98	100.64.3.96	100.64.3.100
				lokal	100.64.3.95	100.64.3.99	100.64.3.97	100.64.3.101
	IPv6			re- mote	2a03:2260:0:1b2a03:2260:0:1b2a03:2260:0:1b2a03:2260:0:1bc::1	2a03:2260:0:1b2a03:2260:0:1b2a03:2260:0:1b2a03:2260:0:1bc::1	2a03:2260:0:1b2a03:2260:0:1b2a03:2260:0:1bc::1	2a03:2260:0:1b2a03:2260:0:1b2a03:2260:0:1bc::1
				lokal	2a03:2260:0:1b2a03:2260:0:1b2a03:2260:0:1b2a03:2260:0:1bc::2	2a03:2260:0:1b2a03:2260:0:1b2a03:2260:0:1b2a03:2260:0:1bc::2	2a03:2260:0:1b2a03:2260:0:1b2a03:2260:0:1bc::2	2a03:2260:0:1b2a03:2260:0:1b2a03:2260:0:1bc::2

## 1.4.6 Konzentratoren

Name	IPv4	IPv6
ff-me-blech1.ffnef.de	37.59.64.72	

## 1.4.7 Subdomänen

Server	IPv4	IPv6	IPv4 Range	IPv6 Range	Bssid 2.4	Bssid 5
met@neander-1	151.80.11.203		10.1.192.1/20	2a03:2260:300e:10::1/64		
met@neander-2	151.80.11.203		10.1.192.3/20	2a03:2260:300e:10::3/64		
met-1	37.59.64.73		10.1.192.4/20	2a03:2260:300e:110::4/64		
hlg@neander-1	151.80.11.203		10.11.112.0/20	2a03:2260:300e:20::1/64		
hlg@neander-2	151.80.11.203		10.11.112.0/20	2a03:2260:300e:20::3/64		
vel@neander-1	151.80.11.203		10.11.80.0/20	2a03:2260:300e:30::1/64		
vel@neander-2	151.80.11.203		10.11.80.0/20	2a03:2260:300e:30::3/64		
mon@neander-1	151.80.11.203		10.1.208.0/21	2a03:2260:300e:40::1/64		
mon@neander-2	151.80.11.203		10.1.208.0/21	2a03:2260:300e:40::3/64		
hld@neander-1	151.80.11.203		10.11.128.0/20	2a03:2260:300e:50::1/64		
hld@neander-2	151.80.11.203		10.11.128.0/20	2a03:2260:300e:50::3/64		
erk@neander-1	151.80.11.203		10.1.224.0/21	2a03:2260:300e:70::1/64		
erk@neander-2	151.80.11.203		10.1.224.0/21	2a03:2260:300e:70::3/64		
rat@neander-1	151.80.11.203		10.11.64.0/20	2a03:2260:300e:80::1/64		
rat@neander-2	151.80.11.203		10.11.64.0/20	2a03:2260:300e:80::3/64		
rat-1	37.59.64.75		10.11.64.4/20	2a03:2260:300e:180::4/64		
han@neander-1	151.80.11.203		10.1.232.0/21	2a03:2260:300e:90::1/64		
han@neander-2	151.80.11.203		10.1.232.0/21	2a03:2260:300e:90::3/64		
lgf@neander-1	151.80.11.203		10.1.240.0/21	2a03:2260:300e:a0::1/64		
lgf@neander-2	151.80.11.203		10.1.240.0/21	2a03:2260:300e:a0::3/64		
wlf@neander-1	151.80.11.203		10.1.248.0/21	2a03:2260:300e:b0::1/64		
wlf@neander-2	151.80.11.203		10.1.248.0/21	2a03:2260:300e:b0::3/64		

## 1.5 Düsseldorf-Flingern

### 1.5.1 Übersicht

Freifunk-Flingern ist ein Düsseldorfer Projekt welches als Ziele sich den bau von möglichst stark vernetzten Meshes gesetzt hat. Es sollen möglichst große Mesh-Wolken gebaut werden, die vergleichsweise wenige (aber kräftige) VPN-Uplinks haben. Bei der Versorgung von Geflüchtetenunterkünften ist die Nutzung von bestehender Freifunk-Technik (im Rahmen des PPA und des MoU) Zielvorgabe, um nicht nur als “Graswurzel-Internetprovider” aufzutreten, sondern echten Freifunk zu den Refugees zu bringen.

### 1.5.2 Websites

Karte	<a href="http://map.ffdus.de/">http://map.ffdus.de/</a>
Firmware	<a href="http://images.ffdus.de/">http://images.ffdus.de/</a>
Projekt	<a href="http://www.twin.world/">http://www.twin.world/</a>
Blog	<a href="http://www.ffdus.de">http://www.ffdus.de</a>

### 1.5.3 BGP-Server

AS	65125
----	-------

Table: broken!

Name		IPvserver	IPffrl	GRE	Berlin A	Berlin B	Düsseldorf A	Düsseldorf B
Flingern-1	IPv4	51.255.150.68	85.66.195.64	re-mote	100.64.2.200	100.64.2.202	100.64.2.204	100.64.2.206
				lokal	100.64.2.201	100.64.2.203	100.64.2.205	100.64.2.207
	IPv6			re-mote	2a03:2260:0:16e2::1	2a03:2260:0:16e2::1	2a03:2260:0:172a::1	2a03:2260:0:172a::1
				lokal	2a03:2260:0:16e2::1	2a03:2260:0:16e2::1	2a03:2260:0:172a::1	2a03:2260:0:172a::1
Flingern-2	IPv4	5.196.239.99	185.66.195.64	re-mote	100.64.4.40	100.64.4.44	100.64.4.42	100.64.4.46
				lokal	100.64.4.41	100.64.4.45	100.64.4.43	100.64.4.47
	IPv6			re-mote	2a03:2260:122::1	2a03:2260:0:2e2a::1	2a03:2260:0:2e2a::1	2a03:2260:0:2e2a::1
				lokal	2a03:2260:122::1	2a03:2260:0:2e2a::1	2a03:2260:0:2e2a::1	2a03:2260:0:2e2a::1

## 1.5.4 Subdomänen

Server	IPv4	IPv6 int	IPv6 ext	nextnode v4	nextnode v6	DHCP v4
w0-9	10.155.0.0/24	2001:a0:747e:ab29:9375::1	2001:a0:747e:ab29:9375::1	10.155.0.1	2001:a0:747e:ab29:9375::1	10.155.1.0-10.155.7.255

## 1.5.5 Team

Nick	Name	Kontakt	Was
Trickster	Silas	<a href="mailto:trickster@forum">trickster@forum</a>	Geld, Logistik, Unterkünfte, Routerdaten
mst	mathias		Uplinks, Offloader, Neurouter
Frankth	Frank		Dokumentation, Coaching
Adorfer	Andreas	<a href="mailto:adorfer@forum">adorfer@forum</a> <a href="mailto:adorferen@gmail.com">adorferen@gmail.com</a>	Firmware, Ourdoorinstallationen

## 1.6 GL.Eulenfunk

### 1.6.1 Übersicht

GL.Eulenfunk ist eine Untergruppe von Freifunk GL (Freifunk im Rheinisch-Bergischen Kreis). Dort sind die Städte Leichlingen und Bergisch Gladbach mit eigenen Supernodes vertreten, während die anderen Städte in der Domäne GL.Wupper Ressourcen beziehen.

### 1.6.2 Websites

Karte	<a href="https://map.ffgl.eu/">https://map.ffgl.eu/</a>
Firmware	<a href="http://firmware.ffgl.eu/">http://firmware.ffgl.eu/</a>
Webseite	<a href="https://freifunk-leichlingen.net/">https://freifunk-leichlingen.net/</a>

### 1.6.3 Team

Nick	Name	Kontakt	Was
Frank	Frank	<a href="mailto:frank@forum">frank@forum</a>	Eisen, Neurouter
PetaByteBoy	Milan	<a href="mailto:petabyteboy@forum">petabyteboy@forum</a>	Eulenk-Karten, VMs

## CHAPTER 2

---

### Infrastruktur

---

#### 2.1 gemietete Hosts

name	owner	hoster	loc	typ	os	FQDN	IPv4 (base)	ipv4 (pool)	IPv6	MAC
dags1	Silas	OVH	RBX6	M-4C8T-32G-2x2T-500M	PM4	dags1.ffgl.eu	154.47.39	196.175.52/30 51.255.150.68/30	2001:41d0:1008:07ef::/64	
paz	Sabine	SYS	RBX4	M-4C8T-32G-2x2T-250M	PM4		46.105.125	105.233.208/29	2001:41d0:2:e8d1::/64	
vpn	An-dreas	NC		V-2C-6G-112G-100M	arch		37.120.171.253		2a03:4000:6:5100:54b:f0:15:12	
ffgek0	An-dreas	NC		V-1C-2G-40G-100M	arch		46.38.238.147		2a03:4000:2:8352684:27:00:19:46	
ff-dus0	An-dreas	NC		V-1C-2G-30G-100M	arch		46.38.234.225		2a03:4000:2:bb966d:cc:64:88:af	
pbbpg	an-dreas	nc		v-2c-6g-230g-100m	arch		5.45.96.247		2a03:4000:5:1ca:831a2:c2:e5:f8	
sil-ver	Frank	SYS			PM4	sil-ver.ffgl.eu	188.165.146	132.31.112/30	2001:41d0:2:8b44::/64	

## 2.2 Virtuelle Hosts

FQDN	host	os	RAM	HDD	mac	ipv4
map.eulenkfunk.de	dags1	arch			02:00:00:d6:a0:10	51.255.150.71
map2.eulenkfunk.de 0	paz	arch			02:00:00:06:2c:d0	51.255.233.214
flingern-3.ffdus.de	paz	lts14.2			02:00:00:58:04:81	51.255.233.215
iserlohn-2.freifunk-mk.de	dags1	lts14.2			02:00:00:69:ee:4b	5.196.175.52
flingern-1.ffdus.de	dags1	lts14.2			02:00:00:a1:81:5f	51.255.150.68
neander-1.ffnef.de	ffrl	lts16.4	1G	16G	00:50:56:07:e1:83	151.80.11.200
neander-3.ffnef.de	ffrl	ub15.10	1G	16G	00:50:56:0c:29:6f	151.80.11.203
service.ffdus.de	dags1	ipfire			02:00:00:d6:2e:36	51.255.150.70
horst.ffdus	LES	arch	33G	500G	36:e2:87:5e:a4:87	10.155.6.112
konzentrator.silver.ffgl.eu	silver	lts14.2			00:50:56:06:5a:33	164.132.31.113
bgl0.ffgl.eu	silver	lts14.2			00:50:56:07:52:60	164.132.31.114
lln0.ffgl.eu	silver	lts14.2			00:50:56:0a:fa:e8	164.132.31.115

---

## Public Keys (people)

---

### 3.1 ssh

Pubkeys, um ssh-Login für die genannten Personen zu einzuräumen:

user	key
pan-dur	ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAIEAmLQ1QW341TIu6csTplCM1xAkpU8uRLCbcDcQb3P2coBj993PMYhmT Pandur
sunta	ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQBAQC3SPq75cC/tZJ9sWKHXIs1XOUzwc1oIOHzn2TrfpNab5AOZDZ1bX cw@bianca
mathias	ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDBgeaL3Fap41iwHYPG/7khPINzeknkdvtoPWXJJrhTyUGwA/3RbRY mathias
lingling	ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQCzSsGrVSdBhrQb94S2fqtUUbwi3aYJnRAGcu2CTIVCNoSIEKYbjX ling@ling
pbb	ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQDGwGwwqw9qSoEq8L+r7U+FRkGN30iBBA2ohc+fnJK7qSCJ3T9bV petabyteboy@pbb-e3
adorfer	ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAIEAufGE6eK/iZTeLKCduy4UEyQpkXX+Z/0SAbYCbkJhJjNpYJaAaMhPI9yP adorfer
Benedikt Wi	ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC9o5jgZqeWNYM7hpoEnbsCEbKI2NDqIXIUKk6Ty8ftXsvY2MUy9 benedikt@kampo
ju-lian	ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC+/qANS2vRvc8w7d2v6avmzE0LvzEzQrcjNAKDeo490g3GbnnsuS8 x@x
plaste	ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQCvMcy/RjnGc/ppzxIqvvyv3WnaQ3Tj495MLw8qV4FpTkVndjluqrY7h plaste
Wurstbrot	ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAQEAnrO+trdNZO5/S4tBRXgWJGKljz4DMB9YODxqm7HiHZZC2RuMZaAo5 wurstbrot
faithinchaos	ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAQEaj/IcUJ8h4RrgEwrBc0QIYs53pS5sdQnAC9b+7Q31h0EIL3PwKj3eWs2fQ faithinchaos
robot	ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDQjdRIoLwaN3DdV7jusUDILfUK4etdS6zhBdpJb5vFxtT8/sb6+iIvQz ffdurobot
tuennes	ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC3E0csrsSpqSPpTkrIt1izfS78BLoMNMi6FYa71+ndi9Xuo5SLItBBh frank@frank-1005HA
domfi	ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQCC3mQ7wQe+ERDAb6VpnxTrfp+NvG23ItVUy+cjFSCHhJnW7dV8t domfi
oetiger	ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQCweucLWW6+o0mZyb4Q1vdnGa8AK53G5Q7sCD5XUhrwKBdyf0S flo@flow
Lutz	ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDKy2WKAmvP7u4ViQ619RNwz0DTq9ZbfNbGIQOcfVIRXj2PLKj3 lutzwulfstieg@Lutz-Mac
trotlf	ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQDYKm98ZO2xdX2WUtStu6pTS/qCA3idw/Iu4mCcaaz7Ec0SJ4oupIL ks@ks-ThinkPad-T430
pvitt	ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDotu6hi/SsqdIza0ejBww11svCLj0Q8svyh3RcSshnhtAG/HcvBxyzjsW5 pvitt

## 3.2 firmware

Signkeys für gluon-Firmware/Autoupdater

key	user
'19a02dd7b50ffc2b59e2cd1f9e76b26b46e33c43ebf641554572e4a677af35cc'	– SenorCafe
'2aa020a8860e5c3f638ed77d313148c7e7c5899be4bebf2cb3406875ef03e835'	– Goldwaage
'fb919d4adc69bd404f5093ce6b43badf351f9e642ad458406be986baf6096247'	– PetaByteBoy
'dd6a9d1aefc175f885705691498e904cbda12cc4602316f04816d78026c7c0f0'	– Benedikt Wi
'2a61930930a240c027f6ca4197203d400b6e4a32f9e92041e5f086907796c9bc'	– adorfer
'd02f8e60fb7a5069556500694ebe512b6017b01e9950476e4cfcf10d5130c296'	– JJX
'7afe187ceb34e83b2cb33c244ab5c8a7e80829c3e83b8d3fc471d2642eb6a602'	– limlug
'610e9acf4d550c3a272b88ec5b4cf0a0e382be203f98b860181fb1bcb1641abd'	– mathias
'01aff79cb3079b5b343cdc099a342434f284329890230e0f23850a488570b8c2'	– AKA47
'579de7b1ded1dc39583515f722d72524f6dce78da635a7ac2d11cfe1dc046e7e'	– tuennes
'd0647b68ff46d35394d99630f9337e39786f51f5bdcee5bd26b7b2c729045cb6'	– jenkins
'a2e21ef5743945befa8f88f10a1a168050909d82e4d836bcf879eb573b9ce777'	– domfi
'96d644ff1ce07d6f67d9329a0eb9a1548d0d01a3519d17ec1fe9d49da3270bfc'	– plaste
'6abd06560a8559e134ad02c8a4082ee0148685ba289e64d8000dbd729068faa5'	– pvitt



## 4.1 Flingern

TREE	Gluon	status	releasename	date	url
Stable	2015.1.2	nur Wupper Server	20150911-stable	2015-09-11	<a href="http://images.ffdus.de/stable/">http://images.ffdus.de/stable/</a>
beta	2015.1.2	nicht nutzen!	20151009-beta	2015-10-09	<a href="http://images.ffdus.de/beta/">http://images.ffdus.de/beta/</a>
Experimental	2015.2pre	MoW defekt	2016011502-exp-ssid	2016-01-15	<a href="http://images.ffdus.de/experimental/">http://images.ffdus.de/experimental/</a>
Broken (nightly)	2016.1pre	untested packages	2016020403-exp	2015-02-04	<a href="http://images.ffdus.de/broken/">http://images.ffdus.de/broken/</a>

*Stand 2016-02-01:*

Vorarbeiten am Gluon Releasekanidaten herumgeschraubt, um beim offiziellen Release schnellstmöglich auch eine stable bringen zu können.  
Ein Testkanidat von Mitte Januar hat erhebliche Probleme mit “MoW” wenn zur Bootzeit kein Ethernetlink auf LAN(!) besteht.

Was in der Release dazukommt:

1. einen wöchentlichen Reboot (freitag morgens zwischen 3 und 5)
2. einen verbesserten Wifi-Powerfix (einige Router haben beim Neufflaschen

etwa 3dB zu wenig Sendeleistung eingestellt. Das ist ein Bug aus dem ChaosCalmer. Da werden die RegDomain-Limits leider nicht ausgeschöpft)

3. eine “Vorrüstung” für “Clientnetz tagsüber ‘aus’” oder “Clientnetz über Nacht ‘aus’”.

Müssen nur zwei uci-statements abgesetzt werden, dann ist das aktiv. Inhaltlich mag ich es nicht, aber es ist für mich das kleinere Übel im Vergleich zu “gar kein Freifunk an Standort x”

4. eine “Vorrüstung” für “Bandbreiten-Limit Zeitschaltuhr für den VPN-Link”, ebenfalls wahlweise tagsüber oder nachts.

(Frage in die Runde: soll ich zu c und d noch was bauen, dass man zwischen Mo-Fr & Sa-So unterschiedlich setzen kann? Irgenwann wäre dann eine Seite im Advanced-Websetup sinnvoll. Falls sich jemand berufen fühlen sollte, den Kampf mit lua-scripts aufzunehmen.)

5. den Wifineighborcheck, um hängende CPE210er (und andere) bei sonst unerkennbarem Verlust des Wifimoduls neu zu starten.

Was ich trotz diverser Versuche nicht hinbekomme und wo Petabyteboy mir aus der Patsche helfen darf ist der "Radiochannel-Keep": Damit die einmal verstellten Frequenzen beim Update nicht wieder auf Default stehen.

(Damit die Kabelmesh-Nodes in den Unterkünften mit ihren verteilten Wlan-Kanälen nicht nach einem Update komplett händisch nachgepflegt werden müssen.)

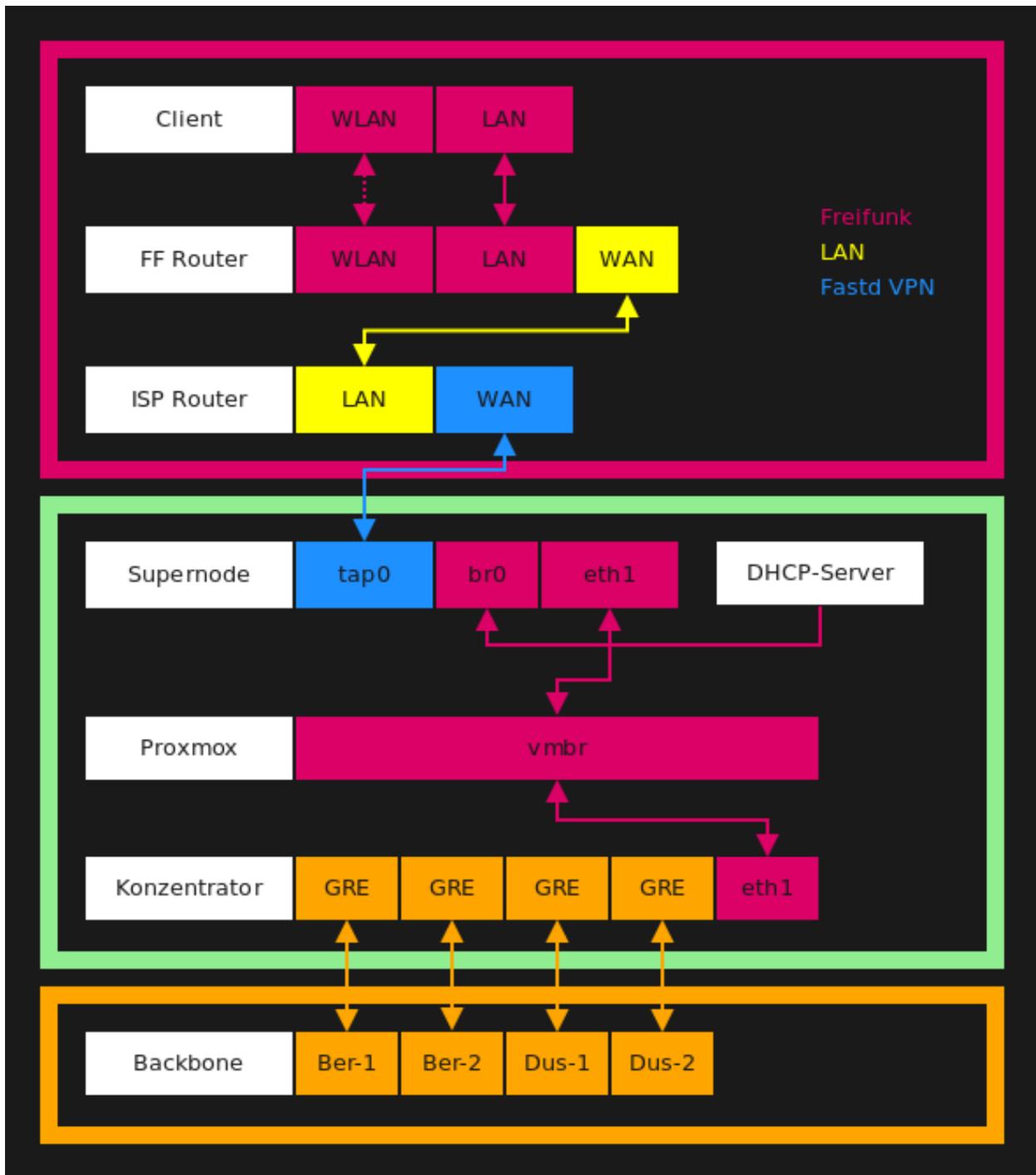
Anleitung zur Einrichtung eines Freifunk Supernodes auf Basis von Proxmox 3.6 und Ubuntu Server 14.04.4 LTS

Das Setup besteht im wesentlichen aus 3 Zonen:

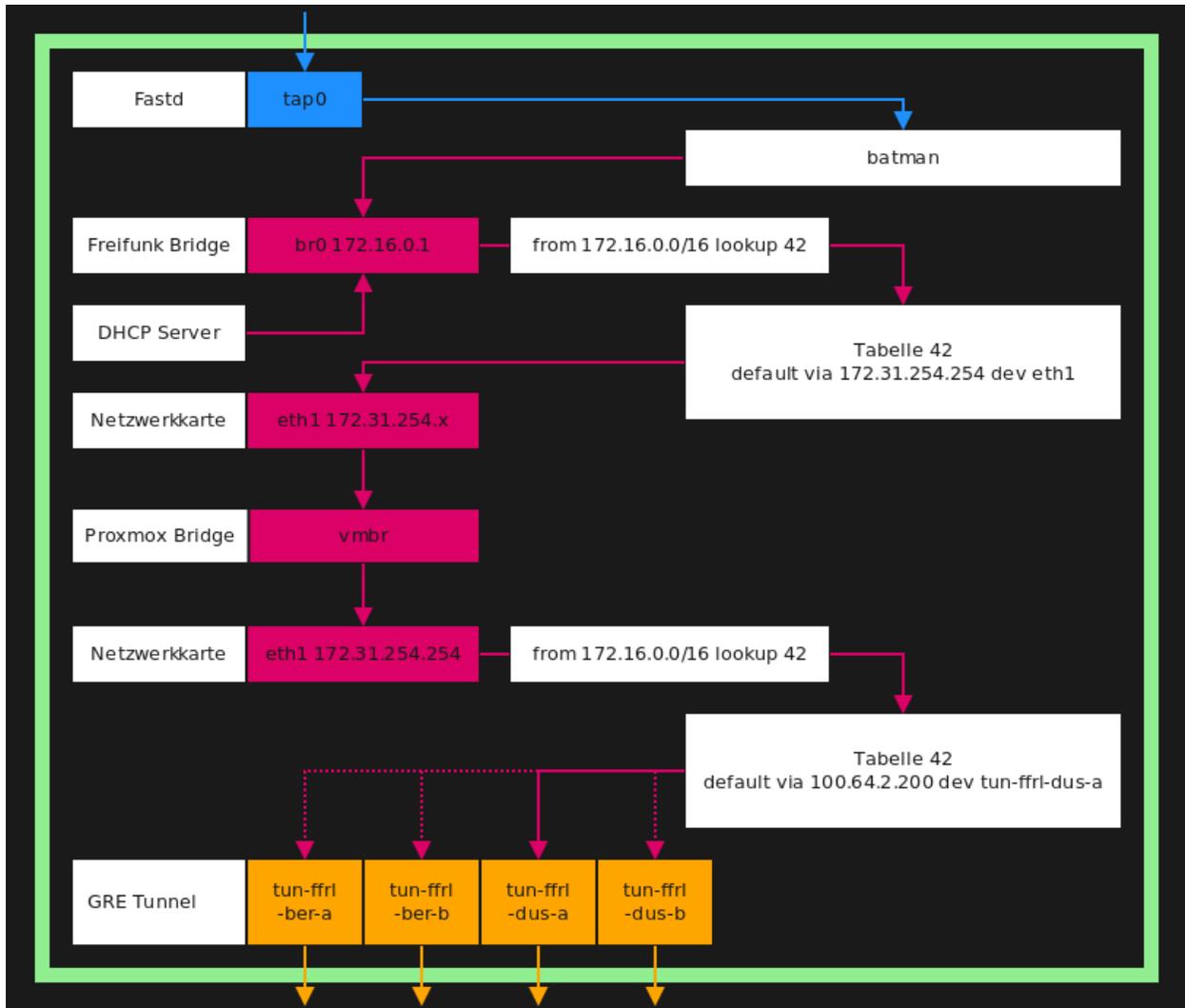
- Die Freifunk Zone vor Ort (rosa): damit haben wir nicht viel zu tun.
- Die Serverzone (grün): um die geht es in dieser Anleitung.
- Das Backbone (orange), das macht der FFRL.

Die Serverzone teilt sich wiederum in 3 Segmente auf:

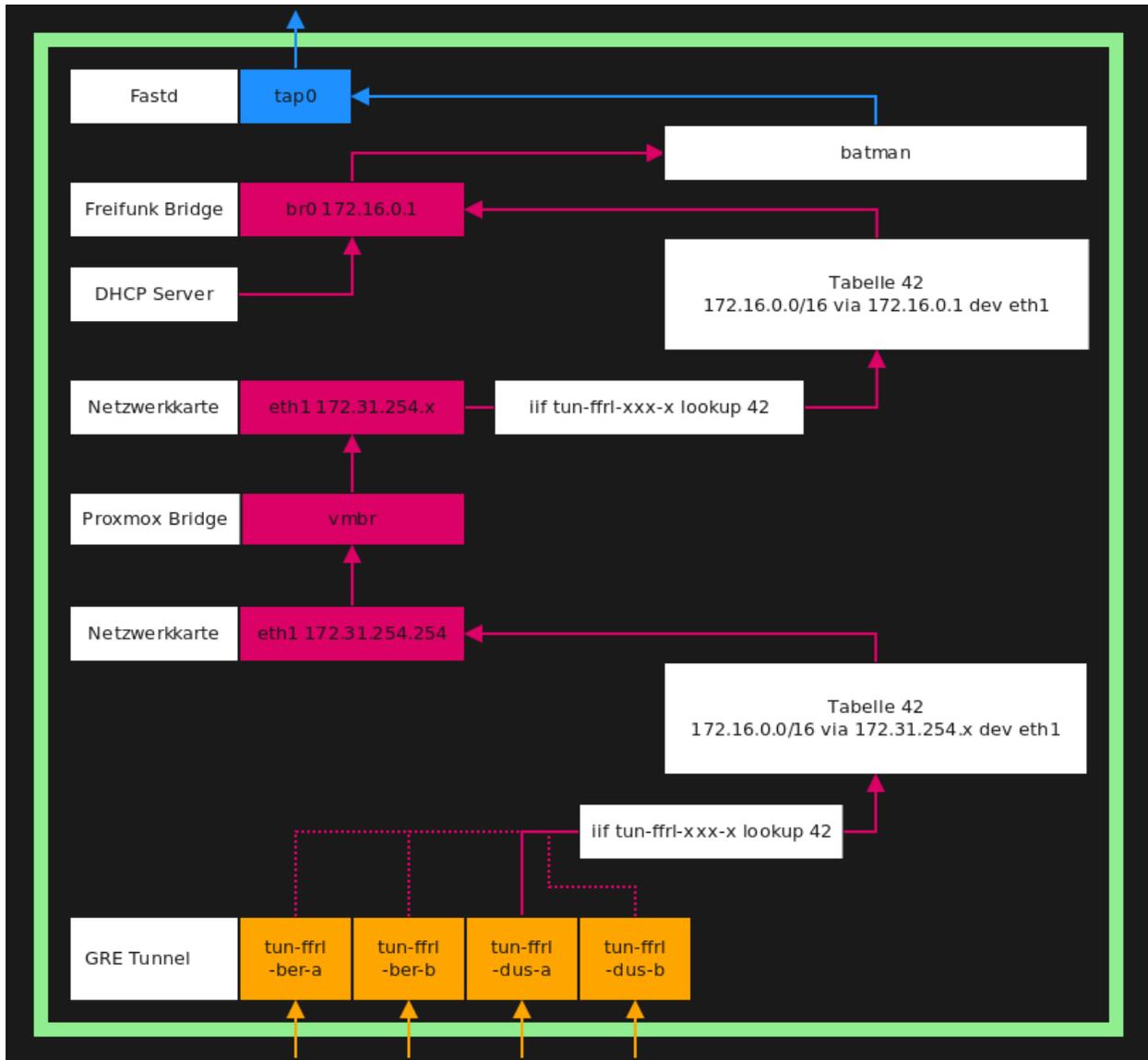
- Der Hypervisor Proxmox, dieser stellt alle Funktionen für den Betrieb von virtuellen Maschinen bereit.
- Der Konzentrador, dieser virtuelle Server stellt die Verbindung zu FFRL Backbone her, und übernimmt NAT und BGP.
- Der Supernode stellt die Fastd VPN Verbindungen für die Router bereit, kümmert sich um Batman, DHCP und radvd.



Vom Client ins Internet gehen die Daten folgenden Weg (IPv4):



Und das ist der Rückweg (IPv4):



Weiterlesen:

## 5.1 Das Blech

Wir treiben ziemlich fiese Dinge mit unseren Servern; CPU und Netzwerktraffic (Volumen und Pakete-Rate) sind die entscheidenden Faktoren.

### 5.1.1 Voraussetzungen

Folgendes sollte euer Wunschserver leisten, damit er für FF tauglich ist:

- 100 Mbit garantierte Bandbreite
  - Nicht 100 Mbit Anbindung oder Peak Bandbreite! Der Server muss 24/7 100 Mbit abkönnen.

- Vollen Zugriff aufs Blech / den Hypervisor
  - Server neu installieren
  - Hardware reboot
  - IPs hinzufügen
- Leistungsstarke CPU
- Zusätzliche IPv4 Adressen (Failover IPs) “zu Einmal-Kosten”

Folgendes sind absolute Ausschlusskriterien für einen Server:

- Trafficbegrenzung
- Fair use
- Vserver

### 5.1.2 Hoster / Rechenzentrum

OVH bzw. deren preiswertere Marke “Soyoustart” (sys) sind gut geeignet.

Die auf “OVH” gebrandeten Server leisten kaum mehr als die SYS Maschinen, kosten aber unverhältnismäßig viel mehr.

### 5.1.3 Bestellvorgang

Wer bei OVH oder SYS die Server bestellt sollte, wenn er Neukunde ist, per Überweisung zahlen. Das erspart zusätzliche Authentifizierungsmethoden und geht daher schneller(!) als Paypal.

### 5.1.4 Sicherheit

Über das OVH/SYS Kundeninterface hat man die Möglichkeit den Server neu zu starten, neu zu installieren oder in den RescueMode zu booten. Man sollte daher dringend den Zugang zum Kundeninterface mit einer Two-Factor Login Methode zusätzlich absichern. Man kann die selbe OATH App nutzen, die man auch für Github und später das Proxmox Webinterface verwenden kann.

Für iOS wurde z.B. die App “OTP Auth” getestet. Auf Ubuntu-Phone lässt sich die App “Authenticator” einsetzen.

## 5.2 Proxmox

### 5.2.1 Einleitung

Proxmox stellt alle Funktionen für den Betrieb von virtuellen Maschinen bereit und bietet per Webinterface eine zentrale Möglichkeit, neue VMs anzulegen und bestehende zu verwalten, inkl. einer KVM-Konsole für VMs und auch den Host selbst. Das funktioniert ohne Spezial-Plugins (d.h. kein Flash, keine JRE etc.)

Die Einrichtung des Proxmox beschränkt sich auf folgende Punkte:

- Installation: Hoster wie OVH/Soyoustart nehmen euch die Arbeit ab
- Einrichtung des SSH Zugriffs per Public-Key
- Absicherung des SSH Servers

- Absicherung des Webinterfaces per Two-Factor-Authentication (Oath)
- Einrichtung des Monitorings per Check\_MK
- Bereitstellung der ISO Datei für Ubuntu Server

## 5.2.2 Installation

Proxmox kommt entweder per Klick als Template vom Provider auf den Server oder muss von Hand installiert werden. Hier ein Beispiel für die Installation über das Soyostart Web-Frontend. Zunächst den passenden Server im Dropdown-Menü auswählen und dann auf “Installieren” klicken:

The screenshot shows the Soyostart web interface. At the top, there are navigation links for 'Support', 'Tasks', and 'Abrechnung'. Below this is a search bar and buttons for 'Reinstallieren', 'Neu starten', and 'NetBoot'. A horizontal menu contains options: 'IP', 'DNS', 'Storage-Backup', 'Lizenzen', 'Installations-Template', 'USB-Gerät', 'KVM IP', and 'ASA Firewall'. The main content area is divided into two columns. The left column displays server details: 'Ablaufdatum' (10.08.2016), 'Rechenzentrum' (RBX3 - Rack), 'Betriebssystem' (VPS Proxmox VE 3.4 (64bits)), 'Boot' (Boot from hard drive (no netboot)), 'Haupt-IP', 'Reverse', and 'Storage-Backup' (0 / 100 GB). The right column shows 'Server-Status' (OK), 'Monitoring' (Aktiviert), 'Eingriffe' (0), and 'Real Time Monitoring' (RTM ist nicht für diesen Server verfügbar). Below this is a traffic graph labeled 'MRTG Traffic' showing data from 15:30 to 21:00. The graph shows a fluctuating traffic pattern with peaks around 75M bps.

Im nächsten Schritt wählt man VPS Proxmox VE 3.4 (64Bit) als Template aus, der Haken bei “Personalisierte Installation” darf NICHT gesetzt sein. Mit Klick auf “Weiter” startet man jetzt die Installation.

The screenshot shows a dialog box titled 'Reinstallation des Servers'. It prompts the user to 'Wählen Sie Ihr Template aus' and shows a dropdown menu with 'VPS Proxmox VE 3.4 (64Bit)' selected. Below this, it asks to 'Wählen Sie die Sprache aus' with a dropdown menu showing 'Englisch'. There is an unchecked checkbox for 'Personalisierte Installation'. At the bottom, there are two buttons: 'Abbrechen' and 'Weiter'.

Wenn die Installation seitens Soyostart abgeschlossen ist, bekommt man eine Benachrichtigung per Mail.

### 5.2.3 SSH

Im laufenden Betrieb erfolgt die komplette Konfiguration über das Webinterface, trotzdem ist es wichtig, sich für Notfälle einen SSH Zugriff einzurichten und natürlich auch den SSH Server abzusichern.

Per SSH mit dem Server verbinden

```
ssh root@111.222.333.444
```

#### Kennwort ändern

Wenn Proxmox durch den Hoster aufgesetzt wurde und das Kennwort per Mail kam, sollte es geändert werden mit passwd

```
passwd
```

#### Normalen Useraccount anlegen

Als zusätzliche Sicherheitsstufe wird der direkte root-Login per ssh komplett untersagt. Der Login erfolgt dann über einen zusätzlich anzulegenden Benutzer. Dieser Benutzer muss über ein sicheres Passwort (TM) abgesichert werden. Nötige administrative Tätigkeiten werden mit sudo ausgeführt.

sudo installieren:

```
apt-get install sudo
```

Neuen User anlegen:

```
useradd meinbenutzername
```

Den neuen User der Gruppe "sudo" hinzufügen:

```
gpasswd -a meinbenutzername sudo
```

```
cd /home/meinbenutzername/
mkdir .ssh
nano .ssh/authorized_keys
```

Im Editor dann den Public Key ("ssh-rsa AAA...") einfügen. Wichtig: Alles von diesem Key muss in eine Zeile. Jeder Administrator bekommt nach dem beschriebenen Verfahren seinen eigenen Account.

Nun das Password-Login auf dem Server deaktivieren. Dazu die sshd\_config editieren:

```
nano /etc/ssh/sshd_config
```

Die Zeile

```
#PasswordAuthentication yes
```

ändern in

```
PasswordAuthentication no
```

Achtung, auch wenn ‘yes’ auskommentiert ist, besteht die Möglichkeit sich per Password zu verbinden, erst wenn ‘no’ gesetzt ist und nicht (mehr) auskommentiert ist, ist der Zugriff nur noch per Key möglich.

Um es den Script-Kiddies und Bots etwas schwerer zu machen, sollte der Port 22 auf einen hohen Port (mindestens über 1024) verändert werden. Dazu die Zeile

```
Port 22
```

ändern z.B. in

```
Port 62954
```

**WICHTIG:** Diesen Port muss man sich dann merken, da man ihn später beim Aufruf von ssh angeben muss.

Nun den direkten Rootlogin sperren.

```
PermitRootLogin yes
```

ändern in

```
PermitRootLogin no
```

Danach den Editor wieder verlassen und den SSH Server neu starten um die Einstellungen zu übernehmen.

```
/etc/init.d/ssh restart
```

Den nachfolgenden ssh Kommandos muss man die Option “-p 62954” (kleines “p”!) und den scp Kommandos die Option “-P 62954” (großes “P”!).

```
ssh -p 62954 meinbenutzername@111.222.333.444
```

### 5.2.4 Updates einspielen

Nun Betriebssystemupdates einspielen und ggf. erfolgende Rückfragen mit einem “J” oder “Y” abnicken, das “autoremove wird nicht viel tun, aber der Vollständigkeit halber sollte man es sich gleich angewöhnen.

```
sudo apt-get update
sudo apt-get dist-upgrade
sudo apt-get autoremove
```

Eine Fehlermeldung im Bereich “Proxmox-Enterprise” kann man entweder ignorieren. Das gibt es nur wenn man ein Support-Abo abgeschlossen hat. Wenn Ihr die Arbeit des Proxmox-Teams unterstützen möchtet:

<https://www.proxmox.com/de/proxmox-ve/preise>

Optional:

Da einzelne Repositories wiederholt nicht oder sehr schlecht per IPv6 erreichbar sind und wir unsere Maschinen grundsätzlich zur IPv6-Nutzung befähigen, empfiehlt es sich, IPv6 zumindest für “apt-get” zu unterbinden.

Dazu wird einmalig aufgerufen:

```
sudo ...!! SDFSDF echo 'Acquire::ForceIPv4 "true";' > /etc/apt/apt.conf.d/99force-ipv4
```

## 5.2.5 Monitoring

Den Check\_MK Agent steht in der Weboberfläche des Check\_MK als .deb Paket bereit:

In die CheckMK-Instanz per Webbrowser einloggen. Dann suchen:

```
-> WATO Configuration (Menü/Box)
-> Monitoring Agents
-> Packet Agents
-> check-mk-agent_1.2.8p11-1_all.deb _(Beispiel)_
```

Den Download-Link in die Zwischenablage kopieren. Im SSH-Terminal nun eingeben: (die Download-URL ist individuell und der Name des .deb-Paketes ändert sich ggf.)

```
wget https://monitoring.eulenfunk.de/eulenfunk/check_mk/agents/check-mk-agent_1.2.
↪8p11-1_all.deb
```

Um das .deb Paket zu installieren wird gdebi empfohlen, ausserdem benötigt der Agent xinetd zum ausliefern der monitoring Daten. Die Installation von gdebi kann durchaus einige Dutzend Pakete holen. Das ist leider normal. Per SSH auf dem Server. (Auch hier: Name des .deb-Files ggf. anpassen)

```
sudo apt-get install gdebi-core xinetd
```

Rückfragen ggf. mit "J" beantworten. Mit dem nun installierten gdebi das check\_mk-Paket installieren:

```
sudo gdebi check-mk-agent_1.2.8p1-1_all.deb
```

Nun noch zusätzliche Check\_MK Plugins hinzufügen

```
cd /usr/lib/check_mk_agent/plugins
sudo wget https://monitoring.eulenfunk.de/eulenfunk/check_mk/agents/plugins/smart
sudo chmod +x smart

cd /usr/lib/check_mk_agent/local
sudo wget https://raw.githubusercontent.com/eulenfunk/check_mk/master/proxmox
sudo chmod +x proxmox
```

```
:: sudo nano /etc/xinetd.d/check_mk
```

Dort die Zeile

```
# only_from = 127.0.0.1 10.0.20.1 10.0.20.2
```

ändern in

```
only_from = 127.0.0.1 94.23.160.148
```

Damit diese Änderungen aktiviert werden, muss der xinetd durchgestartet werden

```
sudo /etc/init.d/xinetd restart
```

Der Rechner hält ab nun Daten zum Abruf bereit.

Eulenfunker müssen dann das Admin-Team kontaktieren, damit der Rechner im CheckMK eingetragen wird.

## 5.2.6 Images hochladen

ISO Files zur installation können zwar über das Webinterface hochgeladen werden, aber je nach Internetanbindung dauert das lange. Per wget wird das Image direkt auf den Server geladen.

```
cd /vz/template/iso
wget http://releases.ubuntu.com/14.04.4/ubuntu-14.04.4-server-amd64.iso
```

## 5.2.7 OATH Two Factor

Der Zugang zum Proxmox ist absolut sicherheitskritisch, wer Zugriff auf den Hypervisor hat hat Zugriff auf alle Maschinen auf dem Blech. Daher muss zusätzlich der Login des Webinterface per OATH Two Factor Authentifizierung abgesichert werden.

-> [https://pve.proxmox.com/wiki/Two-Factor\\_Authentication](https://pve.proxmox.com/wiki/Two-Factor_Authentication)

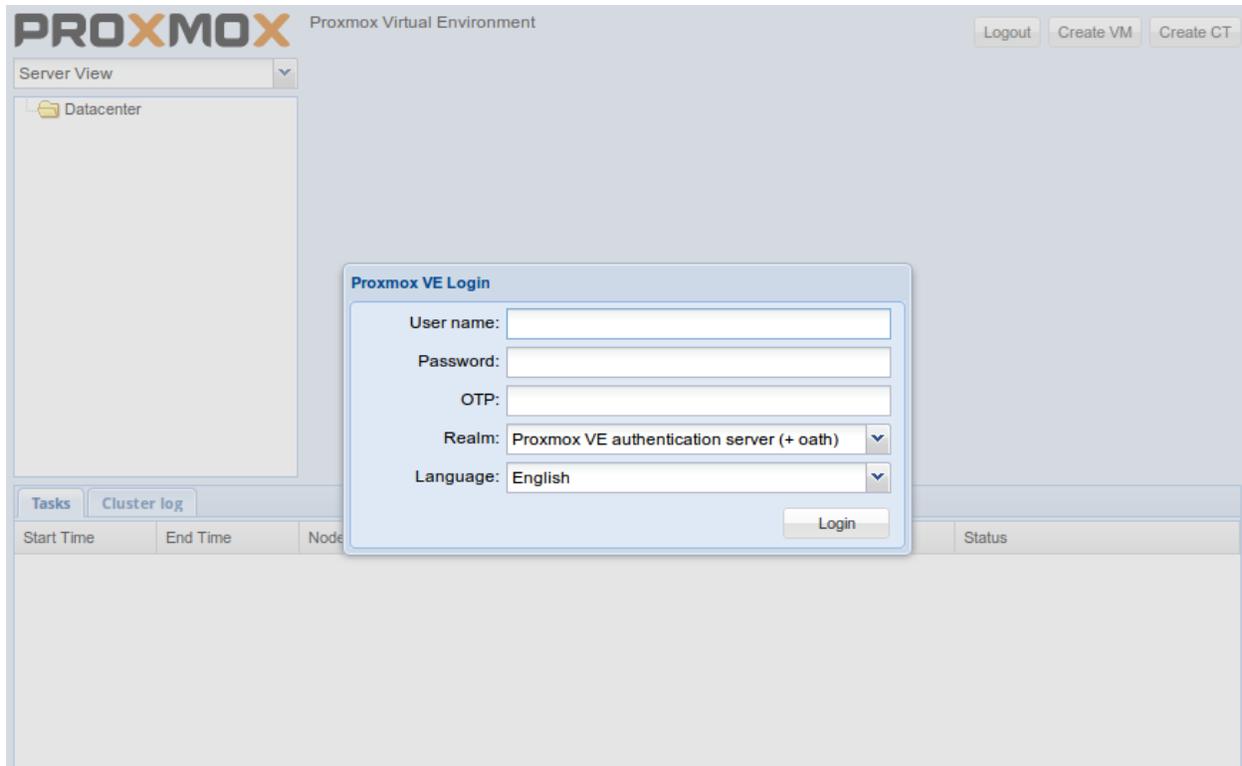
## 5.2.8 Netzwerk einrichten

Ab jetzt geht die Konfiguration über das Proxmox Webinterface im Browser:

```
https://111.222.333.444:8006
```

Beim ersten Aufruf sollte man das Zertifikat im Browser dauerhaft akzeptieren.

Die Anmeldung erfolgt mit Benutzername, Kennwort und OTP Pin. Als Realm muss Linux PAM standard authentication (+ oath) ausgewählt werden.



Nachdem links in der Seitenleiste das Blech ausgewählt wurde rechts im Reiter Network zusätzlich zur vorhandenen vmbr0 über die das Internet rein kommt noch mindestens eine vmbr1 anlegen, über die die Supernodes mit dem Konzentrator kommunizieren.

Bei OVH/Soyoustart kann es sein, dass die vmbr schon vorhanden ist, dann müsst ihr nichts tun.

Proxmox Virtual Environment  
Version: 3.4-3/2fc72fee

You are logged in as 'root@pam'

Server View: Datacenter > node01

Network configuration for Node 'node01':

Name	Type	Active	Autostart	Ports/Slaves	IP address	Subnet mask
eth0	Network Device	No	No			
eth1	Network Device	No	No			
vmbr0	Linux Bridge	Yes	Yes	eth0		
vmbr1	Linux Bridge	Yes	Yes			
vmbr2	Linux Bridge	Yes	Yes			

Pending changes (Please reboot to activate changes)

No changes

Proxmox Virtual Environment  
Version: 3.4-3/2fc72fee

You are logged in as 'root@pam'

Server View: Datacenter > node01

Network configuration for Node 'node01':

Name	Type	Active	Autostart	Ports/Slaves	IP address	Subnet mask
eth0	Network Device	No	No			
eth1	Network Device	No	No			
vmbr0	Linux Bridge	Yes	Yes	eth0		
vmbr1	Linux Bridge	Yes	Yes			
vmbr2	Linux Bridge	Yes	Yes			

Pending changes (Please reboot to activate changes)

No changes

Beim Anlegen muss als Name vmbr1 eingetragen werden und der Haken bei Autostart gesetzt werden.

**Create: Linux Bridge** ✕

Name:  Autostart:

IP address:  Bridge ports:

Subnet mask:

Gateway:

Die vmbr steht erst nach dem Neustart des Blechs zu Verfügung, daher in der Ecke oben rechts “Restart” auswählen.

**PROXMOX** Proxmox Virtual Environment Version: 3.4-3/2fc72fee You are logged in as 'root@pam'

Server View Node 'node01'   Shell

← Search Summary Services **Network** DNS Time Syslog Bootlog Task History UBC S →

Create ▾ Revert changes Edit Remove

Name ▲	Type	Active	Autostart	Ports/Slaves	IP address	Subnet mask
eth0	Network Device	No	No			
eth1	Network Device	No	No			
vmbr0	Linux Bridge	Yes	Yes	eth0		
vmbr1	Linux Bridge	Yes	Yes			
vmbr2	Linux Bridge	Yes	Yes			

Pending changes (Please reboot to activate changes)

No changes

## 5.2.9 Backup anlegen

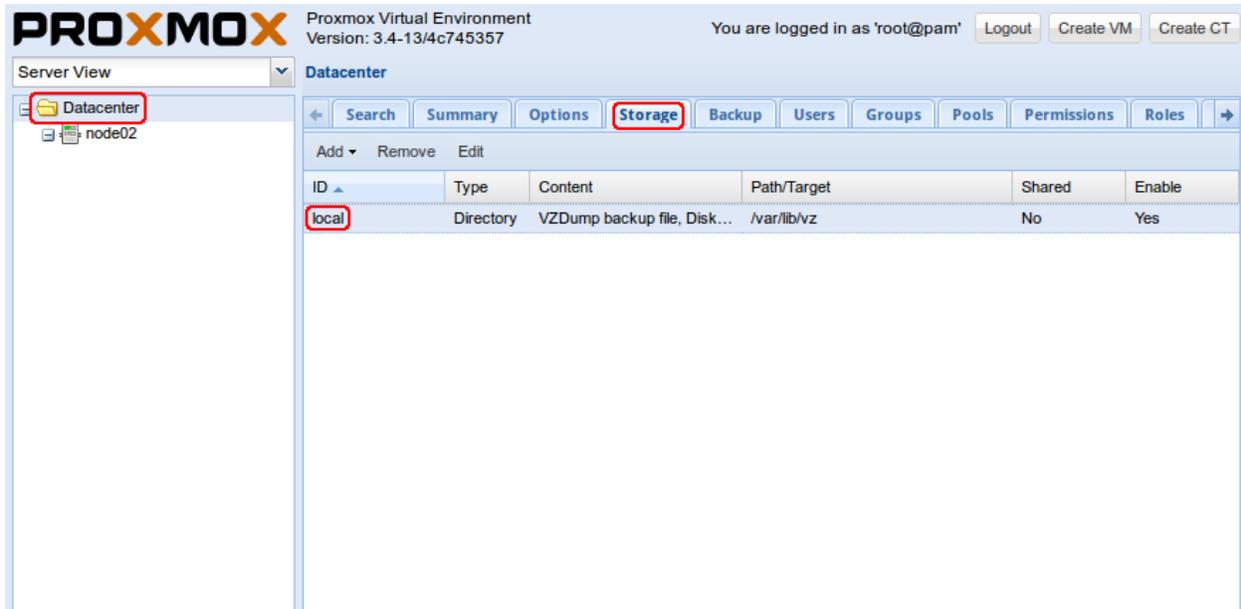
Proxmox ermöglicht es ganz einfach und auf Wunsch automatisiert Backups von den Virtuellen Maschinen anzulegen. Im Idealfall sollten die Backups auf einen externen Server/Storage erfolgen. Aus Gründen der Einfachheit beginnen wir mit einem Backup auf den lokalen Storage. Von dort kann man die Dateien für den Fall eines Totalausfalls des Blechs bei Bedarf per scp oder rsync auf einen anderen Server oder den heimischen Computer sichern.

Das Backup auf dem lokalen Storage erzeugt massiv IO, denn neben den normalen Zugriffen, die die Maschinen im Betrieb erzeugen kommen noch Lesezugriffe auf die zu sichernde VM und Schreibzugriffe auf die Backupdatei dazu.

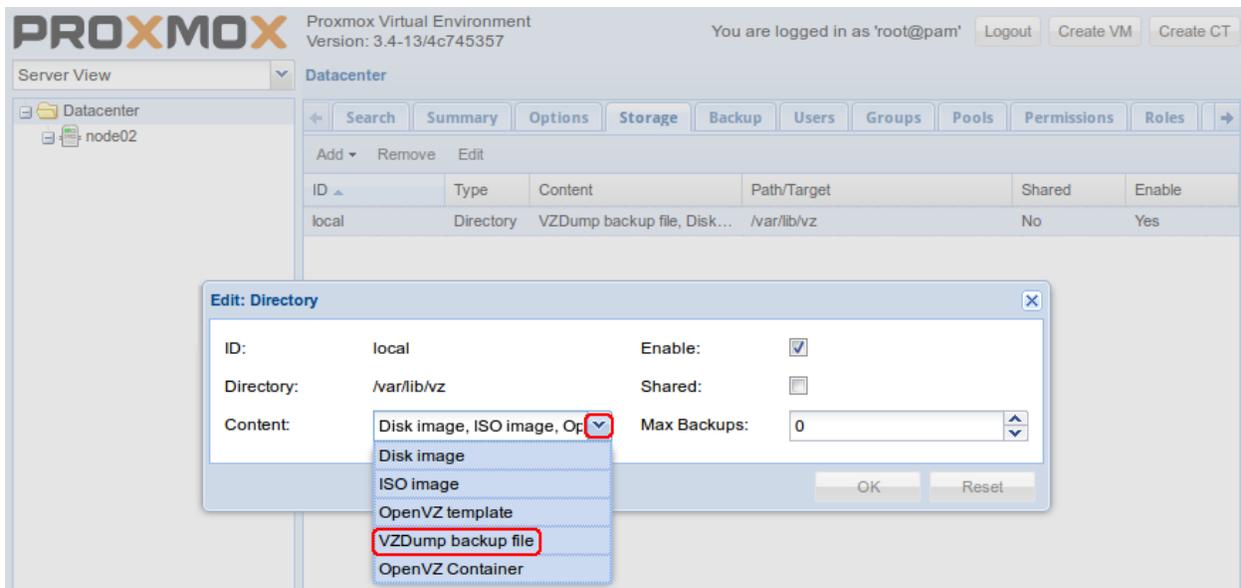
Sobald der IO die Kapazität des Storage übersteigt, gerade bei den einfachen Raids aus klassischen HDDs in den OVH/SYS Servern ist dies schnell der Fall, wird die Performance des gesamten Blechs und aller VMs darunter leiden.

Das Backup sollte daher zur Zeit der geringsten Auslastung erfolgen, z.B. jeden Montag um 1 Uhr in der Nacht.

Zuerst muss ein Backupstorage definiert werden, dazu muss links das Datacenter ausgewählt werden, rechts der Tab Storage und dort der lokale Storage konfiguriert werden.



Dort muss dann VZDump backup file zusätzlich ausgewählt werden (STRG+Klick)



Als nächstes im Reiter Backup einen Backupjob hinzufügen. Bei Node wird “– All –” und bei Mode Snapshot ausgewählt. Storage setzt man auf local. Als Compression wählt man “LZO (fast)” um die Prozessorauslastung gering zu halten.

The screenshot shows the Proxmox Virtual Environment interface. At the top, it says "Proxmox Virtual Environment Version: 3.4-13/4c745357" and "You are logged in as 'root@pam'". There are buttons for "Logout", "Create VM", and "Create CT". The main navigation bar includes "Search", "Summary", "Options", "Storage", "Backup" (highlighted with a red box), "Users", "Groups", "Pools", "Permissions", and "Roles". On the left, there is a "Server View" dropdown and a "Datacenter" sidebar showing a tree view with "node02". The main content area shows the "Backup" configuration page with an "Add" button (circled in red) and a table with columns: Node, Day of week, Start Time, Storage, and Selection.

The screenshot shows the "Create: Backup Job" dialog box. It contains several configuration fields:

- Node:** -- All --
- Storage:** local
- Day of week:** Monday
- Start Time:** 01:00
- Selection mode:** All
- Send email to:** (empty text field)
- Email notification:** Always
- Compression:** LZO (fast)
- Mode:** Snapshot

Below the fields is a table listing existing backup jobs:

<input checked="" type="checkbox"/>	ID ^	Node	Status	Name	Type
<input checked="" type="checkbox"/>	100	node02	stopped	Meinerzhagen-1	qemu
<input checked="" type="checkbox"/>	101	node02	stopped	Altena-1	qemu
<input checked="" type="checkbox"/>	102	node02	running	Luedenscheid-1	qemu
<input checked="" type="checkbox"/>	103	node02	running	Meinerzhagen-1neu	qemu
<input checked="" type="checkbox"/>	104	node02	running	Altena-1neu	qemu
<input checked="" type="checkbox"/>	110	node02	running	fichtenbackbone-2	qemu

At the bottom right of the dialog is a "Create" button.

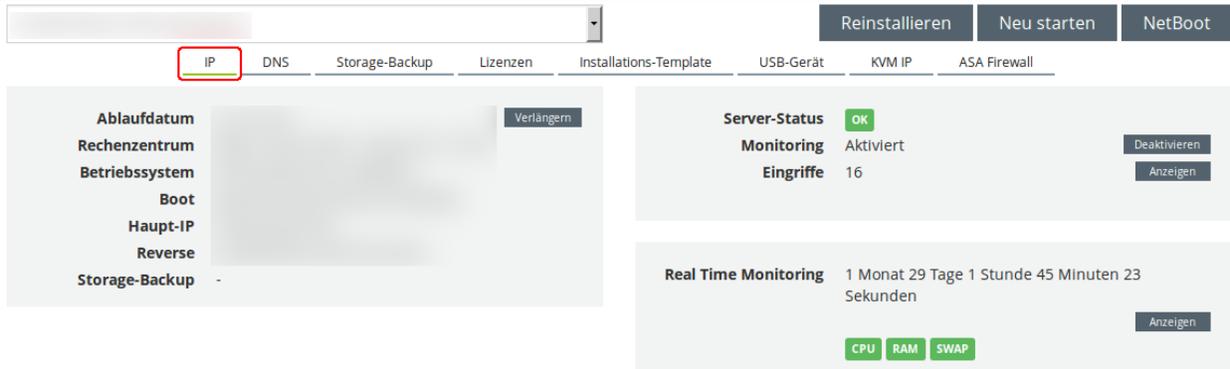
### 5.3 BGP Konzentrador einrichten

Der BGP Konzentrador ist der Backboneseite unserer zwei Freifunk Server, er übernimmt Routing, NAT, Connection tracking, GRE Tunnel und BGP Sessions.

Für die virtuelle Maschine benötigen wir eine öffentliche IPv4 Adresse. Diese könnt ihr beim Rechenzentrum kaufen,

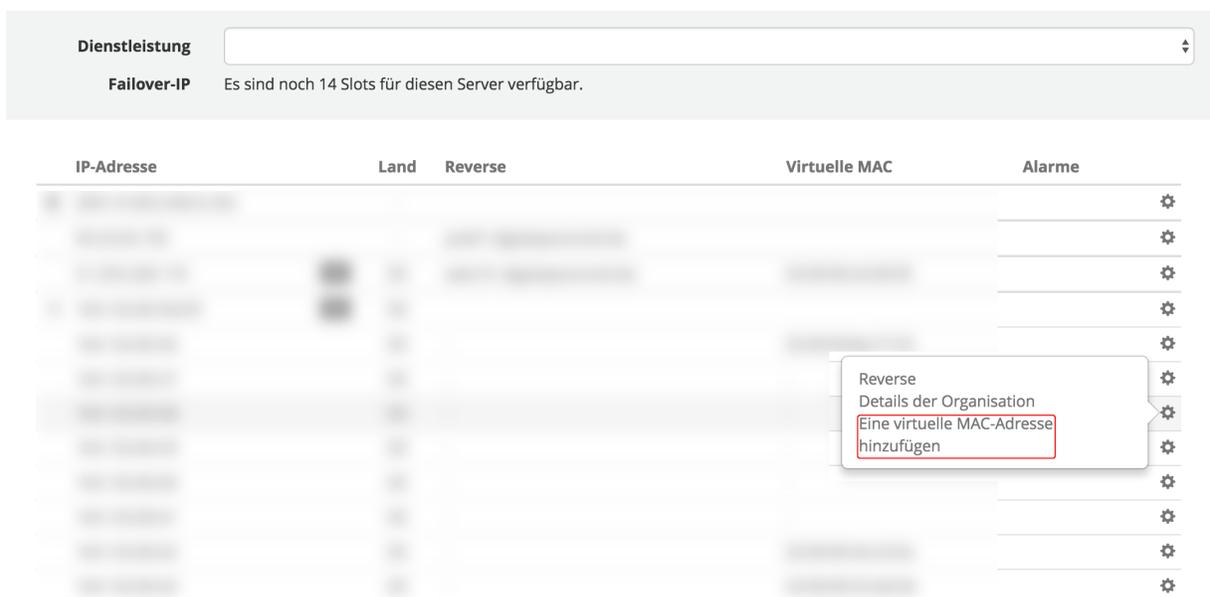
nennt sich z.B. Failover IP. Für diese IP Adresse muss im Kundeninterface eine MAC Adresse erstellt werden, die dann im Proxmox auf der Netzwerkkarte der virtuellen Maschine konfiguriert wird.

Im Kundeninterface wird “IP” ausgewählt



In dem erscheinenden Formular klickt man das Zahnrad an der betreffenden IP-Adresse an und wählt “Eine virtuelle MAC-Adresse hinzufügen”

## Verwaltung der IP-Adressen



Im folgenden muss “Eine neue virtuelle MAC-Adresse erstellen” angeklickt werden und der Name der VM eingetragen werden.

**Die virtuelle MAC-Adresse ändern**
Support ▾

**Server**

**IP-Adresse**

**VM-Name**

**Typ der virtuellen MAC-Adresse**

**Sie möchten:**

Eine neue virtuelle MAC-Adresse erstellen

Eine existierende virtuelle MAC-Adresse verwenden

Abbrechen
Bestätigen

Auf dem Webinterface des Proxmox Servers ist auf der linken Seite das Blech auszuwählen und dann oben rechts 'Create VM' anklicken

PROXMOX Proxmox Virtual Environment Version: 3.4-3/2fc72fee You are logged in as 'root@pam' Logout **Create VM** Create CT

Server View Node 'node01' Restart Shutdown Shell ▾ More ▾

Search Summary Services **Network** DNS Time Syslog Bootlog Task History UBC ↵

Create ▾ Revert changes Edit Remove

Name ▲	Type	Active	Autostart	Ports/Slaves	IP address	Subnet mask
eth0	Network Device	No	No			
eth1	Network Device	No	No			
vmbr0	Linux Bridge	Yes	Yes	eth0		
vmbr1	Linux Bridge	Yes	Yes			
vmbr2	Linux Bridge	Yes	Yes			

Pending changes (Please reboot to activate changes)

No changes

Im Reiter 'General' eine Freie ID und einen Namen festlegen.

The screenshot shows the 'Create: Virtual Machine' dialog box with the 'General' tab selected. The 'Node' dropdown is set to 'node01' and the 'Resource Pool' dropdown is empty. The 'VM ID' is '103'. The 'Name' field contains 'xyzbackbone-1' and is highlighted with a red box. At the bottom right, the 'Next' button is also highlighted with a red box.

Node: node01 Resource Pool:

VM ID: 103

Name: xyzbackbone-1

Back Next

Im Reiter 'OS' 'Linux 4.x/3.x/2.6 Kernel auswählen.

The screenshot shows the 'Create: Virtual Machine' dialog box with the 'OS' tab selected. Under 'Microsoft Windows', there are five radio button options. Under 'Linux/Other OS types', the 'Linux 3.X/2.6 Kernel (I26)' option is selected and highlighted with a red box. At the bottom right, the 'Next' button is also highlighted with a red box.

Microsoft Windows

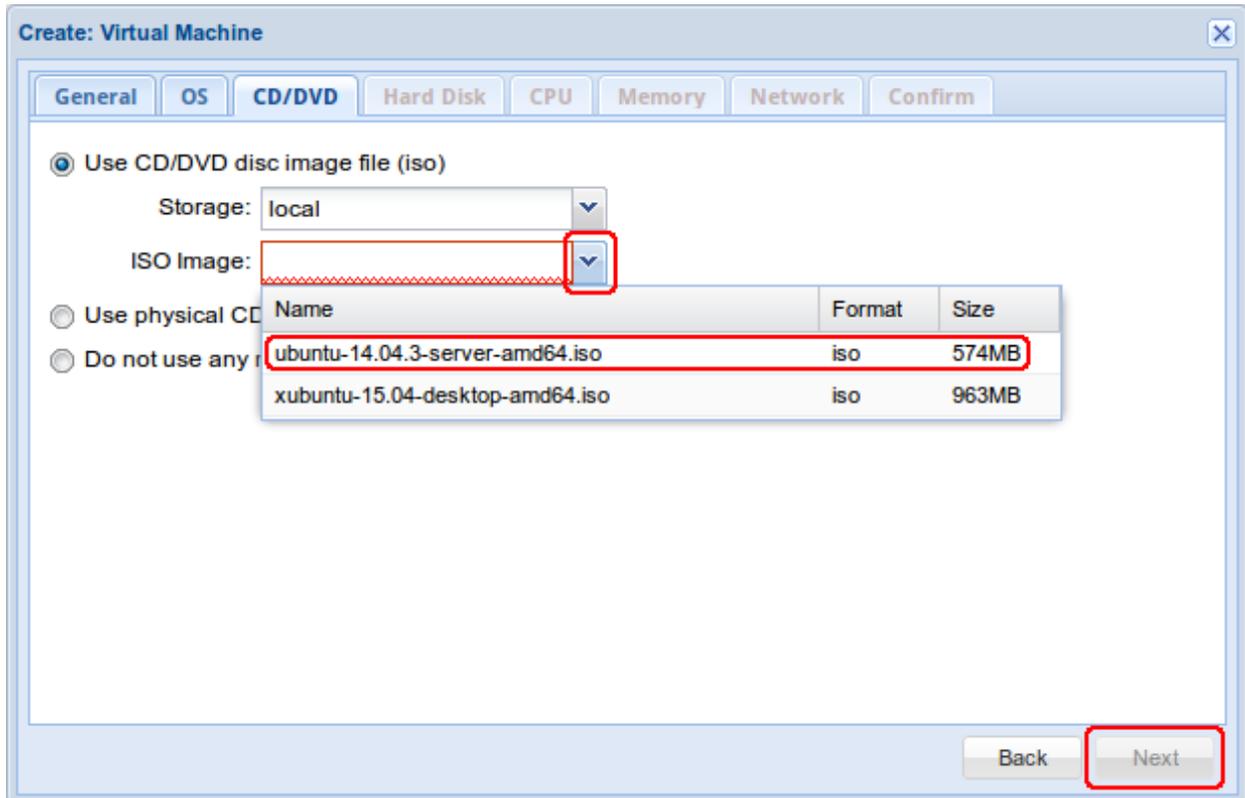
- Microsoft Windows 8/2012 (win8)
- Microsoft Windows 7/2008r2 (win7)
- Microsoft Windows Vista/2008 (w2k8)
- Microsoft Windows XP/2003 (wxp)
- Microsoft Windows 2000 (w2k)

Linux/Other OS types

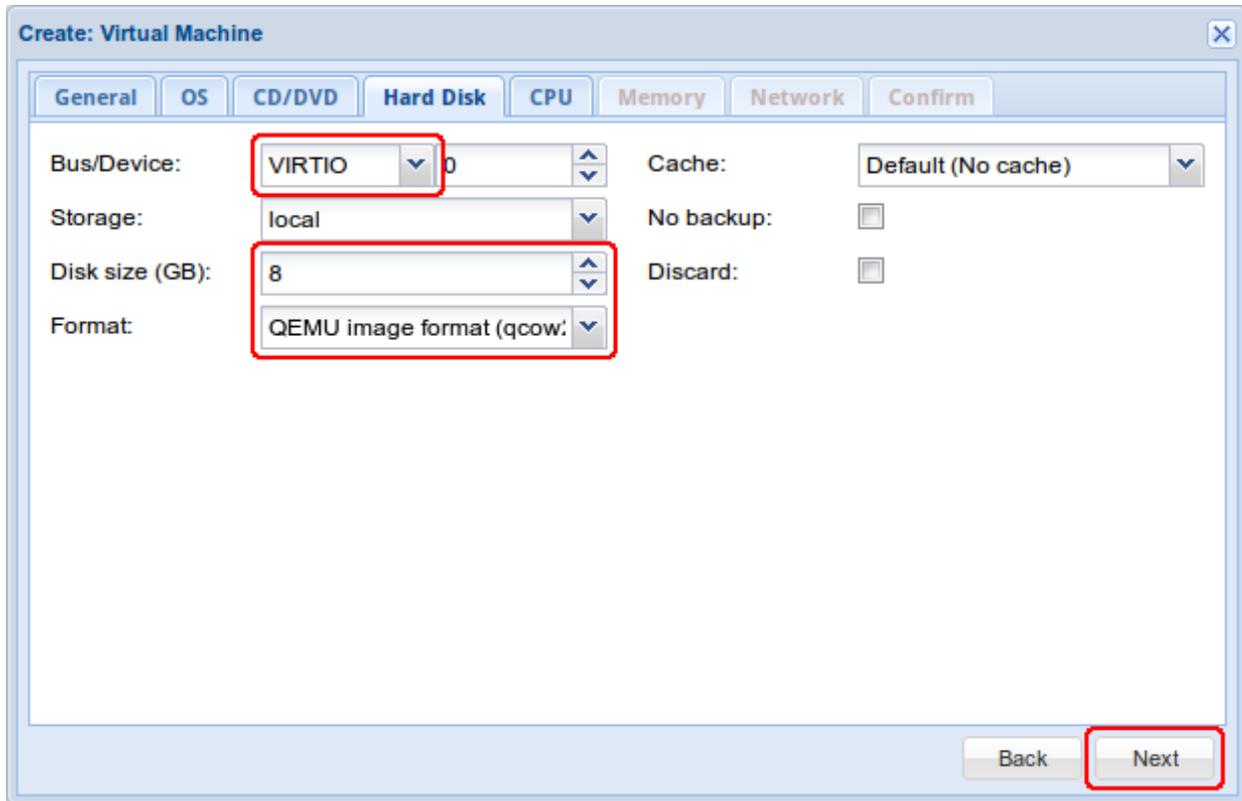
- Linux 3.X/2.6 Kernel (I26)
- Linux 2.4 Kernel (I24)
- Solaris Kernel (solaris)
- Other OS types (other)

Back Next

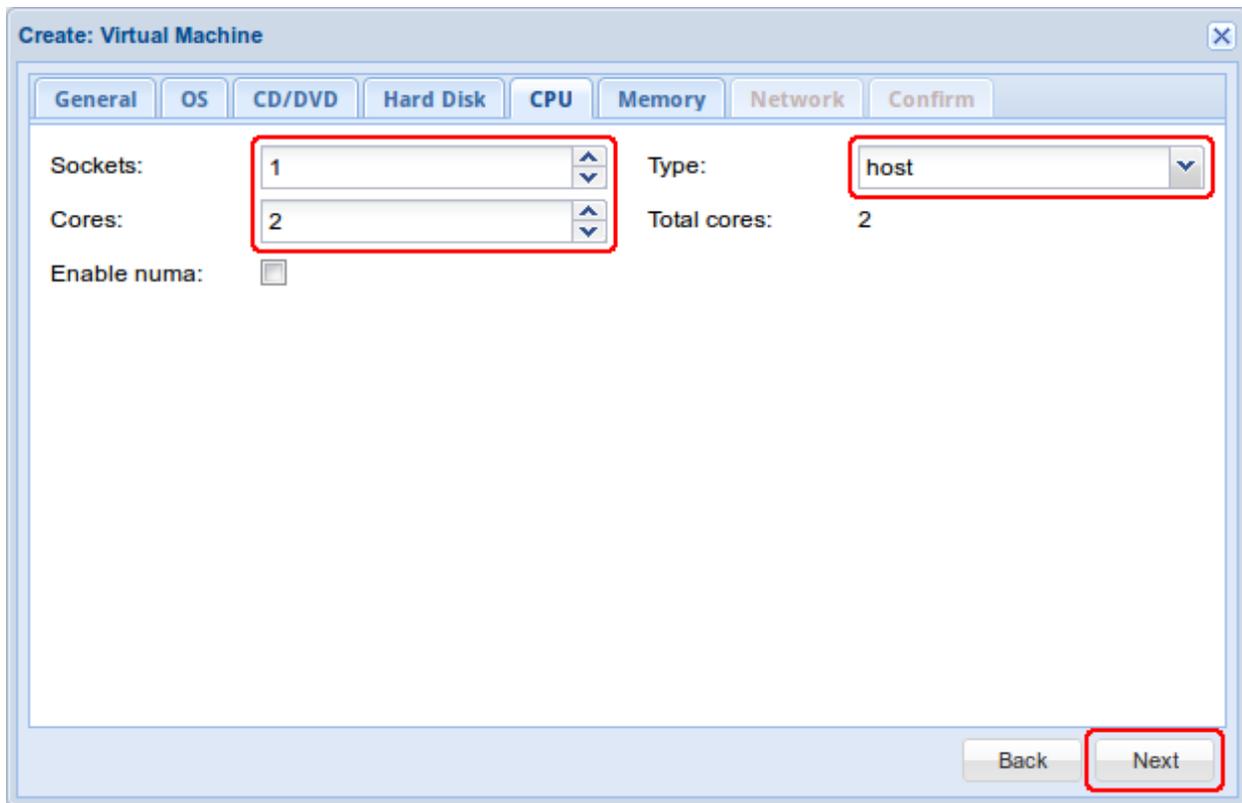
Im Reiter 'CD/DVD' das ISO Image auswählen.



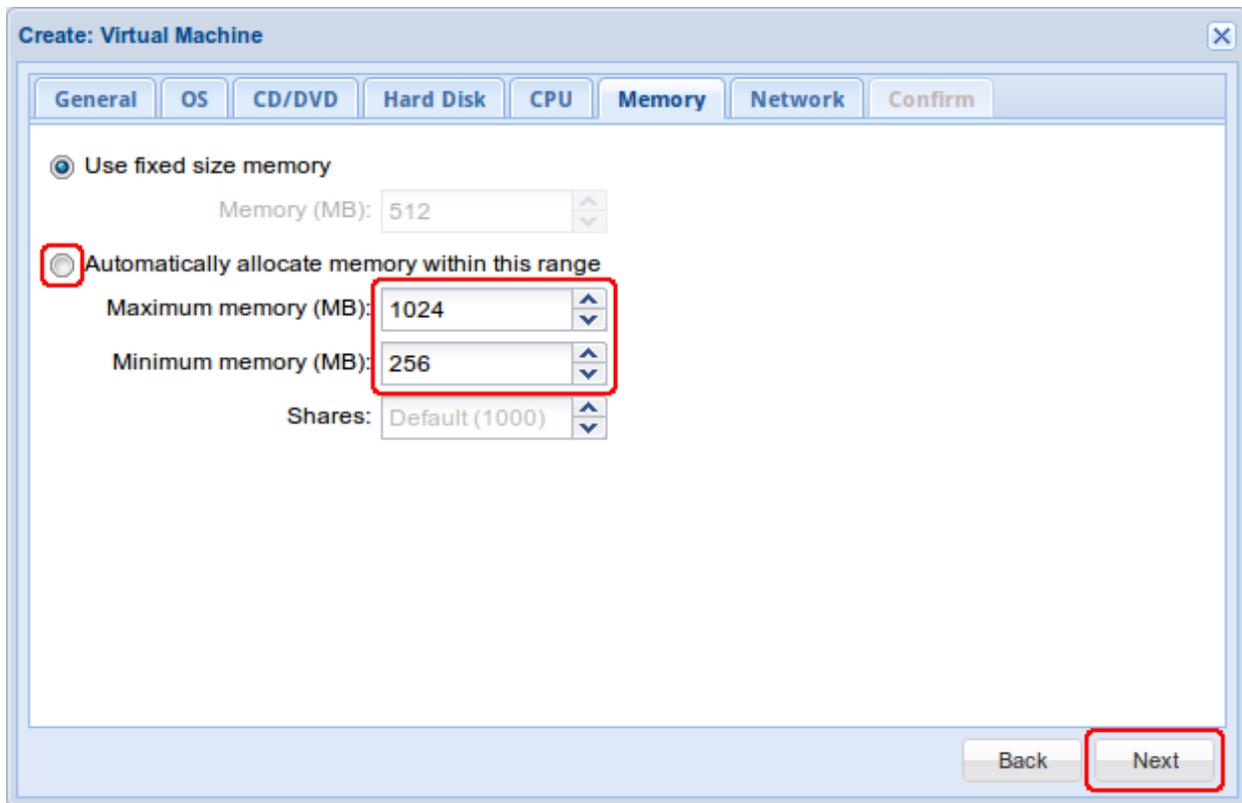
Im Reiter 'Hard Disk' als 'Bus' 'VirtIO' einstellen, die Festplattengröße auf 6GB begrenzen und als Format 'qcow2' wählen. Größere Festplatten machen Backups, Rollbacks und co nur aufwändiger.



Im Reiter 'CPU' ein Prozessorkern zuweisen. Als CPU kann man "host" wählen, das tut der Performance gut und HA nutzen wir ohnehin nicht.



Im Reiter 'Memory' unter 'Automatically allocate memory within this range' 256 - 1024MB festlegen. Weniger als 256 hindert einige Maschinen beim booten, mehr als 1024 werden nicht benötigt.



Im Reiter 'Network' als Netzwerkkarte 'VirtIO' auswählen und die MAC Adresse der für diese VM zu verwendenden öffentlichen IPv4 Adresse eintragen. Bridged Mode übernehmen wir so und vmbr0 auch diese.

Create: Virtual Machine

General OS CD/DVD Hard Disk CPU Memory **Network** Confirm

Bridged mode  
 Model: Intel E1000  
 VLAN Tag: no VLAN  
 MAC address: auto  
 Bridge: vmbr0  
 Rate limit (MB/s): unlimited  
 Firewall:   
 Multiqueues:  
 Disconnect:

NAT mode  
 No network device

Back Next

Bestätigen und Anlegen auswählen.

Create: Virtual Machine

General OS CD/DVD Hard Disk CPU Memory Network **Confirm**

**Settings**

Key	Value
balloon	256
cores	2
cpu	host
ide2	local:iso/ubuntu-14.04.3-server-amd64.iso,media=cdrom
memory	1024
name	xyzbackbone-1
net0	e1000,bridge=vmbr0
nodename	node01
numa	0
ostype	l26
sockets	1

Back Finish

Fehlermeldungen während der Startphase werden unten im Log-Fenster angezeigt, erscheinen immer “oben”, jedoch mit einigen Sekunden Verzögerung. Details lassen sich ausklappen.

Hinweis: Wenn das System später läuft, nicht vergessen, die Option “Start at boot” auf “Yes” zu stellen.

The screenshot shows the Proxmox Virtual Environment interface. The left sidebar displays a tree view of the datacenter with 'node01' and VM '103 (xyzbackbone-1)'. The main panel shows the configuration for VM '103 (xyzbackbone-1)' on 'node01'. The 'Options' tab is selected and highlighted with a red box. The 'Start at boot' option is also highlighted with a red box and is currently set to 'No'.

Options	
Name	xyzbackbone-1
Start at boot	No
Start/Shutdown order	order=any
OS Type	Linux 3.X/2.6 Kernel (i26)
Boot order	Disk 'virtio0', CD-ROM, Network
Use tablet for pointer	Yes
Hotplug	Disk, Network, USB
ACPI support	Yes
SCSI Controller Type	Default (LSI 53C895A)
KVM hardware virtualization	Yes

### 5.3.1 Ubuntu Server Installieren

Die VM links auswählen und oben rechts starten und die Konsole öffnen

The screenshot shows the Proxmox Virtual Environment interface. The left sidebar displays a tree view of the datacenter with 'node01' and VM '103 (xyzbackbone-1)'. The main panel shows the configuration for VM '103 (xyzbackbone-1)' on 'node01'. The 'Start' button is highlighted with a red box, and the 'Console' button is also highlighted with a red box. The 'Options' tab is selected.

Options	
Name	xyzbackbone-1
Start at boot	No
Start/Shutdown order	order=any
OS Type	Linux 3.X/2.6 Kernel (i26)
Boot order	Disk 'virtio0', CD-ROM, Network
Use tablet for pointer	Yes
Hotplug	Disk, Network, USB
ACPI support	Yes
SCSI Controller Type	Default (LSI 53C895A)
KVM hardware virtualization	Yes

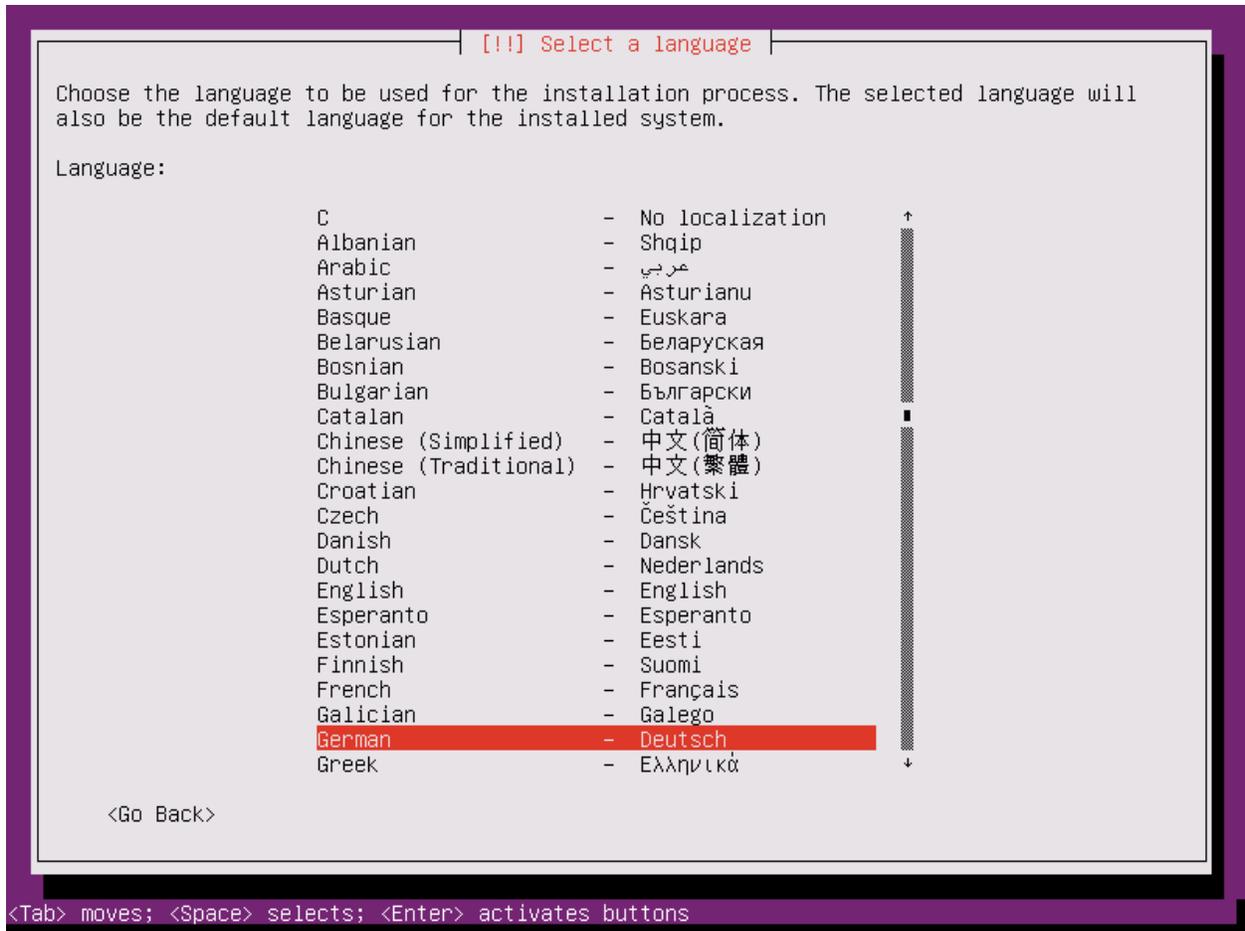
Deutsch als Sprache auswählen und nun Ubuntu Server Installieren

Language			
Amharic	Français	Македонски	Tamil
Arabic	Gaeilge	Malayalam	தமிழ்
Asturiano	Galego	Marathi	Thai
Беларуская	Gujarati	Burmese	Tagalog
Български	Ἰνδία	Nepali	Türkçe
Bengali	Hindi	Nederlands	Uyghur
Tibetan	Hrvatski	Norsk bokmål	Українська
Bosanski	Magyar	Norsk nynorsk	Tiếng Việt
Català	Bahasa Indonesia	Punjabi (Gurmukhi)	中文(简体)
Čeština	Íslenska	Polski	中文(繁體)
Dansk	Italiano	Português do Brasil	
<b>Deutsch</b>	日本語	Português	
Dzongkha	தமிழ்	Română	
Ελληνικά	Қазақ	Русский	
English	Khmer	Sámegillii	
Esperanto	ಕನ್ನಡ	සිංහල	
Español	한국어	Slovenčina	
Eesti	Kurdî	Slovenščina	
Euskara	Lao	Shqip	
عَرَبِيَّة	Lietuviškai	Српски	
Suomi	Latviski	Svenska	

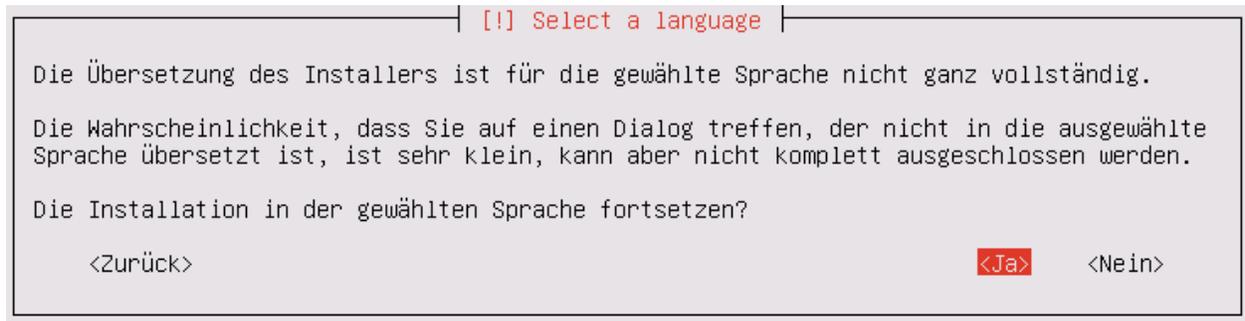
F1 Help F2 Language F3 Keymap F4 Modes F5 Accessibility F6 Other Options



Als Installationssprache jetzt nochmal Deutsch auswählen,



die Auswahl trotz unvollständiger Unterstützung bestätigen,



den Standort auswählen (Deutschland),

## [!] Auswählen des Standorts

Der hier ausgewählte Standort wird verwendet, um die Zeitzone zu setzen und auch, um zum Beispiel das System-Gebietsschema (locale) zu bestimmen. Normalerweise sollte dies das Land sein, in dem Sie leben.

Diese Liste enthält nur eine kleine Auswahl von Standorten, basierend auf der Sprache, die Sie ausgewählt haben. Wählen Sie »weitere«, falls Ihr Standort nicht aufgeführt ist.

Land oder Gebiet:

Belgien  
Deutschland  
Liechtenstein  
Luxemburg  
Österreich  
Schweiz  
weitere

<Zurück>

das Tastaturmodell nicht automatisch erkennen lassen

## [!] Tastatur konfigurieren

Sie können versuchen das Tastaturmodell anhand von Tasteneingaben erkennen zu lassen. Wenn Sie das nicht möchten, können sie das Tastaturmodell aus einer Liste wählen.

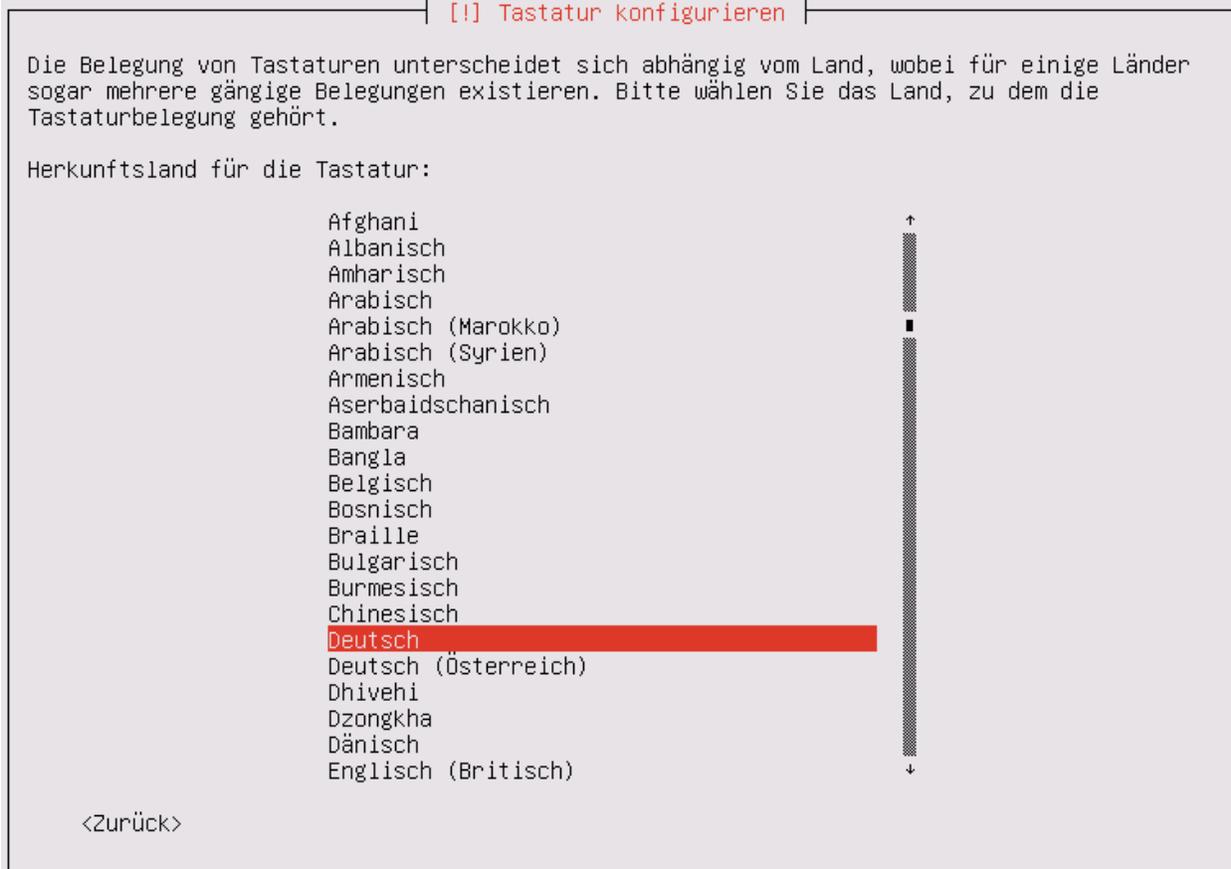
Tastaturmodell erkennen?

<Zurück>

<Ja>

<Nein>

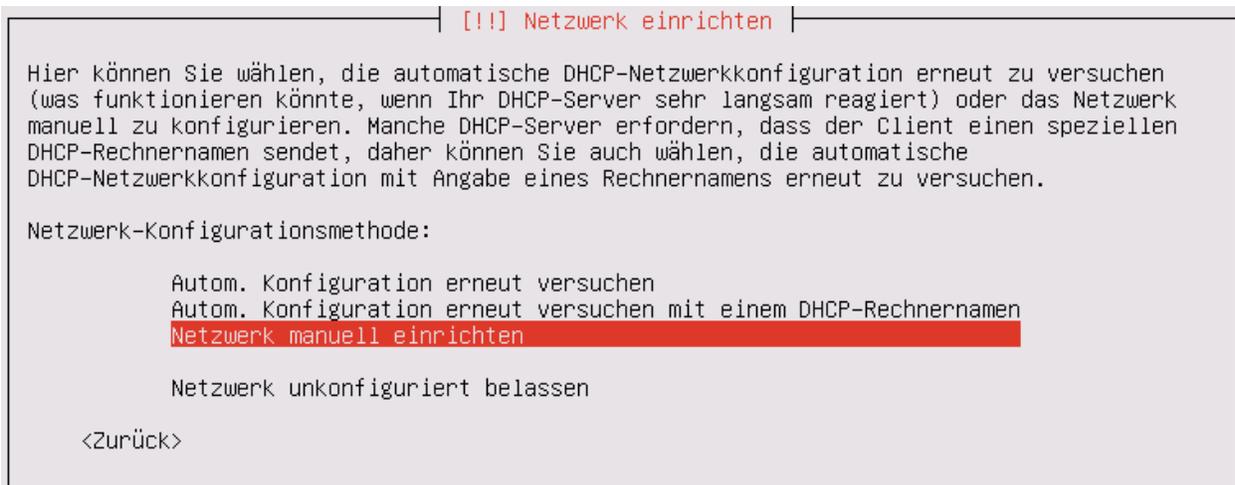
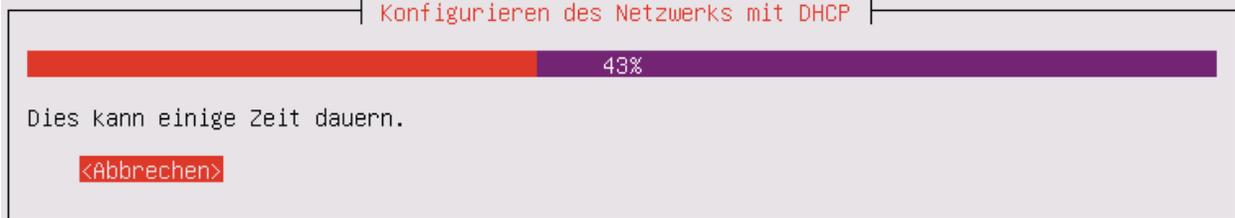
Herkunftsland der Tastatur "Deutsch"



## Tastaturbelegung "Deutsch"



Sobald der Server versucht das Netzwerk automatisch zu konfigurieren, dies abbrechen und die manuelle Netzwerkkonfiguration auswählen.



Die Failover-IP, für die wir vorhin die MAC-Adresse erstellt haben ist beispielsweise die 555.666.777.888

| [!] Netzwerk einrichten |

Die IP-Adresse ist für Ihren Rechner eindeutig und kann zwei verschiedene Formate haben:

- \* vier Zahlen, getrennt durch Punkte (IPv4);
- \* Blöcke von hexadezimalen Zeichen, getrennt durch Doppelpunkte (IPv6).

Sie können auch optional eine CIDR-Netzmaske (wie z.B. »/24«) anfügen.

Wenn Sie nicht wissen, was Sie eingeben sollen, fragen Sie Ihren Netzwerk-Administrator.

IP-Adresse:

555.666.777.888

<Zurück>

<Weiter>

---

Die Subnetzmaske von 255.255.255.0 bleibt in der Regel so

| [!] Netzwerk einrichten |

Durch die Netzmaske kann bestimmt werden, welche Rechner im lokalen Netzwerk direkt angesprochen werden können. Wenn Sie diesen Wert nicht kennen, fragen Sie Ihren Netzwerkadministrator. Die Netzmaske besteht aus vier durch Punkte getrennte Zahlen.

Netzmaske:

255.255.255.0

<Zurück>

<Weiter>

---

Die Gateway Adresse sollte man beim Rechenzentrum erfragen.

Bei OVH/Soyoustart ist das IPv4 Gateway immer auf der 254, also 555.666.777.254

| [!] Netzwerk einrichten |

Geben Sie hier die IP-Adresse (vier durch Punkte getrennte Zahlen) des Gateways ein, auch als Default-Router bekannt. Alle Daten zu Rechnern außerhalb Ihres LAN (zum Beispiel zum Internet) werden über diesen Router gesendet. In seltenen Fällen haben Sie keinen Router, in diesem Fall geben Sie hier einfach nichts ein. Wenn Sie die richtige Antwort hier nicht kennen, fragen Sie Ihren Netzwerkadministrator.

Gateway:

555.666.777.254

<Zurück>

<Weiter>

---

Als DNS geht z.B. der 8.8.8.8 von Google (Böse!).

[!] Netzwerk einrichten

Nameserver (DNS-Server) werden benutzt, um Rechnernamen im Internet aufzulösen. Bitte geben Sie die IP-Adressen (nicht die Rechnernamen) von bis zu drei Nameservern getrennt durch Leerzeichen an. Benutzen Sie keine Kommata. Der erste Server in der Liste wird als erstes abgefragt. Wenn Sie keine Nameserver benutzen möchten, lassen Sie dieses Feld bitte einfach leer.

Adresse des DNS-Servers:

8.8.8.8

<Zurück> <Weiter>

Der Rechnername ist frei wählbar

[!] Netzwerk einrichten

Bitte geben Sie den Namen dieses Rechners ein.

Der Rechnername ist ein einzelnes Wort, das Ihren Rechner im Netzwerk identifiziert. Wenn Sie Ihren Rechnernamen nicht kennen, fragen Sie den Netzwerkadministrator. Wenn Sie ein lokales Heimnetz aufbauen, ist es egal, was Sie angeben.

Rechnername:

Max

<Zurück> <Weiter>

Der Domainname ist hier einzutragen

[!] Netzwerk einrichten

Der Domain-Name ist der rechte Teil Ihrer Internetadresse nach Ihrem Rechnernamen. Er endet oft mit .de, .com, .net oder .org. Wenn Sie ein lokales Heimnetz aufbauen, ist es egal, was Sie angeben. Diese Information sollte dann aber auf allen Rechnern gleich sein.

Domain-Name:

trollfunk.de

<Zurück> <Weiter>

Und der Benutzer angelegt werden. Zunächst der volle Benutzername

[!] Benutzer und Passwörter einrichten

Für Sie wird ein Konto angelegt, das Sie statt dem root-Konto für die alltägliche Arbeit verwenden können.

Bitte geben Sie den vollständigen Namen des Benutzers an. Diese Information wird z.B. im Absender von E-Mails, die er verschickt, oder in Programmen, die den Namen des Benutzers anzeigen, verwendet. Ihr kompletter Name wäre sinnvoll.

Vollständiger Name des neuen Benutzers:

Max

[<Zurück>](#)

[<Weiter>](#)

und dann das gewünschte Login

[!] Benutzer und Passwörter einrichten

Wählen Sie einen Benutzernamen für das neue Benutzerkonto. Der Vorname ist meist eine gute Wahl. Der Benutzername sollte mit einem kleinen Buchstaben beginnen, gefolgt von weiteren kleinen Buchstaben oder auch Zahlen.

Benutzername für Ihr Konto:

max

[<Zurück>](#)

[<Weiter>](#)

Das Kennwort sollte sicher sein und nicht bereits für einen anderen Zweck in Verwendung.

[!] Benutzer und Passwörter einrichten

Ein gutes Passwort enthält eine Mischung aus Buchstaben, Zahlen und Sonderzeichen und wird in regelmäßigen Abständen geändert.

Wählen Sie ein Passwort für den neuen Benutzer:

\*\*\*\*\*

[<Zurück>](#)

[<Weiter>](#)

Da auf dem Server keine persönlichen Dateien gespeichert werden sollen ist es nicht notwendig den persönlichen Ordner zu verschlüsseln.

## [!] Benutzer und Passwörter einrichten

Sie können Ihren persönlichen Ordner verschlüsseln, sodass alle darin gespeicherten Dateien privat bleiben, selbst wenn Ihr Rechner gestohlen wird.

Das System wird Ihren verschlüsselten Ordner bei jedem Anmelden nahtlos einbinden und diesen automatisch aushängen, sobald Sie sich aus allen aktiven Sitzungen abmelden.

Ihren persönlichen Ordner verschlüsseln?

<Zurück>

<Ja>

<Nein>

Zeitzone Prüfen und bestätigen.

Festplatte manuell formatieren

## [!!] Festplatten partitionieren

Der Installer kann Sie durch die Partitionierung einer Festplatte (mit verschiedenen Standardschemata) führen. Wenn Sie möchten, können Sie dies auch von Hand tun. Bei Auswahl der geführten Partitionierung können Sie die Einteilung später noch einsehen und anpassen.

Falls Sie eine geführte Partitionierung für eine vollständige Platte wählen, werden Sie gleich danach gefragt, welche Platte verwendet werden soll.

Partitionierungsmethode:

Geführt - vollständige Festplatte verwenden  
 Geführt - gesamte Platte verwenden und LVM einrichten  
 Geführt - gesamte Platte mit verschlüsseltem LVM  
**Manuell**

<Zurück>

Freien Speicherplatz auswählen und enter

## [!!] Festplatten partitionieren

Dies ist eine Übersicht über Ihre konfigurierten Partitionen und Einbindungspunkte. Wählen Sie eine Partition, um Änderungen vorzunehmen (Dateisystem, Einbindungspunkt, usw.), freien Speicher, um Partitionen anzulegen oder ein Gerät, um eine Partitionstabelle zu erstellen.

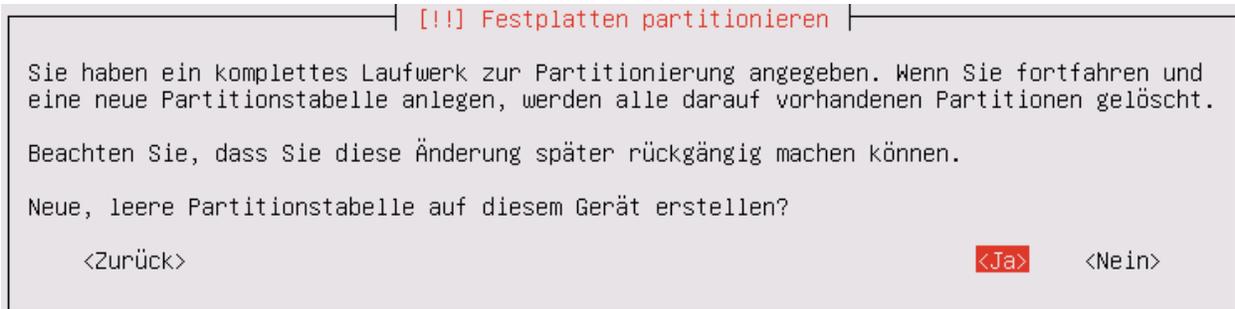
Geführte Partitionierung  
 Configure iSCSI volumes

**Virtuelle Festplatte 1 (vda) - 8.6 GB Virtio Block Device**

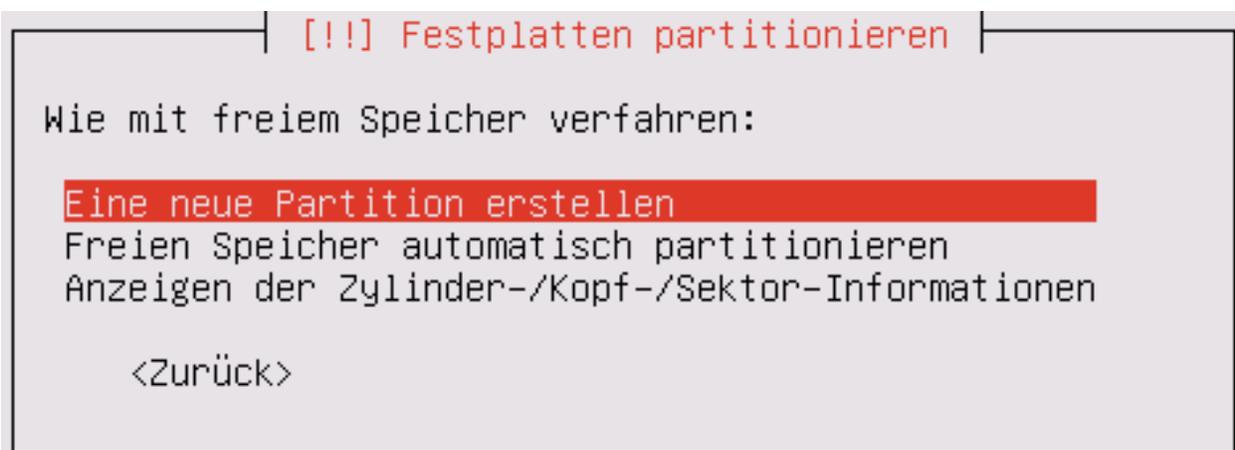
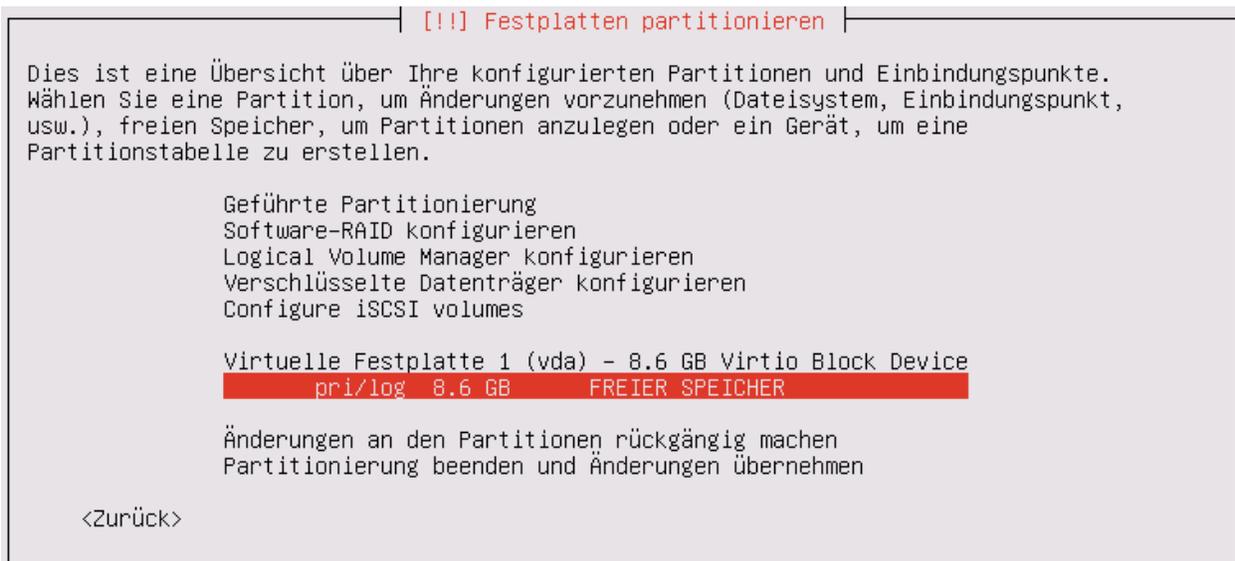
Änderungen an den Partitionen rückgängig machen  
 Partitionierung beenden und Änderungen übernehmen

<Zurück>

Partitionstabelle erstellen



Freien Speicherplatz auswählen und enter



Partitionsgröße 5 GB Primär am Anfang

```
[!!] Festplatten partitionieren

Die maximale Größe für diese Partition beträgt 8.6 GB.

Tipp: »max« kann als Kürzel verwendet werden, um die maximale Größe anzugeben. Alternativ
kann eine prozentuale Angabe (z.B. »20%«) erfolgen, um die Größe relativ zum Maximum
anzugeben.

Neue Größe der Partition:
7 GB
<Zurück>                                     <Weiter>
```

```
[!!] Festplatten partitionieren

Typ der neuen Partition:

  Primär
  Logisch

<Zurück>
```

```
[!!] Festplatten partitionieren

Bitte wählen Sie, ob die neue Partition am Anfang oder am Ende des verfügbaren Speichers
erstellt werden soll.

Position der neuen Partition:

  Anfang
  Ende

<Zurück>
```

Bootflag auf 'ein' setzen und 'Anlegen beenden'

```
| [!] Festplatten partitionieren |
Sie bearbeiten Partition 1 auf Virtuelle Festplatte 1 (vda). Auf dieser Partition wurde
kein vorhandenes Dateisystem gefunden.

Partitionseinstellungen:

    Benutzen als:                               Ext4-Journaling-Dateisystem

    Einbindungspunkt:                             /
    Einbindungsoptionen:                         defaults
    Name:                                          Keiner
    Reservierte Blöcke:                           5%
    Typische Nutzung:                             standard
    Boot-Flag (Boot-fähig-Markierung):          Ein

    Daten von einer anderen Partition kopieren
    Die Partition löschen
    Anlegen der Partition beenden

<Zurück>
```

Freien Speicherplatz auswählen und enter

```
| [!] Festplatten partitionieren |
Dies ist eine Übersicht über Ihre konfigurierten Partitionen und Einbindungspunkte.
Wählen Sie eine Partition, um Änderungen vorzunehmen (Dateisystem, Einbindungspunkt,
usw.), freien Speicher, um Partitionen anzulegen oder ein Gerät, um eine
Partitionstabelle zu erstellen.

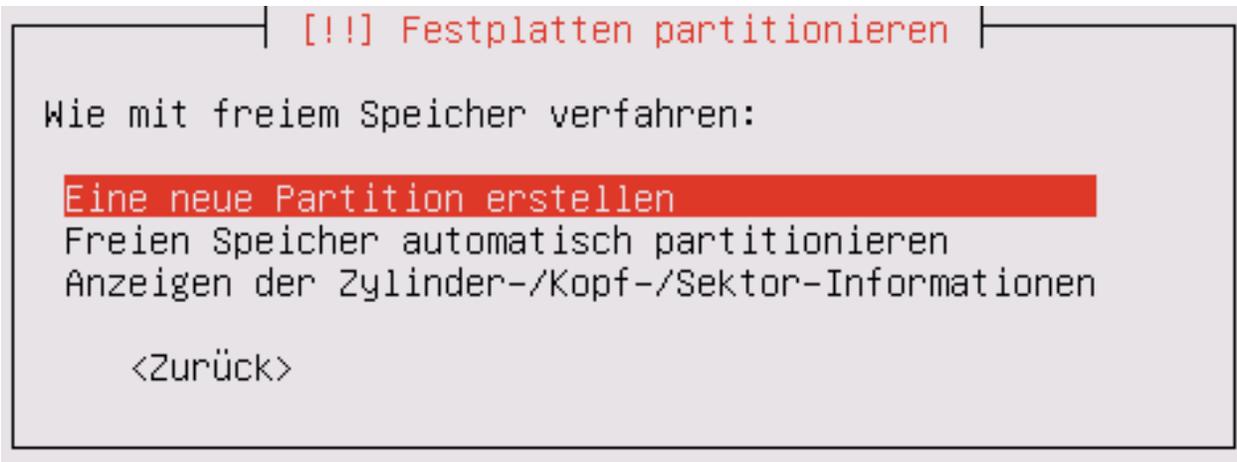
    Geführte Partitionierung
    Software-RAID konfigurieren
    Logical Volume Manager konfigurieren
    Verschlüsselte Datenträger konfigurieren
    Configure iSCSI volumes

    Virtuelle Festplatte 1 (vda) - 8.6 GB Virtio Block Device
    Nr. 1 primär 7.0 GB B f ext4 /
    pri/log 1.6 GB FREIER SPEICHER

    Änderungen an den Partitionen rückgängig machen
    Partitionierung beenden und Änderungen übernehmen

<Zurück>
```

Eine neue Partition erstellen



Größe bestätigen



Primär



Benutzen als 'Auslagerungsspeicher (SWAP)'

'Anlegen beenden'

```
| [!] Festplatten partitionieren |
Sie bearbeiten Partition 2 auf Virtuelle Festplatte 1 (vda). Auf dieser Partition wurde
kein vorhandenes Dateisystem gefunden.

Partitionseinstellungen:

Benutzen als: Auslagerungsspeicher (Swap)

Boot-Flag (Boot-fähig-Markierung): Aus

Daten von einer anderen Partition kopieren
Die Partition löschen
Anlegen der Partition beenden

<Zurück>
```

‘Partitionierung beenden’

```
| [!] Festplatten partitionieren |
Dies ist eine Übersicht über Ihre konfigurierten Partitionen und Einbindungspunkte.
Wählen Sie eine Partition, um Änderungen vorzunehmen (Dateisystem, Einbindungspunkt,
usw.), freien Speicher, um Partitionen anzulegen oder ein Gerät, um eine
Partitionstabelle zu erstellen.

Geführte Partitionierung
Software-RAID konfigurieren
Logical Volume Manager konfigurieren
Verschlüsselte Datenträger konfigurieren
Configure iSCSI volumes

Virtuelle Festplatte 1 (vda) - 8.6 GB Virtio Block Device
  Nr. 1 primär 7.0 GB B f ext4 /
  Nr. 2 primär 1.6 GB f Swap Swap

Änderungen an den Partitionen rückgängig machen
Partitionierung beenden und Änderungen übernehmen

<Zurück>
```

Ja schreiben, noch sind ja keine Daten vorhanden, die überschrieben werden könnten.

## [!] Festplatten partitionieren

Wenn Sie fortfahren, werden alle unten aufgeführten Änderungen auf die Festplatte(n) geschrieben. Andernfalls können Sie weitere Änderungen manuell durchführen.

Die Partitionstabellen folgender Geräte wurden geändert:  
Virtuelle Festplatte 1 (vda)

Die folgenden Partitionen werden formatiert:  
Partition 1 auf Virtuelle Festplatte 1 (vda) als ext4  
Partition 2 auf Virtuelle Festplatte 1 (vda) als Swap

Änderungen auf die Festplatten schreiben?

<Ja>

<Nein>

Warten...

Proxy leer lassen

## [!] Paketmanager konfigurieren

Falls Sie einen HTTP-Proxy benötigen, um das Internet zu erreichen, geben Sie hier bitte Ihre Daten an. Falls nicht, lassen Sie dieses Feld leer.

Die Proxy-Daten sollten im Standardformat »http://[[user]][:pass]@host[:port]/\*« angegeben werden.

HTTP-Proxy-Daten (leer lassen für keinen Proxy):

\_\_\_\_\_

<Zurück>

<Weiter>

Warten...

Automatische Sicherheitsaktualisierungen auswählen

## [!] Konfiguriere tasksel

Das regelmäßiges Einspielen von Aktualisierungen ist wichtig, um Ihr System sicher zu halten..

Standardmäßig müssen Aktualisierungen manuell mit Paketverwaltungswerkzeuge eingespielt werden. Alternativ können Sie festlegen, dass das System automatisch Sicherheitsaktualisierungen herunterlädt und einspielt, oder Sie können festlegen, dass dieses System als Teil eines Systems über das Internet mit dem Landscape-Dienst von Canonical verwaltet wird.

Wie möchten Sie Aktualisierungen auf diesem System verwalten?

Keine automatischen Aktualisierungen

**Sicherheitsaktualisierungen automatisch installieren**

System mit Landscape verwalten

OpenSSH server auswählen (Leertaste benutzen) und weiter



Warten...

Die Installation des GRUB Bootloader bestätigen



Weiter



### 5.3.2 SSH

Per SSH mit dem Server verbinden

```
ssh meinbenutzername@111.222.333.444
```

Den Public-Key für den User hinterlegen:

```
cd /home/meinbenutzername/
mkdir .ssh
nano .ssh/authorized_keys
```

Im Editor dann den Public Key (“ssh-rsa AAA...”) einfügen. Wichtig: Alles von diesem Key muss in eine Zeile. Weitere Adminuser können später angelegt werden.

Nun das Password-Login auf dem Server deaktivieren. Dazu die sshd\_config editieren:

```
sudo nano /etc/ssh/sshd_config
```

Die Zeile

```
#PasswordAuthentication yes
```

ändern in

```
PasswordAuthentication no
```

Achtung, auch wenn ‘yes’ auskommentiert ist, besteht die Möglichkeit sich per Password zu verbinden, erst wenn ‘no’ gesetzt ist und nicht (mehr) auskommentiert ist, ist der Zugriff nur noch per Key möglich.

Um es den Script-Kiddies und Bots etwas schwerer zu machen, sollte der Port 22 auf einen hohen Port (mindestens über 1024) verändert werden. Dazu die Zeile

```
Port 22
```

ändern in

```
Port 62954
```

**WICHTIG:** Diesen Port muss man sich dann merken, da man ihn später beim Aufruf von ssh angeben muss.

Nun den direkten Rootlogin sperren.

```
PermitRootLogin yes
```

ändern in

```
PermitRootLogin no
UsePAM no
```

Danach den Editor wieder verlassen und den SSH Server neu starten um die Einstellungen zu übernehmen.

```
sudo service ssh restart
```

Den nachfolgenden ssh Kommandos muss man die Option “-p 62954” (kleines “p”!) und den scp Kommandos die Option “-P 62954” (großes “P”!).

```
ssh -p 62954 meinbenutzername@111.222.333.444
```

### 5.3.3 Systemaktualisierung

Als Nächstes steht die Systemaktualisierung an; auch hier beim erstmaligen Aufruf die Nutzung von IPv4 erzwingen für's APT-Get

```
sudo apt-get update
sudo apt-get dist-upgrade
sudo apt-get autoremove
```

### 5.3.4 Pakete installieren

```
sudo apt-get install bird bird6 xinetd vnstat vnstati gdebi-core lighttpd git
↪conntrack
```

- bird übernimmt das BGP routing
- bird6 tut das selbe für IPv6
- vnstat monitort den Netzwerktraffic
- vnstati erzeugt daraus Grafiken
- lighttpd stellt diese zum Abruf bereit
- gdebi-core ermöglicht uns die Installation des Check\_mk Agents
- git wird für die Konfigurationsscripte benötigt
- xinetd ist der bei Debian übliche Super-Daemon, über ihn wird der Check\_mk Agent angesprochen
- conntrack überwacht den Auslastungszustand der NAT-Engine

### 5.3.5 Hinzufügen einer Schnittstelle eth1

Für die Verbindung zwischen den Supernodes und dem Konzentrator legen wir eine zweite Netzwerkschnittstelle an. Dazu muss im Proxmox für die VM eine eth1 hinzugefügt werden, die auf der vmbr1 hängt und virtio verwendet.

The screenshot shows the Proxmox Virtual Environment interface. The top bar indicates the user is logged in as 'root@pam'. The main content area shows the configuration for 'Virtual Machine 103 (xyzbackbone-1) on node 'node01''. The 'Hardware' tab is selected, and the 'Add' button is highlighted with a red box. A dropdown menu is open, showing the 'Network Device' option, which is also highlighted with a red box. The configuration table below shows the following details:

Component	Configuration
Hard Disk	Default
CD/DVD Drive	256MB/1.00GB
CD/DVD Drive (ide2)	2 (1 sockets, 2 cores) [host]
CD/DVD Drive (ide2)	local:iso/ubuntu-14.04.3-server-amd64.iso,media=cdrrom
Hard Disk (virtio0)	local:103/vm-103-disk-1.qcow2,format=qcow2,size=8G
Network Device (net0)	e1000=6E:9F:D3:A3:45:62,bridge=vmbr0,link_down=1

**Add: Network Device**

Bridged mode

Model: **VirtIO (paravirtualized)**

VLAN Tag: no VLAN

MAC address: auto

Bridge: **vibr1**

Rate limit (MB/s): unlimited

Firewall:

Multiqueues: [dropdown]

NAT mode

Disconnect:

Add

Danach die VM einmal durchbooten.

### 5.3.6 Eulenfunk BGP-Konzentrator-Konfigurator

**Ist leider noch Baustelle hier...** Bis auf weiteres geht es mit unten bei **ferm\_einrichten\_** weiter.

**Die genauen Hintergründe sollten verstanden werden und sind weiter unten beschrieben!**

Um die Konfiguration zu vereinfachen, wurde ein Script geschrieben, welches die nötigen Parameter abfragt und daraus die Konfigurationsdateien, bzw. Auszüge daraus erzeugt. Diese müssen dann nur noch an die richtige Stelle kopiert werden.

```
sudo mkdir -p /opt/eulenfunk/konzentrator
cd /opt/eulenfunk/konzentrator
sudo git clone https://github.com/eulenfunk/ff-bgp-konzentrator-konfigurator.git
cd ff-bgp-konzentrator-konfigurator
sudo ./bgp-konzentrator-setup.sh
```

Das Script fragt dann die nötigen Werte ab.

#### Beschreibung der abgefragten Werte

##### Allgemeine Parameter

**AS Nummer vom FF-RL** Hier wird die Nummer des autonomen Systems vom Freifunk Rheinland eingetragen. Aktuell ist das 201701.

**Eigene AS Nummer** Ihr benötigt ein eigenes autonomes System. Die Nummer davon gebt ihr hier an. TODO: Link auf Beschreibung zur Beschaffung eines eigenen AS...

**Zugewiesene FFRL-IPV4-Exit-Adresse** Vom Freifunk Rheinland bekommt ihr eine Exit-Adresse. Darauf wird der gesamte IPv4 Verkehr aller an diesem Konzentration angeschlossenen Supernodes bzw. der darüber verbundenen Clients ge-NAT-ed. Diese Adresse sieht in etwa so aus: 185.66.19X.YY

**Zugewiesenes FFRL-IPV6-Netz** Der IPv6 Prefix, der euch vom Freifunk Rheinland zugewiesen wurde. (2a03:2260:XXX::/48)

**Eigene öffentliche IPV4 Adresse** Bei der Einrichtung der VM für diesen Konzentration habt ihr eine IPv4-Adresse konfiguriert (Failover-IP der VM), über die ihr euch auch auf dem Konzentration eingeloggt habt. Also die IPv4-Adresse von *eth1*.

**Eigener SSH-Port** Ihr habt bei der Konfiguration vom *sshd* den Port angepasst (62954), also gebt ihr diesen hier ein. Damit wird sichergestellt, dass die Firewall (*ferm* ...) Verbindungen zu dem alternativen Port überhaupt zulässt. Wenn ihr euch hier vertut, kommt ihr nach dem Neustart nicht mehr per SSH auf euren Server!

### Konfiguration für GRE-Tunnel nach XXX\_Y

Ihr solltet vom Freifunk Rheinland Adressen für 4 Tunnel zum Backbone bekommen haben, jeweils zwei in Berlin und zwei in Düsseldorf. In diesem Abschnitt werden diese konfiguriert. Die folgenden Werte müsst ihr jeweils einmal pro Tunnel passend – also 4 Mal – eingeben:

**IPv4 Adresse für Tunnelendpunkt auf Backbone-Server** Die Tunnel-interne IPv4 Adresse auf dem **Backbone-Server** (100.64.X.YYY gerade).

**IPv4 Adresse für Tunnelendpunkt auf Konzentrator** Die Tunnel-interne IPv4 Adresse für den Tunnelendpunkt auf eurem **Konzentrator** (10.64.X.ZZZ nächste ungerade).

**IPv6 Adresse auf Backbone-Server** Zusätzlich zu den IPv4-Adressen habt ihr eine IPv6 Adresse für den Tunnel bekommen. Die Adresse mit der (...):1/64 hinten ist die Adresse auf dem Backbone-Server (in etwa diese 2a03:2260:Y:XXX::1 ohne die /64!). Diese gebt ihr hier an.

**IPv6 Adresse auf Konzentrator** Die auf die im vorherigen Schritt folgende Adresse, also mit (...):2/64 hinten, ist die Adresse auf eurem Konzentrator (in etwa diese 2a03:2260:Y:XXX::2 ohne die /64!). Diese gebt ihr hier an.

### Ausgaben

Das Script erzeugt folgende Dateien:

- bird.conf.bgp
- bird6.conf.bgp
- interfaces.bgp
- ferm.conf.bgp
- 20-ff-config.conf.bgp

Die erzeugten Dateien sollten nun **überprüft** werden (Beschreibung hierzu siehe unten) und dann an die passenden Stellen kopiert werden:

```
sudo cp bird.conf.bgp /etc/bird/bird.conf
sudo cp bird6.conf.bgp /etc/bird/bird6.conf
sudo mkdir /etc/ferm
sudo cp ferm.conf.bgp /etc/ferm/ferm.conf
sudo cp 20-ff-config.conf.bgp /etc/sysctl.d/20-ff-config.conf
sudo cat interfaces.bgp >> /etc/network/interfaces
```

Da nun ein eventueller alternativer SSH-Port in die *ferm.conf* eingetragen wurde, kann das Firewalling aktiviert werden.

Als erstes *ferm* installieren.

```
sudo apt-get install ferm
```

Bei der Frage, ob *ferm* beim Systemstart gestartet werden soll, mit ja antworten.

Danach kann das System rebootet werden. Die Konfigurationen für die Supernodes werden später wie unten beschrieben angelegt.

## Routing

Zum Routing werden Regeln benötigt, die die Pakete aus dem Freifunk Netz und die Pakete vom FFRL Backbone in eine gesonderte Tabelle (Tabelle 42) leiten. In dieser Tabelle wird vom bird per BGP eine Defaultroute ins Backbone gesetzt und manuell Routen zum eigenen Freifunk Netz (zu den Supernodes).

Um eine Menge Handarbeit zu sparen wird das Anlegen der Rules für die einzelnen Communities/Supernodes per Script erledigt:

```
cd /opt/eulenkfunk/konzentrator
sudo git clone https://github.com/eulenkfunk/konzentrator.git
cd konzentrator
sudo chmod +x *.sh
sudo mkdir config
```

Damit das Script auch beim boot seine Arbeit verrichten kann muss es in die rc.local eingetragen werden.

```
sudo nano /etc/rc.local
```

```
#!/bin/sh -e
# rc.local
/opt/eulenkfunk/konzentrator/konzentrator/bgp-konzentrator-rc.sh
exit 0
```

Im Ordner **config** wird je Supernode ein config file angelegt. Die Beschreibung zum Hinzufügen von Supernodes erfolgt im Dokument "Supernode einrichten".

### 5.3.7 Monitoring

Das Monitoring beinhaltet folgende Komponenten:

- Check\_MK ermöglicht das zentrale Monitoring aller Systemdaten aller eingebundenen Server
- vnstat erstellt Traffic Statistiken, die sich auf der shell anzeigen lassen
- vnstati generiert daraus Grafiken
- lighttpd stellt diese zum Abruf aus dem Internet bereit

#### Check\_MK Agent installieren

Den Check\_MK Agent steht in der Weboberfläche des Check\_MK als .deb Paket bereit:

In die CheckMK-Instanz per Webbrowser einloggen. Dann suchen:

```
-> WATO Configuration (Menü/Box)
-> Monitoring Agents
-> Packet Agents
-> check-mk-agent_1.2.8p11-1_all.deb _(Beispiel)_
```

Den Download-Link in die Zwischenablage kopieren. Im SSH-Terminal nun eingeben: (die Download-URL ist individuell und der Name des .deb-Paketes ändert sich ggf.)

```
wget https://monitoring.eulenkfunk.de/eulenkfunk/check_mk/agents/check-mk-agent_1.2.
↪8p11-1_all.deb
```

Um das .deb Paket zu installieren wird gdebi empfohlen, ausserdem benötigt der Agent xinetd zum Ausliefern der Monitoring Daten.

Per SSH auf dem Server. (Auch hier: Name des .deb-Files ggf. anpassen)

```
sudo gdebi check-mk-agent_1.2.8p1-1_all.deb
```

Anschließend noch das Konzentrador-Plugin hinzufügen:

```
cd /usr/lib/check_mk_agent/local
sudo wget -O konzentrator https://raw.githubusercontent.com/eulenkfunk/check_mk/master/
↳konzentrator
sudo chmod 755 konzentrator
sudo chmod +x konzentrator
```

```
:: sudo nano /etc/xinetd.d/check_mk
```

Dort die Zeile

```
# only_from = 127.0.0.1 10.0.20.1 10.0.20.2
```

ändern in

```
only_from = 127.0.0.1 94.23.160.148
```

Damit diese Änderungen aktiviert werden, muss der xinetd durchgestartet werden

```
sudo /etc/init.d/xinetd restart
```

Der Rechner hält ab nun Daten zum Abruf bereit.

JJX Bescheid sagen, der kümmert sich dann darum.

### vnstat einrichten

Alle 5 Minuten werden die Grafiken der Durchsatzdaten aktualisiert:

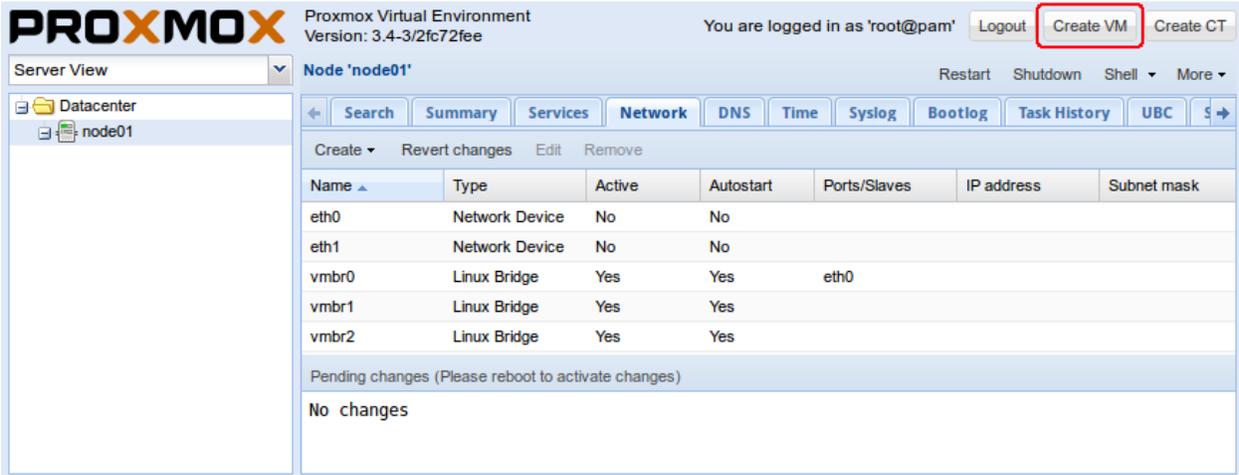
```
sudo mkdir -p /var/www/vnstats/eth0
sudo mkdir -p /var/www/vnstats/eth1
sudo nano /etc/cron.d/vnstat
```

```
*/5 * * * * root vnstati -i eth0 -o /var/www/vnstats/eth0/hours.png -h
*/5 * * * * root vnstati -i eth0 -o /var/www/vnstats/eth0/days.png -d
*/5 * * * * root vnstati -i eth0 -o /var/www/vnstats/eth0/months.png -m
*/5 * * * * root vnstati -i eth0 -o /var/www/vnstats/eth0/summary.png -s
*/5 * * * * root vnstati -i eth1 -o /var/www/vnstats/eth1/hours.png -h
*/5 * * * * root vnstati -i eth1 -o /var/www/vnstats/eth1/days.png -d
*/5 * * * * root vnstati -i eth1 -o /var/www/vnstats/eth1/months.png -m
*/5 * * * * root vnstati -i eth1 -o /var/www/vnstats/eth1/summary.png -s
```

## 5.4 Supernode einrichten

Der Supernode ist der Freifunkseiteige unserer zwei Server. Er übernimmt die Adressvergabe per DHCP / Radvd, den Aufbau der Fastd Tunnel zu den Routern und Batman.

Der Supernode wird im Proxmox Webinterface angelegt indem man auf der linken Seite den Server auswählt und dann oben rechts auf 'Create VM' klickt.



Proxmox Virtual Environment  
Version: 3.4-3/2fc72fee

You are logged in as 'root@pam' Logout **Create VM** Create CT

Server View **Node 'node01'** Restart Shutdown Shell More

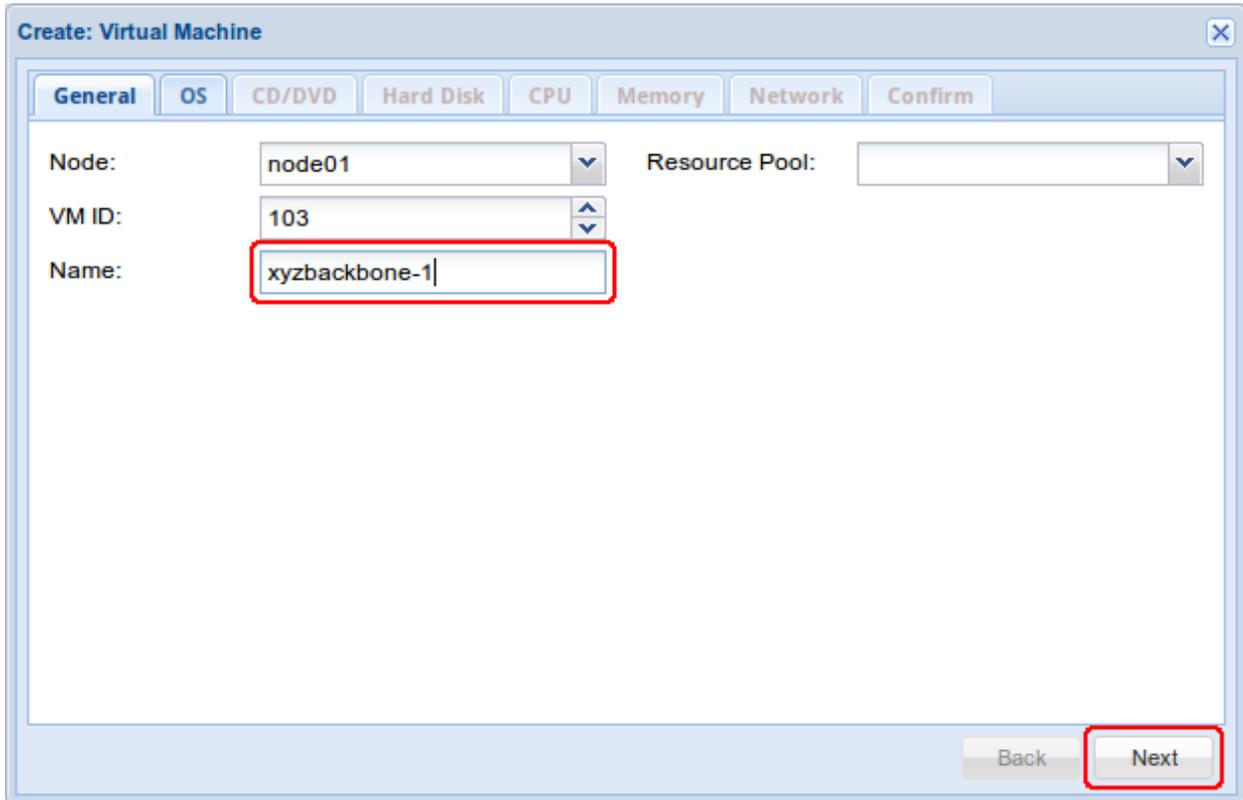
Search Summary Services **Network** DNS Time Syslog Bootlog Task History UBC

Create Revert changes Edit Remove

Name	Type	Active	Autostart	Ports/Slaves	IP address	Subnet mask
eth0	Network Device	No	No			
eth1	Network Device	No	No			
vibr0	Linux Bridge	Yes	Yes	eth0		
vibr1	Linux Bridge	Yes	Yes			
vibr2	Linux Bridge	Yes	Yes			

Pending changes (Please reboot to activate changes)  
No changes

Im Reiter 'General' eine Freie ID und einen Namen (meinstadt-1) festlegen.



Create: Virtual Machine

General OS CD/DVD Hard Disk CPU Memory Network Confirm

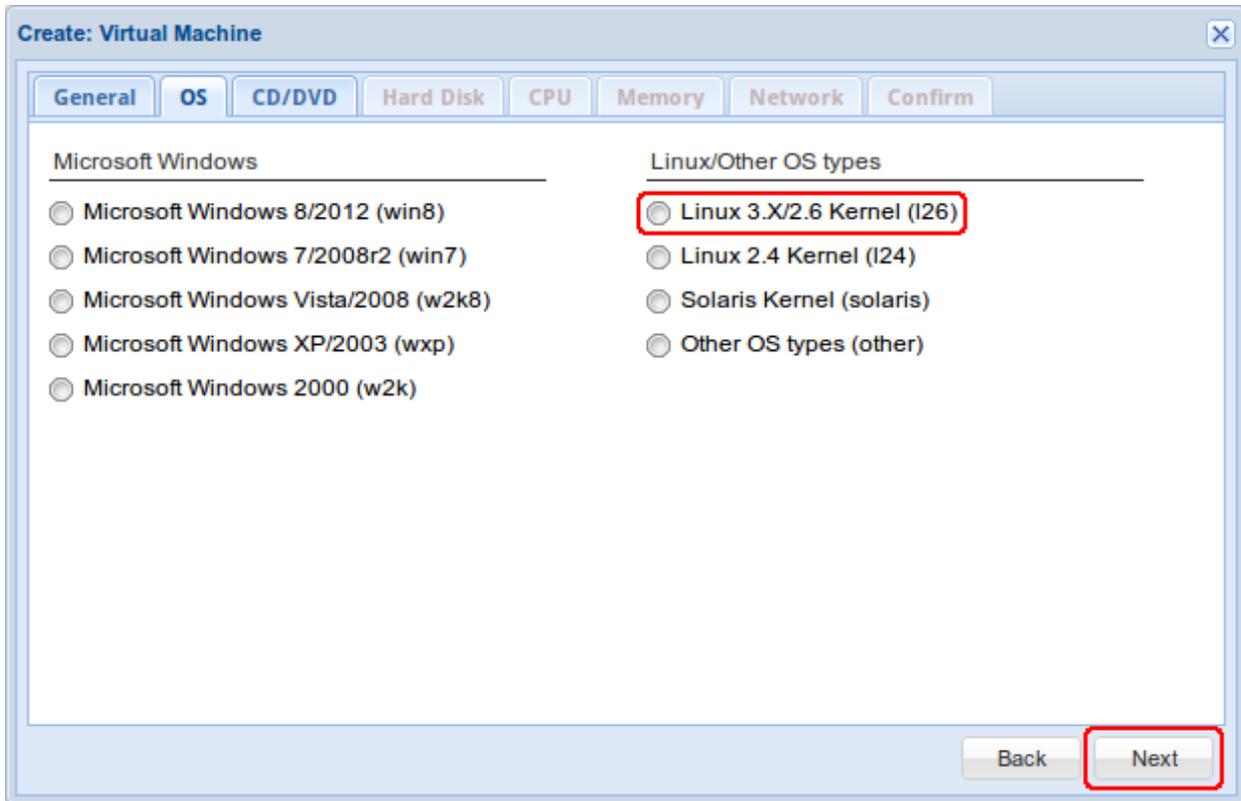
Node: node01 Resource Pool:

VM ID: 103

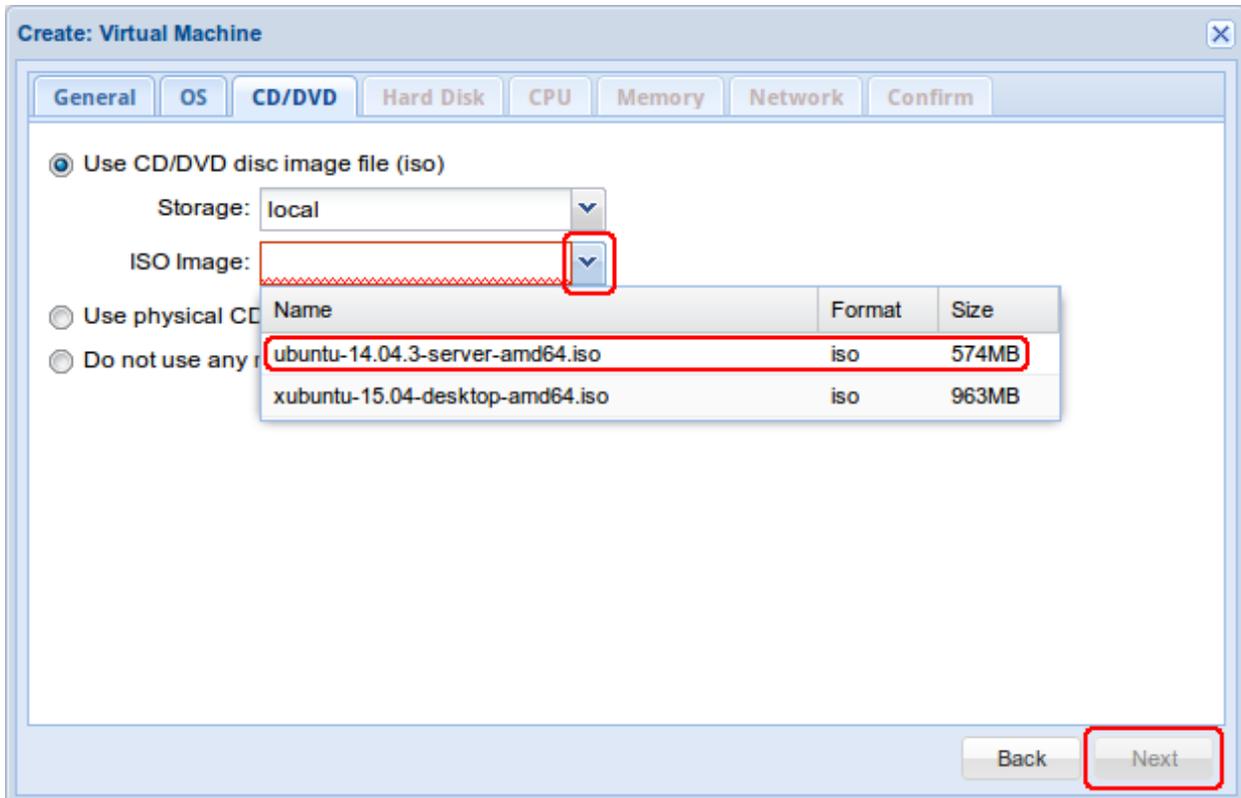
Name: xyzbackbone-1

Back Next

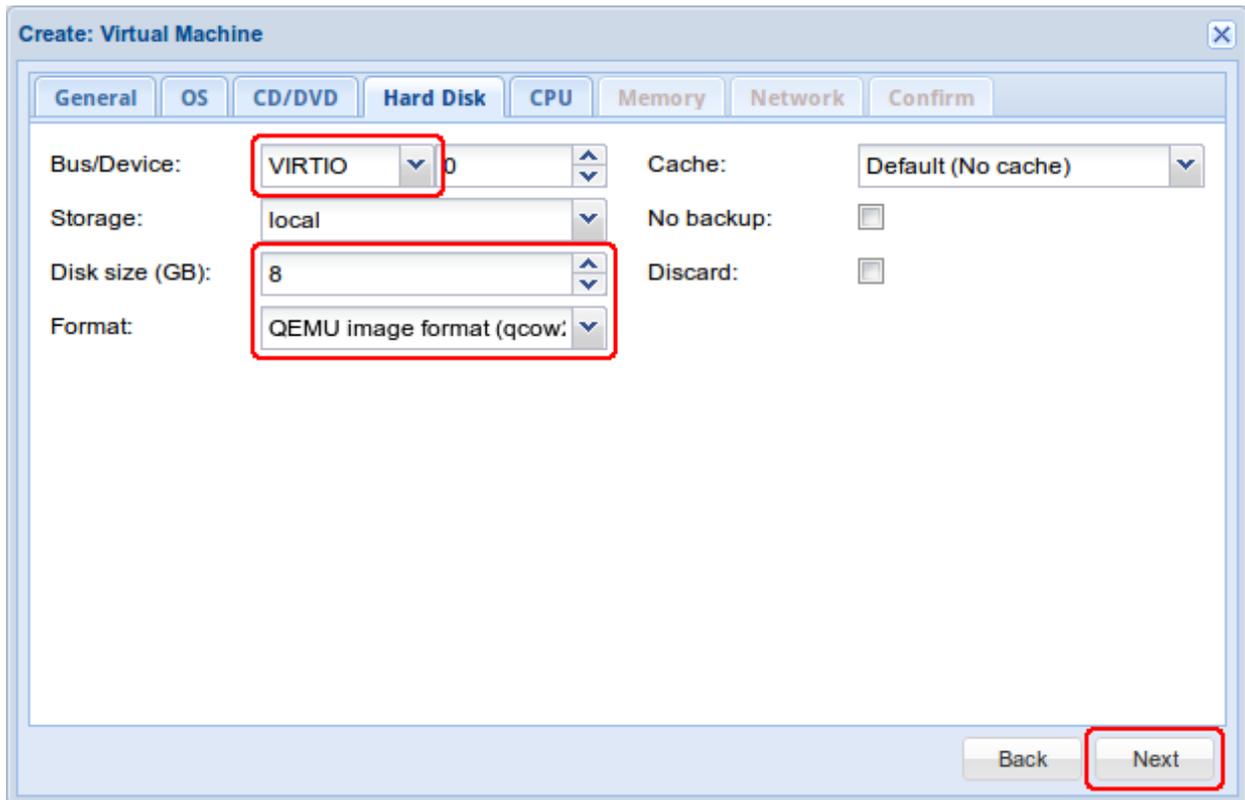
Im Reiter 'OS' 'Linux 4.x/3.x/2.6 Kernel auswählen.



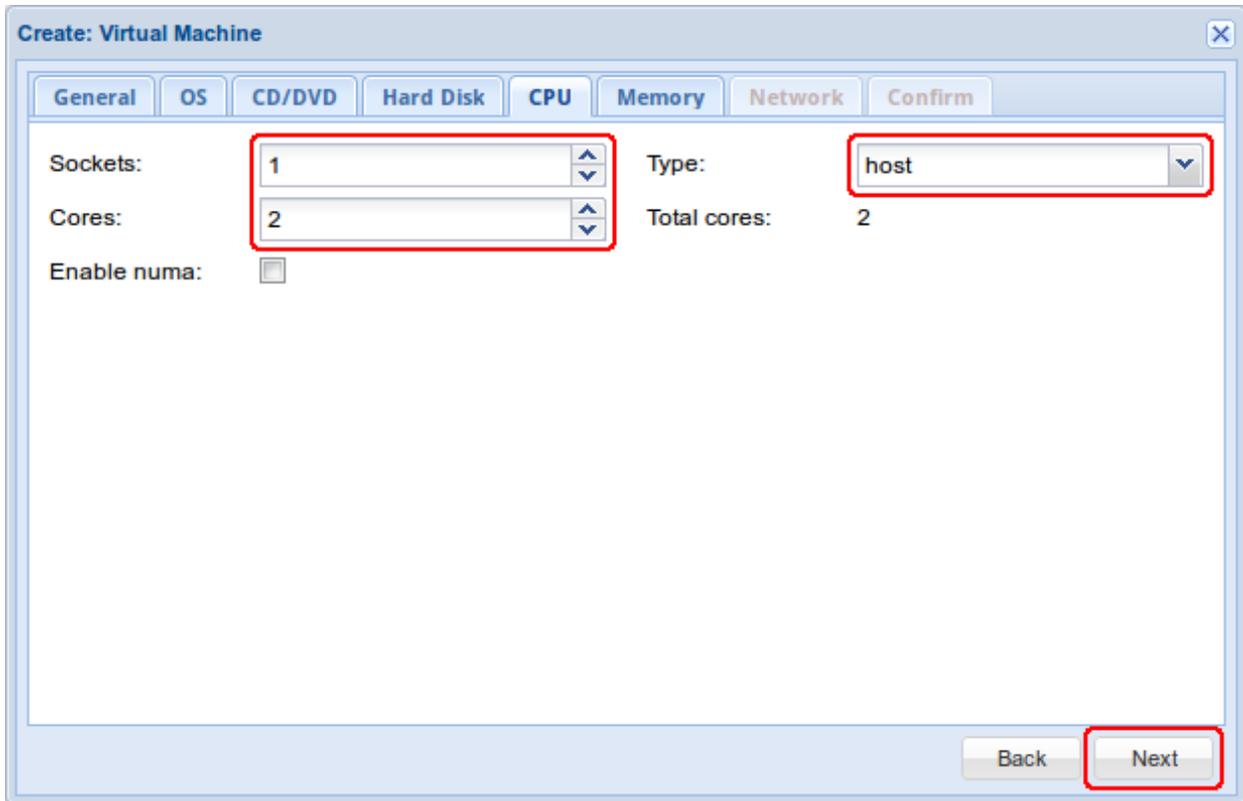
Im Reiter 'CD/DVD' das ISO Image auswählen.



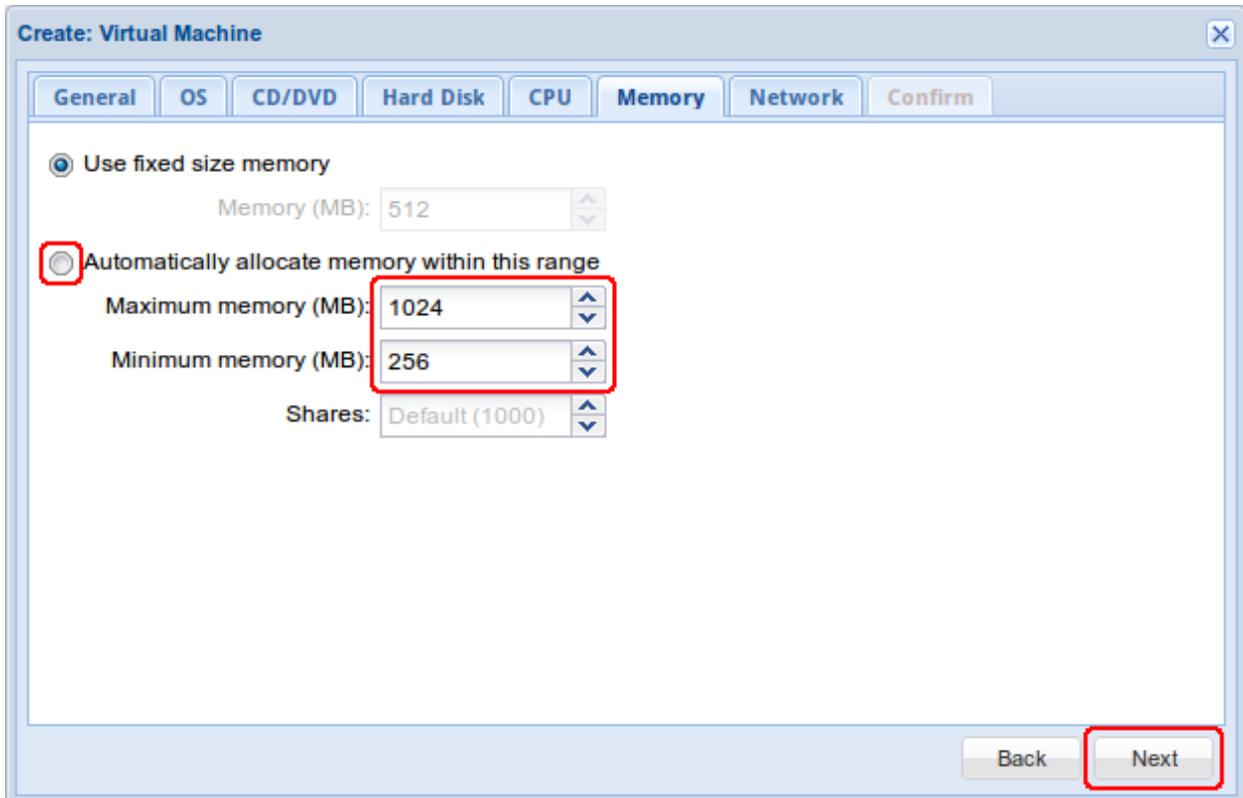
Im Reiter 'Hard Disk' als 'Bus' 'VirtIO' einstellen, die Festplattengröße auf 6GB begrenzen und als Format 'qcow2' wählen.



Im Reiter 'CPU' einen Prozessorkern zuweisen. Type "host" (mehr Performance, weniger Portabilität).



Im Reiter 'Memory' unter 'Automatically allocate memory within this range' 256-2048MB festlegen.



Im Reiter 'Network' als Netzwerkkarte 'VirtIO' auswählen und die MAC Adresse der für diese VM zu verwendenden öffentlichen IPv4 Adresse eintragen. Bridged Mode übernehmen wir so und vmbr0 auch diese.

The screenshot shows the 'Create: Virtual Machine' dialog box with the 'Network' tab selected. The 'Bridged mode' radio button is selected. The 'Model' dropdown is set to 'Intel E1000'. The 'MAC address' field is set to 'auto'. The 'Bridge' dropdown is set to 'vmbr0'. The 'Next' button is highlighted.

Option	Value
Mode	Bridged mode
Model	Intel E1000
MAC address	auto
Bridge	vmbr0
Rate limit (MB/s)	unlimited
Disconnect	<input type="checkbox"/>

Bestätigen und Anlegen, auswählen und anschließend starten.

Create: Virtual Machine

General OS CD/DVD Hard Disk CPU Memory Network Confirm

Settings

Key ▲	Value
balloon	256
cores	2
cpu	host
ide2	local:iso/ubuntu-14.04.3-server-amd64.iso,media=cdrom
memory	1024
name	xyzbackbone-1
net0	e1000,bridge=vibr0
nodename	node01
numa	0
ostype	l26
sockets	1

Back Finish

PROXMOX Proxmox Virtual Environment  
Version: 3.4-3/2fc72fee

You are logged in as 'root@pam' Logout Create VM Create CT

Server View Virtual Machine 103 ('xyzbackbone-1') on node 'node01' Start Shutdown Stop Reset Remove Migrate Console

Summary Hardware Options Task History Monitor Backup Snapshots Firewall Permissions

Edit Revert

Name	xyzbackbone-1
Start at boot	No
Start/Shutdown order	order=any
OS Type	Linux 3.X/2.6 Kernel (l26)
Boot order	Disk 'virtio0', CD-ROM, Network
Use tablet for pointer	Yes
Hotplug	Disk, Network, USB
ACPI support	Yes
SCSI Controller Type	Default (LSI 53C895A)
KVM hardware virtualization	Yes

Fehlermeldungen während der Startphase werden unten im Log-Fenster angezeigt, erscheinen immer “oben”, jedoch mit einigen Sekunden Verzögerung. Details lassen sich ausklappen.

Hinweis: Wenn das System später läuft, nicht vergessen, den Starttyp “at boot time” zu stellen und das CD-ROM-Laufwerk entfernen.

Proxmox Virtual Environment  
Version: 3.4-3/2fc72fee

You are logged in as 'root@pam' Logout Create VM Create CT

Server View Virtual Machine 103 ('xyzbackbone-1') on node 'node01' Start Shutdown Stop Reset Remove Migrate Console

Summary Hardware **Options** Task History Monitor Backup Snapshots Firewall Permissions

Edit Revert

Name	xyzbackbone-1
Start at boot	No
Start/Shutdown order	order=any
OS Type	Linux 3.X/2.6 Kernel (I26)
Boot order	Disk 'virtio0', CD-ROM, Network
Use tablet for pointer	Yes
Hotplug	Disk, Network, USB
ACPI support	Yes
SCSI Controller Type	Default (LSI 53C895A)
KVM hardware virtualization	Yes

## 5.4.1 Ubuntu Server Installieren

Die VM links auswählen und oben rechts starten und die Konsole öffnen

Proxmox Virtual Environment  
Version: 3.4-3/2fc72fee

You are logged in as 'root@pam' Logout Create VM Create CT

Server View Virtual Machine 103 ('xyzbackbone-1') on node 'node01' **Start** Shutdown Stop Reset Remove Migrate **Console**

Summary Hardware **Options** Task History Monitor Backup Snapshots Firewall Permissions

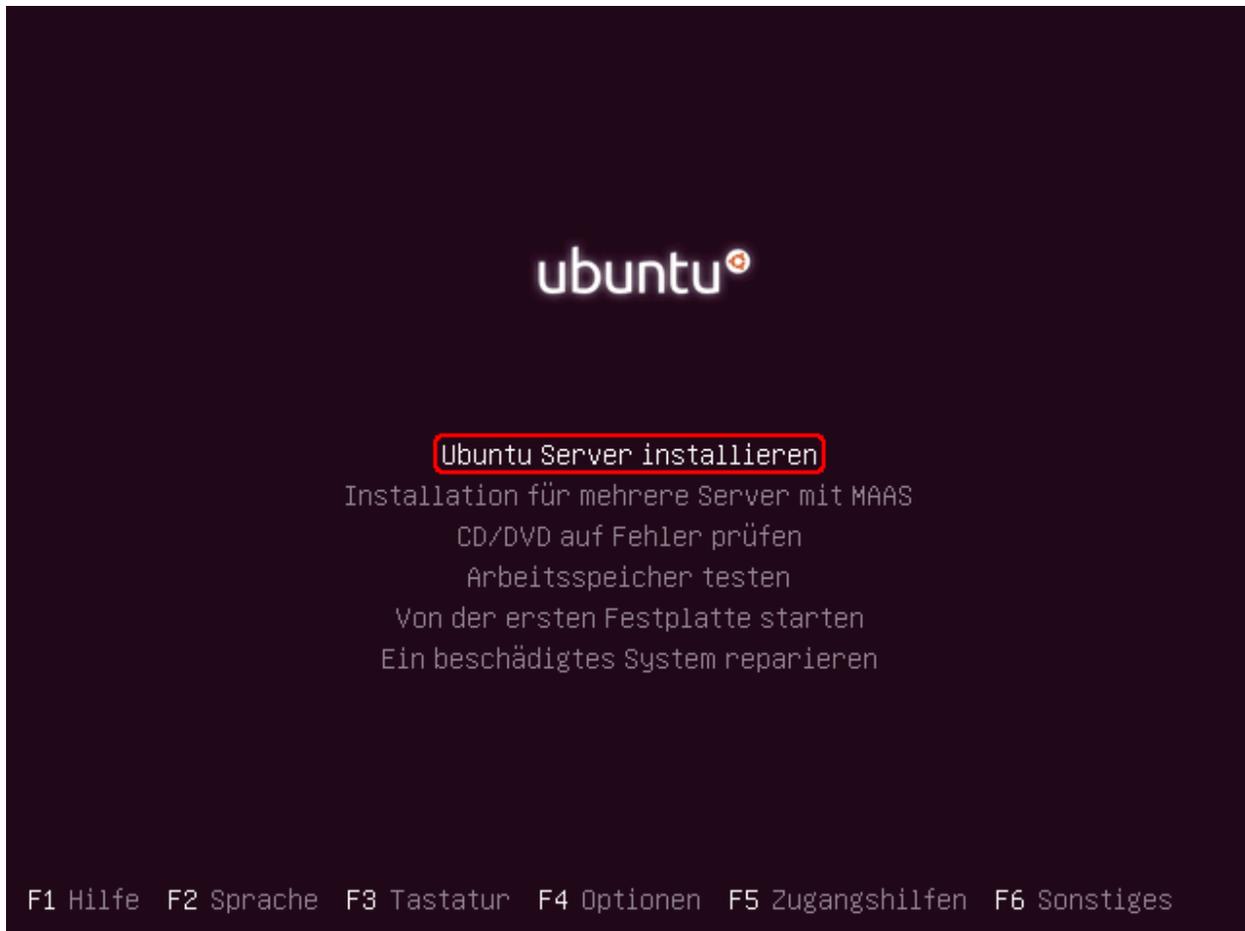
Edit Revert

Name	xyzbackbone-1
Start at boot	No
Start/Shutdown order	order=any
OS Type	Linux 3.X/2.6 Kernel (I26)
Boot order	Disk 'virtio0', CD-ROM, Network
Use tablet for pointer	Yes
Hotplug	Disk, Network, USB
ACPI support	Yes
SCSI Controller Type	Default (LSI 53C895A)
KVM hardware virtualization	Yes

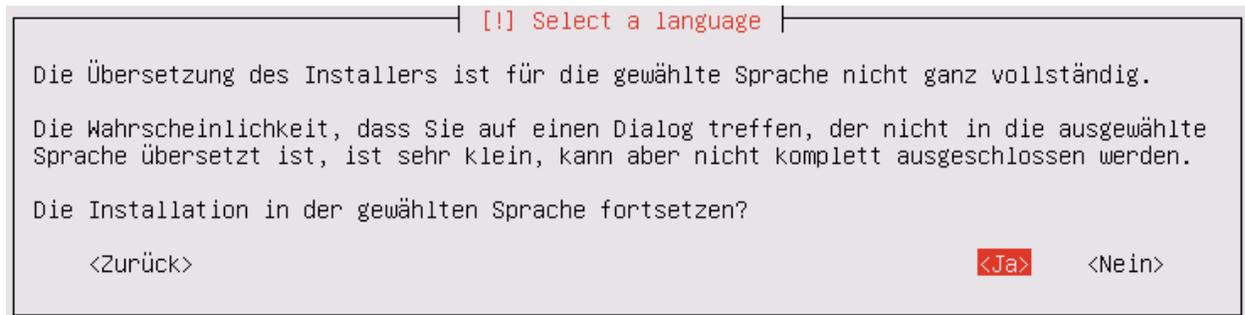
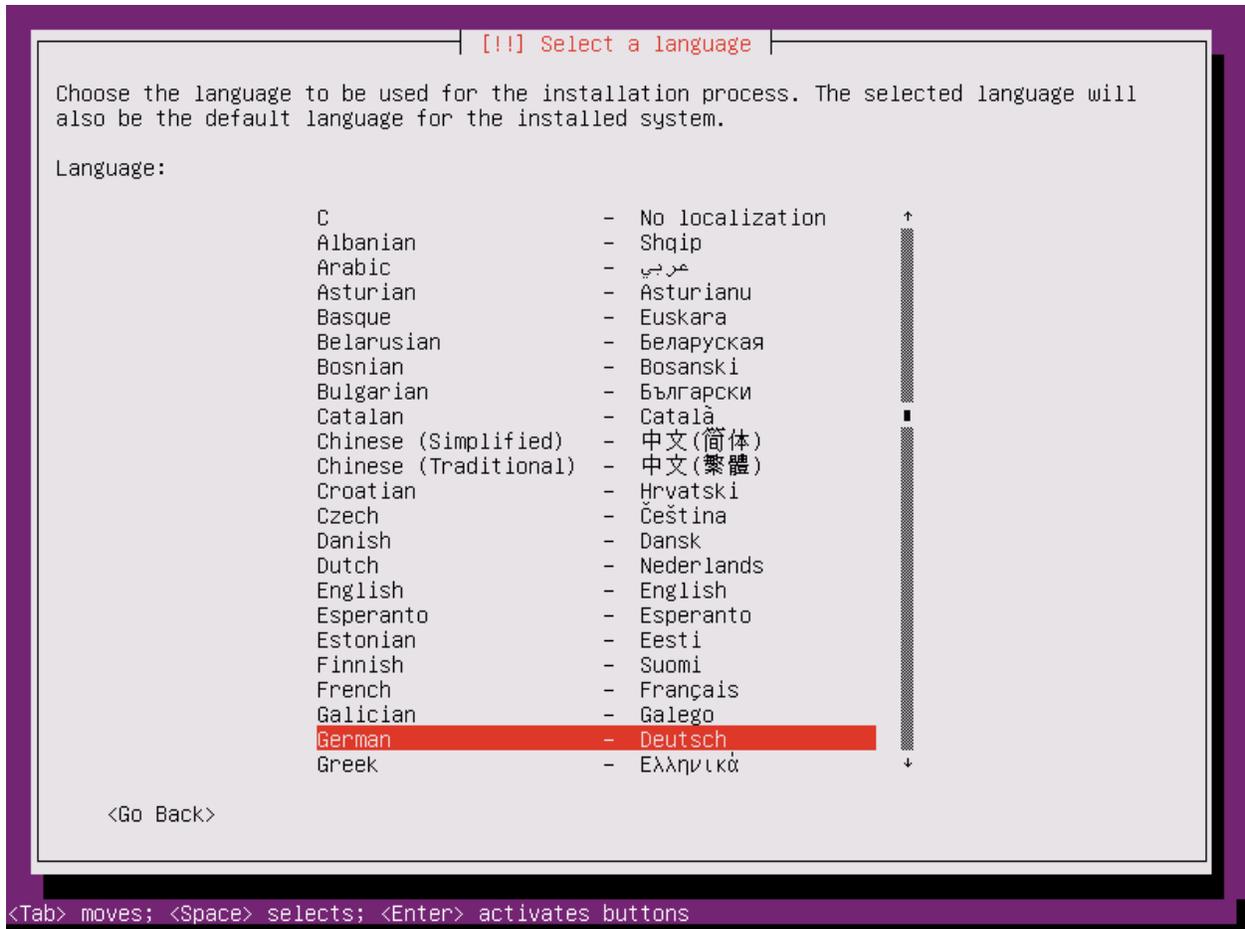
Deutsch als Sprache auswählen und nun Ubuntu Server installieren

Language			
Amharic	Français	Македонски	Tamil
Arabic	Gaeilge	Malayalam	தமிழ்
Asturiano	Galego	Marathi	Thai
Беларуская	Gujarati	Burmese	Tagalog
Български	𐌆𐌗𐌊𐌛	Nepali	Türkçe
Bengali	Hindi	Nederlands	Uyghur
Tibetan	Hrvatski	Norsk bokmål	Українська
Bosanski	Magyar	Norsk nynorsk	Tiếng Việt
Català	Bahasa Indonesia	Punjabi (Gurmukhi)	中文(简体)
Čeština	Íslenska	Polski	中文(繁體)
Dansk	Italiano	Português do Brasil	
<b>Deutsch</b>	日本語	Português	
Dzongkha	தமிழ்	Română	
Ελληνικά	Қазақ	Русский	
English	Khmer	Sámegillii	
Esperanto	ಕನ್ನಡ	සිංහල	
Español	한국어	Slovenčina	
Eesti	Kurdî	Slovenščina	
Euskara	Lao	Shqip	
عَرَبِيَّة	Lietuviškai	Српски	
Suomi	Latviski	Svenska	

F1 Help F2 Language F3 Keymap F4 Modes F5 Accessibility F6 Other Options



Als Installationssprache jetzt nochmal Deutsch auswählen, die Auswahl trotz unvollständiger Unterstützung bestätigen und als nächstes das Tastaturlayout auswählen.



## [!] Auswählen des Standorts

Der hier ausgewählte Standort wird verwendet, um die Zeitzone zu setzen und auch, um zum Beispiel das System-Gebietsschema (locale) zu bestimmen. Normalerweise sollte dies das Land sein, in dem Sie leben.

Diese Liste enthält nur eine kleine Auswahl von Standorten, basierend auf der Sprache, die Sie ausgewählt haben. Wählen Sie »weitere«, falls Ihr Standort nicht aufgeführt ist.

Land oder Gebiet:

Belgien  
Deutschland  
Liechtenstein  
Luxemburg  
Österreich  
Schweiz  
weitere

<Zurück>

## [!] Tastatur konfigurieren

Sie können versuchen das Tastaturmodell anhand von Tasteneingaben erkennen zu lassen. Wenn Sie das nicht möchten, können sie das Tastaturmodell aus einer Liste wählen.

Tastaturmodell erkennen?

<Zurück>

<Ja>

<Nein>

[!] Tastatur konfigurieren

Die Belegung von Tastaturen unterscheidet sich abhängig vom Land, wobei für einige Länder sogar mehrere gängige Belegungen existieren. Bitte wählen Sie das Land, zu dem die Tastaturbelegung gehört.

Herkunftsland für die Tastatur:

- Afghani
- Albanisch
- Amharisch
- Arabisch
- Arabisch (Marokko)
- Arabisch (Syrien)
- Armenisch
- Aserbaidschanisch
- Bambara
- Bangla
- Belgisch
- Bosnisch
- Braille
- Bulgarisch
- Burmesisch
- Chinesisch
- Deutsch**
- Deutsch (Österreich)
- Dhivehi
- Dzongkha
- Dänisch
- Englisch (Britisch)

↑  
↓

<Zurück>

[!] Tastatur konfigurieren

Bitte wählen Sie eine Tastaturbelegung, die zur Tastatur dieses Rechners passt.

Tastaturbelegung:

- Deutsch**
- Deutsch - Deutsch (Dvorak)
- Deutsch - Deutsch (Macintosh)
- Deutsch - Deutsch (Macintosh, ohne Akzenttasten)
- Deutsch - Deutsch (Neo 2)
- Deutsch - Deutsch (Nur Acute-(')Akzentzeichen)
- Deutsch - Deutsch (Nur Grave-(`) und Acute-(')Akzentzeichen)
- Deutsch - Deutsch (Sun-Akzenttasten)
- Deutsch - Deutsch (T3)
- Deutsch - Deutsch (ohne Akzenttasten)
- Deutsch - Deutsch (qwerty)
- Deutsch - Deutsch (veraltet)
- Deutsch - Niedersorbisch
- Deutsch - Niedersorbisch (qwertz)
- Deutsch - Rumänisch (Deutschland)
- Deutsch - Rumänisch (Deutschland, ohne Akzenttasten)
- Deutsch - Russisch (Deutschland, phonetisch)

<Zurück>

Sobald der Server versucht das Netzwerk automatisch zu konfigurieren, dies abbrechen und die manuelle Netz-

erkonfiguration auswählen.

| Konfigurieren des Netzwerks mit DHCP |

43%

Dies kann einige Zeit dauern.

<Abbrechen>

| [!] Netzwerk einrichten |

Die automatische Netzwerkkonfiguration ist fehlgeschlagen

Ihr Netzwerk benutzt möglicherweise nicht das DHCP-Protokoll. Des Weiteren könnte der DHCP-Server sehr langsam sein oder die Netzwerk-Hardware arbeitet nicht korrekt.

<Weiter>

| [!] Netzwerk einrichten |

Hier können Sie wählen, die automatische DHCP-Netzwerkkonfiguration erneut zu versuchen (was funktionieren könnte, wenn Ihr DHCP-Server sehr langsam reagiert) oder das Netzwerk manuell zu konfigurieren. Manche DHCP-Server erfordern, dass der Client einen speziellen DHCP-Rechnernamen sendet, daher können Sie auch wählen, die automatische DHCP-Netzwerkkonfiguration mit Angabe eines Rechnernamens erneut zu versuchen.

Netzwerk-Konfigurationsmethode:

- Autom. Konfiguration erneut versuchen
- Autom. Konfiguration erneut versuchen mit einem DHCP-Rechnernamen
- Netzwerk manuell einrichten
- Netzwerk unkonfiguriert belassen

<Zurück>

Die IP zur mac ist beispielsweise die 555.666.777.888

| [!] Netzwerk einrichten |

Die IP-Adresse ist für Ihren Rechner eindeutig und kann zwei verschiedene Formate haben:

- \* vier Zahlen, getrennt durch Punkte (IPv4);
- \* Blöcke von hexadezimalen Zeichen, getrennt durch Doppelpunkte (IPv6).

Sie können auch optional eine CIDR-Netzmaske (wie z.B. »/24«) anfügen.

Wenn Sie nicht wissen, was Sie eingeben sollen, fragen Sie Ihren Netzwerk-Administrator.

IP-Adresse:

555.666.777.888

<Zurück> <Weiter>

Die Subnetzmaske von 255.255.255.0 bleibt in der Regel so

[!] Netzwerk einrichten

Durch die Netzmaske kann bestimmt werden, welche Rechner im lokalen Netzwerk direkt angesprochen werden können. Wenn Sie diesen Wert nicht kennen, fragen Sie Ihren Netzwerkadministrator. Die Netzmaske besteht aus vier durch Punkte getrennte Zahlen.

Netzmaske:

255.255.255.0

<Zurück>

<Weiter>

Die Gateway Adresse sollte man beim Rechenzentrum bekannt sein.

Bei einem großen Französischen RZ ist das IPv4 Gateway immer auf der 254, also 555.666.777.254

[!] Netzwerk einrichten

Geben Sie hier die IP-Adresse (vier durch Punkte getrennte Zahlen) des Gateways ein, auch als Default-Router bekannt. Alle Daten zu Rechnern außerhalb Ihres LAN (zum Beispiel zum Internet) werden über diesen Router gesendet. In seltenen Fällen haben Sie keinen Router, in diesem Fall geben Sie hier einfach nichts ein. Wenn Sie die richtige Antwort hier nicht kennen, fragen Sie Ihren Netzwerkadministrator.

Gateway:

555.666.777.254

<Zurück>

<Weiter>

Als DNS geht z.B. der 8.8.8.8 von google.

[!] Netzwerk einrichten

Nameserver (DNS-Server) werden benutzt, um Rechnernamen im Internet aufzulösen. Bitte geben Sie die IP-Adressen (nicht die Rechnernamen) von bis zu drei Nameservern getrennt durch Leerzeichen an. Benutzen Sie keine Kommata. Der erste Server in der Liste wird als erstes abgefragt. Wenn Sie keine Nameserver benutzen möchten, lassen Sie dieses Feld bitte einfach leer.

Adresse des DNS-Servers:

8.8.8.8

<Zurück>

<Weiter>

Der Rechnername ist frei wählbar z.b. meinestadt-1

[!] Netzwerk einrichten

Bitte geben Sie den Namen dieses Rechners ein.

Der Rechnername ist ein einzelnes Wort, das Ihren Rechner im Netzwerk identifiziert. Wenn Sie Ihren Rechnernamen nicht kennen, fragen Sie den Netzwerkadministrator. Wenn Sie ein lokales Heimnetz aufbauen, ist es egal, was Sie angeben.

Rechnername:

Max

<Zurück>

<Weiter>

Der Domainname ist hier einzutragen

[!] Netzwerk einrichten

Der Domain-Name ist der rechte Teil Ihrer Internetadresse nach Ihrem Rechnernamen. Er endet oft mit .de, .com, .net oder .org. Wenn Sie ein lokales Heimnetz aufbauen, ist es egal, was Sie angeben. Diese Information sollte dann aber auf allen Rechnern gleich sein.

Domain-Name:

trollfunk.de

<Zurück>

<Weiter>

Und der Benutzername.

[!!] Benutzer und Passwörter einrichten

Für Sie wird ein Konto angelegt, das Sie statt dem root-Konto für die alltägliche Arbeit verwenden können.

Bitte geben Sie den vollständigen Namen des Benutzers an. Diese Information wird z.B. im Absender von E-Mails, die er verschickt, oder in Programmen, die den Namen des Benutzers anzeigen, verwendet. Ihr kompletter Name wäre sinnvoll.

Vollständiger Name des neuen Benutzers:

Max

<Zurück>

<Weiter>

[!!] Benutzer und Passwörter einrichten

Wählen Sie einen Benutzernamen für das neue Benutzerkonto. Der Vorname ist meist eine gute Wahl. Der Benutzername sollte mit einem kleinen Buchstaben beginnen, gefolgt von weiteren kleinen Buchstaben oder auch Zahlen.

Benutzername für Ihr Konto:

max

<Zurück>

<Weiter>

Das Kennwort sollte sicher sein und nicht bereits für einen anderen Zweck in Verwendung.

[!] Benutzer und Passwörter einrichten

Ein gutes Passwort enthält eine Mischung aus Buchstaben, Zahlen und Sonderzeichen und wird in regelmäßigen Abständen geändert.

Wählen Sie ein Passwort für den neuen Benutzer:

\*\*\*\*\*

<Zurück> <Weiter>

Da auf dem Server keine Persönlichen Dateien gespeichert werden sollen ist es nicht notwendig den persönlichen Ordner zu verschlüsseln.

[!] Benutzer und Passwörter einrichten

Sie können Ihren persönlichen Ordner verschlüsseln, sodass alle darin gespeicherten Dateien privat bleiben, selbst wenn Ihr Rechner gestohlen wird.

Das System wird Ihren verschlüsselten Ordner bei jedem Anmelden nahtlos einbinden und diesen automatisch aushängen, sobald Sie sich aus allen aktiven Sitzungen abmelden.

Ihren persönlichen Ordner verschlüsseln?

<Zurück> <Ja> **<Nein>**

Zeitzone prüfen und bestätigen.

Festplatte manuell formatieren

[!] Festplatten partitionieren

Der Installer kann Sie durch die Partitionierung einer Festplatte (mit verschiedenen Standardschemata) führen. Wenn Sie möchten, können Sie dies auch von Hand tun. Bei Auswahl der geführten Partitionierung können Sie die Einteilung später noch einsehen und anpassen.

Falls Sie eine geführte Partitionierung für eine vollständige Platte wählen, werden Sie gleich danach gefragt, welche Platte verwendet werden soll.

Partitionierungsmethode:

- Geführt - vollständige Festplatte verwenden
- Geführt - gesamte Platte verwenden und LVM einrichten
- Geführt - gesamte Platte mit verschlüsseltem LVM
- Manuell**

<Zurück>

Freien Speicherplatz auswählen und Enter

[!] Festplatten partitionieren

Dies ist eine Übersicht über Ihre konfigurierten Partitionen und Einbindungspunkte. Wählen Sie eine Partition, um Änderungen vorzunehmen (Dateisystem, Einbindungspunkt, usw.), freien Speicher, um Partitionen anzulegen oder ein Gerät, um eine Partitionstabelle zu erstellen.

Geführte Partitionierung  
Configure iSCSI volumes

Virtuelle Festplatte 1 (vda) - 8.6 GB Virtio Block Device

Änderungen an den Partitionen rückgängig machen  
Partitionierung beenden und Änderungen übernehmen

<Zurück>

#### Partitionstabelle erstellen

[!] Festplatten partitionieren

Sie haben ein komplettes Laufwerk zur Partitionierung angegeben. Wenn Sie fortfahren und eine neue Partitionstabelle anlegen, werden alle darauf vorhandenen Partitionen gelöscht. Beachten Sie, dass Sie diese Änderung später rückgängig machen können.

Neue, leere Partitionstabelle auf diesem Gerät erstellen?

<Zurück> <Ja> <Nein>

#### Freien Speicherplatz auswählen und Enter

[!] Festplatten partitionieren

Dies ist eine Übersicht über Ihre konfigurierten Partitionen und Einbindungspunkte. Wählen Sie eine Partition, um Änderungen vorzunehmen (Dateisystem, Einbindungspunkt, usw.), freien Speicher, um Partitionen anzulegen oder ein Gerät, um eine Partitionstabelle zu erstellen.

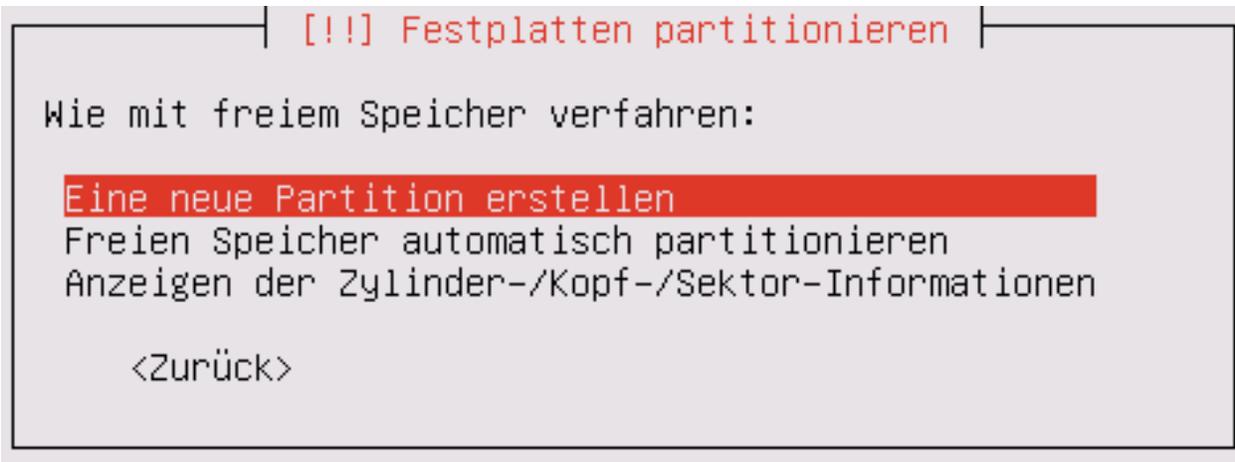
Geführte Partitionierung  
Software-RAID konfigurieren  
Logical Volume Manager konfigurieren  
Verschlüsselte Datenträger konfigurieren  
Configure iSCSI volumes

Virtuelle Festplatte 1 (vda) - 8.6 GB Virtio Block Device

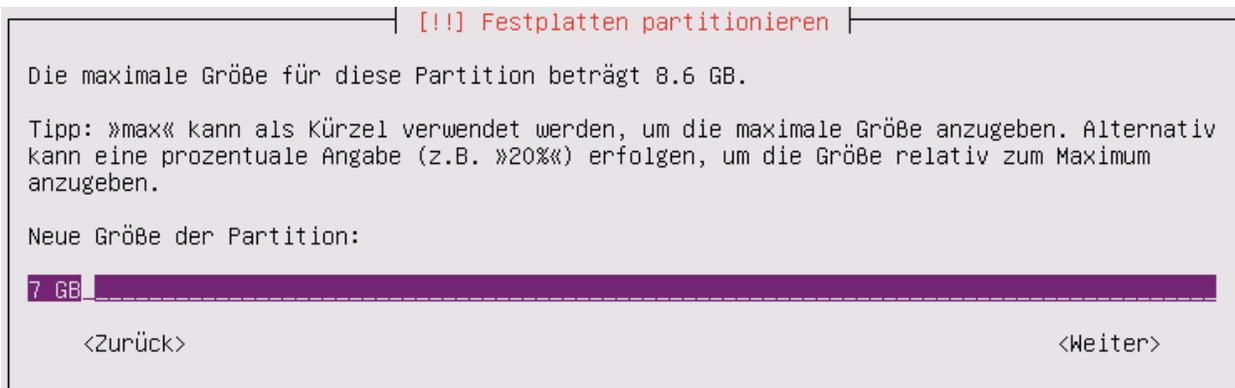
pri/log 8.6 GB FREIER SPEICHER

Änderungen an den Partitionen rückgängig machen  
Partitionierung beenden und Änderungen übernehmen

<Zurück>



Partitionsgröße 5 GB primär am Anfang



```

[!!!] Festplatten partitionieren

Bitte wählen Sie, ob die neue Partition am Anfang oder am Ende des verfügbaren Speichers
erstellt werden soll.

Position der neuen Partition:

Anfang
Ende

<Zurück>

```

Bootflag auf 'ein' setzen und 'Anlegen beenden'

```

[!!!] Festplatten partitionieren

Sie bearbeiten Partition 1 auf Virtuelle Festplatte 1 (vda). Auf dieser Partition wurde
kein vorhandenes Dateisystem gefunden.

Partitionseinstellungen:

Benutzen als:                               Ext4-Journaling-Dateisystem
Einbindungspunkt:                             /
Einbindungsoptionen:                         defaults
Name:                                         Keiner
Reservierte Blöcke:                           5%
Typische Nutzung:                             standard
Boot-Flag (Boot-fähig-Markierung):          Ein

Daten von einer anderen Partition kopieren
Die Partition löschen
Anlegen der Partition beenden

<Zurück>

```

Freien Speicherplatz auswählen und Enter

```

[!!!] Festplatten partitionieren

Dies ist eine Übersicht über Ihre konfigurierten Partitionen und Einbindungspunkte.
Wählen Sie eine Partition, um Änderungen vorzunehmen (Dateisystem, Einbindungspunkt,
usw.), freien Speicher, um Partitionen anzulegen oder ein Gerät, um eine
Partitionstabelle zu erstellen.

Geführte Partitionierung
Software-RAID konfigurieren
Logical Volume Manager konfigurieren
Verschlüsselte Datenträger konfigurieren
Configure iSCSI volumes

Virtuelle Festplatte 1 (vda) - 8.6 GB Virtio Block Device
Nr. 1 primär 7.0 GB B f ext4 /
prl/log 1.6 GB FREIER SPEICHER

Änderungen an den Partitionen rückgängig machen
Partitionierung beenden und Änderungen übernehmen

<Zurück>

```

Einen neue Partition erstellen

```
[!!] Festplatten partitionieren

Wie mit freiem Speicher verfahren:

Eine neue Partition erstellen
Freien Speicher automatisch partitionieren
Anzeigen der Zylinder-/Kopf-/Sektor-Informationen

<Zurück>
```

Größe bestätigen

```
[!!] Festplatten partitionieren

Die maximale Größe für diese Partition beträgt 1.6 GB.

Tipp: »max« kann als Kürzel verwendet werden, um die maximale Größe anzugeben. Alternativ
kann eine prozentuale Angabe (z.B. »20%«) erfolgen, um die Größe relativ zum Maximum
anzugeben.

Neue Größe der Partition:

1.6 GB
<Zurück>                                     <Weiter>
```

Primär

```
[!!] Festplatten partitionieren

Typ der neuen Partition:

Primär
Logisch

<Zurück>
```

Benutzen als 'Auslagerungsspeicher (SWAP)'

'Anlegen beenden'

| [!!] Festplatten partitionieren |

Sie bearbeiten Partition 2 auf Virtuelle Festplatte 1 (vda). Auf dieser Partition wurde kein vorhandenes Dateisystem gefunden.

Partitionseinstellungen:

Benutzen als: Auslagerungsspeicher (Swap)

Boot-Flag (Boot-fähig-Markierung): Aus

Daten von einer anderen Partition kopieren  
Die Partition löschen  
Anlegen der Partition beenden

<Zurück>

#### 'Partitionierung beenden'

| [!!] Festplatten partitionieren |

Dies ist eine Übersicht über Ihre konfigurierten Partitionen und Einbindungspunkte. Wählen Sie eine Partition, um Änderungen vorzunehmen (Dateisystem, Einbindungspunkt, usw.), freien Speicher, um Partitionen anzulegen oder ein Gerät, um eine Partitionstabelle zu erstellen.

Geführte Partitionierung  
Software-RAID konfigurieren  
Logical Volume Manager konfigurieren  
Verschlüsselte Datenträger konfigurieren  
Configure iSCSI volumes

Virtuelle Festplatte 1 (vda) - 8.6 GB Virtio Block Device

Nr. 1	primär	7.0 GB	B	f	ext4	/
Nr. 2	primär	1.6 GB		f	Swap	Swap

Änderungen an den Partitionen rückgängig machen  
Partitionierung beenden und Änderungen übernehmen

<Zurück>

Ja schreiben, noch sind ja keine Daten vorhanden, die überschrieben werden könnten.

| [!!] Festplatten partitionieren |

Wenn Sie fortfahren, werden alle unten aufgeführten Änderungen auf die Festplatte(n) geschrieben. Andernfalls können Sie weitere Änderungen manuell durchführen.

Die Partitionstabellen folgender Geräte wurden geändert:  
Virtuelle Festplatte 1 (vda)

Die folgenden Partitionen werden formatiert:  
Partition 1 auf Virtuelle Festplatte 1 (vda) als ext4  
Partition 2 auf Virtuelle Festplatte 1 (vda) als Swap

Änderungen auf die Festplatten schreiben?

<Ja> <Nein>

Warten...

Proxy leer lassen

[!] Paketmanager konfigurieren

Falls Sie einen HTTP-Proxy benötigen, um das Internet zu erreichen, geben Sie hier bitte Ihre Daten an. Falls nicht, lassen Sie dieses Feld leer.

Die Proxy-Daten sollten im Standardformat »http://[[user][:pass]@]host[:port]/« angegeben werden.

HTTP-Proxy-Daten (leer lassen für keinen Proxy):

<Zurück> <Weiter>

Warten...

Automatische Sicherheitsaktualisierungen auswählen

[!] Konfiguriere tasksel

Das regelmäßiges Einspielen von Aktualisierungen ist wichtig, um Ihr System sicher zu halten..

Standardmäßig müssen Aktualisierungen manuell mit Paketverwaltungswerkzeuge eingespielt werden. Alternativ können Sie festlegen, dass das System automatisch Sicherheitsaktualisierungen herunterlädt und einspielt, oder Sie können festlegen, dass dieses System als Teil eines Systems über das Internet mit dem Landscape-Dienst von Canonical verwaltet wird.

Wie möchten Sie Aktualisierungen auf diesem System verwalten?

Keine automatischen Aktualisierungen  
**Sicherheitsaktualisierungen automatisch installieren**  
System mit Landscape verwalten

OpenSSH Server auswählen (Leertaste benutzen) und weiter



Warten...

Die Installation des GRUB Bootloader bestätigen



Weiter



## 5.4.2 SSH

Per SSH mit dem Server verbinden

```
ssh meinbenutzername@111.222.333.444
```

Den Public-Key für den User hinterlegen:

```
cd /home/meinbenutzername/  
mkdir .ssh  
nano .ssh/authorized_keys
```

Im Editor dann den Public Key (“ssh-rsa AAA...”) einfügen. Wichtig: Alles von diesem Key muss in eine Zeile. Weitere Adminuser können später angelegt werden.

Nun das Password-Login auf dem Server deaktivieren. Dazu die sshd\_config editieren:

```
sudo nano /etc/ssh/sshd_config
```

Die Zeile

```
#PasswordAuthentication yes
```

ändern in

```
PasswordAuthentication no
```

Achtung, auch wenn ‘yes’ auskommentiert ist, besteht die Möglichkeit sich per Password zu verbinden, erst wenn ‘no’ gesetzt ist und nicht (mehr) auskommentiert ist, ist der Zugriff nur noch per Key möglich.

Um es den Script-Kiddies und Bots etwas schwerer zu machen, sollte der Port 22 auf einen hohen Port (mindestens über 1024) verändert werden. Dazu die Zeile

```
Port 22
```

ändern in

```
Port 62954
```

**WICHTIG:** Diesen Port muss man sich dann merken, da man ihn später beim Aufruf von ssh angeben muss.

Nun den direkten Rootlogin sperren.

```
PermitRootLogin yes
```

ändern in

```
PermitRootLogin no  
UsePAM no
```

Danach den Editor wieder verlassen und den SSH Server neu starten um die Einstellungen zu übernehmen.

```
sudo service ssh restart
```

Den nachfolgenden ssh Kommandos muss man die Option “-p 62954” (kleines “p”!) und den scp Kommandos die Option “-P 62954” (großes “P”!).

```
ssh -p 62954 meinbenutzername@111.222.333.444
```

### 5.4.3 Systemaktualisierung

Als Nächstes steht die Systemaktualisierung an; auch hier beim erstmaligen Aufruf die Nutzung von IPv4 erzwingen für's APT-Get

```
sudo apt-get update
sudo apt-get dist-upgrade
sudo apt-get autoremove
```

## 5.4.4 Pakete installieren

Ergänzen der `/etc/apt/sources.list` um das fastd repository

```
sudo nano /etc/apt/sources.list
```

Folgende Zeile hinzufügen

```
deb http://repo.universe-factory.net/debian/ sid main
```

Editor schließen

Den zugehörigen Schlüssel importieren

```
sudo apt-key add - <<EOF
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1

mQINBFLNIUUBEADtYPgKZY/BVjqAp68oV5xpY557+KdGxN4jDrdtANDDMjIDakbX
AD1A1zqXLUREvXMsKA/vacGF2I4/0kwsQhNeOzhGPsBa8y785WFQjxq4LsBJpC4Q
fDvcheI14BeKoHzfUYDp4hgPBrKcaRROBODMwp1FZmJxhRVtiQ2m6piemksF1Wpx
+6wZ1cw4YhQdEnw7QZByYYgABv7ZoxSQZzyeR/Py0G5/zg9ABLcTF56UWq+ZkiLE
Mg/5K5hzUKLYC4h/xNV58mNHBho0k/D4jPmCjXy7bouDzKZjnu+CIsMoW9RjGH39
3GNCC+F3Xuo35g3L41Z89AdNhZ0zeMLJCTx5uYOQN5YZP2eHW2P1VZpwtDOR0zWo
ylc0q6DniYtn0HGStVLuP+MQxuRe2R1oJE7fDRfz7/OFOU6mBVkRyMCCPwWYXyEs
2y8m4akXDvBCPTNMMEPRIy3qcAN4HnOrmnc24qfQzYp9ajFt1YrXMqQySQgcTzuV
YkYVnEMFBhN6P2EKoKU+6Mee01UFb7Ww8atiqG3U0oxsXbOIVLrrno6JONdYeAvy
YuZbAxJivU3/RkGLSygzV53EUCfyoNldDuUL7GuJtn/R2/CsBPM+RH8oOVuh3od2
FrF0PP8p9yYoa2RD7Pfx4WXdnfYv0OWgFgpz0leup9xhoUNE9RknplL1UwARAQAB
tDJNYXR0aG1hcYBTY2hpZmZlciA8bXNjaGlzZmVvYQHVuaXZlcnNlLWZhY3Rvcnku
bmV0P0kCPQQAQoAJwUCUs0hRQIbAwUJA8JnAAULCQgHAwUVCgkICwUWAwIBAAIe
AQIXgAAKcRAW7z9kyAdnB8rD/4u8y3s4azhTwC9RVjtEXdLxZyZG0FkQSoKSBg
SWQUthjgkVnYmv7db3bSNmTZ7NaeCIA33WtQpH19j/nOExy1co4z8wX8WR098TK8
E11DLASi6wnaZWRzU1D/stJzhVNNn33h0kc4HK5b6CFQCocQZAweUBQhiZwcf4C3
U8eM1QrNYWQjsACBLvy7k8oGZF6QWEPnT/okOYCq8ZNg4gKKK1HsWt59yHrAA09C
P85NpiPSJ30bTnVamiKtSD/XvDjC0vUNISqmLheHD4OPXpGgph7Iiggnj7DJCJu+
hB7AYiZmCYhoQ33UTluKih53Bvb12cS5Y0HvG1yms6+/FsbOgtJef1DeDdefI117
ApwqdOWYoejpZFqEo2jtIR6PZJoVVouVbEZjBBCXG9eePhs0aa0gj4EsYOSHIp0C
0SRBpQLBglixtnnc+UsVQBOAdsC718273kIsa041N4541hf7LqluF5mwohn3Ag
Be7q0IGU9SzhWGNwaD09Ce32Kwt/OQc8IEosmDnPiSm/hME01Vxm7qJ2uQUMcwop
ch3oBjVbp4AXCyfImrfeQzkwBepCztaXWbTlnwCj06W07uRUUHqjjCSioXZkcqE
EgZINZMrZEnT1vhRopqd99WziJaVVfxyHz27gW4cAqJAv+jk4rBp51ZCuK3Lts50
SI/DZ4kCQAQTAQoAKgIbAwUJA8JnAAULCQgHAwUVCgkICwUWAwIBAAIeAQIXgAUC
Us0jFAIzAQAKcRAW7z9kyAdnGhbD/9nrpctmD+DRahKEU2xW9KXBZG1qqvoigU/
sePQpNZG1bWfzFBclagI4AC7udHnoj4KzeQ8YkW0qpd60M9E+WHYHm3TtdHZiZMt
SvGr4w4z8FHbqD+beALec7QVYh9pu5HcrXYTEb1d4+uarLUXiqzoxOY6j6stHEKn
oDBJ1XzHj5W4yviyqi3sd1N07HtH7dp7RwmofnKQZMXyWqIuNFHqV+B+T/hNg8z
pBML10P5v+fa/nSDk2G1alubspDrpIRisynF6jCGEYnNPWd2T/x4GLLQbta31EQ
BIMNyyy8xiqzEEsKF+/UWqV/sqar3f0iPYF4en7jDHJV8QoiAQinCD05u8mFT6uc
zUTBVpxFZCbc01S9xm56RmNfLgnXMD3YoVz8SE0E30TowM0QFHwy49aipgurEKUv
FKDTLb5HNYrSszXhk+Uu9dtIJJNpM46QcTLiWdzRuTNoaSo4eq12Sm/0i+msPBM9V
R27dBvLbaC8PUnyec03z8MGx/ZOr20odpar911Zzna3kyRLHzcQ8fkMi/FX351Gs
PMFLi3x1sL411xE8SoeBYEongSc0Fxf0vErJ9Fb4rx7irb27eb0peahYzzuz1SK
```

```
iO+s1VRNVbxeekxK+e19sM74RiE2fPbGLTjEPYN/NjpUuAIEZmXznQBy5rY950+T
9ntcRlKwaokCQAQTAQoAKGIBAwULCQgHAWUVCgkICwUWAwIBAAIeAQIXgAIZAQC
Vo+NowUJBaOf3gAKCRAW7z9kyYAdnCbuD/wMsZ/oAL7s0SY6k4S3yC2e06L1rhUs
gDjfdI+2wFzc5ZzAUjR17VhOnQdII5bNxJJvp+4M5wrFMBG/bVXsu22NDblA+VJ9y
CEfMf49ouKpwSdz3AE7UlgM5AAwGaoNnzrSkzS0RE45+KBhxbCWKsF/Ht6BKWcBx
asWtfn9KZjgMnbfIQDiT64EOUZpSb+PmKlgwUkrJlRWas20z1zFVBCoXDIqByjHU
TC1Qz/iKQUdZR/hshlLKRfWocJi4ek61jRDO8CzvuyQvf3CCBmbgppvQZaU3aJEQ
jMlrPmVz/ZM0g3K1axLKzWfBMPMV8DuQhShFzmGc83ZL976J84eAj57p4JgzPgLx
iFlKrrTs6MC4gbX5bMomXGnFxfnv+Oe8Ce1Jj/1eGhqDYwZjM2bQrmiotIsPjAHh
18fdwVxVcASTobTQV7/NEos/a+y4AmfwW8dREhHPUxkcPe7eUO11UeG6Dukakag9
s67No7KCuEWC0g2wOuRmpjkmK9Q5Mu0xEjPY4/U30/z8YDBDJsgowSmM+IR3SsTK
JVJMGxsOwqLOYSZdaG5m/ZfX/spStVYF4w3PcFcQEHCiYKp/pr89CWkXAKV7t9DZ
kAmvGv6jreyJEZsoiMS4kiY7yeMyESFNzLItPvWsluQ+6L2DEy/ru2qx63CQv2zn
h7CfZTO/vf+IfrkCDQRSzSFFARAawhZQlixkJpypG9Q71m8iD3E7su5pd0xuVYQn
ESq2A/RgGrLxsG9RWN0h8WdZNCX1sRTk9NkxDJo1VKmpbNqyDVH7t2F2gC6vEdGk
P042fF/oyOkOh7B8DnRUwS+Mw+KSrON4kVnfoMFMWAW/GLAWPiokSj+9Fws0DHax
BtcehQAW1F/eudYTdtELfxijYsR1ct72g9z87Xh/47oKn7Tbvff0NoeASQRuIGdI
MI6XsbvY4z9rdCDlC0rBU+kvDWremz4DFtwqxHUzhpJQD/bKo228ovBgG7MWY8
e2A5JdTKRRsZQtONJBQtDDC7nvaUrE+Z8A5dt9CMWYJEU46C0n5o01o9bchK8pI1
le7Wt68duzbV2Jx7Rqx8vsrm07AcoLdrMwy/ZdjkeM7HPfoS37RelKf9g9PZxc5i
yinHeDWw62/kjLFRpZda4wL+9yERfc6xzYaGlXrGk81Bn15VxsbDqqUPVNjY1FCY
Nwf/YoyhJN8/ROjxf9F5nOYBtwuF809MSVX7CmXGafRj5fvkEAO5xyTG3scq7ijj
Ks0tu97wCp087zg9HISL1NA2fxXyQajXUX793FMIEMLAVOGrrBgpzNKHXtIO5tMZ
wgEHL3vYcQKB9b4Bo19DOVOBcwqyQPhOqOSpqrccqNIOUdDQYgMSZ4VAdHhyTwBJR
a0e7tc0AEQEAAyKcJQQYAQoADwIbDAUCVo+NpAUJBaOf3wAKCRAW7z9kyYAdnOLS
D/4k6s78FAqnS9MbcIw241klRDQaiEAzJ+U1p7M1Rjuz3x+wwNU3izcZvbDFm2y
zihcQ+PaLz9TUVYvMoyPbWPsRnBlDefGm+9v49x6PJPVwyzmmrVWIAvpoHPfpnzK
zIZ10V7LXlS9UwWt0Y6vsfacLkMTC0AVFr2hlNwhhBmrwp8N/6MNVkfbGyyuLs1
TB/uKH8EZpicQSy6hSzp7U4Z8iZEmjcyBFQOrVkvZVIU5rEFF9FzvnXAtPfgUY
V2USobQDI7/YlKRQ8EFFpmAGIbf6vs6Wafb9xfpgsu7BHYH8Uz96og5wrzo4bAlc
IGxvBKYE3qDvKozYjYupPqvlDd2eQHA7DS6r9FTM6W2aI0vY1Vav6VM0HgAL/4LE
unYXlQsjsUzpzKvLZXfaELckRYSWJtHXKNgw2LkQ/2YLFuyJDHJ+fg7y9ME868V2
BfWnZ9S7rAjSNQoami+wCwtfbVK37vpKR4+bj57Gu9L6DamQtqQTi7+7YTDLuk9
vBSFx7vyGw33PNff+Tg2L01/bPon1jRt9kTihh0g9gcxizew865QpMHjAxAlpfWr
hHaJWdi+XBbyG2uR7I8wUIutPz2OSCSnL+oG7pZN00Ug9V70XcChCm9YB8KMbHME
elBSE45qsAbY6wi4md4saj3hwJHSRYoeqag7PQeo37WXKQ==
=Xtaw
-----END PGP PUBLIC KEY BLOCK-----
EOF
```

```
sudo apt-get update
sudo apt-get install xinetd git vnstat vnstati gdebi-core lighttpd fastd build-
essential \
bridge-utils isc-dhcp-server radvd libnl-3-dev pkg-config
```

Rückfrage mit “J” bestätigen

Um welche Paket handelt es sich?

- vnstat monitort den Netzwerktraffic
- vnstati erzeugt daraus Grafiken
- lighttpd stellt diese zum Abruf bereit
- gdebi-core ermöglicht uns die Installation des Check\_mk Agents
- xinetd ist der bei Debian übliche Super-Daemon, über ihn wird der Check\_mk Agent angesprochen
- Fastd baut Tunnelverbindungen zu den Routern auf

- build-essential wird zum kompilieren von Batman benötigt
- bridge-utils (brctl) steuert Netzwerkbrücken
- isc-dhcp-server (dhcpd3) verteilt IPv4 Adressen
- radvd verteilt die IPv6 Range
- git wird für die Konfigurationsscripte benötigt
- libnl-3-dev wird für batman benötigt
- pkg-config wird für batctl benötigt

### 5.4.5 Batman kompilieren

Batman kann man bei <http://www.open-mesh.org/projects/open-mesh/wiki/Download> herunterladen

```
cd ~
wget http://downloads.open-mesh.org/batman/stable/sources/batman-adv/batman-adv-2016.
↪0.tar.gz
tar -xf batman-adv-2016.0.tar.gz
cd batman-adv-2016.0
make
sudo make install
```

### 5.4.6 Batctl kompilieren

```
cd ~
sudo wget https://downloads.open-mesh.org/batman/stable/sources/batctl/batctl-2016.0.
↪tar.gz
tar -xf batctl-2016.0.tar.gz
cd batctl-2016.0
make
sudo make install
```

### 5.4.7 Batman Kernelmodul eintragen

Damit das Batman Kernelmodul beim boot geladen wird müssen wir es noch in die /etc/modules eintragen.

Mehr infos gibt es im ubuntuusers wiki <https://wiki.ubuntuusers.de/Kernelmodule#start>

```
sudo nano /etc/modules
```

```
# /etc/modules: kernel modules to load at boot time.
#
# This file contains the names of kernel modules that should be loaded
# at boot time, one per line. Lines beginning with "#" are ignored.
batman-adv
```

### 5.4.8 Fastd einrichten

- Verzeichnis für die Fastd Instanz anlegen

- Dummyverzeichnis für Clients anlegen
- fastd.conf erstellen

```
sudo mkdir -p /etc/fastd/client/dummy
cd /etc/fastd/client
sudo nano fastd.conf
```

```
bind any:10000 default ipv4;
include "secret.conf";
include peers from "dummy";
interface "tap0";
log level info;
mode tap;
method "salsa2012+umac";
peer limit 200;
mtu 1406;
secure handshakes yes;
log to syslog level verbose;
status socket "/run/fastd.client.sock";

on up "
    ip link set address 04:EE:EF:CA:FE:3A dev tap0
    ip link set up tap0
    /usr/local/sbin/batctl -m bat0 if add $INTERFACE
    ip link set address 02:EE:EF:CA:FE:FF:3A dev bat0
    ip link set up dev bat0
    brctl addif br0 bat0
    /usr/local/sbin/batctl -m bat0 it 5000
    /usr/local/sbin/batctl -m bat0 bl 0
    /usr/local/sbin/batctl -m bat0 gw server 48mbit/48mbit
    /usr/local/sbin/batctl -m bat0 vm server
";

on verify "/etc/fastd/client/blacklist.sh $PEER_KEY";
```

Nun das Blacklist-Script anlegen.

```
sudo nano /etc/fastd/client/blacklist.sh
```

Mit Inhalt:

```
#!/bin/bash
PEER_KEY=$1
echo peer "$PEER_KEY" joining
if /bin/grep -Fq $PEER_KEY /etc/fastd/client/fastd-blacklist.json; then
exit 1
else
exit 0
fi
```

dann die Datei ausführbar machen

```
sudo chmod +x /etc/fastd/client/blacklist.sh
```

Und schließlich eine Dummy-Datei anlegen

```
sudo nano /etc/fastd/client/fastd-blacklist.json
```

dort hinein

```
{
"peers":
[
{
"pubkey": "0004df72c02827333bced7680acaf38f36b09597c55241571e90637465831000",
}
]
}
```

Den Editor wieder verlassen und nun einen fastd Key erzeugen, der in passender Syntax in “secret.conf” abgelegt wird.

```
sudo fastd --generate-key > secret.conf
```

In der Datei secret.conf müssen dann manuell Änderungen vorgenommen werden: Die Zeile mit ‘Public’ muss mit ‘#’ auskommentiert werden, die Zeile ‘Secret’ muss angepasst werden.

```
sudo nano secret.conf
```

```
secret "xxx...";
#Public: ...
```

## 5.4.9 Hinzufügen einer Schnittstelle eth1

Nun muss im Proxmox für die VM eine eth1 hinzugefügt werden, die auf der vbr1 hängt und Virtio verwendet.

Proxmox Virtual Environment  
Version: 3.4-3/2fc72fee  
You are logged in as 'root@pam' Logout Create VM Create CT

Server View Virtual Machine 103 ('xyzbackbone-1') on node 'node01' Start Shutdown Stop Reset Remove Migrate Console

Summary Hardware Options Task History Monitor Backup Snapshots Firewall Permissions

Add Remove Edit Resize disk Move disk Disk Throttle Revert

Hard Disk	Default
CD/DVD Drive	256MB/1.00GB
Network Device	2 (1 sockets, 2 cores) [host]
CD/DVD Drive (ide2)	Default
Hard Disk (virtio0)	local:iso/ubuntu-14.04.3-server-amd64.iso,media=cdrrom
Hard Disk (virtio0)	local:103/vm-103-disk-1.qcow2,format=qcow2,size=8G
Network Device (net0)	e1000=6E:9F:D3:A3:45:62,bridge=vbr0,link_down=1

Danach die VM einmal durchbooten.

## 5.4.10 Verbindung zwischen Supernode und Konzentration konfigurieren

### Auf dem Supernode

Zunächst müssen die nötigen Skripte auf den Supernode heruntergeladen und ausführbar gemacht werden:

```
sudo mkdir -p /opt/eulenkunk
cd /opt/eulenkunk
sudo git clone https://github.com/eulenkunk/supernode.git
cd supernode
sudo chmod +x *.sh
sudo chmod +x *.py
```

Nun muss man dem jeweiligen Supernode aus dem vom FFRL zugeteilten IPv6-Adressbereich noch ein /56 heraus-schneiden, ein passendes IPv4 Netz für seine Endgeräte festlegen und die Werte in die Konfigurationsdatei supernode.config schreiben:

```
sudo nano /opt/eulenkunk/supernode/supernode.config
```

Hier ein Beispiel:

```
SUPERNODE_IPV6_PREFIX=2a03:2260:X:Y::/56
SUPERNODE_IPV4_CLIENT_NET=172.19.0.0/16
SUPERNODE_IPV4_TRANS_ADDR=172.31.254.1
```

Die angepasste Konfiguration wird dann durch das Setup verwendet:

```
cd /opt/eulenkunk/supernode
sudo ./supernode-setup.sh
```

```
Ausgaben in:
  interfaces.eulenkunk
  dhcpd.conf.eulenkunk
  radvd.conf.eulenkunk
  20-ff-config.conf.eulenkunk
```

Die so erzeugten Konfigurationsdateien müssen **nach Prüfung** an die passenden Stellen kopiert werden

```
sudo cp dhcpd.conf.eulenfunk /etc/dhcp/dhcpd.conf
sudo cp radvd.conf.eulenfunk /etc/radvd.conf
sudo cp 20-ff-config.conf.eulenfunk /etc/sysctl.d/20-ff-config.conf
```

und die Netzwerkkonfiguration an die vorhandene angehängt werden:

```
sudo cat interfaces.eulenfunk >> /etc/network/interfaces
```

Als letzter Schritt auf dem Supernode muss die `/etc/rc.local` folgendermassen angepasst werden:

```
sudo nano /etc/rc.local
```

```
#!/bin/sh -e
#
# rc.local
#
# This script is executed at the end of each multiuser runlevel.
# Make sure that the script will "exit 0" on success or any other
# value on error.
#
# In order to enable or disable this script just change the execution
# bits.
#
# By default this script does nothing.

/opt/eulenfunk/supernode/supernode-rc.sh

exit 0
```

Das sorgt dafür, dass beim Systemstart durch das Script `supernode-rc.sh` die nötigen Routen und Routing-Policies konfiguriert werden.

### Check\_MK Agent installieren

Den Check\_MK Agent steht in der Weboberfläche des Check\_MK als `.deb` Paket bereit:

In die CheckMK-Instanz per Webbrowser einloggen. Dann suchen:

```
-> WATO Configuration (Menü/Box)
-> Monitoring Agents
-> Packet Agents
-> check-mk-agent_1.2.8p11-1_all.deb _(Beispiel)_
```

Den Download-Link in die Zwischenablage kopieren. Im SSH-Terminal nun eingeben: (die Download-URL ist individuell und der Name des `.deb`-Paketes ändert sich ggf.)

```
wget https://monitoring.eulenfunk.de/eulenfunk/check_mk/agents/check-mk-agent_1.2.
↪8p11-1_all.deb
```

Um das `.deb` Paket zu installieren wird `gdebi` empfohlen, ausserdem benötigt der Agent `xinetd` zum Ausliefern der Monitoring Daten.

Per SSH auf dem Server. (Auch hier: Name des `.deb`-Files ggf. anpassen)

```
sudo gdebi check-mk-agent_1.2.8p1-1_all.deb
```

Anschließend noch das Supernode-Plugin hinzufügen:

```
cd /usr/lib/check_mk_agent/local
sudo wget -O supernode https://raw.githubusercontent.com/eulenkfunkt/check_mk/master/
↪supernode
sudo chmod 755 supernode
sudo chmod +x supernode
```

:: sudo nano /etc/xinetd.d/check\_mk

Dort die Zeile

```
# only_from = 127.0.0.1 10.0.20.1 10.0.20.2
```

ändern in

```
only_from = 127.0.0.1 94.23.160.148
```

Damit diese Änderungen aktiviert werden, muss der xinetd durchgestartet werden

```
sudo /etc/init.d/xinetd restart
```

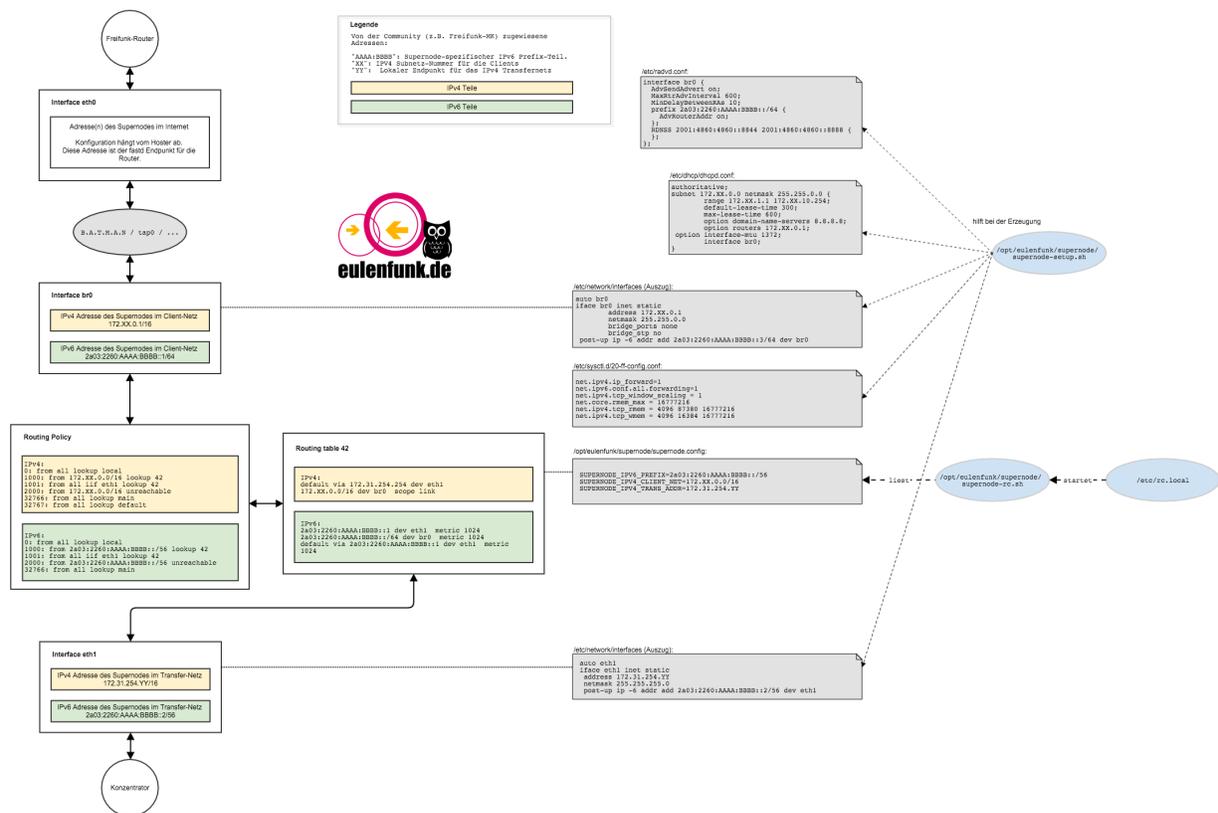
Der Rechner hält ab nun Daten zum Abruf bereit.

JJX Bescheid sagen, der kümmert sich dann darum.

Danach den Supernode rebooten.

Hier eine grafische Übersicht über die beteiligten Konfigurationsdateien auf dem Supernode:

Supernode nach Eulenkfunkt-Schema



## Auf dem Konzentrator

Auf dem Konzentrator muss die zum Supernode passende Konfiguration angelegt werden:

```
cd /opt/eulenfunk/konzentrator/config
sudo nano meinestadt-1
```

Dort müssen folgende Werte eingetragen werden:

```
# Beschreibender Name "stadt-N"
SUPERNODE_NAME=meinestadt-1

# Soll die Netzwerkkonfiguration automatisch beim Systemstart gesetzt werden
AUTOSTART=1

# IPv4 Konfiguration
SUPERNODE_CLIENT_IPV4_NET=<IPv4 Netz fuer die Clients, 172.XX.0.0/16>
SUPERNODE_TRANS_IPV4_NET=<IPv4 Transit-Netz, 172.31.YYY.0/24>
SUPERNODE_TRANS_IPV4_REMOTE=<Supernode IPv4 eth1 Adresse Transit-Netz, 172.31.YYY.1>

# IPv6 Konfiguration
SUPERNODE_CLIENT_IPV6_NET=<IPv6 Netz fuer die Clients, 2a03:2260:AAAA:BBBB::/64>
SUPERNODE_TRANS_IPV6_NET=<IPv6 Supernetz fuer Transit, 2a03:2260:AAAA:BBBB::/56>
SUPERNODE_TRANS_IPV6_LOCAL=<IPv6 Supernetz lokale Adresse, 2a03:2260:AAAA:BBBB::1>
SUPERNODE_TRANS_IPV6_REMOTE=<IPv6 Supernetz remote Adresse, 2a03:2260:AAAA:BBB::2>
```

Man kann dann die Konfiguration folgendermaßen aktivieren:

```
cd /opt/eulenfunk/konzentrator
sudo ./supernode.sh start meinestadt-1
```

Die Konfiguration kann im laufenden Betrieb auch wieder entfernt werden (damit wird die Stadt allerdings vom Freifunk getrennt!)

```
cd /opt/eulenfunk/konzentrator
sudo ./supernode.sh stop meinestadt-1
```

Durch den Parameter AUTOSTART=1 wird beim Reboot des Konzentrators die Konfiguration für diese Stadt automatisch wieder gesetzt.

Den Konzentrator und den Supernode rebooten, um die Reboot-Festigkeit zu testen.

## 5.5 Nützliches

### 5.5.1 Benutzerkennwort zurücksetzen

Hat man sein Kennwort vergessen, kann man einen anderen Nutzer mit Zugriff auf den Server bitten ein neues Kennwort zu setzen

```
sudo passwd Meinbenutzername
```



## CHAPTER 6

---

### Map

---

Nodegraph und Geo-Karte sind unter  
<http://map.eulenfunk.de> (für alle communities) verfügbar.  
-tbd-