

Pi-hole™

Network-wide ad blocking
via your own hardware

Pi-hole is a

Linux

network-level

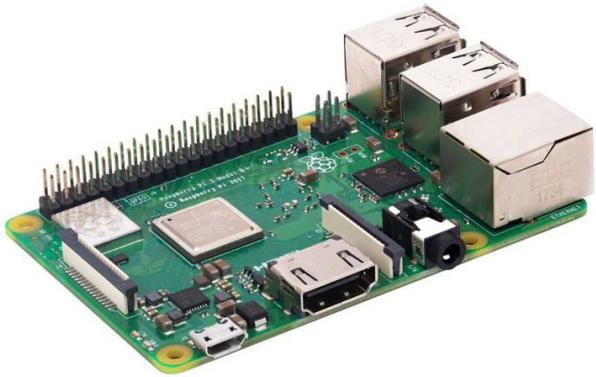
advertisement and internet tracker blocking

application

which acts as a DNS sinkhole

(And optionally a DHCP server)

Voraussetzungen



40 CHF



10 CHF

Evtl. nur USB-Kabel



15 CHF

Raspi-Schachtel
reicht eigentlich



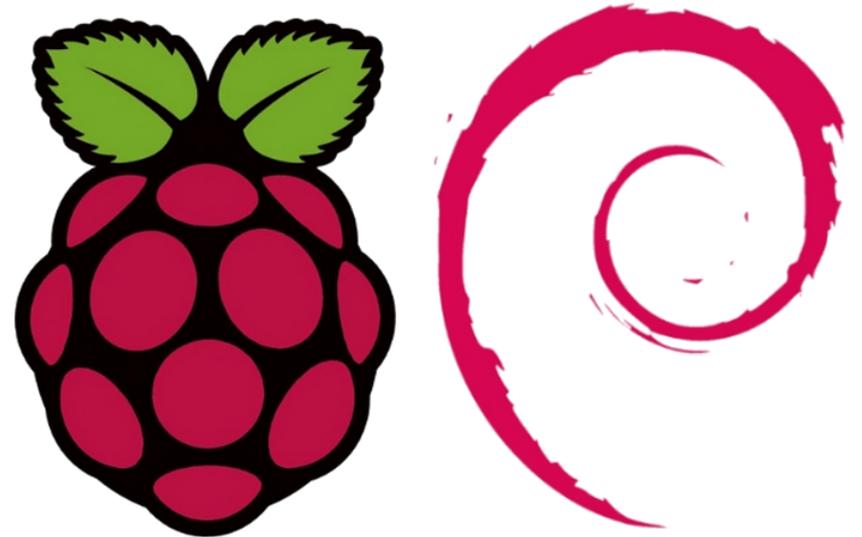
10 CHF

2 GB reicht

Software/Downloads

Raspbian Stretch Lite

- „**Lite**“: Debian für Raspberry **OHNE** Graphik



Raspbian

- <https://www.raspberrypi.org/downloads/raspbian/>
- 2018-11-13-raspbian-stretch-lite.zip
- → 2018-11-13-raspbian-stretch-lite.img
- .img per dd auf SD-Card

```
$ sudo dd if=~/.2018-11-13-raspbian-stretch-lite.img of=/dev/sdX bs=1M
```

- 2 Partitionen auf SD-Card: /boot (fat32) und /root (ext4)
- Boot-Partition mounten und ssh-Zugang einrichten per:
- touch /<Mountpoint>/boot/ssh
- SD-Card unmounten, in Raspberry einschieben

Raspi „aktivieren“

- Netzteil an Raspi anschliessen
- Per Netzkabel ans Heim-Netz/Router
- Netzstecker ans Stromnetz
- Raspi bootet durch den Anschluss an die Stromversorgung!
 - Im Router nach IP von „neuen“ Gerät schauen
 - Per ssh Verbindung mit Raspi aufbauen
 - `ssh -v pi@192.168.x.y`
 - Passwort: raspberry

„im Raspi drin“

- `sudo raspi-config`
 - Sprache
 - Partition ausweiten (eigentlich unnötig)
 - Passwortwechsel
- `sudo apt-get update && sudo apt-get upgrade`
- `sudo reboot`

raspi-config

```
pi@raspberrypi: ~  
Raspberry Pi Software Configuration Tool (raspi-config)  
Setup Options  
1 Expand Filesystem          Ensures that all of the SD card s  
2 Change User Password      Change password for the default u  
3 Enable Boot to Desktop/Scratch Choose whether to boot into a des  
4 Internationalisation Options Set up language and regional sett  
5 Enable Camera             Enable this Pi to work with the R  
6 Add to Rastrack           Add this Pi to the online Raspber  
7 Overclock                 Configure overclocking for your P  
8 Advanced Options         Configure advanced settings  
9 About raspi-config       Information about this configurat  
  
                <Select>                <Finish>
```

Pi-hole installieren

- `ssh -v pi@192.168.x.y`
- Password: *<neues Passwort>*
- `curl -sSL https://install.pi-hole.net | bash`
- Eventuell Anpassungen vornehmen
- `reboot`
- im Browser aufrufen: `http://192.168.x.y/admin`

Bedenkenträger

- „Linuxe schreiben kontinuierlich in /var/log, auch in Mediacenter-Systemen. SanDisk verbietet den Einsatz regulärer (Micro-) SD-Ausführungen in Einplatinen-Computern (dann erlischt die Garantie), sie empfehlen stattdessen "High Endurance"-Ausführungen. Die sind für deutlich höhere Schreibbelastungen ausgelegt und vergleichsweise günstig; daß sie relativ lahm sind, spielt bei RasPis keine Rolle (in deren Slot mögliche Transferraten erreichen sie locker).
- Andere (Marken-) Hersteller verbieten generell den Einsatz sämtlicher Modellein RasPis & Co., von SanDisk immerhin diese "offizielle" Empfehlung. Falls Du kein "Endurance"-Modell anschaffen magst, solltest Du zumindest eine zweite Karte mit einer Kopie des Systems in petto haben ...“

Anpassungen 1

- Schreibzugriffe in SD-Card minimieren
- /var/log in den RAM schieben
- sudo nano /etc/fstab

zum SD-Card schonen:

```
tmpfs /tmp tmpfs defaults,noatime,nosuid,size=100m 0 0
```

```
tmpfs /var/tmp tmpfs defaults,noatime,nosuid,size=100m 0 0
```

```
tmpfs /var/log tmpfs defaults,noatime,nosuid,mode=0755,size=100m 0 0
```

Bedenkenträger II

- „Mir sind Ramdisks für Systemdateien nicht so recht (bei einem Absturz könnte man nicht mal die Logdateien inspizieren um nach Fehlerquellen zu spüren). Adäquate, solide Hardware ist mir lieber.“
- WTF????
- **rsync ist dein Freund!**
- pi@pihole:~ \$ man rsync

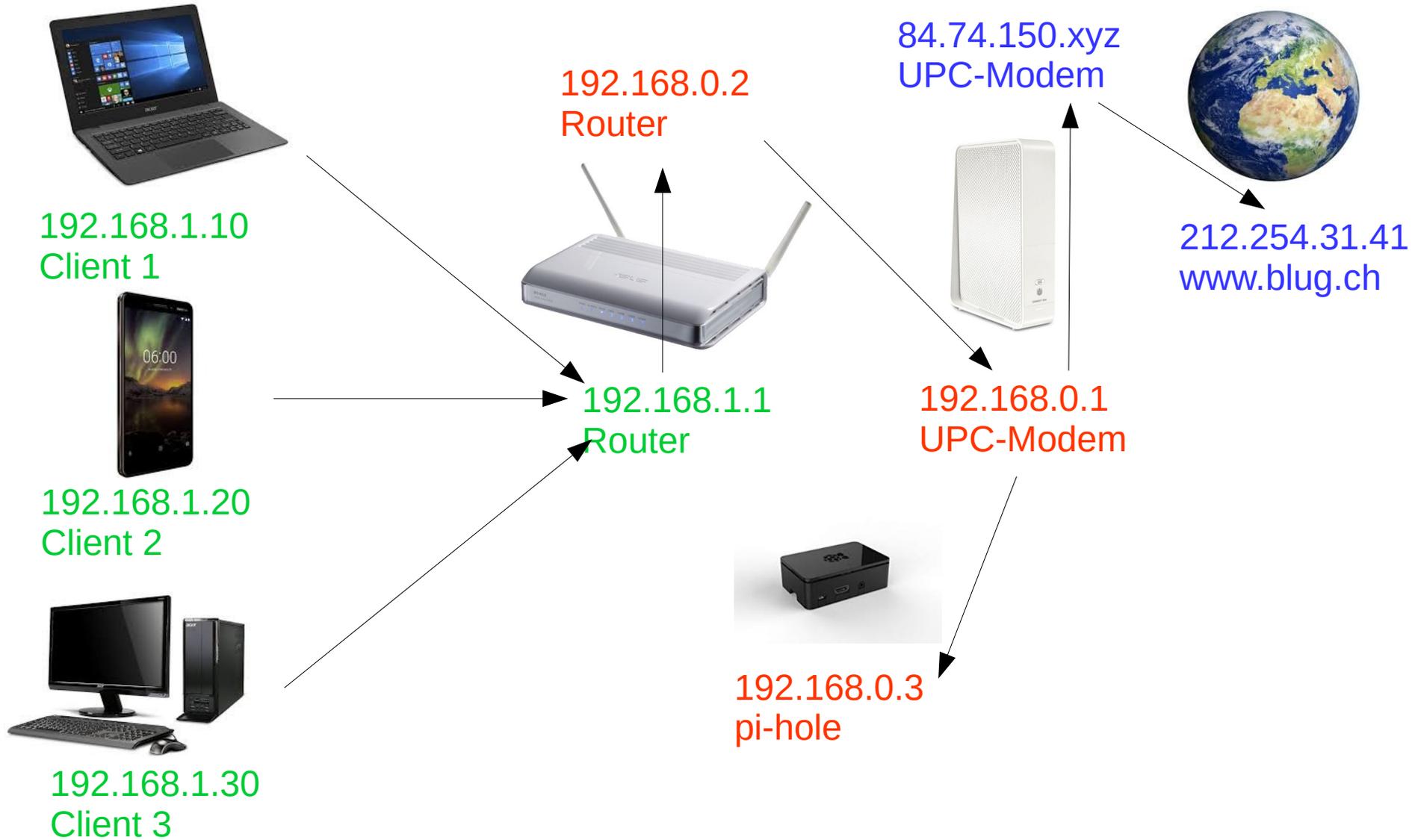
Anpassungen 2

- `sudo touch /etc/pihole/list.preEventHorizon`
(braucht's nicht, nervt mich aber in den logs)
- damit Browser-Admin-Oberfläche startet:
 - `cd /etc/tmpfiles.d/`
 - `sudo nano lighttpd-log.conf`
 - `D /var/log/lighttpd/ 0775 www-data adm`
 - Speichern
- Der IP einen „Namen“ geben:
- `sudo nano /etc/pihole/local.list`
 - `192.168.0.3 pihole`
 - `192.168.0.3 pi.hole`

Anpassungen 3

- statische IP eintragen:
- `sudo nano /etc/dhcpd.conf`
 - `interface eth0`
 - `static ip_address=192.168.x.y/24`
 - `static routers=192.168.x.1`
 - `static domain_name_servers=127.0.0.1`

Netz-Topographie



Der Router sollte es auch wissen...

Not secure | 192.168.1.1/basic-network.asp

Status

- Overview
- Device List
- Web Usage
- Logs

Bandwidth

- Real-Time
- Last 24 Hours
- Daily
- Weekly
- Monthly

IP Traffic

Tools

Basic

- Network**
- IPv6
- Identification
- Time
- DDNS
- Static DHCP/ARP/IPT
- Wireless Filter

Advanced

- Port Forwarding
- Access Restriction
- QoS

MultiWAN

Number of WAN Ports: 1 WAN Please configure VLAN first

Check connections every: Disabled when the network conditions is poor, try use longer detection period

WAN Settings

Type: Static

Wireless Client Mode: Disabled

IP Address: 192.168.0.2

Subnet Mask: 255.255.255.0

Gateway: 192.168.0.1

DNS Server: Manual

DNS 1: 192.168.0.3 

DNS 2:

MTU: Default 1500

Route Modem IP: 192.168.0.1 must be in different subnet to router, 0.0.0.0 to disable

LAN

Bridge	STP	IP Address	Netmask	DHCP	IP Range (first/last)	Lease Time (mins)
br0	Disabled	192.168.1.1	255.255.255.0	Enabled	192.168.1.10 - 51	1440
1	<input type="checkbox"/>			<input type="checkbox"/>		

Web-admin

<http://192.168.x.y/admin>

oder <http://pi.hole/admin/>

DNS-Server eintragen

<https://wiki.ipfire.org/dns/public-servers>

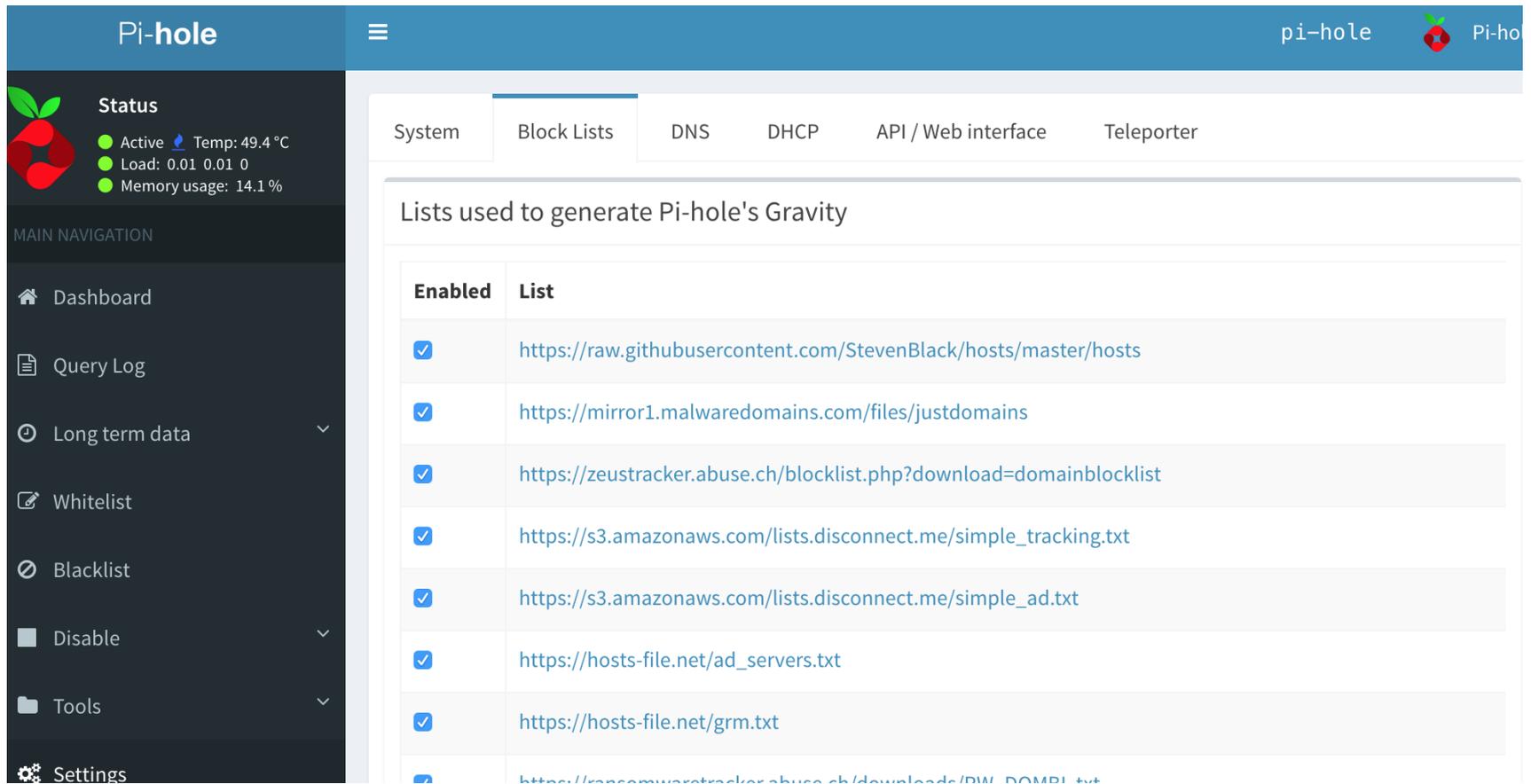
Special: Google-DNS „umbiegen“, (falls gewünscht):

Im ROUTER!! eintragen:

```
iptables -t nat -A PREROUTING -i br0 -p tcp --dport 53 -j DNAT --to <IP von pihole>
```

```
iptables -t nat -A PREROUTING -i br0 -p udp --dport 53 -j DNAT --to <IP von pihole>
```

Weboberfläche



The screenshot displays the Pi-hole web interface. The top navigation bar includes the Pi-hole logo, a hamburger menu, and the text 'pi-hole' with a Raspberry Pi icon. The left sidebar contains a 'Status' section with system metrics and a 'MAIN NAVIGATION' menu with options like Dashboard, Query Log, Long term data, Whitelist, Blacklist, Disable, Tools, and Settings. The main content area is titled 'Block Lists' and shows a table of lists used to generate Pi-hole's Gravity.

Status

- Active Temp: 49.4 °C
- Load: 0.01 0.01 0
- Memory usage: 14.1 %

MAIN NAVIGATION

- Dashboard
- Query Log
- Long term data
- Whitelist
- Blacklist
- Disable
- Tools
- Settings

Block Lists

System | **Block Lists** | DNS | DHCP | API / Web interface | Teleporter

Lists used to generate Pi-hole's Gravity

Enabled	List
<input checked="" type="checkbox"/>	https://raw.githubusercontent.com/StevenBlack/hosts/master/hosts
<input checked="" type="checkbox"/>	https://mirror1.malwaredomains.com/files/justdomains
<input checked="" type="checkbox"/>	https://zeustracker.abuse.ch/blocklist.php?download=domainblocklist
<input checked="" type="checkbox"/>	https://s3.amazonaws.com/lists.disconnect.me/simple_tracking.txt
<input checked="" type="checkbox"/>	https://s3.amazonaws.com/lists.disconnect.me/simple_ad.txt
<input checked="" type="checkbox"/>	https://hosts-file.net/ad_servers.txt
<input checked="" type="checkbox"/>	https://hosts-file.net/grm.txt
<input checked="" type="checkbox"/>	https://zeustracker.abuse.ch/downloads/DW_DOMBL.txt

Blocklisten

- Nach Belieben erweitern...
- Windows-Telemetrie abschalten:
 - <https://github.com/crazy-max/WindowsSpyBlocker/blob/master/data/hosts/spy.txt>
 - More info: <https://github.com/crazy-max/WindowsSpyBlocker>
 - Cave: login mit „microsoft-account“ → ???
- Query-List durchschauen
 - responder.wt.heise.de (Tracker von heise.de)
 - blacklist

Clear DNS cache on a Windows System

- The DNS cache doesn't ever flush, unless you explicitly tell it to or you make a DNS/networking related configuration change. DNS records have a Time To Live (TTL) value associated with them which tells a DNS cache how long the particular record is good for. Records in the cache are kept for their TTL, then re-queried.
-
- On a Windows machine you can see a list of all the records in your cache along with their TTL by executing the following command at the command prompt:
-
- `ipconfig /displaydns`
-
- You can force a flush of all cached DNS records using the following command:
-
- `ipconfig /flushdns`

C:\> Auswählen Eingabeaufforderung - ipconfig /displaydns

```
mobile.pipe.aria.microsoft.com
```

```
-----  
Keine Einträge vom Typ AAAA
```

```
mobile.pipe.aria.microsoft.com
```

```
-----  
Eintragsname . . . . . : mobile.pipe.aria.microsoft.com  
Eintragstyp . . . . . : 1  
Gültigkeitsdauer . . . . : 159874  
Datenlänge . . . . . : 4  
Abschnitt . . . . . : Antwort  
(Host-)A-Eintrag . . . : 0.0.0.0
```

```
bn4sch101121223.wns.windows.com
```

```
-----  
Keine Einträge vom Typ AAAA
```

```
bn4sch101121223.wns.windows.com
```

```
-----  
Eintragsname . . . . . : bn4sch101121223.wns.windows.com  
Eintragstyp . . . . . : 1  
Gültigkeitsdauer . . . . : 159874  
Datenlänge . . . . . : 4  
Abschnitt . . . . . : Antwort  
(Host-)A-Eintrag . . . : 0.0.0.0
```

DNS-Cache bei Linux

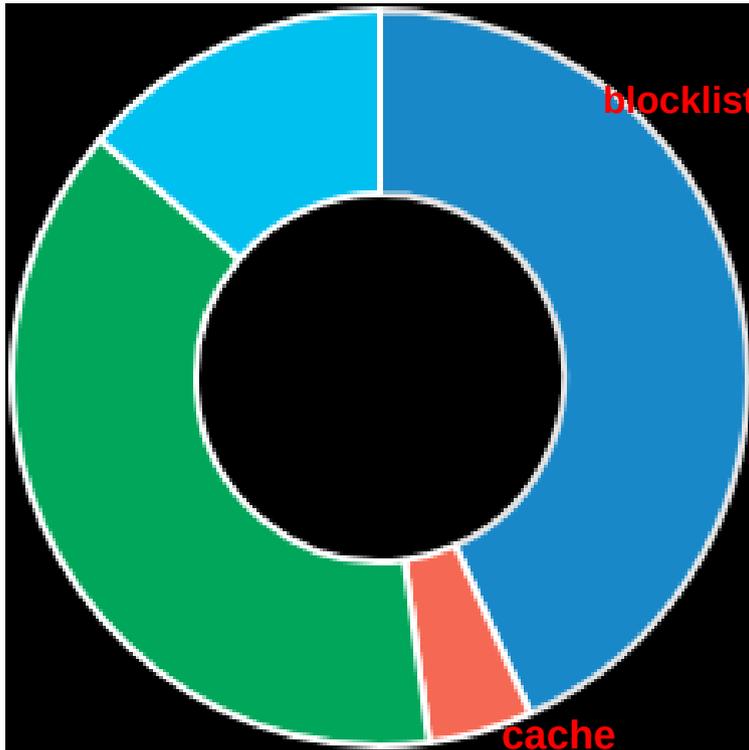
- Linux-Systeme haben keinen standardmäßigen DNS-Cache. Erst durch den Einsatz von entsprechenden Anwendungen wie nscd (Name Service Caching Daemon), pdnsd, dnsclean oder dnsmasq bieten die verschiedenen Distributionen eine Funktion, um DNS-Informationen lokal zwischenspeichern.

Wichtige Befehle

- `pihole -up`: Ein Update des Pi-hole durchführen
 - Evtl `sudo nano /etc/cron.d/pihole`
 - einfügen von:
 - `30 2 * * 7 root PATH="$PATH:/usr/local/bin/" pihole updatePihole`
- `pihole -r`: Den Konfigurator nochmal aufrufen, um bspw. Änderungen am DNS vorzunehmen
- `pihole -g`: Update der Blockierlisten anstossen
-
- `sudo shutdown -h` oder
- „Power off System“ in Admin-Panel

Statistik

- Verbrauch: 2.4 Watt / 11 mA



blocklist

cache

resolver1.opendns.com

quaternary.server.edv-froehlich.de

Speicherplatz

- /dev/root 15G 1.4G 13G 10% /
- tmpfs 464M 12M 452M 3% /run
- tmpfs 5.0M 4.0K 5.0M 1% /run/lock
- tmpfs 100M 1.8M 99M 2% /var/log
- tmpfs 100M 3.3M 97M 4% /tmp
- /dev/mmcblk0p1 44M 23M 22M 52% /boot
- Total benutzt frei Mount

Alternative Stromversorgung

- Mein Pi-Hole steht neben dem SwisscomTelefon-Router
- Der Router verfügt über eine USB-Buchse
- Kabel von Power-USB-Buchse von pi-hole zu USB-Buchse von Swisscom-Router
- Läuft!

Fazit

- Eigener DNS-Server
- Keine Werbung
- Kein Tracking
- Für alle Geräte im eigenen Netz
- Individuell konfigurierbar
- keine Microsoft-Schnüffeleien mehr