Pi-hole DNS Ad-blocking Server

Network-wide ad blocking via own Linux hardware. No client-side software required

- pi-hole Homepage

Fix Me!

Installation von Podman

Step 1 - Update the System and install Podman:

```
# yum update -y

# apt-get install docker-ce
# docker-compose version
```

Installation eines gehärteten Unbound DNS-Servers

```
# yum install unbound

# cd /etc/unbound/
# wget -O root.hints https://www.internic.net/domain/named.root
# chown unbound:unbound /etc/unbound/root.hints

# rm /etc/unbound/conf.d/example.com.conf
# echo "" > /etc/unbound/unbound.conf

# vim /etc/unbound/unbound.conf
```

```

server:
    verbosity: 1
    port: 5353
```

```
    do-ip4: yes
    do-udp: yes
    do-tcp: yes

    # May be set to yes if you have IPv6 connectivity
    do-ip6: no

    # Use this only when you downloaded the list of primary root servers!
    root-hints: "root.hints"

    # Trust glue only if it is within the servers authority
    harden-glue: yes

    # Require DNSSEC data for trust-anchored zones, if such data is absent,
the zone becomes BOGUS
    harden-dnssec-stripped: yes

    # Don't use Capitalization randomization as it known to cause DNSSEC
issues sometimes
    # see
https://discourse.pi-hole.net/t/unbound-stubby-or-dnscrypt-proxy/9378 for
further details
    use-caps-for-id: no

    # Reduce EDNS reassembly buffer size.
    # Suggested by the unbound man page to reduce fragmentation reassembly
problems
    edns-buffer-size: 1472

    # TTL bounds for cache
    cache-min-ttl: 3600
    cache-max-ttl: 86400

    # Perform prefetching of close to expired message cache entries
    # This only applies to domains that have been frequently queried
    prefetch: yes

    # One thread should be sufficient, can be increased on beefy machines
    num-threads: 1

    # Ensure kernel buffer is large enough to not loose messages in traffic
spikes
    so-rcvbuf: 1m

    # Ensure privacy of local IP ranges
    private-address: 192.168.0.0/16
    private-address: 10.0.0.0/8
```

```
# systemctl restart unbound
# systemctl status unbound
```

```
# sealert -a /var/log/audit/audit.log
# ausearch -c 'unbound' --raw | audit2allow -M my-unbound
# semodule -X 300 -i my-unbound.pp

# systemctl restart unbound
# systemctl status unbound

# netstat -tulpn
# dig blackgate.org @127.0.0.1 -p 5353

// ------------------------- TESTING VON DNS-SEC: ------------------------
-
# dig sigfail.verteiltesysteme.net @127.0.0.1 -p 5353
# dig sigok.verteiltesysteme.net @127.0.0.1 -p 5353

# systemctl enable unbound
```

Einrichten und Deployment von pi-hole

Erstellen der benötigten Files und Verzeichnisse

```
# mkdir /opt/podman-pihole
# mkdir /opt/podman-pihole/pihole
# mkdir /opt/podman-pihole/dnsmasq.d
```

Optional: blackGATE custom design! **Achtung:** falls das custom-design nicht gewünscht wird, die ERSTE markierte Zeile im docker_compose.yml WEGLASSEN sowie auch nachfolgende File und den Ordner nicht erstellen.

```
# mkdir /opt/docker-pihole/adminCMS
# vim /opt/docker-pihole/adminCMS/pi-hole.css
```

```
/* Pi-hole: A black hole for Internet advertisements
*  (c) 2017 Pi-hole, LLC (https://pi-hole.net)
*  Network-wide ad blocking via your own hardware.
*  CSS BY MICHU!!!
*  This file is copyright under the latest version of the EUPL.
*  Please see LICENSE file for your rights under this license. */

/* --------------------------blackGATE RULES-------------------------------
----*/
/* BACKGROUND:*/
body {
    background-color: #232323 !important;
}
```

```
.layout-boxed {
    background: url(https://www.blackgate.org/wood.jpg) !important;
}


/* PAGE FORMATING:*/
.skin-blue .main-header .logo {
    background-color: #4a4a4a !important;
}
.skin-blue .main-header .navbar {
    background-color: #383838 !important;
}
.skin-blue .wrapper, .skin-blue .main-sidebar, .skin-blue .left-side {
    background-color: #2b2b2b !important;
}
.skin-blue .sidebar-menu>li.header {
    color: #717171 !important;
    background: #212121 !important;
}
.skin-blue .sidebar-menu>li:hover>a, .skin-blue .sidebar-menu>li.active>a {
    color: #fff;
    background: #383838 !important;
    border-left-color: #b7babb !important;
}
.skin-blue .sidebar-menu>li>.treeview-menu {
    background: #232323 !important;
}
.box {
    background: #eaeaea !important;
    border-top: 3px solid #989898 !important;
    box-shadow: 0 1px 1px rgba(14, 14, 14, 0.31) !important;
}
.box-header.with-border {
    border-bottom: 1px solid #d2d2d2 !important;
}
.table-bordered>thead>tr>th, .table-bordered>tbody>tr>th, .table-
bordered>tfoot>tr>th, .table-bordered>thead>tr>td, .table-
bordered>tbody>tr>td, .table-bordered>tfoot>tr>td {
    border: 1px solid #cecece !important;
}
.skin-blue .main-header li.user-header {
    background-color: #4a4a4a !important;
}
.navbar-nav>.user-menu>.dropdown-menu>.user-body {
    border-bottom: 1px solid #b1b1b1 !important;
    border-top: 1px solid #cecece !important;
}

/* DELETE SOME STUFF:*/
.navbar-nav>.user-menu>.dropdown-menu>.user-footer {
    display: none;
```

```
}
#loginform>.row>.col-xs-12>.box.box-solid.box-info {
    display: none;
}

/*.sidebar-menu>li:last-child {
    display: none;
}*/


/* ---------------------------- START of Default RULES (minified) -----------
-------------------------*/
.small-box{cursor:default;-webkit-user-select:none;-moz-user-select:none;-
ms-user-select:none;-o-user-select:none;user-select:none}.skin-blue .list-
group-item:hover{background:#ddd}@-webkit-keyframes
Pulse{from,to{color:#630030;-webkit-text-shadow:0 0 2px
transparent}50%{color:#e33100;-webkit-text-shadow:0 0 5px
#e33100}}@keyframes Pulse{from,to{color:#630030;text-shadow:0 0 2px
transparent}50%{color:#e33100;text-shadow:0 0 5px #e33100}}a.lookatme{-
webkit-animation-name:Pulse;animation-name:Pulse;-webkit-animation-
duration:2s;animation-duration:2s;-webkit-animation-iteration-
count:infinite;animation-iteration-count:infinite}.table-responsive{-webkit-
overflow-scrolling:touch}#all-queries td:nth-of-type(1),#all-queries td:nth-
of-type(5){white-space:nowrap}#all-queries td:nth-of-type(3){min-
width:200px;word-break:break-all;white-space:pre-wrap}#all-
queries_info{white-space:unset}#all-queries_wrapper
.pagination>li>a{padding-left:6px;padding-right:6px;min-width:34px;text-
align:center}@media screen and (max-width:500px),screen and (min-
width:767px) and (max-width:1000px){#all-queries_wrapper
.pagination>li.next,#all-queries_wrapper
.pagination>li.previous{display:none}#all-queries_wrapper
.pagination>li:nth-of-type(2) a{border-top-left-radius:4px;border-bottom-
left-radius:4px}#all-queries_wrapper .pagination>li:nth-last-of-type(2)
a{border-top-right-radius:4px;border-bottom-right-radius:4px}}.main-
header>.navbar{height:50px}#resetButton{color:red;font-weight:700}.vertical-
alignment-helper{display:table;width:100%;height:100%;pointer-
events:none}.vertical-alignment-helper>.vertical-align-center{display:table-
cell;vertical-align:middle}.vertical-alignment-helper>.vertical-align-
center>.modal-content{width:250px;margin-left:auto;margin-right:auto;word-
wrap:break-word;pointer-
events:all}.alSpinner{top:.1em;left:.1em;width:.8em;height:.8em;border-
radius:50%;border:4px solid silver;border-right-color:transparent;-webkit-
animation:fa-spin 1s infinite linear;animation:fa-spin 1s infinite linear}
/* ---------------------------- END of Default RULES (minified) -------------
-----------------------*/
```

END of Optional

Optional 2: Set Local-Services (FQDN) to Server via DNS!

```
# vim /opt/podman-pihole/dnsmasq.d/localNET.conf
```

```
address=/MYMAINPAGE.ch/192.168.99.11
address=/www.MYMAINPAGE.ch/192.168.99.11
address=/analytics.MYMAINPAGE.ch/192.168.99.11
address=/test.MYMAINPAGE.ch/192.168.99.11
```

END of Optional 2

Anlegen des docker-compose file für pi-hole

Das verwendete Image ist ausschlisslich für x86_x64 Systeme geeignet. Soll Pi-hole auf einem ARM basierten System dokerisiert installiert werden, so kann für das richtige Image HIER geschaut werden.

Wichtig: Alle im **pi-hole-container.service** File markierten Stellen sind zu kontrollieren oder bei Nichtübereinstimmung mit dem eigenen System anzupassen!

```
# vim /etc/systemd/system/pi-hole-container.service
```

```
[Unit]
Description=Pi-Hole-Container
After=network.target

[Service]
Type=simple
TimeoutStartSec=60s

ExecStartPre=-/usr/bin/podman rm "pihole-server"
ExecStart=/usr/bin/podman run --name pihole-server --net=host -e
VIRTUAL_HOST=www.cibolini.ch -e ServerIP=192.168.99.11 -e
DNS1=127.0.0.1#5353 -e DNS2=no -e TZ=Europe/Zurich -e
WEBPASSWORD=MYPASSWORT1234 -e WEB_PORT=82 -e INTERFACE=eno5 -v /opt/podman-
pihole/pihole/:/etc/pihole/:Z -v /opt/podman-
pihole/dnsmasq.d/:/etc/dnsmasq.d/:Z -v /etc/localtime:/etc/localtime:ro
pihole/pihole:latest

ExecReload=-/usr/bin/podman stop "pihole-server"
ExecReload=-/usr/bin/podman rm "pihole-server"

ExecStop=-/usr/bin/podman stop "pihole-server"
Restart=always
RestartSec=30

[Install]
WantedBy=multi-user.target
```

Erklärung zu den Environment Variablen:

- **VIRTUAL_HOST**: Die FQND von welcher später via Web-GUI auf das Pi-hole zugegriffen werden soll.
- **ServerIP**: Die Server IP-Adresse des Docker-Hosts. (Ausserhalb des Containers)
- **DNS1**: Standard Upstream-DNS-Server von Pi-hole.
- **WEBPASSWORD**: Repräsentiert das admin-Passwort welches benötigt wird um sich am Web-GUI anzumelden.
- **WEB_PORT**: Der Port auf welchem der Server das Admin-GUI ausliefert.
- **INTERFACE**: Das Host-Interface. (**Wichtig wenn Standard nicht eth0**)

Starten und testen des pi-hole Docker Containers

```
# docker-compose -f /opt/docker-pihole/docker_compose.yml up -d
# docker ps -a
```

Weiteres

Wiederherstellen der alten pi-hole Konfiguration (Stand: 06.11.2018)

```
# docker-compose -f /opt/docker-pihole/docker_compose.yml down
# vim /opt/docker-pihole/dnsmasq.d/01-pihole.conf
```

```
# Pi-hole: A black hole for Internet advertisements
# (c) 2015, 2016 by Jacob Salmela
# Network-wide ad blocking via your Raspberry Pi
# http://pi-hole.net
# dnsmasq config for Pi-hole
#
# Pi-hole is free software: you can redistribute it and/or modify
# it under the terms of the GNU General Public License as published by
# the Free Software Foundation, either version 2 of the License, or
# (at your option) any later version.

##############################################################################
####
#      FILE AUTOMATICALLY POPULATED BY PI-HOLE INSTALL/UPDATE PROCEDURE.
#
# ANY CHANGES MADE TO THIS FILE AFTER INSTALL WILL BE LOST ON THE NEXT
UPDATE #
#
#
#        IF YOU WISH TO CHANGE THE UPSTREAM SERVERS, CHANGE THEM IN:
```

```
#
#                      /etc/pihole/setupVars.conf
#
#
#
#        ANY OTHER CHANGES SHOULD BE MADE IN A SEPERATE CONFIG FILE
#
#                         OR IN /etc/dnsmasq.conf
#
################################################################################
####

addn-hosts=/etc/pihole/gravity.list
addn-hosts=/etc/pihole/black.list
addn-hosts=/etc/pihole/local.list


localise-queries


no-resolv



cache-size=10000

log-queries=extra
log-facility=/var/log/pihole.log

local-ttl=2

log-async
server=127.0.0.1#5353
domain-needed
bogus-priv
interface=enp1s0
server=/fritz.box/192.168.1.1
server=/1.168.192.in-addr.arpa/192.168.1.1
```

```
# vim /opt/docker-pihole/pihole/blacklist.txt
```

```


bvadtgs.scdn1.secure.raxcdn.com
4b6994dfa47cee4.com
metrics.plex.tv
gebadu.com
pl4518712.puserving.com
```

```
analytics.ff.avast.com
p5-3os3pimkl6tg2-ixzsvd47ghupqap6-659208-i1-v6exp3.ds.metric.gstatic.com
```

```
# vim /opt/docker-pihole/pihole/whitelist.txt
```

```
raw.githubusercontent.com
mirror1.malwaredomains.com
sysctl.org
zeustracker.abuse.ch
s3.amazonaws.com
hosts-file.net
serials.ws
www.serials.ws
www.googleadservices.com
platform.linkedin.com
cdn.ravenjs.com
public-assets.envato-static.com
ipm-provider.ff.avast.com
www.smartredirect.de
```

```
# vim /opt/docker-pihole/pihole/setupVars.conf
```

```
DHCP_START=192.168.1.180
DHCP_END=192.168.1.250
DHCP_ROUTER=192.168.1.1
DHCP_LEASETIME=48
PIHOLE_DOMAIN=local
DHCP_IPv6=true
DHCP_ACTIVE=false
DNS_FQDN_REQUIRED=true
DNS_BOGUS_PRIV=true
DNSSEC=false
CONDITIONAL_FORWARDING=true
CONDITIONAL_FORWARDING_IP=192.168.1.1
CONDITIONAL_FORWARDING_DOMAIN=fritz.box
CONDITIONAL_FORWARDING_REVERSE=1.168.192.in-addr.arpa
PIHOLE_DNS_1=127.0.0.1#5353
PIHOLE_DNS_2=
QUERY_LOGGING=true
INSTALL_WEB_SERVER=true
```

```
INSTALL_WEB_INTERFACE=true
LIGHTTPD_ENABLED=
IPV4_ADDRESS=192.168.1.2
IPV6_ADDRESS=
WEBPASSWORD=d295e1c88d5494f1f40cce9be08428e73a79792d37f4ffa6100ac283901479a
a
PIHOLE_INTERFACE=enp1s0
```

```
# docker-compose -f /opt/docker-pihole/docker_compose.yml up -d
# docker ps
```

Reverse Proxy Setup Beispiel

```
# vim /etc/httpd/conf.d/proxy_https.conf
```

```
define serveradmin "michael.r467@gmail.com"
define ssl_path "/etc/letsencrypt/live/analytics.cibolini.ch"

Protocols h2 h2c http/1.1

SSLProtocol -All +TLSv1.2 +TLSv1.3
SSLCipherSuite      ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-
POLY1305:EECDH+AESGCM:EDH+AESGCM
SSLCipherSuite      TLSv1.3
TLS_CHACHA20_POLY1305_SHA256:TLS_AES_128_GCM_SHA256:TLS_AES_256_GCM_SHA384

<VirtualHost *:443>
 ServerName www.MYMAINPAGE.ch
 #
     ServerAdmin ${serveradmin}
     SSLEngine on
     SSLCertificateFile ${ssl_path}/cert.pem
     SSLCertificateKeyFile ${ssl_path}/privkey.pem
     SSLCertificateChainFile ${ssl_path}/chain.pem

     RewriteEngine on
     RewriteRule ^/pi-hole$ /pi-hole/ [R]

     DocumentRoot /var/www/html/MYMAINPAGE

     <Directory "/var/www/html/MYMAINPAGE">
             Options -Indexes +FollowSymLinks
             AllowOverride None
             Require all granted
     </Directory>
```

```
    ProxyPass          /pi-hole/ http://localhost:82/admin/
    ProxyPassReverse   /pi-hole/ http://localhost:82/admin/
</VirtualHost>
```

Last update: **2020/02/24 15:47**