

Pi-Hole

Docker-compose :

```
version: "3"

# More info at https://github.com/pi-hole/docker-pi-hole/ and https://docs.pi-hole.net/
services:
  pihole:
    container_name: pihole
    image: pihole/pihole:latest
    # For DHCP it is recommended to remove these ports and instead add: network_mode: "host"
    # network_mode: host
    ports:
      - 53:53/tcp
      - 53:53/udp
      #- 67:67/udp # Only required if you are using Pi-hole as your DHCP server
      - 56880:80/tcp
    environment:
      TZ: Europe/Paris
      WEBPASSWORD: password
      WEBTHEME: default-darker
      # WEB_PORT: 5400 # En cas de networkmode: host
    # Volumes store your data between container upgrades
    volumes:
      - data:/etc/pihole
      - dnsmasq:/etc/dnsmasq.d
    # https://github.com/pi-hole/docker-pi-hole#note-on-capabilities
    #cap_add:
    # - NET_ADMIN # Required if you are using Pi-hole as your DHCP server, else not needed
    restart: unless-stopped

volumes:
  data:
  dnsmasq:
```

Liste de blocage :

Liste par défaut :

<https://raw.githubusercontent.com/StevenBlack/hosts/master/hosts>

Liste que j'ai rajouté :

<https://easylist.to/easylist/easylist.txt> ☐ easylist
<https://github.com/uBlockOrigin/uAssets/raw/master/filters/filters-2020.txt> ☐ Ublock filters
<https://github.com/uBlockOrigin/uAssets/raw/master/filters/filters-2021.txt> ☐ Ublock filters
<https://github.com/uBlockOrigin/uAssets/raw/master/filters/filters-2022.txt> ☐ Ublock filters
<https://github.com/uBlockOrigin/uAssets/raw/master/filters/filters-2023.txt> ☐ Ublock filters
<https://github.com/uBlockOrigin/uAssets/raw/master/filters/filters.txt> ☐ Ublock filters
<https://github.com/uBlockOrigin/uAssets/raw/master/filters/badware.txt> ☐ Ublock Badware
<https://github.com/uBlockOrigin/uAssets/raw/master/filters/privacy.txt> ☐ Ublock Privacy
<https://github.com/uBlockOrigin/uAssets/raw/master/filters/quick-fixes.txt> ☐ Ublock Quick Fixes
<https://github.com/uBlockOrigin/uAssets/raw/master/filters/resource-abuse.txt> ☐ Ublock Resource-abuse
<https://github.com/uBlockOrigin/uAssets/raw/master/filters/unbreak.txt> ☐ Ublock unbreak
<https://easylist.to/easylist/easyprivacy.txt> ☐ easyprivacy
<https://malware-filter.gitlab.io/malware-filter/urlhaus-filter-domains.txt> ☐ Online Malicious URL Blocklist
<https://pgl.yoyo.org/adserver/serverlist.php?hostformat=hosts> ☐ Ublock Peter Lowe's Ad and tracking server list

Wireguard :

Comme expliquer dans WireGuard, voici le compose pour Pi-Hole :

```
version: "3"

# More info at https://github.com/pi-hole/docker-pi-hole/ and https://docs.pi-hole.net/
services:
  pihole:
    container_name: pihole
    image: pihole/pihole:latest
    # For DHCP it is recommended to remove these ports and instead add: network_mode: "host"
    # network_mode: host
```

```
ports:
- 53:53/tcp
- 53:53/udp
# - 67:67/udp # Only required if you are using Pi-hole as your DHCP server
- 56880:80/tcp
environment:
  TZ: Europe/Paris
  WEBPASSWORD: password
  WEBTHEME: default-darker
# WEB_PORT: 5400 # En cas d'utilisation de network_mode: host
# Volumes store your data between container upgrades
networks:
  dns_network:
    ipv4_address: 192.168.12.2
volumes:
- data:/etc/pihole
- dnsmasq:/etc/dnsmasq.d
# https://github.com/pi-hole/docker-pi-hole#note-on-capabilities
#cap_add:
# - NET_ADMIN # Required if you are using Pi-hole as your DHCP server, else not needed
restart: unless-stopped
volumes:
  data:
  dnsmasq:
networks:
  dns_network:
    name: dns_network
    driver: bridge
  ipam:
    config:
      - subnet: 192.168.12.0/24
```

Revision #4

Created 31 March 2023 18:27:02 by Julien

Updated 19 February 2024 20:12:13 by Julien