

Pi-hole vs AdGuard Home on Proxmox: Comparison Sheet

Features, install method, DHCP, encrypted DNS and privacy side by side, with a clear pick for each type of user.

Updated **2026-10-29** · Full guide: www.mrplanb.com/blog/pi-hole-vs-adguard-home-on-proxmox-which-dns-blocker-is-better

Both Pi-hole and AdGuard Home block ads and trackers network-wide and run comfortably in a small LXC container on Proxmox. Pi-hole suits you if you want a large community, clear query visibility and flexible blocklists. AdGuard Home suits you if you want encrypted DNS, parental controls and per-client settings built in. Run two instances on separate nodes, because DNS is critical.

2

DNS blockers compared

4

encrypted DNS protocols
AdGuard Home supports:
DoH, DoT, DoQ, DNSCrypt

2

instances recommended, on
separate Proxmox nodes

LXC

recommended Proxmox
platform for either one

Side-by-side comparison

	Pi-hole	AdGuard Home
Community	Larger, extensive documentation	Smaller community
Dashboard	Query log, top blocked domains, long-term SQLite stats	Query stats, client activity, upstream performance
Client policies	Groups of clients and domains, regex rules	Per-client by IP, subnet or encrypted DNS ID
Parental, safe search, malware lists	Possible with extra lists and rules	Built in
Encrypted DNS	Standard upstreams; pair with extra tools	DoH, DoT, DoQ, DNSCrypt, upstream and server
Install	Automated installer on Debian, Ubuntu, Alpine	Standalone binary registered as a service
DHCP	Built in; disable router DHCP first	Built in; needs a static address

Deploy it on Proxmox

- 1 Create a small unprivileged Debian LXC container with a static IP address.
- 2 Install Pi-hole with its installer, or unpack and register the AdGuard Home binary as a service.
- 3 Add blocklists, allowlists and any client or group rules.
- 4 Set the upstream DNS: standard, encrypted, or a local Unbound resolver.
- 5 Hand the DNS address to clients through DHCP.
- 6 Back up the whole LXC in Proxmox and export the application configuration separately.

- 7 Repeat on a second node and give clients both addresses.

Reliability and update checklist

- ☐ Use a static IP on the DNS container.
- ☐ Run two instances on separate Proxmox nodes or physical systems.
- ☐ Do not put both instances on the same Proxmox host.
- ☐ Disable DHCP on the router before enabling a DHCP server on Pi-hole.
- ☐ Read release notes before updating Pi-hole, especially across major versions.
- ☐ Keep a Proxmox backup plus a separate application configuration export.
- ☐ Prefer a native install in LXC over Docker for a single DNS service.

Privacy options

Pi-hole privacy levels

Keep full detail, hide domains, hide clients, or disable most long-term query analysis.

AdGuard Home logging

Query logging with configurable retention and encrypted upstreams without extra software.

Pi-hole with Unbound

Local recursive resolver, so unblocked queries do not all go to one public provider. One more service to maintain.

Limits of encryption

The chosen upstream provider still receives requests, and destinations may be inferred from other traffic.

Which one to pick

- Pi-hole: mature community, troubleshooting resources, flexible blocklists, Unbound for recursion.
- AdGuard Home: encrypted DNS, parental controls, safe search and per-client settings in one application.
- First-time Proxmox users: Pi-hole is usually the familiar, well-documented option.
- More DNS privacy without assembling several tools: AdGuard Home.
- Best test: deploy both in temporary LXC containers and compare dashboards, client identification and blocking.

Sources and notes: Pi-hole documentation, as summarized on the page · AdGuard Home documentation, as summarized on the page · Proxmox VE LXC guidance