Raspberry Pi mit AdguardHome in einem eigenen VLAN

Vorteile eines eigenen VLANs für AdGuard Home/den DNS-Server

- Sicherheit und Abgrenzung: DNS-Server ist von IoT-Geräten getrennt, falls dort Kompromittierungen auftreten.

- Einfacheres Monitoring/Logging: DNS-Verkehr getrennt, leichter zu analysieren.

- Kontrollen und Richtlinien: Schnellere Umsetzung von Filtering-Policies, Blacklists etc. ohne andere Geräte zu beeinflussen.

- Stabilität und Performance: Geringere Broadcast-Stürme im Kernel/Netzwerkpfad, evtl. geringere Latenzen bei DNS-Anfragen von Clients im VLAN.

- Leichte Wartung: Zentralisierte DNS-Konfiguration, einfache Änderungen am Upstream (DoH/DoT) ohne Router-Änderungen.

Was zu beachten ist

- Netzwerk-Topologie: Dein Router/Firewall muss VLANs unterstützen und DNS-Anfragen zwischen VLANs sinnvoll weiterleiten (Inter-VLAN-Routing) oder zumindest clientspezifisch auf das DNS im VLAN verweisen.

- DNS-Verlässlichkeit: Richte eine stabile Weitergabe der Clients auf den AdGuard-Home-Server ein (DHCP-Optionen oder Router-Einstellungen, die DNS auf den Pi zeigen). Stelle sicher, dass kein DHCP-Server im selben VLAN konkurriert.

- Upstream-Verbindung: Lege fest, wie AdGuard Home Upstream-Anfragen außerhalb deines VLANs erreicht (DoH/DoT oder traditionelle Upstream-Resolver). Achte auf Privacy/Performance.

- Sicherheit des Raspberry Pi: Halte das System aktuell, schränke SSH/Remote-Zugriffe ein, nutze eine statische IP oder DHCP-Lease im VLAN, sichere Ports.

- Redundanz/Verfügbarkeit: Falls du Hochverfügbarkeit willst, plane ggf. Failover oder einen zweiten DNS-Server in einem separaten VLAN.

- DNS-Übermittlung an Clients: Du kannst entweder DHCP im VLAN so konfigurieren, dass die Clients den Pi als DNS-Server bekommen, oder auf dem Router eine Weitergabe/Override der DNS-Server-Adresse implementieren.

- NAT/Firewall: Stelle sicher, dass Anfragen korrekt durchgereicht werden und keine Blockaden durch Firewalls entstehen.

Praktische Umsetzung (grob)

- VLAN anlegen (z. B. VLAN 20) und AdGuard Home auf dem Raspberry Pi installieren.

- Pi im VLAN 20 platzieren (Zugriffskonfiguration, statische IP oder DHCP-Reservierung).

- AdGuard Home konfigurieren: DNS-Listener nur auf der VLAN-Schnittstelle aktiv, Upstream so einstellen, wie gewünscht (unverschlüsselt oder DoH/DoT).

- Clients konfigurieren: Entweder per DHCP-Option auf dem Router/ DHCP-Server oder manuell auf den Geräten, dass sie DNS-Server = Pi-IP im VLAN 20 verwenden.

- Optional: DoH/DoT aktivieren, Logging/Blocklisten konfigurieren, ggf. Filterlisten regelmäßig aktualisieren.

- Monitoring: Logs regelmäßig prüfen, Ressourcen (CPU/RAM) auf dem Pi überwachen, Backup der Konfiguration.

Alternative/Ergänzungen

- Wenn du mehrere VLANs oder Systeme isolieren willst, könntest du auch AdGuard Home in einem dedizierten Container/VM betreiben (z. B. Docker) – auf dem Pi oder einem kleinen Server – und nur der DNS-Verkehr geht ins VLAN.

- Für besonders hohe Anforderungen oder zentrale Verwaltung in größeren Netzwerken lohnt sich ggf. ein dediziertes DNS- oder Firewall-Gateway-Gerät statt eines Raspberry Pi, aber für Heimanwender oft ausreichend.

Fazit

- Ja, sinnvoll: Ein eigener VLAN für AdGuard Home erhöht Sicherheit und Kontrolle, ohne nennenswerten Nachteil bei einer ordentlichen Konfiguration (Routing/ DHCP-Verteilung). Achte auf klare DNS-Verteilung, Upstream-Einstellungen und regelmäßige Wartung.