
HomeLab

Samostalno posluživanje servisa

Poglavlje 13 — Skripta kolegija *Računalne mreže*

doc. dr. sc. Sandi Baressi Šegota

Fakultet informatike Sveučilišta Jurja Dobrile u Puli

Poglavlje 13

HomeLab: samostalno posluživanje servisa

HomeLab je vlastita okolina — najčešće poslužitelj kod kuće — na kojoj sami pokrećemo servise koje inače nudi oblak. Motivi su *privatnost* (podaci ostaju kod nas), *kontrola* nad servisima, *učenje* (mreže, Linux, kontejneri) te moguća ušteda na pretplatama. Ovo završno poglavlje povezuje gradivo cijelog kolegija u jedan praktičan projekt: od aplikacijskih servisa i DNS-a, preko mreže i sigurnosti, do kontejnera i reverse proxyja.

Ishodi učenja

Po završetku poglavlja student će moći: objasniti pojam HomeLaba i self-hostinga; odabrati hardver i pokrenuti servise u Dockeru (docker-compose); postaviti Pi-hole, Nextcloud i Jellyfin; objasniti reverse proxy i WireGuard; te primijeniti dobre prakse sigurnosti i sigurnosnog kopiranja.

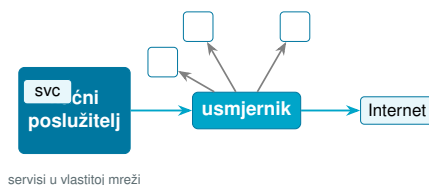


Figure 13.1: HomeLab: vlastiti poslužitelj sa servisima u kućnoj mreži.

13.1 Hardver, OS i Docker

Za HomeLab je dovoljan skroman hardver: *Raspberry Pi* (tih i niske potrošnje), *mini PC* ili stari računalno (više snage) te *NAS* (naglasak na pohrani). Operativni sustav je najčešće **Linux** (npr. Debian ili Ubuntu) zbog stabilnosti i podrške, a njime se obično upravlja daljinski putem *SSH*-a.

Temelj modernog HomeLaba je **Docker**: svaki se servis pokreće u vlastitom *kontejneru*, čime se postiže izolacija, jednostavno instaliranje i ažuriranje te čist sustav bez sukoba ovisnosti. Više servisa opisuje se u jednoj datoteci **docker-compose.yml** i pokreće jednom naredbom, što cijelo postavljanje čini preglednim i ponovljivim. Budući da su kontejneri prolazni, trajni podaci (baze, konfiguracija, mediji) čuvaju se u *volumenima*, dok kontejneri međusobno komuniciraju internom Docker mrežom i pronalaze se po imenu servisa.

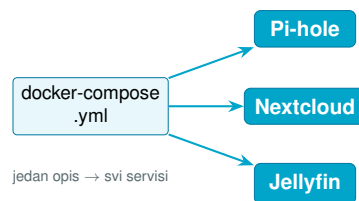


Figure 13.2: Jedna docker-compose datoteka opisuje i pokreće sve servise.

13.2 Popularni servisi

Među najčešćim servisima su **Pi-hole**, **Nextcloud** i **Jellyfin**. *Pi-hole* je DNS poslužitelj za cijelu mrežu koji blokira reklame i pratitelje na razini DNS upita, čime ubrzava i čisti pregledavanje na svim uređajima.

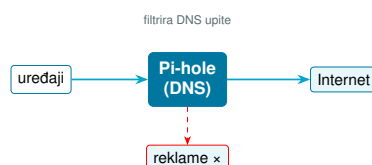


Figure 13.3: Pi-hole filtrira DNS upite i blokira reklame za cijelu mrežu.

Nextcloud je osobni oblak za datoteke sa sinkronizacijom među uređajima (uz kalendar, kontakte i dijeljenje), a *Jellyfin* je besplatan medijski poslužitelj za streaming filmova, glazbe i fotografija na sve uređaje u kući. Uz njih se često pokreću i drugi servisi.

servis	uloga
Pi-hole	DNS i blokiranje reklama za cijelu mrežu
Nextcloud	osobni oblak, sinkronizacija datoteka
Jellyfin	medijski poslužitelj (streaming)
Vaultwarden	upravitelj lozinki
Home Assistant	automatizacija pametnog doma

Table 13.1: Neki popularni self-hosted servisi.

13.3 Pristup, mreža i sigurnost

Kako bi se s više servisa pristupilo preko jedne ulazne točke, koristi se **reverse proxy**: on prima sve zahtjeve i usmjerava ih prema odgovarajućem servisu na temelju *domene*, uz centralizirano upravljanje **HTTPS**-om (besplatni certifikati, npr. *Let's Encrypt*, uz automatsku obnovu).

Za siguran daljinski pristup preporučuje se **WireGuard** — brz i jednostavan VPN koji uspostavlja šifrirani tunel do kućne mreže. Budući da se kućna javna IP adresa mijenja, *dinamički DNS* (DDNS) veže stalno ime uz trenutnu adresu. Ključno sigurnosno načelo jest *ne* izlagati servise izravno Internetu otvaranjem portova (što ih čini metom automatiziranih napada), nego im pristupati kroz VPN, uz jake lozinke i višefaktorsku autentikaciju.

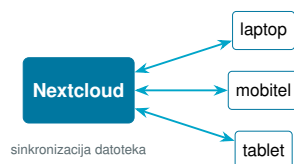


Figure 13.4: Nextcloud sinkronizira datoteke među svim korisnikovim uređajima.

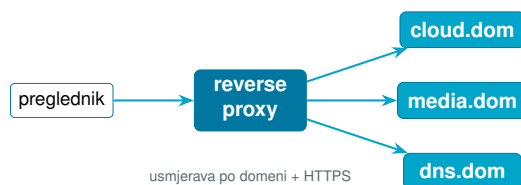


Figure 13.5: Reverse proxy usmjerava po domeni i pruža jedinstveni HTTPS ulaz.

13.4 Održavanje

Pouzdan HomeLab zahtijeva **sigurnosne kopije** po pravilu 3-2-1 (tri kopije, na dva medija, jedna izvan lokacije), redovito i automatski, uz povremenu provjeru obnove. Nužno je i redovito *ažurirati* operativni sustav i kontejnere te pratiti sigurnosne zakrpe, a održavanje se dobrim dijelom može *automatizirati* (zakazani zadaci, alati za automatsko ažuriranje). Konačno, korisno je *nadzirati* resurse (CPU, RAM, disk) i imati dokumentiran *plan oporavka* prije nego zatreba.

Sažetak poglavlja i kolegija

HomeLab je vlastiti poslužitelj na kojem **Docker** i *docker-compose* čine pokretanje servisa jednostavnim i ponovljivim. Popularni servisi su **Pi-hole**, **Nextcloud** i **Jellyfin**, a siguran pristup omogućuju **reverse proxy** (HTTPS) i **WireGuard** (VPN). *Backup* (3-2-1) i redovita ažuriranja temelj su pouzdanosti. HomeLab objedinjuje cijeli kolegij — aplikacijski sloj, mreže, sigurnost i oblak — u jednom praktičnom projektu.



Figure 13.6: WireGuard: šifrirani pristup kućnoj mreži s udaljenog uređaja.



Figure 13.7: Sigurnosno kopiranje po pravilu 3-2-1.