Predstavitev protokola LDAP

Urban Gajšek

7. marec 2025

Kazalo

1 Kaj je LDAP?

Lightweight Directory Access Protocol (LDAP) je odprt aplikacijski protokol za upravljanje in dostop do imenikov storitev (Directory Service) preko IP omrežja.

LDAP je odprt, ker je javno dostopen in definiran v RFC (Request for Comments) dokumentih. Vsak ga lahko implementira, uporablja ali razvija brez licence. Protokol je neodvisen od ponudnikov in platform, kar pomeni, da deluje na različnih operacijskih sistemih in napravah. Kot aplikacijski protokol deluje na aplikacijski plasti (7. plast OSI modela) preko TCP/IP omrežja. Razvit je bil kot lažja alternativa protokolu DAP (Directory Access Protocol), ki je del standarda X.500.

1.1 Namen in uporaba protokola LDAP

Glavni namen LDAP je standardiziran dostop do in upravljanje imenikov storitev preko omrežja. Uporablja se za:

- Centralizirano avtentikacijo,
- Upravljanje uporabnikov in njihovih pravic,
- Pridobivanje podatkov o raznih objektih iz imenika.

1.2 Imenik storitev (Directory Service)

Imenik storitev je specializirana baza podatkov, ki hrani informacije o objektih v drevesni strukturi. Objekti so lahko uporabniki, skupine, naprave, aplikacije itd. Podatki v imeniku so pogosto dostopani in redko spreminjani (npr. imena, telefonske številke, gesla, elektronski naslovi itd.).

Primeri imenikov storitev: Microsoft Active Directory, OpenLDAP, ApacheDS.

1.2.1 Zgradba LDAP imenika

LDAP imenik je organiziran hierarhično kot drevo. Vozlišča drevesa so objekti, katerih struktura je definirana v shemi. Vsak objekt ima svoj edinstven Distinguished Name (DN), ki ga sestavljajo imena vseh nadrejenih objektov in lastno ime.

Primer DN:

```
dc=example,dc=com,ou=administracija,cn=Janez
```

(Domena `example.com`, skupina `administracija`, oseba `Janez`).

2 Delovanje protokola LDAP

2.1 Akterji v protokolu LDAP

Glavna akterja v LDAP protokolu sta:

- **LDAP strežnik** - hrani in upravlja vnose v imeniku.
- **LDAP odjemalec** - poizveduje in prejema odgovore od strežnika (npr. e-poštni strežnik, brskalnik, aplikacija za upravljanje uporabnikov).

2.2 Potek komunikacije

LDAP deluje po modelu strežnik-odjemalec:

1. Odjemalec vzpostavi povezavo s strežnikom.
2. Pošlje zahteve za podatke ali spremembe.
3. Strežnik obdela zahtevo in vrne odgovor.
4. Po končani komunikaciji se povezava prekine.

LDAP povezave same po sebi niso kriptirane, zato je za varnost priporočljiva uporaba TLS.

2.2.1 Vrste LDAP operacij

LDAP podpira več vrst operacij:

- **Add** - doda nov vnos v imenik.
- **Bind** - avtentikacija uporabnika.
- **Delete** - izbriše vnos iz imenika.
- **Search and compare** - iskanje in primerjava vnosov.
- **Modify** - spreminjanje obstoječih vnosov.
- **Modify DN** - spreminjanje DN obstoječega vnosa.

3 Primeri uporabe protokola LDAP

Ena najpogostejših uporab LDAP je avtentikacija uporabnikov v podjetjih.

Predstavljajmo si scenarij, kjer podjetje z več sto zaposlenimi uporablja LDAP za upravljanje dostopa do internih aplikacij (e-pošta, kadrovski portal, intranet itd.). Namesto da bi vsaka aplikacija shranjevala uporabniške podatke ločeno, se uporablja centraliziran LDAP strežnik (npr. Microsoft Active Directory).

Potek avtentikacije:

1. Zaposleni vnese uporabniško ime in geslo v kadrovski portal.
2. Portal pošlje zahtevo za avtentikacijo LDAP strežniku.
3. LDAP strežnik preveri podatke v svoji bazi.
4. Če so podatki pravilni, uporabnik dobi dostop; sicer je dostop zavrnjen.