Kako promijeniti konfiguraciju openldap-a?

VAŽNO: promjene koje radite u konfiguraciji LDAP-a mogu dovesti do prekida rada vašeg LDAP poslužitelja i time onemugućiti autentikaciju korisnika. Sve promjene koje radite radite na vlastitu odgovornost. Ne radite promjene ako niste sigurni u to što radite.

Verzija openldap-a koja dolazi u paketu openldap-aai ima tzv. dinamičku konfiguraciju (konfiguraciju drži u memoriji zajedno s podacima u grani cn=config).

Sve promjene u konfiguraciji zato je potrebno obaviti LDAP klijentom (npr. naredbom ldapmodify uz odgovarajuću ldif datoteku s promjenama koje se primjenjuju na LDAP), a promjene na konfiguraciji se primjenjuju odmah bez potrebe za restartom servisa.

Ako ste na poslužitelju prijavljeni kao root i ako je LDAP podešen da koristi i ldapi (što openldap-aai paket inicijalno jest), onda se za promjene u konfiguraciji na LDAP možete prijaviti koristeći tzv. vanjsku autentikaciju (SASL) pri čemu operativni sustav LDAP-u javi uid i gid korisnika koji je prijavljen, a LDAP na osnovu uid i gid brojeva donosi odluku o tome je li korisnik ovlašten za zahtijevanu akciju.

Ako želite koristiti tzv. vanjsku autentikaciju (SASL) za promjenu konfiguracije, kod pokretanja LDAP klijenta potrebno je navesti sljedeće parametre:

```
naredba -h ldapi:/// -Y EXTERNAL -b cn=config
```

- -h je host,
- ldapi:/// je protokol,
- -Y EXTERNAL znači da se koristi ektsterna metodu autentikacije (SASL), a u standardnoj access listi je već definirano da korisnik koji je root na sustavu smije pristupiti konfiguraciji na taj način. Ne treba upisivati username i password LDAP admin korisnika, već je za bind dovoljno biti prijavljen kao root na stroju.
- -b cn=config znači da se pristupa grani u LDAP-u čiji je base dn cn=config. To je dio stabla u LDAP-u u kojem je pohranjena konfiguracija.

Obzirom da je konfiguracija u memoriji, prihvaćene promjene se odmah primjenjuju bez potrebe za restartom servisa.

Više o podešavanju LDAP-a, te opcijama konfiguracije pročitajte na adresama:

https://www.openldap.org/doc/admin24/slapdconf2.html

https://www.zytrax.com/books/ldap/ch6/slapd-config.html

Promjena konfiguracije uporabom alata ldapvi

Za promjenu konfiguracije moguće je koristiti i alat ldapvi koji omogućuje promjenu konfiguracije "na živo" bez uporabe ldapmodify i ldif datoteka kao da se mijenja
tekstualna datoteka i promjene odmah primjenjuje na konfiguraciju LDAP-a.

ldapvi se pokreće sa sljedećim parametrima:

```
ldapvi -h ldapi:/// -Y EXTERNAL -b cn=config
```

- -h je host,
- ldapi:/// je protokol,
- -Y EXTERNAL znači da se koristi ektsterna metodu autentikacije (SASL), a u standardnoj access listi je već definirano da korisnik koji je root na sustavu smije pristupiti konfiguraciji na taj način. Ne treba upisivati username i password LDAP admin korisnika, već je za bind dovoljno biti prijavljen kao root na stroju.
- -b cn=config znači da se pristupa grani u LDAP-u čiji je base dn cn=config. To je dio stabla u LDAP-u u kojem je pohranjena konfiguracija.

Pokretanje ldapvi na gore opisan način omogućuje pristup kompletnoj konfiguraciji LDAP-a koja je inače zapisana u tom stablu po raznim granama kao da se uređuje tekstualna datoteka što značajno pojednostavljuje upravljanje konfiguracijom jer nije potrebno znati u kojoj grani je koji dio konfiguracije, ali nosi i određene opasnosti - mogućnost da se LDAP krivo podesi. Zato prije svake promjene treba napraviti backup ldap-a i biti siguran što se točno želi promijeniti.

Editor je vi, što znači da vrijede sve komande, a po izlasku iz editora moguće je odabrati hoće li se promjene snimiti i primjeniti na konfiguraciju LDAP-a, ili će se odbaciti. Ako se odabere snimanje promjena, alat će provjeritti sintaksu i pokušati primjeniti promjene.

Promjena konfiguracije uporabom alata ldapmodify

Kod promjena konfiguracije uporabom alata ldapmodify, potrebno je pripremiti ulaznu ldif datoteku u kojoj su opisane promjene koje želite primjeniti na konfiguraciju LDAP-a.

U slučaju da želite npr. promijeniti loglevel ldif datoteka mora imati sljedeći sadržaj:

```
dn: cn=config
changetype: modify
replace: olcLogLevel
olcLogLevel: stats
```

- dn (distiguish name) definira granu stabla u kojoj se nalazi atribut čiju vrijednost želite izmjeniti
- changetype i replace definiraju akciju koja se treba odviti na atributu
- olcLogLevel je atribut u konfiguraciji koji sadrži informaciju o razini logiranja, stats je minimalna razina logiranja. Tablicu s popisom mogućih razina logiranja možete pronaći ovdje.

Nakon što snimite ldif datoteku, promjene primjenjujete naredbom ldapmodify kao u nastavku:

```
ldapmodify -H ldapi:/// -Y EXTERNAL -f ldifdatioteka.ldif
```

S obzirom da sam ldif sadrži informaciju o grani stabla na koju se promjena odnosi, u ovom slučaju prilikom pokretanja ldapmodify naredbe parametar -b nije potreban.

Promjene se primjenjuju odmah po izvršenju naredbe bez potrebe za restartom servisa.