Uputstvo za konfiguraciju ACL na OpenLDAP direktorijumu

Apstrakt: U ovom dokumetu opisane su osnovne smernice za konfiguraciju kontrolnih listi za prisup u okviru OpenLDAP direktorijuma

Sadržaj

Uvodne napomene

Korišćenjem listi za kontrolu pristupa (*Acces Control Lists* - ACL), OpenLDAP omogućava definisanje vrlo preciznih kontrola za pristup LDAP direktorijumu. Tako se npr. može dozvoliti ili zabraniti pretraga, čitanje ili upis vrednosti u određenoj grani, određenom ulazu ili čak u određeni atribut i to na nivou svih ili pojedinačnog korisnika. Jedini izuzetak korisnika koji se ne može ograničiti putem ACL je *super user* (definisan u slapd.conf fajlu sa rootdn/rootpw) koji uvek može izvršavati sve operacije nad LDAP direktorijumom. U slučaju da je zbog naročitih sigurnosnih potreba neophodno da svaki korisnik "prolazi" kroz ACL, *super user* nalog se nakon instalacije LDAPa može ukinuti brisanjem rootdn/rootpw direktiva iz `slapd.conf` fajla.
Preporuka je definisati ACL tako da su dozvoljene samo one operacije nad LDAP direktorijumom koje su potrebne. ACL se dešinišu u `slapd.conf` fajlu i to u globalnoj sekciji ili u sekciji baze podataka. U daljem tekstu je opisan princip postavljanja jednostavnijih ACL bez korišćenja filtera i regularnih izraza, a detaljan opis različitih mogućnosti filtriranja i davanja privilegija se mogu naći na http://www.openldap.org/doc/admin24/access-control.html.

Konfiguracija ACL

ACL pravila definisana su u jednom ili više redova odnosno direktiva kroz koje slapd prolazi po principu od vrha ka dnu. Kada se upari neki red ACLa on se primenjuje i dalja obrada ACL se prekida. Detaljano objašnjenje kako se vrši obrada ACL, dato je u sledećem poglavlju.

Format jednog reda ACL je sledeći:

```
access to <what> [ by <who> <accesslevel> <control> ]+
```

Odnosno u "razvijenom" formatu, jednostavnije za razumevanje, jedan ACL red se može uneti u obliku:

```
# definicija dela stabla na koje se odnosi kontrola pristupa
access to <what>
# definicija ko sme da pristupi i sa kojim privilegijama
                by <who> <accesslevel>
                .......
                by <who> <accesslevel>
```

`<what>` klauzula definiše čemu se ograničava prisup, `<who>` na kog korisnika se odnosi, a `<accesslevel>` nivo pristupa koji je dodeljen. Svaka od ovih klauzula posebno je opisana u poglavljima koja slede.

<what> klauzula

`<what>` klauzula definiše deo stabla, *entry* ili atribut na koji se odnosi kontrola pristupa. Može se opisati korišćenjem DNa, filtra ili regularnog izraza. Filtri se mogu koristiti da bi se se obuhvatili pojedinacni atributi ili objektne klase. Ovde će biti opisan samo prvi navedeni način, korišćenjem DNa kojim se mogu obuhvatiti delovi stabla ili pojedinačni entry.

```
# obuhvata celo stablo
access to *
# obuhvata određene entry-je definisanih DN-om
access to dn.<scope>=<DN>
```

`<scope>` može imati više vrednosti:

- `base` - obuhvata samo *entry* definisan u <DN>
- `one` - obuhvata samo *entry* koji je u LDAP stablu direktno nadređeni (*parrent*) onom definisanom u <DN>
- `subtree` - obuhvata sve *entry*-je koji se u LDAP stablu nalaze ispod *entry*-ja definisanom u <DN>, kao i sam *entry* definisan u <DN>
- `children` - obuhvata sve *entry*-je koji se u LDAP stablu nalaze ispod *entry*-ja definisanom u <DN>, ali ne i sam *entry* definisan u <DN>

Primer:

Ako LDAP sadrži sledeće *entry*-je:

0: o=suffix
1: cn=Manager,o=suffix
2: ou=people,o=suffix
3: uid=kdz,ou=people,o=suffix
4: cn=addresses,uid=kdz,ou=people,o=suffix
5: uid=hyc,ou=people,o=suffix

Onda:

dn.base="ou=people,o=suffix" - obuhvata *entry* 2
dn.one="ou=people,o=suffix" - obuhvata *entry* 3, i 5
dn.subtree="ou=people,o=suffix" - obuhvata *entry* u 2, 3, 4 i 5
dn.children="ou=people,o=suffix" - obuhvata *entry* 3, 4, i 5

`<who>` klauzula

`<who>` klauzula definiše korisnika kome se dodeljuju određene privilegije i može imati sledeće vrednosti:

- * - bilo ko
- `anonymus` - svi neautentifikovani korisnici
- `users` - svi autentifikovani korisnici
- `self` - korisnik koji je definisan u ciljanom <DN>
- `dn.<scope>=<DN>`, korisnik koj je u opsegu definisanom u <DN>; `<scope>` može imati iste vrednosti kao u `<what>` klauzuli

`<accesslevel>` klauzula

`<accesslevel>` klauzula definiše nivo privilegije koje se dodeljuje, odnosno ldap operacije koje se dozvoljavaju. Može imati sledeće vrednosti, pri čemu svaki nivo uključuje i prethodno navedene:

- `none` - zabranjen pristup
- `disclose` - koristi se za razotkrivanje greške
- `auth` -dozvoljava `bind` operaciju
- `compare` - dozvoljava `compare` operaciju
- `search` - dozvoljava `serach` operaciju
- `read` - dozvoljava `read` operaciju
- `write` - dozvoljava `write` operaciju
- `manage` - dozvoljava upravljanje

Obrada ACL

Kada korisnik zahteva da se izvrši neka operacija nad određenim *entry*-jem i/ili atributom, slapd poredi *entry* i/ili atribut sa `<what>` klauzulama u konfiguracionom fajlu.

ACL redovi se ispituju po redu po kome se pojavljuju u konfiguracionom fajlu. Slapd staje na prvoj ACL direktivi gde detektuje poklapanje sa `<what>` klauzulom. Slapd će primeniti pravila definisana u toj direktivi i neće obrađivati dalje ACL redove.

Dalje, slapd poredi entitet koji traži pristup sa `<who>` klauzulama po redu po kome se one pojavljuju. Kada upari korisnika sa `<who>` klauzulom, dalja obrada prestaje i primenjuju se privilegije definisane u `<accesslevel>` klauzuli koja sledi, tako da se zahtevana operacija dozvoljava ili brani. Na kraju ACL reda, nalazi se implicitni deny, što znači da ako se korisnik ne upari ni u jednoj `<who>` direktivi, pristup se ne dozvoljava.

Iz ovoga se može zaključiti da je redosled ispitivanja ACL direktiva odnosno njihov redosled u konfiguracionom fajlu bitan. Ako je određena ACL direktiva više specifična, onda se ona treba pojaviti ranije u konfiguracionom fajlu. Slično ako je `<who>` klauzula unutar jedne ACL direktive više specifična, onda se ona treba pojaviti ranije.