GRANT et REVOKE avec ldap2pg

et sans LDAP

@EtienneBersac

Parlons de vos données – 22 février 2018

À propos

- Étienne BERSAC
- Développeur chez Dalibo SCOP
- github.com/bersace

ldap2pg

- github.com/dalibo/ldap2pg
- industrialisation et sécurisation des accès Postgres.
- cf. dali.bo/pgsession9-ldap2pg (~30m)

Synchro automatique

- réinitialiser (tout)
- redérouler les autorisations
- groupes ro, rw, ddl

Synchro ldap2pg

- introspection.
- autorisation explicite.
- révocation implicite.

Définition d'une ACL

```
acls:
  connect:
    type: datacl  # ou nspacl, defacl, globaldefacl
    inspect: SELECT …
    grant: GRANT CONNECT ON … TO {role};
    revoke: REVOKE CONNECT ON … FROM {role};
  ro:
  - connect
```

ACL prédéfinies

- inclue la requête d’introspection.
- inactive par défaut.
- activable via un groupe actif.
- ldap2pg.rtfd.io/en/latest/wellknown

ALTER DEFAULT PRIVILEGES

- anticiper la modification du modèle.
- lister les propriétaires.
- par schéma ou global.
- … bug :-)

Démo !

Merci !

```
ldapsearch -b dc=pg,dc=meetup,dc=paris (objectClass=question)
```