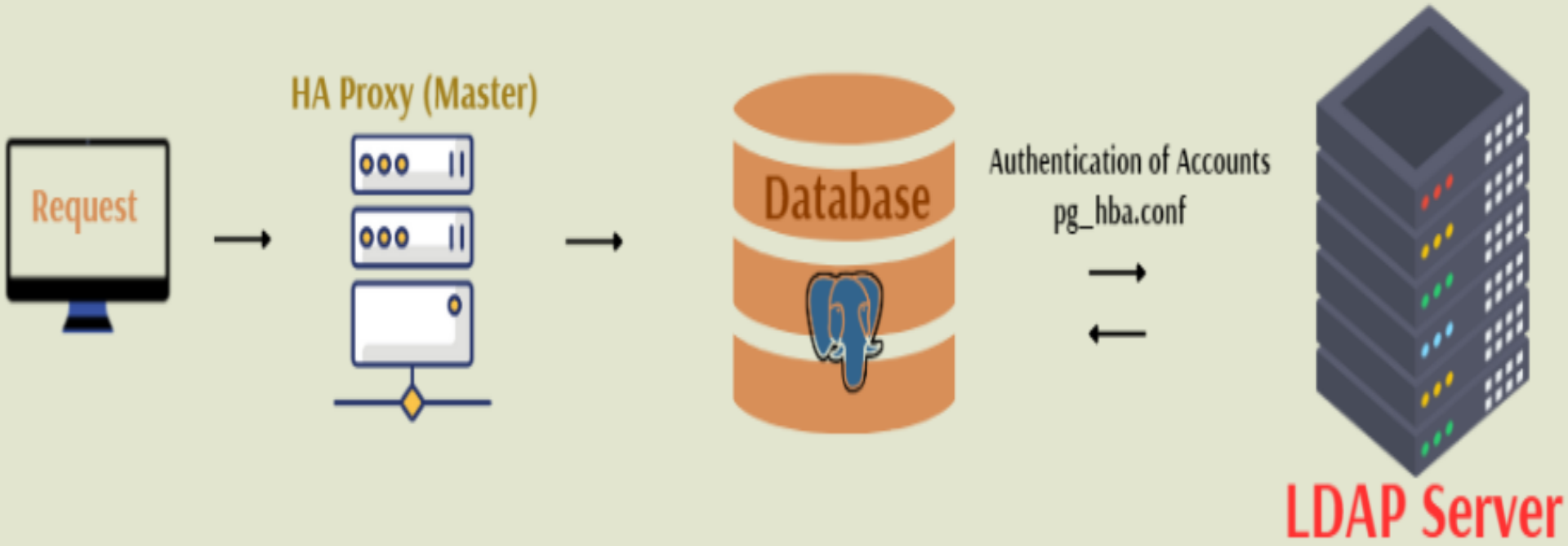
PostgreSQL LDAP Integration – User management automation using LDAP2PG

FUJITSU

FUJITSU

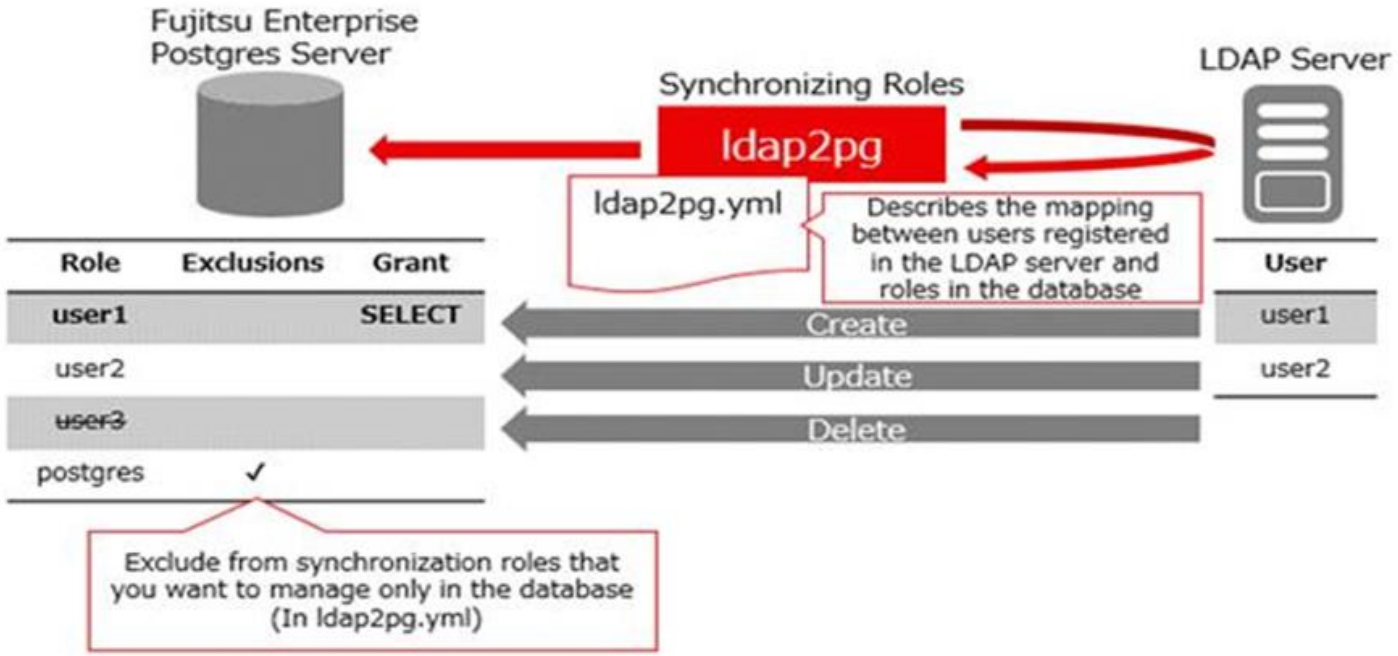
Authentication with LDAP



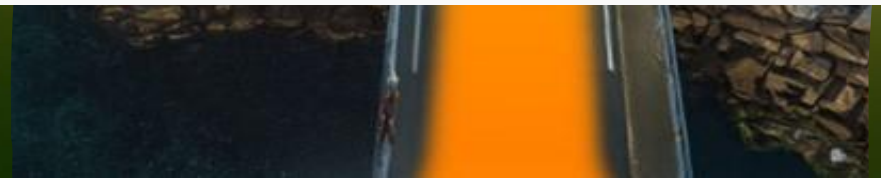
LDAP2PG

FUJITSU

- Before using LDAP2PG you should have previously installed openldap , configured (/etc/openladap/lda.conf) and pg_hba.conf for your LDAP server and have tested you can login with a matching single role using the LDAP credentials
- LDAP2PG requires you first configure the ldap2pg.yml config file with the LDAP server access settings and define all your synchronisation rules along with a database superuser to use for synchronising the users.

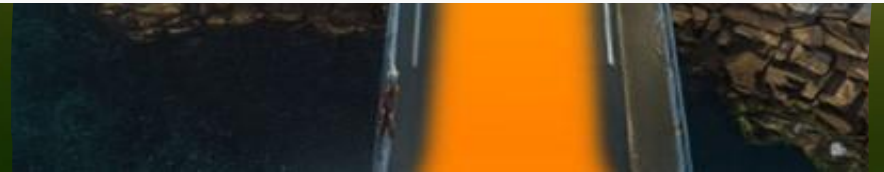


```
# TYPE  DATABASE        USER            ADDRESS                 METHOD
# "local" is for Unix domain socket connections only
local   all             all                                     peer
# IPv4 local connections:
host    all             fepuser         172.35.4.112/29         scram-sha-256
host    all             ldap2pg_admin   172.35.4.112/29         scram-sha-256
host    all             all             172.35.0.0/16           ldap ldapserver=lonpogrp.london.uk ldapscheme=ldaps ldapport=636 ldapbasedn="OU=London
PGusers,dc=lonpogrp,dc=london,dc=uk" ldapbinddn="CN=LNPO-FEP-LDAP,OU=SystemUsers,OU=London PGusers,DC=lonpogrp,DC=London,DC=uk" ldapbindpasswd="bindpw4U!"
ldapsearchattribute="sAMAccountName"
hostssl all             all             172.35.0.0/16           scram-sha-256
```



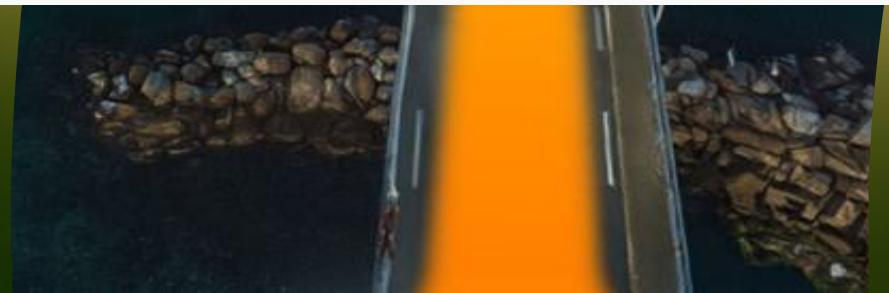
```
postgres:
  roles_blacklist_query:
    - postgres
    - fepuser
    - "pg_*"
    - "pgx_update_profile_status"
    - "pgx_cgroup_role_*"
    - public
  databases_query: select datname from pg_catalog.pg_database where datname not in ( 'template0' , 'template1') and datallowconn is true ;

privileges:
  reading:
  - __connect__
  - __usage_on_schemas__
  - __select_on_tables__

  writing:
  - reading
  - __insert_on_tables__
  - __update_on_tables__
  - __delete_on_tables__

  owning:
  - writing
  - __create_on_schemas__
  - __truncate_on_tables__
```

```
rules:
  - role:
      names:
      - appname_readonly
      - appname_readwrite
      - appname_admin
        options: NOLOGIN
      comment: "Parent group roles managed by LDAP2PG"

  - grant:
    - privilege: reading
      role: appname_readonly
      database: db1_dev
    - privilege: writing
      role: appname_readwrite
      database: db1_dev
    - privilege: owning
      role: appname_admin
      database: db1_dev
```



```
  - description: "Sync appname readonly roles from LDAP to PostgreSQL"
    ldapsearch:
      base: "ou=London PGusers,dc=lonpogrp,dc=london,dc=uk"
      filter: "(&(memberOf:1.2.840.113556.1.4.1941:=cn=GG_FEP_appname_readonly,ou=FEP,ou=Globale group,ou=London PGusers,dc=lonpogrp,dc=london,dc=uk)
(objectClass=person))"
    role:
      name: "{sAMAccountName.lower()}"
      options: LOGIN
      parent: "appname_readonly"
    grant:
      privilege: reading
      database: db1_dev
      schema: db_appname_dev
      role: appname_readonly

  - description: "Sync appname readwrite roles from LDAP to PostgreSQL"
    ldapsearch:
      base: "ou=London PGusers,dc=lonpogrp,dc=london,dc=uk"
      filter: "(&(memberOf:1.2.840.113556.1.4.1941:=cn=GG_FEP_appname_readwrite,ou=FEP,ou=Globale group,ou=London PGusers,dc=lonpogrp,dc=london,dc=uk)
(objectClass=person))"
    role:
      name: "{sAMAccountName.lower()}"
      options: LOGIN
      parent: "appname_readwrite"
    grant:
      privilege: writing
      database: db1_dev
      schema: db_appname_dev
      role: appname_readwrite
```

```
- description: "Sync appname admin roles from LDAP to PostgreSQL"
  ldapsearch:
    base: "ou=London PGusers,dc=lonpogrp,dc=london,dc=uk"
    filter: "(&(memberOf:1.2.840.113556.1.4.1941:=cn=GG_FEP_appname_admin,ou=FEP,ou=Globale group,ou=Londn PGusers,dc=lonpogrp,dc=london,dc=uk)
(objectClass=person))"
  role:
    name: "{sAMAccountName.lower()}"
    options: LOGIN
    parent: "appname_admin"
  grant:
    privilege: owning
    database: db1_dev
    schema: db_appname_dev
    role: appname_admin
```



```
#!/bin/bash
####################
# LDAP2PG Sync Script #
####################
export BIN=/opt/fsepv17ldap2pg/bin
export PGUSER=fepuser
export PGDATABASE=postgres
export PGHOST=`hostname -i`
export PORT=27500
export LDAPURI=ldaps://lonpogrp.london.uk:636
export LDAPBINDDN=""   # Please correct this to what we added to .bash_profile
export LDAPPASSWORD=""             # Please correct this to what we added to .bash_profile
export HOUSEKEEP=1  #adjust for number of days to keep logfiles

$BIN/ldap2pg --real --config /etc/ldap2pg/ldap2pg.yml
```