



AD und PostgreSQL Rollen verknüpfen mit dem Höllenhund

Michael Schulz

Freiburg, 12. März 2020

Im Überblick

- FOSSGIS Stack in nonFOSS Umgebung in Freiburg
- Zentrale Geo-DB in der Stadtverwaltung
- Welche Komponenten spielen zusammen
- Active Directory, Kerberos und PostgreSQL
- Definition von Rollenkonzepten
- Idap2pg als „man-in-the-middle“

FOSSGIS in nonFOSS Stack

- Stadtverwaltung Freiburg, +4000 MA, +40 Ämter, Eigenbetriebe, städt. Gesellschaften u. Beteiligungen
- Bewegte OSS Geschichte:
OpenOffice – „there and back again“
- Zentrale IT: Microsoft, Citrix, SLES,
- Geo-Bereich hat durchgehend OSS Einsatz

FOSSGIS in nonFOSS Stack



OGC®

OGC®



GDI-FR

Zentrale Dienste

Zentrale Geo-DB

- Zentrale PostGIS-Datenbank (2.3 on 9.6, 2.5 on 10.6)
- Szenario 1: Datenbanken für Anwendungen
 - PostNAS, XPlanBox, GeoNetwork, 3DCityDB, Mapbender, etc.
 - ← Service-User Anwendungsbezogen
- Szenario 2: Datenbanken für Geodatenhaltung
 - Schemas für Ämter, spezielle Themen, einzelne User (?)
 - ← Ämter-User Schema-bezogen

Zentrale Geo-DB

- Fachämter (VermA, StplA, GuT, etc.) sind verantwortlich für ihre fachlichen Datensätze
 - jedes Amt hat ein/mehrere Schema mit einem Schema-User
 - Schema-übergreifender Zugriff schwierig (Datenschutz), teilweise aber notwendig
 - temporäre DB-Arbeitsbereiche für Analysen etc.? User-bezogen?
- GeodatenManagement (GDM) und VermA können auf alle Schemas zugreifen, z.B. für übergreifende Analysen
 - nicht originäre Aufgabe

Zentrale Geo-DB

- Ziele:
 - Erhöhung Sicherheit: Einzelbenutzer autorisieren
 - Verbesserung Administration: Einbindung in zentrales IDM
 - Erhöhung Nutzbarkeit
 - Single-Sign-On ermöglichen (QGIS)
 - zusätzliche Funktionale Schemas (Referenz-Datensätze)
 - zusätzliche Einzeluser-Schema als Arbeitsbereich

Komponenten

- Zentrales Benutzerverzeichnis: Active Directory (bzw. Novell eDirectory)
- Client OS: Windows 10 z.B. mit QGIS
- PostgreSQL-Cluster auf SLES 12 SP4

- Zwei wichtige Komponenten fehlen noch
 - Wie erreicht man Bindung QGIS an PG an AD ? *Authentifizierung*
 - Wie kommen Rollen und Benutzer von AD in PG? *Autorisierung*

Komponenten

- Verbindung PostgreSQL an AD:
 - Kerberos – verteilter Authentifizierungsdienst
 - vereinfacht handeln drei Endpunkte die Authentifizierung aus:
 - Kerberos Client (z.B. Windows PC)
 - Key Distribution Center (KDC)
 - Kerberos (enabled) Service (PostgreSQL)



Quelle: <http://web.mit.edu/KERBEROS/>

*Kerberos (auch Zerberus) - gr. Mythologie: dreiköpfiger **Höllenhund**, der den Eingang zur Unterwelt bewacht, damit kein Lebender eindringt und kein Toter herauskommt. (Wikipedia)*

Komponenten

- Synchronisation Rollen (Autorisierung):
 - Idap2pg ermöglicht dabei:
 - Auslesen von Rollen aus LDAP/AD
 - Anlegen, Ändern und Löschen von Rollen in PG
 - Zuweisen/Entziehen von Rollenmitgliedschaften
 - Zuweisen/Entziehen von Berechtigungen
 - Anlegen von statischen Rollen



Idap2pg

PostgreSQL roles and ACL management

Quelle: <https://labs.dalibo.com/Idap2pg/>

Active Directory, Kerberos und PostgreSQL

■ PostgreSQL und Kerberos

```
geodev:~ # zypper se krb5
```

S	Name	Summary
i+	krb5	MIT Kerberos5 Implementation--Libraries
i+	krb5-32bit	MIT Kerberos5 Implementation--Libraries
i+	krb5-client	MIT Kerberos5 implementation - client programs

– Kerberos Konfiguration im System: in /etc/krb5.conf

```
[libdefaults]
  dns_lookup_kdc = true
  default = freiburg.intern
  default_realm = FREIBURG.INTERN
  ticket_lifetime = 24000
  clock_skew = 300
  default_ccache_name = FILE:/tmp/krb5cc_${uid}
```

```
[realms]
  freiburg.intern = {
    kdc = .freiburg.intern
    kdc = .freiburg.intern
    kdc = .freiburg.intern
    kdc = .freiburg.intern
    default_domain = FREIBURG.INTERN
  }
```

Active Directory, Kerberos und PostgreSQL

■ PostgreSQL und Kerberos

- Herstellen und testen der Verbindung zum KDC

```
GEODEV:~ # kinit -V service_gis@FREIBURG.INTERN
Using default cache: /tmp/krb5cc 0
Using principal: service_gis@FREIBURG.INTERN
Password for service_gis@FREIBURG.INTERN:
Authenticated to Kerberos v5
```

- Kerberos-relevante Konfiguration in postgresql.conf

```
# GSSAPI using Kerberos
krb_server_keyfile = '/opt/..._gis.keytab'
krb_caseins_users = on
```

- Postgres pg_hba.conf, pg_ident.conf anpassen (host, db, user, method)

```
# Zugriff von staetischen Benutzernamen via Kerberos/AD, DB-spezifisch (Bsp. für DB xplan5_test)
host      xplan5_test          all          10.180.0.0/16          gss map=kerberos
```

```
# MAPNAME          SYSTEM-USERNAME          PG-USERNAME
kerberos          /^(.*)@FREIBURG\..INTERN$          \1
```

Rollenkonzeption

- Trennen von Benutzer-, Gruppen- und Berechtigungsrollen
 - Benutzer-AD Konten entsprechen PG-Login-Rollen
 - AD-Gruppen entsprechen dabei PG-NoLogin-Rollen und PG-Schemas
 - AD-“Berechtigungs“-Gruppen entsprechen PG-Privilegien

- Namenskonzeption erstellen
 - L_Sub_GeoDB_<Schema>
 - L_Sub_GeoDB_<Schema>_<Privilege>

Idap2pg als „man-in-the-middle“

- Idap2pg mittels YAML-Datei konfiguriert
 - PostgreSQL Verbindung und LDAP/AD Verbindung

```
postgres:  
  # Connection string  
  dsn: postgres://...@localhost:5432/  
  # Scope the database where to purge objects when dropping roles. This is the  
  # scope of grant on `__all__` databases.  
  databases_query: [postgres, xplan5_test]  
ldap:  
  uri: ldaps://freiburg.intern:636  
  user: schulmi  
  binddn: "schulmi@freiburg.intern"
```

ldap2pg als „man-in-the-middle“

- ldap2pg erstmals ausführen

```
GEODEV:/opt/ldap2pg # ldap2pg -n -v
[ldap2pg.config] INFO] Starting ldap2pg 5.1.
[ldap2pg.config] DEBUG] Trying ./ldap2pg.yml.
[ldap2pg.config] INFO] Using /opt/ldap2pg/ldap2pg.simple.yml.
[ldap2pg.config] DEBUG] Read dry from argv.
[ldap2pg.config] DEBUG] Read verbosity from argv.
[ldap2pg.config] DEBUG] Read ldap:uri from YAML.
[ldap2pg.config] DEBUG] Read ldap:binddn from YAML.
[ldap2pg.config] DEBUG] Read ldap:user from YAML.
[ldap2pg.config] DEBUG] Read ldap:password from YAML.
[ldap2pg.config] DEBUG] Read postgres:dsn from YAML.
[ldap2pg.config] DEBUG] Read postgres:databases_query from YAML.
[ldap2pg.ldap] DEBUG] Connecting to LDAP server ldaps://freiburg.intern:636.
[ldap2pg.ldap] DEBUG] Trying SASL DIGEST-MD5 auth.
[ldap2pg.ldap] DEBUG] Doing: ldapwhoami -Y DIGEST-MD5 -U schulmi -W
```

Idap2pg als „man-in-the-middle“

- Idap2pg: statische Rollen definieren

```
sync_map:  
# keep AD reference  
- role:  
  names:  
  - ad_roles  
  - ad_users
```

- Idap2pg: Gruppenrollen aus AD lesen (Schemas)

```
# create AD group roles aka schemas  
- ldap:  
  base: OU=FRedgroups,DC=freiburg,DC=intern  
  filter: "(&(objectClass=group)(CN=Freigis_*))"  
  role:  
    name: '{cn}'  
    options: NOLOGIN  
    parent:  
      - ad_roles  
    comment: "synced from AD: {dn}"
```

Idap2pg als „man-in-the-middle“

- Idap2pg: AD Benutzer aus spezieller Gruppe auslesen

```
# create AD users belonging to specific AD group
- ldap:
  base: DC=freiburg,DC=intern
  filter: "(&(objectClass=user)(memberOf=CN=Freigis_Gutachter,OU=FreDgroups,DC=freiburg,DC=intern))"
  roles:
    name: '{sAMAccountName}'
    options: LOGIN
    parent:
      - ad_users
    comment: "synced from AD: {dn}"
```

ldap2pg als „man-in-the-middle“

■ ldap2pg ausführen

```
[ldap2pg.manager INFO] Querying LDAP OU=FreDgroups,DC=freibur... (&(objectCla...
[ldap2pg.ldap DEBUG] Doing: ldapsearch -Y DIGEST-MD5 -U schulmi -W -b OU=FreDgroups,DC=freiburg,DC=int
sub '(&(objectClass=group)(CN=Freigis_*))' cn
[ldap2pg.manager DEBUG] Got 5 entries from LDAP.

[ldap2pg.manager DEBUG] Found role Freigis_Gutachter from CN=Freigis_Gutachter,OU=FreDgroups,DC=freiburg,
ern.
[ldap2pg.manager DEBUG] Role Freigis_Gutachter is member of ad_roles.

[ldap2pg.manager INFO] Querying LDAP DC=freiburg,DC=intern... (&(objectCla...
[ldap2pg.ldap DEBUG] Doing: ldapsearch -Y DIGEST-MD5 -U schulmi -W -b DC=freiburg,DC=intern -s sub '(&
tClass=user)(memberOf=CN=Freigis_Gutachter,OU=FreDgroups,DC=freiburg,DC=intern))' sAMAccountName
[ldap2pg.manager DEBUG] Got 20 entries from LDAP.

[ldap2pg.manager DEBUG] Found role SchulMi from CN=Schulz\, Michael,OU=FreDusers,DC=freiburg,DC=intern.
[ldap2pg.manager DEBUG] Role SchulMi is member of ad_users.

[ldap2pg.manager DEBUG] LDAP inspection completed. Post processing.
[ldap2pg.role WARN] Role SchulMi already exists in cluster. Reusing.

[ldap2pg.psql CHANG] Would create Freigis_Gutachter.
[ldap2pg.psql DEBUG] Would execute: CREATE ROLE "Freigis_Gutachter" WITH NOSUPERUSER NOBYPASSRLS NOCRE
E NOREPLICATION NOCREATEDB NOLOGIN INHERIT;
[ldap2pg.psql DEBUG] COMMENT ON ROLE "Freigis_Gutachter" IS 'synced from AD: CN=Freigis_Gutachter,OU=Fre
ups,DC=freiburg,DC=intern';
```


Neue PostGIS-Verbindung erzeugen

Verbindung zu kerberos war erfolgreich.

Verbindungsinformationen

Name: kerberos

Dienst:

Host: geodev

Port: 5432

Datenbank: xplan5_test

SSL-Modus: abschalten

Authentifizierung

Konfigurationen: Basic

Benutzername: Speichern

Passwort (d): Optional Speichern

Warnung: Zugangsdaten werden in Klartext in Projektdatei gespeichert.

Konfiguration umwandeln

▼ Aktuelle Umgebungsvariablen (schreibgeschützt - Fett bedeutet Änderung beim Start)

Variable	Wert
USERNAME	SchulMi
USERDNSDOMAIN	FREIBURG.INTERN
USERDOMAIN	FREIBURG

OK Abbrechen Hilfe

Browser

- Favoriten
 - Home
 - C:\
- GeoPackage
- SpatiaLite
- PostGIS
 - kerberos
 - BP_Aufschuettung_Abgrabung_Bodenschaeetze
 - BP_Basisobjekte
 - BP_Bebauung
 - BP_Erhaltungssatzung_und_Denkmalschutz
 - BP_Gemeinbedarf_Spiel_und_Sportanlagen
 - BP_Landwirtschaft_Wald_und_Gruen
 - BP_Naturschutz_Landschaftsbild_Naturhaushalt
 - BP_Sonstiges
 - BP_Umwelt
 - BP_Ver_und_Entsorgung
 - BP_Verkehr

```
# Zugriff von staedtischen Benutzernamen via Kerberos:  
host xplan5_test all 10.180.0.0/16  
  
# MAPNAME SYSTEM_USERNAME PG-USERNAME  
kerberos ^(.*)FREIBURG\..INTERN$ \1
```

AD und PostgreSQL Rollen verknüpfen
mit dem Höllenhund

Vielen Dank für Ihre Aufmerksamkeit

Fragen?

Michael Schulz

michael.schulz@stadt.freiburg.de