LOXODATA

GÉRER LA SÉCURITÉ DANS POSTGRESQL : DE L'ACCÈS AU SERVEUR À LA DONNÉE

OSXP 2024

5 DÉCEMBRE 2024

Stéphane SCHILDKNECHT

LOXODATA

QUI SUIS-JE ?

Stéphane Schildknecht

- Passionné de PostgreSQL depuis 25 ans
- Fondateur de PostgreSQLFr (Président 2005-2010)
- Fondateur de LOXODATA en 2010
- @saschild

LOXODATA

Entreprise disposant de 3 piliers d'expertises

PostgreSQL

DevOps

Cloud

LOXODATA

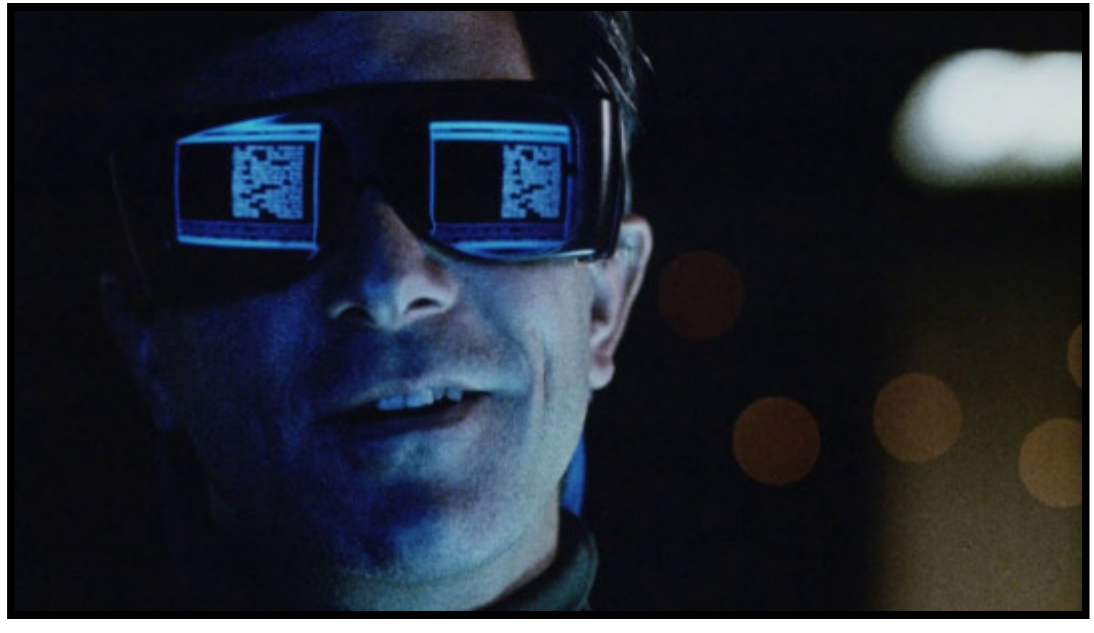
Une large palette de services

DE QUOI S'AGIT-IL ?

Sécuriser votre bien le plus précieux

- Restreindre les accès (serveur/bases)
- Gérer les droits (sur les objets)
- Gérer la visibilité (des données)

QUELLES SONT LES MENACES ?



Risques

- Accès non autorisé
- Vol de données
- Utilisateur (indélicat/maladroit)

LOXODATA

OUVRIR LES ACCÈS

LOXODATA

POSTGRESQL.CONF

- Ecoute socket
- Ecoute réseau
- Authentification
- SSL

PG_HBA.CONF

- Configuration superficielle par défaut
- Différentes méthodes d'authentification
  - internes (trust/ident/peer/password/md5/scram-sha-56)
  - externes (LDAP/Radius/kerberos/GSSAPI/SSPI)
  - par certificat (SSL/TLS)

LOXODATA

ET SI ON INVITAIT DU MONDE ?

CRÉATION ET GESTION DES RÔLES

```
CREATE ROLE jonathan LOGIN;
CREATE ROLE joe LOGIN;
CREATE USER davide WITH PASSWORD 'jw8s0F4';
CREATE ROLE admins WITH CREATEDB CREATEROLE;
CREATE ROLE wheel;
CREATE ROLE island;
GRANT admins TO joe WITH INHERIT TRUE;
GRANT wheel TO admin WITH INHERIT FALSE;
GRANT island TO joe WITH INHERIT TRUE, SET FALSE;
REVOKE admins FROM joe;
```

UTILISATION DES RÔLES

```
SET ROLE admin;
SET ROLE joe;
SET ROLE NONE;
RESET ROLE;
SET SESSION AUTHORIZATION joe;
```

SUPPRESSION DE RÔLES

1. Attribuer ses objets à un autre rôle
2. Supprimer le rôle

LOXODATA

ON A DES COPAINS, MAIS QUE PEUVENT-ILS FAIRE ?

ACCORDER DES DROITS

- Sur les bases
- Sur les schémas
- Sur les objets
  - Tables, colonnes, séquences, domaines
  - Foreign Data Wrapper / Foreign server
  - Fonctions, langages

```
GRANT SELECT ON mytable TO PUBLIC;
GRANT SELECT, UPDATE, INSERT ON mytable TO admin;
GRANT SELECT (col1), UPDATE (col1) ON mytable TO miriam_rw;
GRANT SELECT ON ALL TABLES IN SCHEMA beach TO PUBLIC;
```

DROITS PAR DÉFAUT

Et pour les prochains copains, on fait quoi ?

```
ALTER DEFAULT PRIVILEGES IN SCHEMA myschema GRANT SELECT ON TABLES TO PUBLIC;
ALTER DEFAULT PRIVILEGES IN SCHEMA myschema GRANT INSERT ON TABLES TO webuser;
ALTER DEFAULT PRIVILEGES IN SCHEMA myschema REVOKE SELECT ON TABLES FROM PUBLIC;
ALTER DEFAULT PRIVILEGES IN SCHEMA myschema REVOKE INSERT ON TABLES FROM webuser;
ALTER DEFAULT PRIVILEGES FOR ROLE admin REVOKE EXECUTE ON FUNCTIONS FROM PUBLIC;
ALTER DEFAULT PRIVILEGES IN SCHEMA public REVOKE EXECUTE ON FUNCTIONS FROM PUBLIC;
```

SUPPRIMER LES DROITS

Est-ce qu'on peut tout se dire ?

```
REVOKE INSERT ON films FROM PUBLIC;
REVOKE ALL PRIVILEGES ON kinds FROM manuel;
REVOKE admins FROM joe;
```

RÔLES PRÉDÉFINIS

Rôle	Autorisations
pg_read_all_data / pg_write_all_data	Lire/Écrire dans toutes les tables (sauf RLS)
pg_read_all_settings	Lire tous les paramètres de configuration
pg_read_all_stats	Lire toutes les vues de statistiques
pg_stat_scan_tables	Exécuter les fonctions de monitoring
pg_monitor	Lire et exécuter les fonctions et vues de monitoring
pg_database_owner	Implicite propriétaire de la BDD
pg_signal_backend	Signaler un autre backend d'annuler une requête ou terminer un backend
pg_read_server_files / pg_write_server_files	Lire/Écrire des fichiers sur le serveur
pg_execute_server_program	Exécuter des programmes sur le serveur
pg_checkpoint	Exécuter la commande `CHECKPOINT`
pg_use_reserved_connections	Utiliser les connexions réservées `reserved_connections`
pg_create_subscription	Créer une souscription
pg_maintain (17)	Exécuter VACUUM, ANALYZE, CLUSTER, REFRESH MATERIALIZED VIEW, REINDEX, LOCK TABLE

```
GRANT pg_signal_backend TO admin_user;
```

CONSULTER LES DROITS

Privilege	Abbreviation	Applicable Object Types
SELECT	r (“read”)	LO, Séquence, Table, colonnes
INSERT	a (“append”)	Table, colonnes
UPDATE	w (“write”)	LO, Séquence, Table, colonnes
DELETE	d	Table
TRUNCATE	D	Table
REFERENCES	x	Table, colonnes
TRIGGER	t	Table
CREATE	C	Base, Schema, Tablespace
CONNECT	c	Base
TEMPORARY	T	Base
EXECUTE	X	Fonction, Procédure
USAGE	U	Domaine, FDW, Foreign Server, Langage, Schema, Sequence, Type
SET	s	Paramètre
ALTER SYSTEM	A	Paramètre

LOXODATA

CONSULTER LES DROITS

```
sas=# \dp beach.objects
                                    Droits d accès
 Schéma |   Nom   | Type  |   Droits d accès    | Droits d accès à la colonne | Politiques
--------+---------+-------+---------------------+-----------------------------+------------
 beach  | objects | table | sas=arwdDxt/sas    +|                             |
        |         |       | player=r/sas       +|                             |
        |         |       | player2=arwdDxt/sas |                             |

sas=# ALTER DEFAULT PRIVILEGES IN SCHEMA  beach GRANT SELECT ON TABLES TO PUBLIC;

sas=# \ddp beach
          Droits d accès par défaut
 Propriétaire | Schéma | Type  | Droits d accès
--------------+--------+-------+----------------
 postgres     | beach  | table | =r/postgres

sas=# select * from pg_default_acl;
  oid  | defaclrole | defaclnamespace | defaclobjtype |   defaclacl
-------+------------+-----------------+---------------+---------------
 18067 |         10 |           18057 | r             | {=r/postgres}
```

RESTREINDRE L'ACCÈS AUX DONNÉES

- Droits sur un objet
- Droits sur une colonne
- Utiliser une vue
- Fonctions
- Rules
- RLS

ROW LEVEL SECURITY

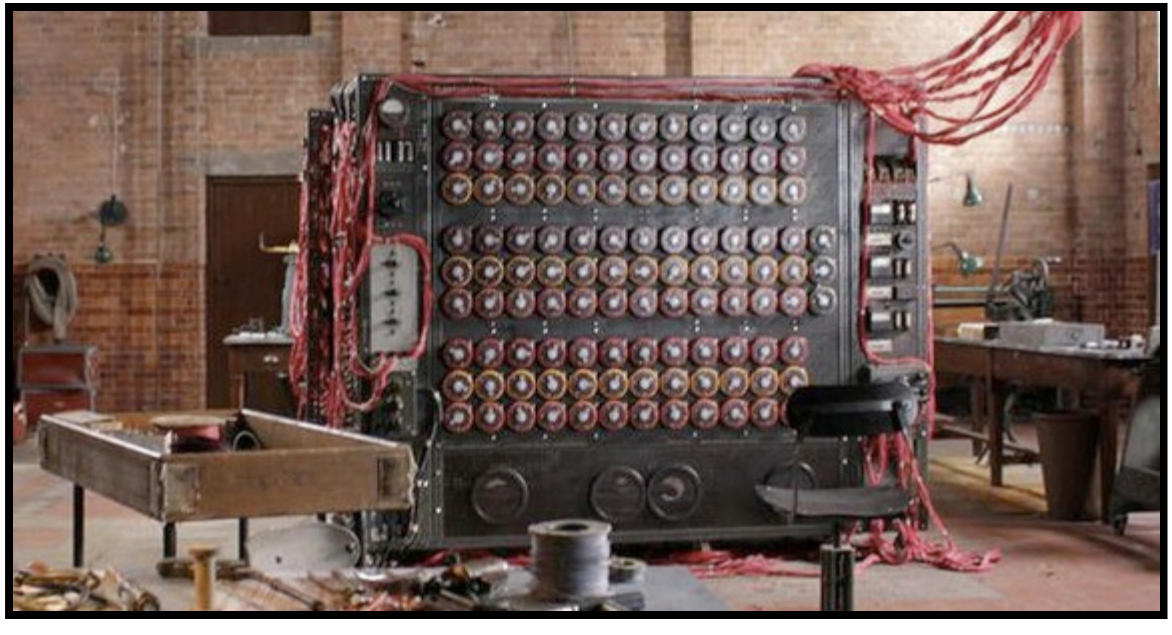
- Qui peut voir quelles lignes
- Par rôle, par commande, ou les deux

```
CREATE TABLE accounts (manager text, company text, contact_email text);
ALTER TABLE accounts ENABLE ROW LEVEL SECURITY;
CREATE POLICY account_managers ON accounts TO managers
    USING (manager = current_user);
CREATE POLICY user_sel_policy ON users
    FOR SELECT
    USING (true);
CREATE POLICY user_mod_policy ON users
    USING (user_name = current_user);
```

https://www.postgresql.org/docs/current/ddl-rowsecurity.html

LOXODATA

PEUT-ON SÉCURISER LES DONNÉES



CHIFFREMENT DES DONNÉES

- TDE : pas natif
- Pas de chiffrement de base
- Pas de chiffrement de table
- Pas de chiffrement de colonne
- Pas de type natif

=> Stockage en clair

SOLUTIONS

1. Chiffrement stockage
2. pgcrypto
3. pgsodium

LOXODATA

IL Y A D'AUTRES MANIÈRES DE LAISSER L'INFORMATION FUITER

ACCÈS À LA MACHINE

1. Sécuriser l'accès au datacenter
2. Sécuriser l'accès au serveur
3. Gérer les mots de passe des comptes d'administration

SYSOOPS/DEVOOPS/DATAOOPS

- Mauvaise manipulation
- Données confidentielles en public
- Accès à la production à une société externe

TRACES D'ACTIVITÉ

- Peuvent contenir des informations sensibles
- Peuvent servir à tracer les accès

SAUVEGARDES

- Tout y est !
- Chiffrer
- Externaliser

MISES À JOUR

- Impératives
- Pas uniquement l'application
- Pas uniquement la base
- CVE

CONCLUSION

- Lire la documentation (pléthorique)
- User et abuser de l'expertise du DBA
- Vous n'avez toujours pas de DBA ?
- Better call LOXODATA!