CYBERTEC
DATA SCIENCE & POSTGRESQL

PostgreSQL Security

Hans-Jürgen Schönig
www.cybertec-postgresql.com

Über Cybertec

Cybertec: PostgreSQL seit 1999

CYBERTEC
DATA SCIENCE & POSTGRESQL

- Wir bieten Services für PostgreSQL und Data Science
  - 24x7 Support
  - Training
  - Consulting
  - Performance Tuning
  - Clustering

Cybertec: Weltweite Services

CYBERTEC
DATA SCIENCE & POSTGRESQL

- Büros in . . .
  - Wiener Neustadt, Österreich
  - Zürich, Schweiz
  - Tallinn, Estland
  - Montevideo, Uruguay

PostgreSQL Security: Überblick

Hans-Jürgen Schönig
www.cybertec-postgresql.com

PostgreSQL Security: Die Layer

CYBERTEC
DATA SCIENCE & POSTGRESQL

- Security auf verschiedenen Ebenen
  - Transportverschlüsselung
  - User und Rechteverwaltung
  - Datenverschlüsselung

User und Rechteverwaltung

CYBERTEC
DATA SCIENCE & POSTGRESQL

1. Bind Adressen: listen_addresses in postgresql.conf
2. Netzwerkfreigaben: pg_hba.conf
3. Instanzebene
4. Databaseebene
5. Schemaebene
6. Tabellenebene
7. Spaltenebene
8. Row-Level-Security

Bind Adressen:

CYBERTEC
DATA SCIENCE & POSTGRESQL

- postgresql: listen_addresses
  - Auf wen wird gehört?

```
listen_addresses = 'localhost'
port = 5432
max_connections = 100
superuser_reserved_connections = 3
```

Netzwerk: pg_hba.conf (1)

CYBERTEC
DATA SCIENCE & POSTGRESQL

- Welche Netzwerke dürfen sich wie einloggen?
- Wollen wir SSL oder nicht?
- Regeln können definiert werden

Netzwerk: pg_hba.conf (2)

CYBERTEC
DATA SCIENCE & POSTGRESQL

```
# TYPE DATABASE    USER    ADDRESS          METHOD
local  all         all                      trust
host   all         all     127.0.0.1/32     trust
host   all         all     ::1/128          trust
host   all         all     192.168.0.0/16   scram-sha-256
host   all         all     192.168.5.5/32   reject
```

Welche Methoden gibt es?

CYBERTEC
DATA SCIENCE & POSTGRESQL

- trust
- reject
- md5
- password
- scram-sha-256
- gss
- sspi
- ident
- peer
- pam
- ldap
- radius
- cert

Instanzebene (1):

CYBERTEC
DATA SCIENCE & POSTGRESQL

- Manche Dinge leben auf Instanzebene:
  - User / Rollen
  - Tablespaces
- CREATE USER und CREATE ROLE sind “ident”

Instanzebene (2):

CYBERTEC
DATA SCIENCE & POSTGRESQL

- Rechte:
  - CREATEROLE / CREATEUSER
  - CREATEDB
  - SUPERUSER
  - LOGIN / NOLOGIN
  - REPLICATION

GRANT und REVOKE

CYBERTEC
DATA SCIENCE & POSTGRESQL

- Alle Rechte auf Databases, Schemata, Tabellen und Spalten werden mit GRANT und REVOKE vergeben

Databaseebene:

CYBERTEC
DATA SCIENCE & POSTGRESQL

- CONNECT:
  - Eine Instanz hat viele Datenbank
  - Zu welcher Datenbank darf ich mich verbinden?
- CREATE:
  - Darf ich Schemata anlegen?
  - NICHT Database anlegen !

Schemaebene:

CYBERTEC
DATA SCIENCE & POSTGRESQL

- CREATE:
  - In einem Schema ein Objekt anlegen (Table, Function, etc.)
- USAGE:
  - Darf ich den System Catalog sehen?
  - Benötigt man, um auf Tabellen in einem Schema zugreifen zu dürfen

Tabellenebene:

- SELECT, INSERT, UPDATE, DELETE, TRUNCATE, REFERENCES, TRIGGER
- Es gibt keine impliziten Rechte:
  - INSERT kann ohne SELECT existieren

Spaltenebene:

CYBERTEC
DATA SCIENCE & POSTGRESQL

- Man kann den Zugriff auf Spalten reduzieren
- “SELECT *” klappt möglicherweise nicht mehr
  - Man muss Spalten explizit listen
  - Das kann Applikationen brechen

Default Rechte und automatische Vergabe

PUBLIC: Unix-World style

- “PUBLIC” hat automatisch CONNECT-Rechte auf eine Database
- “PUBLIC” hat automatisch CREATE / USAGE Rechte auf das “public” Schema
  - Benutzer können sich anmelden und Tabellen anlegen
  - Das will man möglicherweise nicht

```
REVOKE ALL ON DATABASE test FROM public;
REVOKE ALL ON SCHEMA public FROM public;
```

Automatische Rechtevergabe

CYBERTEC
DATA SCIENCE & POSTGRESQL

- Nehmen wir an, es gibt ein Schema namens “buchhaltung”
- In diesem Schema gibt es 100 Tabellen

```
GRANT SELECT ON ALL TABLES IN SCHEMA buchhaltung TO xy;
```

- Was passiert, wenn die 101. Tabelle angelegt wird?
  - “FOR ALL TABLES IN SCHEMA” ist nur eine Schleife

ALTER DEFAULT PRIVILEGES

CYBERTEC
DATA SCIENCE & POSTGRESQL

```
Command:     ALTER DEFAULT PRIVILEGES
Description: define default access privileges
Syntax:
ALTER DEFAULT PRIVILEGES
    [ FOR { ROLE | USER } target_role [, ...] ]
    [ IN SCHEMA schema_name [, ...] ]
    abbreviated_grant_or_revoke

where abbreviated_grant_or_revoke is one of:

GRANT { { SELECT | INSERT | UPDATE | DELETE |
      TRUNCATE | REFERENCES | TRIGGER }
    [, ...] | ALL [ PRIVILEGES ] }
    ON TABLES ...
```

Row Level Security

Hans-Jürgen Schönig
www.cybertec-postgresql.com

Row-Level-Security (1):

CYBERTEC
DATA SCIENCE & POSTGRESQL

- Manchmal ist es nötig, die Sicht auf die Daten einzuschränken
- Andere Hersteller nennen das “Virtual Private Database”
- Beispiel:
  - User A sieht nur Männer
  - User B sieht nur Frauen
  - User C sieht alle Einträge

Row-Level-Security (2):

CYBERTEC
DATA SCIENCE & POSTGRESQL

```
test=# \h CREATE POLICY
Command:     CREATE POLICY
Description: define a new row level security
    policy for a table
Syntax:
CREATE POLICY name ON table_name
    [ AS { PERMISSIVE | RESTRICTIVE } ]
    [ FOR { ALL | SELECT | INSERT | UPDATE | DELETE } ]
    [ TO { role_name | PUBLIC | CURRENT_USER |
    SESSION_USER } [, ...] ]
    [ USING ( using_expression ) ]
    [ WITH CHECK ( check_expression ) ]
```

Row-Level-Security (3):

CYBERTEC
DATA SCIENCE & POSTGRESQL

```
test=# CREATE TABLE t_test AS SELECT *
    FROM generate_series(1, 5) AS id;
SELECT 5
test=# ALTER TABLE t_test ENABLE ROW LEVEL SECURITY;
ALTER TABLE
test=# CREATE USER joe LOGIN;
CREATE ROLE
test=# GRANT ALL ON t_test TO joe;
GRANT
```

Row-Level-Security (4):

CYBERTEC
DATA SCIENCE & POSTGRESQL

```
iMac:~ hs$ psql test -U joe
test=> SELECT * FROM t_test;
 id
----
(0 rows)
```

Row-Level-Security (5):

CYBERTEC
DATA SCIENCE & POSTGRESQL

```
test=# CREATE POLICY mypol ON t_test
    FOR SELECT TO joe USING (id < 3);
CREATE POLICY
test=# \q

iMac:~ hs$ psql test -U joe

test=> SELECT * FROM t_test;
 id
----
  1
  2
(2 rows)
```

Security auf Funktionsebene

CYBERTEC
DATA SCIENCE & POSTGRESQL

```
test=# \h CREATE FUNCTION
Command:     CREATE FUNCTION
Description: define a new function
Syntax:
CREATE [ OR REPLACE ] FUNCTION name ( ... )
...
    [ EXTERNAL ] SECURITY INVOKER |
    [ EXTERNAL ] SECURITY DEFINER
```

- Läuft die Funktion als Caller oder als “Autor”?

PostgreSQL TDE

CYBERTEC
DATA SCIENCE & POSTGRESQL

- “Data At Rest Encryption”
- Manchmal will man die ganze Instanz verschlüsseln
- Der Key wird beim Start der Instanz von einem Modul “beschafft”
- Wir versuchen den Code in PostgreSQL 13 zu bekommen
  - Derzeit für ältere Versionen bei uns verfügbar

Any questions?

Contact us

CYBERTEC
DATA SCIENCE & POSTGRESQL

Cybertec Schönig & Schönig GmbH
Hans-Jürgen Schönig
Gröhrmühlgasse 26
A-2700 Wiener Neustadt

Email: hs@cybertec.at
www.cybertec-postgresql.com

Follow us on Twitter: @PostgresSupport