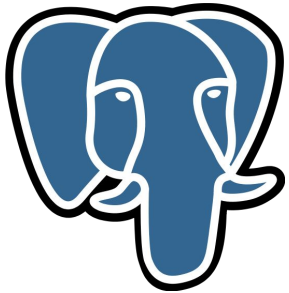
PostgreSQL'de Güvenlik

Güvenlik!



Şahap Aşcı

Cooksoft

sahap.asci@cooksoft.com.tr

@sahapasci

sahapasci


ÖNCE
Veri
İŞ
GÜVENLİĞİ

PostgreSQL Güvenlik Yaklaşımı

PostgreSQL güvenlik güncellemeleri öncelikle küçük (minor) sürüm yükseltmelerinde yayınlanır. Yeni bir büyük (major) versiyon çıktığında bilinen bütün güvenlik sorunları düzeltilmiş olarak çıkar.

PostgreSQL Güvenlik Yaklaşımı

PostgreSQL geliştirme grubu, güvenlik bilgilerinin doğruluğu, eksiksizliği ve kullanılabilirliği kullanıcılarımız için çok önemli olduğuna inanmaktadır. Güvenlik ile ilgili bir açık bulduğunuzu düşündüğünüzde;

security@postgresql.org

PostgreSQL Güvenlik Özellikleri

	11	10	9.6	9.5	9.4	9.3
Channel binding for SCRAM authentication	Yes	No	No	No	No	No
Column level permissions	Yes	Yes	Yes	Yes	Yes	Yes
Default permissions	Yes	Yes	Yes	Yes	Yes	Yes
GRANT/REVOKE ON ALL TABLES/SEQUENCES /FUNCTIONS	Yes	Yes	Yes	Yes	Yes	Yes
GSSAPI support	Yes	Yes	Yes	Yes	Yes	Yes
krb5 authentication (without gssapi)	Obsolete	Obsolete	Obsolete	Obsolete	Obsolete	Yes
Large object access controls	Yes	Yes	Yes	Yes	Yes	Yes
Native LDAP authentication	Yes	Yes	Yes	Yes	Yes	Yes
Native RADIUS authentication	Yes	Yes	Yes	Yes	Yes	Yes
Per user/database connection limits	Yes	Yes	Yes	Yes	Yes	Yes
ROLES	Yes	Yes	Yes	Yes	Yes	Yes
Row-Level Security	Yes	Yes	Yes	Yes	No	No
SCRAM-SHA-256 Authentication	Yes	Yes	No	No	No	No
Search+bind mode operation for LDAP authentication	Yes	Yes	Yes	Yes	Yes	Yes
security_barrier option on views	Yes	Yes	Yes	Yes	Yes	Yes
Security Service Provider Interface (SSPI)	Yes	Yes	Yes	Yes	Yes	Yes
SSL certificate validation in libpq	Yes	Yes	Yes	Yes	Yes	Yes
SSL client certificate authentication	Yes	Yes	Yes	Yes	Yes	Yes
SSPI authentication via GSSAPI	Yes	Yes	Yes	Yes	Yes	Yes

https://www.postgresql.org/about/featurematrix/#security

İçerik

- *Ağ (Network)*
- *İşletim sistemi (host)*
- **PostgreSQL**
  1. İstemci Kimlik Denetimi (Client Authentication)
  2. Veritabanı Rolleri (Database Roles)
  3. Sütun Bazlı Yetkilendirme (Privileges)
  4. Satır Bazlı Ayrıcalıklandırma (Row Security Policies)
  5. pgcrypto

1

İstemci Kimlik Denetimi

Client Authentication

Client Authentication

Makine bazlı kimlik denetimi (Host Based Authentication)

- pg_hba.conf – kimlik denetimi ana dosyası
  - Konfigurasyon parametresi: hba_file
- ident.conf – kullanıcı eşleştirme dosyası
  - Konfigurasyon parametresi: ident_file

pg_hba.conf

```
# TYPE  DATABASE        USER            ADDRESS                 METHOD

# "local" is for Unix domain socket connections only
local   all             all                                     peer
# IPv4 local connections:
host    all             all             127.0.0.1/32            md5
# IPv6 local connections:
host    all             all             ::1/128                 md5
# Allow replication connections from localhost, by a user with the
# replication privilege.
local   replication     all                                     peer
host    replication     all             127.0.0.1/32            md5
host    replication     all             ::1/128                 md5
```

pg_hba.conf

- TYPE
- DATABASE
- USER
- ADDRESS veya IP-ADDRESS + IP-MASK
- METHOD
- OPTIONS

pg_hba.conf - TYPE

local - local unix socket

istemci ve pg aynı makine - şifreleme yok

host - TCP/IP socket ssl veya nossl

istemci ve pg aynı veya farklı makine - ssl'e istemci karar versin

hostssl - TCP/IP socket ssl

istemci ve pg aynı veya farklı makine - istemci ssl'siz bağlanamasın

hostnossl - TCP/IP socket nossl

istemci ve pg aynı veya farklı makine - istemci ssl'siz bağlansın

pg_hba.conf - DATABASE

all	- tüm veritabanları
sameuser	- kullanıcı ile aynı
samerole	- kullanıcının bağlı olduğu rol ile aynı
~~(samegroup)~~	- kullanmayın
replication	- replication protokolü
@dosya_ismi	- listeyi bu dosyadan al

- Virgülle ayırarak liste verebilirsiniz

pg_hba.conf - USER

all – tüm kullanıcılar

+*roleismi* – bu rol'e bağlı tüm kullanıcılar

@dosya_ismi – listeyi bu dosyadan al

- Virgülle ayırarak liste verebilirsiniz

pg_hba.conf - ADDRESS

IPv4

0.0.0.0/0	- Her yerden
84.51.58.74/32	- Sadece bu IP'den
10.1.2.0/24	- 10.1.2 ile başlayan

IPv6

::1/128	- localhost

Host name

localhost	
.cooksoft.com.tr	- cooksoft hariç alt domainler

* host name kullanacaksanız nscd (name service cache daemon) kullanın.

pg_hba.conf - IP-ADDRESS + IP-MASK

84.51.58.74/32 yerine	84.51.58.74	255.255.255.255
10.1.2.0/24 yerine	10.1.2.0	255.255.255.0

pg_hba.conf - METHOD

trust	- şifreleme
reject	- kapı dışarı
scram-sha-256	- yeni geldi en güvenli
md5	- md5 veya scram-sha-256
password	- yalın düz şifre
ident	- işletim sistemi kullanıcısı ile eşleştir

ident.conf

map-name	system-username	database-username
dba	sahap.asci	postgres
dba	zekiye.aydemir	postgres
veya		
dba	/^(.*)@cooksoft\.com\.tr$	postgres

pg_hba.conf:

```
host  all  all  192.168.10.0/24  ident  map=dba
```

pg_hba.conf - METHOD

peer – yerel işletim sistemi kullanıcısı ile eşleştir

ldap – Ldap

```
host   db     +developer  10.10.10.0/24
       ldap ldapserver="server1.net,server2.net" ldapprefix="domainname\"
```

radius – Radius

cert – SSL istemci sertifikası

pam – PAM service

bsd – BSD Authentication service

scram-sha-256

- Simple Authentication and Security Layer (SASL)
- SCRAM-SHA-256
- Password_encryption (enum)
  - md5
  - scram-sha-256

SSL

Centos;

postgresql.conf

ssl=on

```
openssl req -new -text -out cert.req
openssl rsa -in privkey.pem -out cert.pem
openssl req -x509 -in cert.req -text \
-key cert.pem -out cert.cert
cp cert.pem $PGDATA/server.key
cp cert.cert $PGDATA/server.crt
chmod 600 $PGDATA/server.key
chmod 600 $PGDATA/server.crt
```

Debian;

postgresql.conf

ssl=on

2

Veritabanı Rolleri

Database Roles

Veritabanı Rolleri

```
CREATE ROLE …
      SUPERUSER | NOSUPERUSER                    | CREATEDB | NOCREATEDB
      CREATEROLE | NOCREATEROLE                  | INHERIT | NOINHERIT
      LOGIN | NOLOGIN                           | REPLICATION | NOREPLICATION
      *BYPASSRLS | NOBYPASSRLS                  | CONNECTION LIMIT connlimit
      [ ENCRYPTED ] PASSWORD 'password'          | VALID UNTIL 'timestamp'
      IN ROLE role_name [, ...]                  | IN GROUP role_name [, ...]
      ROLE role_name [, ...]                     | ADMIN role_name [, ...]
      USER role_name [, ...]
      | SYSID uid
```

* row level security

3

Sütun Bazlı Yetkilendirme

Privileges

GRANT / REVOKE

- DATABASE
  - CREATE, CONNECT, TEMPORARY, TEMP
- SCHEMA
  - CREATE, USAGE
- TABLE
  - SELECT, INSERT, UPDATE, DELETE, TRUNCATE, REFERENCES, TRIGGER

GRANT / REVOKE

- SEQUENCE
  - USAGE (*currval, nextval*), SELECT, UPDATE
- FUNCTION
  - EXECUTE
- GRANT role_name .. TO role_name
  - WITH ADMIN OPTION

GRANT / REVOKE

GRANT …. ALL TABLES IN SCHEMA … TO ..

GRANT … ALL SEQUENCES IN SCHEMA …TO ..

…

- PUBLIC
- CURRENT_USER
- SESSION_USER

GRANT / REVOKE

Örnekler;

```
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 INSERT ON films TO PUBLIC;
GRANT ALL PRIVILEGES ON kinds TO manuel;
GRANT admins TO joe;
GRANT SELECT ON ALL TABLES IN SCHEMA public TO readonly_role;
```

public schema

```
cooksoftdb=# \dn+
                          List of schemas
  Name   |  Owner   |  Access privileges   |      Description
---------+----------+----------------------+------------------------
 public  | postgres | postgres=UC/postgres+| standard public schema
         |          | =UC/postgres         |
(1 row)
```

```
REVOKE CREATE ON SCHEMA public FROM PUBLIC;
```

4

Satır Bazlı Ayrıcalıklandırma

Row Security Policies

Satır Bazlı Ayrıcalıklandırma

postgresql.conf;

row_security = on (istemci varsayılanı)

on : kurallara (policy) uymayan kayıtları göstermez.

off : kurallara uymayıp gösterilmeyen bir kayıt olursa hata fırlatır.

Satır Bazlı Ayrıcalıklandırma

```
ALTER TABLE t1 ENABLE ROW LEVEL SECURITY;
CREATE POLICY p1 ON t1 FOR SELECT
  USING (expression);
CREATE POLICY p2 ON t1 FOR UPDATE
  USING (expression);
```

- current_user

Satır Bazlı Ayrıcalıklandırma

- TRUNCATE kapsam dışı

5

pgcrypto

pgcrypto

pgcrypto

Pgcrypto ne işe yarar?

- Kriptografik fonksiyonlar bu bileşen içerisinde toplanmıştır. Sağladığı fonksiyonlarda algoritma seçenekleri de verir.

pgcrypto

```
CREATE EXTENSION pgcrypto;
digest(data text, type text) returns bytea
    type: md5, sha1, sha224, sha256, sha384 ve sha512
```

```
gen_salt(type text [, iter_count integer ]) returns text
    Type: bf(72), md5(unlimited), xdes(8), des(8)

crypt(password text, salt text) returns text

    UPDATE ... SET pswhash = crypt('new password',
gen_salt('md5'));
```

pgcrypto

Örnek;

```
UPDATE ... SET sifre = crypt('şifre', gen_salt('md5'));
```

```
SELECT (sifre = crypt('girilen şifre', sifre)) AS onaylandi
FROM ... ;
```

pgcrypto

`gen_random_uuid() returns uuid`

- v4 UUID döner. uuid-ossp bileşenindeki uuid_generate_v4() fonksiyonundan daha hızlıdır.

Teşekkürler!

Varsa soruları alalım?

İletişim

- @sahapasci
- sahap.asci@cooksoft.com.tr

Referanslar

PostgreSQL Dokümantasyonu;

- Security Information
- Client Authentication
- Database Roles
- Privileges
- Row Security Policies
- Pgcrypto