Member-only story

How To Use pgcrypto Extension in Postgresql

MynotesoracleDBA · Follow
3 min read · Mar 15, 2024

Listen Share More

Here, we are going to explore encryption and decryption using pgcrypto in detail

What is a Pgcrypto?

- The `**pgcrypto**` extension enhances PostgreSQL by introducing a suite of cryptographic functions directly within the database environment.
- It supports a broad spectrum of cryptographic operations, such as encryption and decryption, hashing, and the creation and verification of digital signatures.
- `pgcrypto` requires OpenSSL and won't be installed if OpenSSL support was not selected when PostgreSQL was built.

Source: Google

Let us see an example of using **pgcrypto** for password encryption:

S-1: Create a table

- First, we'll create a table named **Team_india**. This table will store the playername, the encrypted mobile, and an email (also encrypted for demonstration purposes).
- We'll use the `bytea` data type for the encrypted fields to accommodate binary data resulting from the encryption process.

```
CREATE TABLE Team_india(
    user_id serial PRIMARY KEY,
    Playername varchar(255) NOT NULL UNIQUE,
    Player_mobileno bytea NOT NULL,
    Player_email bytea NOT NULL
);
```

S-2: Create an extension

```
CREATE EXTENSION PGCRYPTO;
```

- Verify the extension details using **\dx** and function details **\df**

S-3: Insert Sample Data

- To insert data into our **Team_india** table, we'll encrypt the password and email fields using the `pgp_sym_encrypt` function.
- Assume we use a simple symmetric key for this example, though in a real-world scenario, key management practices would be more complex.

```
INSERT INTO Team_india ( playername, player_mobileno,player_email)
VALUES
```

```
('Dhoni', pgp_sym_encrypt('12345890', 'Team_India_Icici'), pgp_sym_encrypt('mah
('Kohli', pgp_sym_encrypt('1234567890', 'Team_India_Icici'), pgp_sym_encrypt('V
```

S-4: Querying and Decrypting Data

- When you need to authenticate a user or display their email, you will decrypt the data on the fly using the `pgp_sym_decrypt` function.
- Here's how you can retrieve and decrypt the email address of a specific user:

```
--without decryption details

select * from Team_india
;
-[ RECORD 1 ]---+------------------------------------------------------------
user_id         | 1
playername      | Dhoni
player_mobileno | \xc30d04070302a98d119eed7407fc67d23901bcedab7e27f3ce682c12f2c
player_email    | \xc30d040703025c05aa90e503958766d23f016dc0e02c65fc35d4ad79290
-[ RECORD 2 ]---+------------------------------------------------------------
user_id         | 2
playername      | Kohli
player_mobileno | \xc30d0407030270ea3745e3c4c6c37fd23b017a0da57ec482d5adb2d3dbf
player_email    | \xc30d040703029f1c48e2c47226cd7fd2430121a89f476437b01d42b04b0



--using a secret key to decryption

select playername,
pgp_sym_decrypt(player_mobileno, 'Team_India_Icici') as Mobileno,
pgp_sym_decrypt(player_email, 'Team_India_Icici') as email
from
Team_india;

-[ RECORD 1 ]------------------
playername | Dhoni
mobileno   | 12345890
email      | mahi@gmail.com
-[ RECORD 2 ]------------------
playername | Kohli
mobileno   | 1234567890
email      | Viruksha@gmail.com
```

S-5: Storing Secret Key in a View

- Sometimes, we might find it cumbersome to manually execute the select query every time. Thus, we can create a view based on the select decryption query.
- This allows anyone with access to simply read the data without needing the secret key, just by using the view.

```
CREATE VIEW team_india_key AS
SELECT
 playername,
 pgp_sym_decrypt(player_mobileno, 'Team_India_Icici') AS Mobileno,
 pgp_sym_decrypt(player_email, 'Team_India_Icici') AS email
FROM
 Team_india;
```

- However, a problem arises here: even if a user doesn't have access to this view, they can see the structure of the view. This means other users can easily obtain the secret key details.

```
\d+ team_india_key
                                View "public.team_india_key"
   Column   |          Type          | Collation | Nullable | Default | Storage
------------+------------------------+-----------+----------+---------+--------
 playername | character varying(255) |           |          |         | extende
 mobileno   | text                   |           |          |         | extende
 email      | text                   |           |          |         | extende
View definition:
 SELECT team_india.playername,
    pgp_sym_decrypt(team_india.player_mobileno, 'Team_India_Icici'::text) AS mc
    pgp_sym_decrypt(team_india.player_email, 'Team_India_Icici'::text) AS email
   FROM team_india;
```

- To mitigate this issue, we can create a separate table to store the key and then pass it into the view. This ensures that other users cannot read the stored key details.

S-6: Create a table to store secret-key values

```
create table Team_india_keys (
    key_id integer NOT NULL,
    secret_key text NOT NULL,
    CONSTRAINT Team_india_keys_pk PRIMARY KEY (key_id)
    );


INSERT INTO Team_india_keys (key_id, secret_key) VALUES (1, 'Team_India_Icici')
```

S-7: Decrypt the values

- We can decrypt the values like below without using them anywhere

```
select playername,
pgp_sym_decrypt(player_mobileno, dec_key.seckey) as Mobileno,
pgp_sym_decrypt(player_email, dec_key.seckey) as email
from
Team_india
cross join
(select secret_key as seckey from Team_india_keys) as dec_key;

 playername |  mobileno  |       email
------------+------------+--------------------
 Dhoni      | 12345890   | mahi@gmail.com
 Kohli      | 1234567890 | Viruksha@gmail.com
(2 rows)
```

- You can also create a view based on the above select query. This ensures that non-privileged users cannot read the secret key value unless they have access to the `**Team_india_keys**` table.

Postgres | Postgresql | Extension | Tutorial | Database Administration

Follow

Written by MynotesoracleDBA

311 Followers · 14 Following

As a DBA we are going to write and discuss multiple database administration concepts. “Nothing Grows In Comfort Zone”.

No responses yet

Gvadakte

What are your thoughts?

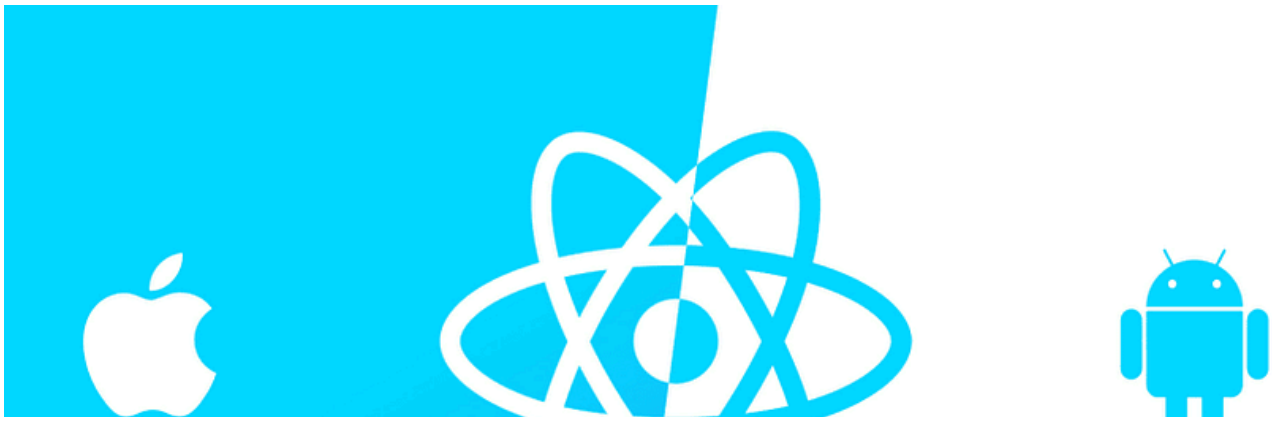
More from MynotesoracleDBA

In Nerd For Tech by MynotesoracleDBA

What Is A PGA In Oracle?

Here we are going to understand the components of PGA

Feb 6, 2022 5



In Geek Culture by Anshul Borawake

React Native Generate APK—Debug and Release APK

Generate Debug and Release APK in React Native; Windows, iOS and Linux

Apr 3, 2021 1.8K 16

In Geek Culture by Hasitha Subhashana

Circuit Breaker Pattern (Design Patterns for Microservices)

In a distributed system we have no idea how other components would fail. Network issues could occur, components could fail or a router or a...

Jun 12, 2021 906 11

In Nerd For Tech by MynotesoracleDBA

How a SQL Statement is processed in Oracle?| Interview Q& A

Here we are going to understand the SQL statement processing steps in oracle

Dec 7, 2021 3

See all from MynotesoracleDBA

Recommended from Medium

In Databases by Sergey Egorenkov

Making SQL query 40x faster for 10 million rows table

Make your SQL query really fast using this approach

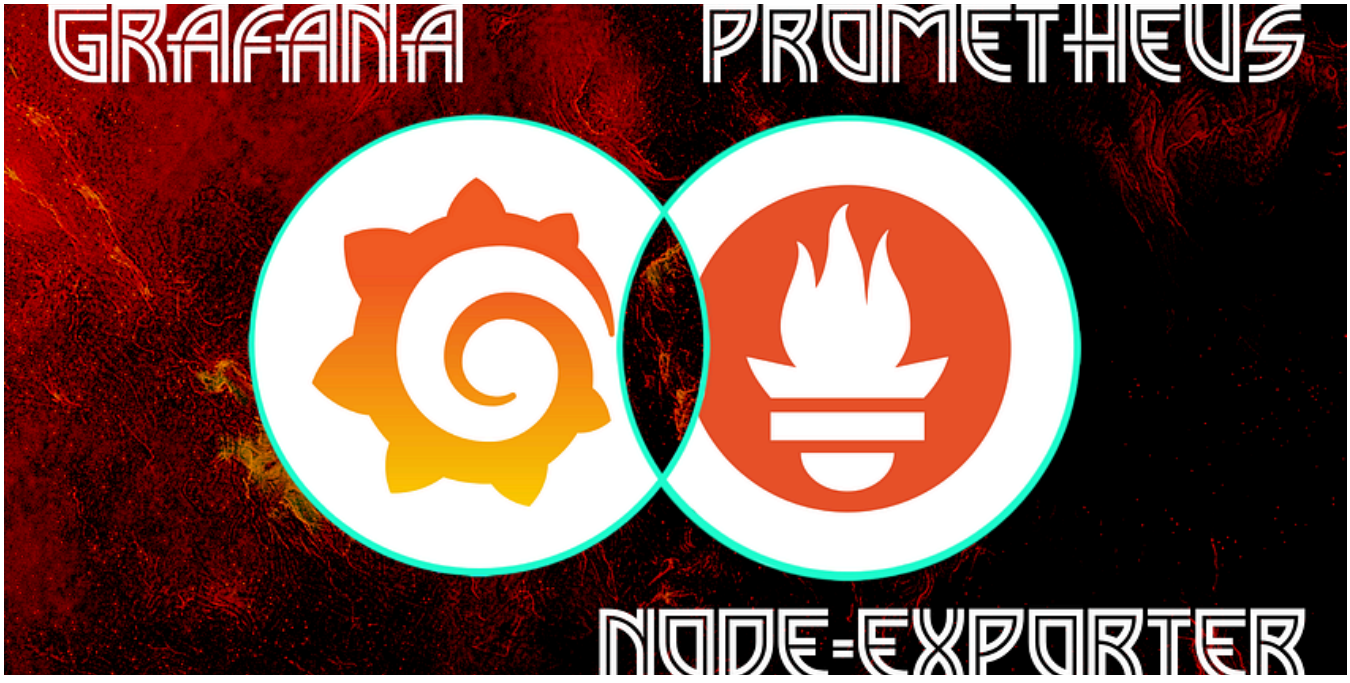
Mar 17 10

Tihomir Manushev

Vector Search with pgvector in PostgreSQL

Simple AI-powered similarity search

Mar 9



crptcpchk

Grafana, Prometheus & Node-Exporter | Setup Guide

Grafana open source software enables you to query, visualize, alert on, and explore your metrics, logs, and traces wherever they are stored...

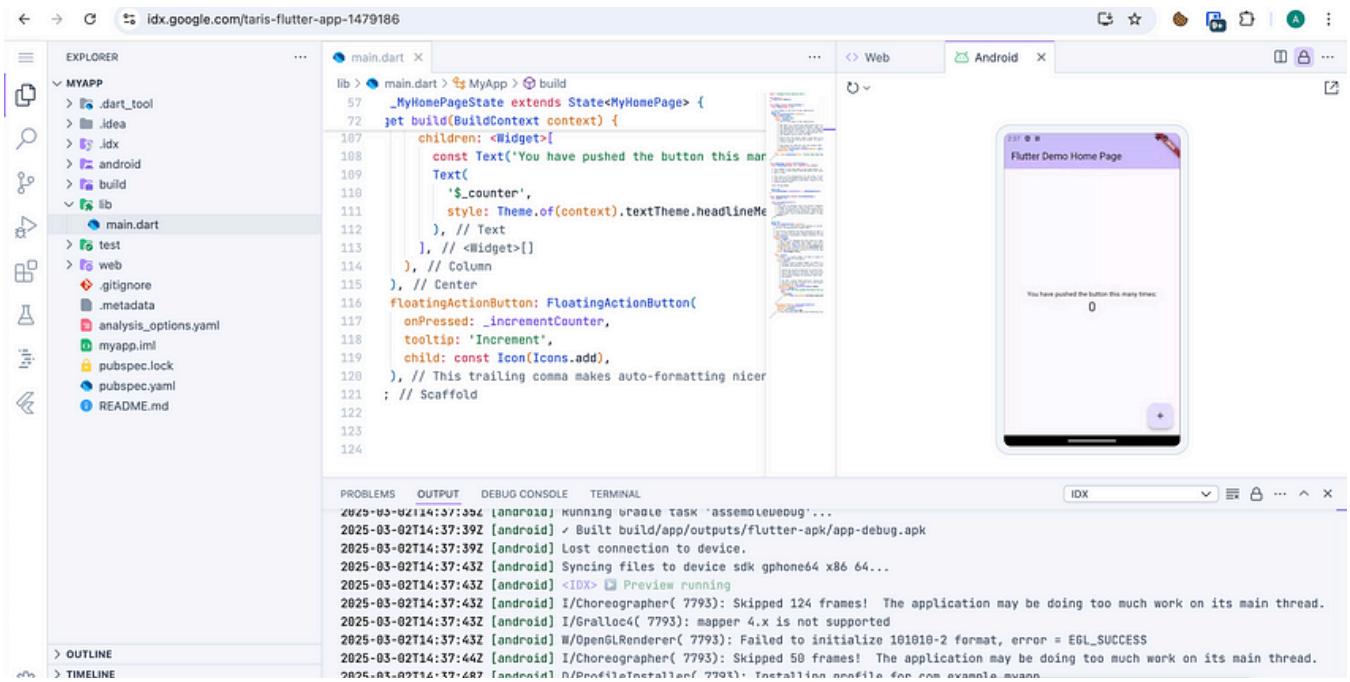
Oct 30, 2024 8 1

In Hack the Stack by Coders Stop

9 Database Optimization Tricks SQL Experts Are Hiding From You

Most developers learn enough SQL to get by—SELECT, INSERT, UPDATE, DELETE, and maybe a few JOINs. They might even know how to create...

Mar 27 196 5

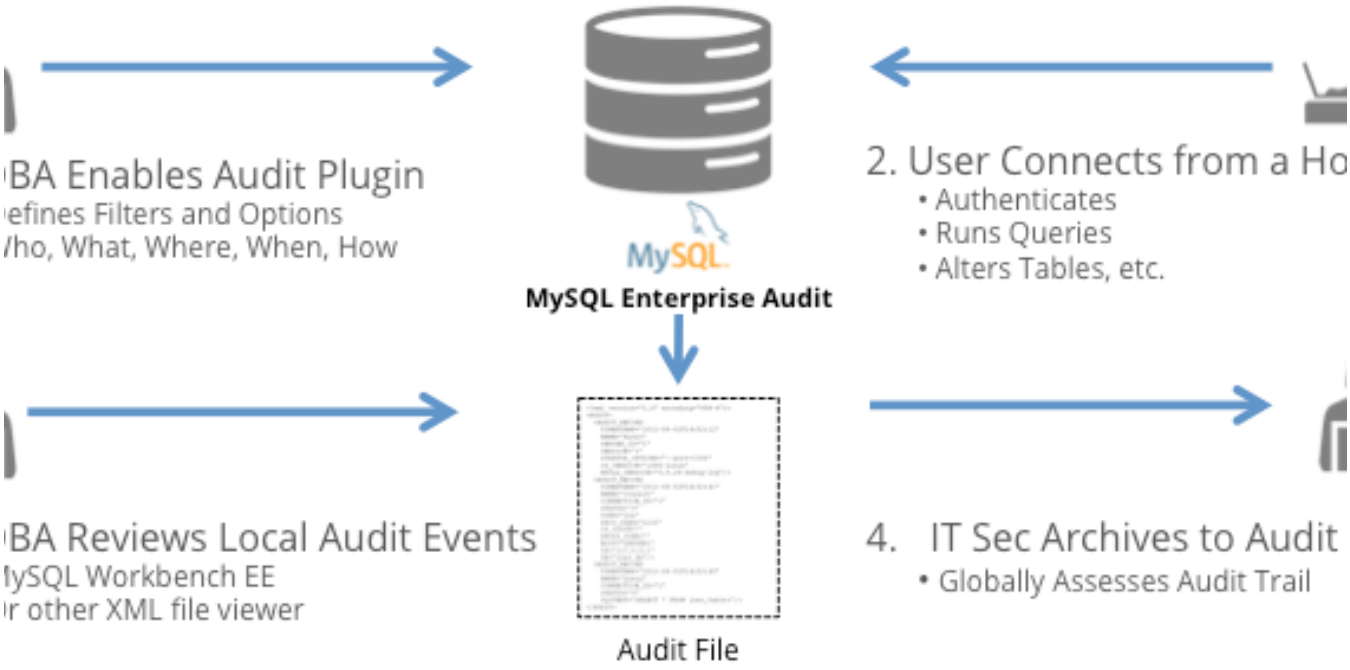


In Coding Beauty by Tari Ibaba

This new IDE from Google is an absolute game changer

This new IDE from Google is seriously revolutionary.

Mar 12 3.7K 201



Hari

How to Enable MYSQL DB audit logs

Step 1: Install the MySQL Enterprise Audit Plugin

Nov 12, 2024 53

See more recommendations