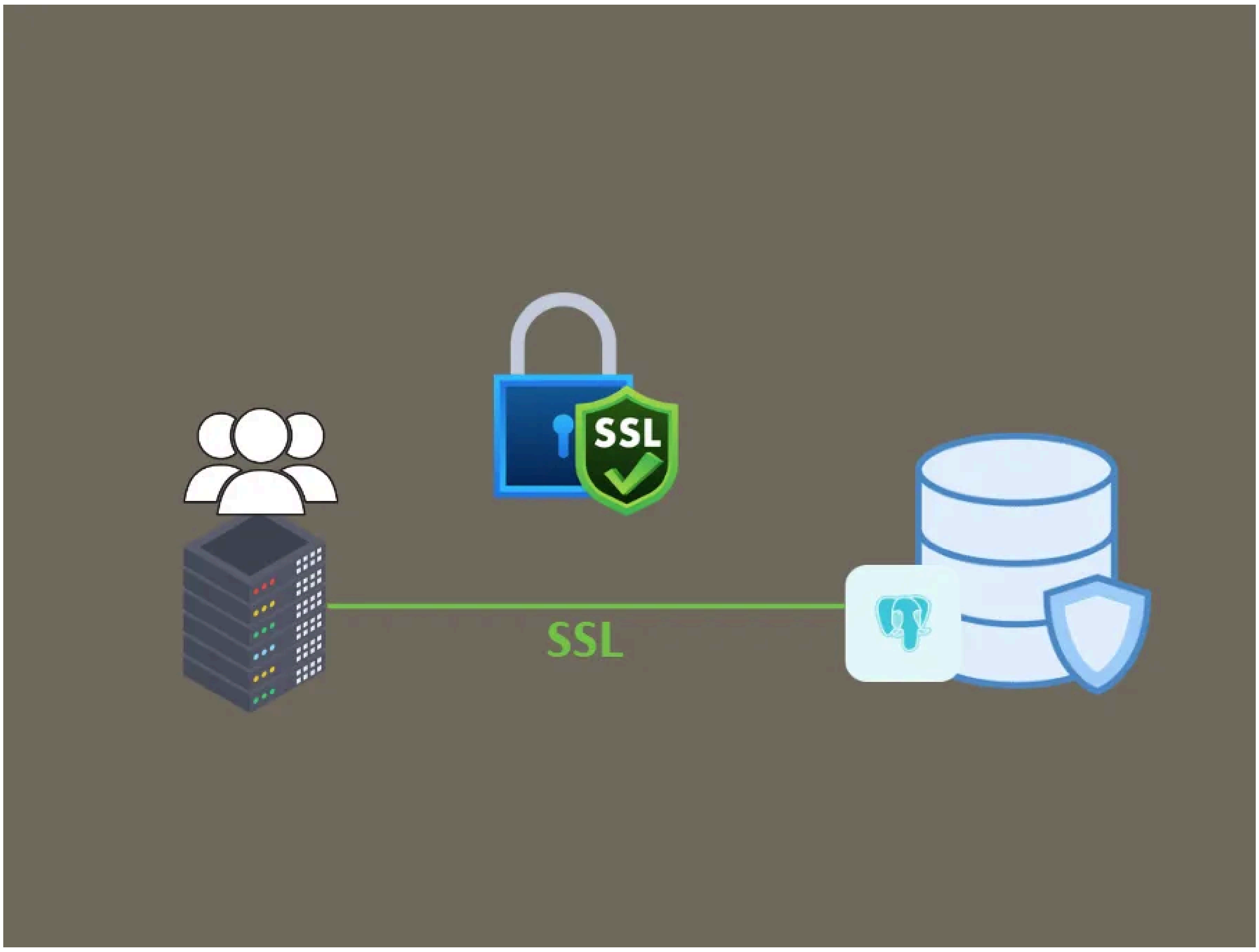
Securing PostgreSQL with SSL Encryption

Oz · Following
3 min read · Jun 10, 2024

When implementing Patroni for PostgreSQL high availability, ensuring secure connections is paramount. One essential aspect is configuring SSL encryption to safeguard data transmission. Below is a step-by-step guide to configure SSL encryption for Patroni-managed PostgreSQL instances, along with detailed explanations at each stage.



Step 1: Patroni Configuration Update

```
patronictl -c /etc/patroni/patroni.yml edit-config
```

Adjust the `patroni.yml` configuration file to incorporate SSL encryption:

```
# force clients to use TLS v1.3 or newer

postgresql:
  parameters:
    ssl: true
    ssl_ca_file: /var/data/root.crt
    # (change requires restart)
    ssl_cert_file: /var/data/server.crt
    ssl_ciphers: TLS_AES_256_GCM_SHA384:TLS_AES_128_GCM_SHA256:TLS_AES_128_CCM_
    ssl_crl_file: ''
    # (change requires restart)
    ssl_key_file: server.key
    # force clients to use TLS v1.3 or newer
```

```
      ssl_min_protocol_version: TLSv1.3
      ssl_passphrase_command: This is only test
      ssl_prefer_server_ciphers: true
```

Ensure to specify SSL-related parameters including the CA file, server certificate, key file, and preferred ciphers. Set other parameters such as `loop_wait` and `maximum_lag_on_failover` to tailor Patroni's behavior.

Step 2: SSL Key and Certificate Generation

To create a simple self-signed certificate for the server, valid for 3650 days, use the following OpenSSL command, replacing ***`dbhost.yourdomain.com`*** with the server's host name:

```
cd /var/data/

openssl req -new -x509 -days 3650 -nodes -text -out server.crt \
  -keyout server.key -subj "/CN=dbhost.yourdomain.com"

chmod og-rwx server.key
```

To create a server certificate whose identity can be validated by clients, first create a certificate signing request (CSR) and a public/private key file:

```
openssl req -new -nodes -text -out root.csr \
  -keyout root.key -subj "/CN=root.yourdomain.com"
chmod og-rwx root.key
```

Then, sign the request with the key to create a root certificate authority (using the default OpenSSL configuration file location on Linux):

```
openssl x509 -req -in root.csr -text -days 3650 \
  -extfile /etc/ssl/openssl.cnf -extensions v3_ca \
  -signkey root.key -out root.crt
```

Step 3: Generate trusted root certificate

Finally, create a server certificate signed by the new root certificate authority:

```
openssl req -new -nodes -text -out server.csr \
  -keyout server.key -subj "/CN=dbhost.yourdomain.com"
chmod og-rwx server.key

openssl x509 -req -in server.csr -text -days 3650 \
  -CA root.crt -CAkey root.key -CAcreateserial \
  -out server.crt
```

Step 4: Bonus: create chain of trust that includes intermediate certificates:

```
# root
openssl req -new -nodes -text -out root.csr \
  -keyout root.key -subj "/CN=root.yourdomain.com"
chmod og-rwx root.key
openssl x509 -req -in root.csr -text -days 3650 \
  -extfile /etc/ssl/openssl.cnf -extensions v3_ca \
  -signkey root.key -out root.crt

# intermediate
openssl req -new -nodes -text -out intermediate.csr \
  -keyout intermediate.key -subj "/CN=intermediate.yourdomain.com"
chmod og-rwx intermediate.key
openssl x509 -req -in intermediate.csr -text -days 1825 \
  -extfile /etc/ssl/openssl.cnf -extensions v3_ca \
  -CA root.crt -CAkey root.key -CAcreateserial \
  -out intermediate.crt

# leaf
openssl req -new -nodes -text -out server.csr \
  -keyout server.key -subj "/CN=dbhost.yourdomain.com"
chmod og-rwx server.key
openssl x509 -req -in server.csr -text -days 365 \
  -CA intermediate.crt -CAkey intermediate.key -CAcreateserial \
  -out server.crt
```

Step 5: Update pg_hba.conf

Edit the `pg_hba.conf` file to allow SSL-encrypted connections:

```
hostssl all all 10.10.80.68/32 md5
```

Specify the appropriate authentication method (`md5`) and SSL settings.

Step 6: Test SSL Connection and Check

```
psql 'host=10.10.80.68 user=postgres sslmode=require'

select name, setting from pg_settings where name like 'ssl%file';
        name         |       setting
---------------------+----------------------
 ssl_ca_file         | /var/data/root.crt
 ssl_cert_file       | /var/data/server.crt
 ssl_crl_file        |
 ssl_dh_params_file |
 ssl_key_file        | server.key
(5 rows)
```

Step 7: Additional Information

1. Use TYPE hostssl when administrating the database cluster as a superuser.
2. Use TYPE hostnossl for performance purposes and when DML operations are deemed safe without SSL connections.
3. A self-signed certificate can be used for **testing**, but a certificate signed by a certificate authority (CA) (either one of the global CAs or a local one) should be used in **production** so that clients can verify the server's identity. **If all the database clients are local to the organization, using a local CA is recommended.**

Connect to the PostgreSQL server using `psql` with SSL mode set to `require` . Input the necessary credentials and observe successful SSL connection establishment. By meticulously following these steps alongside the provided configuration commands, SSL encryption can be seamlessly integrated into Patroni-managed PostgreSQL instances, fortifying data security during transmission. For more detailed and technical articles like this, keep following our blog on Medium. If you have any questions or need further assistance, feel free to reach out in the comments below and directly.

Ssl Certificate · Secure Socket Layer · Openssl · Pem · Database Security

Following

Written by Oz

149 Followers · 13 Following

Database Administrator 🐘

No responses yet

Gvadakte

What are your thoughts?

More from Oz

Oz

Managing Time Series Data Using TimeScaleDB on Postgres

TimescaleDB is an open-source time-series database optimized for fast ingest and complex queries, built on PostgreSQL. This guide will help…

Jul 18, 2024 125

Queries

time	Service	username	Query	Execution_time
2024-09-26 13:15:00	pmm-server-postgresql	pmm-ma…	SELECT /* agent='pgstatstatements' */ "pg_stat_statements"."userid", "pg_stat_statements"."dbid", "pg_stat_statements"."queryi…	0.0242
2024-09-26 13:19:00	pmm-server-postgresql	pmm-ma…	SELECT current_database() datname, schemaname, relname, heap_blks_read, heap_blks_hit, idx_blks_read, idx_blks_hit, toast_b…	0.0165
2024-09-26 13:10:48	pmm-server-postgresql	pmm-ma…	SELECT * FROM pg_stat_database_conflicts	0.0159
2024-09-26 13:18:00	pmm-server-postgresql	pmm-ma…	SELECT /* agent='pgstatstatements' */ "pg_stat_statements"."userid", "pg_stat_statements"."dbid", "pg_stat_statements"."queryi…	0.0131
2024-09-26 13:19:00	pmm-server-postgresql	pmm-ma…	SELECT /* agent='pgstatstatements' */ "pg_stat_statements"."userid", "pg_stat_statements"."dbid", "pg_stat_statements"."queryi…	0.0131
2024-09-26 13:12:00	pmm-server-postgresql	pmm-ma…	SELECT /* agent='pgstatstatements' */ "pg_stat_statements"."userid", "pg_stat_statements"."dbid", "pg_stat_statements"."queryi…	0.0126
2024-09-26 13:15:00	pmm-server-postgresql	pmm-ma…	SELECT current_database() datname, schemaname, relname, heap_blks_read, heap_blks_hit, idx_blks_read, idx_blks_hit, toast_b…	0.0113

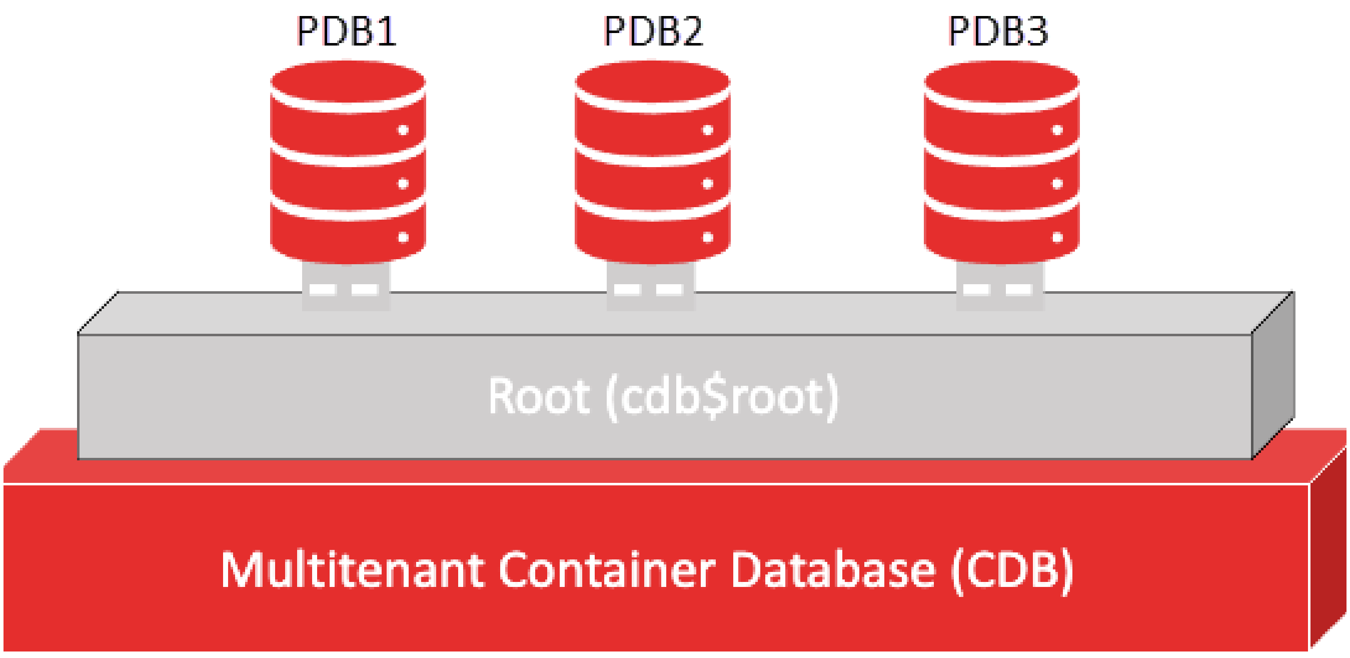
1 - 7 of 538 rows

Oz

Installing Percona Monitoring & Management (PMM) with Postgres

Introduction:

Sep 26, 2024 54 1

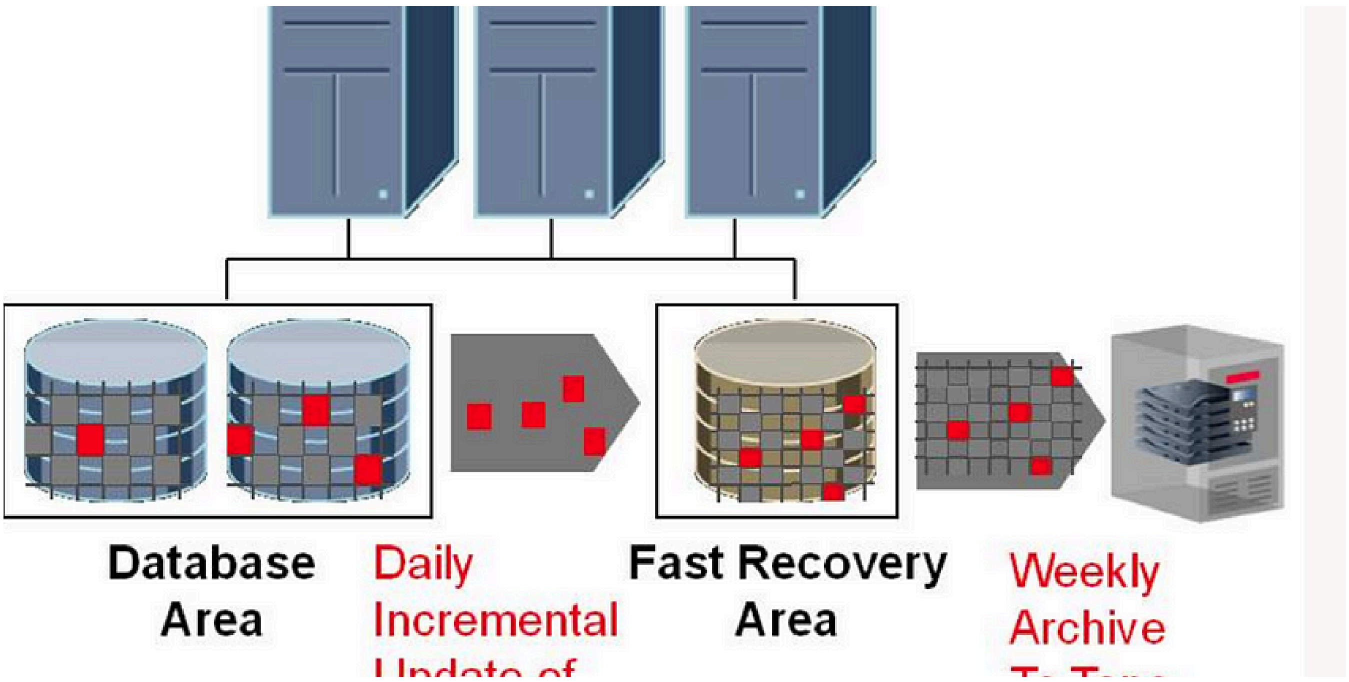


Oz

Pluggable Database Command

—————————— -————————————— - create pluggable database pdb1 admin user root identified by test123; alter pluggable database…

May 12, 2023



Oz

RMAN Backup Basic Commands

rman target / rman target sys/password@YDKTST; backup database; backup database format '/backup/path/%d_%t_%s.rman'; backup tablespace…

May 11, 2023 1

See all from Oz

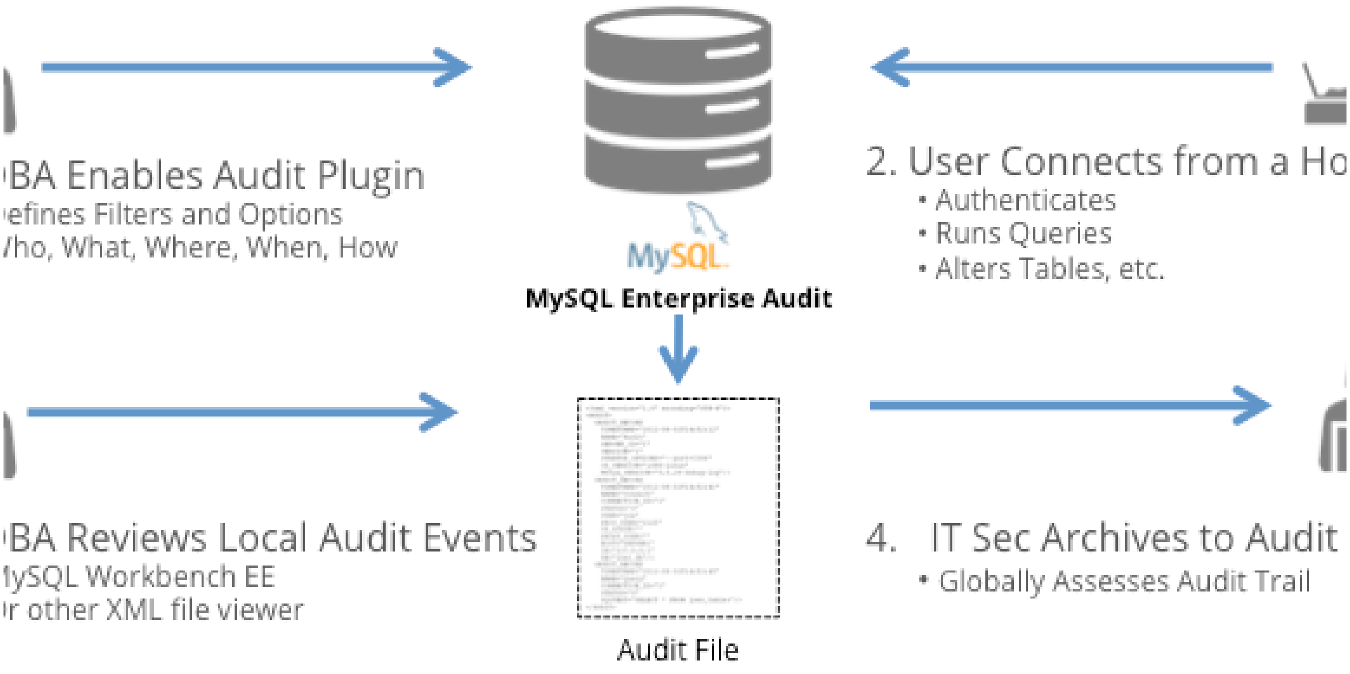
Recommended from Medium

Anubhav Bhardwaj

PostgreSQL Monitoring Script with Email Alerts

Overview

Jan 14 5


BA Enables Audit Plugin
efines Filters and Options
/ho, What, Where, When, How
MySQL Enterprise Audit
2. User Connects from a Ho
• Authenticates
• Runs Queries
• Alters Tables, etc.
BA Reviews Local Audit Events
1ySQL Workbench EE
r other XML file viewer
Audit File
4. IT Sec Archives to Audit
• Globally Assesses Audit Trail

Hari

How to Enable MYSQL DB audit logs

Step 1: Install the MySQL Enterprise Audit Plugin

Nov 12, 2024 53

In Towards Dev by Nakul Mitra

PostgreSQL Performance Optimization — Cleaning Dead Tuples & Reindexing

Performance optimization is crucial in PostgreSQL to ensure efficient query execution and minimal resource consumption.

Mar 28 1

mehmetozanguven

Running PostgreSQL with Podman

Instead of running PostgresSQL locally, we can easily run with Podman. Here are the basic steps you should follow.

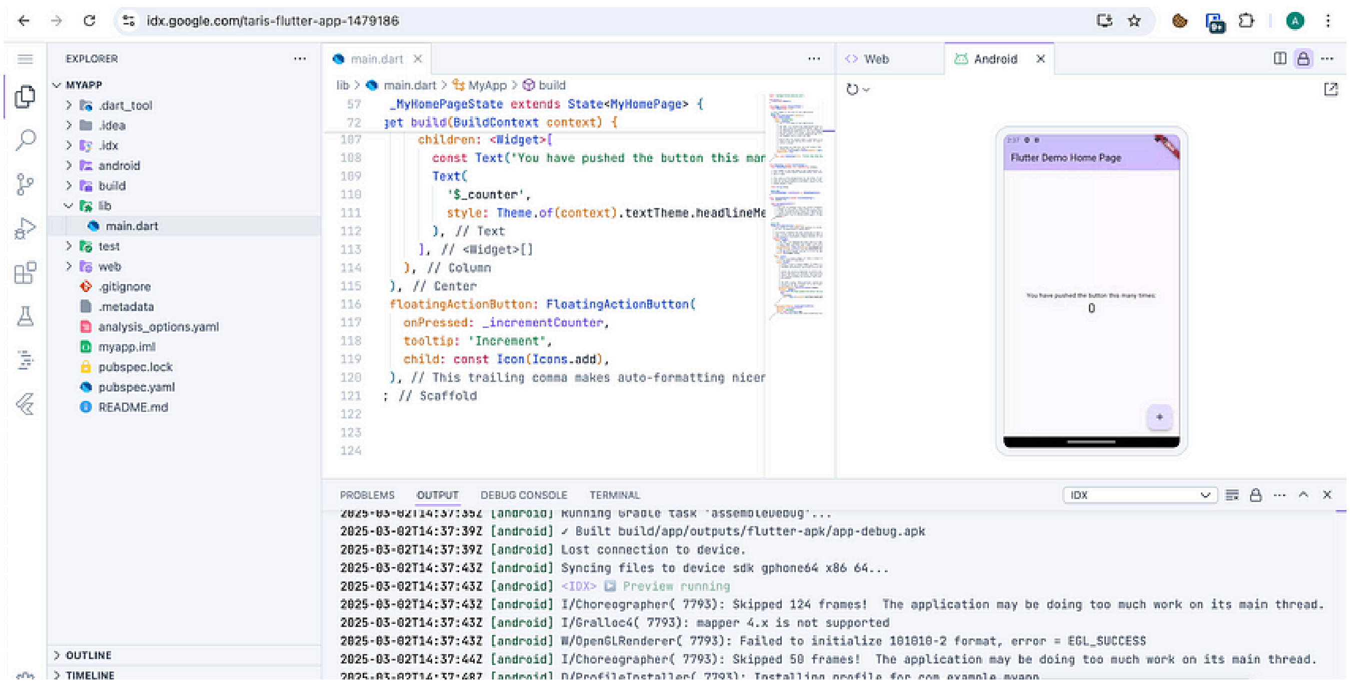
Mar 28 2

Dickson Gathima

Patroni PostgreSQL High Availability with pgBackRest

In my previous post, I configured a 4-node PostgreSQL HA cluster to ensure high availability and failover capabilities. Now, I'd like to...

Mar 24 52 1



```
_MyHomePageState extends State<MyHomePage> {
jet build(BuildContext context) {
      children: <Widget>[
        const Text('You have pushed the button this man
        Text(
          '$_counter',
          style: Theme.of(context).textTheme.headlineMe
        ), // Text
      ], // <Widget>[]
    ), // Column
  ), // Center
  floatingActionButton: FloatingActionButton(
    onPressed: _incrementCounter,
    tooltip: 'Increment',
    child: const Icon(Icons.add),
  ), // This trailing comma makes auto-formatting nicer
; // Scaffold
```

```
2025-03-02T14:37:35Z [android] Running Gradle task 'assembleDebug'...
2025-03-02T14:37:39Z [android] ✓ Built build/app/outputs/flutter-apk/app-debug.apk
2025-03-02T14:37:39Z [android] Lost connection to device.
2025-03-02T14:37:43Z [android] Syncing files to device sdk gphone64 x86 64...
2025-03-02T14:37:43Z [android] <IDX> Preview running
2025-03-02T14:37:43Z [android] I/Choreographer( 7793): Skipped 124 frames!  The application may be doing too much work on its main thread.
2025-03-02T14:37:43Z [android] I/Gralloc4( 7793): mapper 4.x is not supported
2025-03-02T14:37:43Z [android] W/OpenGLRenderer( 7793): Failed to initialize 101010-2 format, error = EGL_SUCCESS
2025-03-02T14:37:44Z [android] I/Choreographer( 7793): Skipped 50 frames!  The application may be doing too much work on its main thread.
2025-03-02T14:37:48Z [android] D/ProfileInstaller( 7793): Installing profile for com.example.myapp
```

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 3.6K 200

See more recommendations