EDB
Postgres® for the AI Generation

EDB Postgres® AI

Webinaire - Sécurité et conformité de vos bases de données PostgreSQL

Eric Pillon, **Strategic Account Executive**
Raphael Chir, **Senior Sales Engineer**

April 29, 2025

EDB
Postgres for the AI Generation

Agenda

- Who is EDB?
- DORA
- Security layers
- Demo

Who is EDB?

Who is EDB?

1500+ Enterprises and Growing

EDB deeply understands Enterprise Postgres needs.

79 Countries around the World

Global footprint and employee base.

Millions of people using Postgres in the world

Long-term customers and deep Postgres capabilities.

3 of 7 Postgres Core Team Members, 7 Committers, 40+ Contributors

EDB is the leading Postgres community contributor.

30% of Postgres Code Contributed in 2023

Driving the innovation and foundation of Postgres.

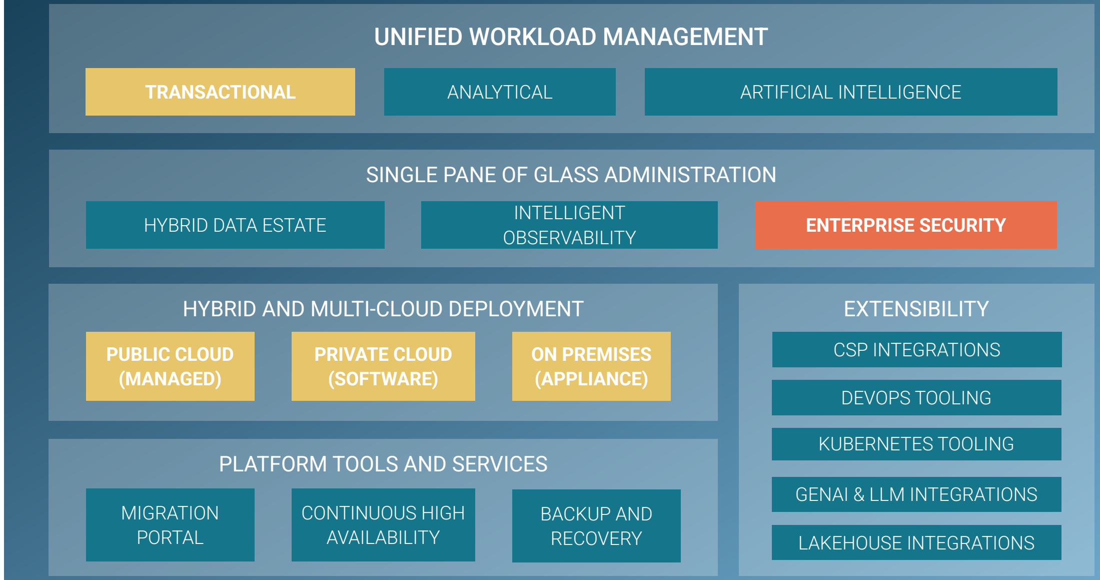
>300 Dedicated Postgres engineers

Unparalleled expertise in Postgres.

EDB
Postgres® AI

An intelligent platform for unified management of transactional, analytical, and AI workloads - powered by Postgres.

EDB POSTGRES AI PLATFORM



UNIFIED WORKLOAD MANAGEMENT

- TRANSACTIONAL
- ANALYTICAL
- ARTIFICIAL INTELLIGENCE

SINGLE PANE OF GLASS ADMINISTRATION

- HYBRID DATA ESTATE
- INTELLIGENT OBSERVABILITY
- ENTERPRISE SECURITY

HYBRID AND MULTI-CLOUD DEPLOYMENT

- PUBLIC CLOUD (MANAGED)
- PRIVATE CLOUD (SOFTWARE)
- ON PREMISES (APPLIANCE)

PLATFORM TOOLS AND SERVICES

- MIGRATION PORTAL
- CONTINUOUS HIGH AVAILABILITY
- BACKUP AND RECOVERY

EXTENSIBILITY

- CSP INTEGRATIONS
- DEVOPS TOOLING
- KUBERNETES TOOLING
- GENAI & LLM INTEGRATIONS
- LAKEHOUSE INTEGRATIONS

Delivered with world-class strategic partners:

carahsoft

Red Hat

IBM

SUPERMICRO

NUTANIX

Which Core EDB Plan Is Right for Your Organization?

EDB Community 360 Plan

Protect PostgreSQL with EDB Expert Support

Software:
PostgreSQL

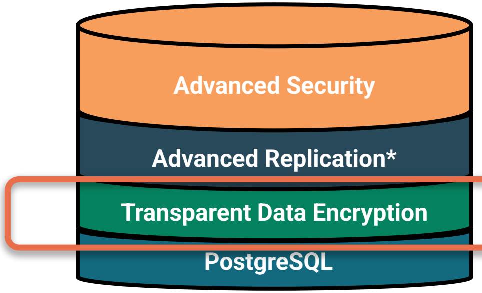
PostgreSQL

- Open Source Tools
- Community PostgreSQL
- EDB & Community Support
- CloudNativePG

EDB Standard Plan

Strengthen and extend PostgreSQL with enhanced security, resiliency, reliability and optimization.

Software:
EDB Postgres Extended

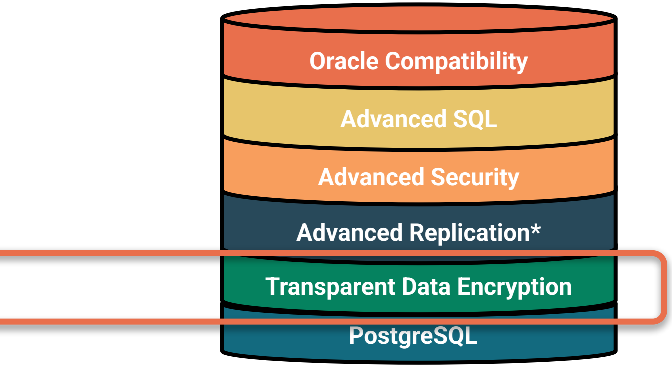


- Open Source Tools
- Community PostgreSQL
- EDB & Community Support
- EDB Postgres for Kubernetes
- EDB Tools & Extension - including PEM
- EDB Postgres Distributed Add-on*
- EDB Postgres Extended

EDB Enterprise Plan

Migrate costly Oracle workloads to Postgres or elevate Postgres to enterprise-grade with advanced security, reliability and much more.

Software:
EDB Postgres Advanced Server (EPAS)



- Open Source Tools
- Community PostgreSQL
- EDB & Community Support
- EDB Postgres for Kubernetes
- EDB Tools & Extension - Including PEM
- EDB Postgres Distributed Add-on*
- EDB Postgres Extended
- EDB Postgres Advanced Server

DORA

DORA

In the context of banking, DORA stands for the Digital Operational Resilience Act, a regulatory framework established by the European Union (EU) to strengthen the digital resilience of financial entities. It applies to banks, investment firms, payment institutions, and other entities operating within the EU financial sector.

Objectives

- Ensure that financial institutions can withstand, respond to, and recover from all types of ICT (Information and Communication Technology) disruptions and threats.
- Create a harmonized regulatory **framework** across the EU to reduce fragmentation in cybersecurity and ICT risk management.

Core requirements

- ICT Risk Management: Institutions must establish robust frameworks for managing ICT risks, including governance, internal controls, and incident response mechanisms.
- Incident Reporting
- Digital Operational Resilience Testing
- Third-Party Risk Management
- Information Sharing

Timeline

- Adopted in 2022
- **Implementation expected by January 2025**

Why is DORA important?

- Cybersecurity
- Consumer Trust
- Regulatory consistency

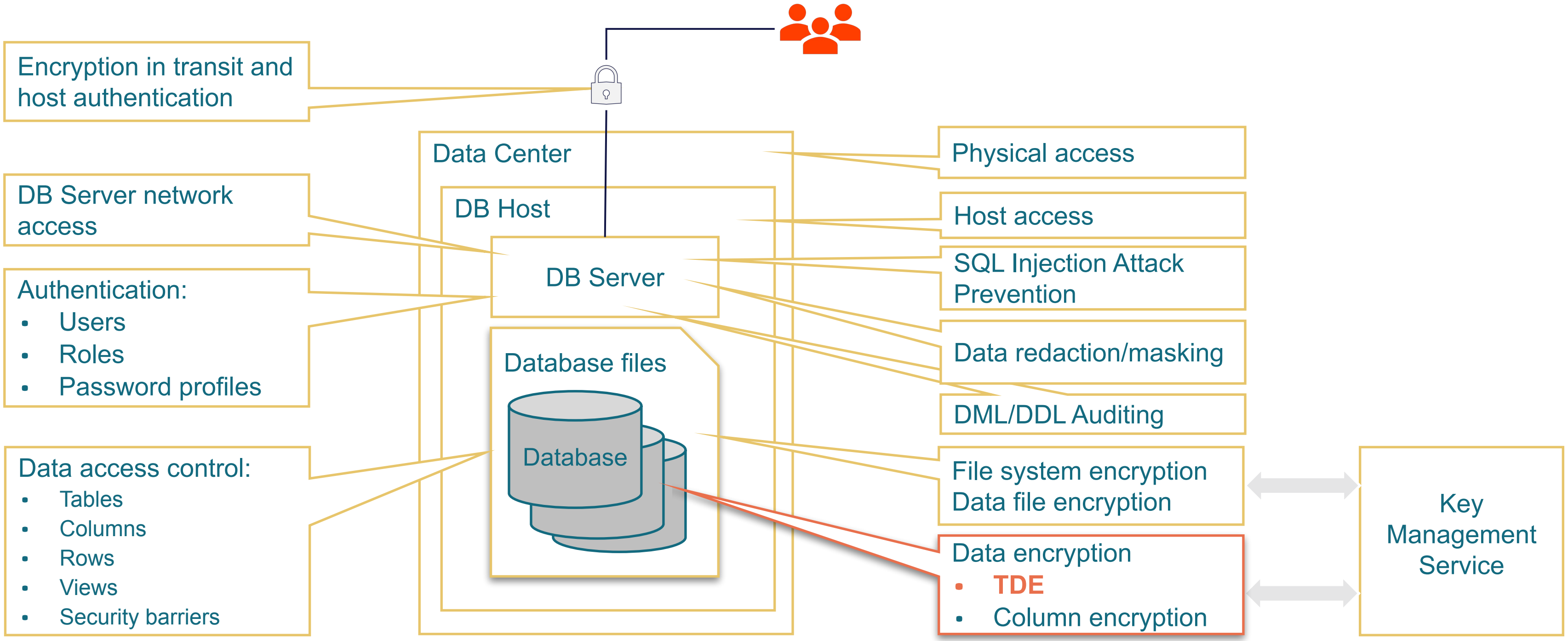
Security, security, security

Security: Where we are today!

Here are some general figures and trends that were relevant up to that date:

- **Number of Data Leaks**: The number of reported data leaks has increased in recent years, with thousands reported each year worldwide.
- **Number of Data Exposed**: The number of records or data exposed in these leaks varies considerably, ranging from a few thousand to hundreds of millions or even billions of records.
- **Targeted sectors**: The most frequently targeted sectors include healthcare, financial services, retail, government agencies and the technology industry.
- **Data Leakage Methods**: Common methods of data leakage include ransomware attacks, security breaches, human error, phishing and internal data leaks.
- **Financial consequences**: Data leaks can entail huge costs for companies, including remediation, loss of reputation and legal penalties.

Multiple layers of security



Encryption in transit and host authentication

DB Server network access

Authentication:
- Users
- Roles
- Password profiles

Data access control:
- Tables
- Columns
- Rows
- Views
- Security barriers

Physical access

Host access

SQL Injection Attack Prevention

Data redaction/masking

DML/DDL Auditing

File system encryption
Data file encryption

Data encryption
- **TDE**
- Column encryption

Key Management Service

What is TDE?

1. **Transparent Data Encryption** (TDE) is a **feature** of EDB Postgres Advanced Server and EDB Postgres Extended Server that prevents unauthorized viewing of data in operating system files on the database server and on backup storage

2. **Data encryption and decryption is managed by the database** and does not require application changes or updated client drivers

3. Data will be unintelligible for unauthorized users if stolen or misplaced

Key Management Service

- **Data Encryption**: Encrypt data at rest (such as in databases or storage) or in transit using encryption keys.
- **Key Lifecycle Management**: Create, rotate, and retire cryptographic keys in a secure manner.
- **Access Control**: Control who has access to certain keys and ensure only authorized entities can use them.
- **Compliance**: Helps meet regulatory requirements for handling sensitive data and encryption.

Key Management Service supported

- HashiCorp Vault (**KMIP Secrets Engine** and **Transit Secrets Engine**)
- Amazon AWS Key Management Service (KMS)
- Google Cloud - Cloud Key Management Service
- Microsoft Azure Key Vault
- Thales CipherTrust Manager

HashiCorp Vault

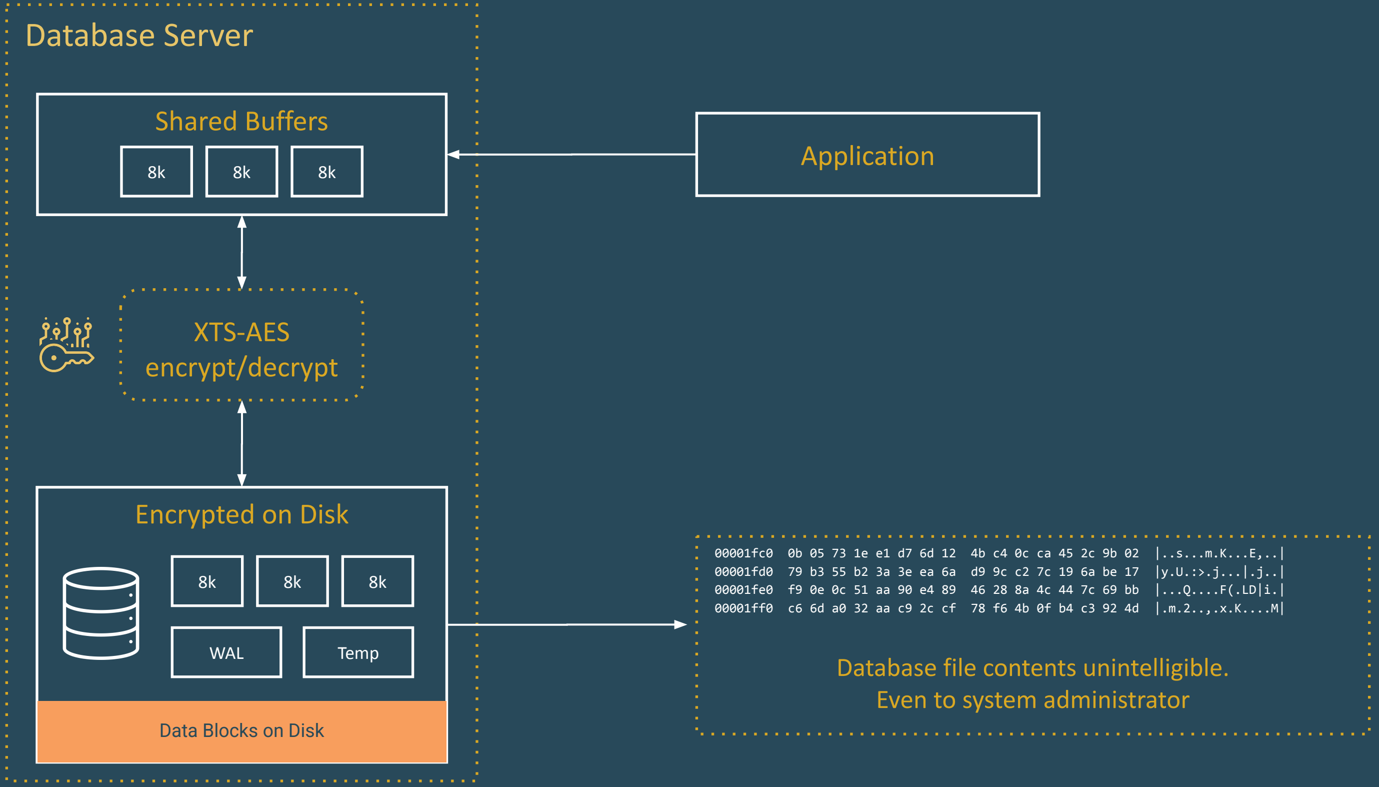
AWS KMS

Azure Key Vault

Google KMS

Thales CipherTrust Manager

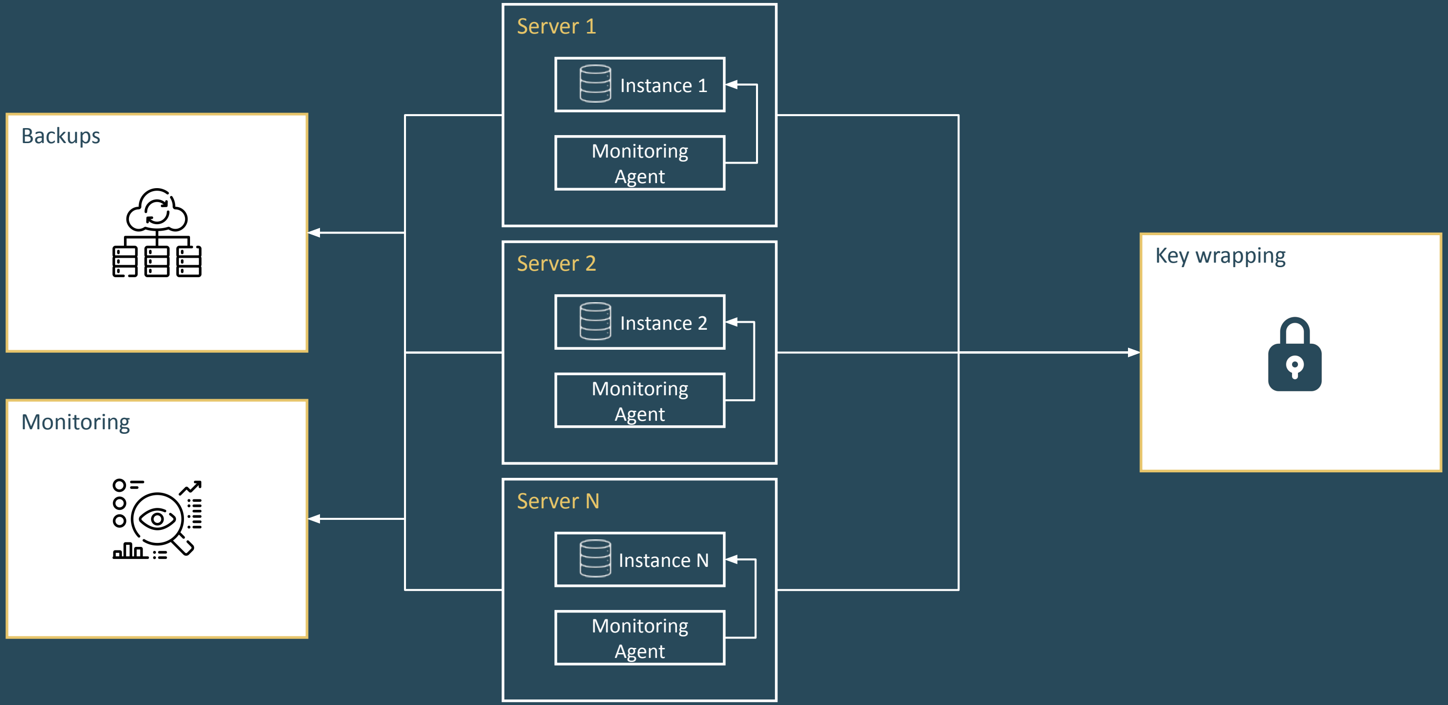
High Level Overview of TDE



```
00001fc0  0b 05 73 1e e1 d7 6d 12  4b c4 0c ca 45 2c 9b 02  |..s...m.K...E,..|
00001fd0  79 b3 55 b2 3a 3e ea 6a  d9 9c c2 7c 19 6a be 17  |y.U.:>.j...|.j..|
00001fe0  f9 0e 0c 51 aa 90 e4 89  46 28 8a 4c 44 7c 69 bb  |...Q....F(.LD|i.|
00001ff0  c6 6d a0 32 aa c9 2c cf  78 f6 4b 0f b4 c3 92 4d  |.m.2..,.x.K....M|
```

Database file contents unintelligible.
Even to system administrator

Transparent Data Encryption (TDE)



What exactly is encrypted?

- All Data files
  - Tables
  - Sequences
  - Indexes
  - TOAST tables
  - System catalogs
- Write Ahead Log (WAL)
- Temporary files
  - tuplestore
  - sort
  - hash join

What isn’t encrypted?

- Metadata internal to the operation of the database (does not contain user data): pg_subtrans, pg_xact, etc.
- File names and file system structure in PGDATA
- Data in foreign tables
- Server diagnostics log
- Configuration files (pg_hba.conf, postgresql.conf)

How is the TDE enabled?

- Transparent data encryption is enabled when the database cluster is first initialized
- The Database Encryption Key (DEK) is generated and encrypted by initdb and stored in a directory within **PGDATA**
- To secure the DEK, it should be wrapped by encrypting it with another key

```
export PGDATAKEYWRAPCMD='openssl enc -e -aes128-wrap -pbkdf2 -out "%p"'
export PGDATAKEYUNWRAPCMD='openssl enc -d -aes128-wrap -pbkdf2 -in "%p"'

initdb --data-encryption
```

- The EDB implementation is flexible and allows any command to be used to WRAP and UNWRAP the DEK
- Data is encrypted with AES-128-XTS

Source: https://www.enterprisedb.com/blog/TDE-Postgres-Advanced-Server-15-Launch

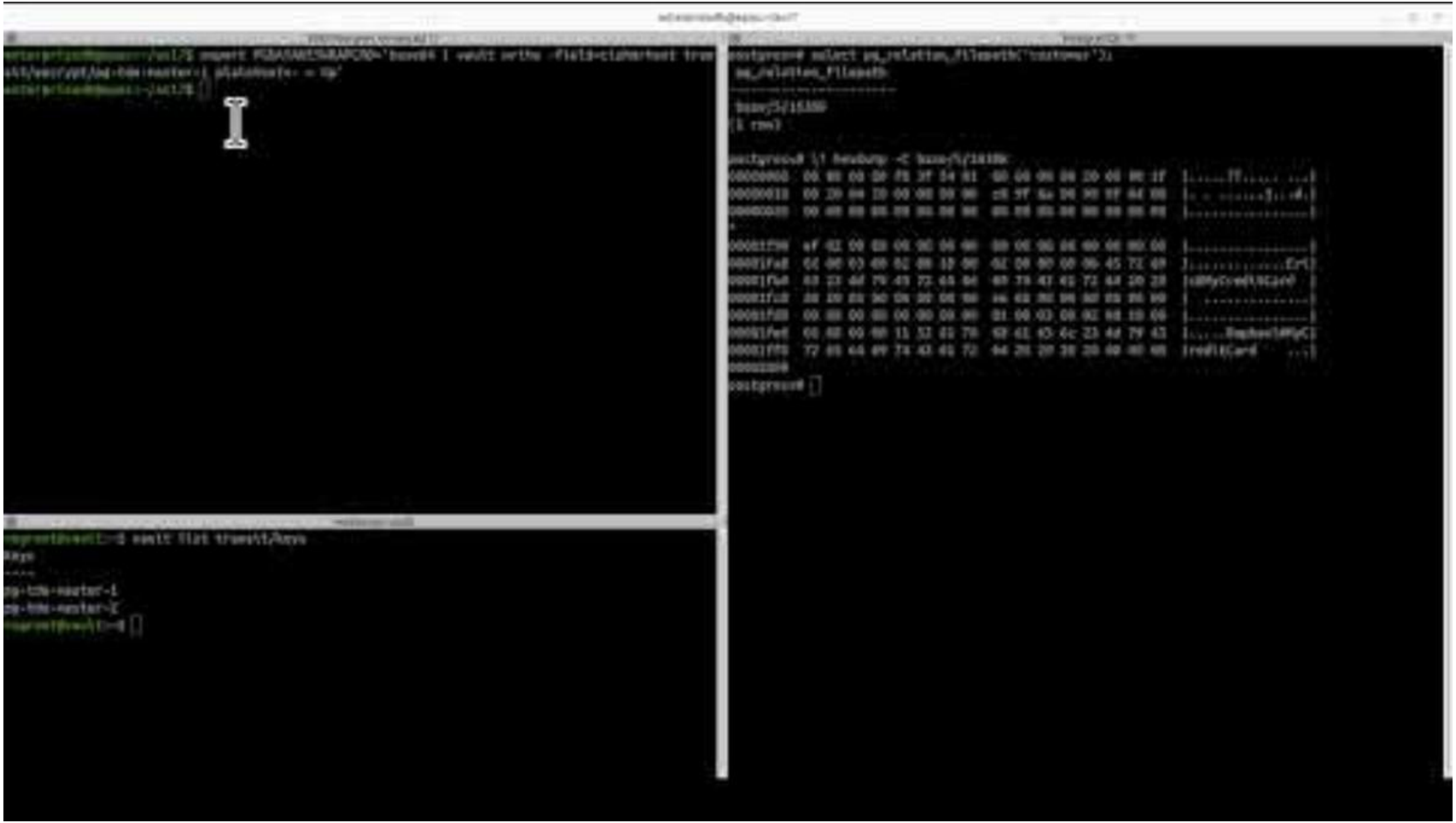
Performance

When the system CPU is not overloaded, using a low number of virtual users, the impact of enabling TDE on performance is not significant.

When the system CPU usage is intense, with a high number of virtual users, the impact of TDE has been measured to a 7.3% drop in terms of transaction rate that the database system can handle.

In this TPC-C-like (TPROC-C) context, according to the PGWAL Write throughput chart, enabling TDE does not seem to lead to a higher database page rate or a bigger database size.

DEMO



```
enterprisedb@pgsql:~/vault$ export PGDATAKEYWRAPCMD='base64 | vault write -field=ciphertext tran
sit/encrypt/pg-tde-master-1 plaintext=- > %p'
enterprisedb@pgsql:~/vault$ 
```

```
postgres=# select pg_relation_filepath('customer');
 pg_relation_filepath
----------------------
 base/5/16388
(1 row)

postgres=# \! hexdump -C base/5/16388
00000000  [illegible]                                         |......??.... ...|
00000010  [illegible]                                         |.. ........]...d.|
00000020  [illegible]                                         |................|
*
00001f90  [illegible]                                         |................|
00001fa0  [illegible]                               45 72 69  |.............Eri|
00001fb0  43 23 4d 79 43 72 65 64  69 74 43 61 72 64 20 20  |c#MyCreditCard  |
00001fc0  [illegible]                                         |  ..............|
00001fd0  [illegible]                                         |................|
00001fe0  [illegible]  52 61 70 68 61 65 6c 23 4d 79 43     |.....Raphael#MyC|
00001ff0  72 65 64 69 74 43 61 72  [illegible]              |reditCard    ...|
00002000
postgres=# 
```

```
vagrant@vault:~$ vault list transit/keys
Keys
----
pg-tde-master-1
pg-tde-master-2
vagrant@vault:~$ 
```

https://github.com/raphael-chir/tde-demo

Thank you

EDB