EDB DAYS · TRACK 04

Mission-Critical Postgres

A Deep Dive on Security, Resiliency & Operations

Flavio Balassiano · Senior Resident Architect · September 2026

© EDB 2026 — ALL RIGHTS RESERVED

ABOUT THE SPEAKER

Flavio Balassiano

Senior Resident Architect

CONNECT ON LINKEDIN

Scan to view profile

Cloud Architecture Leader

Over 8 years of deep AWS ecosystem experience, including 3 years managing Solutions Architecture teams for top AWS Partners.

4x AWS Certified Specialist

Holds AWS Solutions Architect Associate & Professional, Database Specialty, and Security Specialty certifications.

Modern Database Expertise

Specialized in advanced performance tuning and complex, large-scale migrations across Postgres, Oracle, SQL Server, and MySQL.

Current Focus

Architecting highly secure, resilient, mission-critical PostgreSQL environments across on-premise and multi-cloud landscapes for enterprises.

© EDB 2026 — ALL RIGHTS RESERVED

WHAT WE'LL COVER

Agenda

01

Security and Compliance Framework

- Implementing Controls & Regulatory Adherence
- Modern Cyber Recovery Strategies

02

Architecting for Extreme Resiliency and Scale

- The RPO=0 Challenge (Zero Data Loss)
- Data Sovereignty & Hybrid Management

03

Enterprise Operations at Scale

- SOP Best Practices for Large Fleets
- Zero-Downtime Operations
- Holistic Monitoring

© EDB 2026 — ALL RIGHTS RESERVED

SECTION 01

SECURITY AND COMPLIANCE FRAMEWORK

© EDB 2026 — ALL RIGHTS RESERVED

THE BUSINESS CASE

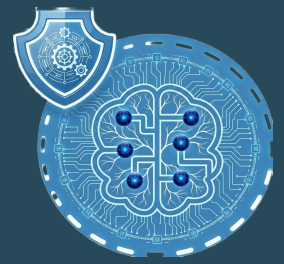
The Mastercard Challenge

Regulation & controls

A resilient database solution is a necessity, not a luxury…

…and it requires a layered security model — defense in depth.

INTERNAL MANDATES



Architect for a “database of record” and satisfy stringent internal risk and controls mandates.

EXTERNAL REGULATIONS

Provide the tools and configurations to achieve and prove compliance with standards such as PCI DSS, GDPR, GLBA, and SOX.

© EDB 2026 — ALL RIGHTS RESERVED

LAYER 1 · IDENTITY & ACCESS

Implementing the AAA Security Model

Authentication, authorization, and auditing

AUTHENTICATION

Who are you?

- **Strong hashing:** SCRAM-SHA-256 is now default for EFM passwords in TPA, replacing deprecated MD5 (PG18).
- **OAuth 2.0:** modern identity integration.
- **Centralized identity:** LDAP or Kerberos/GSSAPI integration with Mastercard identity systems.
- **Enforced policies:** EPAS password profiles enforce complexity, reuse limits, and account lockout.

AUTHORIZATION

What can you do?

- **Least privilege:** grant only the minimum rights required.
- **Row-level security:** restrict rows by role/policy; EDB VPD extends this further.
- **Data redaction:** dynamically mask PII/PANs for non-privileged users.
- **Logs redaction:** prevents credentials from leaking into log files.
- **Predefined roles:** delegate privileges (pg_monitor, pg_maintain, and others) without superuser.
- **TDE:** Transparent Data Encryption — prevents unauthorized viewing of data in OS files.

AUDITING

Who did what, and when?

- **Connection tracking:** successful and failed logins, by user (edb_audit_connect).
- **DDL & DML tracking:** audit structural changes and data modification in real time.
- **Session tag auditing:** link app users/IPs to DB activity, not just DB users.
- **Audit engine enhancements:** nested SQL in functions, system catalogs, COPY transfers.
- **%L log_line_prefix:** emits client IP on every log line for SIEM correlation.

© EDB 2026 — ALL RIGHTS RESERVED

LAYER 2 · INCIDENT RESPONSE

Cyber Repave Runbook

Recover from malicious data compromise, not just infrastructure failure

1 Determine recovery path

PITR path: restore to a known-good timestamp. Clean standby path: promote a standby verified to have halted replication before the intrusion.

2 Rebuild environment

Redeploy all infrastructure from golden images and IaC (Ansible, Terraform) to guarantee clean OS and binaries.

3 Determine restore path

Perform the restore in a “clean room” — an isolated network disconnected from production.

4 Validate data

Run pg_checksums and application-level integrity checks.

5 Rotate all credentials

Regenerate all database users, replication users, SSH keys, and TLS certificates.

6 Preserve evidence

Snapshot compromised systems before cleanup for forensic analysis.

© EDB 2026 — ALL RIGHTS RESERVED

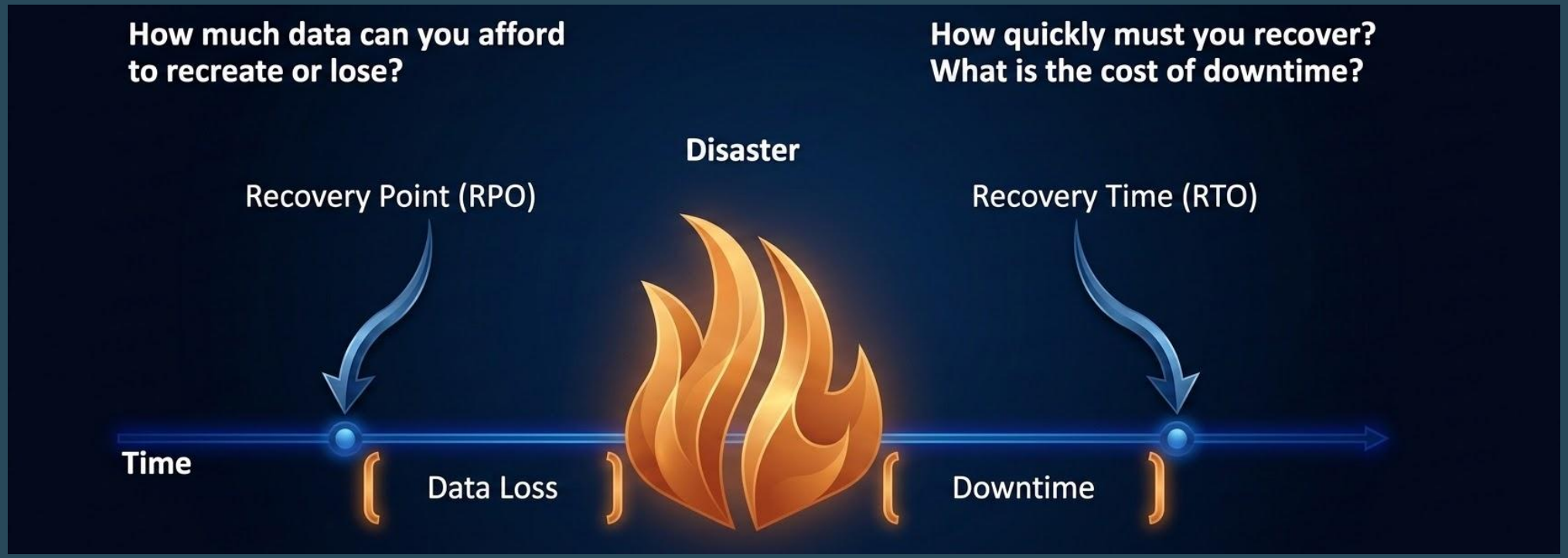
SECTION 02

ARCHITECTING FOR EXTREME RESILIENCY AND SCALE

© EDB 2026 — ALL RIGHTS RESERVED

RTO & RPO Definitions

RTO VS RPO



Source: Disaster Recovery (DR) Architecture on AWS

© EDB 2026 — ALL RIGHTS RESERVED

THE RPO=0 CHALLENGE

Zero Data Loss in Two Data Centers

RPO = 0

ZERO DATA LOSS

- Demands synchronous replication
- Creates a major performance problem

Achieving RPO=0 requires synchronous replication.

In a cross-datacenter topology — especially in geo-distributed setups — this creates a major performance problem.

The primary node must wait for a commit confirmation from the remote standby for every single transaction.

This write latency is tied directly to your network's round-trip time (RTT), which can cripple application performance.

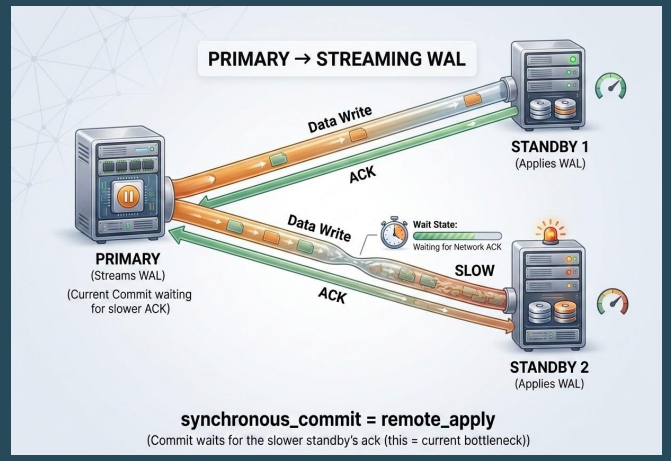
© EDB 2026 — ALL RIGHTS RESERVED

ARCHITECTURE DECISION

Native Replication vs. EDB Postgres Distributed

NATIVE POSTGRES REPLICATION

- **How:** primary streams WAL to a standby using synchronous_commit = remote_apply
- **Pros:** built-in; guarantees RPO=0
- **High write latency:** all transactions are penalized by network RTT
- **Not active-active:** the standby is read-only
- **Manual failover:** requires external tool such as EDB Failover Manager (EFM)



EDB POSTGRES DISTRIBUTED (PGD)

- **How:** a multi-initiator cluster in which every node is writable.
- **Solves latency:** apps write locally, eliminating cross-DC latency.
- **Extreme HA (RTO < 5s):** Connection Manager auto-routes traffic — no manual promotion.
- **Simplified consistency:** tune performance vs. durability with commit scopes.

NEW

Quorum Commit: replaces Group Commit to guarantee zero data divergence and RTO 0 via synchronous, eager conflict resolution — ideal for payments and core banking.

© EDB 2026 — ALL RIGHTS RESERVED

PGD is not just for HA.

It’s a powerful tool for compliance in a multi-cloud landscape.

© EDB 2026 — ALL RIGHTS RESERVED

GLOBAL COMPLIANCE

Data Sovereignty & Hybrid Management

Data must remain within a geographic boundary — data repatriation, GDPR and similar mandates.

EDB Postgres Distributed (PGD) 6 provides a true active-active hybrid cloud — spanning on-prem and multi-cloud, with built-in connection routing and no vendor lock-in.

Regional localization: architect PGD with autonomous regional clusters.

Replication sets: control which tables replicate where — sensitive regional data (e.g., EU PII) stays local, while global reference data is shared.

Tiered storage & AutoPartition: automates data lifecycle, offloading older data to cost-effective object storage (Apache Iceberg) while remaining fully SQL-queryable.

Built-in Connection Manager: automatic traffic routing with integrated connection pooling.

Geo-fenced backups: each PGD node backs up independently, so backup data adheres to local regulations too.

© EDB 2026 — ALL RIGHTS RESERVED

SECTION 03

ENTERPRISE OPERATIONS AT SCALE

© EDB 2026 — ALL RIGHTS RESERVED

OPERATIONAL EXCELLENCE

Operational Best Practices: Automation & IaC

Treat infrastructure as code

TRUSTED POSTGRES ARCHITECT (TPA)

- **EDB's Ansible-based orchestration tool** for deploying HA Postgres clusters on proven EDB best practices.
- **Declarative:** define your entire cluster in a single YAML file.
- **Idempotent:** safely rerun playbooks to reconfigure or scale out new nodes.
- **Consistency:** the same playbooks run across dev, test, and prod.

SECURE SUPPLY CHAIN

- **CI/CD:** use TPA and schema migration tools (e.g., EDB MTK) in your pipeline.
- **Trusted sources:** source all packages only from EDB's authorized repositories.
- **Golden images:** build with EDB's certified STIGs (Security Technical Implementation Guides).
- **Encrypted mail:** UTL_SMTP with STARTTLS + AUTH (EPAS 18) enables TLS-encrypted SMTP for Oracle-compatible migrations.

© EDB 2026 — ALL RIGHTS RESERVED

OPERATIONAL EXCELLENCE

Operational Best Practices: Zero-Downtime Operations

PATCHING & MINOR UPGRADES (ROLLING)

Standard HA streaming replication architecture

1. Patch all standby nodes, one by one.

2. Perform a controlled switchover to a patched standby/shadow primary (PGD).

3. The old primary is now a standby.

4. Patch the (now) standby old primary.

MAJOR VERSION UPGRADES

Native pg_upgrade: requires downtime.

- **Logical replication method:** stand up a new cluster on the target version, replicate via logical replication, then cut over once in sync.
- **PGD method (blue/green):** safely executes major upgrades by testing on a new “green” data group, redirecting workloads, and retiring the “blue” data group.

Result: zero application downtime

© EDB 2026 — ALL RIGHTS RESERVED

OBSERVABILITY

Holistic Monitoring: Single Pane of Glass

METRICS

- **Replication lag:** pg_wal_lsn_diff (sent_lsn, replay_lsn) — this is your RPO risk.
- **TXID wraparound risk:** age(datfrozenxid) — this is critical.
- **Problem sessions:** state = 'idle in transaction' holds locks and blocks vacuum.
- **Slow queries:** pg_stat_statements plus log_min_duration_statement for queries over threshold.
- **Connection logging:** log_connections reports per-stage durations for richer audit trails.

MONITORING

- **Postgres Enterprise Manager (PEM):** monitoring, alerting, and management in one — including SQL Profiler and Index Advisor.
- **Hybrid Manager:** next-gen observability platform.
- **Open-source integration:** built-in exporters for Prometheus and Grafana.
- **Single pane of glass:** Hybrid Manager monitors self-managed, cloud-managed (CSP), and HM-managed databases in one console.

© EDB 2026 — ALL RIGHTS RESERVED

CLOSING

Takeaways + Q&A

TOTAL SECURITY & COMPLIANCE

EDB Postgres provides granular, layered controls (RLS, TDE, EDB Audit) to meet stringent Mastercard and regulatory mandates.

EDB POSTGRES DISTRIBUTED (PGD 6)

Built-in Connection Manager with integrated pooling eliminates external proxy dependencies. Predefined commit scopes simplify RPO=0 configuration. Zero-downtime rolling upgrades and maintenance.

ENTERPRISE OPERATIONS AT SCALE

Automation (TPA) and observability (PEM / Hybrid Manager) let you manage your entire Postgres fleet reliably, consistently, and securely.

Questions? Let's talk — find Flavio on LinkedIn.

© EDB 2026 — ALL RIGHTS RESERVED

THANK YOU

Flavio Balassiano · linkedin.com/in/flaviobalassiano

© EDB 2026 — ALL RIGHTS RESERVED