EDB POSTGRES AI

JPMorganChase

Mission-Critical Postgres: A Deep Dive on Security, Resiliency, and Operations

Vibhor Kumar
VP, CX Technical Advisor
January 2026

Speaker Introduction

Vibhor Kumar

VP, CX Technical Advisor

Vibhor is a Global Vice President at EDB, specializing in performance engineering and cloud-native database architecture.
With 20+ years of experience, he is a recognized thought leader in deploying production-ready PostgreSQL on Kubernetes. He holds a Master's in Computer Applications and possesses extensive expertise in Oracle, DB2, and digital transformation.

Connect on Linkedin

Agenda

Security and Compliance Framework

- Implementing Controls andRegulatory Adherence
- Modern Cyber Recovery Strategies

Architecting for Extreme Resiliency and Scale

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

Enterprise Operations at Scale

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

Security and Compliance Framework

The JPMC Challenge: Regulation and Controls

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

INTERNAL MANDATES

Architectfor “DBof regulation” andsatisfy stringent internal risks and controls.

EXTERNAL REGULATIONS

Providethe tools andconfigurationsto achieve and prove compliance with standards such as PCI DSS, GDPR, GLBA, and SOX.

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

Layer 1: Implementing JPMC Controls (AAA Model)

Authentication, authorization, and auditing

Authentication (who are you?)

- Strong hashing: Move beyond MD5 to SCRAM-SHA-256 for password hashing.
- Centralized identity: Integrate directly with JPMC identity systems via LDAP or Kerberos/GSSAPI.
- Enforced policies: Use EDB Postgres Advanced Server (EPAS) password profiles to enforce complexity, reuse limits, and account lockout.

Layer 1: Implementing JPMC Controls (AAA Model)

Authentication, **authorization**, and auditing

Authorization (what can you do?)

- Principle of least privilege: Grant only the minimum rights required.
- Row-level security (RLS): Restrict access to specific rows based on user role or policy (e.g., a trader can only see their own trades). EDB's Virtual Private Database (VPD) extends this capability.
- Data redaction: Dynamically mask sensitive data (such as PII or PANs for PCI compliance) for non-privileged users.

Layer 1: Implementing JPMC Controls (AAA Model)

Authentication, authorization, and **auditing**

Auditing (what happened?)

- Track and analyze database activities
- Record connections by database Users: Successful and failed
- Record SQL activity by database Users; Errors, rollbacks, all DDL, all DML, all SQL statements
- Session Tag Auditing: Associate middle-tier application data with specific activities in the database log (e.g. track application Users or IP addresses not just database users)

Layer 2: Advanced Auditing for Compliance

Recover from malicious data compromise, not just infrastructure failure

Cyber repave runbook

1 Determine recovery path

PITR path: Restore from backups to a “known-good” time stamp before the incident.

Clean standby path: Promote a standby that was verified to have halted replication before the intrusion.

2 Rebuild environment

Redeploy all infrastructure from “golden images” and onfrastructure-as-code (IaC) (e.g., Ansible, Terraform) to guarantee that the OS and binaries are clean.

3 Determine recovery path

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

4 Validate date

Run pg_verify _checksums and application- level integrity checks.

5 Rotate all credentials

Regenerate all database users, replication users, SSH keys, and TLS cer tificates.

6 Preserve evidence

Snapshot compromised systems before cleanup for forensic analysis

Architecting for Extreme Resiliency and Scale

JPMorganChase

The RPO=0 Challenge in Two Data Centers

RPO = 0 (zero data loss)

- Demands synchronousreplication
- Creates a major performance problem

Achieving RPO=0 requires **synchronous replication**. In a **two-datacenter topology**, especially across a geographic distance, 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.

Solution Analysis: Native vs. EDB Postgres Distributed (PGD)

Native Postgres synchronous replication

How: Primary streams WAL to a standby using synchronous_commit = remote_apply

Pros: Built-in, guarantees RPO=0

Cons:

- High write latency: All transactions are penalized by network RTT
- Not active-active: The standby is read-only
- Manual failover: Requires an external tool such as EDB Failover Manager (EFM) to monitor health, promote the standby, and prevent split-brain scenarios

EDB Postgres Distributed (PGD) (active-active)

How: A multi-initiator cluster in which every node is writable Pros:

- Solves latency: Applications write to their local node, eliminating cross-DC latency
- Extreme HA (RTO < 5s): If a DC fails, traffic is simply routed to the other active node; no “promotion event” is needed
- Flexible consistency: PGD offers granular “commit scopes”
- vs. CockroachDB: PGD provides this geo-distributed, active-active capability on Postgres, maintaining 100% compatibility with the Postgres ecosystem, extensions, and your team's existing skills

PGD is not just for HA. It’s a powerful tool for compliance in a multi-cloud landscape.

Data Sovereignty and Hybrid Management

Data must remain within a geographic boundary (data repatriation, GDPR, etc.)

EDB Postgres AI Distributed HA provides a true active-active hybrid cloud, spanning on-prem and multi-cloud and avoiding vendor lock-in.

Regional localization: Architect PGD with autonomous regional clusters.

Replication sets: This is the key.

EDB audit (EPAS enhancement)

- Keep sensitive data local: E.g., EU customer PII remains only in the EU cluster.
- Replicate global data: E.g., product catalogs to all nodes worldwide.

Geo-fenced backups: Each PGD node can be backed up independently, ensuring that backup data also adheres to local regulations.

Enterprise Operations at Scale

SOP Best Practices: Automation and IaC

Treat infrastructure as code (IaC)

Trusted Postgres Architect (TPA)

EDB'sAnsible-based orchestrationtool.

Deploys HA Postgres clusters based on proven EDB best practices.

- Declarative: Define your entire cluster in a single YAML file.
- Idempotent: Safely rerun playbooks to apply configuration changes or scale out new nodes.

Ensure consistency across dev, test, and prod.

Secure supply chain

UseTPA andschema migration tools (e.g., Flyway) in your CI/CD pipeline.

Source all packages only from EDB's authorized repositories.
Build "golden images" with EDB's certified STIGs (Security Technical Implementation Guides).

SOP Best Practices: Zero-Downtime Operations

Highest-risk operational procedures

Patching and minor version upgrades (rolling)

Standard HA streaming replication architecture

Standard operating procedures:

1. Patch all standby nodes, one by one.
2. Perform a controlled switchover (using EFM) to a patched standby.
3. The old primary is now a standby.
4. Patch the (now) standby old primary.

Result: Zero application downtime

Major version upgrades (zero downtime)

Native pg_upgrade: Requires downtime

Logical replication method:

1. Set up a new cluster on the target version (e.g., Postgres 16).
2. Use logical replication to replicate data from the old cluster (e.g., Postgres 15) to the new one.
3. Once in sync, cut over application traffic.

PGD Method (blue/green): PGD supports advanced blue-green and canary deployments, allowing you to gradually shift traffic to a new version cluster while maintaining bidirectional replication.

Holistic Monitoring (Single Pane of Glass)

Monitoring is the feedback loop that enables proactive issue detection

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'—these hold locks and block vacuums.

Slow queries: Use pg_stat_statements to find queries with high total_exec_time and log queries over a threshold with log_min_duration_statement.

Monitoring

Postgres Enterprise Manager (PEM): Monitoring, alerting, and management in one—includes SQL Profiler and Index Advisor

Hybrid Manager: Next-gen observability platform

Open source integration: Built-in exporters for Prometheus and Grafana

The single pane of glass: Hybrid Manager: Monitor all your databases—self-managed, cloud-managed (CSP), and HM-managed—in one console.

Takeaways + Q&A

Total security and compliance

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

EDB Postgres Distributed (PGD)

Thepremiersolution for RPO=0, active-active, and geo-distributed workloads, solving the “two-DC” latency problem while maintaining 100% Postgres compatibility.

Enterprise operations at scale

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

Thank You

Please complete the survey for EDB Days Track 5 now.

BOURNEMOUTH TECHNOLOGY CENTRE

Gaia Postgres Day Feedback

Thursday, February 26 | 9:00am GMT
The Hub D1S

Scan the QR code or go/BMTHPGD
to provide feedback.

Glasgow
Technology Centre

Gaia Postgres Day Feedback

Tuesday, March 3 | 9:00am – 5:00pm GMT
L1 Ideation and L10 Event Space
315 Argyle Street, Glasgow

Scan the **QR code** to provide feedback.