

“The role of a DBA is dead”

... is it?

At HSBC DBAs led the charge

From VMs to Kubernetes in a Large Global Bank: A DBA's Journey

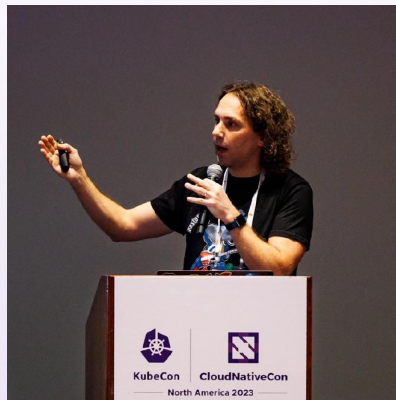
Gabriele Bartolini, EDB

Laurent Parodi, HSBC



**DATA ON
KUBERNETES DAY
EUROPE**

CLOUD NATIVE THEATER



Gabriele Bartolini

VP, Chief Architect @ EDB
CloudNativePG maintainer
PostgreSQL Contributor
DoK Community Ambassador



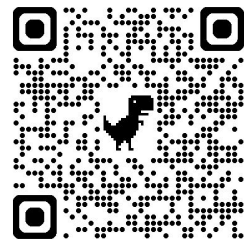
Laurent Parodi

Global PostgreSQL product owner @ HSBC



Remembering **Simon Riggs**

26th March 2024



"The Next 20 Years"
Keynote PGConf.EU 2023

- Part 1 - The comfort zone: our VM heritage
- Part 2 - The new foundation: our blueprint
- Part 3 - Raising the bar: modernising the stack
- Part 4 - The engine: CloudNativePG
- Part 5 - The path ahead



Part 1

The comfort zone: our VM heritage

"The Windmill at Wijk bij Duurstede"

by Jacob van Ruisdael

- Many years of experience with PostgreSQL on VMs
- We built our own reliable world using VMs and scripts with orchestration
- High Availability, backups, and patching were managed by DBAs
- This "safety" relied on:
 - Manual intervention required for failures
 - "Ticket-Ops", which created a bottleneck

- **Database as a Commodity**
 - Teams lack bandwidth for advanced database topics (replication failures, PITR, ...)
 - They want a connection string: “Dev”, not “Ops”
- **Comparison with public clouds**
 - “instant” deployments of Public Cloud vs. hours on premises
 - Continuous flow of new features, extensions and versions
- **Automation mandate : zero touch model**
 - We moved toward APIs and Ansible
 - Onerous to maintain, slow to improve

- The **Non-Negotiables**: Stringent Regulatory Environment
 - Public cloud solutions are not always applicable; on-premises deployments remain necessary.
 - Mandatory cyber security controls: auditing, patching SLAs, and secrets management.
- The **Sovereignty** Mandate:
 - Vendor lock-in is no longer acceptable

- **The entire bank was moving to Kubernetes**
- We, the central DBA team, found ourselves at a crossroad:
 - **Is Kubernetes mature for data?**
 - **How do we stay relevant?**
 - How do we **accelerate**?



Part 2

The new foundation: our blueprint

"The Night Watch"
by Rembrandt

The new foundation

01	Sovereign DBaaS strategy	• 100% Open Source core - No vendor lock-in • No public cloud dependency - Digital Sovereignty • Cloud-neutral architecture
02	Agility	• Provisioning within minutes not hours • Scale compute or storage immediately • 100% self-service
03	Self-Healing	• Insulation from HW failures • Automated failover • Recreation of replicas
04	Compliance	• Backup & restore including PITR • Auditing • Vulnerability management is enforced (patching)
05	Observability	• From custom legacy monitoring to native Prometheus metrics • Deep visibility into the performance of the entire fleet

- Keen interest in the DoK landscape since 2019
 - Zalando, Crunchy PGO and then CloudNativePG in late 2023
- Prefer a native k8s approach over Patroni in a container
 - less “complexity” for the end user
- Gain knowledge with local meetups, and a workshop organized by EDB in Zürich (CH) in early 2025
- CloudNativePG is a CNCF project with strong community adoption, and inspiring maintainers



Part 3

Raising the bar: modernising the stack

"The Avenue at Middelharnis"

by Meindert Hobbema

- Multi-tenant clusters
- Namespace-based isolation by application :
 - Strict RBAC
 - Zero direct namespace access for application teams
- **Secure Self-Service**
 - Declarative-only interactions via APIs
 - Integrated with in-house entitlements solution
- Native integration with Hashicorp Vault (db secret engine)
- Managed disaster recovery - replica clusters
- Controlled patching

- **Image Catalog Management**

- Weekly ingestion of new CNPG operands into private registries
 - With zero CVEs
- Namespaced Image Catalogs for version control

- **Risk Mitigation**

- Phased updates: Non-Prod → Production
- Cluster-by-cluster rollouts to ensure a small blast radius
- Dynamic scheduling:
 - Monthly baseline, or
 - Rapid response for critical CVEs

Part 4

The engine: CloudNativePG

"A scholar in his study"

by Rembrandt



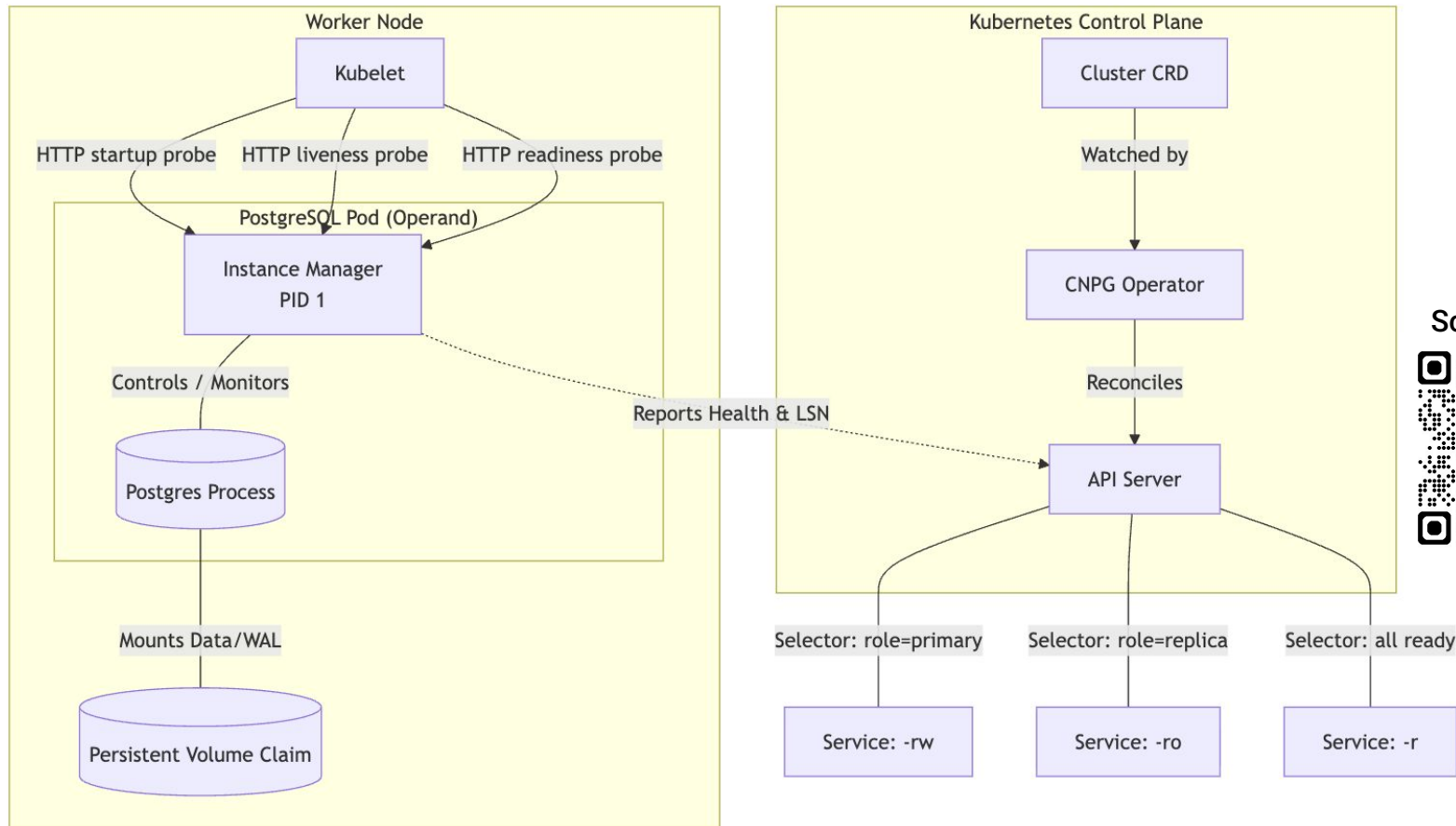
A CNCF Sandbox Project

- Originally created by EDB (conceived in 2019)
- Officially joined the CNCF Sandbox in 2025
- Vendor-neutral governance and open-source sustainability
- Community-led Innovation
- The "Standard" for Postgres on K8s



- **Leveraging the Kubernetes API**
 - No external managers and external consensus, just K8s
 - **The Instance Manager is the entry point (PID 1)**
 - Lightweight controller that controls the Postgres process
 - Handles Kubelet probes (Startup, Liveness, Readiness)
- **Reduced Attack Surface**
 - **Minimalist Footprint:** no extra pods
 - **Fewer moving parts** = fewer binaries to run and scan

Suggested reading: CloudNativePG architecture



- **Direct volume management (no StatefulSets)**
 - Orchestrating Pods and PVCs directly for granular, role-aware control
 - Role-aware Lifecycle: managing primary and standbys differently
- **Optimized Rolling Updates**
 - Tailored patching sequences: update replicas first, then controlled restart/switchover
- **Pluggable Backup & Recovery**
 - No hard dependency on specific backup tools for PostgreSQL
 - Barman Cloud plugin for native integration with object storage (S3 compatible)
- **Storage-Native Resilience**
 - Support for Kubernetes Volume Snapshots (and Volume Group Snapshots)

- **Zero-Persistence Logging**

- Logs are never stored on the container filesystem
- Immediate streaming to stdout prevents local tampering and data leakage

- **Multi-Channel JSON Streams**

- Separate channels for Postgres engine and other events, including pgaudit
- Native JSON format for seamless integration with log management systems

- **Native Metrics**

- Built-in Prometheus exporter inside the Instance Manager
- Provided 50+ core database and replication metrics
- Custom metrics and Grafana dashboard



Part 5

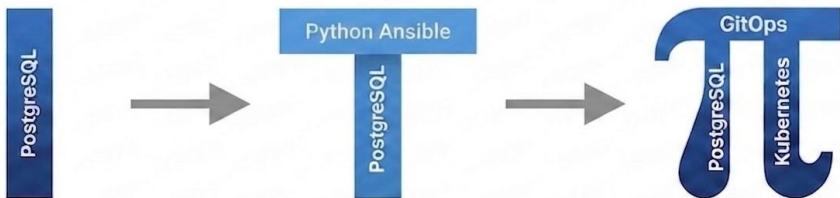
The path ahead

"The Night School"
by Gerard Dou

- CNCF Incubation
- PostgreSQL extensions distributed as image volumes (1.29)
- Conformance program for plugins
 - Remove Barman Cloud from in-core
 - Officialise Barman Cloud Plugin
- OpenSSF compliance
- Declarative database roles
- Comprehensive Data Control Language support for databases

- **The Pi-shaped engineer**

- Beyond the "Comfort Zone"
- Upskilling DBAs into Platform Engineers



- **Making it happen**

- Cultural shift: Ownership of the "Full Stack"
- DBAs leading the architectural charge

- **Managing maintenance windows**
 - Current state: external scheduler engine for automated patching
 - Future state: Integration with the CloudNativePG roadmap
- **Strict role segregation**
 - No cluster-admin access for DBAs ("Least Privilege" in practice)
 - Hardened RBAC for image catalogs & operator controller resources
- **The air-gapped imperative**
 - Full support for isolated banking environments
 - Leveraging Kustomize overlays for site-specific compliance

- **Empowering application teams**

- Focus shifted: business deliverables, not infrastructure maintenance
- Observability: Moving from 'Up/Down' to 'Performance & Tuning'

- **The future**

- Harnessing CNPG Image Volume Extensions
 - Requiring PostgreSQL 18 and Kubernetes 1.35+
- Investigating AI-assisted tuning for workload optimization



Gabriele Bartolini

LinkedIn: gbartolini

Blog: gabrielebartolini.it

**Find me at
EDB booth #896**

Questions?



Laurent Parodi

LinkedIn: laurentparodi