

Database Backup & Recovery Platform Modernizing Mission-Critical Data Protection with Kubernetes-Native Architecture

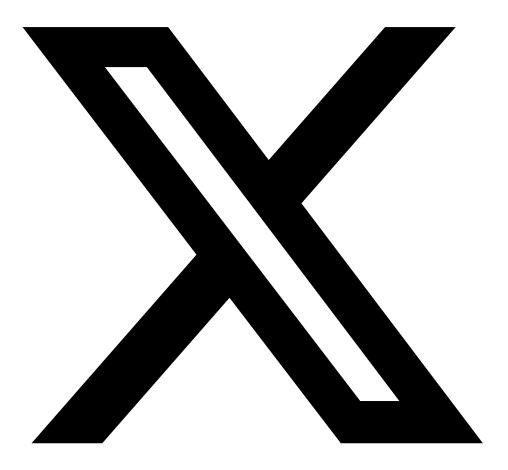
Posted on September 7, 2025 by meetkaneriya011@gmail.com



Case Study



<u>Linkedin</u> <u>X-twitter</u>



<u>Facebook</u>



Database Backup & Recovery Platform Modernizing Mission-Critical Data Protection with Kubernetes-Native Architecture

Client

A global IoT solutions provider managing massive smart city and industrial deployments across hybrid cloud environments. With a complex infrastructure consisting of MySQL, MongoDB, and Elasticsearch clusters deployed on Kubernetes, they needed a unified backup and recovery system that was fast, flexible, and compliant.



The Challenge

In a data-intensive ecosystem, backing up and restoring mission-critical systems is often fragmented, slow, and error-prone. The client faced:



backup management across databases

No centralized



• High recovery times and manual failover interventions



risks due to lack of point-in-time restore (PITR)

Compliance



Security gaps in handling access and encryption



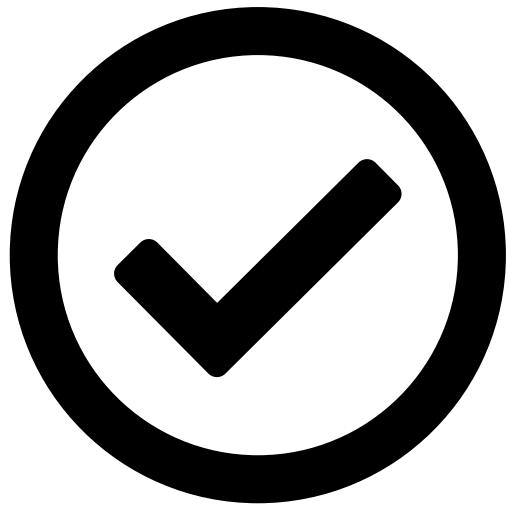
tooling across Kubernetes workloads

Inconsistent

Our Strategy

We engineered a cloud-native backup platform designed specifically for Kubernetes and modern enterprise data stacks. It's modular, open-source-first, and highly automated and built for scale.

Platform Highlights:



• **Kubernetes**Native Architecture: Containerized DB utilities deployed on Kubernetes with support for horizontal scaling and fault tolerance via Rancher.



Unified

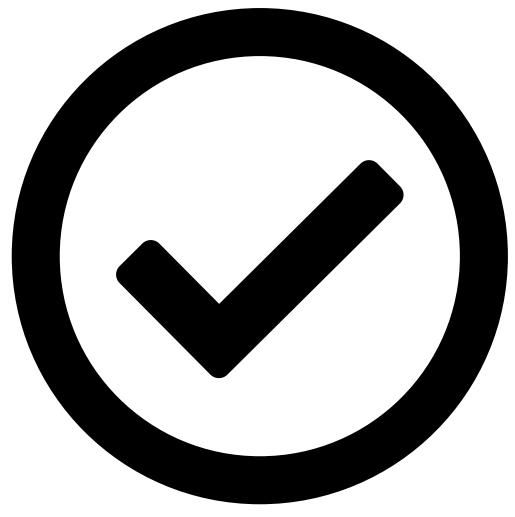
Backup Utility (DB Utility): Handles full, incremental, and PITR backups across
MySQL, MongoDB, and Elasticsearch.



Secure Web-Based GUI Dashboard: Built using AngularJS and NodeJS, allowing users to trigger, schedule, and monitor backups in real-time.



Modular Automation Triggers: Used Crontab for scheduled backups and LDAP for user-role authentication.



Cloud Storage

Integration: Backups stored via MinIO (S3-compatible) with encryption and redundancy.

Tech Stack:



Backup Tools:

XtraBackup (MySQL), PBM Agent (MongoDB), SLM (Elasticsearch)



Messaging & Triggering: REST APIs, Crontab



MinIO (HA), Secure File System

Data Layer:



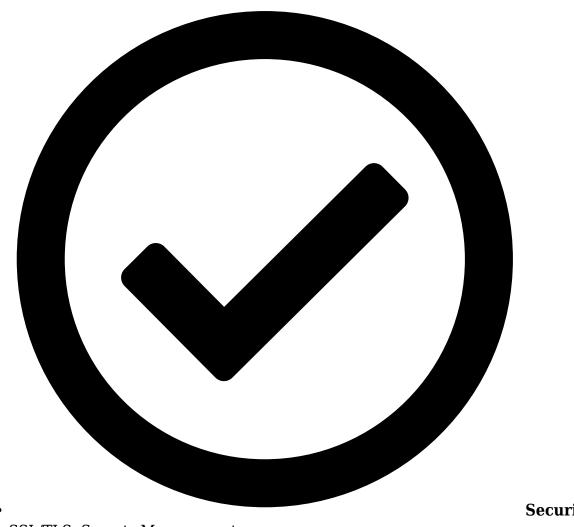
Orchestration

 ${\bf \&\ Platform:}\ {\bf Kubernetes\ via\ Rancher\ (Multi-master,\ Multi-node)}$



NodeJS (Non-HA mode), LDAPS authentication

UI: Angular +



SSL/TLS, Secrets Management

Security: IAM,

Impact & Results

Metric	Before TechTez	After TechTez Implementation
Backup Time	~3 hours (manual)	<30 minutes (automated)
Recovery Time	~6 hours	<1 hour (with PITR)
Admin Overhead	High (script-based)	80% reduction (central dashboard)
Data Loss	Frequent critical cases	Zero critical loss post-deployment
Total Cost (TCO)	High (proprietary tools)	40% reduction (open-source stack)

Why It Matters

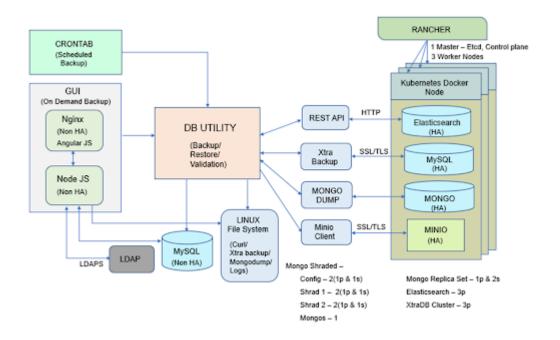
With TechTez, the client moved from a fragmented and fragile backup strategy to a scalable, resilient, and Kubernetes-ready data protection platform. We didn't just automate the backups, we redefined reliability.

Built for compliance ,Designed for observability,Delivered with precision

Your Data with TechTez

Let's reimagine your backup strategy and make it secure, fast, and built to scale.

CTA: Schedule a Discovery Session Today

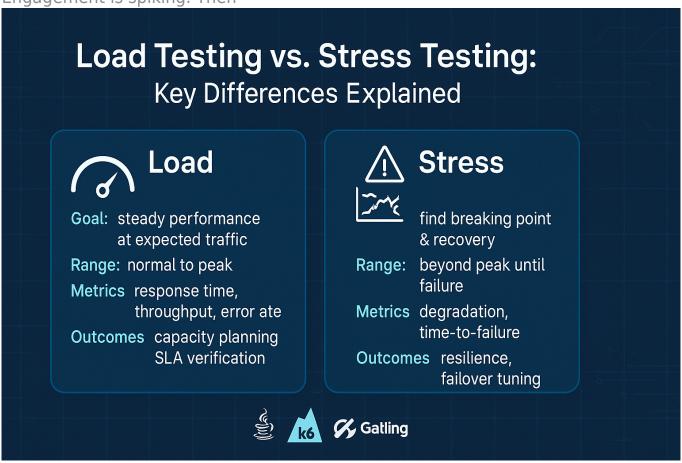


Our Thought Leadership Guides

Case Study

Load Testing vs. Stress Testing: Key Differences Explained

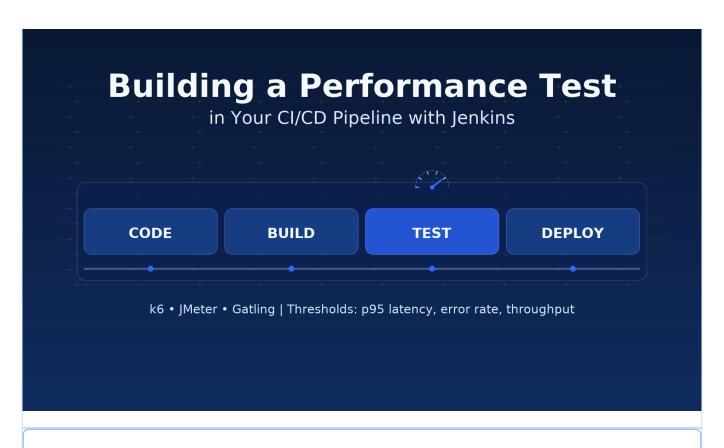
It's launch day. Thousands of users flood your app. Cart values are up. Engagement is spiking. Then



• Case Study

Building a Performance Test in Your CI/CD Pipeline with Jenkins

In the world of rapid software delivery, releasing fast is no longer enough—releasing fast...



• Case Study

Conversational Chatbot Powered by Document Intelligence

A mid-sized SaaS company specializing in HR and payroll management faced a growing barrier:

