QBurst | A High AI-Q™ Company

Jenkins Modernization for a Global Healthcare Provider

Executing a mission-critical infrastructure upgrade from Jenkins 2.227.4 to 2.504.3 LTS to remediate a DEFCON2 security vulnerability while maintaining zero downtime for over 140 daily users and 680 active pipelines.

Overview

Faced with a critical DEFCON2 security vulnerability in their outdated Jenkins 2.227.4 system, the client required a rapid, large-scale migration to the latest LTS version (2.504.3) within a one-month window.

- Successfully migrated a complex infrastructure involving 680+ pipelines, 180+ scheduled jobs, and 140+ users with zero downtime and zero disruption to daily development operations.
- Modernized core components, including upgrading the Java runtime from JDK 8 to JDK 21, enhancing performance, security, and future readiness.
- Employed a "No-Fail" risk mitigation strategy, utilizing parallel cloned environments, ESXi snapshots, and Git-versioned configurations to ensure comprehensive rollback capability.
- Eliminated the critical security risk, improved system stability, and achieved future readiness (including positioning for a potential GitHub Actions migration).

Client Profile

One of the premier academic medical centers in the United States dedicated to excellence in patient care, education, and research. Consistently ranked among the top 10 hospitals in the U.S. News & World Report 'Best Hospitals' list.

Challenges: Vulnerability and Legacy Complexity

- **DEFCON2 Security Risk:** The critical CVE-2024-23897 vulnerability necessitated immediate, high-priority remediation under an accelerated timeline (one month).

- **Massive Scale & Complexity:** The migration involved ensuring compatibility for 140+ plugins and flawlessly moving 680+ active pipelines and 180+ scheduled jobs.
- **Zero-Downtime Mandate:** The mission-critical nature of Jenkins meant the upgrade had to be executed without any interruption to the 140+ users' daily work.
- **Technological Debt:** The jump from Jenkins 2.227.4 (2020) to 2.504.3 LTS (2024) required significant compatibility checks and collateral upgrades (e.g., JDK).

QBurst Solution: Structured, No-Fail Parallel Migration

QBurst implemented a highly structured, three-phase "No-Fail" strategy centered on minimizing risk and ensuring backward compatibility throughout the compressed schedule.

- **Parallel Environment Strategy:** A cloned environment was built completely separate from the production system for comprehensive testing, ensuring zero impact on daily operations.
- **Multi-layered Backup:** Risk was mitigated through multiple layers of redundancy: ESXi Snapshots for instant rollback, local data backups, and Git repositories for configuration version control.
- **Comprehensive Modernization:** Executed key technical upgrades in parallel with the security fix:
  - JDK Upgrade: Migrated the runtime environment from Java 8 to Java 21 for enhanced performance and security.
  - Plugin Management: Assessed and ensured compatibility for all 140+ plugins, utilizing GenAI assistance to rapidly resolve compatibility issues.
- **Three-Phase Execution:** The migration progressed systematically through Preparation (server provisioning, local tests), Migration (parallel system setup, job migration, user testing), and Cutover (domain repointing, scheduled job activation) to ensure controlled progression.

Technical Highlights

- **Jenkins LTS Upgrade:** Successfully moved from the vulnerable 2.227.4 to the latest secure 2.504.3 LTS.
- **JDK Migration:** Upgraded the core Java runtime from 8 to 21, future-proofing the platform.
- **GenAI Assisted Problem Resolution:** Leveraged AI tools to accelerate troubleshooting and decision-making for complex plugin compatibility issues.
- **Structured Data Migration:** Moved Jenkins data directory to the standard/apps location for improved resource management.
- **Backward Compatibility:** Ensured all existing 680+ pipeline configurations and workflows continued to function seamlessly.

Impact: Significant Improvements in Security, Reliability, and Business Continuity

- **Zero Downtime:** Achieved a successful cutover without any business interruption, maintaining continuous operations and productivity.
- **Security Compliance:** DEFCON2 vulnerability remediated, achieving regulatory compliance and eliminating a critical security risk.
- **680+ Pipelines Secured:** All mission-critical development workflows were successfully moved and maintained operational status.
- **Performance Improvement:** The JDK 21 upgrade resulted in faster response times and improved resource utilization.
- **Future Readiness:** The modernization positioned the system for future CI/CD evolution, including potential migration to platforms like GitHub Actions.