Product Engineering for Enhanced Customer Experience Automation Platform

Customer Overview

The customer has purpose-built an AI-powered digital customer experience automation, no-code platform to transform the entire enterprise customer experience. The cloud-native, SaaS platform is a complete omni-channel solution to deliver intelligent automation with personalized user experiences.

The Context

The platform provides a variety of services to automate routine processes. Task automation is easily achieved by creating reusable and portable workflows that can be configured without any code, triggered, and delivered through any of multiple channels. However, the platform had some serious issues relating to security, asynchronous communication, memory, access control, inefficient use of AWS S3 services, and more. The customer was looking to resolve these immediately and get certified as a secure platform to onboard more clients.

Type of Service Provided

Product Engineering

Technologies Used

AWS, Spring Boot, MongoDB, RabbitMQ, MySQL, Microservices, Java, Node.js, React, JavaScript

The Solution

The team of experts from GS Lab | GAVS worked on several core technical aspects to remediate the drawbacks, and to enhance platform services. Key solution components:

1. Implemented multi-pronged solution to fix security gaps
   a. RBAC for secure workflows; specific read/write/trigger access for workflows, cross-enterprise access
   b. Several frontend and backend patches
   c. Server configuration for some issues
   d. REST endpoint updation for secure file upload
   e. Updation of packages, encryption/decryption algorithms, server headers
   f. API level restriction for user data
   g. Narrowed scope of upload API
   h. Input sanitation for UI and backend
   i. Validation of users, upload content, upload file signature
   j. Enhanced filter at platform with various privilege levels
   k. Efficient use of CDN
   l. Parameter checks and more
2. Configured easily portable intermediate queue to protect and persist data even across instances
3. Changed acknowledgement of messages in queue with tracking of services processing messages
4. Provided support for upload of large files to AWS S3 using multi-part file upload strategy
5. Optimized memory usage and code for some targeted services
6. Enhanced log rotation policy for services
7. Suggested solutions/changes for message queue, code review, process acceleration, 3rd party tools

Challenges

- Critical security lapses in platform
- RBAC not done for some cases – for example, enterprise admin workflow contained data restricted for others
- Demand from current clients and prospects for security certification
- Issues with asynchronous communication
  - Message queue losing data when service restarted or OOM occured
  - Users not acknowledged if their data was lost mid-process; only way was to check log
- AWS S3 services not implemented for direct use for UI; no direct secure communication with UI
- Memory issues when services handled large numbers of file transformations
- High upload time for large files through AWS services
- Inefficient handling of loads by services due to poor memory optimization – especially for file transformations
- Low number of file processes due to high memory consumption
- Inadequate log rotation policy causing unnecessary memory utilization

Solution Highlights

- Resolution of issues relating to security, AWS S3 implementation
- Data persistence across instances
- Memory and code optimizations

Solution Impact

- Security certification for platform
- Exponential growth of clients and enhanced user experience through
  - High performance of enterprise applications
  - Robust data security, restrictive authorizations
  - All round efficiencies

To find out how GS Lab | GAVS can help your organization, please visit
www.gavstech.com