

Industry	Technology
Use Case Title	Managed Cloud Services for No-code AI Platform
About the Customer	The Customer is a Tech Start-up based in UK. Their No-code AI Platform, Zinia, is a revolutionary AI Powered platform which was developed with an end object that the users with no expertise in AI should be able to build AI models easily using the user friendly web application.
Technical Requirements/problem	<p>1. Slow and Asynchronous Deployment: Efficient automated deployment refers to the streamlined, error-free, and quick process of deploying software applications through automation, minimizing manual intervention and ensuring reliability.</p> <p>2. Scalability and Availability: Ensure the system can handle varying workloads and maintain uninterrupted service by implementing scalable architecture and measures for high availability.</p> <p>3. Monitoring and Alerting: Implement robust monitoring and alerting capabilities to proactively identify and address system issues, ensuring optimal performance and security.</p> <p>4. Accessibility and Secure Communication: Enable seamless accessibility for authorized users while ensuring secure communication channels to protect sensitive data.</p> <p>5. Configuration and Environment Management: Utilize infrastructure-as-code (IaC) using Terraform, to automate the provisioning and configuration of infrastructure resources.</p>
Solution	<p>1. Efficient automated Deployment: Implement an automated CI/CD pipeline Jenkins, continuous code quality inspection, configuration management, containerization, and continuous monitoring to streamline the deployment process and ensure efficient, error-free deployments.</p> <p>2. Scalability and Availability: Scalability and Availability using Blue-Green Deployment with ELB: Utilize a blue-green deployment approach with an ELB to maintain two identical environments, allowing for seamless switching between them to ensure high availability and minimize downtime during deployments or updates.</p> <p>3. Monitoring and Alerting: Implement a robust monitoring and alerting system that continuously monitors the health and performance of the system. Utilize tools like Prometheus, Grafana, or ELK Stack to collect and analyze metrics, set</p>

	<p>up thresholds, and generate alerts based on predefined conditions. This allows for proactive identification of issues, quick response to incidents, and ensures the availability and reliability of the system.</p> <p>4.Networking and Security:</p> <p>Routing and TLS Encryption: We have set up routing protocols and implemented TLS encryption to ensure the secure transmission of data between the different components. This helps protect sensitive information and prevents unauthorized access.</p> <p>NGINX as Reverse Proxy and Web Server: NGINX is utilized as a reverse proxy and web server to enhance security. We have implemented access control lists (ACLs) and whitelisted specific IP addresses, allowing access only to authorized users. This helps in preventing unauthorized access and safeguarding the application.</p> <p>Web Application Security: To protect against common cyber-attacks such as cross-site scripting (XSS), distributed denial of service (DDoS), and SQL injection, we have implemented robust web application security measures. These include configuring security features and implementing best practices to mitigate potential vulnerabilities.</p> <p>Source Code Analysis: Integrate SonarQube into the development process to perform static code analysis, enforce coding standards, identify issues, and provide actionable insights for improving code quality and security. Continuously analyze code during development to ensure ongoing improvement and adherence to best practices..</p>
Outcome	<p>Efficient Deployment and Configuration Management: Streamlined deployment processes and ensured consistency across environments.</p> <p>Enhanced Scalability and Availability: The system achieves 99.99% availability through the use of Blue green deployment scaling mechanisms.</p> <p>Effective Monitoring and Alerting: Real-time downtime alerts and easy log access ensure quick recovery and minimize system downtime.</p> <p>Strengthened Networking and Security: Secured communication, restricted access to authorized users, and implemented measures to protect against cyber-attacks.</p>
Value Adds	<p>Developed and Implemented a Central monitoring System to effectively capture and monitor the instance resource consumption and provide the alert. This enhances infrastructure visibility and optimizing overall performance.</p>