



A Government Agency: Application Modernization and DevOps Journey

CAPABILITIES SHOWN



Advisory
Services



Cloud
Migration



Digital
Transformation



Cloud
Engineering



Observability
& Monitoring

ABOUT THE COMPANY

We are an ISO 9001:2008, 9001:27001, 20000-1:2018, CMMI Level 3, EDWOSB providing superior, affordable and innovative business management and information technology services to federal and private sector clients nationwide. We specialize in Software Development, Business Intelligence (BI), Data Management, Data Governance, Cyber Security, Data Quality, Master Data Management, Advanced Data Analytics and Cloud Services.



ABOUT THE CUSTOMER – Government Sector


A government organization in the process of modernizing the application from on-premises to cloud. Government organizations often face unique challenges in adopting modern software development practices due to stringent regulations, legacy systems, and the need for high security and compliance. Implementing DevOps in such an environment can significantly improve efficiency, collaboration, and delivery of digital services. This case study provides a high-level view for integrating DevOps practices into a government organization.

CHALLENGES

- ✓ **Siloed Departments:** Traditional government IT departments often operate in silos, with limited collaboration between development, operations, and security teams.
- ✓ **Slow-Release Cycles:** Government organizations typically have long release cycles due to manual processes, extensive reviews, and rigid procedures.
- ✓ **Legacy Systems:** Many government agencies rely on outdated legacy systems that are difficult to maintain and integrate with modern technologies.
- ✓ **Compliance and Security:** Government organizations must comply with stringent regulatory requirements and maintain high security standards, often resulting in slow and cumbersome processes.

SOLUTION

DevOps introduces automation in the form of Continuous Integration (CI) and Continuous Deployment (CD) pipelines. This automation reduces manual intervention, speeds up the release process, and ensures that updates are deployed quickly and reliably. DevOps practices such as Infrastructure as Code (IaC) and containerization (e.g., using AWS ECS) allow legacy systems to be managed more effectively. IaC enables consistent and automated provisioning of infrastructure, while containerization helps in modernizing legacy applications. DevOps integrates security practices into the development lifecycle (DevSecOps), ensuring that security and compliance are automated and continuous. Tools like AWS Security Hub help in identifying and addressing vulnerabilities early in the process.



Assessment and Planning

- Current State Analysis: Evaluate existing infrastructure, development practices, and tools.
- Identify Goals: Define specific objectives such as faster release cycles, improved quality, and enhanced security.
- Roadmap Creation: Develop a phased plan for DevOps adoption, prioritizing high-impact areas.



Cultural Transformation

- Leadership Buy-In: Secure commitment from top management to support the DevOps initiative.
- Training and Workshops: Conduct training sessions to educate teams on DevOps principles and practices.
- Cross-Functional Teams: Create integrated teams that include members from development, operations, and security.



Automation

- CI/CD Pipelines: Implement Continuous Integration and Continuous Deployment (CI/CD) pipelines using tools like AWS CodePipeline.
- Infrastructure as Code (IaC): Use IaC tools like Terraform or AWS CloudFormation to automate infrastructure provisioning and management.
- Automated Testing: Integrate automated testing frameworks to ensure quality at every stage of the development lifecycle.




Monitoring and Logging

- Centralized Logging: Implement centralized logging using tools like AWS CloudTrail and AWS CloudWatch.
- Real-Time Monitoring: Set up real-time monitoring and alerting systems with tools like CloudTrail and AWS CloudWatch.
- Performance Metrics: Continuously monitor application performance and infrastructure health.



Security and Compliance

- Security Integration: Embed security practices into the CI/CD pipeline (DevSecOps) using tools like SonarQube, Dependency-Check, security scans using OWASP, Ironbank secure images, ECR Scan, container security using Falco and Anchore, and vulnerability management using grype
- Compliance Automation: Use compliance as code to ensure adherence to regulatory requirements (e.g., using AWS Config).
- Regular Audits: Conduct regular security audits and vulnerability assessments.



Continuous Improvement

- Feedback Loops: Establish feedback loops through regular retrospectives and stakeholder reviews.
- Performance Reviews: Monitor key performance indicators (KPIs) and use data to drive improvements.

- Community of Practice: Create a community of practice to share knowledge, tools, and best practices across teams.

✓ Tools and Technologies

- Version Control: Git, GitHub, GitLab
- CI/CD: AWS CodePipeline, AWS CodeBuild, AWS Code Deploy, SonarQube, Dependency-Check, security scans using OWASP
- IaC: Terraform, AWS CloudFormation
- Configuration Management: AWS config
- Monitoring and Logging: OpenSearch, CloudTrail, AWS CloudWatch
- Containerization: Docker, AWS ECS
- Security: OWASP, Anchore

SERVICES USED




To address these challenges, A government agency implemented a comprehensive AWS DevOps solution that leveraged several key services:

- ✓ AWS S3 (Simple Storage Service): Used for storing objects and data, including static resources and backups.
- ✓ Amazon RDS (Relational Database Service): Used for hosting databases, specifically Aurora and Postgres.
- ✓ Amazon ECS (Elastic Container Service): Used for deploying and managing containerized applications.
- ✓ AWS Lambda: Used for serverless functions and integration into the application.
- ✓ AWS Secrets Manager: Used for managing application credentials and secrets.
- ✓ Amazon API Gateway: Used for managing APIs and routing requests to the appropriate services.
- ✓ CI/CD: AWS CodePipeline, AWS CodeBuild, AWS Code Deploy, SonarQube, Dependency-Check, security scans using OWASP

THE BENEFITS



- ✓ **Automated Test Pass Rate:** The percentage of automated tests that pass successfully during the CI/CD pipeline has increased by more than 80% due to DevOPS implementation.
- ✓ **Code Commit to Deployment Time:** Code commit to deployment time has reduced by 70% due to DevOPS implementation.
- ✓ **Deployment Success Rate:** Deployment success rate has increased by 80% due to automated deployments.

- 
- ✔ **Enhanced Data Accessibility:** Provided raw data for download in various formats and through API access, leading to a 30% increase in data utilization and enabling faster ad-hoc analysis.
 - ✔ **Personalized Experience:** Offered customizable features, leading to a 15% improvement in user satisfaction and a 40% reduction in report customization time.
 - ✔ **Continuous Availability:** Enabled 24/7 access to business-critical data, leading to a 15% increase in operational efficiency and timely financial reporting.
 - ✔ **Benchmarking Advantage:** Allowed industry benchmarking, resulting in a 10% improvement in performance optimization efforts and strategic alignment.
 - ✔ **Portfolio Optimization:** Unlocked insights for better portfolio management, resulting in a 12% increase in portfolio value and a 25% reduction in underperforming assets.