



DevOps Solutions:

Open Source, Role Based,
DevOps Intranet

DevOps Solutions: Open Source, Role Based, DevOps Intranet

Problem:

A large, independent federal agency required a modernization of its intranet platform to support multiple organizational divisions with shared processes while maintaining clear separation of duties. The challenge included accommodating various teams and projects operating concurrently, with a focus on enabling self-service for developers and release managers. Furthermore, the agency had stringent security requirements, necessitating compliance with Federal FedRAMP, NIST, and FISMA standards.

Solution:

To address these challenges, CTAC devised a robust and highly available DevOps and delivery platform, ensuring security compliance. The solution leveraged AWS and more than 20 AWS services, coupled with partnerships with AWS technology providers. The key components and details of the solution included:

- **Integration with AWS:** CTAC seamlessly integrated AWS services with Jenkins, an open-source automation server, forming the foundation of the DevOps intranet platform.
- **Job Categorization:** Jenkins was configured to orchestrate various types of defined Jobs, each with predefined processes suitable for different teams and projects. Job categories included Admin Only, Build, Deploy, and Utility.
- **Role-based Access Control (RBAC):** Three distinct roles were established within Jenkins- Admin, Developer, and Release Manager. The Admin role is responsible for system and service administration and managing permissions for project resources. The Developer roles grants access to project logs, initiation of application builds, and execution of pre-production actions such as deployments and database loading. The Release Manager possesses all permissions of the Developer role, along with the capability to deploy to production environments.
- **Role and Project Permission:** Users were required to be granted both role-type and project-specific permissions to access predefined Jobs, ensuring restricted access to relevant tasks.

- **Reduced System Administrator Dependency:** The solution significantly reduced reliance on the System Administrator group. While only Admins had access to systems, Developers and Release Managers gained access to logs and diagnostic information necessary for issue resolution without compromising system integrity.
- **Automated Patch Management:** The process of creating servers from up-to-date templates served as an automated patch management solution. Every team actively participated in the patching process, enhancing self-service capabilities and agility while ensuring compliance.
- **Traceability:** To monitor user actions across multiple concurrent projects, the solution provided traceability, allowing tracking of each user's activities within the system.

Outcome:

CTAC successfully addressed the federal agency's requirements by integrating open-source automation services in AWS to create a modern DevOps approach for its enterprise intranet needs. The solution achieved several key objectives:

- **Removing Bottlenecks and Errors:** Deployment processes were streamlined, reducing bottlenecks and minimizing human errors.
- **Empowering Developers:** Developers gained access to troubleshooting tools, allowing them to respond effectively to issues, thereby improving efficiency and responsiveness.
- **Auditing and Compliance:** The solution offered push-button deployments with built-in auditing and compliance measures, ensuring adherence to security standards and regulations.

By implementing this comprehensive solution, CTAC empowered the federal agency to embrace a modern DevOps approach that not only met security requirements but also enhanced efficiency, collaboration, and compliance throughout its intranet platform.