NASCIO 2020 State IT Recognition Award Nomination

Category: Emerging & Innovative Technologies

Title: DevOps platform including initial apps such as ePay, Machine Learning and others

State: Wisconsin

Sponsor: Thomas Johnson, CIO, Dept of Corrections

Contact: Christine Hougaard, Enterprise Architecture and Business Intelligence Manager

Ph. (608)240-5705 – email Christine.Hougaard@wisconsin.gov

Project Initiation: 5/1/2019

Project End: 6/19/2020

Executive Summary

The Wisconsin Department of Corrections (WIDOC) has implemented a new technology platform utilizing DevOps and containers. Why? WIDOC started using Docker containers several years ago to run business intelligence modules and API micro-services. As the number of production containers grew, the support model for those containers became more burdensome. At the same time, legacy web applications running in a WebSphere environment were becoming more outdated and brittle. The process to update Java and other libraries was manual and difficult because of inter-dependencies between applications. These technical limitations combined with increasing demand for enhanced and new applications from business partners led to an evaluation of the development methodologies, standards, environment and operations. Historical development practices would not be able to support strategic business initiatives calling for mobile applications, machine learning, web app modernization, and agile development practices.

The underlying technology for the new platform is based on on-premise Kubernetes to develop, implement and operate applications as containers. This platform supports a Polyglot environment, enabling many different technologies to run on one server cluster, rather than specialized web application platforms. WIDOC also moved to combined Development and Operations (DevOps) approaches. These approaches require that development teams and operations teams communicate frequently and approach their worth with empathy for their teammates. Developers work closely with IT operations to speed software builds, tests and releases, without sacrificing reliability.

The implementation of this new technology platform was approached in two phases over 2 years, with additional supporting implementation projects. Phase 1 assessed the WIDOC environment and culture to adopt a DevOps approach and select tooling. WIDOC selected best-of-breed, cloud native tools to meet best practice goals. Phase 2 implemented an entire toolchain as a minimal viable product for areas that included development and version control, infrastructure as code, continuous integration (CI) pipeline including processes to scan and build, continuous delivery/deployment (CD) pipeline to automate promotion with approvals, containerization, orchestration, security and monitoring.

The assessment phase evaluated WIDOC current state for people, processes and technology.

- People: Define roles and responsibilities between development and operations teams
- Processes: Planning, Development, Testing, Infrastructure configuration, Monitoring, Security.
- Technology: Evaluate and recommend future state tools

The implementation phase delivered components to all verticals of the toolchain. Tools to support the planning processes were rolled out to the entire bureau of technology at one time, aligned with a move to agile project methodologies. Adoption of tools to support version control, testing and continuous integration was staggered by development team. The platform hosted production workloads starting in December 2019, including machine learning modules and a public facing application to facilitate client account payments.

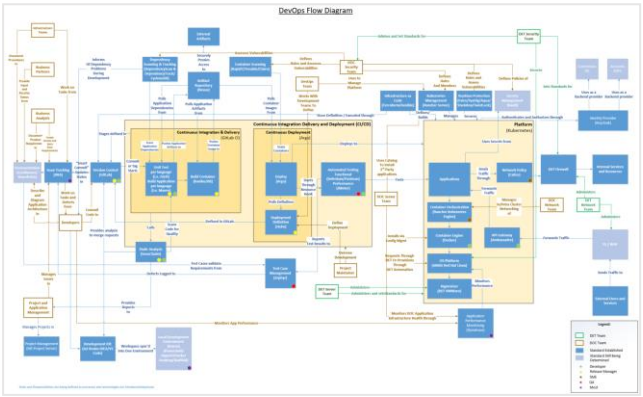
The move to a leading edge architecture positions WIDOC to be nimble. It has enhanced the agency's capabilities for mobile development, machine learning, and micro-services.

Concept

An initial review evaluated the state of DevOps for WIDOC, identified alternatives, determined impact on roles and responsibilities between development and operations teams, and defined recommendations for each major solution set.

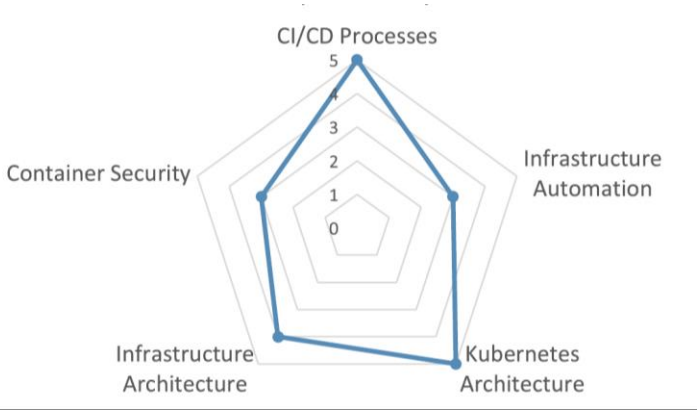
- Assess current state – people, process, and technology
  - Utilize a survey to capture current state information.
  - Research industry trends/capabilities.
  - Identify opportunities and barriers.
- Determine future state
  - Define future state processes.
  - Evaluate and recommend future state technologies for each stage of process.
  - Define reference architecture based on these technologies.
  - Identify any impacts and/or changes needed for roles and responsibilities.
- Identify phasing plan
  - Determine which areas to focus on first (aka prioritize and understand dependencies).
  - Layout roadmap including processes and solution areas.
- Coordinate with State of Wisconsin DevOps Center of Excellence (participating agencies)

A DevOps flow diagram was created and used to discuss DevOps in the context of people, processes, and technology during the implementation. Boxes were labeled with the process and supporting technology. Lines indicate the flow of work with descriptions. Several color coding schemes were used to identify team's responsibility and areas of impact. The diagram was used as a training tool to introduce the new architecture and how development and operations teams would work together.

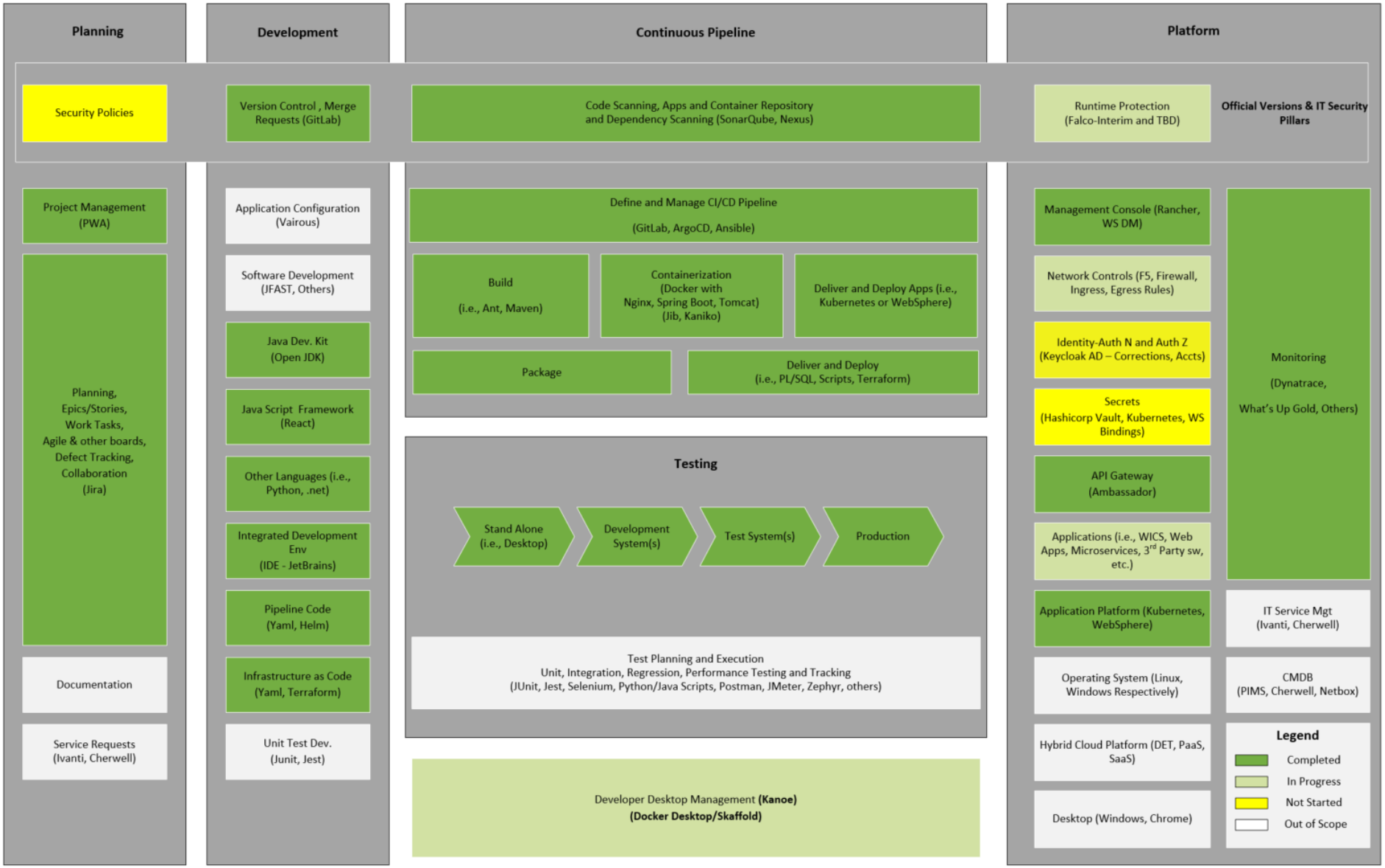


Boxboat, a DevOps/Kubernetes industry leading third-party, assessed our overall platform implementation in May 2020. The diagram below shows WIDOC maturity results in 5 key areas of evaluation.

WIDOC rated above average in all categories compared to other organizations the vendor has evaluated. The high marks reflected a well thought-out architecture that will transform our development and operations to support key business goals.



The process and tools diagram, on the following page, shows the breadth of the implementations across all pillars of the toolchain.


Planning
Development
Continuous Pipeline
Platform
Security Policies
Version Control , Merge Requests (GitLab)
Code Scanning, Apps and Container Repository and Dependency Scanning (SonarQube, Nexus)
Runtime Protection (Falco-Interim and TBD)
Official Versions & IT Security Pillars
Project Management (PWA)
Planning, Epics/Stories, Work Tasks, Agile & other boards, Defect Tracking, Collaboration (Jira)
Documentation
Service Requests (Ivanti, Cherwell)
Application Configuration (Vairous)
Software Development (JFAST, Others)
Java Dev. Kit (Open JDK)
Java Script Framework (React)
Other Languages (i.e., Python, .net)
Integrated Development Env (IDE - JetBrains)
Pipeline Code (Yaml, Helm)
Infrastructure as Code (Yaml, Terraform)
Unit Test Dev. (Junit, Jest)
Define and Manage CI/CD Pipeline (GitLab, ArgoCD, Ansible)
Build (i.e., Ant, Maven)
Containerization (Docker with Nginx, Spring Boot, Tomcat) (Jib, Kaniko)
Deliver and Deploy Apps (i.e., Kubernetes or WebSphere)
Package
Deliver and Deploy (i.e., PL/SQL, Scripts, Terraform)
Testing
Stand Alone (i.e., Desktop)
Development System(s)
Test System(s)
Production
Test Planning and Execution
Unit, Integration, Regression, Performance Testing and Tracking
(JUnit, Jest, Selenium, Python/Java Scripts, Postman, JMeter, Zephyr, others)
Developer Desktop Management (Kanoe)
(Docker Desktop/Skaffold)
Management Console (Rancher, WS DM)
Network Controls (F5, Firewall, Ingress, Egress Rules)
Identity-Auth N and Auth Z (Keycloak AD – Corrections, Accts)
Secrets (Hashicorp Vault, Kubernetes, WS Bindings)
API Gateway (Ambassador)
Applications (i.e., WICS, Web Apps, Microservices, 3rd Party sw, etc.)
Application Platform (Kubernetes, WebSphere)
Operating System (Linux, Windows Respectively)
Hybrid Cloud Platform (DET, PaaS, SaaS)
Desktop (Windows, Chrome)
Monitoring (Dynatrace, What's Up Gold, Others)
IT Service Mgt (Ivanti, Cherwell)
CMDB (PIMS, Cherwell, Netbox)
Legend
Completed
In Progress
Not Started
Out of Scope

Significance

Agency and divisional planning identified strategic business initiatives calling for mobile applications, machine learning, web app modernization, and agile development practices. It would have been difficult to support these initiatives using historical development practices and platforms. Therefore the DevOps technology project was prioritized by the WIDOC enterprise architecture review committee, comprised of program division leadership.

The following requirements were identified during DevOps Architecture planning sessions and then used to evaluate processes, procedures, and technology for implementation.

1. Limit vendor lock-in
2. Support builds of multiple code languages (Polyglot)
    a. Runs as a container
    b. Support database changes (PL/SQL, Schema Changes, Data Manipulation)
3. Enforce granular security
    a. Secrets integration
    b. Security check throughout pipeline
4. Ability to connect/relate a change in the code to an issue
    a. Tag / identify changes
    b. Integration with Agile collaboration tool
    c. Authenticate pipeline inputs (eliminate injection)
    d. Integrates with Git and Subversion (SVN)
    e. Build deploy WIP branches
5. Track steps in the pipeline (CI/CD)
    a. Automatic notifications of build and testing failures
    b. Version control hooks to trigger build
    c. Build artifacts without build-pack
    d. Build metrics / stats
    e. Build alerts / monitoring
6. Failure notification with troubleshooting hints
    a. Ability to rollback; Rollback/Version
    b. Ability to support code review including approval before checking in code
7. Automate pipeline testing validation
    a. Enforce testing standards for numerous levels of testing
        i. Unit testing benchmarks to shift left (identify bugs faster)
        ii. Integration testing
    b. Automation
        i. Ability to run automated test scripts
        ii. Automatically test build and notify status
8. Easy to use
    a. Flexible workflow set up / modification
    b. CI pipeline as code
        i. Able to version control CI/CD scripts
        ii. Declarative syntax
    c. Easy to control the destination environments deployment
        i. Deploys to platform that we choose
        ii. Integrates with Kubernetes (K8)
9. Provide audit trail
10. Integrated application monitoring

Based on evaluation and requirements, projects were activated to transition to agile development methodologies, implement new project planning and tracking tool, move to micro-services architecture, containerization/ orchestration as target platform, layered security and application monitoring. Agile development practices included engaging business product owners through the entire development lifecycle to deliver smaller components of functionality faster. Enhanced project planning tools and task tracking provided greater transparency to accelerate collaboration between technology groups and with business partners.

Also, as the State of WI ventures into newer technologies, it is important to establish enterprise and de facto standards to expedite adoption, reduce R&D (to the extent agencies are able to share their findings), and provide consistent practices with other agencies to deliver timely services with quality. Specifically as part of this initiative WIDOC will assist in improving process around container based host virtual machine (VM) configuration whether via VM templates or through a configuration management tooling in order to meet security standards. This is in addition to previous commitments to assisting with automated network / server provisioning. Over time WIDOC will update the DevOps toolchain to account for these advanced procedures.

WIDOC is also an active member of the DevOps Center of Excellence (CoE) as well as the Application Modernization Collaboration Center (AMCC) and Business Intelligence Collaboration Center (BICC). We will use these forums to share and learn alongside other agencies. As also suggested, we will act as a guide for agencies that need to understand container platforms.

Impact

The container platform utilizing a DevOps toolchain and orchestration has provided mechanisms for the WIDOC bureau of technology to be more responsive to our program divisions' requests for solutions. Containerization provided development flexibility, supporting a transition of legacy apps while hosting new micro-services architecture. Orchestration lifted the burden of manual scaling and increased reliability. The inclusion of code scanning and unit tests has shifted development efforts left by identifying potential problems earlier in the development cycle, reducing the cost of bug resolution. Automation has sped time to delivery of application features, in some cases to a day rather than weeks. Issue management software increased transparency and collaboration between development and operations teams. Dependency checking reduced risk by flagging outdated libraries with known vulnerabilities, and then remediated. Application monitoring utilizing artificial intelligence measures performance and can alert the support team before the customer is impacted.

The transition strategy includes both big bang and phased rollout approaches, depending the specific DevOps process and tools involved.

Big bang for most solution areas includes:

- Planning and task management (Jira)
- Source code repository, continuous integration and delivery (GitLab Premium)
- Code scanning (Sonarqube)
- Image repository (Nexus)
- Monitoring and tracing (Dynatrace)

Phased rollout by application:

- Containers (Docker)
- Container orchestration (Rancher/Kubernetes)
- Microservices/container security authorization (Hashicorp Vault)
- Container runtime protection (Falco)

The big bang approach was completed within the first year. The phased rollout included 4 waves. The initial applications supported on this new platform includes those that were already using containers on the "single container" platform (Docker) as well as a few small internal web apps to gain experience with the migration work. The next 10 web apps will also be small (<1,000 users) internal apps. The larger and external facing apps will be covered in the third and fourth waves.

The implementation of the DevOps platform and supporting toolset has driven development and fueled collaboration across teams. In the last 5 months the number of tasks created over two 10 week periods has increased by 65%, the percentage of tasks completed in those same 10 week periods increased from 49% to 60%. The average length of time from issue creation to resolution has shrunk by 33%. The number of code repositories in the new target CI/CD tool has grown from 355 to 527 in the last 5 months. Up to 5 million lines of code have been scanned for vulnerabilities. Code dependencies are tracked during the application build phase and flagged for any vulnerabilities.

New applications are already being deployed to the platform, utilizing a full DevOps toolchain. WIDOC's ePay application went live in January 2020. The application allows clients to check their DOC account balances and make on-line payments for obligations. Before ePay, probation and parole agents were tasked with physically collecting and processing obligation payments from clients. Now payments can be an electronic transaction, making it contactless during the recent pandemic when agents and clients were meeting virtually. Total collections exceeded $1,000,000 in the first six months.

Recently, both Rancher and Kubernetes versions were upgraded. The upgrades required only 3 lines of code to change and there was absolutely no outage to any customer during the process. Per the assessment vendor, while a minority of organizations are starting to leverage GitOps for continuous delivery, WIDOC has already implemented GitOps with ArgoCD. The new DevOps platform has delivered on its time to delivery, reliability and resiliency.

After implementing an application change to production in less than 2 days after the business partner made the request, a member of the development staff had this to say regarding the re-platforming, "We can do things pretty quickly now!" Developer. "This is very impressive – the ability to process a change request in two days based on my experience is pretty unique. " Tom Johnson, CIO.