DevOps Guidelines

This document is a guideline on the DevOps approach to be followed for software delivery and deployment. It is a living document that will be updated regularly to consider new technologies and best practices.

- Introduction
- Scope and objectives
- Version Control
  - Branching[Mandatory]
  - Source Code Versioning [Mandatory]
  - Tagging[Mandatory]
  - Version control[Mandatory]
- Automation
  - Infrastructure as Code [Mandatory]
  - Containerization and service orchestration [Mandatory]
  - Continuous integration & Continuous Delivery (CI/CD) [Recommended]
- Infrastructure
  - Operating System (OS)[Recommended]
  - Access Control[Mandatory]
  - Backup[Mandatory]
  - Different environments[Mandatory]
  - Monitoring [Mandatory]
  - Auditing [Mandatory]

Introduction

DevOps is a set of practices and tools that integrate and automate the work of software development and IT operations as a means for improving and shortening the systems development life cycle. This document is a guideline on the DevOps approach to be followed for software delivery and deployment. It is a living document that will be updated regularly to consider new technologies and best practices.

Scope and objectives

This document covers the DevOps approach to be followed by Government institutions in Rwanda. The intended audience are software developers, system administrators, DevOps engineers and engineering managers in software development companies that are working with Government institutions in Rwanda.

Version Control

Version control is the practice of tracking and managing changes to software code. Version control is important as it protects the source code from irreparable harm, giving the development team the freedom to make and test changes without causing damage or creating code conflicts. The following guidelines should be applied to manage software version control:

Version Control

Branching[Mandatory]

Each application hosted on VCS must have at minimum three protected branches: **development**, **test** and **production**. Direct commits to protected branches is prohibited. Only reviewed and approved merge/pull requests shall be allowed to land on protected branches.

Version Control

Source Code Versioning [Mandatory]

Software development teams must use **Git** for code versioning and tracking of changes made on files.

Version Control

Tagging[Mandatory]

Test branch must always contain tagged version from development branch and production branch must always contain tagged version from the test branch.

Version control[Mandatory]

A Version Control System (VCS) must be used within the organization to host git repositories. At minimum, the VCS should have the following features: concurrent development, automation, team collaboration, tracking of changes, high availability and disaster recovery.

> Source codes of government owned applications must be hosted on government VCS which is GitLab https://www.git.risa.gov.rw/

Automation

The following guidance should be applied in automating DevOps processes:

Automation

Infrastructure as Code [Mandatory]

Infrastructure as code is the process of managing and provisioning computer data centers through machine-readable definition files, rather than physical hardware configuration or interactive configuration tools. All deployment, delivery, packaging configurations, and infrastructure setup must be done using configuration files. Ansible is the recommended software to use for this automation.

Automation

Containerization and service orchestration [Mandatory]

Containers provide an isolated environment for running software. Docker or Kubernetes is the recommended containerization technology, and each developed application/software must have a containerized version.

Automation

Continuous integration & Continuous Delivery (CI/CD) [Recommended]

The technical goal of CI/CD is to establish a consistent and automated way to build, package, test and deliver applications. All repositories hosting source codes must be configured for CI/CD and each push or merge to any protected branch of the VCS must trigger a CI/CD pipeline.

Infrastructure

The following guidance applies to managing infrastructure and supporting technologies:

Infrastructure

Operating System (OS)[Recommended]

Linux-based Operating systems are recommended and the same version of the OS must be installed in all environments.

Infrastructure

Access Control[Mandatory]

SSH login for root user must be disabled and a dedicated user with sudo access for CI/CD pipelines and automation must be created and used. All users must use passwordless authentication to access the servers. User access to software and database must be configured to allow strict access to software and database needed by their applications only.

Infrastructure

Backup[Mandatory]

Regular backup of data and of the whole OS must be taken and this task must be automated.

Infrastructure

Different environments[Mandatory]

Different environments must be available for deployment of applications in development, testing and production. Access to these environments must be given to very few persons and they must use personalized login credentials. The web server must also be configured as a bastion server for each environment.

Infrastructure

Monitoring [Mandatory]

Monitoring tools for infrastructure must be available and configured with alerts for when servers malfunction.

Infrastructure

Auditing [Mandatory]

Each server must be configured to track and log each access to the server. These access logs must be available on an additional different server for failover.