## Proposed DevOps Approach

The proposed deployment approach is integrated with the existing Tata Motors System/platform.  Continuous Integration and Continuous Deployment are configured with the existing/proposed tools. The services are isolated and deployed in the specific namespace in the AWS account.

The below table gives the details about the tool's integration.

|  |  |
| --- | --- |
| **Tools** | **Description** |
| Elastic Kubernetes Service | EKS managed cluster is distributed across the region with High Availability, Autoscaling will be configured as part of the replica. Ingress Controller (AWS ALB) will be configured for path-based routing. |
| Elastic Container Registry | Docker images are created with JDK base image to run the jar files for the containers to be deployed on EKS. We use ECR centralized storage for configuring and uploading the docker images of non-prod and prod environments. |
| Terraform | The infrastructure will be defined as code using Terraform, enabling consistent and repeatable provisioning of AWS (Amazon Web Services) resources. This approach ensures the entire infrastructure is version-controlled, allows for easy tracking of changes, and simplifies collaboration. |
| Cloud Watch | This is centralized and configured in the region for extracting and maintaining the logs. |
| AWS IAM | AWS Identity and Access Management (IAM) is used to specify who or what can access services and resources in AWS, centrally manage fine-grained permissions, and analyze access to refine permissions across AWS. |
| AWS S3 | S3 bucket can be used to host the static website and to store the application processed Documents, images and reports. |
| AWS API Gateway | Configuring API Gateway to manage API endpoints. It helps for creating, publishing, maintaining, monitoring, and securing REST, HTTP, and WebSocket APIs at any scale. |
| SES | Simple Email Service (SES) is a flexible, highly scalable, and cost-effective service that allows application developers to send emails from within the application. We can use it for transactional emails, marketing emails, and sending emails in bulk. |
| SQS | Simple Queue Service (SQS) is a fully managed service offering from Amazon. It helps to decouple and scale microservices, serverless applications, and distributed systems. It removes the complexity and overhead associated with managing and operating message-oriented middleware. |
| SNS | Simple Notification Service (SNS) is a fully managed service offered by Amazon. It is helpful for application-to-application (A2A) and application-to-person (A2P) communication. Its A2A functionality offers high-throughput, push-based, many-to-many messaging between microservices, event-driven serverless applications, and distributed systems. |
| Amazon Cognito | Amazon Cognito used to add user sign-up and authentication to mobile and web apps. Amazon Cognito also enables to authenticate users through an external identity provider and provides temporary security credentials to access app's backend resources in AWS or any service behind Amazon API Gateway. |
| AWS Secret Manager | AWS Secrets Manager is a service provided by Amazon Web Services (AWS) that helps to protect sensitive information such as API keys, database credentials, and other secrets. It enables you to securely store, manage, and retrieve secrets for your applications and services. |
| AWS Lambda | AWS Lambda is a serverless compute service provided by Amazon Web Services (AWS). It allows you to run your code without provisioning or managing servers, enabling you to focus on writing code and building applications without the need to worry about infrastructure. |

CI/CD Approach:

Below is the proposed solution architecture/technology landscape to achieve DevOps CI-CD automation.

A diagram of a software development process

Description automatically generated

The following are the steps execution as part of the pipeline the CICD pipeline is configured with all the requirement stages for the build execution:

* CICD Pipeline is configured with multi-stage build process for the pipeline build execution.
* Continuous Integration of the build process starts and triggers the staged build process.
* The triggered build process on compilation is successful proceed with the next gated check with the code quality.
* During the process, the image is validated for all the security integration with the scanning using the tool.
* The image of having the vulnerability criteria falls into criteria like high, medium, and low grouping.
* The rules are being set with the expectation for the code to be passed in and to upload on to the Registry.
* On successful compilation the build is uploaded onto the Container Registry.
* The artifact is then called using the Continuous Integration process for the artifact deployment onto the K8 cluster.

**Release process**

* The releases are done using the templates configured with the chart for the specific repos and the same can be reused across the board. The releases are version controlled and the roll back can be done at any point of time.
* All the artifacts are stored on the Container Repo and tagged with the defined labels.
* The promotion model is being set so that the same artifact can be promoted onto the next environment using the pipeline.
* Non prod environment setup done for doing their testing without disturbing any existing environment.
* Performance test scripts are integrated to run on the code deployed and validated.
* Alerts are being configured at all levels in case of failure to trigger so that they are completely monitored with the tools.

For continuous integration and continuous deployment (CI/CD), we will utilize the following tools and practices:

* **Code repository**: GitHub/Bit Bucket for version control and collaboration.
* **Code Quality**: SonarQube (formerly Sonar) is an open-source platform for continuous inspection of code quality to perform automatic reviews with static analysis of code to detect bugs.
* **Containerization**: Docker will be used to containerize the microservices.
* **Container Registry**: AWS Elastic Container Registry (ECR) will be used to store and manage Docker images.
* **Orchestration:** AWS Elastic Kubernetes Service (EKS) will be used to deploy the microservices.
* **Continuous Integration and Deployment**: Jenkins will be used to establish a robust CI/CD pipeline. It will integrate with the version control system (e.g., Git) to trigger automated builds, perform code quality checks and deploy the applications to the EKS cluster. Jenkins pipelines will be defined using declarative syntax for easy maintenance and scalability.
* **Infrastructure Updates**: Infrastructure updates will be handled using Terraform, triggered by the Jenkins CI/CD pipeline.

Notification Center:

* **Event Bus Integration:** AWS EventBridge to subscribe to events and process notifications.
* **Notification Services:**

**SNS (Simple Notification Service):** SNS for distributing notifications to multiple subscribers (e.g., SMS, email, push notifications).

**SES (Simple Email Service):** Use SES for sending email notifications.

Notification Modules:

* **Notification Listener Service:** Event bus (AWS EventBridge) for process incoming messages.
* **Notification Processor:** Validate incoming data and determine if it matches any user-defined rules. Use SNS and SES to send notifications.
* **Adapters:** Implement custom adapters for each notification channel (SMS, email, push notifications).
* **Notifications Management API:** Provide APIs for the frontend to set and manage notifications.
* **Scheduler Service:** Schedule periodic notifications and integrate with SNS/SES for sending.
* **Bulk Notification Service:** Send bulk notifications using SNS for scalability.

Application and Infrastructure Monitoring

To monitor the deployed infrastructure and applications, we will implement the following:

* **Prometheus and Grafana**: Prometheus and Grafana are widely used open-source tools for monitoring, logging, and alerting in Kubernetes environments, including AWS EKS.

Prometheus will send the metrics data it collects from the AWS EKS Cluster, and Grafana uses it to create the visualizations.

* **Alerting with Prometheus Alert Manager:** Configure Prometheus Alert Manager to receive and manage alerts generated by Prometheus. Define alerting rules in Prometheus based on your monitoring requirements. These rules define the conditions that trigger alerts. Configure Alert Manager to send alerts via various notification channels such as email, Slack, or other custom integrations.

Branching strategy

A diagram of a project

Description automatically generated

**Proposed Flow**:

* Standard conventions are followed for the branching strategy so that the product is uniquely identified.
* The feature branches are short lived branches which are being developed and merged into the development branches.
* The development branches are then merged on to the supporting branches called the Release branches.
* Tags are being created from the branches to do the releases.
* The release is then tagged based on the short outcomes of the releases.
* Finally approved changes are being merged back into the Master branch and the deployment happens from this branch.
* The master branch is then again branched out for the latest changes in development/feature to worked upon by developers.

The hotfix branches are created in case of any critical issues to be fixed on the production release being done from the master branch.

Release Process

* The release process will be created with the managers & cab approval obtained prior to the releases.
* Release processes are defined with the CI/CD Integrated
* Deployment will be done through the build tool.
* Frequent branches and the tagging process will be created for the deployment.
* Release will be tagged and stored as a Tag in the Repo.
* Hotfix branches will be created during the process of any critical fixes that need to be part of the deployment.
* Communicate to the Stake holders on the release complete
* The Release will be deployed using the pipeline with the specific branching Tag created for the deployment.
* The Releases will be version controlled and deployed from the specific pipeline.
* The promotion of artifacts will be done using pipelines.

Deployment Strategy

Rolling Update Deployment Strategy:

We recommend adopting a Rolling Update deployment strategy, which allows for incremental updates to the application without requiring downtime. In a Rolling Update, new instances of the application are gradually introduced while old instances are removed, ensuring continuous availability. The key steps of this strategy are as follows:

* Develop an automated deployment pipeline using the tool Jenkins to facilitate the deployment process. The pipeline supports the rolling update process, including the ability to deploy to a subset of instances at a time.
* Implement automated testing suites that run against each batch of updated instances to ensure functional and performance validation.
* Defining the release criteria and establishing a rollback strategy to quickly revert to previous stable version if any issues or unexpected behavior are detected during the deployment.
* Gradually replace old instances with new ones using the load balancer. Mean time monitor their performance, and proceed with the next batch if no issues are detected.
* Monitor key performance indicators (KPIs) and track user feedback to ensure a successful deployment and identify any potential issues that may require further attention.

**Benefits and Deliverables:**

* Minimized downtime and reduced risks during software deployments, ensuring a seamless user experience.
* Enhanced reliability and quality of deployments through automated testing and validation.
* Real-time monitoring and metrics tracking to measure the success and impact of each deployment.
* Rolling updates ensure that there is always a set of instances running the stable version, maintaining service availability.
* Rolling updates make efficient use of resources by only requiring a subset of instances to be updated at a time.

DevOps Cloud Security for Application

* Security Virtual Private cloud will be configured.
* Security Rules for the private and public cloud configured.
* Access Identity and Management (IAM) Access Analyzer
* Key Management Service Integrated for encrypting the keys used by the applications and supported AWS services in multiple Regions around the world from a single console.
* Security assessments on the firewall rules & configuration
* Access to the corresponding repos

Cost-Effectiveness, High Availability, and Scalability:

To achieve cost-effectiveness, high availability, and scalability, we will employ the following strategies:

* **AWS Auto Scaling**: EKS clusters can be configured with AWS Auto Scaling, allowing the cluster to scale horizontally based on demand and workload metrics.
* **Load Balancing**: We will utilize AWS Elastic Load Balancer (ELB) or AWS Application Load Balancer (ALB) to distribute traffic across multiple instances of the microservices and ensuring high availability and load distribution.
* **Cost Analysis:** Cost analysis will be performed to optimize expenses while maintaining a highly available and scalable architecture. This includes right-sizing EC2 instances, using spot instances for non-critical workloads, leveraging reserved instances for cost savings, and utilizing auto-scaling features to match resource usage to demand.