About Customer: Ruah Technologies and Solutions

Ruah Tech Solutions is one of the leading Web & Mobile App development company in Australia. They are into multiple domain like VR Technology, UI/UX Design, Mobile Apps development, Web App development and Blockchain.

They are helping global companies charter uncharted waters by delivering impeccable tailor-made solutions to a leading service provider in Shipping and Logistics. They are Impacting the world with impeccable security and Integrated Healthcare. They have delivered over 100+ projects successfully.

Customer Challenge

Ruah Tech was building an OTT based application to run on the cloud. As the software development phase was nearing completion, the project team wanted to focus on adopting and operating the application reliably on the cloud. They realised the operating model on the cloud was vastly different from what they were previously used to on premise. The in-house development team had limited expertise on DevOps practises and AWS Cloud and wanted expert guidance for implementing the following key requirements.

- To create a cloud native deployment architecture for the OTT Platform and web application with the best practices in place.
- The development team wanted to primarily focus only on the development of new features and services rather than managing servers on the cloud.
- The media based web application was to operate securely on the cloud and scale on-demand with minimal operations overhead
- Monitoring of the application metrics on production was a key requirement to identify and troubleshoot issues on the cloud.
- Automated Build, Deployment and Rollback was required to reduce manual intervention by developers in production. The changes to both the application and infrastructure was desired to be automated.
- To have high availability and fault-tolerant architecture on the cloud within a region.

To address these requirements, Ruah Tech engaged with Workmates to implement the application infrastructure on the AWS Cloud and also make it DevOps compliant with secure, high-performing, resilient, and efficient infrastructure for their applications.

Our DevOps Solution Approach

Workmates, an AWS DevOps specialist, helped Ruah Tech adopt the DevOps methodology to their software development and release processes. The application architecture for the AWS cloud was designed with the right balance of managed services to both reduce operational overhead while keeping the costs low. Most of the undifferentiated activities on the cloud was automated, thus reducing the overall time and risk in deployment of new services. The key aspects of the solution design includes:

- Micro services based architecture for the web application and API's using Kubernetes (AWS EKS)
- Automated provisioning of the infrastructure on the cloud using Cloudformation and EKSCTL
- A fully featured CI CD pipeline using Jenkins for the micro services. The CI CD pipeline also included the feature for rollback when the deployment fails.
- Helm is used to define manifest templates for Kubernetes application and easily perform installation, rollback, and upgradation of Kubernetes application.
- ECR used as Docker container registry and the Authentication to the registry done via IAM role.
- Highly Available Nginx Ingress backed by AWS NLB was setup for API traffic management. The TLS offloading happens at the NLB level using AWS ACM.
- Infrastructure and applications monitoring enabled using AWS CloudWatch and Opensource tool for micro service monitoring including Prometheus and Grafana.
- The Standard output and error logs for the micro service running on the containers are managed on the centralized Cloud Watch Logs. This has been implemented using AWS CloudWatch Logs Insight.
- All the Infra and DB backup are stored on S3 storage service with 15 days retention and can be accessible at any point of time. This was achieved using Velero. Backup and restore in place and scheduled automated backup using Velero, which can be useful to perform disaster recovery was achieved.
- Highly available Mongo DB cluster setup on the Kubernetes Cluster with persistent volumes.
- Highly available Redis Sentinel Cluster was setup on the Kubernetes Cluster with persistent volume to improve performance through caching.
- To handle extreme spikes in traffic Kubernetes HPA and Cluster AutoScaler was implemented.
- AWS Config setup for Continuous Monitoring, assessment and change management for the AWS resource's configurations.
- SSM Patch Manager configured to scan EC2 instances and report compliance on a schedule, install available patches on a schedule, and patch or scan instances on demand.
- Parameter Store (SSM) was opted for storing the secrets and credentials, the secrets get offloaded during deploy stage on the CICD pipeline.

Key Services Used

| AWS Services Used	Use Case
AWS EKS	Managed Kubernetes Control Plane
AWS EC2	Container Workload Management
AWS Network Load balancer	Kubernetes Ingress, Traffic Management across the microservices
S3	Object Storage for Media related Contents
Amazon EBS GP2	Persistent Storage for Stateful apps such as DB
AWS KMS	For EBS and S3 encryption
AWS ECR	Container Registry for docker images
Amazon CloudFront	Content Delivery Network
AWS CloudFormation	Creation of VPC, EKS cluster and ASG
Amazon CloudWatch Logs	Logging Solution for all microservice applications
AWS Config	Conduct assessment and audit of the AWS resources
AWS Systems Manager	For On demand Patching EC2 Servers.

| Third-Party Tools	UseCase
Jenkins	Build, test, and deploy the microservices using Jenkinsfile
Helm	Templating the manifest files for all microservices
Git	Software Version Control - Bitbucket
Velero	Backup and restore for Kubernetes cluster resources
Prometheus Alertmanager	Monitoring and alerting toolkit for Kubernetes
Grafana	Observability dashboards for Prometheus Metrics
OpenVpn	Secure access to AWS Infrastructure

Security Considerations

- AWS IAM role based access control to restrict users to only the required resources.
- Access to the EKS API server access is restricted to certain roles and IAM user and is accessible inside the VPC network only.
- Deep visibility into API calls are maintained through AWS Cloud Trail, including who, what, and from where calls were made. All user related activities are tracked and logged.
- For any Administrative task Remote user have need to connect to VPN client for accessing the servers. All the RDP/SSH port are bound with OpenVPN server, also default ports will be changed to the custom port.

- The DB and Redis ports are accessible only from the Application containers and are restricted using Kubernetes ClusterIP.
- All the container workloads are under the private subnets, the microservices are exposed using the Nginx Ingress. TLS listeners has been setup for Nginx Ingress which runs behind the Network Load balancer and the TLS certificate has been issued using AWS ACM.
- Jenkins Build Server has been setup for the CICD on the private subnet and exposed via AWS Load balancer.
- Encryption enabled both in rest and transit using KMS and ACM

Solution Architecture
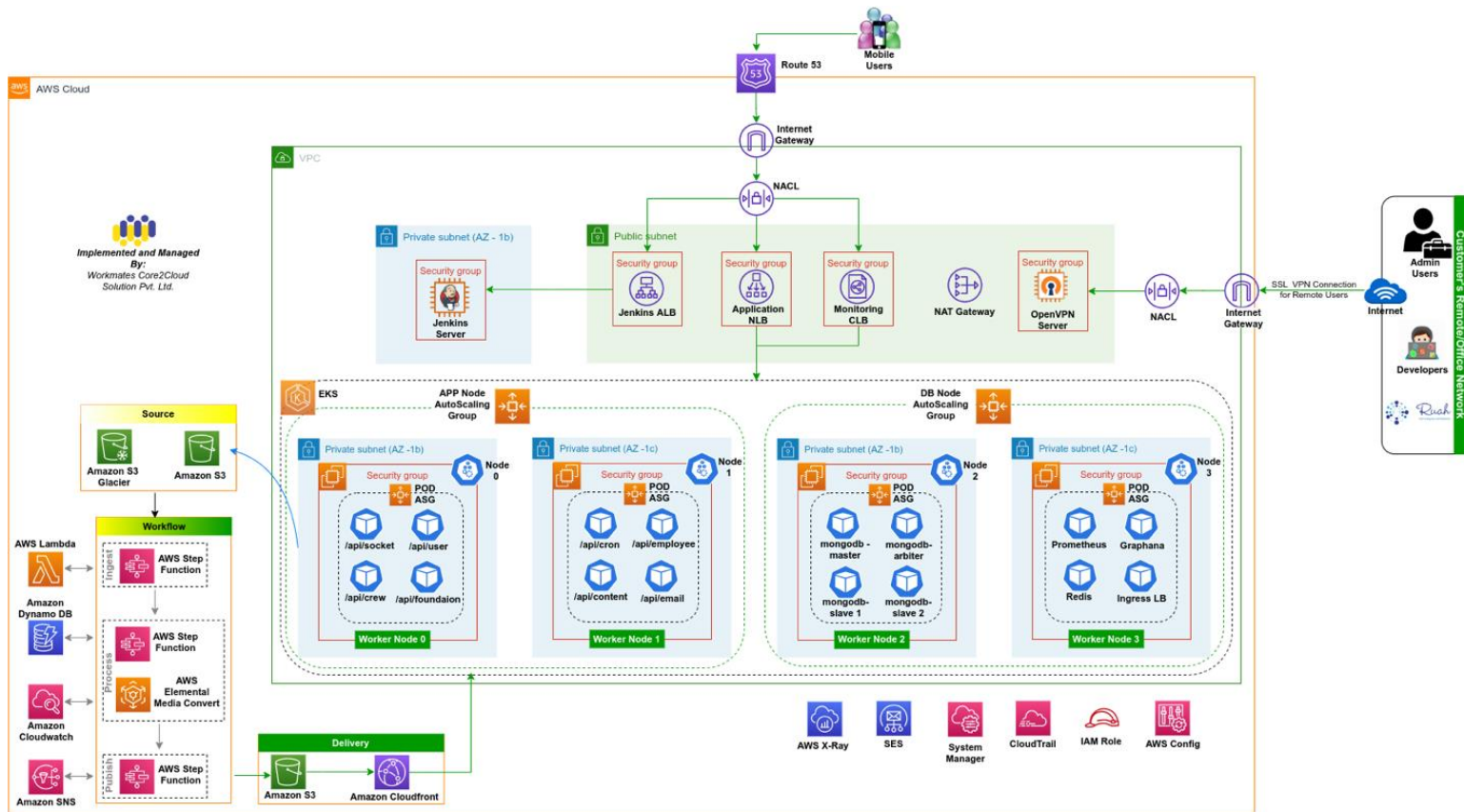
Continuous Integration and Continuous Deployment
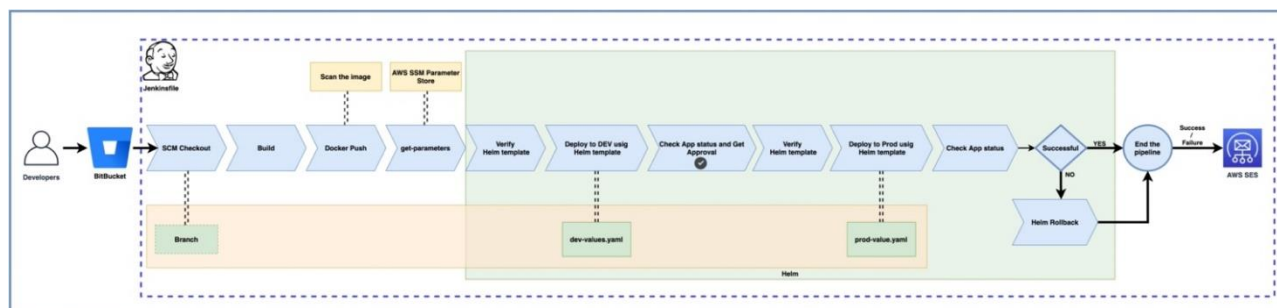
The build of any microservices is triggered with commit on Bit Bucket. The CICD workflow is written in Jenkinsfile and is a pipeline job containing series of stages. And Jenkins provides a Pipeline Stage view on which it is very easy to visualize the current state of the pipeline. The CICD stages of pipeline includes the following:

1. The Reviewer merges the code into the Bitbucket repository's master branch, this triggers the initial stage of the pipeline i.e Git checkout, and here source code is pushed into the Jenkins workspace.
2. Since all the apps are NodeJS apps , there is no need to compile the code. So the next step is running the Build and Unit Test using docker-compose.
3. Now we tag the docker image obtained from the previous stage and push it to the Amazon ECR. We have also enabled ECR scan on push for scanning any security vulnerabilities on the image.
4. Now the CD process starts, in this process, here first we download the secrets.yaml form the AWS SSM parameter store, than verify the Helm template is valid, and then we deploy into the Development EKS cluster using helm chart. The status of the deployment is also verified here.
5. Once the Deployment on Dev Environment is completed there is a testing done from the developers team and once the testing is successful the Developer approves the promotion for Production Deployment.
6. Finally the same Image is now deployed in to the Production EKS cluster and the status of the deployment and application is verified.

In the above Pipeline we have also included error handling mechanism, also the status of the whole build process is sent as email to the developer team. The Production Deployment has one more stage which is a manual Rollback stage. If the Production deployment fails or developers finds it buggy the developer can roll back to the previous working state of the application.

Results and Benefits

Ruah Tech OTT and backend application was successfully deployed on AWS environment while meeting all security & high availability guidelines as per the stated compliance directives. The following are some of the key benefits for the customer

1. A secure, scalable and fault tolerant application architecture on the cloud
2. Micro services based application architecture allowed for modular development, independent testing and smaller frequent releases.
3. Enhanced monitoring and alerting capability to notify the DevOps team on any production issues so they can mitigate it immediately.
4. The automated deployment of the AWS stack and code has freed developers of infrastructure administration and scaling tasks
5. Along with significant savings in time to build and deploy, the effort, cost, and time for infrastructure planning and maintenance has also reduced.
6. The overall security posture on the cloud is improved using cloud native security features like encryption and private networks and continuous compliance using AWS Config.

By adopting the DevOps methodology, the team is far more focused on their core expertise of creating great products and application. To put it in a nutshell, they are now on the fast track to success.

About Workmates

Workmates core2cloud Solution Pvt. Ltd is an AWS Advance consulting partner and Leading Cloud Management Company in Eastern India. Workmates Core2cloud is a cloud managed services company focused on AWS services, the fastest growing AWS Advanced Consulting Partner in India. We focus on Managed services, Cloud Migration and Implementation of various value-added services on the cloud including but not limited to Cyber Security and Analytics. Our skills cut across various workloads like Microsoft, SAP, Media Solutions, DevOps ,E-commerce, Analytics, IOT, Machine Learning, VR, AR etc. Our VR services are transforming many businesses.
Workmates has a yellow theme which is the color of youth. Our Vibrant team of 100% certified resources brings the edge to customers for an End to End AWS partner, committed towards quality and supporting their business on a 24X7 basis.