

About Customer: Vawsum Schools

Vawsum is an ecosystem of students-parents-teachers-alumni-school-corporate to "Make Learning Awesome" Vawsum App is a parent-teacher engagement application which aims to revolutionize how parents and teachers engage with each other. Be it simple updates update the classes, homework, pictures, fees collection, updates about school bus locations, we have it all covered. Be Vawsum is a program that brings together school & corporate help students imbibe good values, inculcate good habits and build personalities.

Customer Challenge

Vawsum has 2 web application and mobile application to run on the AWS cloud. As the application were running on third party tool i.e Plesk Panel and customer required the secure and reliable application configuration on AWS cloud. Vawsum was looking for expert guidance for implementing the following key requirements.

- To configure the multiple Web & mobile applications with Apache reverse proxy configuration on top of the private EC2 instance.
- Plesk Panel doesn't support the autoscaling feature and website are going down frequently.
- Least privileges for application developers to access the application logs and images stored on S3 bucket. Also, want to disable the deletion privileges of each user.
- Database was accessible to worldwide and can be accessible easily through Plesk Panel
- Institution application logs were stopped unexpected intermittently.
- Lots of application images were stored inside the application folder which was consuming Disk more space.
- Regular MySQL Backup mechanism required in case of server failure.
- Monitoring of the AWS production resources was the main requirement to troubleshoot and debug the infrastructure issues.
- Infra and application monitoring was their main concern, they were not able to get the notification of server utilisation.
- Application Deployment pipeline was not automated. Developers were facing issue to manage the code and deployment issues.
- Rollback mechanism was not there for the production resources. And alert management was required during the new deployment.

Vawsum collabes with Workmates to address out the above requirements. Vawsum wants the fixes of the Apache reverse proxy permanently on the AWS Cloud. Thier main concern was scaling the infra as per the load increases. Also, customer want the compliant with secure, high-performing, resilient, and efficient infrastructure for their web and mobile applications.

Our Solution Approach

Workmates helped Vawsum to adopt the AWS best practices to their web and app applications. 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:

- 2 tier-based architecture for the php web application & MySQL server. Also, APIs are residing in php server itself.
- Templates for provisioning the collection of resources together as a single unit using CloudFormation service.
- All images are placed in S3 bucket and calling all the images using AWS php SDK tool. We are using static website for all images and mapped the bucket name with subdomain.
- Application load balancer endpoint is used for updating the Teacher/Parents/Students feeds, appointments, pushing the notification to doctor/patient from the Web Admin Portal.
- MySQL backups are stored on S3 storage service with 15 days retention and can be accessible and restorable at any point of time in case of server failure. It was scheduled using shell script and it run every midnight 12 pm sharp. RTO is max 2 hours and RPO is 24 hours, which can be achieved to perform disaster recovery.
- Auto deployment is done using Bash script placed inside the UAT server and configured the bash script to execute as a Linux command. When the script executes, it deploys the master branch code to each VMs registered in the Autoscaling group.
- S3 Buckets are encrypted using CMK keys and can be accessible through application web feeds to Student/Teacher/Parents.
- Configured the tags for EC2 instances and have registered in load balancer to manage incoming traffic during the deployment process. The load balancer blocks traffic from each instance while it's being deployed to and allows traffic to it again after the deployment succeeds.
- Infrastructure monitoring enabled using AWS CloudWatch service and application logs are pushed to CloudWatch log groups to check the errors immediately with logging into the server.

- AWS Config setup for Continuous Monitoring, assessment and change management for the AWS resource's configurations.
- IAM role attached to the EC2 Instances for uploading the MySQL Backup. Specific S3 event policy (Inline Policy) is assigned to the Role for performing the backup mechanism.
- 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 quarterly basis.
- Bitbucket repositories having only source code and database secrets and credentials were stored in S3 storage bucket. The secrets get offloaded during deploy stage on the Deployment process for both applications.

AWS Services Used

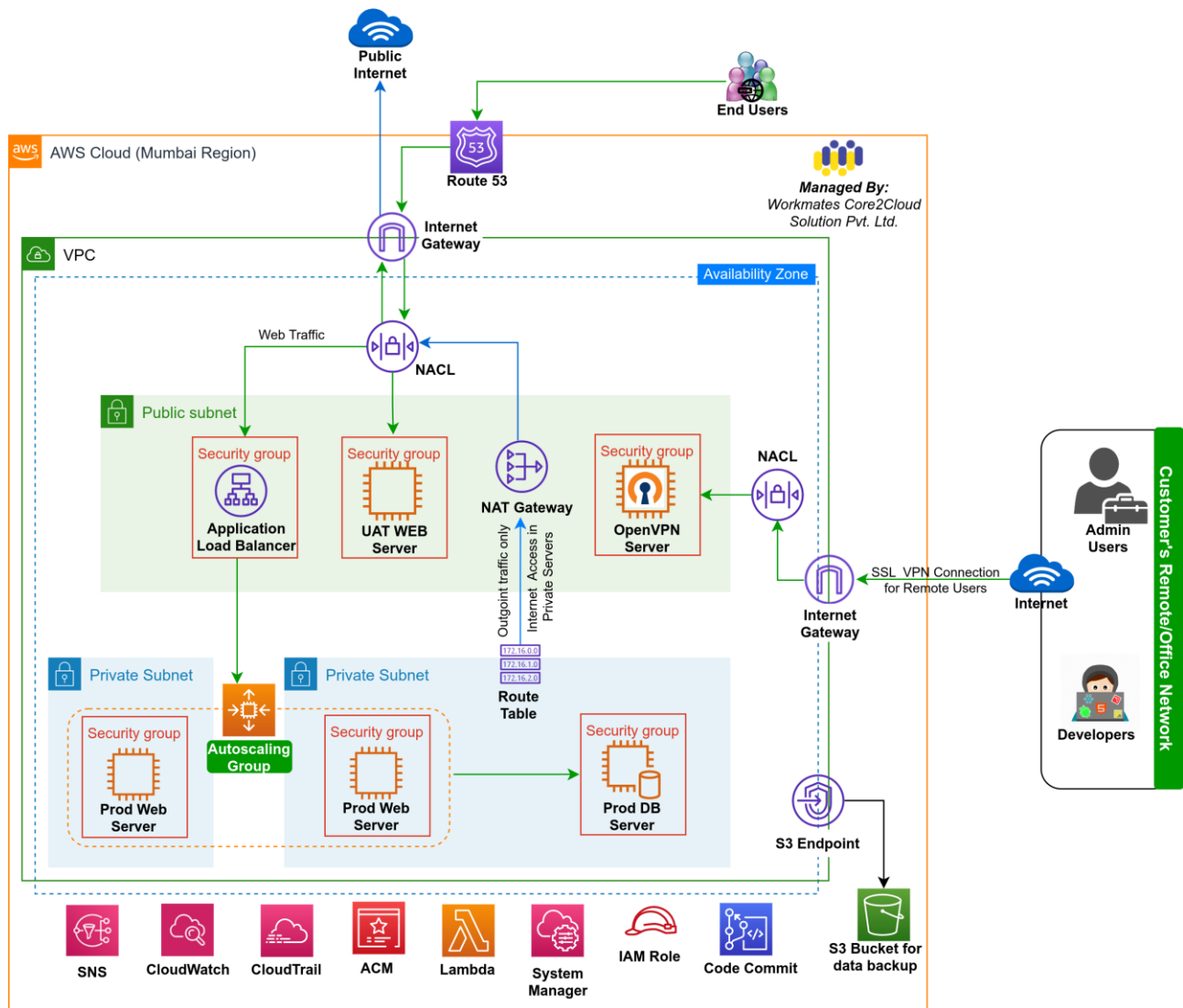
AWS Services Used	Use Case
AWS EC2	For hosting the Mongo database and Angular web application
AWS Application Load balancer	Public endpoint for accessing backend Admin portal only.
AWS Autoscaling	For scaling the number of VMs
S3	Object Storage for database backup and logs
AWS KMS	S3 Buckets encryption
AWS Cloud Trail	For capturing the API calls
AWS CloudFormation	Creation of isolated VPC, OpenVPN server
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.
AWS Resource Group	For creating group to enable the patch cycle through SSM

Third-Party Tools	UseCase
OpenVpn	Secure access for AWS resources
NewRelic	For application monitoring

Security Considerations

- AWS Asynchronous KMS Encryption is enabled for all provisioned S3 Storage buckets and in transit data is encrypted using AWS ACM.
- AWS IAM role-based access control to restrict users to the required resources only. Custom and Inline policy are attached to AWS IAM Roles. Specific events actions are place into the Inline policy.
- Web and Database Server are hosted in private subnet and internet is accessible through NAT gateway for updating the Linux packages and for patching activities.
- Web server is exposed via AWS application load balancer and both applications are serving traffic through 443 port only.
- DB Admins are accessing their private MySQL databases though OpenVPN only. MySQL database service port is restricted to OpenVPN client and application server only.
- Each application is hosted on Apache virtualhosts and database service. Custom SSH port is used for the administrative tasks.
- Strong IAM password provided to each user. IAM users are given minimal access privileges to AWS resources that still allows them to fulfil their job responsibilities
- Mutli Factor Authentication is enabled for extra layer of protection for Root user name and password.
- CloudTrail logs enabled for tracking all kind of activities performed for AWS resources across all regions. Administrator can get the deep insights of API call of each AWS user.
- Bitbucket git credentials are managed by customer and were rotated on quarterly basis.
- Developer can push the modified code to the staging branch and respective Manager approves the changes and merge the changes/releases to production branch. Respective manager will deploy the code to production VMs.
- APIs and PHP application are hosted in private subnet and deployed on top the Apache web server.
- S3 Buckets are not in public and can be accessible within the AWS resources.

Solution Architecture



Results and Benefits

Web application and mobile application was successfully deployed on AWS environment and meets all security & guidelines as per the AWS best practices. The following are some of the key benefits for the customer

1. Automated deployment bash script help a lot to the developer to deliver updates quickly and frequently without any downtime.
2. Satisfactory feedback after completing the Apache and load balancer configuration for multiple applications.
3. After the CI/CD implemented, developers are more focused to build more business functionality in their application and freed the developers of Infrastructure administration tasks.

4. The automated deployment enabled the developers and operations teams to achieve their results faster.
5. Infra monitoring Alerts are triggered to customer and support team.
6. A secure, reliable and fault tolerant application architecture on the AWS cloud.
7. CloudWatch monitoring and alert actions to notify the Developer and Operations team on any production issues, so they can take action and can mitigate it on immediate basis.
8. AWS native security features are highly secured and data/secrets were encrypted using Asynchronous customer managed key (CMK) and remediating the noncompliant AWS resources using AWS Config service.
9. Lead Time for Changes is very fast and efficient. Also reduces the time, cost, human effort, Maintenance time.

AWS best practices make the developer and Ops team to more focused on their core area of expertise. By Building out the secure and scalable infra is a success of resiliency, persistence, and drive. Also, Vawsum team has adopted the AWS best practices and they are very much appreciating for this success implementation.

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.