DevOps – EnParadigm Case Study

Executive Summary

This report describes the challenges that the EnParadigm team has faced while deploying the application using traditional methods and explains how Axiom has helped to solve the issues by using DevOps principles on AWS. In this document, we provide the details of the technologies leveraged and the resources we deployed in the client environment.

The Challenges

As part of the modernization plan, EnParadigm has migrated its infrastructure and application from on-prem to AWS cloud to reap the benefits of the cloud and its services.

- The team at EnParadigm has been managing application deployments manually and over the time, they ran into lot of issues like Build failures, version mismatches, lack of consistency in delivery timelines which lead to business impact.
- There were security challenges like DDOS attacks due to a lack of tracking and monitoring of the resources.

Why Axiom?

Axiom is an end-to-end digital transformation services provider. We believe in “Harnessing the real power of the cloud”. We are an advanced consulting partner with AWS and one among the 30 certified EUC competency partners across the globe.

We have been delivering services around DevOps and infrastructure automation to our customers across the globe for more than 5 years. To date, we have delivered over 20+ end to end DevOps projects and have been managing some of them on a 24/5 model. We have a custom automation framework for large scale DevOps deployments.

The Solution

Axiom has been approached by the client to help them to set up an automated deployment process. As a standard practice, we have started with a discovery phase, where we have analyzed the application and infrastructure landscape in detail. Post discovery, we have proposed the below:

About EnParadigm

EnParadigm is a tech-driven learning solutions company. They develop proprietary algorithms and leverage AI to build advanced digital simulations, SMART micro-learning platforms, and sales enablement apps.

EnParadigm is a mid-sized firm with over 80 employees generating an estimated revenue of $13.2M yearly.

Technologies Stack

AWS

AWS Resource Access Manager
AWS Assume Role
AWS Service Control Policies
AWS Backup
AWS CloudTrail
AWS Config
Amazon CloudWatch
AWS CodeBuild
AWS KMS
Amazon VPC
AWS CodeCommit
Elastic Load Balancing
AWS Systems Manager
VPN

- DevOps solution with one click approach, where the developers push their code changes to AWS CodeCommit where the application code is stored. When any code changes are made to the code, AWS CodeCommit triggers the AWS CodeBuild which renders AWS CloudFormation template and applies them. AWS CloudFormation does the deployment of the required services thus Creating complete, automated software release workflows for continuous integration and delivery.

All the infra that is part of our design is listed below and is managed by AWS CloudFormation templates:

- Load balancing, security, and all other best practices taken into consideration to increase the scalability and performance thereby reducing the downtime.
- AWS CloudTrail to record actions taken by user, role, or an AWS service as events to help enable governance, compliance, operational and risk auditing.
- Centralized log system to make it easy to monitor everything at one place.
- RDS instances, Linux machines that host the website are created on a private network with Elastic Load Balancer for security and availability.
- Configured Simple Notification Service, created alarms to send notification emails if any changes are made with the resources for instantaneous delivery and flexibility as it supports multiple endpoints.

Amazon EBS Encryption

We have enabled EBS encryption in environment with KMS service to Encrypt data.

Note: Default EBS volume encryption only applies to newly created EBS volumes. Existing EBS volumes are not converted automatically.

VPN

AWS Client VPN

Security Components

IAM

We have enabled IAM password policy and MFA (multi-factor authentication) for users.

VPC FLOW LOGS

We have enabled VPC flow logs in all environments, which logs all incoming and outgoing IP flows within a VPC network. We have restricted security groups and allow only certain ports according to the client requirement.

AWS CloudTrail

We have enabled CloudTrail in all AWS regions and it is integrated with CloudWatch Logs. Also, enabled CloudTrail log file validation and restricted the public S3 bucket CloudTrail and there are not publicly accessible.

Amazon CloudWatch

We have configured multiple CloudWatch log metric filters and enabled alarms to identify if, any configuration changes are done in the environment. Enabled SNS service for notifications alerts and encrypted with KMS key.

Amazon S3(simple storage service)

We have blocked public access to S3 buckets. Enabled S3 buckets encryption with KMS key and S3 server access logs which trace all user activity on the objects in the bucket. Also, enabled Life cycle management which deletes the log files for every 365days for Cost optimization.

AWS KMS(Key Management service.)

We have enabled KMS in all environments for Encryption and decryption of data and enabled key rotation for every year. Which it helps in Encryption and decryption of data.

AWS Config

AWS Config is enabled in all regions, and We have configured Multiple rules in AWS config, which monitor and alerts us if, there is any configuration changes and suspicious activity done in the environment.

Amazon Relational Database Service

We have blocked public access to RDS snapshots. Enabled Encryption for RDS DB instances with KMS key and RDS clusters deletion protection In the Environment.

- Implemented WAF with CloudFront to prevent DDOS attacks.
- AWS CloudWatch with security hub is enabled for continuous vulnerability scans.
- We do have stand-alone jobs that uses AWS Systems Manager to apply OS patches and create golden images.
- Apart from CloudFormation templates, the other part the operator performs manually is organizing the multiple accounts into a hierarchy using AWS Organizations to centrally manage and govern the environment.

About the partner

Axiom helps global businesses take a dynamic approach to digital transformation and cloud adoption. With a unique combination of industry knowledge and cross-platform expertise, we offer end-to-end solutions to adopt efficient and economical cloud models.

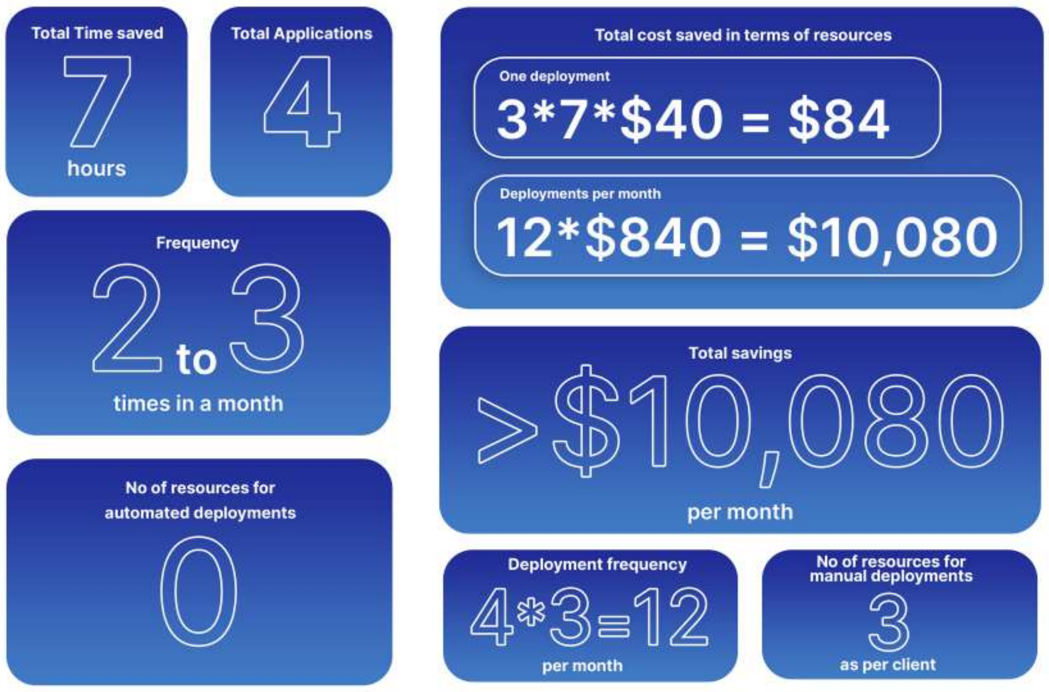
We enable organizations to navigate the complexities of cloud adoption, and transition into smarter, agile, and effective processes, and stay ahead in today’s world.

Client Base: Alphaserve Technologies, Wipro, NIIT Technologies, BlueYonder and more.

The Result

This automation framework helped to manage deployments across Pre-Prod and Production environments, seamlessly and with utmost security. It also resulted in preventing DDOS attacks with the implementation of WAF and CloudFront with a DevOps Pipeline. This solution has saved a lot of effort, which otherwise would take almost **8 hours** now takes only **1 hour**, thus saving **7 hours** of time for each build. The client witnessed a reduction in the cost and efforts to a greater extent.

Key Metrics:


Total Time saved
hours
Total Applications
Frequency
2 to 3
times in a month
No of resources for automated deployments
Total cost saved in terms of resources
One deployment
3*7*$40 = $84
Deployments per month
12*$840 = $10,080
Total savings
>$10,080
per month
Deployment frequency
4*3=12
per month
No of resources for manual deployments
as per client