

Leading Bank Migrates Workload to Cloud

TABLE OF CONTENTS

1. About our Client	1
2. The Challenge	2
3. The ACC Solution	2
a. AWS Shield Standard	2
b. AWS WAF (Web Application Firewall)	3
c. AWS GuardDuty	3
d. AWS IAM	4
e. Amazon CloudWatch	4
f. AWS CloudTrail	5
g. Application Load Balancer	5
4. Benefits	7

Leading Bank Migrates Workload to Cloud



About our client

2 Our client is India's Major distribution franchise, being the second largest non-bank mutual fund distributor. They serve both domestic and international clients and is empanelled with a large cross section of such institutional clients. It consists of 5 pillars of business, namely in retail equity, financial product distribution, Private wealth management, Institutional equity and corporate finance.

The challenge: -

The client was in the middle of evaluating whether they should be hosting their application on Premise or Cloud.

The ACC Team worked together for hours to bring the best possible solution for the client and made them understand the benefits of using cloud over on-premise data servers.

The ACC Solution: -

Our client works on many financial services simultaneously, which means application security and uptime are paramount.

ACC deployed a large number of AWS services and infrastructure improvements as part of the project.

The security services used for this particular project by the ACC Team are as follows: -

- **AWS Shield Standard**

AWS Shield is a managed Distributed Denial of Solution (DDoS) prevention service for Amazon Web Services (AWS) applications. There is no need to contact AWS Support to benefit from DDoS protection since AWS Shield delivers always-on monitoring and automated inline mitigations that minimise application downtime and latency.

AWS Shield Standard provides default safeguards to all AWS customers at no additional cost. AWS Shield Standard protects your website or apps from the most prevalent and frequent network and transport layer DDoS assaults.

By Using AWS Shield Standard, we were able to provide automatic protections to our client at no additional cost. It further helped the client in protecting their website from the most prevalent and frequent network & transport layer DDos assaults.

- **AWS WAF (Web Application Firewall)**

Web applications are becoming more and more important to businesses and individuals (e.g., web portals, enterprise web apps, business automation web solutions, eCommerce web apps, etc.). On layer 7 of the OSI model, a WAF monitors HTTP/HTTPS requests and protects web applications from harmful actions. As a result, a WAF is an essential safeguard against an ever-increasing number of web security risks.

WAF's Advantages

1. Other security measures, such as firewalls and intrusion prevention systems, are completed.
2. Reduces cloud security expenses by removing the need for costly specialised hardware or IT security personnel.
3. Filters and monitors traffic at the application layer (layer 7), something that no other firewall can do.
4. Prevents sensitive data from being sent outside of the application without permission.
5. Reduce the chances of data theft, downtime, and security breaches.
6. WAF may be scaled to guard against the most powerful layer 7 DDoS assaults

- **AWS GuardDuty**

Amazon GuardDuty is a threat detection service that protects your Amazon Web Services accounts, workloads, and data stored in Amazon S3 by continually monitoring for harmful activities and illegal conduct.

Although the cloud makes it easier to gather and aggregate account and network activity, security teams may find it time demanding to regularly examine event log data for possible risks. You now have a smart and cost-effective solution for continuous threat monitoring in Amazon Web Services Cloud with GuardDuty. To identify and prioritise possible threats, the service employs machine learning, anomaly detection, and integrated threat intelligence. GuardDuty examines tens of billions of events from a variety of Amazon Web Services data sources, including Amazon CloudTrail event logs, Amazon VPC Flow Logs, and DNS logs.

- **AWS IAM**

AWS Identity and Access Management (IAM) allows for fine-grained access management throughout the whole AWS infrastructure. You can control who has access to which services and resources, and under what conditions, using IAM. You control rights to your workforce and systems with IAM policies to guarantee least-privilege permissions.

IAM is a free service provided by Amazon Web Services. Go to the IAM console to get started with IAM, or if you've already enrolled with AWS.

- **Amazon CloudWatch**

For DevOps engineers, developers, site reliability engineers (SREs), IT managers, and product owners, Amazon CloudWatch provides a monitoring and observability solution. To monitor your apps, respond to system-wide performance changes, and optimise resource use, CloudWatch offers you with data and actionable insights. CloudWatch logs, metrics, and events are used to collect monitoring and operational data. You obtain total visibility of your AWS resources, apps, and services running on AWS and on-premises, as well as a single picture of operational health. To keep your apps running smoothly, you can use CloudWatch to detect aberrant behaviour in your environments, trigger alarms, analyse logs and metrics side by side, take automated actions, troubleshoot issues, and find insights.

Benefits of Using Cloud Watch

CloudWatch provides several advantages to organisations that use AWS resources and applications.

The following are related to the information that CloudWatch can provide, as well as its user-friendly interface.

- Provides basic function ease of use;
- Visibility for all AWS monitoring data on one platform;
- Effectively collects metrics for AWS environments;
- Increases and optimizes the operational performance of AWS and on-premises resources;
- Insights into correlations and other relationships in system performance;
- stability and reliability;
- and integration with other AWS resources
- AWS Security Hub

AWS Security Hub is a cloud security posture management service that checks for best practices, aggregates alerts, and enables automated remediation.

AWS Security Hub provides a comprehensive view of your AWS security state and assists you in comparing your environment to security industry standards and best practices.

Security Hub collects security data from AWS accounts, services, and supported third-party partner products and assists you in analyzing security trends and identifying the most critical security issues.



- **AWS CloudTrail**

AWS CloudTrail is an AWS service that allows you to manage your AWS account's governance, compliance, operational, and risk auditing. CloudTrail records actions made by a user, role, or AWS service as events. AWS Management Console, AWS Command Line Interface, and AWS SDKs and APIs activities are all included in events.

When you create an AWS account, CloudTrail is activated. A CloudTrail event is created whenever something happens in your AWS account. When you create an AWS account, CloudTrail is activated. A CloudTrail event is created whenever something happens in your AWS account. By heading to Event history in the CloudTrail console, you can simply view events.

You can see, search, and export the last 90 days of activity in your AWS account using event history. You can also establish a CloudTrail trail to save, analyse, and react to changes in your AWS resources. A trail is a setting that allows events to be delivered to an Amazon S3 bucket that you define. With Amazon CloudWatch Logs and Amazon CloudWatch Events, you can also distribute and analyse events in a trail. The CloudTrail console, as well as the AWS console, can be used to build a trail.

Benefits of using cloud trail

a. Security Examination and Troubleshooting

The user will be able to discover and troubleshoot security and operational issues with AWS CloudTrail by capturing a comprehensive history of changes that occurred in the AWS account at intervals.

b. Easier Compliance

AWS CloudTrail modifies compliance audits by automatically recording and storing event logs for actions performed on the AWS account at regular intervals. The integration with Amazon CloudWatch Logs makes it simple to search within the log data.

- Application Load Balancer

An Application Load Balancer spreads your incoming traffic over different targets in one or more Availability Zones, such as EC2 instances, containers, and IP addresses. It keeps track of the health of its registered targets and only sends traffic to those who are in good shape. Elastic Load Balancing allows you to scale your load balancer as your incoming traffic fluctuates. It can scale to the vast majority of workloads automatically. Application Load Balancers, Network Load Balancers, Gateway Load Balancers, and Classic Load Balancers are all supported by Elastic Load Balancing.

The Benefits: -

- Our client may now fully benefit from the value proposition put in place by AWS Premier Consulting Partner: ACC.
- Infrastructure automation dramatically improved the quality and repeatability of deployments, resulting in less dependency on development personnel.
- The managed services lowered IT overhead and maintenance expenses due to the nature of the solution installed on AWS.
- Auto scaling's resulted in cost savings and allowed for limitless scalability on demand. Finally, the new design eliminated single points of failure and process bottlenecks that were visible and permanent in the client's previous data centre solution, resulting in high availability, highly secure services, and decreased latency.

ABOUT ACC

ACC is an AWS Advance Partner with AWS Mobility Competency. Awarded The Best BFSI industry Consulting Partner for the year 2019, ACC has had several successful cloud migration and application development projects to its credit.

Our business offerings include Digitalisation, Cloud Services, Product Engineering, Big Data & Analytics and Cloud Security. ACC has developed several products to its credit. These include Ottohm – Enterprise Video and OTT Platform, Atlas API – API Management and Development Platform, Atlas CLM – Cloud Life Cycle Management, Atlas HCM – HR Digital Onboarding and Employee Management, Atlas ITSM – Vendor Onboarding and Service Management and Smart Contracts – Contract Automation and Management.



www.appliedcloudcomputing.com

Shubho Pramanik

(+91) 90297 20294

shubho@acc.ltd

Rogin Rappai

(+91) 8828478321

rogin.rappai@acc.ltd

also reach us at

