

Case Study - Re-Architecting and Cloud Migration



A leading financial services company providing clearing and settlement services to the financial markets. The company processes financial transactions, providing clearance, settlement and IT services for financial sector companies.

CHALLENGE:

Client has on-premise applications, which are integrated with a single sign-on service. The main requirement is to migrate all the applications to cloud in phases. The plan is to start with the single sign-on application. The approach is to avoid any application disruptions during cutover to the cloud and to allow the on-premise applications to integrate with each other.

Technical Challenges include:

- Re-architect the on-premise application to leverage various AWS Services for scalability, performance, and reliability
- Improve reliability with auto-failover on the redundant environment
- Build an efficient log analysis framework to analyze application & infrastructure
- Provision an environment to ensure data security.

SOLUTION:

Idexcel worked with client to review the functional and nonfunctional requirement along with the compliance requirements. Our team met with stakeholders in the risk and compliance groups and utilized their feedback throughout the process. The solution leverages serverless computing to achieve scalability, performance, reliability and to allow easy integration with the on-premise applications that will be migrated at a later time. It also incorporates replication of environments across multiple availability zones with intelligent fail over routing. Finally, it includes a Splunk based analytical framework to support data privacy and to enhance the team's ability to respond to incidents.



Find out how Idexcel solutions can help your business. Contact us today!

inquiry@idexcel.com | www.idexcel.com

AWS Services utilized in our solution include:

- AWS CloudTrail - CloudTrail is used to log, continuously monitor account activity related to AWS infrastructure actions using Console & SDK
- AWS CloudWatch - All logs are accumulated in CloudWatch log groups and then streamed to Splunk
- SNS - CloudWatch integrated alert mechanism to trigger incident alerts
- IAM - IAM users & roles with specific policies have been implemented to allow console access and programmatic access using SDKs.
- Lambda - Lambda has been used to stream the CloudWatch logs to Splunk and also to authenticate the API Gateway request between the applications
- Route 53 - Route 53 has been used to provide a DNS name to the API URL and to provide intelligent fail over routing in case of an outage
- ELB - ELB has been used to load balance the request from users for Splunk
- AutoScale - AutoScale has been used to scale up & down the EC2 instances hosting Splunk.
- API Gateway - API Gateway is the interface between the caller applications and the authentication service
- RDS (Aurora) - The authentication service stores the temporary keys generated by Lambda to authenticate the service request
- EC2 - EC2 has been used to host Splunk.
- WAF - WAF has been used to protect the API Gateway calls from IP Spoofing and DoS attack
- S3 - S3 has been used to store files and lambda codes. S3 is synchronized across the region to replicate code for smooth lambda deployment.
- Terraform - Terraform has been used for building, changing, and versioning infrastructure safely and efficiently
- Trusted Advisor - A trusted advisor is implemented for efficient insight into cost, security & performance parameters.
- CodeCommit - The code repository for Lambda code
- CodePipeLine - The orchestration to build & release the lambda code
- CodeBuild - Integrated with CodePipeLine to build the code
- CodeDeploy - To deploy the new version of lambda

BENEFITS:

The client team was able to integrate both cloud & on-premise applications through the migrated & re-architected single sign-on application. The serverless approach provided high availability, reliability & performance with a substantially reduced infrastructural expenditure.

The Serverless architecture in conjunction with the API Gateway & WAF also reduced the number of attacks aimed at the application.

The continuous integration and delivery solution resulted in:

- One click releases at any time in multiple environments
- A reduction of integration obstacles allowing for faster development and deployment of software solutions
- Complete insight on infrastructural and application monitoring parameters
- Automation of deployment and quality assurance
- Higher levels of security and isolation with less internal constraints

IDEXCEL COMPETENCIES



Find out how Idexcel solutions can help your business. Contact us today!

inquiry@idexcel.com | www.idexcel.com