Jeys Consulting Group

# Cloud Infrastructure Design

D088 Final Assessment

Chris Jeys

10-19-2022

Western Governors University

## CONTENTS

A. Authentication Process ..... 3
B. Remote Access ..... 3
C. Application Security ..... 3
D. Network Security ..... 4
E. Internal APIs ..... 4
F. External APIs ..... 5
G. Deployment Plan ..... 5
H. Maintenance Strategy ..... 6
I. Disaster Recovery Plan ..... 7
J. Regulatory Compliance ..... 8
K. Sources ..... 8

## A. AUTHENTICATION PROCESS

For the overall solution, the wide range of *AWS Identity Services* will be utilized. For device authentication specifically, *Amazon Cognito* has been chosen to satisfy this business requirement. With *Amazon Cognito*, multi-factor authentication is supported and compliant with PCI DSS along with other security standards and compliance certifications. The MFA functionality can be pushed to the user-base via email, SMS text messages, or time-based one-time password generators like Google Authenticator.

User pools is another feature of *Amazon Cognito* that will be used in this solution. User pools allow policy-based access control to the banking app and sign-on thru 3rd party providers like Apple, Google, and SAML identity providers. This will be critical to the quick access and ease of use for the banking consumer.

Finally, for web browser security, protection and authentication, the *Amazon Cognito* service has been chosen as it allows users the ability to use any identity provider or even multiple identity providers. With the use of *Identity Pools*, specific permissions and access can be granted to authenticated users. In addition, a separate set of permissions and access can be granted for unauthenticated users. Granting both authenticated and unauthenticated users access to Merrilton Bank's cloud application in this way will foster widespread adoption in an effective and secure manner.

## B. REMOTE ACCESS

The *AWS Client VPN* solution will be used to provide employees secure access to the AWS cloud environment allowing for admin and general system maintenance. *AWS Client VPN* utilizes the OpenVPN protocol, supporting users of various operating systems. This service is fully scalable to support current demand and provides multi-factor authentication through Active Directory and external identity providers.

## C. APPLICATION SECURITY

Security is paramount for all applications. *AWS Direct Connect + VPN* is the perfect solution that provides security on multiple levels. Encryption is performed with IPsec on the client side, protecting data in transit. To provide additional security at the perimeter, *AWS WAF* (web application firewall) and AWS Shield provide security at the perimeter. *AWS WAF* will help protect applications, and associated resources, against common security vulnerabilities, while *AWS Shield* will safeguard against Distributed Denial of Service (DDoS) attacks.

## D. NETWORK SECURITY

To provide the maximum security, *AWS Direct Connect + AWS Transit Gateway + VPN* is the recommended solution for communication between the Atlanta, GA, data center and the cloud infrastructure. *AWS Transit Gateway* provides a network transit hub for all private cloud instances and the on-premises network. *AWS Direct Connect + VPN* will provide an IPSec VPN that connects directly to the AWS network infrastructure. This proposed solution provides not only maximum security, but also with minimum latency and a consistent network experience due to network traffic never traversing the public internet and rather the massive and global AWS network infrastructure.

## E. INTERNAL APIS

In the banking industry, fraud schemes have increased dramatically over the past decade. To protect API interactions against these new and evolving fraud schemes, *AWS Fraud Detector* is the service chosen. *AWS Fraud Detector* is a fully managed solution that will automatically detect potential fraud activities like fake account creation and unauthorized transactions.

To provide APIs with branch location information, the *Amazon Location* service has been selected. The *Amazon Location* service provides applications geospatial data and location-based functionality and supports integration with other Amazon services. This will allow the new Merrilton Bank application to simplify future development, provide or restrict user access based on their geographic location,

and quickly deploy with all the security and compliance features built into the *Amazon Location* service.

For auditing and compliance purposes, *AWS CloudTrail* will be used to record all log data and internal API calls to an AWS S3 bucket for archiving. This will ensure that Merrilton Bank continues its longstanding record of maintaining local and federal regulations with the new banking application.

To interconnect all these services as the API interface and create a banking application for Merrilton Bank, *AWS Lambda* functions have been chosen. *AWS Lambda* will be called to pass confidential user and banking information to the different services. This will ensure that the final solution developed for Merrilton Bank and its users is a secure and robust banking application that meets all goals and expectations.

## F. EXTERNAL APIS

It's standard industry practice for single sign-on(SSO) to be implemented to ease and improve a user's experience while accessing applications. For this purpose, IAM Identity Center has been selected as Merrilton Bank's new banking application solution. For further integration with credit score providers like Equifax and Experian, the *AWS Secrets Manager* solution will allow external APIs to rotate database credentials, API keys, and other secrets as required.

Location data look-up will be achieved with the *Amazon Location* service, similar to the implementation for internal APIs. To provide the external API interconnect between this service with *AWS Secrets Manager*, *AWS Lambda* will be utilized to pass along and process the real-time. This will give users quick and secure access to the banking application based on their geographic location.

## G. DEPLOYMENT PLAN

The deployment plan is critical to successfully launching and adopting Merrilton Bank's new banking application. The *Refactoring* strategy is being adopted for this deployment plan. This strategy is essentially an evaluation and architecture using the cloud-native features available in AWS. To support this strategy, the *AWS Migration Evaluator* will use real-time data points about Merrillton Bank's environment and then provide accurate data-driven recommendations for the timeline to provision the cloud infrastructure, right-sizing those resources, and the associated cost estimates for the bank application. The *AWS Migration Evaluator* will also ensure the appropriate number of resources are provisioned and deployed for the right price point allowing Merrilton Bank to stay within budget when developing and deploying the new cloud application.

Redundancy planning is also critical and available within the *AWS Migration Evaluator*. With this tool, planning for the costs associated with adding redundancy to a cloud environment but they are also critical to a successful deployment plan. For this solution, availability zones, load balancing, & auto-scaling groups will be used as they are all essential and necessary features in an ever-changing cloud environment. Availability zones will provide redundancy at the data center level to the banking application. The application is being deployed across multiple availability zones reduces the risk of application downtime due to natural disasters and other scenarios within a geographic area. For network traffic, *Elastic Load Balancing(ELB)* will be utilized to distribute traffic across the cloud infrastructure to help improve application scalability, security, and maintain service level agreement(SLA) compliance for business users and government regulators. The final step in redundancy planning for this solution is the use of auto-scaling groups(ASG). ASGs allow for the automatic scaling of EC2 instances to meet the changing demand of users for Merrilton Bank's app. A minimum amount of instances can be maintained for cost savings while also providing the ability to auto-scale the solution during heavy workloads to deliver a consistent user experience no matter the time of day.

## H. MAINTENANCE STRATEGY

*AWS DevOps* services, and the associated *DevOps* model, will be used to help Merrilton Bank deliver a banking experience that can evolve and improve based on customer's needs and feedback. The *AWS DevOps* delivery pipeline phases consist of Build, Test, & Release. These phases can be used for short and long-term patch management. This solution will be optimal for quickly patching major security vulnerabilities while also providing the framework for planned patch management like major OS or database upgrades. The *DevOps* model also provides a feedback loop that facilitates communication and collaboration. This allows business users and developers to proactively plan for future updates while also being reactive to issues resulting from recent changes.

The *AWS DevOps* service will also be used for updates and redevelopment work. The iterative process laid out by the *DevOps* model will allow for quick turnarounds on updates to the banking app, making them available in the Google Play and Apple App Store. This will be scheduled to occur on a 30-day update cycle. If there are critical bugs or issues raised from user feedback, redevelopment can be quickly ramped up to resolve the bug and provide a fix to the banking app's user community.

A Blue-Green strategy will be utilized to support the smooth rollout of updates and redevelopment work. This strategy uses one active and one passive system that can be swapped interchangeably during update and redevelopment rollouts. This makes the banking application a high-availability solution that minimizes disruption for banking users.

## I. DISASTER RECOVERY PLAN

There are several layers of this solution to help overcome system faults and disaster recovery scenarios. To endure system faults, network load balancers and failover EC2 instances have been built into the banking app's architecture. This will ensure the network is routed evenly across the EC2 instances while quickly diverting network traffic if an EC2 instance goes down and is replaced by another. *AWS Availability Zones* are another feature that will help overcome system faults and maintain continuous operations. With the use of *AWS Availability Zones*, the

banking cloud infrastructure will have redundancy and fault tolerance built into the solution allowing for the automation of processes and procedures needed to maintain continuous operations during unforeseen circumstances.

For disaster recovery scenarios, it's more appropriate to have a Disaster Recovery Plan to document processes and procedures that should be taken in the event of natural disasters or similar scenarios. The creation of a Disaster Recovery Plan is outside of the scope of this project. However, it's strongly advised that the Disaster Recovery Plan is tested regularly and includes a communication plan, means for impact analysis, and an accurate inventory of all systems. This will ensure that all infrastructure components are accounted for, the banking application is highly available, and all parties that assist in recovery efforts are well-versed and have practiced implementing the Disaster Recovery Plan.

## J. REGULATORY COMPLIANCE

Maintaining regulatory compliance helps mitigate risks, data loss, and builds trust with stakeholders and customers. To this point, AWS provides banking institutions with a compliance framework and security tools to maintain legal and regulatory compliance consistent with FFIEC and FDIC Guidance. *AWS Audit Manager* provides a compliance framework to help Merrilton Bank audit AWS usage to simplify risk management and compliance with regulations and industry standards such as PCIDSS, SOX, GBLA, & FISMA. AWS's commitment to abide by, provide, and satisfy these legal and regulatory requirements will ensure financial governance and a reputable future for Merrilton Bank and its stakeholders.

## K. SOURCES


- AWS Identity Services
  - https://aws.amazon.com/identity/
- Amazon Cognito – Identity Mgmt for your apps

- https://aws.amazon.com/cognito/
- Authentication with Amazon Cognito in the Browser
  - https://aws.amazon.com/blogs/developer/authentication-with-amazon-cognito-in-the-browser/
- AWS Client VPN
  - https://aws.amazon.com/vpn/client-vpn/
- AWS Direct Connect + VPN
  - https://docs.aws.amazon.com/whitepapers/latest/aws-vpc-connectivity-options/aws-direct-connect-vpn.html
- AWS WAF - Web Application Firewall
  - https://aws.amazon.com/waf/
- AWS Shield
  - https://aws.amazon.com/shield/?whats-new-cards.sort-by=item.additionalFields.postDateTime&whats-new-cards.sort-order=desc
- AWS Direct Connect + AWS Transit Gateway + VPN
  - https://docs.aws.amazon.com/whitepapers/latest/aws-vpc-connectivity-options/aws-direct-connect-aws-transit-gateway-vpn.html
- What is a transit gateway?
  - https://docs.aws.amazon.com/vpc/latest/tgw/what-is-transit-gateway.html
- Episode 2: Securing your app's infrastructure
  - https://aws.amazon.com/blogs/publicsector/episode-2-securing-your-apps-infrastructure/
- Amazon Location APIs
  - https://docs.aws.amazon.com/location/latest/developerguide/location-actions.html
- Welcome to Amazon Location Service
  - https://docs.aws.amazon.com/location/latest/APIReference/welcome.html
- AWS Lambda Features
  - https://aws.amazon.com/lambda/features/
- 7 Strategies for Migrating Applications to the Cloud, introducing AWS Mainframe Modernization and AWS Migration Hub Refactor Spaces

    - https://aws.amazon.com/blogs/enterprise-strategy/new-possibilities-seven-strategies-to-accelerate-your-application-migration-to-aws/
- Auto Scaling groups
    - https://docs.aws.amazon.com/autoscaling/ec2/userguide/auto-scaling-groups.html
- Regulatory Overview Financial Services — United States
    - https://d1.awsstatic.com/fs-compliance-center/pdf-summaries/united-states.pdf
- AWS Compliance Programs
    - https://aws.amazon.com/compliance/programs/
- Effective compliance and audit management using Amazon Web Services (AWS) Audit Manager
    - https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-deloitte-aws-audit-manager-whitepaper-clean.pdf
- Gramm-Leach-Bliley Act
    - https://docs.aws.amazon.com/audit-manager/latest/userguide/gramm-leach-bliley-act.html