Test Project

Cloud Computing

Day four

Submitted by: Qiang Wang CN

Contents

Contents **3**
Description of project and tasks ..... Error! Bookmark not defined.
Service Details ..... Error! Bookmark not defined.
Reference ..... Error! Bookmark not defined.

Contents

This Test Project consists of the following documentation/files:

1. WSC2022SE_TP53_MainDocument_actual_en
2. WSC2022SE_TP53_Day1_actual_en
3. WSC2022SE_TP53_Day2_actual_en
4. WSC2022SE_TP53_Day3_actual_en
5. **WSC2022SE_TP53_Day4_actual_en**

Description of project and tasks

Today's Test Project is 6.5 hours (until 15:30).

The goal this Test Project is further test specific cloud computing skills through a series of unique modules. There will be nine jam challenges for you to complete in any order that you choose.

Tasks

1. Log into the AWS Provided testing platform using the same credentials you've used previously
2. Read the documentation thoroughly (Outlined below)
3. Continue until the Test Project day has completed (6.5 hours)

AWS Jam - Challenge 1

Summary

The application is running on Amazon Elastic Compute Cloud (Amazon EC2) with an Application Load Balancer and Amazon CloudFront for content delivery. CloudFront brings content closer to customers and improves the security posture while caching helps to reduce load on the backend servers.

The customer has requested support and needs your AWS expertise! You are expected to troubleshoot immediately to further secure the application and improve the end user experience. The application team has provided an architecture diagram (see below).

Amazon CloudFront is a requirement but this service has not been properly secured. Both Origins, static failover content, and the application's backend are directly accessible from the public internet.

Two additional teams woke up to an AWS expert within the office! They ask you to have a "quick" look into their issues (make sure to take a break while testing the static failover content, CloudFront changes can take some time). Stay curious, an interesting troubleshooting session is ahead.

You will use the following AWS services: Amazon CloudFront, Amazon Simple Storage Service (Amazon S3), Elastic Load Balancing, and Amazon EC2.

Inventory

- CloudFront Distribution
- CloudFront Origin Access Identity
- Jam S3 static content bucket
- Application Load Balancer

AWS Jam – Challenge 2

Summary

You have been hired by Travelme as AI/ML Expert. It is a global company and a lot of employees travel constantly. The company reimburses them for the travel expense when they submit the receipts. The CFO has a team of 10 people who manually go through each receipt and enter it in the system. This takes a lot of time and sometimes delays the reimbursement process. The employees complain if they do not get their reimbursement in a week.
As part of the new initiative, the CFO came to you and asked him to assist in automating the invoice entering process.

Inventory

- Lambda
- Textract API
- S3

AWS Jam – Challenge 3

Summary

This JAM Challenge will walk you through configuring enhanced routing in your Egress or Inspection VPC to insert a firewall between NAT Gateway in multiple AZ's and the Internet Gateway. This is new functionality as of August 2021 that allows re-directing ingress and inter-subnet traffic to the AWS Network Firewall.

You are a new network security engineer at a financial institution. You are taking over for a former employee that has left the company in the middle of implementing AWS Network Firewall to block streaming video services for instances running in their AWS environment. You task is to implement the AWS Network Firewall endpoints, configure routing to utilize the endpoints, and add additional rules to the firewall policy.

The company's AWS network consists of a single account and VPC, with instances in private subnets in two AZ's that egress out NAT GW's. Using the principals and best practice of AZI (Availability Zone Independence) implement AWS Network Firewall, and modify the VPC configuration to utilize this new feature.

Here is the diagram of the VPC as deployed at the start of this assignment. Your predecessor created subnets for your firewall to live in, and create the base rule groups for you to use. Now it's up to you to finish the job.

Note that you will use SSM to access the test instances within the private subnets.

Inventory

- AWS Network Firewall Rule Groups: icmp-alert, domain-deny
- Inspection VPC
- Subnets: Network Firewall Subnet A, Network Firewall Subnet B

AWS Jam – Challenge 4

Summary

Sam joined an IoT device manufacturing company as a Cloud native application developer. The application team has built several unsecured REST APIs using Amazon API Gateway and AWS Lambda.

Sam's first task was to enforce JSON Web Token (JWT) token-based authorization for those APIs. She implemented a Proof-of-Concept(PoC) in one of the APIs using a Lambda authorizer.

However, the deployment of the PoC resulted in the API to return errors.

The challenge is to troubleshoot the API Gateway configuration, such that the API functions as expected again.

Inventory

- "Device-ID-Generator" REST API
- Lambda function

AWS Jam – Challenge 5

Summary

Your company, which operates an e-commerce site, has been under attack intermittently since last week. According to a security team report, there are some vulnerabilities in the API for the internet. Specifically, SQL Injection.

You just received an urgent email from CISO.

According to the email, he has appointed to you as our best AWS specialist to solve this issue. You need to carry out the transition to the new API today.

To solve issue quickly, you will use some AWS services, such as Amazon API Gateway, AWS WAF

Inventory

- Application Load Balancer
- Lambda function

AWS Jam – Challenge 6

Summary

You are hired new as an AWS Certified Security Administrator for your company.

You notice that the company's AWS account has bunch of services and all of them are using a single KMS key. You see that Amazon Simple Storage Service (S3) and Amazon Simple Queue Service (SQS) are encrypting objects using the very same Key Management Service (KMS) key.

You are aware of the security best practice and you want to stop using same key for different services. Having different keys reduces your exposure to risk of unauthorized access to KMS keys.

In this challenge

1. You will implement one key for one service, and thereby limit your security exposure.
2. You will edit resource policy to limit keys to a single account only to limit exposure.
3. And finally, you want to enable key rotation.

Solve this challenge to fortify your AWS accounts security posture.

Inventory

- Amazon S3
- AWS KMS
- Amazon SQS queue

AWS Jam – Challenge 7

Summary

Your company has have given your developers the ability to create IAM Roles. It has been discovered, that some of the maverick developers created roles with privileged access to bypass the restrictions placed on the Developer Roles. The Security team has come to ask for your help to come up with a creative method to prevent improper developer privilege escalation.

Inventory

- EC2: AdminHost
- IAM Permissions Boundary Policy: NoPrivilegeEscalation-PermissionsBoundary-REGION
- IAM Role for EC2: See Output Properties for oAdminHostRoleName
- CloudTrail: jam-iam-cloud-trail

AWS Jam – Challenge 8

Summary

As you were reviewing application code in a github repository for vulnerabilities, you found an IAM Access Key pair in plain text. You need to identify the IAM user and AWS Account number associated with it to start your investigation of how it ended up there.

Inventory

- IAM Key Pair

AWS Jam – Challenge 9

Summary

You have been recently hired by Best FinServe Corp (a major financial services company) as a data scientist. Best FinServe is embarking upon a digital transformation and has set a goal to automate 80% of manual processes within two years. Your boss asks you to develop a POC solution that automatically extracts information from *SEC Form S-1* filings. SEC Form S-1 is a registration statement that is filed by companies to the Securities and Exchange Commission (SEC) before their initial public offering (IPO) in the U.S. The SEC Form S-1 contains information such as the number of shares offered and the offering price, which are very valuable information for the investors.

Due to tight deadlines, your team can only get 300 documents annotated, which is likely not enough for training a model from scratch. You have limited experience in the Natural Language Processing (NLP) domain, and can greatly benefit from an AI service that simplifies NLP for data scientists.

Inventory

- SageMaker Notebook Instance
- Partially filled Jupyter Notebook