AWS Solutions Architect Associate - Reviewer 1

Designing a Secure Applications and Architectures 1

Question 1: A company is designing a banking portal that uses Amazon ElastiCache for Redis as its distributed session management component. Since the other Cloud Engineers in your department have access to your ElastiCache cluster, you have to secure the session data in the portal by requiring them to enter a password before they are granted permission to execute Redis commands.

As the Solutions Architect, which of the following should you do to meet the above requirement?

a. **Authenticate the users using Redis AUTH by creating a new Redis Cluster with both the --transit-encryption-enabled and --auth-token parameters enabled.**
b. Set up a Redis replication group and enable the AtRestEncryptionEnabled parameter.
c. Set up an IAM Policy and MFA which requires the Cloud Engineers to enter their IAM credentials and token before they can access the ElastiCache cluster.
d. Enable the in-transit encryption for Redis replication groups.

Question 2: A company needs to design an online analytics application that uses Redshift Cluster for its data warehouse. Which of the following services allows them to monitor all API calls in Redshift instances and can also provide secured data for auditing and compliance purposes?

a. Amazon CloudWatch
b. Amazon Redshift Spectrum
c. AWS X-Ray
d. **AWS CloudTrail**

Question 3: A media company has an Amazon ECS Cluster, which uses the Fargate launch type, to host its news website. The database credentials should be supplied using environment variables, to comply with strict security compliance. As the Solutions Architect, you have to ensure that the credentials are secure and that they cannot be viewed in plaintext on the cluster itself. Which of the following is the most suitable solution in this scenario that you can implement with minimal effort?

a. In the ECS task definition file of the ECS Cluster, store the database credentials using Docker Secrets to centrally manage these sensitive data and securely transmit it to only those containers that need access to it. Secrets are encrypted during transit and at rest. A given secret is only accessible to those services which have been granted explicit access to it via IAM Role, and only while those service tasks are running.

b. Use the AWS Systems Manager Parameter Store to keep the database credentials and then encrypt them using AWS KMS. Create an IAM Role for your Amazon ECS task execution role (taskRoleArn) and reference it with your task definition, which allows access to both KMS and the Parameter Store. Within your container definition, specify secrets with the name of the environment variable to be set in the container and the full ARN of the Systems Manager Parameter Store parameter containing the sensitive data to present to the container.

c. Store the database credentials in the ECS task definition file of the ECS Cluster and encrypt it with KMS. Store the task definition JSON file in a private S3 bucket and ensure that HTTPS is enabled on the bucket to encrypt the data in-flight. Create an IAM role to the ECS task definition script that allows access to the specific S3 bucket and then pass the --cli-input-json parameter when calling the ECS register-task-definition. Reference the task definition JSON file in the S3 bucket which contains the database credentials.

d. Use the AWS Secrets Manager to store the database credentials and then encrypt them using AWS KMS. Create a resource-based policy for your Amazon ECS task execution role (taskRoleArn) and reference it with your task definition which allows access to both KMS and AWS Secrets Manager. Within your container definition, specify secrets with the name of the environment variable to set in the container and the full ARN of the Secrets Manager secret which contains the sensitive data, to present to the container.

Question 4: An online medical system hosted in AWS stores sensitive Personally Identifiable Information (PII) of the users in an Amazon S3 bucket. Both the master keys and the unencrypted data should never be sent to AWS to comply with the strict compliance and regulatory requirements of the company. Which S3 encryption technique should the Architect use?

a. Use S3 client-side encryption with a KMS-managed customer master key.

b. Use S3 client-side encryption with a client-side master key.

c. Use S3 server-side encryption with a customer provided key.

d. Use S3 server-side encryption with a KMS managed key.

Question 5: A government entity is conducting a population and housing census in the city. Each household information uploaded on their online portal is stored in encrypted files in Amazon S3. The government assigned its Solutions Architect to set compliance policies that verify sensitive data in a manner that meets their compliance standards. They should also be alerted if there are compromised files detected containing personally identifiable information (PII), protected health information (PHI) or intellectual properties (IP). Which of the following should the Architect implement to satisfy this requirement?

a. **Set up and configure Amazon Macie to monitor and detect usage patterns on their Amazon S3 data.**
b. Set up and configure Amazon Inspector to send out alert notifications whenever a security violation is detected on their Amazon S3 data.
c. Setup and configure Amazon GuardDuty to monitor malicious activity on their Amazon S3 data.
d. Set up and configure Amazon Rekognition to monitor and recognize patterns on their Amazon S3 data.

Question 6: A software development company is using serverless computing with AWS Lambda to build and run applications without having to set up or manage servers. They have a Lambda function that connects to a MongoDB Atlas, which is a popular Database as a Service (DBaaS) platform and also uses a third party API to fetch certain data for their application. One of the developers was instructed to create the environment variables for the MongoDB database hostname, username, and password as well as the API credentials that will be used by the Lambda function for DEV, SIT, UAT, and PROD environments.

Considering that the Lambda function is storing sensitive database and API credentials, how can this information be secured to prevent other developers in the team, or anyone, from seeing these credentials in plain text? Select the best option that provides maximum security.

a. **Create a new KMS key and use it to enable encryption helpers that leverage on AWS Key Management Service to store and encrypt the sensitive information.**
b. Enable SSL encryption that leverages on AWS CloudHSM to store and encrypt the sensitive information.
c. AWS Lambda does not provide encryption for the environment variables. Deploy your code to an EC2 instance instead.
d. There is no need to do anything because, by default, AWS Lambda already encrypts the environment variables using the AWS Key Management Service.

Question 7: A Solutions Architect is hosting a website in an Amazon S3 bucket named tutorialsdojo. The users load the website using the following URL: http://tutorialsdojo.s3-website-us-east-1.amazonaws.com and there is a new requirement to add a JavaScript on the webpages in order to make authenticated HTTP GET requests against the same bucket by using the Amazon S3 API endpoint (tutorialsdojo.s3.amazonaws.com). Upon testing, you noticed that the web browser blocks JavaScript from allowing those requests. Which of the following options is the MOST suitable solution that you should implement for this scenario?

a. Enable Cross-Region Replication (CRR).
b. Enable Cross-origin resource sharing (CORS) configuration in the bucket.
c. Enable cross-account access.
d. Enable Cross-Zone Load Balancing.

Question 8: A Solutions Architect needs to make sure that the On-Demand EC2 instance can only be accessed from this IP address (110.238.98.71) via an SSH connection. Which configuration below will satisfy this requirement?

a. Security Group Inbound Rule: Protocol – UDP, Port Range – 22, Source 110.238.98.71/0
b. Security Group Inbound Rule: Protocol – UDP, Port Range – 22, Source 110.238.98.71/32
c. Security Group Inbound Rule: Protocol – TCP. Port Range – 22, Source 110.238.98.71/0
d. Security Group Inbound Rule: Protocol – TCP. Port Range – 22, Source 110.238.98.71/32

Question 9: A web application is using CloudFront to distribute their images, videos, and other static contents stored in their S3 bucket to its users around the world. The company has recently introduced a new member-only access to some of its high quality media files. There is a requirement to provide access to multiple private media files only to their paying subscribers without having to change their current URLs. Which of the following is the most suitable solution that you should implement to satisfy this requirement?

a. Configure your CloudFront distribution to use Field-Level Encryption to protect your private data and only allow access to members.
b. Configure your CloudFront distribution to use Match Viewer as its Origin Protocol Policy which will automatically match the user request. This will allow access to the private content if the request is a paying member and deny it if it is not a member.
c. Create a Signed URL with a custom policy which only allows the members to see the private files.
d. Use Signed Cookies to control who can access the private files in your CloudFront distribution by modifying your application to determine whether a user should have access to your content. For members, send the required Set-Cookie headers to the viewer which will unlock the content only to them.

Question 10: A travel photo sharing website is using Amazon S3 to serve high-quality photos to visitors of your website. After a few days, you found out that there are other travel websites linking and using your photos. This resulted in financial losses for your business. What is the MOST effective method to mitigate this issue?

a. Block the IP addresses of the offending websites using NACL.
b. Use CloudFront distributions for your photos.
c. Store and privately serve the high-quality photos on Amazon WorkDocs instead.
d. Configure your S3 bucket to remove public read access and use pre-signed URLs with expiry dates.

Question 11: A company has 3 DevOps engineers that are handling its software development and infrastructure management processes. One of the engineers accidentally deleted a file hosted in Amazon S3 which has caused disruption of service.

What can the DevOps engineers do to prevent this from happening again?

a. Use S3 Infrequently Accessed storage to store the data.
b. Enable S3 Versioning and Multi-Factor Authentication Delete on the bucket.
c. Create an IAM bucket policy that disables delete operation.
d. Set up a signed URL for all users.

Question 12: A financial application is composed of an Auto Scaling group of EC2 instances, an Application Load Balancer, and a MySQL RDS instance in a Multi-AZ Deployments configuration. To protect the confidential data of your customers, you have to ensure that your RDS database can only be accessed using the profile credentials specific to your EC2 instances via an authentication token.

As the Solutions Architect of the company, which of the following should you do to meet the above requirement?

a. Use a combination of IAM and STS to restrict access to your RDS instance via a temporary token.
b. Enable the IAM DB Authentication.
c. Configure SSL in your application to encrypt the database connection to RDS.
d. Create an IAM Role and assign it to your EC2 instances which will grant exclusive access to your RDS instance.

Question 13: An application that records weather data every minute is deployed in a fleet of Spot EC2 instances and uses a MySQL RDS database instance. Currently, there is only one RDS instance running in one Availability Zone. You plan to improve the database to ensure high availability by synchronous data replication to another RDS instance.

Which of the following performs synchronous data replication in RDS?

a. DynamoDB Read Replica
b. CloudFront running as a Multi-AZ deployment
c. RDS Read Replica
d. RDS DB instance running as a Multi-AZ deployment

Question 14: A pharmaceutical company has resources hosted on both their on-premises network and in AWS cloud. They want all of their Software Architects to access resources on both environments using their on-premises credentials, which is stored in Active Directory.

In this scenario, which of the following can be used to fulfill this requirement?

a. Set up SAML 2.0-Based Federation by using a Web Identity Federation.
b. Use IAM users
c. Use Amazon VPC
d. Set up SAML 2.0-Based Federation by using a Microsoft Active Directory Federation Service (AD FS).

Question 15: A newly hired Solutions Architect is assigned to manage a set of CloudFormation templates that are used in the company's cloud architecture in AWS. The Architect accessed the templates and tried to analyze the configured IAM policy for an S3 bucket.

```
{
"Version": "2012-10-17",
"Statement": [
 {
  "Effect": "Allow",
  "Action": [
   "s3:Get*",
   "s3:List*"
  ],
  "Resource": "*"
 },
 {
  "Effect": "Allow",
  "Action": "s3:PutObject",
  "Resource": "arn:aws:s3:::boracay/*"
 }
]
}
```

What does the above IAM policy allow? (Select THREE.)

a. **An IAM user with this IAM policy is allowed to read objects from all S3 buckets owned by the account.**
b. An IAM user with this IAM policy is allowed to read objects in the boracay S3 bucket but not allowed to list the objects in the bucket.
c. An IAM user with this IAM policy is allowed to change access rights for the boracay S3 bucket.
d. **An IAM user with this IAM policy is allowed to read objects from the boracay S3 bucket.**
e. **An IAM user with this IAM policy is allowed to write objects into the boracay S3 bucket.**
f. An IAM user with this IAM policy is allowed to read and delete objects from the boracay S3 bucket.

Question 16: A company is in the process of migrating their applications to AWS. One of their systems requires a database that can scale globally and handle frequent schema changes. The application should not have any downtime or performance issues whenever there is a schema change in the database. It should also provide a low latency response to high-traffic queries. Which is the most suitable database solution to use to achieve this requirement?

a. An Amazon Aurora database with Read Replicas
b. Redshift
c. Amazon DynamoDB
d. An Amazon RDS instance in Multi-AZ Deployments configuration

Question 17: A Solutions Architect identified a series of DDoS attacks while monitoring the VPC. The Architect needs to fortify the current cloud infrastructure to protect the data of the clients. Which of the following is the most suitable solution to mitigate these kinds of attacks?

a. Using the AWS Firewall Manager, set up a security layer that will prevent SYN floods, UDP reflection attacks, and other DDoS attacks.
b. A combination of Security Groups and Network Access Control Lists to only allow authorized traffic to access your VPC.
c. Use AWS Shield Advanced to detect and mitigate DDoS attacks.
d. Set up a web application firewall using AWS WAF to filter, monitor, and block HTTP traffic.

Question 18: A Solutions Architect designed a serverless architecture that allows AWS Lambda to access an Amazon DynamoDB table named tutorialsdojo in the US East (N. Virginia) region. The IAM policy attached to a Lambda function allows it to put and delete items in the table. The policy must be updated to only allow two operations in the tutorialsdojo table and prevent other DynamoDB tables from being modified.

Which of the following IAM policies fulfill this requirement and follow the principle of granting the least privilege?

a.
```
{

        "Version": "2012-10-17",

        "Statement": [

        {

        "Sid": "TutorialsdojoTablePolicy",

        "Effect": "Allow",
        "Action": [
        "dynamodb:PutItem",
        "dynamodb:DeleteItem"
        ],
        "Resource": "arn:aws:dynamodb:us-east-1:120618981206:table/tutorialsdojo"
        }
        ]
```

} **(Correct)**

b. {

```
"Version": "2012-10-17",
"Statement": [
{
"Sid": "TutorialsdojoTablePolicy",
"Effect": "Allow",
"Action": [
"dynamodb:PutItem",
"dynamodb:DeleteItem"
],
"Resource": "arn:aws:dynamodb:us-east-1:120618981206:table/*"
}
]
}
```

```
    }
```

c.

```
{
    "Version": "2012-10-17",
    "Statement": [
    {
    "Sid": "TutorialsdojoTablePolicy1",
    "Effect": "Allow",
    "Action": [
    "dynamodb:PutItem",
    "dynamodb:DeleteItem"
    ],
    "Resource":
    "arn:aws:dynamodb:us-east-1:1206189812061898:table/tutorialsdojo"
    },
    {
    "Sid": "TutorialsdojoTablePolicy2",
    "Effect": "Deny",
    "Action": "dynamodb:*",
    "Resource": "arn:aws:dynamodb:us-east-1:1206189812061898:table/*"
    }
    ]
    }
```

d.

```
{
    "Version": "2012-10-17",
    "Statement": [
    {
    "Sid": "TutorialsdojoTablePolicy1",
    "Effect": "Allow",
    "Action": [
    "dynamodb:PutItem",
    "dynamodb:DeleteItem"
    ],
    "Resource":
    "arn:aws:dynamodb:us-east-1:1206189812061898:table/tutorialsdojo"
    },
    {
    "Sid": "TutorialsdojoTablePolicy2",
    "Effect": "Allow",
    "Action": "dynamodb:*",
    "Resource":
    "arn:aws:dynamodb:us-east-1:1206189812061898:table/tutorialsdojo"
    }
    ]
    }
```

Question 19: A company hosted an e-commerce website on an Auto Scaling group of EC2 instances behind an Application Load Balancer. The Solutions Architect noticed that the website is receiving a large number of illegitimate external requests from multiple systems with IP addresses that constantly change. To resolve the performance issues, the Solutions Architect must implement a solution that would block the illegitimate requests with minimal impact on legitimate traffic. Which of the following options fulfills this requirement?

a. Create a custom rule in the security group of the Application Load Balancer to block the offending requests.
b. Create a regular rule in AWS WAF and associate the web ACL to an Application Load Balancer.
c. Create a custom network ACL and associate it with the subnet of the Application Load Balancer to block the offending requests.
d. Create a rate-based rule in AWS WAF and associate the web ACL to an Application Load Balancer.

Question 20: In a government agency that you are working for, you have been assigned to put confidential tax documents on AWS cloud. However, there is a concern from a security perspective on what can be put on AWS.

What are the features in AWS that can ensure data security for your confidential documents? (Select TWO.)

a. S3 On-Premises Data Encryption
b. Public Data Set Volume Encryption
c. S3 Server-Side Encryption
d. S3 Client-Side Encryption
e. EBS On-Premises Data Encryption

Question 21: A tech company that you are working for has undertaken a Total Cost Of Ownership (TCO) analysis evaluating the use of Amazon S3 versus acquiring more storage hardware. The result was that all 1200 employees would be granted access to use Amazon S3 for storage of their personal documents.

Which of the following will you need to consider so you can set up a solution that incorporates a single sign-on feature from your corporate AD or LDAP directory and also restricts access for each individual user to a designated user folder in an S3 bucket? (Select TWO.)

a. **Set up a Federation proxy or an Identity provider, and use AWS Security Token Service to generate temporary tokens.**
b. **Configure an IAM role and an IAM Policy to access the bucket.**
c. Map each individual user to a designated user folder in S3 using Amazon WorkDocs to access their personal documents.
d. Set up a matching IAM user for each of the 1200 users in your corporate directory that needs access to a folder in the S3 bucket.
e. Use 3rd party Single Sign-On solutions such as Atlassian Crowd, OKTA, OneLogin and many others.

Question 22: A company requires all the data stored in the cloud to be encrypted at rest. To easily integrate this with other AWS services, they must have full control over the encryption of the created keys and also the ability to immediately remove the key material from AWS KMS. The solution should also be able to audit the key usage independently of AWS CloudTrail.

Which of the following options will meet this requirement?

a. Use AWS Key Management Service to create a CMK in a custom key store and store the non-extractable key material in Amazon S3.
b. **Use AWS Key Management Service to create a CMK in a custom key store and store the non-extractable key material in AWS CloudHSM.**
c. Use AWS Key Management Service to create AWS-owned CMKs and store the non-extractable key material in AWS CloudHSM.
d. Use AWS Key Management Service to create AWS-managed CMKs and store the non-extractable key material in AWS CloudHSM.