AWS Solutions Architect Associate - Reviewer 1

Designing a Resilient Architectures 1

Question 1: A Solutions Architect is working for a company which has multiple VPCs in various AWS regions. The Architect is assigned to set up a logging system which will track all of the changes made to their AWS resources in all regions, including the configurations made in IAM, CloudFront, AWS WAF, and Route 53. In order to pass the compliance requirements, the solution must ensure the security, integrity, and durability of the log data. It should also provide an event history of all API calls made in AWS Management Console and AWS CLI.

Which of the following solutions is the best fit for this scenario?

a. Set up a new CloudWatch trail in a new S3 bucket using the CloudTrail console and also pass the --is-multi-region-trail parameter then encrypt log files using KMS encryption. Apply Multi Factor Authentication (MFA) Delete on the S3 bucket and ensure that only authorized users can access the logs by configuring the bucket policies.
b. Set up a new CloudWatch trail in a new S3 bucket using the AWS CLI and also pass both the --is-multi-region-trail and --include-global-service-events parameters then encrypt log files using KMS encryption. Apply Multi Factor Authentication (MFA) Delete on the S3 bucket and ensure that only authorized users can access the logs by configuring the bucket policies.
c. **Set up a new CloudTrail trail in a new S3 bucket using the AWS CLI and also pass both the --is-multi-region-trail and --include-global-service-events parameters then encrypt log files using KMS encryption. Apply Multi Factor Authentication (MFA) Delete on the S3 bucket and ensure that only authorized users can access the logs by configuring the bucket policies.**
d. Set up a new CloudTrail trail in a new S3 bucket using the AWS CLI and also pass both the --is-multi-region-trail and --no-include-global-service-events parameters then encrypt log files using KMS encryption. Apply Multi Factor Authentication (MFA) Delete on the S3 bucket and ensure that only authorized users can access the logs by configuring the bucket policies.

Question 2: A company conducted a surprise IT audit on all of the AWS resources being used in the production environment. During the audit activities, it was noted that you are using a combination of Standard and Convertible Reserved EC2 instances in your applications. They argued that you should have used Spot EC2 instances instead as it is cheaper than the Reserved Instance.

Which of the following are the characteristics and benefits of using these two types of Reserved EC2 instances, which you can use as justification? (Select TWO.)

a. It can enable you to reserve capacity for your Amazon EC2 instances in multiple Availability Zones and multiple AWS Regions for any duration.
b. Reserved Instances don't get interrupted unlike Spot instances in the event that there are not enough unused EC2 instances to meet the demand.
c. It runs in a VPC on hardware that's dedicated to a single customer.
d. Standard Reserved Instances can be later exchanged for other Convertible Reserved Instances
e. Convertible Reserved Instances allow you to exchange for another Convertible Reserved instance with a different instance type and tenancy.

Question 3: An IT consultant is working for a large financial company. The role of the consultant is to help the development team build a highly available web application using stateless web servers.

In this scenario, which AWS services are suitable for storing session state data? (Select TWO.)

a. Redshift Spectrum
b. ElastiCache
c. RDS
d. Glacier
e. DynamoDB

Question 4: A suite of web applications is hosted in an Auto Scaling group of EC2 instances across three Availability Zones and is configured with default settings. There is an Application Load Balancer that forwards the request to the respective target group on the URL path. The scale-in policy has been triggered due to the low number of incoming traffic to the application.

Which EC2 instance will be the first one to be terminated by your Auto Scaling group?

a. The instance will be randomly selected by the Auto Scaling group
b. The EC2 instance which has been running for the longest time
c. The EC2 instance which has the least number of user sessions
d. The EC2 instance launched from the oldest launch configuration

Question 5: There are a lot of outages in the Availability Zone of your RDS database instance to the point that you have lost access to the database. What could you do to prevent losing access to your database in case that this event happens again?

a. **Enabled Multi-AZ failover**
b. Make a snapshot of the database
c. Create a read replica
d. Increase the database instance size

Question 6: An organization needs a persistent block storage volume that will be used for mission-critical workloads. The backup data will be stored in an object storage service and after 30 days, the data will be stored in a data archiving storage service/

What should you do to meet the above requirement?

a. Attach an EBS volume in your EC2 instance. Use Amazon S3 to store your backup data and configure a lifecycle policy to transition your objects to Amazon S3 One Zone-IA.
b. Attach an instance store volume in your existing EC2 instance. Use Amazon S3 to store your backup data and configure a lifecycle policy to transition your objects to Amazon S3 Glacier.
c. **Attach an EBS volume in your EC2 instance. Use Amazon S3 to store your backup data and configure a lifecycle policy to transition your objects to Amazon S3 Glacier.**
d. Attach an instance store volume in your EC2 instance. Use Amazon S3 to store your backup data and configure a lifecycle policy to transition your objects to Amazon S3 One Zone-IA.

Question 7: A telecommunications company is planning to give AWS Console access to developers. Company policy mandates the use of identity federation and role-based access control. Currently, the roles are already assigned using groups in the corporate Active Directory.

In this scenario, what combination of the following services can provide developers access to the AWS console? (Select TWO.)

a. **AWS Directory Service AD Connector**
b. Lambda
c. IAM Groups
d. **IAM Roles**
e. AWS Directory Service Simple AD

Question 8: A company has a cloud architecture that is composed of Linux and Windows EC2 instances that process high volumes of financial data 24 hours a day, 7 days a week. To ensure high availability of the systems, the Solutions Architect needs to create a solution that allows them to monitor the memory and disk utilization metrics of all the instances.

Which of the following is the most suitable monitoring solution to implement?

a. Enable the Enhanced Monitoring option in EC2 and install CloudWatch agent to all the EC2 instances to be able to view the memory and disk utilization in the CloudWatch dashboard.
b. Use the default CloudWatch configuration to EC2 instances where the memory and disk utilization metrics are already available. Install the AWS Systems Manager (SSM) Agent to all the EC2 instances.
c. Use Amazon Inspector and install the Inspector agent to all EC2 instances.
d. Install the CloudWatch agent to all the EC2 instances that gathers the memory and disk utilization data. View the custom metrics in the Amazon CloudWatch console.

Question 9: A company needs to deploy at least 2 EC2 instances to support the normal workloads of its application and automatically scale up to 6 EC2 instances to handle the peak load. The architecture must be highly available and fault-tolerant as it is processing mission-critical workloads.

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

a. Create an Auto Scaling group of EC2 instances and set the minimum capacity to 2 and the maximum capacity to 6. Deploy 4 instances in Availability Zone A.
b. Create an Auto Scaling group of EC2 instances and set the minimum capacity to 4 and the maximum capacity to 6. Deploy 2 instances in Availability Zone A and another 2 instances in Availability Zone B.
c. Create an Auto Scaling group of EC2 instances and set the minimum capacity to 2 and the maximum capacity to 4. Deploy 2 instances in Availability Zone A and 2 instances in Availability Zone B.
d. Create an Auto Scaling group of EC2 instances and set the minimum capacity to 2 and the maximum capacity to 6. Use 2 Availability Zones and deploy 1 instance for each AZ.

Question 10: A company has a hybrid cloud architecture that connects their on-premises data center and cloud infrastructure in AWS. They require a durable storage backup for their corporate documents stored on-premises and a local cache that provides low latency access to their recently accessed data to reduce data egress charges. The documents must be stored to and retrieved from AWS via the Server Message Block (SMB) protocol. These files must immediately be accessible within minutes for six months and archived for another decade to meet the data compliance.

Which of the following is the best and most cost-effective approach to implement in this scenario?

a. Use AWS Snowmobile to migrate all of the files from the on-premises network. Upload the documents to an S3 bucket and set up a lifecycle policy to move the data into Glacier for archival.
b. Establish a Direct Connect connection to integrate your on-premises network to your VPC. Upload the documents on Amazon EBS Volumes and use a lifecycle policy to automatically move the EBS snapshots to an S3 bucket, and then later to Glacier for archival.
c. Launch a new tape gateway that connects to your on-premises data center using AWS Storage Gateway. Upload the documents to the tape gateway and set up a lifecycle policy to move the data into Glacier for archival.
d. Launch a new file gateway that connects to your on-premises data center using AWS Storage Gateway. Upload the documents to the file gateway and set up a lifecycle policy to move the data into Glacier for data archival.

Question 11: Question 33: Skipped

There was an incident in your production environment where the user data stored in the S3 bucket has been accidentally deleted by one of the Junior DevOps Engineers. The issue was escalated to your manager and after a few days, you were instructed to improve the security and protection of your AWS resources.

What combination of the following options will protect the S3 objects in your bucket from both accidental deletion and overwriting? (Select TWO.)

a. **Enable Multi-Factor Authentication Delete**
b. Enable Amazon S3 Intelligent-Tiering
c. Disallow S3 Delete using an IAM bucket policy
d. Enable Versioning
e. Provide access to S3 data strictly through pre-signed URL only

Question 12: A Forex trading platform, which frequently processes and stores global financial data every minute, is hosted in your on-premises data center and uses an Oracle database. Due to a recent cooling problem in their data center, the company urgently needs to migrate their infrastructure to AWS to improve the performance of their applications. As the Solutions Architect, you are responsible for ensuring that the database is properly migrated and should remain available in case of database server failure in the future.

Which of the following is the most suitable solution to meet the requirement?

a. **Create an Oracle database in RDS with Multi-AZ deployments.**
b. Launch an Oracle Real Application Clusters (RAC) in RDS.
c. Convert the database schema using the AWS Schema Conversion Tool and AWS Database Migration Service. Migrate the Oracle database to a non-cluster Amazon Aurora with a single instance.
d. Launch an Oracle database instance in RDS with Recovery Manager (RMAN) enabled.

Question 13: An online cryptocurrency exchange platform is hosted in AWS which uses ECS Cluster and RDS in Multi-AZ Deployments configuration. The application is heavily using the RDS instance to process complex read and write database operations. To maintain the reliability, availability, and performance of your systems, you have to closely monitor how the different processes or threads on a DB instance use the CPU, including the percentage of the CPU bandwidth and total memory consumed by each process.

Which of the following is the most suitable solution to properly monitor your database?

a. Create a script that collects and publishes custom metrics to CloudWatch, which tracks the real-time CPU Utilization of the RDS instance, and then set up a custom CloudWatch dashboard to view the metrics.
b. Use Amazon CloudWatch to monitor the CPU Utilization of your database.
c. Check the CPU% and MEM% metrics which are readily available in the Amazon RDS console that shows the percentage of the CPU bandwidth and total memory consumed by each database process of your RDS instance.
d. **Enable Enhanced Monitoring in RDS.**

Question 14: A retail website has intermittent, sporadic, and unpredictable transactional workloads throughout the day that are hard to predict. The website is currently hosted on-premises and is slated to be migrated to AWS. A new relational database is needed that auto scales capacity to meet the needs of the application's peak load and scales back down when the surge of activity is over.

Which of the following options is the MOST cost-effective and suitable database setup in this scenario?

a. **Launch an Amazon Aurora Serverless DB cluster then set the minimum and maximum capacity for the cluster.**
b. Launch an Amazon Aurora Provisioned DB cluster with burstable performance DB instance class types.
c. Launch an Amazon Redshift data warehouse cluster with Concurrency Scaling.
d. Launch a DynamoDB Global table with Auto Scaling enabled.

Question 15: An application consists of multiple EC2 instances in private subnets in different availability zones. The application uses a single NAT Gateway for downloading software patches from the Internet to the instances. There is a requirement to protect the application from a single point of failure when the NAT Gateway encounters a failure or if its availability zone goes down.

How should the Solutions Architect redesign the architecture to be more highly available and cost-effective

a. Create a NAT Gateway in each availability zone. Configure the route table in each public subnet to ensure that instances use the NAT Gateway in the same availability zone.
b. Create two NAT Gateways in each availability zone. Configure the route table in each public subnet to ensure that instances use the NAT Gateway in the same availability zone.
c. Create three NAT Gateways in each availability zone. Configure the route table in each private subnet to ensure that instances use the NAT Gateway in the same availability zone.
d. **Create a NAT Gateway in each availability zone. Configure the route table in each private subnet to ensure that instances use the NAT Gateway in the same availability zone**

Question 16: A company plans to migrate its on-premises workload to AWS. The current architecture is composed of a Microsoft SharePoint server that uses a Windows shared file storage. The Solutions Architect needs to use a cloud storage solution that is highly available and can be integrated with Active Directory for access control and authentication. Which of the following options can satisfy the given requirement?

a. Create a Network File System (NFS) file share using AWS Storage Gateway.
b. Create a file system using Amazon EFS and join it to an Active Directory domain.
c. Create a file system using Amazon FSx for Windows File Server and join it to an Active Directory domain in AWS.
d. Launch an Amazon EC2 Windows Server to mount a new S3 bucket as a file volume.

Question 17: A multi-tiered application hosted in your on-premises data center is scheduled to be migrated to AWS. The application has a message broker service which uses industry standard messaging APIs and protocols that must be migrated as well, without rewriting the messaging code in your application.

Which of the following is the most suitable service that you should use to move your messaging service to AWS?

a. Amazon SWF
b. Amazon SQS
c. Amazon MQ
d. Amazon SNS

Question 18: A company plans to host a web application in an Auto Scaling group of Amazon EC2 instances. The application will be used globally by users to upload and store several types of files. Based on user trends, files that are older than 2 years must be stored in a different storage class. The Solutions Architect of the company needs to create a cost-effective and scalable solution to store the old files yet still provide durability and high availability.

Which of the following approaches can be used to fulfill this requirement? (Select TWO.)

a. Use Amazon S3 and create a lifecycle policy that will move the objects to Amazon S3 Standard-IA after 2 years.
b. Use Amazon EBS volumes to store the files. Configure the Amazon Data Lifecycle Manager (DLM) to schedule snapshots of the volumes after 2 years.
c. Use Amazon S3 and create a lifecycle policy that will move the objects to Amazon S3 Glacier after 2 years.
d. Use Amazon EFS and create a lifecycle policy that will move the objects to Amazon EFS-IA after 2 years.
e. Use a RAID 0 storage configuration that strips multiple Amazon EBS volumes together to store the files. Configure the Amazon Data Lifecycle Manager (DLM) to schedule snapshots of the volumes after 2 years.

Question 19: A company hosts multiple applications in their VPC. While monitoring the system, they noticed that multiple port scans are coming in from a specific IP address block that is trying to connect to several AWS resources inside their VPC. The internal security team has requested that all offending IP addresses be denied for the next 24 hours for security purposes. Which of the following is the best method to quickly and temporarily deny access from the specified IP addresses?

a. Add a rule in the Security Group of the EC2 instances to deny access from the IP Address block.
b. Create a policy in IAM to deny access from the IP Address block.
c. Configure the firewall in the operating system of the EC2 instances to deny access from the IP address block.
d. Modify the Network Access Control List associated with all public subnets in the VPC to deny access from the IP Address block.

Question 20: An online shopping platform is hosted on an Auto Scaling group of Spot EC2 instances and uses Amazon Aurora PostgreSQL as its database. There is a requirement to optimize your database workloads in your cluster where you have to direct the write operations of the production traffic to your high-capacity instances and point the reporting queries sent by your internal staff to the low-capacity instances.

Which is the most suitable configuration for your application as well as your Aurora database cluster to achieve this requirement?

a. Configure your application to use the reader endpoint for both production traffic and reporting queries, which will enable your Aurora database to automatically perform load-balancing among all the Aurora Replicas.
b. Do nothing since by default, Aurora will automatically direct the production traffic to your high-capacity instances and the reporting queries to your low-capacity instances.
c. Create a custom endpoint in Aurora based on the specified criteria for the production traffic and another custom endpoint to handle the reporting queries.
d. In your application, use the instance endpoint of your Aurora database to handle the incoming production traffic and use the cluster endpoint to handle reporting queries.

Question 21: A Solutions Architect needs to set up a relational database and come up with a disaster recovery plan to mitigate multi-region failure. The solution requires a Recovery Point Objective (RPO) of 1 second and a Recovery Time Objective (RTO) of less than 1 minute. Which of the following AWS services can fulfill this requirement?

a. Amazon Aurora Global Database
b. Amazon DynamoDB global tables
c. Amazon RDS for PostgreSQL with cross-region read replicas
d. AWS Global Accelerator