DUMPSQUEEN

AWS Certified Solutions Architect - Associate (SAA-C03)

Amazon AWS SAA-C03

Version Demo

Total Demo Questions: 20

Total Premium Questions: 409

Buy Premium PDF

https://dumpsqueen.com

support@dumpsqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Exam Pool A	113
Topic 2, Exam Pool B	86
Topic 3, Exam Pool C	210
Total	409

QUESTION NO: 1

A solutions architect is developing a multiple-subnet VPC architecture. The solution will consist of six subnets in two Availability Zones. The subnets are defined as public, private and dedicated for databases. Only the Amazon EC2 instances running in the private subnets should be able to access a database.

Which solution meets these requirements?

A. Create a now route table that excludes the route to the public subnets' CIDR blocks. Associate the route table to the database subnets.

B. Create a security group that denies ingress from the security group used by instances in the public subnets. Attach the security group to an Amazon RDS DB instance.

C. Create a security group that allows ingress from the security group used by instances in the private subnets. Attach the security group to an Amazon RDS DB instance.

D. Create a new peering connection between the public subnets and the private subnets. Create a different peering connection between the private subnets and the database subnets.

ANSWER: C

Explanation:

Security groups are stateful. All inbound traffic is blocked by default. If you create an inbound rule allowing traffic in, that traffic is automatically allowed back out again. You cannot block specific IP address using Security groups (instead use Network Access Control Lists).

"You can specify allow rules, but not deny rules." "When you first create a security group, it has no inbound rules. Therefore, no inbound traffic originating from another host to your instance is allowed until you add inbound rules to the security group." Source: https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html#VPCSecurityGroups

QUESTION NO: 2

A company is designing a cloud communications platform that is driven by APIs. The application is hosted on Amazon EC2 instances behind a Network Load Balancer (NLB). The company uses Amazon API Gateway to provide external users with access to the application through APIs. The company wants to protect the platform against web exploits like SQL injection and also wants to detect and mitigate large, sophisticated DDoS attacks.

Which combination of solutions provides the MOST protection? (Select TWO.)

A. Use AWS WAF to protect the NLB.

B. Use AWS Shield Advanced with the NLB.

C. Use AWS WAF to protect Amazon API Gateway.

D. Use Amazon GuardDuty with AWS Shield Standard.

E. Use AWS Shield Standard with Amazon API Gateway.

ANSWER: B C

Explanation:

AWS Shield Advanced provides expanded DDoS attack protection for your Amazon EC2 instances, Elastic Load Balancing load balancers, CloudFront distributions, Route 53 hosted zones, and AWS Global Accelerator standard accelerators.

AWS WAF is a web application firewall that lets you monitor the HTTP and HTTPS requests that are forwarded to your protected web application resources. You can protect the following resource types:

Amazon CloudFront distribution

Amazon API Gateway REST API

Application Load Balancer

AWS AppSync GraphQL API

Amazon Cognito user pool

https://docs.aws.amazon.com/waf/latest/developerguide/what-is-aws-waf.html

QUESTION NO: 3

A company's compliance team needs to move its file shares to AWS. The shares run on a Windows Server SMB file share. A self-managed on-premises Active Directory controls access to the files and folders.

The company wants to use Amazon FSx for Windows File Server as part of the solution. The company must ensure that the on-premises Active Directory groups restrict access to the FSx for Windows File Server SMB compliance shares, folders, and files after the move to AWS. The company has created an FSx for Windows File Server file system.

Which solution will meet these requirements?

A. Create an Active Directory Connector to connect to the Active Directory. Map the Active Directory groups to IAM groups to restrict access.

B. Assign a tag with a Restrict tag key and a Compliance tag value. Map the Active Directory groups to IAM groups to restrict access.

C. Create an IAM service-linked role that is linked directly to FSx for Windows File Server to restrict access.

D. Join the file system to the Active Directory to restrict access.

ANSWER: D

Explanation:

Joining the FSx for Windows File Server file system to the on-premises Active Directory will allow the company to use the existing Active Directory groups to restrict access to the file shares, folders, and files after the move to AWS. This option allows the company to continue using their existing access controls and management structure, making the transition to AWS more seamless.

QUESTION NO: 4

A company hosts a three-tier web application that includes a PostgreSQL database The database stores the metadata from documents The company searches the metadata for key terms to retrieve documents that the company reviews in a report each month The documents are stored in Amazon S3 The documents are usually written only once, but they are updated frequency The reporting process takes a few hours with the use of relational queries The reporting process must not affect any document modifications or the addition of new documents.

What are the MOST operationally efficient solutions that meet these requirements? (Select TWO)

A. Set up a new Amazon DocumentDB (with MongoDB compatibility) cluster that includes a read replica Scale the read replica to generate the reports.

B. Set up a new Amazon RDS for PostgreSQL Reserved Instance and an On-Demand read replica Scale the read replica to generate the reports

C. Set up a new Amazon Aurora PostgreSQL DB cluster that includes a Reserved Instance and an Aurora Replica issue queries to the Aurora Replica to generate the reports.

D. Set up a new Amazon RDS for PostgreSQL Multi-AZ Reserved Instance Configure the reporting module to query the secondary RDS node so that the reporting module does not affect the primary node

E. Set up a new Amazon DynamoDB table to store the documents Use a fixed write capacity to support new document entries Automatically scale the read capacity to support the reports

ANSWER: B C

QUESTION NO: 5

A solutions architect is implementing a document review application using an Amazon S3 bucket for storage. The solution must prevent accidental deletion of the documents and ensure that all versions of the documents are available. Users must be able to download, modify, and upload documents.

Which combination of actions should be taken to meet these requirements? (Choose two.)

A. Enable a read-only bucket ACL.

B. Enable versioning on the bucket.

C. Attach an IAM policy to the bucket.

D. Enable MFA Delete on the bucket.

E. Encrypt the bucket using AWS KMS.

ANSWER: B D

QUESTION NO: 6

A company uses a 100 GB Amazon RDS for Microsoft SQL Server Single-AZ DB instance in the us-east-1 Region to store customer transactions. The company needs high availability and automate recovery for the DB instance.

The company must also run reports on the RDS database several times a year. The report process causes transactions to take longer than usual to post to the customer‘ accounts.

Which combination of steps will meet these requirements? (Select TWO.)

A. Modify the DB instance from a Single-AZ DB instance to a Multi-AZ deployment.

B. Take a snapshot of the current DB instance. Restore the snapshot to a new RDS deployment in another Availability Zone.

C. Create a read replica of the DB instance in a different Availability Zone. Point All requests for reports to the read replica.

D. Migrate the database to RDS Custom.

E. Use RDS Proxy to limit reporting requests to the maintenance window.

ANSWER: A C

Explanation:

https://medium.com/awesome-cloud/aws-difference-between-multi-az-and-read-replicas-in-amazon-rds-60fe848ef53a

QUESTION NO: 7

A company wants to manage Amazon Machine Images (AMIs). The company currently copies AMIs to the same AWS Region where the AMIs were created. The company needs to design an application that captures AWS API calls and sends alerts whenever the Amazon EC2 CreateImage API operation is called within the company's account.

Which solution will meet these requirements with the LEAST operational overhead?

A. Create an AWS Lambda function to query AWS CloudTrail logs and to send an alert when a CreateImage API call is detected.

B. Configure AWS CloudTrail with an Amazon Simple Notification Service (Amazon SNS) notification that occurs when updated logs are sent to Amazon S3. Use Amazon Athena to create a new table and to query on CreateImage when an API call is detected.

C. Create an Amazon EventBridge (Amazon CloudWatch Events) rule for the CreateImage API call. Configure the target as an Amazon Simple Notification Service (Amazon SNS) topic to send an alert when a CreateImage API call is detected.

D. Configure an Amazon Simple Queue Service (Amazon SQS) FIFO queue as a target for AWS CloudTrail logs. Create an AWS Lambda function to send an alert to an Amazon Simple Notification Service (Amazon SNS) topic when a CreateImage API call is detected.

ANSWER: C

Explanation:

https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/monitor-ami-events.html#:~:text=For%20example%2C%20you%20can%20create%20an%20EventBridge%20rule%20that%20detects%20when%20the%20AMI%20creation%20process%20has%20completed%20and%20then%20invokes%20an%20Amazon%20SNS%20topic%20to%20send%20an%20email%20notification%20to%20you.

QUESTION NO: 8

A company is migrating an application from on-premises servers to Amazon EC2 instances. As part of the migration design requirements, a solutions architect must implement infrastructure metric alarms. The company does not need to take action if CPU utilization increases to more than 50% for a short burst of time. However, if the CPU utilization increases to more than 50% and read IOPS on the disk are high at the same time, the company needs to act as soon as possible. The solutions architect also must reduce false alarms.

What should the solutions architect do to meet these requirements?

A. Create Amazon CloudWatch composite alarms where possible.

B. Create Amazon CloudWatch dashboards to visualize the metrics and react to issues quickly.

C. Create Amazon CloudWatch Synthetics canaries to monitor the application and raise an alarm.

D. Create single Amazon CloudWatch metric alarms with multiple metric thresholds where possible.

ANSWER: A

QUESTION NO: 9

A company's application runs on AWS. The application stores large documents in an Amazon S3 bucket that uses the S3 Standard-infrequent Access (S3 Standerd-IA) storage class. The company will continue paying to store the data but wants to save on its total S3 costs. The company wants authorized external users to have the ability to access the documents in milliseconds.

Which solution will meet these requirements MOST cost-effectively?

A. Configure the S3 bucket to be a Requester Pays bucket

B. Change the storage tier to S3 Standard for all existing and future objects.

C. Turn on S3 Transfer Acceleration tor the S3 Docket

D. Use Amazon CloudFront to handle all the requests to the S3 bucket

ANSWER: D

QUESTION NO: 10

A company is moving its on-premises Oracle database to Amazon Aurora PostgreSQL. The database has several applications that write to the same tables. The applications need to be migrated one by one with a month in between each migration. Management has expressed concerns that the database has a high number of reads and writes. The data must be kept in sync across both databases throughout the migration.

What should a solutions architect recommend?

A. Use AWS DataSync for the initial migration. Use AWS Database Migration Service (AWS DMS) to create a change data capture (CDC) replication task and a table mapping to select all tables.

B. Use AWS DataSync for the initial migration. Use AWS Database Migration Service (AWS DMS) to create a full load plus change data capture (CDC) replication task and a table mapping to select all tables.

C. Use the AWS Schema Conversion Tool with AWS Database Migration Service (AWS DMS) using a memory optimized replication instance. Create a full load plus change data capture (CDC) replication task and a table mapping to select all tables.

D. Use the AWS Schema Conversion Tool with AWS Database Migration Service (AWS DMS) using a compute optimized replication instance. Create a full load plus change data capture (CDC) replication task and a table mapping to select the largest tables.

ANSWER: C

QUESTION NO: 11

A company wants to reduce the cost of its existing three-tier web architecture. The web, application, and database servers are running on Amazon EC2 instances for the development, test, and production environments. The EC2 instances average 30% CPU utilization during peak hours and 10% CPU utilization during non-peak hours.

The production EC2 instances run 24 hours a day. The development and test EC2 instances run for at least 8 hours each day. The company plans to implement automation to stop the development and test EC2 instances when they are not in use.

Which EC2 instance purchasing solution will meet the company's requirements MOST cost-effectively?

A. Use Spot Instances for the production EC2 instances. Use Reserved Instances for the development and test EC2 instances.

B. Use Reserved Instances for the production EC2 instances. Use On-Demand Instances for the development and test EC2 instances.

C. Use Spot blocks for the production EC2 instances. Use Reserved Instances for the development and test EC2 instances.

D. Use On-Demand Instances for the production EC2 instances. Use Spot blocks for the development and test EC2 instances.

ANSWER: B

QUESTION NO: 12

A solutions architect needs to securely store a database user name and password that an application uses to access an Amazon RDS DB instance. The application that accesses the database runs on an Amazon EC2 instance. The solutions architect wants to create a secure parameter in AWS Systems Manager Parameter Store.

What should the solutions architect do to meet this requirement?

A. Create an IAM role that has read access to the Parameter Store parameter. Allow Decrypt access to an AWS Key Management Service (AWS KMS) key that is used to encrypt the parameter. Assign this IAM role to the EC2 instance.

B. Create an IAM policy that allows read access to the Parameter Store parameter. Allow Decrypt access to an AWS Key Management Service (AWS KMS) key that is used to encrypt the parameter. Assign this IAM policy to the EC2 instance.

C. Create an IAM trust relationship between the Parameter Store parameter and the EC2 instance. Specify Amazon RDS as a principal in the trust policy.

D. Create an IAM trust relationship between the DB instance and the EC2 instance. Specify Systems Manager as a principal in the trust policy.

ANSWER: B

Explanation:

https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_aws-services-that-work-with-iam.html

QUESTION NO: 13

A hospital is designing a new application that gathers symptoms from patients. The hospital has decided to use Amazon Simple Queue Service (Amazon SOS) and Amazon Simple Notification Service (Amazon SNS) in the architecture.

A solutions architect is reviewing the infrastructure design Data must be encrypted at test and in transit. Only authorized personnel of the hospital should be able to access the data.

Which combination of steps should the solutions architect take to meet these requirements? (Select TWO.)

A. Turn on server-side encryption on the SQS components Update tie default key policy to restrict key usage to a set of authorized principals.

B. Turn on server-side encryption on the SNS components by using an AWS Key Management Service (AWS KMS) customer managed key Apply a key policy to restrict key usage to a set of authorized principals.

C. Turn on encryption on the SNS components Update the default key policy to restrict key usage to a set of authorized principals. Set a condition in the topic pokey to allow only encrypted connections over TLS.

D. Turn on server-side encryption on the SOS components by using an AWS Key Management Service (AWS KMS) customer managed key Apply a key pokey to restrict key usage to a set of authorized principals. Set a condition in the queue pokey to allow only encrypted connections over TLS.

E. Turn on server-side encryption on the SOS components by using an AWS Key Management Service (AWS KMS) customer managed key. Apply an IAM pokey to restrict key usage to a set of authorized principals. Set a condition in the queue pokey to allow only encrypted connections over TLS

ANSWER: B D

QUESTION NO: 14

A solutions architect needs to help a company optimize the cost of running an application on AWS. The application will use Amazon EC2 instances, AWS Fargate, and AWS Lambda for compute within the architecture.

The EC2 instances will run the data ingestion layer of the application. EC2 usage will be sporadic and unpredictable. Workloads that run on EC2 instances can be interrupted at any time. The application front end will run on Fargate, and Lambda will serve the API layer. The front-end utilization and API layer utilization will be predictable over the course of the next year.

Which combination of purchasing options will provide the MOST cost-effective solution for hosting this application? (Choose two.)

A. Use Spot Instances for the data ingestion layer

B. Use On-Demand Instances for the data ingestion layer

C. Purchase a 1-year Compute Savings Plan for the front end and API layer.

D. Purchase 1-year All Upfront Reserved instances for the data ingestion layer.

E. Purchase a 1-year EC2 instance Savings Plan for the front end and API layer.

ANSWER: A C

QUESTION NO: 15

A company needs to configure a real-time data ingestion architecture for its application. The company needs an API, a process that transforms data as the data is streamed, and a storage solution for the data.

Which solution will meet these requirements with the LEAST operational overhead?

A. Deploy an Amazon EC2 instance to host an API that sends data to an Amazon Kinesis data stream. Create an Amazon Kinesis Data Firehose delivery stream that uses the Kinesis data stream as a data source. Use AWS Lambda functions to transform the data. Use the Kinesis Data Firehose delivery stream to send the data to Amazon S3.

B. Deploy an Amazon EC2 instance to host an API that sends data to AWS Glue. Stop source/destination checking on the EC2 instance. Use AWS Glue to transform the data and to send the data to Amazon S3.

C. Configure an Amazon API Gateway API to send data to an Amazon Kinesis data stream. Create an Amazon Kinesis Data Firehose delivery stream that uses the Kinesis data stream as a data source. Use AWS Lambda functions to transform the data. Use the Kinesis Data Firehose delivery stream to send the data to Amazon S3.

D. Configure an Amazon API Gateway API to send data to AWS Glue. Use AWS Lambda functions to transform the data. Use AWS Glue to send the data to Amazon S3.

ANSWER: C

QUESTION NO: 16

An application development team is designing a microservice that will convert large images to smaller, compressed images. When a user uploads an image through the web interface, the microservice should store the image in an Amazon S3 bucket, process and compress the image with an AWS Lambda function, and store the image in its compressed form in a different S3 bucket.

A solutions architect needs to design a solution that uses durable, stateless components to process the images automatically.

Which combination of actions will meet these requirements? (Choose two.)

A. Create an Amazon Simple Queue Service (Amazon SQS) queue Configure the S3 bucket to send a notification to the SQS queue when an image is uploaded to the S3 bucket

B. Configure the Lambda function to use the Amazon Simple Queue Service (Amazon SQS) queue as the invocation source When the SQS message is successfully processed, delete the message in the queue

C. Configure the Lambda function to monitor the S3 bucket for new uploads When an uploaded image is detected write the file name to a text file in memory and use the text file to keep track of the images that were processed

D. Launch an Amazon EC2 instance to monitor an Amazon Simple Queue Service (Amazon SQS) queue When items are added to the queue log the file name in a text file on the EC2 instance and invoke the Lambda function

E. Configure an Amazon EventBridge (Amazon CloudWatch Events) event to monitor the S3 bucket When an image is uploaded. send an alert to an Amazon Simple Notification Service (Amazon SNS) topic with the application owner's email address for further processing

ANSWER: A B

Explanation:

Amazon SQS is a fully managed message queuing service that enables you to decouple and scale microservices, distributed systems, and serverless applications. SQS eliminates the complexity and overhead associated with managing and operating-message oriented middleware, and empowers developers to focus on differentiating work. When new images are uploaded to the S3 bucket, SQS will trigger the Lambda function to process the image and compress it. Once the image is processed, the SQS message is deleted, ensuring that the Lambda function is stateless and durable.

QUESTION NO: 17

A company hosts an application on AWS Lambda functions mat are invoked by an Amazon API Gateway API The Lambda functions save customer data to an Amazon Aurora MySQL database Whenever the company upgrades the database, the Lambda functions fail to establish database connections until the upgrade is complete The result is that customer data Is not recorded for some of the event

A solutions architect needs to design a solution that stores customer data that is created during database upgrades

Which solution will meet these requirements?

A. Provision an Amazon RDS proxy to sit between the Lambda functions and the database Configure the Lambda functions to connect to the RDS proxy

B. Increase the run time of me Lambda functions to the maximum Create a retry mechanism in the code that stores the customer data in the database

C. Persist the customer data to Lambda local storage. Configure new Lambda functions to scan the local storage to save the customer data to the database.

D. Store the customer data m an Amazon Simple Queue Service (Amazon SOS) FIFO queue Create a new Lambda function that polls the queue and stores the customer data in the database

ANSWER: D

Explanation:

https://www.learnaws.org/2020/12/13/aws-rds-proxy-deep-dive/

RDS proxy can improve application availability in such a situation by waiting for the new database instance to be functional and maintaining any requests received from the application during this time. The end result is that the application is more resilient to issues with the underlying database.

This will enable solution to hold data till the time DB comes back to normal. RDS proxy is to optimally utilize the connection between Lambda and DB. Lambda can open multiple connection concurrently which can be taxing on DB compute resources, hence RDS proxy was introduced to manage and leverage these connections efficiently.

QUESTION NO: 18

A company has deployed a Java Spring Boot application as a pod that runs on Amazon Elastic Kubernetes Service (Amazon EKS) in private subnets. The application needs to write data to an Amazon DynamoDB table. A solutions architect must ensure that the application can interact with the DynamoDB table without exposing traffic to the internet.

Which combination of steps should the solutions architect take to accomplish this goal? (Choose two.)

A. Attach an IAM role that has sufficient privileges to the EKS pod.

B. Attach an IAM user that has sufficient privileges to the EKS pod.

C. Allow outbound connectivity to the DynamoDB table through the private subnets' network ACLs.

D. Create a VPC endpoint for DynamoDB.

E. Embed the access keys in the Java Spring Boot code.

ANSWER: A D

Explanation:

https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/vpc-endpoints-dynamodb.html

https://aws.amazon.com/about-aws/whats-new/2019/09/amazon-eks-adds-support-to-assign-iam-permissions-to-kubernetes-service-accounts/

QUESTION NO: 19

A company has a data ingestion workflow that consists the following:

· An Amazon Simple Notification Service (Amazon SNS) topic for notifications about new data deliveries

· An AWS Lambda function to process the data and record metadata

The company observes that the ingestion workflow fails occasionally because of network connectivity issues. When such a failure occurs, the Lambda function does not ingest the corresponding data unless the company manually reruns the job.

Which combination of actions should a solutions architect take to ensure that the Lambda function ingests all data in the future? (Select TWO.)

A. Configure the Lambda function In multiple Availability Zones.

B. Create an Amazon Simple Queue Service (Amazon SQS) queue, and subscribe It to me SNS topic.

C. Increase the CPU and memory that are allocated to the Lambda function.

D. Increase provisioned throughput for the Lambda function.

E. Modify the Lambda function to read from an Amazon Simple Queue Service (Amazon SQS) queue

ANSWER: B E

QUESTION NO: 20

A company runs its two-tier ecommerce website on AWS. The web tier consists of a load balancer that sends traffic to Amazon EC2 instances. The database tier uses an Amazon RDS DB instance. The EC2 instances and the RDS DB instance should not be exposed to the public internet. The EC2 instances require internet access to complete payment processing of orders through a third-party web service. The application must be highly available.

Which combination of configuration options will meet these requirements? (Choose two.)

A. Use an Auto Scaling group to launch the EC2 instances in private subnets. Deploy an RDS Multi-AZ DB instance in private subnets.

B. Configure a VPC with two private subnets and two NAT gateways across two Availability Zones. Deploy an Application Load Balancer in the private subnets.

C. Use an Auto Scaling group to launch the EC2 instances in public subnets across two Availability Zones. Deploy an RDS Multi-AZ DB instance in private subnets.

D. Configure a VPC with one public subnet, one private subnet, and two NAT gateways across two Availability Zones. Deploy an Application Load Balancer in the public subnet.

E. Configure a VPC with two public subnets, two private subnets, and two NAT gateways across two Availability Zones. Deploy an Application Load Balancer in the public subnets.

ANSWER: A E

Explanation:

Before you begin: Decide which two Availability Zones you will use for your EC2 instances. Configure your virtual private cloud (VPC) with at least one public subnet in each of these Availability Zones. These public subnets are used to configure the load balancer. You can launch your EC2 instances in other subnets of these Availability Zones instead.