Braindump2go Guarantee All Exams 100% Pass One Time!

- Vendor: Amazon
- Exam Code: AWS-Developer-Associate
- Exam Name: AWS Certified Developer - Associate (DVA-C01)
- New Updated Questions from Braindump2go (Updated in June/2020)

Visit Braindump2go and Download Full Version AWS-Developer-Associate Exam Dumps

QUESTION 556
A software company needs to make sure user-uploaded documents are securely stored in Amazon S3. The documents must be encrypted at rest in Amazon S3. The company does not want to manage the security infrastructure in-house, but the company still needs extra protection to ensure it has control over its encryption keys due to industry regulations.
Which encryption strategy should a Developer use to meet these requirements?

A. Server-side encryption with Amazon S3 managed keys (SSE-S3)
B. Server-side encryption with customer-provided encryption keys (SSE-C)
C. Server-side encryption with AWS KMS managed keys (SSE-KMS)
D. Client-side encryption

Answer: A
Explanation:
https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingServerSideEncryption.html

QUESTION 557
A Developer uses Amazon S3 buckets for static website hosting. The Developer creates one S3 bucket for the code and another S3 bucket for the assets, such as image and video files. Access is denied when a user attempts to access the assets bucket from the code bucket, with the website application showing a 403 error.
How should the Developer solve this issue?

A. Create an IAM role and apply it to the assets bucket for the code bucket to be granted access.
B. Edit the bucket policy of the assets bucket to open access to all principals.
C. Edit the cross-origin resource sharing (CORS) configuration of the assets bucket to allow any origin to access the assets.
D. Change the code bucket to use AWS Lambda functions instead of static website hosting.

Answer: B
Explanation:
https://docs.aws.amazon.com/AmazonS3/latest/user-guide/static-website-hosting.html

QUESTION 558
A Developer migrated a web application to AWS. As part of the migration, the Developer implemented an automated continuous integration/continuous improvement (CI/CD) process using a blue/green deployment. The deployment provisions new Amazon EC2 instances in an Auto Scaling group behind a new Application Load Balancer. After the migration was completed, the Developer began receiving complaints from users getting booted out of the system. The system also requires users to log in after every new deployment.

AWS-Developer-Associate Exam Dumps AWS-Developer-Associate Exam Questions
AWS-Developer-Associate PDF Dumps AWS-Developer-Associate VCE Dumps
https://www.braindump2go.com/aws-developer-associate.html

How can these issues be resolved?

A. Use rolling updates instead of a blue/green deployment
B. Externalize the user sessions to Amazon ElastiCache
C. Turn on sticky sessions in the Application Load Balancer
D. Use multicast to replicate session information

Answer: C

QUESTION 559
A Developer wants to insert a record into an Amazon DynamoDB table as soon as a new file is added to an Amazon S3 bucket.
Which set of steps would be necessary to achieve this?

A. Create an event with Amazon CloudWatch Events that will monitor the S3 bucket and then insert the records into DynamoDB.
B. Configure an S3 event to invoke a Lambda function that inserts records into DynamoDB.
C. Create a Lambda function that will poll the S3 bucket and then insert the records into DynamoDB.
D. Create a cron job that will run at a scheduled time and insert the records into DynamoDB.

Answer: B

QUESTION 560
A Developer is building an application that needs to store data in Amazon S3. Management requires that the data be encrypted before it is sent to Amazon S3 for storage. The encryption keys need to be managed by the Security team.
Which approach should the Developer take to meet these requirements?

A. Implement server-side encryption using customer-provided encryption keys (SSE-C).
B. Implement server-side encryption by using a client-side master key.
C. Implement client-side encryption using an AWS KMS managed customer master key (CMK).
D. Implement client-side encryption using Amazon S3 managed keys.

Answer: D
Explanation:
https://aws.amazon.com/s3/faqs/

QUESTION 561
A Developer has written an Amazon Kinesis Data Streams application. As usage grows and traffic increases over time, the application is regularly receiving ProvisionedThroughputExceededException error messages.
Which steps should the Developer take to resolve the error? (Choose two.)

A. Use Auto Scaling to scale the stream for better performance
B. Increase the delay between the GetRecords call and the PutRecords call
C. Increase the number of shards in the data stream
D. Specify a shard iterator using the ShardIterator parameter
E. Implement exponential backoff on the GetRecords call and the PutRecords call

Answer: CD
Explanation:
https://docs.aws.amazon.com/streams/latest/dev/troubleshooting-consumers.html

QUESTION 562
A Developer is publishing critical log data to a log group in Amazon CloudWatch Logs, which was created 2 months ago. The Developer must encrypt the log data using an AWS KMS customer master key (CMK) so future data can be

encrypted to comply with the company's security policy.
How can the Developer meet this requirement?

A. Use the CloudWatch Logs console and enable the encrypt feature on the log group
B. Use the AWS CLI create-log-group command and specify the key Amazon Resource Name (ARN)
C. Use the KMS console and associate the CMK with the log group
D. Use the AWS CLI associate-kms-key command and specify the key Amazon Resource Name (ARN)

Answer: D
Explanation:
https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/encrypt-log-data-kms.html

QUESTION 563
A Developer has code running on Amazon EC2 instances that needs read-only access to an Amazon DynamoDB table.
What is the MOST secure approach the Developer should take to accomplish this task?

A. Create a user access key for each EC2 instance with read-only access to DynamoDB. Place the keys in the code. Redeploy the code as keys rotate.
B. Use an IAM role with an AmazonDynamoDBReadOnlyAccess policy applied to the EC2 instances.
C. Run all code with only AWS account root user access keys to ensure maximum access to services.
D. Use an IAM role with Administrator access applied to the EC2 instance.

Answer: D

QUESTION 564
A Developer decides to store highly secure data in Amazon S3 and wants to implement server-side encryption (SSE) with granular control of who can access the master key. Company policy requires that the master key be created, rotated, and disabled easily when needed, all for security reasons.
Which solution should be used to meet these requirements?

A. SSE with Amazon S3 managed keys (SSE-S3)
B. SSE with AWS KMS managed keys (SSE-KMS)
C. SSE with AWS Secrets Manager
D. SSE with customer-provided encryption keys

Answer: B
Explanation:
https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingKMSEncryption.html

QUESTION 565
A Developer is migrating an on-premises application to AWS. The application currently takes user uploads and saves them to a local directory on the server. All uploads must be saved and made immediately available to all instances in an Auto Scaling group.
Which approach will meet these requirements?

A. Use Amazon EBS and configure the application AMI to use a snapshot of the same EBS instance on boot.
B. Use Amazon S3 and rearchitect the application so all uploads are placed in S3.
C. Use instance storage and share it between instances launched from the same Amazon Machine Image (AMI).

D. Use Amazon EBS and file synchronization software to achieve eventual consistency among the Auto Scaling group.

Answer: C

QUESTION 566
A Developer implemented a static website hosted in Amazon S3 that makes web service requests hosted in Amazon API Gateway and AWS Lambda. The site is showing an error that reads:
"No `Access-Control-Allow-Origin' header is present on the requested resource. Origin `null' is therefore not allowed access."
What should the Developer do to resolve this issue?

A. Enable cross-origin resource sharing (CORS) on the S3 bucket.
B. Enable cross-origin resource sharing (CORS) for the method in API Gateway
C. Add the Access-Control-Request-Method header to the request
D. Add the Access-Control-Request-Headers header to the request

Answer: B
Explanation:
https://forums.aws.amazon.com/thread.jspa?threadID=252972

QUESTION 567
A Developer is writing an application in AWS Lambda. To simplify testing and deployments, the Developer needs the database connections string to be easily changed without modifying the Lambda code.
How can this requirement be met?

A. Store the connection string as a secret in AWS Secrets Manager.
B. Store the connection string in an IAM user account.
C. Store the connection string in AWS KMS.
D. Store the connection string as a Lambda layer.

Answer: C
Explanation:
https://aws.amazon.com/blogs/developer/net-core-configuration-provider-for-aws-systems-manager/