DVA-C01 Q&As

AWS Certified Developer - Associate (DVA-C01)

Pass Amazon DVA-C01 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/aws-certified-developer-associate.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Amazon Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

A company is running an application on AWS Elastic Beanstalk in a single-instance environment. The company\\'s deployments must avoid any downtime. Which deployment option will meet these requirements?

A. All at once

B. Rolling

C. Rolling with additional batch

D. Immutable

Correct Answer: D

Reference: https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/using-features.rolling-version-deploy.html

QUESTION 2

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 1AM 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.

Correct Answer: C

The Web Site code will run on the client machine (the browser). It is sad it will fetch the asset from the other bucket so there is some JS code. Bucket B is considered another origin so we have a CORS error here. It\\'s C.

It can\\'t be because there is no point in adding a bucket policy to allow all principles because we are accessing the file from the client machine not within aws

Note that CORS can result in 403 errors in some cases.

Example: https://medium.com/collaborne-engineering/403-cursed-by-cors-d1700cab754

https://docs.aws.amazon.com/AmazonS3/latest/dev/cors-troubleshooting.html

QUESTION 3

You run an ad-supported photo sharing website using S3 to serve photos to visitors of your site. At some point you find out that other sites have been linking to the photos on your site, causing loss to your business. What is an effective

method to mitigate this?

A. Store photos on an EBS volume of the web server

B. Remove public read access and use signed URLs with expiry dates.

C. Use CloudFront distributions for static content.

D. Block the IPs of the offending websites in Security Groups.

Correct Answer: B

https://aws.amazon.com/getting-started/projects/building-fast-session-caching-with-amazon- elasticache-for-redis/1/

QUESTION 4

A Developer is writing a mobile application that allows users to view images from an S3 bucket. The users must be able to log in with their Amazon login, as well as Facebook?and/or Google?accounts. How can the Developer provide this authentication functionality?

A. Use Amazon Cognito with web identity federation.

B. Use Amazon Cognito with SAML-based identity federation.

C. Use AWS IAM Access/Secret keys in the application code to allow Get* on the S3 bucket.

D. Use AWS STS AssumeRole in the application code and assume a role with Get* permissions on the S3 bucket.

Correct Answer: A

QUESTION 5

A company has deployed web servers on Amazon EC2 instances with Amazon Linux in the us-east-1 Region. The EC2 instances are backed by Amazon Elastic Block Store (Amazon EBS). A developer wants to ensure that all of these instances will provide encryption at rest by using an AWS Key Management Service (AWS KMS) key.

How can the developer enable encryption at rest on existing and new instances by using an AWS KMS key?

A. Use AWS Certificate Manager (ACM) to generate a TLS certificate. Store the private key in AWS KMS. Use AWS KMS on the instances to enable TLS encryption.

B. Manually enable EBS encryption with AWS KMS on running instances. Then enable EBS encryption by default for new instances.

C. Enable EBS encryption by default. Create snapshots from the running instances. Replace running instances with new instances from snapshots.

D. Export the AWS KMS key to the application. Encrypt all application data by using the exported key. Enable EBS encryption by default to encrypt all other data.

Correct Answer: C

Reference: https://aws.amazon.com/blogs/compute/must-know-best-practices-for-amazon-ebs-encryption/

DVA-C01 PDF Dumps DVA-C01 Practice Test DVA-C01 Study Guide