If you encrypt a bucket on S3, what type of encryption does AWS use?

- International Data Encryption Algorithm (IDEA).
- Data Encryption Standard (DES)
- Advanced Encryption Standard (AES) 128
- Advanced Encryption Standard (AES) 256

If you want to enable a user to download your private data directly from S3, you can insert a pre-signed URL into a web page before giving it to your user.



False

How does S3 determine which partition to use to store files?

- S3 automatically stores your files on a random partition
- The key name determines which partition the file is stored in
- By default, all files in the same bucket are stored on the same partition
- The bucket name determines which partition the file is stored in

Sorry!

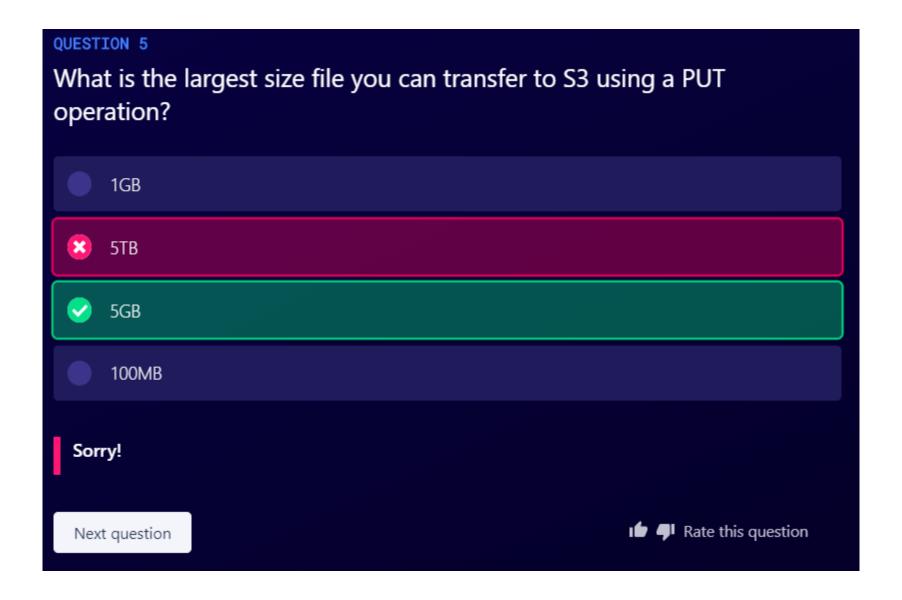
Which of the following options allows users to have secure access to private files located in S3?

Choose 3



Good work!

There are three options in the question which can be used to secure access to files stored in S3 and therefore can be considered correct. Signed URLs and Signed Cookies are different ways to ensure that users attempting access to files in an S3 bucket can be authorised. One method generates URLs and the other generates special cookies but they both require the creation of an application and policy to generate and control these items. An Origin Access Identity on the other hand, is a virtual user identity that is used to give the CloudFront distribution permission to fetch a private object from an S3 bucket. Public S3 buckets should never be used unless you are using the bucket to host a public website and therefore this is an incorrect option.



Your application is consistently reading and writing 100s of objects per second to S3 and your workload is steadily rising. What can you do to achieve the best performance from S3?



Do nothing, S3 can cope with a much higher read and write operation than is being experienced

- Add a hex hash suffix to the objects key name
- Configure an additional bucket and distribute the files evenly between the two buckets
- Configure a CloudFront CDN and use the S3 bucket as the origin

Sorry!

Correct Answer

Amazon S3 now provides increased performance to support at least 3,500 requests per second to add data and 5,500 requests per second to retrieve data. This negates the previous optimisation guidance for randomising your object key names to increase throughput

When you first create an S3 bucket, this bucket is publicly accessible by default. False Good work!

You are using S3 in AP-Northeast to host a static website in a bucket called "acloudguru". What would the new URL endpoint be?

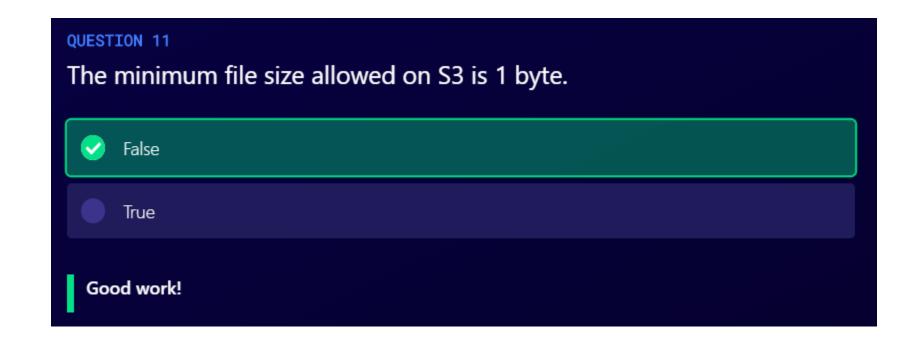
- http://acloudguru.s3-website-ap-northeast-1.amazonaws.com
- https://s3-ap-northeast-1.amazonaws.com/acloudguru/
- http://acloudguru.s3-website-ap-southeast-1.amazonaws.com
- http://www.acloudguru.s3-website-ap-northeast-1.amazonaws.com

Sorry!

You are hosting a static website in an S3 bucket that uses Javascript to reference assets in another S3 bucket. For some reason, these assets are not displaying when users browse to the site. What could be the problem?

- You need to open port 80 on the appropriate security group in which the S3 bucket is located.
- You haven't enabled Cross-origin Resource Sharing (CORS) on the bucket where the assets are stored.
- You cannot use one S3 bucket to reference another S3 bucket.
- Amazon S3 does not support Javascript.

QUESTION 10 What is the HTTP code you would see once you successfully place a file in an S3 bucket? 404 312 524 200 Good work!



Which feature of AWS can you use to configure S3 to allow web applications being hosted in one S3 bucket to access files in another S3 bucket?



CORS

Bucket Policy



Bucket ACL

QUESTION 13 Which of the following encryption methods are supported in S3? Choose 3 SSE-C SSE-S3 SSE-KMS SSE-AES Sorry!

