Home / Dashboard / My Courses / AWS Certified Security Specialty / CloudFront - Quiz / Report

← Back to the **Course**

Level: Advanced

AWS Certified Security Specialty

CloudFront - Quiz

Completed on **Sun, 27 Feb 2022**

1st
Attempt

0/5
Marks Obtained

0.00%
Your Score

0h 0m 3s
Time Taken

FAIL
Result

Domain wise Quiz Performance Report

Join us on Slack community

No.	Domain	Total Question	Correct	Incorrect	Unattempted
1	Other	5	0	0	0
Total	All Domains	5	0	0	0

Review the Answers

Filter By All Questions

Question 1

Unattempted

Domain: Other

Your company is planning to use an S3 bucket and a CloudFront distribution to distribute objects to users worldwide. They want to use their own domain name with the CloudFront distribution and ensure that the communication is secure. Which of the following steps need to be part of the implementation plan? (Select TWO.)

A. Change the Viewer protocol Policy to require HTTPS between viewers and CloudFront. right

B. Import an SSL certificate to ACM and use the certificate in the CloudFront distribution. right

C. Create a KMS CMK Key and use the key in the CloudFront distribution.

D. Apply CORS for the CloudFront distribution.

Explanation:

Answer – A and B

This is mentioned in the AWS Documentation.

· If you're using the domain name that CloudFront assigned to your distribution, such as d111111abcdef8.cloudfront.net, you change the Viewer Protocol Policy setting for one or more cache behaviors to require HTTPS communication. In that configuration, CloudFront provides the SSL/TLS certificate.

To change the value of Viewer Protocol Policy by using the CloudFront console, see the procedure later in this section.

· If you're using your own domain name, such as example.com, you need to change several CloudFront settings. You also need to use an SSL/TLS certificate provided by AWS Certificate Manager (ACM), import a certificate from a third-party certificate authority into ACM or the IAM certificate store.

Option C is incorrect since you need to use SSL certificates and not KMS keys.

Option D is incorrect since CORS is used for access between domains.

For more information on using CNAMEs and HTTPs, please visit the below URL

https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/using-https-viewers-to-cloudfront.html

https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/using-https-alternate-domain-names.html

Ask our Experts

View Queries

Question 2 Unattempted

Domain: Other

Your company is planning to use an S3 bucket and a CloudFront distribution to distribute objects to users worldwide. They want to ensure that users can only access the objects via the CloudFront URLs. Which of the following implementation steps need to be carried out? Choose 2 answers from the options given below.

A. Create an IAM User with the desired Access Keys.

B. Create an origin access identity. right

C. Change the permissions on the bucket for the IAM users to have read permission.

D. Change the permission on the bucket so that only the origin access identity has read permissions. right

Explanation:

Answer – B and D

This is mentioned in the AWS Documentation.

To ensure that your users access your objects using only CloudFront URLs, regardless of whether the URLs are signed, perform the following tasks.

1. Create an origin access identity, which is a special CloudFront user, and associate the origin access identity with your distribution. (For web distributions, you associate the origin access identity with origins. So you can secure all or just some of your Amazon S3 content.)

2. Change the permissions either on your Amazon S3 bucket or on the objects in your bucket. So only the origin access identity has read permission (or read and download permission).

Since the documentation gives the recommended steps, the other options are invalid.

For more information on serving private content via CloudFront, please visit the below URL

https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-restricting-access-to-s3.html

Ask our Experts

⊕ View Queries 👍 👎

Question 3 Unattempted

Domain: Other

A team has set up a Cloudfront distribution with a web application hosted on an EC2 Instance as the Origin point. There is a security requirement to ensure that all requests via Cloudfront are recorded. Which of the following implementation steps need to be carried out? Choose 2 answers from the options given below.

A. Enable the standard log/access log for the CloudFront distribution. right

B. Enable the VPC flow logs in the CloudFront distribution.

C. Create a destination S3 bucket for the logs. right

D. Create a CloudWatch Log group to store the logs.

Explanation:

Answer – A and C

This is mentioned in the AWS Documentation.

When you enable logging for distribution, you specify the Amazon S3 bucket that you want CloudFront to store log files in. If you're using Amazon S3 as your origin, we recommend that you do not use the same bucket for your log files. Using a separate bucket simplifies maintenance.

You can store the log files for multiple distributions in the same bucket. When you enable logging, you can specify an optional prefix for the file names. So you can keep track of which log files are associated with which distributions.

Option B is incorrect because, for the CloudFront logging, it should be standard logs or access logs instead of VPC flow logs.

Option D is incorrect because CloudFront logging uses S3 to store the logs instead of the CloudWatch Log Groups.

For more information on Cloudfront Access logs, please visit the below URL

https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/AccessLogs.html

Ask our Experts

⊕ View Queries

👍 👎

Question 4

Unattempted

Domain: Other

A team has set up a CloudFront distribution with a web application hosted on an EC2 Instance as the Origin point. The Web application serves videos (HLS format) to various users. There is a requirement to ensure that a certain section of files needs to be accessed by only a certain subscriber on the website. Which of the following would you consider for this requirement?

A. Use Pre-signed URLs.

B. Use signed cookies. right

C. Implement CORS.

D. Use Lambda@Edge.

Explanation:

Answer - B

This is mentioned in the AWS Documentation.

Use signed cookies in the following cases.

- You want to provide access to multiple restricted files, for example, all of the files for a video in HLS format or all of the files in the subscribers' area of a website.
- You don't want to change your current URLs.

Option A is incorrect since this is used when you want to restrict access to individual files.

Option C is incorrect since CORS is used for access between domains.

Option D is incorrect since Lambda@Edge is an extension of AWS Lambda, a compute service that lets you execute functions that customize the content that CloudFront delivers.

For more information on choosing between signed URLs and cookies, please visit the below URL

https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-choosing-signed-urls-cookies.html

Ask our Experts

⊕ View Queries

Question 5 Unattempted

Domain: Other

A team has set up a Cloudfront distribution with a web application hosted on an EC2 Instance as the Origin point. A security requirement mandates that all configuration changes to the Cloudfront distribution need to be recorded. Which of the following options is the most straightforward?

A. AWS Config resources. right

B. AWS Config rule.

C. AWS CloudTrail that records all configuration changes.

D. AWS CloudWatch Event rule with a Lambda function as its target.

Explanation:

Answer – A

This is mentioned in the AWS Documentation.

You can use AWS Config to record configuration changes for CloudFront distribution settings changes. For example, you can capture changes to distribution states, price classes, origins, geo-restriction settings, and Lambda@Edge configurations.

Option B is incorrect since you have to configure a custom AWS Config rule and a Lambda function is required to provide the logic when the rule is evaluated. It is not the most straightforward method.

Option C is incorrect because, unlike AWS Config, CloudTrail does not show the detailed configuration changes for an AWS resource.

Option D is incorrect because you have to maintain the CloudWatch Event rule and the Lambda function. It is not the easiest approach.

For more information on tracking changes in AWS Config, please visit the below URL

https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/TrackingChanges.html

Ask our Experts

⊕ View Queries

Finish Review

Certification

- Cloud Certification
- Java Certification
- PM Certification
- Big Data Certification

Company

- Become Our Instructor
- Support
- Discussions
- Blog
- Business

Support

- Contact Us
- Help Topics

Join us on Slack!

Join our open **Slack community** and get your queries answered instantly! Our experts are online to answer your questions!