← Back to the **Course**

Level: Advanced

AWS Certified Security Specialty

Amazon Kinesis - Quiz

Completed on **Sun, 27 Feb 2022**

1st	0/10	0.00%
Attempt	Marks Obtained	Your Score

0h 0m 6s	FAIL
Time Taken	Result

Domain wise Quiz Performance Report

Join us on Slack community

No.	Domain	Total Question	Correct	Incorrect	Unattempted
1	Identity and Access Management	2	0	0	0
2	Data Protection	1	0	0	0
3	Identity and Access Management	7	0	0	0
Total	**All Domains**	**10**	**0**	**0**	**0**

Review the Answers

Filter By All Questions

Question 1

Unattempted

Domain: Data Protection

You are planning to use AWS Kinesis Data Streams for an application developed for a company. The company policy mandates that all data stored at rest should be encrypted.

How can you accomplish this in the easiest way for Kinesis Data Streams?

A. Use the SDK for Kinesis to encrypt the data before being stored at rest.

B. Enable server-side encryption for Kinesis Data Streams. right

C. Enable client-side encryption for Kinesis Data Streams.

D. Use the AWS CLI to encrypt the data.

Explanation:

Answer: B

Options A is incorrect because this would involve too much effort for encrypting and decrypting the streams by using SDK.

Option B is CORRECT because server-side encryption is a feature in Amazon Kinesis Data Streams that automatically encrypts data before it's at rest by using an AWS KMS customer master key (CMK) you specify. Data is encrypted before it's written to the Kinesis Data Stream storage layer and decrypted after it's retrieved from storage. As a result, your data is encrypted at rest within the Kinesis Data Streams service. This allows you to meet strict regulatory requirements and enhance the security of your data.

Options C is incorrect because this would involve too much effort for encrypting and decrypting the streams by using client-side encryption.

Option D is incorrect since this is the same as encrypting the data before it reaches the Kinesis Data Stream which is not required as per the asks.

Reference:

https://docs.aws.amazon.com/streams/latest/dev/what-is-sse.html

Ask our Experts

View Queries

Question 2 Unattempted

Domain: Other

Your company is making use of Kinesis streams. There are several applications that are built on EC2 Instances with access to Kinesis streams via IAM Roles. As per the security audit, it is required to track the calls made to create streams within the Kinesis service. Which method can be used to achieve the requirement?

A. Use the Kinesis API tracker to track the requests made to the streams.

B. Create a CloudTrail trail to track all management activities.

C. Create a CloudTrail trail and include the Amazon Kinesis Data Streams service. right

D. There is no AWS service or tool that can trace the Amazon Kinesis Data Streams activities.

Explanation:

Answer – C

The AWS Documentation mentions the following.

Amazon Kinesis Data Streams is integrated with AWS CloudTrail, which captures API calls made by or on behalf of Kinesis Data Streams and delivers the log files to the Amazon S3 bucket that you specify. The API calls can be made indirectly by using the Kinesis Data Streams console or directly by using the Kinesis Data Streams API. Using the information collected by CloudTrail, you can determine what request was made to Kinesis Data Streams, the source IP address from which the request was made, who made the request, when it was made, and so on.

Option A is incorrect because there is no API tracker with AWS Kinesis.

Option B is incorrect because there is no need to include all management activities in the trail.

Option C is CORRECT because CloudTrail supports the Amazon Kinesis Data Streams service.

For more information on logging with CloudTrail, please refer to the below URL

https://docs.aws.amazon.com/streams/latest/dev/logging-using-cloudtrail.html

Ask our Experts

View Queries

Question 3 Unattempted

Domain: Identity and Access Management

Your development team is planning on using the Kinesis Client Library (KCL) for its application. They have started developing and access the streams using their IAM user Access Keys, but the library keeps on throwing errors of not being able to perform functions pertinent to the streams.

Which of the following could be the underlying issue?

A. Ensure that the policy applied to the users has access to DynamoDB and CloudWatch. right

B. Ensure that the policy applied to the users has access to SQS and CloudWatch.

C. Ensure that the access keys have access to AWS Kinesis.

D. Ensure that the access keys have access to CloudWatch.

Explanation:

Answer: A

Option A is CORRECT because If you are developing an application when using the Kinesis Client Library (KCL), your policy must include permissions for Amazon DynamoDB and Amazon CloudWatch. The KCL uses DynamoDB to track state information for the application and CloudWatch to send KCL metrics to CloudWatch on your behalf.

Option B is incorrect because KCL does not require access to SQS for the IAM user policy.

Options C is incorrect because you need to provide access to the IAM user policy and not the access keys themselves for your application to use KCL.

Options D is incorrect because you need to provide access to the IAM user policy and not the access key policy for AWS CloudWatch.

Reference:

https://docs.aws.amazon.com/streams/latest/dev/controlling-access.html

Ask our Experts

View Queries

Question 4 Unattempted

Domain: Other

Your company is making use of Kinesis streams. There are several applications that are built on EC2 Instances with access to Kinesis streams via IAM Role. As part of the security policy, it is mandated that metrics be recorded for the streams at the shard level. How can this be accomplished?

A. Make use of AWS CloudTrail logs.

B. By default, the basic monitoring in CloudWatch for Kinesis covers the metrics at the shard level. The metrics can be found in the AWS/Kinesis namespace.

C. Enable Enhanced Monitoring in CloudWatch for the shard level data of Kinesis streams. Check the metrics in the AWS/Kinesis namespace. right

D. Make use of AWS DynamoDB for storing the logs.

Explanation:

Answer – C

The AWS Documentation mentions the following.

The following table describes basic stream-level and enhanced shard-level monitoring for

Type	Description
Basic (stream-level)	Stream-level data is sent automatically every minute at no charge.
Enhanced (shard-level)	Shard-level data is sent every minute for an additional cost. To get th EnableEnhancedMonitoring operation. For information about pricing, see the Amazon CloudWatch product

All other options are incorrect because of the exact requirement which is given in the AWS Documentation.

For more information on monitoring with Cloudwatch, please refer to the below URL

https://docs.aws.amazon.com/streams/latest/dev/monitoring-with-cloudwatch.html

Ask our Experts

View Queries

Question 5 Unattempted

Domain: Other

You're planning to use Kinesis Data Firehose. The data would be sent to an S3 bucket. The data would be encrypted at rest using a KMS key. You need to create an IAM role with suitable IAM policies to grant Kinesis Data Firehose access to the S3 bucket. Which of the following permissions need to be included in the IAM policies? (Select TWO.)

A. Kms:Decrypt right

B. Kms:Import-key-material

C. Kms:GenerateCustomerKey

D. Kms:GenerateDataKey right

Explanation:

Answer – A and D

If Kinesis Firehose needs to access an S3 bucket where encryption is enabled using KMS, the following permissions need to be included in the IAM policies.

```
},
{
    "Effect": "Allow",
    "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey"
```

Since the documentation clearly mentions what access needs to be given, the other options are invalid.

For more information on controlling access, please refer to the below URL

https://docs.aws.amazon.com/firehose/latest/dev/controlling-access.html#using-iam-s3

Ask our Experts

View Queries

Question 6 Unattempted

Domain: Other

You have an application that is going to be hosted on an EC2 Instance. The application needs to access Kinesis Data streams. There is a security mandate that no data should leave the VPC onto the Internet. Which of the following would help you ensure the application adheres to the security requirement?

A. Enable VPC Enhanced Routing.

B. Make use of a NAT gateway.

C. Make use of a VPC Endpoint gateway.

D. Make use of a VPC Endpoint Interface. right

Explanation:

Answer - D

The AWS Documentation mentions the following.

You can use an interface VPC endpoint to keep traffic between your Amazon VPC and Kinesis Data Streams from leaving the Amazon network. Interface VPC endpoints don't require an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection.

Option A is incorrect because VPC Enhanced Routing is a feature for Amazon Redshift and does not help in this scenario.

Option B is incorrect because the traffic still traverses to the internet with a NAT gateway.

Option C is incorrect because a VPC Endpoint gateway is only used for S3 and DynamoDB.

For more information on accessing Kinesis streams via a VPC, please refer to the below URL

https://docs.aws.amazon.com/streams/latest/dev/vpc.html

Ask our Experts

View Queries

Question 7

Unattempted

Domain: Other

You're developing an application that is going to make use of Kinesis Data Streams. The data streams are going to be processed by Lambda functions. Which of the following steps are required to ensure that the Lambda functions have suitable permissions to manage resources related to your Kinesis data streams? (Select TWO.)

A. Create a service role of the type AWS Kinesis.

B. Create a Lambda execution role for the Lambda functions. right

C. Use the AWSLambdaExecutionRole.

D. Attach the AWSLambdaKinesisExecutionRole policy to the Lambda execution role. right

Explanation:

Answer- B and D

Option A is incorrect because the change should be in the Lambda execution role.

Option B is CORRECT because the Lambda execution role should be created for the Lambda function with suitable permissions.

Option C is incorrect because there is no AWS managed IAM policy AWSLambdaExecutionRole.

Option D is CORRECT because the AWS managed policy AWSLambdaKinesisExecutionRole has suitable permissions for Lambda functions to manage Kinesis data streams.

For more information on using Kinesis with AWS Lambda, please refer to the below URL

https://docs.aws.amazon.com/lambda/latest/dg/with-kinesis.html

Ask our Experts

View Queries

Question 8

Unattempted

Domain: Identity and Access Management

Your team is developing an application that will be making use of Kinesis Analytics. The Analytics application will be reading records from Kinesis data streams.

Which of the following actions need to be part of the permission policy? (Select all that apply)

A. Kinesis:GetRecords right

B. Kinesis:PutRecords

C. Kinesis:DescribeStream right

D. Kinesis:GetShardIterator right

Explanation:

Answer: A, C and D

Options A, C, and D are CORRECT because if you are creating an IAM role to allow Amazon Kinesis Data Analytics to read from an application's streaming source, you must grant permissions for relevant read actions.

Option B is incorrect because the data is being read from the stream and not put in the stream. The permission of Kinesis: PutRecords is not needed over here.

Permissions Policy for Reading a Kinesis Stream

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ReadInputKinesis",
      "Effect": "Allow",
      "Action": [
        "kinesis:DescribeStream",
        "kinesis:GetShardIterator",
        "kinesis:GetRecords"
      ],
      "Resource": [
        "arn:aws:kinesis:aws-region:aws-account-id:stream/inputStreamName"
```

```
        ]
      }
    ]
}
```

Reference:

https://docs.aws.amazon.com/kinesisanalytics/latest/dev/iam-role.html

Ask our Experts

View Queries

Question 9 Unattempted

Domain: Other

Your team is developing an application that will be making use of Kinesis streams. A load test was conducted to get 15000 records in GetRecords requests. The requests failed with ProvisionedThroughputExceededException. Which of the following could be a reason for this?

A. AWS Kinesis only allows 1000 records to be read per second.

B. You can only have 100 shards with 10 records processed per shard.

C. The GetRecords requests hit the payload limit. right

D. There is a limit on the number of streams.

Explanation:

Answer – C

Amazon Kinesis Data Streams has the following limits for GetRecords.

> GetRecords can retrieve up to 10 MiB of data per call from a single shard and up to 10,000 records per call. Each call to GetRecords is counted as one read transaction.

For more information on service limits with Kinesis, please refer to the below URL

https://docs.aws.amazon.com/streams/latest/dev/service-sizes-and-limits.html

Ask our Experts

View Queries

Question 10 Unattempted

Domain: Other

Your team is developing an application that will make use of Kinesis streams. Which of the following permissions need to be given to the producers for the streams? Choose 2 answers from the options given below.

A. DescribeStream right

B. GetStream

C. PutRecord right

D. GetRecords

Explanation:

Answer – A and C

Option A is CORRECT because DescribeStream is used for the producer to check if the stream exists and is active.

Option C is CORRECT because PutRecord is used for the producer to write records to Kinesis Data Streams.

Options B and D are incorrect because either GetStream or GetRecords is used for the Kinesis streams consumer instead of producer.

For more information on the policies that need to be assigned, please refer to the below URL

https://docs.aws.amazon.com/streams/latest/dev/tutorial-stock-data-kplkcl-iam.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!