ExamsIndex
Practice Materials & Tests

DEMO VERSION

Amazon

SCS-C02 Exam

AWS Certified Security - Specialty

Exam Latest Version: 17.5

Question 1. (Single Select)

[Identity and Access Management]

You have an S3 bucket defined in IAM. You want to ensure that you encrypt the data before sending it across the wire. What is the best way to achieve this.

Please select:

A: Enable server side encryption for the S3 bucket. This request will ensure that the data is encrypted first.
B: Use the IAM Encryption CLI to encrypt the data first
C: Use a Lambda function to encrypt the data before sending it to the S3 bucket.
D: Enable client encryption for the bucket

Correct Answer: B

Explanation:

One can use the IAM Encryption CLI to encrypt the data before sending it across to the S3 bucket. Options A and C are invalid because this would still mean that data is transferred in plain text Option D is invalid because you cannot just enable client side encryption for the S3 bucket For more information on Encrypting and Decrypting data, please visit the below URL:

https://IAM.amazonxom/blogs/securirv/how4o-encrvpt-and-decrypt-your-data-with-the-IAM-encryption-cl

The correct answer is: Use the IAM Encryption CLI to encrypt the data first Submit your Feedback/Queries to our Experts

---

Question 2. (Multi Select)

[Incident Response]

A company needs a forensic-logging solution for hundreds of applications running in Docker on Amazon EC2 The solution must perform real-time analytics on the togs must support the replay of messages and must persist the logs.

Which IAM services should be used to meet these requirements? (Select TWO)

A: Amazon Athena
B: Amazon Kinesis
C: Amazon SQS
D: Amazon Elasticsearch
E: Amazon EMR

Correct Answer: B, D

Explanation:

Amazon Kinesis and Amazon Elasticsearch are both suitable for forensic-logging solutions. Amazon Kinesis can collect, process, and analyze streaming data in real time3. Amazon Elasticsearch can store, search, and analyze log data using the popular open-source tool Elasticsearch. The other options are not designed for forensic-logging purposes. Amazon Athena is a query service that can analyze data in S3, Amazon SQS is a message queue service that can decouple and scale microservices, and AmazonEMR is a big data platform that can run Apache Spark and Hadoop clusters.

Question 3. (Single Select)

[Identity and Access Management]

A company's IAM account consists of approximately 300 IAM users. Now there is a mandate that an access change is required for 100 IAM users to have unlimited privileges to S3.As a system administrator, how can you implement this effectively so that there is no need to apply the policy at the individual user level?

Please select:

A: Create a new role and add each user to the IAM role

B: Use the IAM groups and add users, based upon their role, to different groups and apply the policy to group
C: Create a policy and apply it to multiple users using a script
D: Create an S3 bucket policy with unlimited access which includes each user's IAM account ID

Correct Answer: B

Explanation:

Option A is incorrect since you don't add a user to the IAM Role

Option C is incorrect since you don't assign multiple users to a policy

Option D is incorrect since this is not an ideal approach

An IAM group is used to collectively manage users who need the same set of permissions. By having groups, it becomes easier to manage permissions. So if you change the permissions on the group scale, it will affect all the users in that group

For more information on IAM Groups, just browse to the below URL:

https://docs.IAM.amazon.com/IAM/latest/UserGuide/id_eroups.html

The correct answer is: Use the IAM groups and add users, based upon their role, to different groups and apply the policy to group

Submit your Feedback/Queries to our Experts

Question 4. (Single Select)

[Identity and Access Management]

You need to create a policy and apply it for just an individual user. How could you accomplish this in the right way?

Please select:

A: Add an IAM managed policy for the user
B: Add a service policy for the user
C: Add an IAM role for the user
D: Add an inline policy for the user

Correct Answer: D

Explanation:

Options A and B are incorrect since you need to add an inline policy just for the user

Option C is invalid because you don't assign an IAM role to a user

The IAM Documentation mentions the following

An inline policy is a policy that's embedded in a principal entity (a user, group, or role)—that is, the policy is an inherent part of the principal entity. You can create a policy and embed it in a principal entity, either when you create the principal entity or later.

For more information on IAM Access and Inline policies, just browse to the below URL:

https://docs.IAM.amazon.com/IAM/latest/UserGuide/access

The correct answer is: Add an inline policy for the user Submit your Feedback/Queries to our Experts

---

Question 5. (Single Select)

[Infrastructure Security]

Your company is planning on using bastion hosts for administering the servers in IAM. Which of the following is the best description of a bastion host from a security perspective?

Please select:

A: A Bastion host should be on a private subnet and never a public subnet due to security concerns

B: A Bastion host sits on the outside of an internal network and is used as a gateway into the private network and is considered the critical strong point of the network
C: Bastion hosts allow users to log in using RDP or SSH and use that session to S5H into internal network to access private subnet resources.
D: A Bastion host should maintain extremely tight security and monitoring as it is available to the public

Correct Answer: C

Explanation:

A bastion host is a special purpose computer on a network specifically designed and configured to withstand attacks. The computer generally hosts a single application, for example a proxy server, and all other services are removed or limited to reduce the threat to the computer.

In IAM, A bastion host is kept on a public subnet. Users log on to the bastion host via SSH or RDP and then use that session to manage other hosts in the private subnets.

Options A and B are invalid because the bastion host needs to sit on the public network. Option D is invalid because bastion hosts are not used for monitoring For more information on bastion hosts, just browse to the below URL:

https://docsIAM.amazon.com/quickstart/latest/linux-bastion/architecture.htl

The correct answer is: Bastion hosts allow users to log in using RDP or SSH and use that session to SSH into internal network to access private subnet resources.

Submit your Feedback/Queries to our Experts

ExamsIndex

Demo PDF Complete

Your SCS-C02 Demo (5 Questions)

Get the Complete Version

Full Questions with Detailed Explanations

Interactive Web-Based Exams Available

To get 50% off, use Coupon Code: OCT50

https://examsindex.com/exam/scs-c02