SCS-C02 Q&As

AWS Certified Security - Specialty

Pass Amazon SCS-C02 Exam with 100% Guarantee

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

https://www.pass4itsure.com/scs-c02.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 operating a website using Amazon CloudFornt. CloudFront servers some content from Amazon S3 and other from web servers running EC2 instances behind an Application. Load Balancer (ALB). Amazon DynamoDB is used as the data store. The company already uses IAM Certificate Manager (ACM) to store a public TLS certificate that can optionally secure connections between the website users and CloudFront. The company has a new requirement to enforce end-to-end encryption in transit. Which combination of steps should the company take to meet this requirement? (Select THREE.)

A. Update the CloudFront distribution. configuring it to optionally use HTTPS when connecting to origins on Amazon S3

B. Update the web application configuration on the web servers to use HTTPS instead of HTTP when connecting to DynamoDB

C. Update the CloudFront distribution to redirect HTTP corrections to HTTPS

D. Configure the web servers on the EC2 instances to listen using HTTPS using the public ACM TLS certificate Update the ALB to connect to the target group using HTTPS

E. Update the ALB listen to listen using HTTPS using the public ACM TLS certificate. Update the CloudFront distribution to connect to the HTTPS listener.

F. Create a TLS certificate Configure the web servers on the EC2 instances to use HTTPS only with that certificate. Update the ALB to connect to the target group using HTTPS.

Correct Answer: BCE

QUESTION 2

A company is migrating one of its legacy systems from an on-premises data center to AWS. The application server will run on AWS, but the database must remain in the on- premises data center for compliance reasons. The database is

sensitive to network latency. Additionally, the data that travels between the on-premises data center and AWS must have IPsec encryption.

Which combination of AWS solutions will meet these requirements? (Choose two.)

A. AWS Site-to-Site VPN

B. AWS Direct Connect

C. AWS VPN CloudHub

D. VPC peering

E. NAT gateway

Correct Answer: AB

The correct combination of AWS solutions that will meet these requirements is A. AWS Site-to-Site VPN and B. AWS Direct Connect. A. AWS Site-to-Site VPN is a service that allows you to securely connect your on-premises data center

to your AWS VPC over the internet using IPsec encryption. This solution meets the requirement of encrypting the data in transit between the on-premises data center and AWS.

B. AWS Direct Connect is a service that allows you to establish a dedicated network connection between your on-premises data center and your AWS VPC. This solution meets the requirement of reducing network latency between the on-premises data center and AWS.

C. AWS VPN CloudHub is a service that allows you to connect multiple VPN connections from different locations to the same virtual private gateway in your AWS VPC. This solution is not relevant for this scenario, as there is only one on-premises data center involved. D. VPC peering is a service that allows you to connect two or more VPCs in the same or different regions using private IP addresses. This solution does not meet the requirement of connecting an on-premises data center to AWS, as it only works for VPCs. E. NAT gateway is a service that allows you to enable internet access for instances in a private subnet in your AWS VPC. This solution does not meet the requirement of connecting an on-premises data center to AWS, as it only works for outbound traffic from your VPC.

QUESTION 3

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 4

An organization is moving non-business-critical applications to IAM while maintaining a mission-critical application in an on-premises data center. An on-premises application must share limited confidential information with the applications in

IAM. The internet performance is unpredictable.

Which configuration will ensure continued connectivity between sites MOST securely?

A. VPN and a cached storage gateway

B. IAM Snowball Edge

C. VPN Gateway over IAM Direct Connect

D. IAM Direct Connect

Correct Answer: C

https://docs.IAM.amazon.com/whitepapers/latest/IAM-vpc-connectivity-options/IAM-direct- connect-plus-vpn-network-to-amazon.html

QUESTION 5

A company manages multiple IAM accounts using IAM Organizations. The company\\'s security team notices that some member accounts are not sending IAM CloudTrail logs to a centralized Amazon S3 logging bucket. The security team wants to ensure there is at least one trail configured (or all existing accounts and for any account that is created in the future.

Which set of actions should the security team implement to accomplish this?

A. Create a new trail and configure it to send CloudTrail logs to Amazon S3. Use Amazon EventBridge (Amazon CloudWatch Events) to send notification if a trail is deleted or stopped.

B. Deploy an IAM Lambda function in every account to check if there is an existing trail and create a new trail, if needed.

C. Edit the existing trail in the Organizations master account and apply it to the organization.

D. Create an SCP to deny the cloudtrail:Delete" and cloudtrail:Stop\\' actions. Apply the SCP to all accounts.

Correct Answer: C