



SCS-C01^{Q&As}

AWS Certified Security - Specialty (SCS-C01)

Pass Amazon SCS-C01 Exam with 100% Guarantee

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

<https://www.pass4itsure.com/aws-certified-security-specialty.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 pharmaceutical company has digitized versions of historical prescriptions stored on premises. The company would like to move these prescriptions to AWS and perform analytics on the data in them. Any operation with this data requires that the data be encrypted in transit and at rest.

Which application flow would meet the data protection requirements on AWS?

- A. Digitized files -> Amazon Kinesis Data Analytics
- B. Digitized files -> Amazon Kinesis Data Firehose -> Amazon S3 -> Amazon Athena
- C. Digitized files -> Amazon Kinesis Data Streams -> Kinesis Client Library consumer -> Amazon S3 -> Athena
- D. Digitized files -> Amazon Kinesis Data Firehose -> Amazon Elasticsearch

Correct Answer: B

QUESTION 2

A new application will be deployed on EC2 instances in private subnets. The application will transfer sensitive data to and from an S3 bucket. Compliance requirements state that the data must not traverse the public internet. Which solution meets the compliance requirement?

Please select:

- A. Access the S3 bucket through a proxy server
- B. Access the S3 bucket through a NAT gateway.
- C. Access the S3 bucket through a VPC endpoint for S3
- D. Access the S3 bucket through the SSL protected S3 endpoint

Correct Answer: C

The AWS Documentation mentions the following A VPC endpoint enables you to privately connect your VPC to supported AWS services and VPC endpoint services powered by PrivateLink without requiring an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. Instances in your VPC do not require public IP addresses to communicate with resources in the service. Traffic between your VPC and the other service does not leave the Amazon network. Option A is invalid because using a proxy server is not sufficient enough Option B and D are invalid because you need secure communication which should not traverse the internet For more information on VPC endpoints please see the below link <https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-endpoints.html>
The correct answer is: Access the S3 bucket through a VPC endpoint for S3

QUESTION 3

A security engineer is responsible for providing secure access to AWS resources for thousands of developer in a company's corporate identity provider (idp). The developers access a set of AWS services from the corporate premises using IAM credential. Due to the volume of require for provisioning new IAM users, it is taking a long time to grant access permissions. The security engineer receives reports that developer are sharing their IAM credentials with others to avoid



provisioning delays. The causes concern about overall security for the security engineer.

Which actions will meet the program requirements that address security?

- A. Create an Amazon CloudWatch alarm for AWS CloudTrail Events Create a metric filter to send a notification when the same set of IAM credentials is used by multiple developer
- B. Create a federation between AWS and the existing corporate IdP Leverage IAM roles to provide federated access to AWS resources
- C. Create a VPN tunnel between the corporate premises and the VPC Allow permissions to all AWS services only if it originates from corporate premises.
- D. Create multiple IAM roles for each IAM user Ensure that users who use the same IAM credentials cannot assume the same IAM role at the same time.

Correct Answer: B

Reference: https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_common-scenarios_federated-users.html

QUESTION 4

A company wants to encrypt data locally while meeting regulatory requirements related to key exhaustion. The encryption key can be no more than 10 days old or encrypt more than 2^{16} objects. Any encryption key must be generated on a FIPS-validated hardware security module (HSM). The company is cost-conscious, as it plans to upload an average of 100 objects to Amazon S3 each second for sustained operations across 5 data producers.

Which approach MOST efficiently meets the company's needs?

- A. Use the AWS Encryption SDK and set the maximum age to 10 days and the minimum number of messages encrypted to 2^{16} . Use AWS Key Management Service (AWS KMS) to generate the master key and data key Use data key caching with the Encryption SDK during the encryption process.
- B. Use AWS Key Management Service (AWS KMS) to generate an AWS managed CMK. Then use Amazon S3 client-side encryption configured to automatically rotate with every object
- C. Use AWS CloudHSM to generate the master key and data keys. Then use Boto 3 and Python to locally encrypt data before uploading the object Rotate the data key every 10 days or after 2^{16} objects have been Uploaded to Amazon S3
- D. Use server-side encryption with Amazon S3 managed encryption keys (SSE-S3) and set the master key to automatically rotate.

Correct Answer: C

QUESTION 5

A company requires deep packet inspection on encrypted traffic to its web servers in its VPC. Which solution will meet this requirement?

- A. Decrypt traffic by using an Application Load Balancer (ALB) that is configured for TLS termination. Configure the ALB



to send the traffic to an AWS Network Firewall endpoint for the deep packet inspection.

B. Decrypt traffic by using a Network Load Balancer (NLB) that is configured for TLS termination. Configure the NLB to send the traffic to an AWS Network Firewall endpoint for the deep packet inspection.

C. Decrypt traffic by using an Application Load Balancer (ALB) that is configured for TLS termination. Configure the ALB to send the traffic to an AWS WAF endpoint for the deep packet inspection.

D. Decrypt traffic by using a Network Load Balancer (NLB) that is configured for TLS termination. Configure the NLB to send the traffic to an AWS WAF endpoint for the deep packet inspection.

Correct Answer: A

[SCS-C01 PDF Dumps](#)

[SCS-C01 Practice Test](#)

[SCS-C01 Study Guide](#)