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.leads4pass.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 company has been using the AW5 KMS service for managing its keys. They are planning on carrying out housekeeping activities and deleting keys which are no longer in use. What are the ways that can be incorporated to see which keys are in use? Choose 2 answers from the options given below

Please select:

A. Determine the age of the master key

B. See who is assigned permissions to the master key

C. See Cloudtrail for usage of the key

D. Use AWS cloudwatch events for events generated for the key

Correct Answer: BC

The direct ways that can be used to see how the key is being used is to see the current access permissions and cloudtrail logs Option A is invalid because seeing how long ago the key was created would not determine the usage of the key Option D is invalid because Cloudtrail Event is better for seeing for events generated by the key This is also mentioned in the AWS Documentation Examining CMK Permissions to Determine the Scope of Potential Usage Determining who or what currently has access to a customer master key (CMK) might help you determine how widely the CM was used and whether it is still needed. To learn how to determine who or what currently has access to a CMK, go to Determining Access to an AWS KMS Customer Master Key. Examining AWS CloudTrail Logs to Determine Actual Usage AWS KMS is integrated with AWS CloudTrail, so all AWS KMS API activity is recorded in CloudTrail log files. If you have CloudTrail turned on in the region where your customer master key (CMK) is located, you can examine your CloudTrail log files to view a history of all AWS KMS API activity for a particular CMK, and thus its usage history. You might be able to use a CMK\\'s usage history to help you determine whether or not you still need it For more information on determining the usage of CMK keys, please visit the following URL: https://docs.aws.amazon.com/kms/latest/developerguide/deleting-keys-determining-usage.html The correct answers are: See who is assigned permissions to the master key. See Cloudtrail for usage of the key

---

QUESTION 2

A company is developing a new mobile app for social media sharing. The company\\'s development team has decided to use Amazon S3 to store at media files generated by mobile app users The company wants to allow users to control whether their own tiles are public, private, of shared with other users in their social network

What should the development team do to implement the type of access control with the LEAST administrative effort?

A. Use individual ACLs on each S3 object.

B. Use IAM groups tor sharing files between application social network users

C. Store each user\\'s files in a separate S3 bucket and apery a bucket policy based on the user\\'s sharing settings

D. Generate presigned UPLs for each file access

Correct Answer: A

QUESTION 3

A company is planning on using AWS EC2 and AWS Cloudfrontfor their web application. For which one of the below attacks is usage of Cloudfront most suited for? Please select:

A. Cross side scripting

B. SQL injection

C. DDoS attacks

D. Malware attacks

Correct Answer: C

The below table from AWS shows the security capabilities of AWS Cloudfront AWS Cloudfront is more prominent for DDoS attacks.

Type of Access Control	AWS Account-Level Control?	User-LevelControl?
IAM Policies	No	Yes
ACLs	Yes	No
Bucket Policies	Yes	Yes

Options A,B and D are invalid because Cloudfront is specifically used to protect sites against DDoS attacks For more information on security with Cloudfront, please refer to the below Link:
https://d1.awsstatic.com/whitepapers/Security/Secure content delivery with CloudFront whitepaper.pdf The correct answer is: DDoS attacks

QUESTION 4

A company is building a data processing application mat uses AWS Lambda functions. The application\\'s Lambda functions need to communicate with an Amazon RDS OB instance that is deployed within a VPC in the same AWS account

Which solution meets these requirements in the MOST secure way?

A. Configure the DB instance to allow public access Update the DB instance security group to allow access from the Lambda public address space for the AWS Region

B. Deploy the Lambda functions inside the VPC Attach a network ACL to the Lambda subnet Provide outbound rule access to the VPC CIDR range only Update the DB instance security group to allow traffic from 0.0.0.0/0

C. Deploy the Lambda functions inside the VPC Attach a security group to the Lambda functions Provide outbound rule access to the VPC CIDR range only Update the DB instance security group to allow traffic from the Lambda security group

D. Peer the Lambda default VPC with the VPC that hosts the DB instance to allow direct network access without the need for security groups

Correct Answer: C

This solution ensures that the Lambda functions are deployed inside the VPC and can communicate with the Amazon RDS DB instance securely. The security group attached to the Lambda functions only allows outbound traffic to the VPC CIDR range, and the DB instance security group only allows traffic from the Lambda security group. This solution ensures that the Lambda functions can communicate with the DB instance securely and that the DB instance is not exposed to the public internet.

QUESTION 5

A development team is using an AWS Key Management Service (AWS KMS) CMK to try to encrypt and decrypt a secure string parameter from AWS Systems Manager Parameter Store. However, the development team receives an error message on each attempt.

Which issues that are related to the CMK could be reasons for the error? (Choose two.)

A. The CMK is used in the attempt does not exist.

B. The CMK is used in the attempt needs to be rotated.

C. The CMK is used in the attempt is using the CMK\\'s key ID instead of the CMK ARN.

D. The CMK is used in the attempt is not enabled.

E. The CMK is used in the attempt is using an alias.

Correct Answer: AD

Most of the Parameter Store failures related to KMS keys are caused by the following problems:

The KMS key is not found.This typically happens when you use an incorrect identifier for the KMS key.

The KMS key is not enabled. When this occurs, Parameter Store returns an InvalidKeyId exception with a detailed error message from AWS KMS.

QUESTION 6

Your company is planning on developing an application in AWS. This is a web based application. The application user will use their facebook or google identities for authentication. You want to have the ability to manage user profiles without having to add extra coding to manage this. Which of the below would assist in this.

Please select:

A. Create an OIDC identity provider in AWS

B. Create a SAML provider in AWS

C. Use AWS Cognito to manage the user profiles

D. Use IAM users to manage the user profiles

Correct Answer: C

The AWS Documentation mentions the following A user pool is a user directory in Amazon Cognito. With a user pool, your users can sign in to your web or mobile app through Amazon Cognito. Your users can also sign in through social

identity providers like Facebook or Amazon, and through SAML identity providers. Whether your users sign in directly or through a third party, all members of the user pool have a directory profile that you can access through an SDK.

User pools provide:

Sign-up and sign-in services.

A built-in, customizable web UI to sign in users. Social sign-in with Facebook, Google, and Login with Amazon, as well as sign-in with SAML identity providers from your user pool.

User directory management and user profiles.

Security features such as multi-factor authentication (MFA), checks for compromised credentials, account takeover protection, and phone and email verification. Customized workflows and user migration through AWS Lambda triggers.

Options A and B are invalid because these are not used to manage users Option D is invalid because this would be a maintenance overhead For more information on Cognito User Identity pools, please refer to the below Link:

https://docs.aws.amazon.com/coenito/latest/developerguide/cognito-user-identity-pools.html

The correct answer is: Use AWS Cognito to manage the user profiles

QUESTION 7

A company is observing frequent bursts of unusual traffic to its corporate website. The IP address ranges that inflate the requests keep changing, and the volumes of traffic are increasing.

A security engineer needs to implement a solution to protect the website from a potential DDoS attack. The solution must rack the rate of requests from IP addresses. When the requests from a particular IP address exceed a specific rate, the

solution must limit the amount of traffic that can reach the website from that IP address.

Which solution will meet these requirements?

A. Setup Amazon Inspector on the backend servers. Create assessment targets with a rate-based configuration to block any offending IP address.

B. Create a rate-based rule in AWS WAF to block an IP address when that IP address exceeds the configured threshold rate.

C. Identity the offending client IP address ranges. Create a regular rule in AWS WAF to block the offending IP address ranges.

D. Create a rate-based rule in Amazon GuardDuty to block an IP address when that IP address exceeds the configured threshold rate

Correct Answer: C

QUESTION 8

A company is using AWS Organizations to manage multiple AWS accounts. The company has an application that allows users to assume the AppUser IAM role to download files from an Amazon S3 bucket that is encrypted with an AWS KMS CMK However when users try to access the files in the S3 bucket they get an access denied error.

What should a Security Engineer do to troubleshoot this error? (Select THREE)

A. Ensure the KMS policy allows the AppUser role to have permission to decrypt for the CMK

B. Ensure the S3 bucket policy allows the AppUser role to have permission to get objects for the S3 bucket

C. Ensure the CMK was created before the S3 bucket.

D. Ensure the S3 block public access feature is enabled for the S3 bucket.

E. Ensure that automatic key rotation is disabled for the CMK

F. Ensure the SCPs within Organizations allow access to the S3 bucket.

Correct Answer: BDE

QUESTION 9

A company is running an Amazon RDS for MySQL DB instance in a VPC. The VPC must not send or receive network traffic through the internet.

A security engineer wants to use AWS Secrets Manager to rotate the DB instance credentials automatically. Because of a security policy, the security engineer cannot use the standard AWS Lambda function that Secrets Manager provides to rotate the credentials. The security engineer deploys a custom Lambda function in the VPC. The custom Lambda function will be responsible for rotating the secret in Secrets Manager. The security engineer edits the DB instance\\'s security group to allow

connections from this function. When the function is invoked, the function cannot communicate with Secrets Manager to rotate the secret properly. What should the security engineer do so that the function can rotate the secret?

A. Add an egress-only internet gateway to the VPC. Allow only the Lambda function\\'s subnet to route traffic through the egress-only internet gateway.

B. Add a NAT gateway to the VPC. Configure only the Lambda function\\'s subnet with a default route through the NAT gateway.

C. Configure a VPC peering connection to the default VPC for Secrets Manager. Configure the Lambda function\\'s subnet to use the peering connection for routes.

D. Configure a Secrets Manager interface VPC endpoint. Include the Lambda function\\'s private subnet during the configuration process.

Correct Answer: C

QUESTION 10

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

QUESTION 11

A company requires that IP packet data be inspected for invalid or malicious content.

Which of the following approaches achieve this requirement? (Choose two.)

A. Configure a proxy solution on Amazon EC2 and route all outbound VPC traffic through it. Perform inspection within proxy software on the EC2 instance.

B. Configure the host-based agent on each EC2 instance within the VPC. Perform inspection within the host-based agent.

C. Enable VPC Flow Logs for all subnets in the VPC. Perform inspection from the Flow Log data within Amazon CloudWatch Logs.

D. Configure Elastic Load Balancing (ELB) access logs. Perform inspection from the log data within the ELB access log files.

E. Configure the CloudWatch Logs agent on each EC2 instance within the VPC. Perform inspection from the log data within CloudWatch Logs.

Correct Answer: AB

"EC2 Instance IDS/IPS solutions offer key features to help protect your EC2 instances. This includes alerting administrators of malicious activity and policy violations, as well as identifying and taking action against attacks. You can use AWS services and third party IDS/IPS solutions offered in AWS Marketplace to stay one step ahead of potential attackers."

QUESTION 12

A company has deployed servers on Amazon EC2 instances in a VPC. External vendors access these servers over the internet. Recently, the company deployed a new application on EC2 instances in a new CIDR range. The company needs

to make the application available to the vendors.

A security engineer verified that the associated security groups and network ACLs are allowing the required ports in the inbound diction. However, the vendors cannot connect to the application.

Which solution will provide the vendors access to the application?

A. Modify the security group that is associated with the EC2 instances to have the same outbound rules as inbound rules.

B. Modify the network ACL that is associated with the CIDR range to allow outbound traffic to ephemeral ports.

C. Modify the inbound rules on the internet gateway to allow the required ports.

D. Modify the network ACL that is associated with the CIDR range to have the same outbound rules as inbound rules.

Correct Answer: D

QUESTION 13

A company has hundreds of AWS accounts, and a centralized Amazon S3 bucket used to collect AWS CloudTrail logs for all of these accounts. A Security Engineer wants to create a solution that will enable the company to run ad hoc queries against its CloudTrail logs dating back 3 years from when the trails were first enabled in the company\\'s AWS account.

How should the company accomplish this with the least amount of administrative overhead?

A. Run an Amazon EMP cluster that uses a MapReduce job to be examine the CloudTrail trails.

B. Use the events history/feature of the CloudTrail console to query the CloudTrail trails.

C. Write an AWS Lambda function to query the CloudTrail trails Configure the Lambda function to be executed whenever a new file is created in the CloudTrail S3 bucket.

D. Create an Amazon Athena table that tools at the S3 bucket the CloudTrail trails are being written to Use Athena to run queries against the trails.

Correct Answer: B

QUESTION 14

You have private video content in S3 that you want to serve to subscribed users on the Internet. User IDs, credentials, and subscriptions are stored in an Amazon RDS database. Which configuration will allow you to securely serve private content to your users?

Please select:

A. Generate pre-signed URLs for each user as they request access to protected S3 content

B. Create an IAM user for each subscribed user and assign the GetObject permission to each IAM user

C. Create an S3 bucket policy that limits access to your private content to only your subscribed users\\'credentials

D. Crpafp a Cloud Front Clriein Identity user for vnur suhsrrihprl users and assign the GptOhiprt oprmissinn to this user

Correct Answer: A

All objects and buckets by default are private. The pre-signed URLs are useful if you want your user/customer to be able upload a specific object to your bucket but you don\\'t require them to have AWS security credentials or permissions.

When you create a pre-signed URL, you must provide your security credentials, specify a bucket name, an object key, an HTTP method (PUT for uploading objects), and an expiration date and time. The pre-signed URLs are valid only for the

specified duration.

Option B is invalid because this would be too difficult to implement at a user level.

Option C is invalid because this is not possible

Option D is invalid because this is used to serve private content via Cloudfront For more information on pre-signed urls, please refer to the Link:

http://docs.aws.amazon.com/AmazonS3/latest/dev/PresienedUrlUploadObiect.htmll The correct answer is: Generate pre-signed URLs for each user as they request access to protected S3 content

QUESTION 15

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