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

Unapproved changes were previously made to a company\\'s Amazon S3 bucket. A security engineer configured AWS Config to record configuration changes made to the company\\'s S3 buckets. The engineer discovers there are S3 configuration changes being made, but no Amazon SNS notifications are being sent. The engineer has already checked the configuration of the SNS topic and has confirmed the configuration is valid.

Which combination of steps should the security engineer take to resolve the issue? (Select TWO.)

A. Configure the S3 bucket ACLs to allow AWS Config to record changes to the buckets.

B. Configure policies attached to S3 buckets to allow AWS Config to record changes to the buckets.

C. Attach the AmazonS3ReadOnryAccess managed policy to the IAM user.

D. Verify the security engineer\\'s IAM user has an attached policy that allows all AWS Config actions.

E. Assign the AWSConfigRole managed policy to the AWS Config role

Correct Answer: AD

Reference: https://aws.amazon.com/blogs/security/how-to-use-aws-config-to-monitor-for-and-respond-to-amazon-s3-buckets-allowing-public-access/

QUESTION 2

A Security Engineer is working with the development team to design a supply chain application that stores sensitive inventory data in an Amazon S3 bucket. The application will use an AWS KMS customer master key (CMK) to encrypt the data on Amazon S3. The inventory data on Amazon S3 will be shared of vendors. All vendors will use AWS principals from their own AWS accounts to access the data on Amazon S3. The vendor list may change weekly, and the solution must support cross-account access.

What is the MOST efficient way to manage access control for the KMS CMK7?

A. Use KMS grants to manage key access. Programmatically create and revoke grants to manage vendor access.

B. Use an IAM role to manage key access. Programmatically update the IAM role policies to manage vendor access.

C. Use KMS key policies to manage key access. Programmatically update the KMS key policies to manage vendor access.

D. Use delegated access across AWS accounts by using IAM roles to manage key access.Programmatically update the IAM trust policy to manage cross-account vendor access.

Correct Answer: A

QUESTION 3

A Developer is building a serverless application that uses Amazon API Gateway as the front end. The application will not be publicly accessible. Other legacy applications running on Amazon EC2 will make calls to the application A Security Engineer Has been asked to review the security controls for authentication and authorization of the application

Which combination of actions would provide the MOST secure solution? (Select TWO)

A. Configure an IAM policy that allows the least permissive actions to communicate with the API Gateway Attach the policy to the role used by the legacy EC2 instances

B. Enable AWS WAF for API Gateway Configure rules to explicitly allow connections from the legacy EC2 instances

C. Create a VPC endpoint for API Gateway Attach an IAM resource policy that allows the role of the legacy EC2 instances to call specific APIs

D. Create a usage plan Generate a set of API keys for each application that needs to call the API.

E. Configure cross-origin resource sharing (CORS) in each API Share the CORS information with the applications that call the API.

Correct Answer: AE

QUESTION 4

A company recently set up Amazon GuardDuty and is receiving a high number of findings from IP addresses within the company. A security engineer has verified that these IP addresses are trusted and allowed. Which combination of steps should the security engineer take to configure GuardDuty so that it does not produce findings for these IP addresses? (Choose two.)

A. Create a plaintext configuration file that contains the trusted IP addresses.

B. Create a JSON configuration file that contains the trusted IP addresses.

C. Upload the configuration file directly to GuardDuty.

D. Upload the configuration file to Amazon S3. Add a new trusted IP list to GuardDuty that points to the file.

E. Manually copy and paste the configuration file data into the trusted IP list in GuardDuty.

Correct Answer: DE

QUESTION 5

A company Is planning to use Amazon Elastic File System (Amazon EFS) with its on-premises servers. The company has an existing AWS Direct Connect connection established between its on-premises data center and an AWS Region Security policy states that the company\\'s on-premises firewall should only have specific IP addresses added to the allow list and not a CIDR range. The company also wants to restrict access so that only certain data center-based servers have access to Amazon EFS How should a security engineer implement this solution?

A. Add the file-system-id efs aws-region amazonaws com URL to the allow list for the data center firewall Install the AWS CLI on the data center-based servers to mount the EFS file system in the EFS security group add the data center IP range to the allow list Mount the EFS using the EFS file system name

B. Assign an Elastic IP address to Amazon EFS and add the Elastic IP address to the allow list for the data center firewall Install the AWS CLI on the data center-based servers to mount the EFS file system In the EFS security group, add the IP addresses of the data center servers to the allow list Mount the EFS using the Elastic IP address

C. Add the EFS file system mount target IP addresses to the allow list for the data center firewall In the EFS security

group, add the data center server IP addresses to the allow list Use the Linux terminal to mount the EFS file system using the IP address of one of the mount targets

D. Assign a static range of IP addresses for the EFS file system by contacting AWS Support In the EFS security group add the data center server IP addresses to the allow list Use the Linux terminal to mount the EFS file system using one of the static IP addresses

Correct Answer: B

QUESTION 6

You are planning on using the AWS KMS service for managing keys for your application. For which of the following can the KMS CMK keys be used for encrypting? Choose 2 answers from the options given below

Please select:

A. Image Objects

B. Large files

C. Password

D. RSA Keys

Correct Answer: CD

The CMK keys themselves can only be used for encrypting data that is maximum 4KB in size. Hence it can be used for encryptii information such as passwords and RSA keys. Option A and B are invalid because the actual CMK key can only be used to encrypt small amounts of data and not large amoui of data. You have to generate the data key from the CMK key in order to encrypt high amounts of data For more information on the concepts for KMS, please visit the following URL: https://docs.aws.amazon.com/kms/latest/developereuide/concepts.htmll The correct answers are: Password, RSA Keys

QUESTION 7

A Lambda function reads metadata from an S3 object and stores the metadata in a DynamoDB table. The function is

triggered whenever an object is stored within the S3 bucket.

How should the Lambda function be given access to the DynamoDB table?

Please select:

A. Create a VPC endpoint for DynamoDB within a VPC. Configure the Lambda function to access resources in the VPC.

B. Create a resource policy that grants the Lambda function permissions to write to the DynamoDB table. Attach the poll to the DynamoDB table.

C. Create an IAM user with permissions to write to the DynamoDB table. Store an access key for that user in the Lambda environment variables.

D. Create an IAM service role with permissions to write to the DynamoDB table. Associate that role with the Lambda

function.

Correct Answer: D

The ideal way is to create an IAM role which has the required permissions and then associate it with the Lambda function The AWS Documentation additionally mentions the following Each Lambda function has an IAM role (execution role) associated with it. You specify the IAM role when you create your Lambda function. Permissions you grant to this role determine what AWS Lambda can do when it assumes the role. There are two types of permissions that you grant to the IAM role: If your Lambda function code accesses other AWS resources, such as to read an object from an S3 bucket or write logs to CloudWatch Logs, you need to grant permissions for relevant Amazon S3 and CloudWatch actions to the role. If the event source is stream-based (Amazon Kinesis Data Streams and DynamoDB streams), AWS Lambda polls these streams on your behalf. AWS Lambda needs permissions to poll the stream and read new records on the stream so you need to grant the relevant permissions to this role. Option A is invalid because the VPC endpoint allows access instances in a private subnet to access DynamoDB Option B is invalid because resources policies are present for resources such as S3 and KMS, but not AWS Lambda Option C is invalid because AWS Roles should be used and not IAM Users For more information on the Lambda permission model, please visit the below URL: https://docs.aws.amazon.com/lambda/latest/dg/intro-permission-model.html The correct answer is: Create an IAM service role with permissions to write to the DynamoDB table. Associate that role with the Lambda function.

QUESTION 8

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 9

Developers in an organization have moved from a standard application deployment to containers. The Security Engineer is tasked with ensuring that the containers are secure. Which strategies will reduce the attack surface and enhance the security of the containers? (Select TWO.)

A. Use the containers to automate security deployments.

B. Limit resource consumption (CPU, memory), networking connections, ports, and unnecessary container libraries.

C. Segregate containers by host, function, and data classification.

D. Use Docker Notary framework to sign task definitions.

E. Enable container breakout at the host kernel.

Correct Answer: AC

QUESTION 10

Which option for the use of the AWS Key Management Service (KMS) supports key management best practices that focus on minimizing the potential scope of data exposed by a possible future key compromise?

A. Use KMS automatic key rotation to replace the master key, and use this new master key for future encryption operations without re-encrypting previously encrypted data.

B. Generate a new Customer Master Key (CMK), re-encrypt all existing data with the new CMK, and use it for all future encryption operations.

C. Change the CMK alias every 90 days, and update key-calling applications with the new key alias.

D. Change the CMK permissions to ensure that individuals who can provision keys are not the same individuals who can use the keys.

Correct Answer: B

"automatic key rotation has no effect on the data that the CMK protects. It does not rotate the data keys that the CMK generated or re-encrypt any data protected by the CMK, and it will not mitigate the effect of a compromised data key. You might decide to create a new CMK and use it in place of the original CMK. This has the same effect as rotating the key material in an existing CMK, so it\\'s often thought of as manually rotating the key." https://docs.aws.amazon.com/kms/ latest/developerguide/rotate-keys.html

QUESTION 11

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 12

A security engineer is attempting to assign a virtual multi-factor authentication (MFA) device to an IAM user whose current virtual MFA device is faulty. The security engineer receives an error message that indicates that the security engineer is not authorized to perform iam:DeleteVirtualMFADevice.

The IAM role that the security engineer is using has the correct permissions to delete, list, and create a virtual MFA device. The IAM user also has permissions to delete their own virtual MFA device, but only if the IAM user is authenticated with MFA.

What should the security engineer do to resolve this issue?

A. Modify the policy for the IAM user to allow the IAM user to delete the virtual MFA device without using MFA authentication.

B. Sign in as the AWS account root user. Modify the MFA device by using the IAM console to generate a new synchronization quick response (QR) code.

C. Use the AWS CLI or AWS API to find the ARN of the virtual MFA device and to delete the device.

D. Sign in as the AWS account root user. Delete the virtual MFA device by using the IAM console.

Correct Answer: D

QUESTION 13

Your company is planning on developing an application in AWS. This is a web based application. The application users 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: B

The AWS Documentation mentions the following The AWS Documentation mentions the following OIDC identity providers are entities in IAM that describe an identity provider (IdP) service that supports the OpenID Connect (OIDC) standard. You use an OIDC identity provider when you want to establish trust between an OIDC-compatible IdP--such

as Google, Salesforce, and many others--and your AWS account This is useful if you are creating a mobile app or web application that requires access to AWS resources, but you don\\'t want to create custom sign-in code or manage your own user identities Option A is invalid because in the security groups you would not mention this information/ Option C is invalid because SAML is used for federated authentication Option D is invalid because you need to use the OIDC identity provider in AWS For more information on ODIC identity providers, please refer to the below Link: https://docs.aws.amazon.com/IAM/latest/UserGuide/id roles providers create oidc.html The correct answer is: Create an OIDC identity provider in AWS

QUESTION 14

A company is running a dynamic website by using an Application Load Balancer (ALB). A security engineer notices that bots from different IP addresses are using brute-force attacks to invoke a service endpoint frequently. What is the FASTEST way to mitigate this problem?

A. Create an AWS Lambda function to process ALB logs. Block the bots' IP addresses in the ALB\\'s security group.

B. Create an AWS WAF web ACL for the ALB. Add a rate-based rule to the web ACL to block the bots.

C. Create an ALB listener rule. Combine source-ip and path-pattern as the conditions to match bots. Specify a fixed-response action to return an HTTP 403 status.

D. Create an AWS WAF web ACL for the ALB. Add a rate-based rule to a rule group to block the bots. Attach the rule to the web ACL.

Correct Answer: A

QUESTION 15

Your company has defined privileged users for their AWS Account. These users are administrators for key resources defined in the company. There is now a mandate to enhance the security authentication for these users. How can this be accomplished?

Please select:

A. Enable MFA for these user accounts

B. Enable versioning for these user accounts

C. Enable accidental deletion for these user accounts

D. Disable root access for the users

Correct Answer: A

The AWS Documentation mentions the following as a best practices for IAM users. For extra security, enable multi-factor authentication (MFA) for privileged IAM users (users who are allowed access to sensitive resources or APIs). With MFA, users have a device that generates unique authentication code (a one-time password, or OTP). Users must provide both their normal credentials (like their user name and password) and the OTP. The MFA device can either be a special piece of hardware, or it can be a virtual device (for example, it can run in an app on a smartphone). Option B,C and D are invalid because no such security options are available in AWS For more information on IAM best practices, please visit the below URL https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html The correct answer

is: Enable MFA for these user accounts