SCS-C02$^{\text{Q\&As}}$

AWS Certified Security - Specialty

Pass Amazon SCS-C02 Exam with 100% Guarantee

Following Questions and Answers are all new published by Amazon Official Exam Center

QUESTION 1

A company\\'s Chief Security Officer has requested that a Security Analyst review and improve the security posture of each company IAM account The Security Analyst decides to do this by Improving IAM account root user security.

Which actions should the Security Analyst take to meet these requirements? (Select THREE.)

A. Delete the access keys for the account root user in every account.

B. Create an admin IAM user with administrative privileges and delete the account root user in every account.

C. Implement a strong password to help protect account-level access to the IAM Management Console by the account root user.

D. Enable multi-factor authentication (MFA) on every account root user in all accounts.

E. Create a custom IAM policy to limit permissions to required actions for the account root user and attach the policy to the account root user.

F. Attach an IAM role to the account root user to make use of the automated credential rotation in IAM STS.

Correct Answer: ADE

because these are the actions that can improve IAM account root user security. IAM account root user is a user that has complete access to all AWS resources and services in an account. IAM account root user security is a set of best practices that help protect the account root user from unauthorized or accidental use. Deleting the access keys for the account root user in every account can help prevent programmatic access by the account root user, which reduces the risk of compromise or misuse. Enabling MFA on every account root user in all accounts can help add an extra layer of security for console access by requiring a verification code in addition to a password. Creating a custom IAM policy to limit permissions to required actions for the account root user and attaching the policy to the account root user can help enforce the principle of least privilege and restrict the account root user from performing unnecessary or dangerous actions. The other options are either invalid or ineffective for improving IAM account root user security.

QUESTION 2

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 JSON script

D. Create an S3 bucket policy with unlimited access which includes each user\\'s IAM account ID

Correct Answer: B

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

QUESTION 3

A company deploys a distributed web application on a fleet of Amazon EC2 instances. The fleet is behind an Application Load Balancer (ALB) that will be configured to terminate the TLS connection. All TLS traffic to the ALB must stay secure, even if the certificate private key is compromised.

How can a security engineer meet this requirement?

A. Create an HTTPS listener that uses a certificate that is managed by IAM Certificate Manager (ACM).

B. Create an HTTPS listener that uses a security policy that uses a cipher suite with perfect toward secrecy (PFS).

C. Create an HTTPS listener that uses the Server Order Preference security feature.

D. Create a TCP listener that uses a custom security policy that allows only cipher suites with perfect forward secrecy (PFS).

Correct Answer: A

QUESTION 4

A company has a web server in the AWS Cloud. The company will store the content for the web server in an Amazon S3 bucket. A security engineer must use an Amazon CloudFront distribution to speed up delivery of the content. None of the files can be publicly accessible from the S3 bucket direct.

Which solution will meet these requirements?

A. Configure the permissions on the individual files in the S3 bucket so that only the CloudFront distribution has access to them.

B. Create an origin access identity (OAI). Associate the OAI with the CloudFront distribution. Configure the S3 bucket permissions so that only the OAI can access the files in the S3 bucket.

C. Create an S3 role in AWS Identity and Access Management (IAM). Allow only the CloudFront distribution to assume the role to access the files in the S3 bucket.

D. Create an S3 bucket policy that uses only the CloudFront distribution ID as the principal and the Amazon Resource Name (ARN) as the target.

Correct Answer: B

QUESTION 5

A security engineer is designing an IAM policy for a script that will use the AWS CLI. The script currently assumes an IAM role that is attached to three AWS managed IAM policies: AmazonEC2FullAccess, AmazonDynamoDBFullAccess, and Ama-zonVPCFullAccess.

The security engineer needs to construct a least privilege IAM policy that will replace the AWS managed IAM policies that are attached to this role.

Which solution will meet these requirements in the MOST operationally efficient way?

A. In AWS CloudTrail, create a trail for management events. Run the script with the existing AWS managed IAM policies. Use IAM Access Analyzer to generate a new IAM policy that is based on access activity in the trail. Replace the existing AWS managed IAM policies with the generated IAM poli-cy for the role.

B. Remove the existing AWS managed IAM policies from the role. Attach the IAM Access Analyzer Role Policy Generator to the role. Run the script. Return to IAM Access Analyzer and generate a least privilege IAM policy. Attach the new IAM policy to the role.

C. Create an account analyzer in IAM Access Analyzer. Create an archive rule that has a filter that checks whether the PrincipalArn value matches the ARN of the role. Run the script. Remove the existing AWS managed IAM poli-cies from the role.

D. In AWS CloudTrail, create a trail for management events. Remove the exist-ing AWS managed IAM policies from the role. Run the script. Find the au-thorization failure in the trail event that is associated with the script. Create a new IAM policy that includes the action and resource that caused the authorization failure. Repeat the process until the script succeeds. Attach the new IAM policy to the role.

Correct Answer: A

SCS-C02 PDF Dumps SCS-C02 VCE Dumps SCS-C02 Study Guide