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 recent security audit found that IAM CloudTrail logs are insufficiently protected from tampering and unauthorized access Which actions must the Security Engineer take to address these audit findings? (Select THREE)

A. Ensure CloudTrail log file validation is turned on

B. Configure an S3 lifecycle rule to periodically archive CloudTrail logs into Glacier for long- term storage

C. Use an S3 bucket with tight access controls that exists m a separate account

D. Use Amazon Inspector to monitor the file integrity of CloudTrail log files.

E. Request a certificate through ACM and use a generated certificate private key to encrypt CloudTrail log files

F. Encrypt the CloudTrail log files with server-side encryption with IAM KMS-managed keys (SSE-KMS)

Correct Answer: ADE

QUESTION 2

A company\\'s Security Engineer is copying all application logs to centralized Amazon S3 buckets. Currently, each of the company\\'s applications is in its own IAM account, and logs are pushed into S3 buckets associated with each account. The Engineer will deploy an IAM Lambda function into each account that copies the relevant log files to the centralized S3 bucket.

The Security Engineer is unable to access the log files in the centralized S3 bucket. The Engineer\\'s IAM user policy from the centralized account looks like this:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": "s3:Put*",
            "Resource":"arn:aws:s3:::centralizedbucket/*",
            "Effect": "Deny"
        },
        {
            "Action": ["s3:Get*","s3:List*"],
            "Resource": [
                "arn:aws:s3:::centralizedbucket/*",
                "arn:aws:s3:::centralizedbucket/"
            ],
            "Effect": "Allow"
        }
    ]
}
```

The centralized S3 bucket policy looks like this:

```
{
    "Version": "2012-10-17",    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::111122223333:role/LogCopier",
                    "arn:aws:iam::444455556666:role/LogCopier"
                ]
            },
            "Action": ["s3:PutObject","s3:PutObjectAcl"],
            "Resource": "arn:aws:s3:::centralizedbucket/*"
        }
    ]
}
```

Why is the Security Engineer unable to access the log files?

A. The S3 bucket policy does not explicitly allow the Security Engineer access to the objects in the bucket.

B. The object ACLs are not being updated to allow the users within the centralized account to access the objects

C. The Security Engineers IAM policy does not grant permissions to read objects in the S3 bucket

D. The s3:PutObject and s3:PutObjectAcl permissions should be applied at the S3 bucket level

Correct Answer: C

QUESTION 3

A Devops team is currently looking at the security aspect of their CI/CD pipeline. They are making use of IAM resource? for their infrastructure. They want to ensure that the EC2 Instances don\\'t have any high security vulnerabilities. They want to ensure a complete DevSecOps process. How can this be achieved?

A. Use IAM Config to check the state of the EC2 instance for any sort of security issues.

B. Use IAM Inspector API\\'s in the pipeline for the EC2 Instances

C. Use IAM Trusted Advisor API\\'s in the pipeline for the EC2 Instances

D. Use IAM Security Groups to ensure no vulnerabilities are present

Correct Answer: B

Amazon Inspector offers a programmatic way to find security defects or misconfigurations in your operating systems and applications. Because you can use API calls to access both the processing of assessments and the results of your assessments, integration of the findings into workflow and notification systems is simple. DevOps teams can integrate Amazon Inspector into their CI/CD pipelines and use it to identify any pre- existing issues or when new issues are introduced. Option A.C and D are all incorrect since these services cannot check for Security Vulnerabilities. These can only be checked by the IAM Inspector service. For more information on IAM Security best practices, please refer to below URL: https://d1.IAMstatic.com/whitepapers/Security/IAM Security Best Practices.pdl The correct answer is: Use

IAM Inspector API\\'s in the pipeline for the EC2 Instances Submit your Feedback/Queries to our Experts

QUESTION 4

A Security Engineer is implementing a solution to allow users to seamlessly encrypt Amazon S3 objects without having to touch the keys directly. The solution must be highly scalable without requiring continual management. Additionally, the organization must be able to immediately delete the encryption keys.

Which solution meets these requirements?

A. Use IAM KMS with IAM managed keys and the ScheduleKeyDeletion API with a PendingWindowInDays set to 0 to remove the keys if necessary.

B. Use KMS with IAM imported key material and then use the DeleteImportedKeyMaterial API to remove the key material if necessary.

C. Use IAM CloudHSM to store the keys and then use the CloudHSM API or the PKCS11 library to delete the keys if necessary.

D. Use the Systems Manager Parameter Store to store the keys and then use the service API operations to delete the key if necessary.

Correct Answer: B

https://docs.IAM.amazon.com/kms/latest/developerguide/importing-keys- delete-key-material.html

QUESTION 5

You need to establish a secure backup and archiving solution for your company, using IAM. Documents should be immediately accessible for three months and available for five years for compliance reasons. Which IAM service fulfills these requirements in the most cost-effective way? Choose the correct answer:

A. Upload data to S3 and use lifecycle policies to move the data into Glacier for long-term archiving.

B. Upload the data on EBS, use lifecycle policies to move EBS snapshots into S3 and later into Glacier for long-term archiving.

C. Use Direct Connect to upload data to S3 and use IAM policies to move the data into Glacier for long-term archiving.

D. Use Storage Gateway to store data to S3 and use lifecycle policies to move the data into Redshift for long-term archiving.

Correct Answer: A

amazon Glacier is a secure, durable, and extremely low-cost cloud storage service for data archiving and long-term backup. Customers can reliably store large or small amounts of data for as little as $0,004 per gigabyte per month, a significant savings compared to on-premises solutions. With Amazon lifecycle policies you can create transition actions in which you define when objects transition to another Amazon S3 storage class. For example, you may choose to transition objects to the STANDARDJA (IA, for infrequent access) storage class 30 days after creation, or archive objects to the GLACIER storage class one year after creation. Option B is invalid because lifecycle policies are not available for EBS volumes Option C is invalid because IAM policies cannot be used to move data to Glacier Option D is invalid because lifecycle policies is not used to move data to Redshif For more information on S3 lifecycle policies, please visit the URL: http://docs.IAM.amazon.com/AmazonS3/latest/dev/obiect-lifecycle-mgmt.html The correct answer

is: Upload data to S3 and use lifecycle policies to move the data into Glacier for long-term archiving. Submit your Feedback/Queries to our Experts

QUESTION 6

Your application currently use IAM Cognito for authenticating users. Your application consists of different types of users. Some users are only allowed read access to the application and others are given contributor access. How wou you manage the access effectively?

A. Create different cognito endpoints, one for the readers and the other for the contributors.

B. Create different cognito groups, one for the readers and the other for the contributors.

C. You need to manage this within the application itself

D. This needs to be managed via Web security tokens

Correct Answer: B

The IAM Documentation mentions the following You can use groups to create a collection of users in a user pool, which is often done to set the permissions for those users. For example, you can create separate groups for users who are readers, contributors, and editors of your website and app. Option A is incorrect since you need to create cognito groups and not endpoints Options C and D are incorrect since these would be overheads when you can use IAM Cognito For more information on IAM Cognito user groups please refer to the below Link: https://docs.IAM.amazon.com/coenito/latest/developersuide/cognito-user-pools-user- groups.htmll The correct answer is: Create different cognito groups, one for the readers and the other for the contributors. Submit your Feedback/Queries to our Experts

QUESTION 7

A company plans to migrate a sensitive dataset to Amazon S3. A Security Engineer must ensure that the data is encrypted at rest. The encryption solution must enable the company to generate its own keys without needing to manage key storage or the encryption process.

What should the Security Engineer use to accomplish this?

A. Server-side encryption with Amazon S3-managed keys (SSE-S3)

B. Server-side encryption with IAM KMS-managed keys (SSE-KMS)

C. Server-side encryption with customer-provided keys (SSE-C)

D. Client-side encryption with an IAM KMS-managed CMK

Correct Answer: B

Reference https://IAM.amazon.com/s3/faqs/

QUESTION 8

Your company has defined a number of EC2 Instances over a period of 6 months. They want to know if any of the

security groups allow unrestricted access to a resource. What is the best option to accomplish this requirement?

A. Use IAM Inspector to inspect all the security Groups

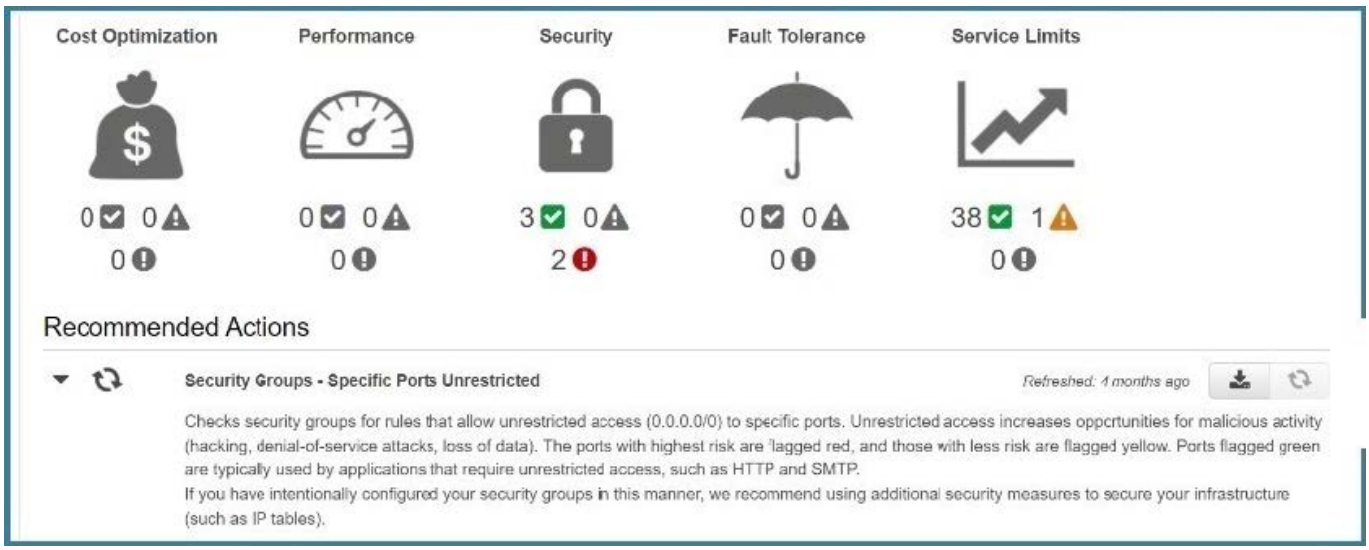
B. Use the IAM Trusted Advisor to see which security groups have compromised access.

C. Use IAM Config to see which security groups have compromised access.

D. Use the IAM CLI to query the security groups and then filter for the rules which have unrestricted accessd

Correct Answer: B

The IAM Trusted Advisor can check security groups for rules that allow unrestricted access to a resource. Unrestricted access increases opportunities for malicious activity (hacking, denial-of-service attacks, loss of data). If you go to IAM Trusted Advisor, you can see the details Option A is invalid because IAM Inspector is used to detect security vulnerabilities in instances and not for security groups. Option C is invalid because this can be used to detect changes in security groups but not show you security groups that have compromised access. Option Dis partially valid but would just be a maintenance overhead For more information on the IAM Trusted Advisor, please visit the below URL: https://IAM.amazon.com/premiumsupport/trustedadvisor/best-practices; The correct answer is: Use the IAM Trusted Advisor to see which security groups have compromised access. Submit your Feedback/Queries to our Experts



QUESTION 9

You have just received an email from IAM Support stating that your IAM account might have been compromised.

Which of the following steps would you look to carry out immediately? Choose 3 answers from the options below.

A. Change the root account password.

B. Rotate all IAM access keys

C. Keep all resources running to avoid disruption

D. Change the password for all IAM users.

Correct Answer: ABD

One of the articles from IAM mentions what should be done in such a scenario

If you suspect that your account has been compromised, or if you have received a notification from IAM that the account has been compromised, perform the following tasks:

Change your IAM root account password and the passwords of any IAM users. Delete or rotate all root and IAM Identity and Access Management (IAM) access keys. Delete any resources on your account you didn\\'t create, especially running

EC2 instances, EC2 spot bids, or IAM users.

Respond to any notifications you received from IAM Support through the IAM Support Center.

Option C is invalid because there could be compromised instances or resources running on your environment. They should be shutdown or stopped immediately. For more information on the article, please visit the below URL:

https://IAM.amazon.com/premiumsupport/knowledee-center/potential-account- compromise>

The correct answers are: Change the root account password. Rotate all IAM access keys. Change the password for all IAM users. Submit your Feedback/Queries to our Experts

QUESTION 10

A company wants to remove all SSH keys permanently from a specific subset of its Amazon Linux 2 Amazon EC2 instances that are using the same 1AM instance profile However three individuals who have IAM user accounts will need to access these instances by using an SSH session to perform critical duties

How can a security engineer provide the access to meet these requirements\\'?

A. Assign an 1AM policy to the instance profile to allow the EC2 instances to be managed by AWS Systems Manager Provide the 1AM user accounts with permission to use Systems Manager Remove the SSH keys from the EC2 instances Use Systems Manager Inventory to select the EC2 instance and connect

B. Assign an 1AM policy to the 1AM user accounts to provide permission to use AWS Systems Manager Run Command Remove the SSH keys from the EC2 instances Use Run Command to open an SSH connection to the EC2 instance

C. Assign an 1AM policy to the instance profile to allow the EC2 instances to be managed by AWS Systems Manager Provide the 1AM user accounts with permission to use Systems Manager Remove the SSH keys from the EC2 instances Use Systems Manager Session Manager to select the EC2 instance and connect

D. Assign an 1AM policy to the 1AM user accounts to provide permission to use the EC2 service in the AWS Management Console Remove the SSH keys from the EC2 instances Connect to the EC2 instance as the ec2-user through the AWS Management Console\\'s EC2 SSH client method

Correct Answer: C

To provide access to the three individuals who have IAM user accounts to access the Amazon Linux 2 Amazon EC2 instances that are using the same IAM instance profile, the most appropriate solution would be to assign an IAM policy to the instance profile to allow the EC2 instances to be managed by AWS Systems Manager, provide the IAM user accounts with permission to use Systems Manager, remove the SSH keys from the EC2 instances, and use Systems Manager Session Manager to select the EC2 instance and connect. References: : AWS Systems Manager Session Manager - AWS Systems Manager : AWS Systems Manager - AWS Management Console : AWS Identity and Access Management - AWS Management Console : Amazon Elastic Compute Cloud - Amazon Web Services : Amazon Linux 2 - Amazon Web Services : AWS Systems Manager - AWS Management Console : AWS Systems Manager - AWS Management Console : AWS Systems Manager - AWS Management Console

QUESTION 11

A company has a set of resources defined in IAM. It is mandated that all API calls to the resources be monitored. Also all API calls must be stored for lookup purposes. Any log data greater than 6 months must be archived. Which of the following meets these requirements? Choose 2 answers from the options given below. Each answer forms part of the solution.

A. Enable CloudTrail logging in all accounts into S3 buckets

B. Enable CloudTrail logging in all accounts into Amazon Glacier

C. Ensure a lifecycle policy is defined on the S3 bucket to move the data to EBS volumes after 6 months.

D. Ensure a lifecycle policy is defined on the S3 bucket to move the data to Amazon Glacier after 6 months.

Correct Answer: AD

Cloudtrail publishes the trail of API logs to an S3 bucket Option B is invalid because you cannot put the logs into Glacier from CloudTrail Option C is invalid because lifecycle policies cannot be used to move data to EBS volumes For more information on Cloudtrail logging, please visit the below URL: https://docs.IAM.amazon.com/IAMcloudtrail/latest/usereuide/cloudtrail-find-log-files.htmll You can then use Lifecycle policies to transfer data to Amazon Glacier after 6 months For more information on S3 lifecycle policies, please visit the below URL: https://docs.IAM.amazon.com/AmazonS3/latest/dev/object-lifecycle-mgmt.html The correct answers are: Enable CloudTrail logging in all accounts into S3 buckets. Ensure a lifecycle policy is defined on the bucket to move the data to Amazon Glacier after 6 months. Submit your Feedback/Queries to our Experts

QUESTION 12

A Systems Administrator has written the following Amazon S3 bucket policy designed to allow access to an S3 bucket for only an authorized IAM IAM user from the IP address range 10.10.10.0/24:

```
{
  "Version": "2012-10-17",
  "Id": "S3Policy1",
  "Statement": [
  {
   "Sid": ["OfficeAllowIP"],
   "Effect": ["Allow"],
   "Principal": ["*"],
   "Action": ["s3:*"],
   "Resource": ["arn:aws:s3:::Bucket"],
   "Condition": {
     "IpAddress": [
       {"aws: SourceIp": "10.10.10.0/24"}
      ]
     }
   }]
}
```

When trying to download an object from the S3 bucket from 10.10.10.40, the IAM user receives an access denied message. What does the Administrator need to change to grant access to the user?

A. Change the "Resource" from "arn: IAM:s3:::Bucket" to "arn:IAM:s3:::Bucket/*".

B. Change the "Principal" from "*" to {IAM:"arn:IAM:iam: : account-number: user/username"}

C. Change the "Version" from "2012-10-17" to the last revised date of the policy

D. Change the "Action" from ["s3:*"] to ["s3:GetObject", "s3:ListBucket"]

Correct Answer: A

QUESTION 13

A security engineer is designing an incident response plan to address the risk of a compromised Amazon EC2 instance. The plan must recommend a solution to meet the following requirements:

1.

A trusted forensic environment must be provisioned

2.

Automated response processes must be orchestrated

Which IAM services should be included in the plan? {Select TWO)

A. IAM CloudFormation

B. Amazon GuardDuty

C. Amazon Inspector

D. Amazon Macie

E. IAM Step Functions

Correct Answer: AE

QUESTION 14

A security engineer recently rotated all IAM access keys in an AWS account. The security engineer then configured AWS Config and enabled the following AWS

Config managed rules; mfa-enabled-for-iam-console-access, iam-user-mfa-enabled, access-key-rotated, and iam-user-unused-credentials-check.

The security engineer notices that all resources are displaying as noncompliant after the IAM GenerateCredentialReport API operation is invoked.

What could be the reason for the noncompliant status?

A. The IAM credential report was generated within the past 4 hours.

B. The security engineer does not have the GenerateCredentialReport permission.

C. The security engineer does not have the GetCredentialReport permission.

D. The AWS Config rules have a MaximumExecutionFrequency value of 24 hours.

Correct Answer: A

QUESTION 15

A company is storing data in Amazon S3 Glacier. A security engineer implemented a new vault lock policy for 10 TB of

data and called the initiate-vault-lock operation 12 hours ago. The audit team identified a typo in the policy that is allowing unintended access to the vault.

What is the MOST cost-effective way to correct this error?

A. Call the abort-vault-lock operation. Update the policy. Call the initiate-vault-lock operation again.

B. Copy the vault data to a new S3 bucket. Delete the vault. Create a new vault with the data.

C. Update the policy to keep the vault lock in place

D. Update the policy. Call the initiate-vault-lock operation again to apply the new policy.

Correct Answer: A

The most cost-effective way to correct a typo in a vault lock policy during the 24-hour initiation period is to call the abort-vault-lock operation. This action stops the vault lock process, allowing the security engineer to correct the policy and re-initiate the vault lock with the corrected policy. This approach avoids the need for data transfer or creating a new vault, thus minimizing costs and operational overhead.