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.geekcert.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 security team is creating a response plan in the event an employee executes unauthorized actions on AWS infrastructure. They want to include steps to determine if the employee\\'s IAM permissions changed as part of the incident.

What steps should the team document in the plan?

Please select:

A. Use AWS Config to examine the employee\\'s IAM permissions prior to the incident and compare them to the employee\\'s current IAM permissions.

B. Use Made to examine the employee\\'s IAM permissions prior to the incident and compare them to the employee\\'s A current IAM permissions.

C. Use CloudTrail to examine the employee\\'s IAM permissions prior to the incident and compare them to the employee\\'s current IAM permissions.

D. Use Trusted Advisor to examine the employee\\'s IAM permissions prior to the incident and compare them to the employee\\'s current IAM permissions.

Correct Answer: A

You can use the AWSConfig history to see the history of a particular item. The below snapshot shows an example configuration for a user in AWS Config

A.
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "secretsmanager:*",
            "Principal": {"AWS": "444455556666"},
            "Resource": "*"
        }
    ]
}
```

B.
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "secretsmanager:*",
            "Principal": {"AWS": "111122223333"},
            "Resource": "*"
        }
    ]
}
```

C.
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "secretsmanager:GetSecretValue",
            "Principal": {"AWS": "111122223333"},
            "Resource": "*"
        }
    ]
}
```

D.
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "secretsmanager:GetSecretValue",
            "Principal": {"AWS": "444455556666"},
            "Resource": "*"
        }
    ]
```

Option B,C and D are all invalid because these services cannot be used to see the history of a particular configuration item. This can only be accomplished by AWS Config. For more information on tracking changes in AWS Config, please visit the below URL: https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/TrackineChanees.htmll

The correct answer is: Use AWS Config to examine the employee\\'s IAM permissions prior to the incident and compare

them the employee\\'s current IAM permissions.

QUESTION 2

A company has decided to migrate sensitive documents from on-premises data centers to Amazon S3. Currently, the hard drives are encrypted to meet a compliance requirement regarding data encryption. The CISO wants to improve security by encrypting each file using a different key instead of a single key. Using a different key would limit the security impact of a single exposed key.

Which of the following requires the LEAST amount of configuration when implementing this approach?

A. Place each file into a different S3 bucket. Set the default encryption of each bucket to use a different AWS KMS customer managed key.

B. Put all the files in the same S3 bucket. Using S3 events as a trigger, write an AWS Lambda function to encrypt each file as it is added using different AWS KMS data keys.

C. Use the S3 encryption client to encrypt each file individually using S3-generated data keys

D. Place all the files in the same S3 bucket. Use server-side encryption with AWS KMS- managed keys (SSE-KMS) to encrypt the data

Correct Answer: A

QUESTION 3

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 4

Which approach will generate automated security alerts should too many unauthorized AWS API requests be identified?

A. Create an Amazon CloudWatch metric filter that looks for API call error codes and then implement an alarm based on that metric\\'s rate.

B. Configure AWS CloudTrail to stream event data to Amazon Kinesis. Configure an AWS Lambda function on the stream to alarm when the threshold has been exceeded.

C. Run an Amazon Athena SQL query against CloudTrail log files. Use Amazon QuickSight to create an operational dashboard.

D. Use the Amazon Personal Health Dashboard to monitor the account\\'s use of AWS services, and raise an alert if service error rates increase.

Correct Answer: A

https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudwatch-alarms-for-cloudtrail.html#cloudwatch-alarms-for-cloudtrail-authorization-failures Open the CloudWatch console at https://console.aws.amazon.com/cloudwatch/. In the navigation pane, choose Logs. In the list of log groups, select the check box next to the log group that you created for CloudTrail log events. Choose Create Metric Filter. On the Define Logs Metric Filter screen, choose Filter Pattern and then type the following: { ($.errorCode = "*UnauthorizedOperation") || ($.errorCode = "AccessDenied*") } Choose Assign Metric. For Filter Name, type AuthorizationFailures. For Metric Namespace, type CloudTrailMetrics. For Metric Name, type AuthorizationFailureCount.

QUESTION 5

A Security Engineer has been tasked with enabling AWS Security Hub to monitor Amazon EC2 instances fix CVE in a single AWS account The Engineer has already enabled AWS Security Hub and Amazon Inspector m the AWS Management Console and has installed me Amazon Inspector agent on an EC2 instances that need to be monitored.

Which additional steps should the Security Engineer lake 10 meet this requirement?

A. Configure the Amazon inspector agent to use the CVE rule package

B. Configure the Amazon Inspector agent to use the CVE rule package Configure Security Hub to ingest from AWS inspector by writing a custom resource policy

C. Configure the Security Hub agent to use the CVE rule package Configure AWS Inspector lo ingest from Security Hub by writing a custom resource policy

D. Configure the Amazon Inspector agent to use the CVE rule package Install an additional Integration library Allow the Amazon Inspector agent to communicate with Security Hub

Correct Answer: D