



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.passapply.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

You currently operate a web application in the AWS US-East region. The application runs on an auto-scaled layer of EC2 instances and an RDS Multi-AZ database. Your IT security compliance officer has tasked you to develop a reliable and durable logging solution to track changes made to your EC2, IAM, and RDS resources. The solution must ensure the integrity and confidentiality of your log data. Which of these solutions would you recommend?

Please select:

- A. Create a new CloudTrail trail with one new S3 bucket to store the logs and with the global services option selected. Use IAM roles, S3 bucket policies, and Multi Factor Authentication (MFA) Delete on the S3 bucket that stores your logs.
- B. Create a new CloudTrail with one new S3 bucket to store the logs. Configure SNS to send log file delivery notifications to your management system. Use IAM roles and S3 bucket policies on the S3 bucket that stores your logs.
- C. Create a new CloudTrail trail with an existing S3 bucket to store the logs and with the global services option selected. Use S3 ACLs and Multi Factor Authentication (MFA) Delete on the S3 bucket that stores your logs.
- D. Create three new CloudTrail trails with three new S3 buckets to store the logs: one for the AWS Management console, one for AWS SDKs, and one for command line tools. Use IAM roles and S3 bucket policies on the S3 buckets that store your logs.

Correct Answer: A

AWS Identity and Access Management (IAM) is integrated with AWS CloudTrail, a service that logs AWS events made by or on behalf of your AWS account. CloudTrail logs authenticated AWS API calls and also AWS sign-in events, and collects this event information in files that are delivered to Amazon S3 buckets. You need to ensure that all services are included. Hence option B is partially correct. Option B is invalid because you need to ensure that global services is selected. Option C is invalid because you should use bucket policies. Option D is invalid because you should ideally just create one S3 bucket. For more information on CloudTrail, please visit the below URL:

<http://docs.aws.amazon.com/IAM/latest/UserGuide/cloudtrail-integration.html> The correct answer is: Create a new CloudTrail trail with one new S3 bucket to store the logs and with the global services option selected. Use IAM roles, S3 bucket policies, and Multi Factor Authentication (MFA)

QUESTION 2

An organization has setup multiple IAM users. The organization wants that each IAM user accesses the IAM console only within the organization and not from outside. How can it achieve this?

Please select:

- A. Create an IAM policy with the security group and use that security group for AWS console login
- B. Create an IAM policy with a condition which denies access when the IP address range is not from the organization
- C. Configure the EC2 instance security group which allows traffic only from the organization's IP range
- D. Create an IAM policy with VPC and allow a secure gateway between the organization and AWS Console

Correct Answer: B

You can actually use a Deny condition which will not allow the person to log in from outside. The below example shows the Deny condition to ensure that any address specified in the source address is not allowed to access the resources in



aws. Option A is invalid because you don't mention the security group in the 1AM policy Option C is invalid because security groups by default don't allow traffic Option D is invalid because the 1AM policy does not have such an option For more information on 1AM policy conditions, please visit the URL:
<http://docs.aws.amazon.com/IAM/latest/UserGuide/accesspoliciesexamples.html#iam-policy-example-ec2-twocondition!>
The correct answer is: Create an 1AM policy with a condition which denies access when the IP address range is not from the organization

QUESTION 3

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 4

A security engineer needs to ensure their company's use of AWS meets AWS security best practices. As part of this, the AWS account root user must not be used for daily work. The root user must be monitored for use, and the security team must be alerted as quickly as possible if the root user is used.

Which solution meets these requirements?

- A. Set up an Amazon CloudWatch Events rule that triggers an Amazon SNS notification.
- B. Set up an Amazon CloudWatch Events rule that triggers an Amazon SNS notification logs from S3 and generate notifications using Amazon SNS.
- C. Set up a rule in AWS config to trigger root user events. Trigger an AWS Lambda function and generate notifications using Amazon SNS.
- D. Use Amazon Inspector to monitor the usage of the root user and generate notifications using Amazon SNS

Correct Answer: C



QUESTION 5

Your company has an external web site. This web site needs to access the objects in an S3 bucket. Which of the following would allow the web site to access the objects in the most secure manner?

Please select:

- A. Grant public access for the bucket via the bucket policy
- B. Use the aws:Referer key in the condition clause for the bucket policy
- C. Use the aws:sites key in the condition clause for the bucket policy
- D. Grant a role that can be assumed by the web site

Correct Answer: B

An example of this is given in the AWS Documentation Restricting Access to a Specific HTTP Referrer. Suppose you have a website with domain name (www.example.com or example.com) with links to photos and videos stored in your S3 bucket examplebucket. By default, all the S3 resources are private, so only the AWS account that created the resources can access them. To allow read access to these objects from your website, you can add a bucket policy that allows s3:GetObject permission with a condition, using the aws:referrer key, that the get request must originate from specific webpages. The following policy specifies the StringLike condition with the aws:Referer condition key.

```
{
  "Version": "2012-10-17",
  "Id": "http referer policy example",
  "Statement": [
    {
      "Sid": "Allow get requests originating from www.example.com and example.com.",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::examplebucket/*",
      "Condition": {
        "StringLike": {
          "aws:Referer": ["http://www.example.com/*", "http://example.com/*"]
        }
      }
    }
  ]
}
```



Option A is invalid because giving public access is not a secure way to provide access

Option C is invalid because aws:sites is not a valid condition key Option D is invalid because IAM roles will not be assigned to web sites For more information on example bucket policies please visit the below Link: 1
<https://docs.aws.amazon.com/AmazonS3/latest/dev/example-bucket-policies.html> The correct answer is: Use the aws:Referer key in the condition clause for the bucket policy

[SCS-C01 PDF Dumps](#)

[SCS-C01 Practice Test](#)

[SCS-C01 Exam Questions](#)



To Read the [Whole Q&As](#), please purchase the [Complete Version](#) from [Our website](#).

Try our product !

- 100% Guaranteed Success
- 100% Money Back Guarantee
- 365 Days Free Update
- Instant Download After Purchase
- 24x7 Customer Support
- Average 99.9% Success Rate
- More than 800,000 Satisfied Customers Worldwide
- Multi-Platform capabilities - [Windows](#), [Mac](#), [Android](#), [iPhone](#), [iPod](#), [iPad](#), [Kindle](#)

We provide exam PDF and VCE of Cisco, Microsoft, IBM, CompTIA, Oracle and other IT Certifications. You can view Vendor list of All Certification Exams offered:

<https://www.passapply.com/allproducts>

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket:



 <p>One Year Free Update Free update is available within One Year after your purchase. After One Year, you will get 50% discounts for updating. And we are proud to boast a 24/7 efficient Customer Support system via Email.</p>	 <p>Money Back Guarantee To ensure that you are spending on quality products, we provide 100% money back guarantee for 30 days from the date of purchase.</p>	 <p>Security & Privacy We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.</p>
---	---	--

Any charges made through this site will appear as Global Simulators Limited.
All trademarks are the property of their respective owners.
Copyright © passapply, All Rights Reserved.