# SCS-C01<sup>Q&As</sup>

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.pass2lead.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

**QUESTION 1**

For compliance reasons a Security Engineer must produce a weekly report that lists any instance that does not have the latest approved patches applied. The Engineer must also ensure that no system goes more than 30 days without the latest approved updates being applied

What would the MOST efficient way to achieve these goals?

A. Use Amazon inspector to determine which systems do not have the latest patches applied, and after 30 days, redeploy those instances with the latest AMI version

B. Configure Amazon EC2 Systems Manager to report on instance patch compliance and enforce updates during the defined maintenance windows

C. Examine AWS CloudTrail togs to determine whether any instances have not restarted in the last 30 days, and redeploy those instances

D. Update the AMIs with the latest approved patches and redeploy each instance during the defined maintenance window

Correct Answer: B

**QUESTION 2**

A company hosts its public website on Amazon EC2 instances behind an Application Load Balancer (ALB). The instances are in an EC2 Auto Scaling group across multiple Availability Zones. The website is under a DDoS attack by a specific loT device brand that is visible in the user agent A security engineer needs to mitigate the attack without impacting the availability of the public website.

What should the security engineer do to accomplish this?

A. Configure a web ACL rule for AWS WAF to block requests with a string match condition for the user agent of the loT device. Associate the v/eb ACL with the ALB.

B. Configure an Amazon CloudFront distribution to use the ALB as an origin. Configure a web ACL rule for AWS WAF to block requests with a string match condition for the user agent of the loT device. Associate the web ACL with the ALB Change the public DNS entry of the website to point to the CloudFront distribution.

C. Configure an Amazon CloudFront distribution to use a new ALB as an origin. Configure a web ACL rule for AWS WAF to block requests with a string match condition for the user agent of the loT device. Change the ALB security group to alow access from CloudFront IP address ranges only Change the public DNS entry of the website to point to the CloudFront distribution.

D. Activate AWS Shield Advanced to enable DDoS protection. Apply an AWS WAF ACL to the ALB. and configure a listener rule on the ALB to block loT devices based on the user agent.

Correct Answer: D

**QUESTION 3**

A company recently began using Amazon Route 53 as its DNS provider. The company must log public DNS queries that

Route 53 receives. The company has activated Route 53 public DNS query logging. The queries must be stored in a highly durable storage solution that deletes logs that are older than 1 year.

Which solution will meet these requirements MOST cost-effectively?

A. Configure Route 53 to export log data to Amazon S3. Configure an S3 Lifecycle policy that deletes objects in the target S3 bucket that are older than 1 year.

B. Configure Route 53 to export log data to Amazon S3. Configure an AWS Lambda function to run every hour to delete log files that are older than 1 year.

C. Configure Route 53 to export log data to Amazon CloudWatch Logs. For the target CloudWatch Logs log group, set the retention period to 1 year.

D. Configure Route 53 to export log data to Amazon CloudWatch Logs. Use CloudWatch Logs Insights to identify and delete log entries that are older than 1 year.

Correct Answer: A

**QUESTION 4**

Your IT Security team has advised to carry out a penetration test on the resources in their company\\'s AWS Account. This is as part of their capability to analyze the security of the Infrastructure. What should be done first in this regard?

Please select:

A. Turn on Cloud trail and carry out the penetration test

B. Turn on VPC Flow Logs and carry out the penetration test

C. Submit a request to AWS Support

D. Use a custom AWS Marketplace solution for conducting the penetration test

Correct Answer: C

This concept is given in the AWS Documentation How do I submit a penetration testing request for my AWS resources? Issue I want to run a penetration test or other simulated event on my AWS architecture. How do I get permission from AWS to do that? Resolution Before performing security testing on AWS resources, you must obtain approval from AWS. After you submit your request AWS will reply in about two business days. AWS might have additional questions about your test which can extend the approval process, so plan accordingly and be sure that your initial request is as detailed as possible. If your request is approved, you\\'ll receive an authorization number. Option A.B and D are all invalid because the first step is to get prior authorization from AWS for penetration tests For more information on penetration testing, please visit the below URL

*

https://aws.amazon.com/security/penetration-testing/

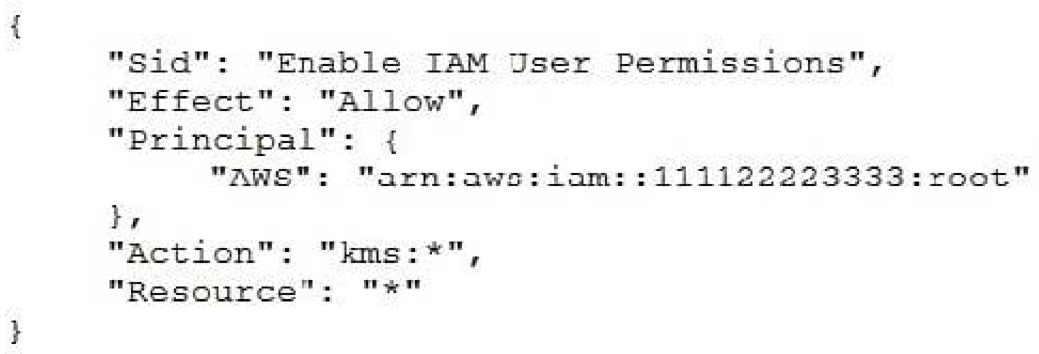
*

https://aws.amazon.com/premiumsupport/knowledge-center/penetration-testing/ ( The correct answer is: Submit a request to AWS Support

**QUESTION 5**

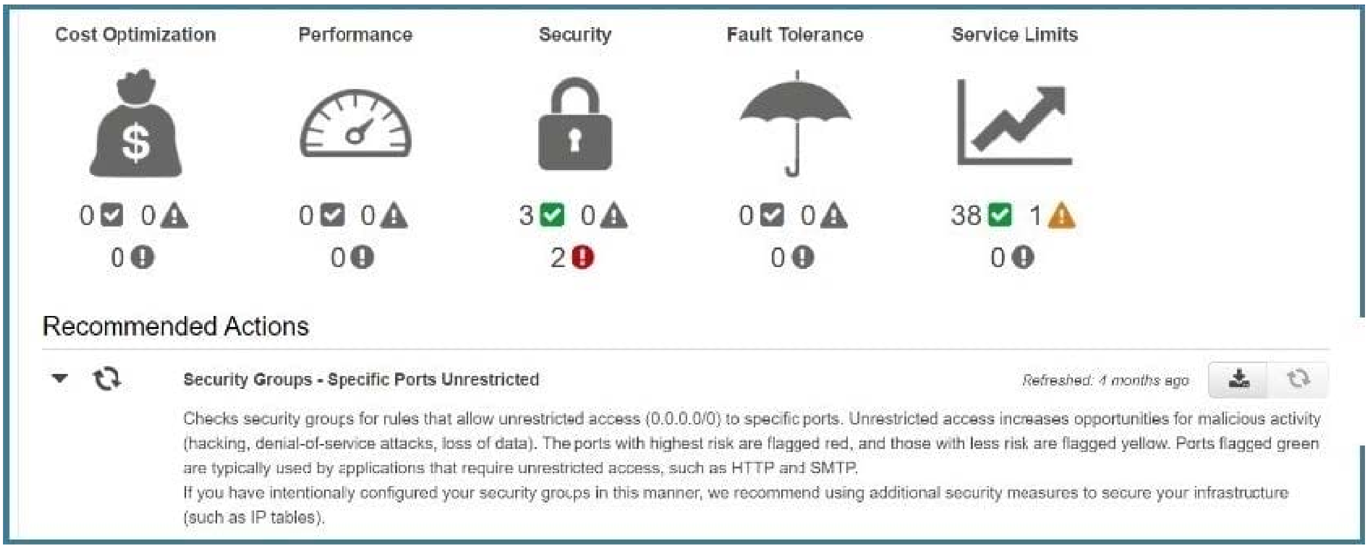
A company uses identity federation to authenticate users into an identity account (987654321987) where the users assume an IAM role named IdentityRole. The users then assume an IAM role named JobFunctionRole in the target AWS account (123456789123) to perform their job functions.

A user is unable to assume the IAM role in the target account. The policy attached to the role in the identity account is:



```
{
        "Sid": "Enable IAM User Permissions",
        "Effect": "Allow",
        "Principal": {
             "AWS": "arn:aws:iam::111122223333:root"
        },
        "Action": "kms:*",
        "Resource": "*"
}
```

What should be done to enable the user to assume the appropriate role in the target account?



Recommended Actions

Security Groups - Specific Ports Unrestricted

Refreshed: 4 months ago

Checks security groups for rules that allow unrestricted access (0.0.0.0/0) to specific ports. Unrestricted access increases opportunities for malicious activity (hacking, denial-of-service attacks, loss of data). The ports with highest risk are flagged red, and those with less risk are flagged yellow. Ports flagged green are typically used by applications that require unrestricted access, such as HTTP and SMTP.

If you have intentionally configured your security groups in this manner, we recommend using additional security measures to secure your infrastructure (such as IP tables).

A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: A

[Latest SCS-C01 Dumps](#) [SCS-C01 VCE Dumps](#) [SCS-C01 Study Guide](#)