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.lead4pass.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 company hosts data in S3. There is now a mandate that going forward all data in the S3 bucket needs to encrypt at rest. How can this be achieved? Please select:

A. Use AWS Access keys to encrypt the data

B. Use SSL certificates to encrypt the data

C. Enable server side encryption on the S3 bucket

D. Enable MFA on the S3 bucket

Correct Answer: C

The AWS Documentation mentions the following Server-side encryption is about data encryption at rest-that is, Amazon S3 encrypts your data at the object level as it writes it to disks in its data centers and decrypts it for you when you access it. As long as you authenticate your request and you have access

permissions, there is no difference in the way you access encrypted or unencrypted objects.

Options A and B are invalid because neither Access Keys nor SSL certificates can be used to encrypt

data.

Option D is invalid because MFA is just used as an extra level of security for S3 buckets For more

information on S3 server side encryption, please refer to the below Link:

https://docs.aws.amazon.com/AmazonS3/latest/dev/serv-side-encryption.html

QUESTION 2

A Security Analyst attempted to troubleshoot the monitoring of suspicious security group changes. The Analyst was told that there is an Amazon CloudWatch alarm in place for these AWS CloudTrail log events. The Analyst tested the monitoring setup by making a configuration change to the security group but did not receive any alerts.

Which of the following troubleshooting steps should the Analyst perform?

A. Ensure that CloudTrail and S3 bucket access logging is enabled for the Analyst\\'s AWS account.

B. Verify that a metric filter was created and then mapped to an alarm. Check the alarm notification action.

C. Check the CloudWatch dashboards to ensure that there is a metric configured with an appropriate dimension for security group changes.

D. Verify that the Analyst\\'s account is mapped to an IAM policy that includes permissions for cloudwatch: GetMetricStatistics and Cloudwatch: ListMetrics.

Correct Answer: B

MetricFilter:

Type: \\'AWS::Logs::MetricFilter\\'

Properties:

LogGroupName: \\'\\'

FilterPattern: >{ ($.eventName = AuthorizeSecurityGroupIngress) || ($.eventName = AuthorizeSecurityGroupEgress) ||

($.eventName =

RevokeSecurityGroupIngress) || ($.eventName = RevokeSecurityGroupEgress) || ($.eventName =

CreateSecurityGroup) || ($.eventName = DeleteSecurityGroup) } MetricTransformations:

-MetricValue: \\'1\\' MetricNamespace: CloudTrailMetrics MetricName: SecurityGroupEventCount

QUESTION 3

Your company has a requirement to work with a DynamoDB table. There is a security mandate that all data should be encrypted at rest. What is the easiest way to accomplish this for DynamoDB.

Please select:

A. Use the AWS SDK to encrypt the data before sending it to the DynamoDB table

B. Encrypt the DynamoDB table using KMS during its creation

C. Encrypt the table using AWS KMS after it is created

D. Use S3 buckets to encrypt the data before sending it to DynamoDB

Correct Answer: B

The most easiest option is to enable encryption when the DynamoDB table is created. The AWS Documentation mentions the following Amazon DynamoDB offers fully managed encryption at rest. DynamoDB encryption at rest provides enhanced security by encrypting your data at rest using an AWS Key Management Service (AWS KMS) managed encryption key for DynamoDB. This functionality eliminates the operational burden and complexity involved in protecting sensitive data. Option A is partially correct, you can use the AWS SDK to encrypt the data, but the easier option would be to encrypt the table before hand. Option C is invalid because you cannot encrypt the table after it is created Option D is invalid because encryption for S3 buckets is for the objects in S3 only. For more information on securing data at rest for DynamoDB please refer to below URL: https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/EncryptionAtRest.htmll The correct answer is: Encrypt the DynamoDB table using KMS during its creation

QUESTION 4

An organization receives an alert that indicates that an EC2 instance behind an ELB Classic Load Balancer has been compromised.

What techniques will limit lateral movement and allow evidence gathering?

A. Remove the instance from the load balancer and terminate it.

B. Remove the instance from the load balancer, and shut down access to the instance by tightening the security group.

C. Reboot the instance and check for any Amazon CloudWatch alarms.

D. Stop the instance and make a snapshot of the root EBS volume.

Correct Answer: B

https://d1.awsstatic.com/whitepapers/aws_security_incident_response.pdf

QUESTION 5

A Security Engineer is troubleshooting an issue with a company\\'s custom logging application. The application logs are written to an Amazon S3 bucket with event notifications enabled to send events lo an Amazon SNS topic. All logs are encrypted at rest using an AWS KMS CMK. The SNS topic is subscribed to an encrypted Amazon SQS queue. The logging application polls the queue for new messages that contain metadata about the S3 object. The application then reads the content of the object from the S3 bucket for indexing.

The Logging team reported that Amazon CloudWatch metrics for the number of messages sent or received is showing zero. No togs are being received.

What should the Security Engineer do to troubleshoot this issue?

A. Add the following statement to the AWS managed CMKs:

```
{
    "Sid": "Allow Amazon SNS to use this key",
    "Effect": "Allow",
    "Principal": {
        "Service": ["sns.amazonaws.com", "sqs.amazonaws.com", "s3.amazonaws.com"]
    },
    "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey*"
    ],
    "Resource": "*"
}
```

B. Add the following statement to the CMK key policy:

```
{
    "Sid": "Allow Amazon SNS to use this key",
    "Effect": "Allow",
    "Principal": {
        "Service": "sns.amazonaws.com"
    },
    "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey*"
    ],
    "Resource": "*"
}
```

Lead4Pass.com

C. Add the following statement to the CMK key policy:

```
{
    "Sid": "Allow Amazon SNS to use this key",
    "Effect": "Allow",
    "Principal": {
        "Service": "sqs.amazonaws.com"
    },
    "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey*"
    ],
    "Resource": "*"
}
```

D. Add the following statement to the CMK key policy:

```
{
    "Sid": "Allow Amazon SNS to use this key",
    "Effect": "Allow",
    "Principal": {
        "Service": "s3.amazonaws.com"
    },
    "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey*"
    ],
    "Resource": "*"
}
```

Lead4Pass.com

A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: D

QUESTION 6

Your team is experimenting with the API gateway service for an application. There is a need to implement a custom module which can be used for authentication/authorization for calls made to the API gateway. How can this be achieved?

Please select:

A. Use the request parameters for authorization

B. Use a Lambda authorizer

C. Use the gateway authorizer

D. Use CORS on the API gateway

Correct Answer: B

The AWS Documentation mentions the following An Amazon API Gateway Lambda authorizer (formerly known as a custom authorize?) is a Lambda function that you provide to control access to your API methods. A Lambda authorizer uses bearer token authentication strategies, such as OAuth or SAML. It can also use information described by headers, paths, query strings, stage variables, or context variables request parameters. Options A,C and D are invalid because these cannot be used if you need a custom authentication/authorization for calls made to the API gateway For more information on using the API gateway Lambda authorizer please visit the URL: https://docs.aws.amazon.com/apisateway/latest/developerguide/apieateway-use-lambda-authorizer.htmll The correct answer is: Use a Lambda authorizer

QUESTION 7

A Security Engineer launches two Amazon EC2 instances in the same Amazon VPC but in separate Availability Zones. Each instance has a public IP address and is able to connect to external hosts on the internet. The two instances are able to communicate with each other by using their private IP addresses, but they are not able to communicate with each other when using their public IP addresses.

Which action should the Security Engineer take to allow communication over the public IP addresses?

A. Associate the instances to the same security groups.

B. Add 0.0.0.0/0 to the egress rules of the instance security groups.

C. Add the instance IDs to the ingress rules of the instance security groups.

D. Add the public IP addresses to the ingress rules of the instance security groups.

Correct Answer: D

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/security-group-rules- reference.html#sg-rulesother-instances

QUESTION 8

A website currently runs on Amazon EC2 with mostly static content on the site. Recently, the site was subjected to a ODoS attack, and a Security Engineer was tasked with redesigning the edge security to help mitigate this risk in the future

What are some ways the Engineer could achieve this? (Select THREE)

A. Use AWS X-Ray to inspect the traffic going 10 the EC2 instances

B. Move the state content to Amazon S3 and font this with an Amazon CloudFront distribution

C. Change the security group configuration to block the source of the attack traffic

D. Use AWS WAF security rules to inspect the inbound traffic

E. Use Amazon inspector assessment templates to inspect the inbound traffic

F. Use Amazon Route 53 to distribute traffic

Correct Answer: BDF

QUESTION 9

A company has an encrypted Amazon S3 bucket. An Application Developer has an IAM policy that allows access to the S3 bucket, but the Application Developer is unable to access objects within the bucket.

What is a possible cause of the issue?

A. The S3 ACL for the S3 bucket fails to explicitly grant access to the Application Developer

B. The AWS KMS key for the S3 bucket fails to list the Application Developer as an administrator

C. The S3 bucket policy fails to explicitly grant access to the Application Developer

D. The S3 bucket policy explicitly denies access to the Application Developer

Correct Answer: C

QUESTION 10

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.

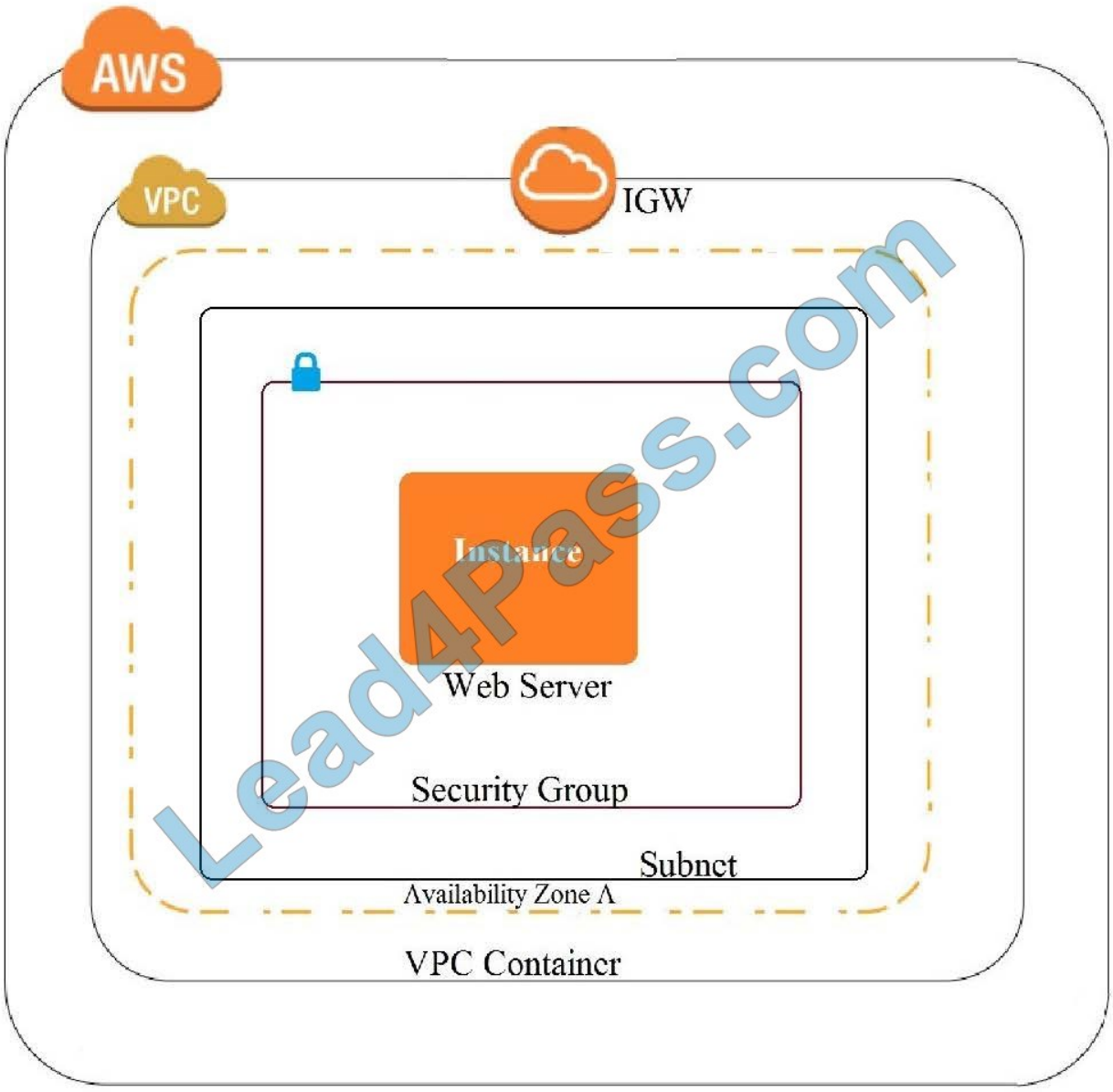
D. Activate AWS Shield Advanced to enable DDoS protection. Apply an AWS WAF ACL to the ALB. and configure a listener rule on the ALB to block loT devices based on the user agent.

Correct Answer: D

QUESTION 11

A company recently experienced a DDoS attack that prevented its web server from serving content. The website is static and hosts only HTML, CSS, and PDF files that users download.

Based on the architecture shown in the image, what is the BEST way to protect the site against future attacks while minimizing the ongoing operational overhead?



Lead4Pass.com

A. Move all the files to an Amazon S3 bucket. Have the web server serve the files from the S3 bucket.

B. Launch a second Amazon EC2 instance in a new subnet. Launch an Application Load Balancer in front of both instances.

C. Launch an Application Load Balancer in front of the EC2 instance. Create an Amazon CloudFront distribution in front of the Application Load Balancer.

D. Move all the files to an Amazon S3 bucket. Create a CloudFront distribution in front of the bucket and terminate the web server.

Correct Answer: D

https://docs.aws.amazon.com/AmazonS3/latest/dev/WebsiteHosting.html

QUESTION 12

A company is running an application on Amazon EC2 instances in an Auto Scaling group. The application stores logs locally A security engineer noticed that logs were lost after a scale-in event. The security engineer needs to recommend a solution to ensure the durability and availability of log data All logs must be kept for a minimum of 1 year for auditing purposes

What should the security engineer recommend?

A. Within the Auto Scaling lifecycle, add a hook to create and attach an Amazon Elastic Block Store (Amazon EBS) log volume each time an EC2 instance is created. When the instance is terminated, the EBS volume can be reattached to another instance for log review.

B. Create an Amazon Elastic File System (Amazon EFS) file system and add a command in the user data section of the Auto Scaling launch template to mount the EFS file system during EC2 instance creation Configure a process on the instance to copy the logs once a day from an instance Amazon Elastic Block Store (Amazon EBS) volume to a directory in the EFS file system.

C. Build the Amazon CloudWatch agent into the AMI used in the Auto Scaling group. Configure the CloudWatch agent to send the logs to Amazon CloudWatch Logs for review.

D. Within the Auto Scaling lifecycle, add a lifecycle hook at the terminating state transition and alert the engineering team by using a lifecycle notification to Amazon Simple Notification Service (Amazon SNS). Configure the hook to remain in the Terminating:Wait state for 1 hour to allow manual review of the security logs prior to instance termination.

Correct Answer: A

QUESTION 13

A Security Engineer receives alerts that an Amazon EC2 instance on a public subnet is under an SFTP brute force attack from a specific IP address, which is a known malicious bot. What should the Security Engineer do to block the malicious bot?

A. Add a deny rule to the public VPC security group to block the malicious IP

B. Add the malicious IP to AWS WAF backhsted IPs

C. Configure Linux iptables or Windows Firewall to block any traffic from the malicious IP D. Modify the hosted zone in

Amazon Route 53 and create a DNS sinkhole for the malicious IP

Correct Answer: D

Latest SCS-C01 Dumps SCS-C01 VCE Dumps SCS-C01 Study Guide

To Read the Whole Q&As, please purchase the Complete Version from Our website.

Try our product !

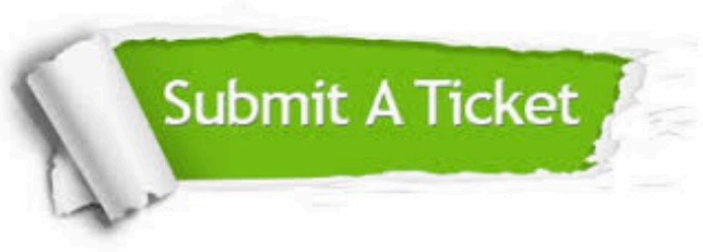
100% Guaranteed Success
100% Money Back Guarantee
365 Days Free Update
Instant Download After Purchase
24x7 Customer Support
Average 99.9% Success Rate
More than 800,000 Satisfied Customers Worldwide
Multi-Platform capabilities - Windows, Mac, Android, iPhone, iPod, iPad, Kindle

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.lead4pass.com/allproducts

Need Help

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



Any charges made through this site will appear as Global Simulators Limited.
All trademarks are the property of their respective owners.
Copyright © lead4pass, All Rights Reserved.