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.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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Development teams in your organization use S3 buckets to store the log files for various applications hosted ir development environments in AWS. The developers want to keep the logs for one month for troubleshooting purposes, and then purge the logs. What feature will enable this requirement?

Please select:

A. Adding a bucket policy on the S3 bucket.

B. Configuring lifecycle configuration rules on the S3 bucket.

C. Creating an IAM policy for the S3 bucket.

D. Enabling CORS on the S3 bucket.

Correct Answer: B

The AWS Documentation mentions the following on lifecycle policies Amazon Lifecycle configuration enables you to specify the lifecycle management of objects in a bucket. The configuration is a set of one or more rules, where each rule

defines an action for Amazon S3 to apply to a group of objects. These actions can be classified a follows:

Transition actions - In which you define when objects transition to another . 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. Expiration actions - In which you specify when the objects expire. Then Amazon S3 deletes the expired objects on your behalf.

Option A and C are invalid because neither bucket policies neither IAM policy\\'s can control the purging of logs

Option D is invalid CORS is used for accessing objects across domains and not for purging of logs For more information on AWS S3 Lifecycle policies, please visit the following URL:

com/AmazonS3/latest/d

The correct answer is: Configuring lifecycle configuration rules on the S3 bucket.

QUESTION 2

A company has multiple production AWS accounts. Each account has AWS CloudTrail configured to log to a single Amazon S3 bucket in a central account. Two of the production accounts have trails that are not logging anything to the S3 bucket.

Which steps should be taken to troubleshoot the issue? (Choose three.)

A. Verify that the log file prefix is set to the name of the S3 bucket where the logs should go.

B. Verify that the S3 bucket policy allows access for CloudTrail from the production AWS account IDs.

C. Create a new CloudTrail configuration in the account, and configure it to log to the account\\'s S3 bucket.

D. Confirm in the CloudTrail Console that each trail is active and healthy.

E. Open the global CloudTrail configuration in the master account, and verify that the storage location is set to the correct S3 bucket.

F. Confirm in the CloudTrail Console that the S3 bucket name is set correctly.

Correct Answer: BDF

QUESTION 3

A company is using HTTPS for all its public endpoints. A third-party certificate authority (CA) issues the certificates. The company imports the certificates and attaches the certificates to an Elastic Load Balancer or an Amazon CloudFront

distribution. The company also is using a third-party DNS hosting provider.

The certificates are near expiration. The company wants to migrate to AWS Certificate Manager (ACM) with automatic renewal. When the company adds the CNAME record during DNS validation, the certificate status changes to Failed.

What is the root cause of this issue?

A. DNS validation requires the domain to be hosted on Amazon Route 53.

B. Automatic renewal for domain validation requires the domain to be hosted on Amazon Route 53.

C. The domain has Certification Authority Authorization (CAA) DNS records that allow only specific certificate authorities.

D. DNS validation requires a TXT record instead of a CNAME record.

Correct Answer: D

QUESTION 4

A company created an AWS account for its developers to use for testing and learning purposes Because MM account will be shared among multiple teams of developers, the company wants to restrict the ability to stop and terminate Amazon EC2 instances so that a team can perform these actions only on the instances it owns.

Developers were Instructed to tag al their instances with a Team tag key and use the team name in the tag value One of the first teams to use this account is Business Intelligence A security engineer needs to develop a highly scalable solution for providing developers with access to the appropriate resources within the account The security engineer has already created individual 1AM roles for each team.

Which additional configuration steps should the security engineer take to complete the task?

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": "*"
}
```

A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: A

QUESTION 5

A company\\'s security engineer wants to receive an email alert whenever Amazon GuardDuty, AWS Identity and Access Management Access Analyzer, or Amazon Made generate a high-severity security finding. The company uses AWS Control Tower to govern all of its accounts. The company also uses AWS Security Hub with all of the AWS service integrations turned on.

Which solution will meet these requirements with the LEAST operational overhead?

A. Set up separate AWS Lambda functions for GuardDuty, IAM Access Analyzer, and Macie to call each service\\'s public API to retrieve high-severity findings. Use Amazon Simple Notification Service (Amazon SNS) to send the email alerts. Create an Amazon EventBridge rule to invoke the functions on a schedule.

B. Create an Amazon EventBridge rule with a pattern that matches Security Hub findings events with high severity. Configure the rule to send the findings to a target Amazon Simple Notification Service (Amazon SNS) topic. Subscribe the desired email addresses to the SNS topic.

C. Create an Amazon EventBridge rule with a pattern that matches AWS Control Tower events with high severity. Configure the rule to send the findings to a target Amazon Simple Notification Service (Amazon SNS) topic. Subscribe the desired email addresses to the SNS topic.

D. Host an application on Amazon EC2 to call the GuardDuty, IAM Access Analyzer, and Macie APIs. Within the application, use the Amazon Simple Notification Service (Amazon SNS) API to retrieve high-severity findings and to send the findings to an SNS topic. Subscribe the desired email addresses to the SNS topic.

Correct Answer: B

The AWS documentation states that you can create an Amazon EventBridge rule with a pattern that matches Security Hub findings events with high severity. You can then configure the rule to send the findings to a target Amazon Simple Notification Service (Amazon SNS) topic. You can subscribe the desired email addresses to the SNS topic. This method is the least operational overhead way to meet the requirements. References: AWS Security Hub User Guide