SCS-C02 Q&As

AWS Certified Security - Specialty

Pass Amazon SCS-C02 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/scs-c02.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Amazon Official Exam Center

QUESTION 1

A security team is responsible for reviewing IAM API call activity in the cloud environment for security violations. These events must be recorded and retained in a centralized location for both current and future IAM regions.

What is the SIMPLEST way to meet these requirements?

A. Enable IAM Trusted Advisor security checks in the IAM Console, and report all security incidents for all regions.

B. Enable IAM CloudTrail by creating individual trails for each region, and specify a single Amazon S3 bucket to receive log files for later analysis.

C. Enable IAM CloudTrail by creating a new trail and applying the trail to all regions. Specify a single Amazon S3 bucket as the storage location.

D. Enable Amazon CloudWatch logging for all IAM services across all regions, and aggregate them to a single Amazon S3 bucket for later analysis.

Correct Answer: C

Explanation: https://docs.IAM.amazon.com/IAMcloudtrail/latest/userguide/creating-trail- organization.html

QUESTION 2

In response to the past DDoS attack experiences, a Security Engineer has set up an Amazon CloudFront distribution for an Amazon S3 bucket. There is concern that some users may bypass the CloudFront distribution and access the S3 bucket directly.

What must be done to prevent users from accessing the S3 objects directly by using URLs?

A. Change the S3 bucket/object permission so that only the bucket owner has access.

B. Set up a CloudFront origin access identity (OAI), and change the S3 bucket/object permission so that only the OAI has access.

C. Create IAM roles for CloudFront, and change the S3 bucket/object permission so that only the IAM role has access.

D. Redirect S3 bucket access to the corresponding CloudFront distribution.

Correct Answer: B

https://docs.IAM.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content- restricting-access-to-s3.html

QUESTION 3

A company uses Amazon API Gateway to present REST APIs to users. An API developer wants to analyze API access patterns without the need to parse the log files. Which combination of steps will meet these requirements with the LEAST effort? (Select TWO.)

A. Configure access logging for the required API stage.

B. Configure an AWS CloudTrail trail destination for API Gateway events. Configure filters on the userIdentity, userAgent, and sourceIPAddress fields.

C. Configure an Amazon S3 destination for API Gateway logs. Run Amazon Athena queries to analyze API access information.

D. Use Amazon CloudWatch Logs Insights to analyze API access information.

E. Select the Enable Detailed CloudWatch Metrics option on the required API stage.

Correct Answer: CD

QUESTION 4

A company has an application hosted in an Amazon EC2 instance and wants the application to access secure strings stored in IAM Systems Manager Parameter Store When the application tries to access the secure string key value, it fails. Which factors could be the cause of this failure? (Select TWO.)

A. The EC2 instance role does not have decrypt permissions on the IAM Key Management Sen/ice (IAM KMS) key used to encrypt the secret

B. The EC2 instance role does not have read permissions to read the parameters In Parameter Store

C. Parameter Store does not have permission to use IAM Key Management Service (IAM KMS) to decrypt the parameter

D. The EC2 instance role does not have encrypt permissions on the IAM Key Management Service (IAM KMS) key associated with the secret

E. The EC2 instance does not have any tags associated.

Correct Answer: AB

Explanation: https://docs.IAM.amazon.com/systems-manager/latest/userguide/sysman- paramstore-access.html

QUESTION 5

A company created an IAM 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 IAM roles for each team.

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

A. For each team, create an AM policy similar to the one that fellows Populate the ec2:
ResourceTag/Team condition key with a proper team name Attach resulting policies to the corresponding IAM roles.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "NotAction": [
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ]
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/Team": "BusinessIntelligence"
                }
            }
        }
    ]
}
```

B. For each team create an IAM policy similar to the one that follows
Populate the IAM TagKeys/Team condition key with a proper team name.
Attach the resuming policies to the corresponding IAM roles.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "NotAction": [
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys/Team": "BusinessIntelligence"
                }
            }
        }
    ]
}
```

C. Tag each IAM role with a Team lag key. and use the team name in the tag value.
Create an IAM policy similar to the one that follows, and attach 4 to all the IAM roles used by developers.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "NotAction": [
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/Team": "${aws:PrincipalTag/Team}"
                }
            }
        }
    ]
}
```

D. Tag each IAM role with the Team key, and use the team name in the tag value.
Create an IAM policy similar to the one that follows, and it to all the IAM roles used by developers.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "NotAction": [
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys/Team": "${aws:PrincipalTag/Team}"
                }
            }
        }
    ]
}
```

A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: A