# SCS-C02<sup>Q&As</sup>

## AWS Certified Security - Specialty

## Pass Amazon SCS-C02 Exam with 100% Guarantee

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

**https://www.pass2lead.com/scs-c02.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 is building a data processing application mat uses AWS Lambda functions. The application\'s Lambda functions need to communicate with an Amazon RDS OB instance that is deployed within a VPC in the same AWS account

Which solution meets these requirements in the MOST secure way?

A. Configure the DB instance to allow public access Update the DB instance security group to allow access from the Lambda public address space for the AWS Region

B. Deploy the Lambda functions inside the VPC Attach a network ACL to the Lambda subnet Provide outbound rule access to the VPC CIDR range only Update the DB instance security group to allow traffic from 0.0.0.0/0

C. Deploy the Lambda functions inside the VPC Attach a security group to the Lambda functions Provide outbound rule access to the VPC CIDR range only Update the DB instance security group to allow traffic from the Lambda security group

D. Peer the Lambda default VPC with the VPC that hosts the DB instance to allow direct network access without the need for security groups

Correct Answer: C

This solution ensures that the Lambda functions are deployed inside the VPC and can communicate with the Amazon RDS DB instance securely. The security group attached to the Lambda functions only allows outbound traffic to the VPC CIDR range, and the DB instance security group only allows traffic from the Lambda security group. This solution ensures that the Lambda functions can communicate with the DB instance securely and that the DB instance is not exposed to the public internet.

---

**QUESTION 2**

A security engineer needs to create an Amazon S3 bucket policy to grant least privilege read access to IAM user accounts that are named User=1, User2. and User3. These IAM user accounts are members of the AuthorizedPeople IAM group. The security engineer drafts the following S3 bucket policy: When the security engineer tries to add the policy to the S3 bucket, the following error message appears: "Missing required field Principal." The security engineer is adding a Principal element to the policy. The addition must provide read access to only User1. User2, and User3.

```
{
    "Version": "2012-10-17",
    "Id": "AuthorizedPeoplePolicy",
    "Statement": [
        {
            "Sid": "Actions-Authorized-People",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": "arn:aws:s3:::authorized-people-bucket/*"
        }
    ]
}
```

Which solution meets these requirements?

A. Option A

```
"Principal": {
    "AWS": [
        "arn:aws:iam::1234567890:user/User1",
        "arn:aws:iam::1234567890:user/User2",
        "arn:aws:iam::1234567890:user/User3"
    ]
}
```

B. Option B

```
"Principal": {
    "AWS": [
        "arn:aws:iam::1234567890:root"
    ]
}
```

C. Option C

```
"Principal": {
    "AWS": [
        "*"
    ]
}
```

D. Option D

```
"Principal": {
    "AWS": "arn:aws:iam::1234567890:group/AuthorizedPeople"
}
```

A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: A

**QUESTION 3**

A company is testing its incident response plan for compromised credentials. The company runs a database on an Amazon EC2 instance and stores the sensitive data-base credentials as a secret in AWS Secrets Manager. The secret has rotation configured with an AWS Lambda function that uses the generic rotation function template. The EC2 instance and the Lambda function are deployed in the same pri-vate subnet. The VPC has a Secrets Manager VPC endpoint. A security engineer discovers that the secret cannot rotate. The security engi-neer determines that the VPC endpoint is working as intended. The Amazon Cloud-Watch logs contain the following error:

"setSecret: Unable to log into database".

Which solution will resolve this error?

A. Use the AWS Management Console to edit the JSON structure of the secret in Secrets Manager so that the secret automatically conforms with the struc-ture that the database requires.

B. Ensure that the security group that is attached to the Lambda function al-lows outbound connections to the EC2 instance. Ensure that the security group that is attached to the EC2 instance allows inbound connections from the security group that is attached to the Lambda function.

C. Use the Secrets Manager list-secrets command in the AWS CLI to list the secret. Identify the database credentials. Use the Secrets Manager rotate-secret command in the AWS CLI to force the immediate rotation of the se-cret.

D. Add an internet gateway to the VPC. Create a NAT gateway in a public sub-net. Update the VPC route tables so that traffic from the Lambda function and traffic from the EC2 instance can reach the Secrets Manager public endpoint.

Correct Answer: B

This answer is correct because ensuring that the security groups allow bidirectional communication between the Lambda function and the EC2 instance will resolve the error. The error indicates that the Lambda function cannot connect to the database, which might be due to firewall rules blocking the traffic. By allowing outbound connections from the Lambda function and inbound connections to the EC2 instance, the security engineer can enable the rotation function to access and update the database credentials.

**QUESTION 4**

A company wants to monitor the deletion of customer managed CMKs A security engineer must create an alarm that will notify the company before a CMK is deleted The security engineer has configured the integration of IAM CloudTrail with Amazon CloudWatch

What should the security engineer do next to meet this requirement?

A. Use inbound rule 100 to allow traffic on TCP port 443 Use inbound rule 200 to deny traffic on TCP port 3306 Use

outbound rule 100 to allow traffic on TCP port 443

B. Use inbound rule 100 to deny traffic on TCP port 3306. Use inbound rule 200 to allow traffic on TCP port range 1024-65535. Use outbound rule 100 to allow traffic on TCP port

C. Use inbound rule 100 to allow traffic on TCP port range 1024-65535 Use inbound rule 200 to deny traffic on TCP port 3306 Use outbound rule 100 to allow traffic on TCP port

D. Use inbound rule 100 to deny traffic on TCP port 3306 Use inbound rule 200 to allow traffic on TCP port 443 Use outbound rule 100 to allow traffic on TCP port 443

Correct Answer: A

**QUESTION 5**

A startup company is using a single AWS account that has resources in a single AWS Region. A security engineer configures an AWS Cloud Trail trail in the same Region to deliver log files to an Amazon S3 bucket by using the AWS CLI.

Because of expansion, the company adds resources in multiple Regions. The secu-rity engineer notices that the logs from the new Regions are not reaching the S3 bucket.

What should the security engineer do to fix this issue with the LEAST amount of operational overhead?

A. Create a new CloudTrail trail. Select the new Regions where the company added resources.

B. Change the S3 bucket to receive notifications to track all actions from all Regions.

C. Create a new CloudTrail trail that applies to all Regions.

D. Change the existing CloudTrail trail so that it applies to all Regions.

Correct Answer: D

The correct answer is D. Change the existing CloudTrail trail so that it applies to all Regions. According to the AWS documentation, you can configure CloudTrail to deliver log files from multiple Regions to a single S3 bucket for a single account. To change an existing single-Region trail to log in all Regions, you must use the AWS CLI and add the --is-multi-region-trail option to the update-trail command. This will ensure that you log global service events and capture all management event activity in your account. Option A is incorrect because creating a new CloudTrail trail for each Region will incur additional costs and increase operational overhead. Option B is incorrect because changing the S3 bucket to receive notifications will not affect the delivery of log files from other Regions. Option C is incorrect because creating a new CloudTrail trail that applies to all Regions will result in duplicate log files for the original Region and also incur additional costs.

[Latest SCS-C02 Dumps](#)          [SCS-C02 Exam Questions](#)          [SCS-C02 Braindumps](#)