SCS-C02Q&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.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 security engineer receives an IAM abuse email message. According to the message, an Amazon EC2 instance that is running in the security engineer\\'s IAM account is sending phishing email messages.

The EC2 instance is part of an application that is deployed in production. The application runs on many EC2 instances behind an Application Load Balancer. The instances run in an Amazon EC2 Auto Scaling group across multiple subnets and multiple Availability Zones.

The instances normally communicate only over the HTTP. HTTPS, and MySQL protocols. Upon investigation, the security engineer discovers that email messages are being sent over port 587. All other traffic is normal.

The security engineer must create a solution that contains the compromised EC2 instance, preserves forensic evidence for analysis, and minimizes application downtime. Which combination of steps must the security engineer take to meet these requirements? (Select THREE.)

A. Add an outbound rule to the security group that is attached to the compromised EC2 instance to deny traffic to 0.0.0.0/0 and port 587.

B. Add an outbound rule to the network ACL for the subnet that contains the compromised EC2 instance to deny traffic to 0.0.0.0/0 and port 587.

C. Gather volatile memory from the compromised EC2 instance. Suspend the compromised EC2 instance from the Auto Scaling group. Then take a snapshot of the compromised EC2 instance.

D. Take a snapshot of the compromised EC2 instance. Suspend the compromised EC2 instance from the Auto Scaling group. Then gather volatile memory from the compromised EC2 instance.

E. Move the compromised EC2 instance to an isolated subnet that has a network ACL that has no inbound rules or outbound rules.

F. Replace the existing security group that is attached to the compromised EC2 instance with a new security group that has no inbound rules or outbound rules.

Correct Answer: ACE

QUESTION 2

A company is using Amazon Route 53 Resolver for its hybrid DNS infrastructure. The company has set up Route 53 Resolver forwarding rules for authoritative domains that are hosted on on-premises DNS servers.

A new security mandate requires the company to implement a solution to log and query DNS traffic that goes to the on-premises DNS servers. The logs must show details of the source IP address of the instance from which the query originated. The logs also must show the DNS name that was requested in Route 53 Resolver.

Which solution will meet these requirements?

A. Use VPC Traffic Mirroring. Configure all relevant elastic network interfaces as the traffic source, include amazon-dns in the mirror filter, and set Amazon CloudWatch Logs as the mirror target. Use CloudWatch Insights on the mirror session logs to run queries on the source IP address and DNS name.

B. Configure VPC flow logs on all relevant VPCs. Send the logs to an Amazon S3 bucket. Use Amazon Athena to run SQL queries on the source IP address and DNS name.

C. Configure Route 53 Resolver query logging on all relevant VPCs. Send the logs to Amazon CloudWatch Logs. Use CloudWatch Insights to run queries on the source IP address and DNS name.

D. Modify the Route 53 Resolver rules on the authoritative domains that forward to the on-premises DNS servers. Send the logs to an Amazon S3 bucket. Use Amazon Athena to run SQL queries on the source IP address and DNS name.

Correct Answer: C

According to the AWS documentation, Route 53 Resolver query logging lets you log the DNS queries that Route 53 Resolver handles for your VPCs. You can send the logs to CloudWatch Logs, Amazon S3, or Kinesis Data Firehose. The logs include information such as the following:

The AWS Region where the VPC was created The ID of the VPC that the query originated from The IP address of the instance that the query originated from The instance ID of the resource that the query originated from The date and time that the query was first made The DNS name requested (such as prod.example.com) The DNS record type (such as A or AAAA) The DNS response code, such as NoError or ServFail The DNS response data, such as the IP address that is returned in response to the DNS query You can use CloudWatch Insights to run queries on your log data and analyze the results using graphs and statistics. You can filter and aggregate the log data based on any field, and use operators and functions to perform calculations and transformations. For example, you can use CloudWatch Insights to find out how many queries were made for a specific domain name, or which instances made the most queries. Therefore, this solution meets the requirements of logging and querying DNS traffic that goes to the on-premises DNS servers, showing details of the source IP address of the instance from which the query originated, and the DNS name that was requested in Route 53 Resolver.

The other options are incorrect because:

A. Using VPC Traffic Mirroring would not capture the DNS queries that go to the on-premises DNS servers, because Traffic Mirroring only copies network traffic from an elastic network interface of an EC2 instance to a target for analysis. Traffic Mirroring does not include traffic that goes through a Route 53 Resolver outbound endpoint, which is used to forward queries to on-premises DNS servers. Therefore, this solution would not meet the requirements. B. Configuring VPC flow logs on all relevant VPCs would not capture the DNS name that was requested in Route 53 Resolver, because flow logs only record information about the IP traffic going to and from network interfaces in a VPC. Flow logs do not include any information about the content or payload of a packet, such as a DNS query or response. Therefore, this solution would not meet the requirements. D. Modifying the Route 53 Resolver rules on the authoritative domains that forward to the on-premises DNS servers would not enable logging of DNS queries, because Resolver rules only specify how to forward queries for specified domain names to your network. Resolver rules do not have any logging functionality by themselves. Therefore, this solution would not meet the requirements.

References:

1: Resolver query logging -Amazon Route 53

2: Analyzing log data with CloudWatch Logs Insights -Amazon CloudWatch

3: What is Traffic Mirroring -Amazon Virtual Private Cloud

4: Outbound Resolver endpoints -Amazon Route 53

5: Logging IP traffic using VPC Flow Logs -Amazon Virtual Private Cloud

6: Managing forwarding rules -Amazon Route 53

QUESTION 3

A security engineer is troubleshooting an AWS Lambda function that is named MyLambdaFunction. The function is

encountering an error when the function attempts to read the objects in an Amazon S3 bucket that is named DOC-EXAMPLEBUCKET. The S3 bucket has the following bucket policy:

```
{
    "Effect": "Allow",
    "Principal": {
        "Service": "lambda.amazonaws.com"
    },
    "Action": "s3:GetObject",
    "Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET",
    "Condition": {
        "ArnLike": {
            "aws:SourceArn": "arn:aws:lambda:::function:MyLambdaFunction"
        }
    }
}
```

Which change should the security engineer make to the policy to ensure that the Lambda function can read the bucket objects?

A. Remove the Condition element. Change the Principal element to the following: { "AWS": "arn "aws" ::: lambda ::: function:MyLambdaFunction" }

B. Change the Action element to the following: " s3:GetObject*" " s3:GetBucket*"

C. Change the Resource element to "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*".

D. Change the Resource element to "arn:aws:lambda:::function:MyLambdaFunction". Change the Principal element to the following:

{

"Service": "s3.amazonaws.com"

}

Correct Answer: C

The correct answer is C. Change the Resource element to "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*".

The reason is that the Resource element in the bucket policy specifies which objects in the bucket are affected by the policy. In this case, the policy only applies to the bucket itself, not the objects inside it. Therefore, the Lambda function

cannot access the objects with the

s3:GetObject permission. To fix this, the Resource element should include a wildcard (*) to match all objects in the bucket. This way, the policy grants the Lambda function permission to read any object in the bucket.

The other options are incorrect for the following reasons:

A. Removing the Condition element would not help, because it only restricts access based on the source IP address of the request. The Principal element should not be changed to the Lambda function ARN, because it specifies who is allowed or denied access by the policy. The policy should allow access to any principal ("*") and rely on IAM roles or

policies to control access to the Lambda function. B. Changing the Action element to include s3:GetBucket* would not help, because it would grant additional permissions that are not needed by the Lambda function, such as s3:GetBucketAcl or s3:GetBucketPolicy. The s3:GetObject* permission is sufficient for reading objects in the bucket.

D. Changing the Resource element to the Lambda function ARN would not make sense, because it would mean that the policy applies to the Lambda function itself, not the bucket or its objects. The Principal element should not be changed to s3.amazonaws.com, because it would grant access to any AWS service that uses S3, not just Lambda.

QUESTION 4

A company\\'s Security Auditor discovers that users are able to assume roles without using multi-factor authentication (MFA). An example of a current policy being applied to these users is as follows:

```
{
    "Version": "2012-10-17",
    "Statement": [
    {
        "Effect": "Deny",
        "Principal": {
        "AWS": "arn:aws:iam::555555555555:root"
    },
        "Action": "sts:AssumeRole",
        "Condition": {
        "Bool": { "aws:MultiFactorAuthPresent": false}
            }
        }
    ]
}
```

The Security Auditor finds that the users who are able to assume roles without MFA are alt coming from the IAM CLI. These users are using long-term IAM credentials. Which changes should a Security Engineer implement to resolve this security issue? (Select TWO.)

A.
```
"Effect": "Deny",
"Condition": { "Bool": { "aws:MultiFactorAuthPresent": false} }
```

B.
```
"Effect": "Allow",
"Condition": { "Bool": { "aws:MultiFactorAuthPresent": true} }
```

C.
```
"Effect": "Allow","Condition": { "BoolIfExists": { "aws:MultiFactorAuthPresent": true} }
```

D.
```
"Effect": "Deny","Condition": { "BoolIfExists": { "aws:MultiFactorAuthPresent": false} }
```

E.
```
"Effect": "Deny","Condition": { "BoolIfNotExist": { "aws:MultiFactorAuthPresent": true} }
```

A. Option A

B. Option B

C. Option C

D. Option D

E. Option E

Correct Answer: AD

QUESTION 5

A security engineer is configuring a new website that is named example.com. The security engineer wants to secure communications with the website by requiring users to connect to example.com through HTTPS.

Which of the following is a valid option for storing SSL/TLS certificates?

A. Custom SSL certificate that is stored in AWS Key Management Service (AWS KMS)

B. Default SSL certificate that is stored in Amazon CloudFront.

C. Custom SSL certificate that is stored in AWS Certificate Manager (ACM)

D. Default SSL certificate that is stored in Amazon S3

Correct Answer: C