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.geekcert.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 Network Load Balancer (NLB) target instance is not entering the InService state. A security engineer determines that health checks are failing. Which factors could cause the health check failures? (Choose three.)

A. The target instance\\'s security group does not allow traffic from the NLB.

B. The target instance\\'s security group is not attached to the NLB.

C. The NLB\\'s security group is not attached to the target instance.

D. The target instance\\'s subnet network ACL does not allow traffic from the NLB.

E. The target instance\\'s security group is not using IP addresses to allow traffic from the NLB.

F. The target network ACL is not attached to the NLB.

Correct Answer: ADF

QUESTION 2

A Security Engineer has been asked to troubleshoot inbound connectivity to a web server. This single web server is not receiving inbound connections from the internet, whereas all other web servers are functioning properly.

The architecture includes network ACLs, security groups, and a virtual security appliance. In addition, the Development team has implemented Application Load Balancers (ALBs) to distribute the load across all web servers. It is a

requirement that traffic between the web servers and the internet flow through the virtual security appliance.

The Security Engineer has verified the following:

1.

The rule set in the Security Groups is correct

2.

The rule set in the network ACLs is correct

3.

The rule set in the virtual appliance is correct

Which of the following are other valid items to troubleshoot in this scenario? (Choose two.)

A. Verify that the 0.0.0.0/0 route in the route table for the web server subnet points to a NAT gateway.

B. Verify which Security Group is applied to the particular web server\\'s elastic network interface (ENI).

C. Verify that the 0.0.0.0/0 route in the route table for the web server subnet points to the virtual security appliance.

D. Verify the registered targets in the ALB.

E. Verify that the 0.0.0.0/0 route in the public subnet points to a NAT gateway.

Correct Answer: CD

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html

QUESTION 3

The CFO of a company wants to allow one of his employees to view only the AWS usage report page. Which of the below mentioned IAM policy statements allows the user to have access to the AWS usage report page?

Please select:

A. "Effect": "Allow". "Action": ["Describe"], "Resource": "Billing"

B. "Effect": "Allow", "Action": ["AccountUsage], "Resource": "*"

C. "Effect\\': "Allow", "Action": ["aws-portal:ViewUsage"," aws-portal:ViewBilling"], "Resource": "*"

D. "Effect": "Allow", "Action": ["aws-portal: ViewBilling"], "Resource": "*"

Correct Answer: C

the aws documentation, below is the access required for a user to access the Usage reports page and as per this, Option C is the right answer.

A. An SCP is attached to the account with the following permission statement:
[Missing the exhibit]

B. A permission boundary policy is attached to the System Administrator role with the following permission statement:
[Missing the exhibit]

C. A permission boundary is attached to the System Administrator role with the following permission statement:

D. An SCP is attached to the account with the following statement:

QUESTION 4

A company needs to encrypt all of its data stored in Amazon S3. The company wants to use AWS Key Management Service (AWS KMS) to create and manage its encryption keys. The company\\'s security policies require the ability to

Import the company\\'s own key material for the keys, set an expiration date on the keys, and delete keys immediately, if needed.

How should a security engineer set up AWS KMS to meet these requirements?

A. Configure AWS KMS and use a custom key store. Create a customer managed CMK with no key material Import the company\\'s keys and key material into the CMK

B. Configure AWS KMS and use the default Key store Create an AWS managed CMK with no key material Import the company\\'s key material into the CMK

C. Configure AWS KMS and use the default key store Create a customer managed CMK with no key material import the company\\'s key material into the CMK

D. Configure AWS KMS and use a custom key store. Create an AWS managed CMK with no key material. Import the company\\'s key material into the CMK.

Correct Answer: A

Reference: https://docs.aws.amazon.com/kms/latest/developerguide/overview.html

QUESTION 5

A company uses AWS Organizations. According to compliance requirements, the company\\'s applications that are hosted on Amazon EC2 instances must never use IAM credentials from Instance Metadata Service Version 1 (IMDSv1).

What should a security engineer do to meet this requirement?

A. Create a security group that denies access on HTTP to 169.254.169.254. Attach this security group to all EC2 instances.

B. Deactivate all access to IMDSv1 through the instance metadata options when using the AWS CLI, AWS API, or AWS Management Console to launch an EC2 instance.

C. Attach the following SCP to the root OU in AWS Organizations:

{

"Version": "2012-10-17",

"Statement": [

{

"Effect": "Deny",

"Action": "ec2:RunInstances",

"Resource": "arn:aws:ec2:*:*:instance/*",

"Condition": {

"StringNotEquals": {

"ec2:MetadataHttpTokens": "required"

}

}

}

]

}

D. Attach the following SCP to the root OU in AWS Organizations:

{

"Version": "2012-10-17",

"Statement": [

{

"Effect": "Deny",

"Action": "*",

"Resource": "*",

"Condition": {

"NumericLessThan": {

"ec2:RoleDelivery": "2.0"

}

}

}

]

}

Correct Answer: B