# SCS-C01<sup>Q&As</sup>

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**

A company wants to have an Intrusion detection system available for their VPC in AWS. They want to have complete control over the system. Which of the following would be ideal to implement? Please select:

A. Use AWS WAF to catch all intrusions occurring on the systems in the VPC

B. Use a custom solution available in the AWS Marketplace

C. Use VPC Flow logs to detect the issues and flag them accordingly.

D. Use AWS Cloudwatch to monitor all traffic

Correct Answer: B

Sometimes companies want to have custom solutions in place for monitoring Intrusions to their systems. In such a case, you can use the AWS Marketplace for looking at custom solutions.

```
A  Set up an AWS Organizations hierarchy, and replace the FullAWSAccess policy with the following Service Control
   Policy for the governed organization units:
   {
         "Version": "2012-10-17",
         "Statement": [
               {
                     "Action": [
                           "dynamodb:*", "rds:*", "ec2:*",
   "s3:*", "sts:*"
                     ],
                     "Effect": "Allow",
                     "Resource": "*"
               }
         ]
   }
```

Option A.C and D are all invalid because they cannot be used to conduct intrusion detection or prevention. For more information on using custom security solutions please visit the below URL
https://d1.awsstatic.com/Marketplace/security/AWSMP_Security_Solution%200verview.pdf For more information on using custom security solutions please visit the below URL: https://d1 .awsstatic.com/Marketplace/security/AWSMP Security Solution%20Overview.pdf

The correct answer is: Use a custom solution available in the AWS Marketplace

---

**QUESTION 2**

A company is planning on extending their on-premise AWS Infrastructure to the AWS Cloud. They need to have a solution that would give core benefits of traffic encryption and ensure latency is kept to a minimum. Which of the following would help fulfil this requirement? Choose 2 answers from the options given below
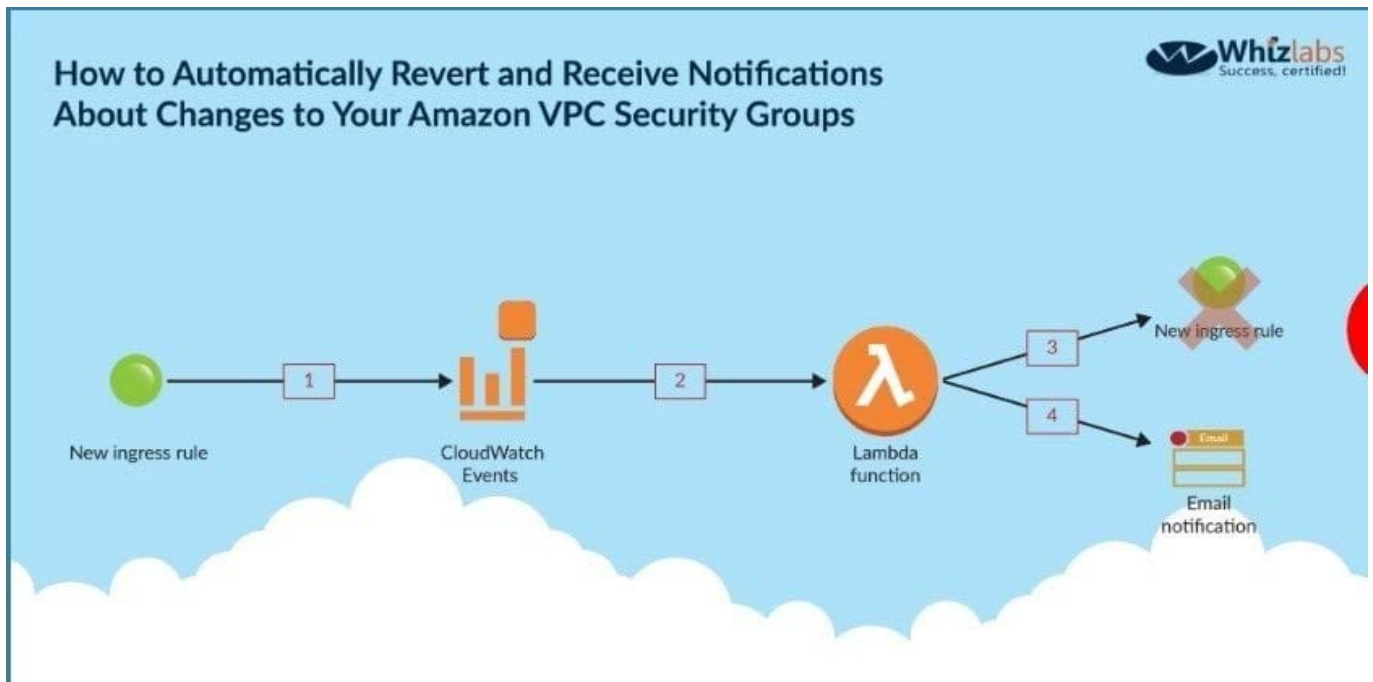
Please select:

A. AWS VPN

B. AWS VPC Peering

C. AWS NAT gateways

D. AWS Direct Connect

Correct Answer: AD

The AWS Document mention the following which supports the requirement



Option B is invalid because VPC peering is only used for connection between VPCs and cannot be used to connect On-premise infrastructure to the AWS Cloud. Option C is invalid because NAT gateways is used to connect instances in a private subnet to the internet For more information on VPN Connections, please visit the following url https://docs.aws.amazon.com/AmazonVPC/latest/UserGuideA/pn-connections.html The correct answers are: AWS VPN, AWS Direct Connect

**QUESTION 3**

A company uses AWS Organization to manage 50 AWS accounts. The finance staff members log in as AWS IAM users in the FinanceDept AWS account. The staff members need to read the consolidated billing information in the MasterPayer AWS account. They should not be able to view any other resources in the MasterPayer AWS account. IAM access to billing has been enabled in the MasterPayer account.

Which of the following approaches grants the finance staff the permissions they require without granting any unnecessary permissions?

A. Create an IAM group for the finance users in the FinanceDept account, then attach the AWS managed ReadOnlyAccess IAM policy to the group.

B. Create an IAM group for the finance users in the MasterPayer account, then attach the AWS managed ReadOnlyAccess IAM policy to the group.

![Pass2Lead Logo](https://Pass2Lead.com)
C. Create an AWS IAM role in the FinanceDept account with the ViewBilling permission, then grant the finance users in the MasterPayer account the permission to assume that role.

D. Create an AWS IAM role in the MasterPayer account with the ViewBilling permission, then grant the finance users in the FinanceDept account the permission to assume that role.

Correct Answer: D

AWS Region that You Request a Certificate In (for AWS Certificate Manager) If you want to require HTTPS between viewers and CloudFront, you must change the AWS region to US East (N. Virginia) in the AWS Certificate Manager console before you request or import a certificate. If you want to require HTTPS between CloudFront and your origin, and you\\'re using an ELB load balancer as your origin, you can request or import a certificate in any region. https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/cnames-and-https-requirements.html

**QUESTION 4**

Which of the following are valid configurations for using SSL certificates with Amazon CloudFront? (Select THREE )

A. Default AWS Certificate Manager certificate

B. Custom SSL certificate stored in AWS KMS

C. Default CloudFront certificate

D. Custom SSL certificate stored in AWS Certificate Manager

E. Default SSL certificate stored in AWS Secrets Manager

F. Custom SSL certificate stored in AWS IAM

Correct Answer: CDF

ACM(recommended) lets you import third-party certificates from the ACM console, as well as programmatically. (Not recommended) Use the Amazon CLI command to upload your third-party certificate to the IAM certificate store. You can use their default SSL certificate by accessing the distribution as .cloudfront.net

**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"

}

}

}

]

![Pass2Lead](https://Pass2Lead.com)
}

Correct Answer: B