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.geekcert.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

You want to launch an EC2 Instance with your own key pair in IAM. How can you achieve this? Choose 3 answers from the options given below.

A. Use a third party tool to create the Key pair

B. Create a new key pair using the IAM CLI

C. Import the public key into EC2

D. Import the private key into EC2

Correct Answer: ABC

This is given in the IAM Documentation Creating a Key Pair You can use Amazon EC2 to create your key pair. For more information, see Creating a Key Pair Using Amazon EC2. Alternatively, you could use a third-party tool and then import the public key to Amazon EC2. For more information, see Importing Your Own Public Key to Amazon EC2. Option B is Correct, because you can use the IAM CLI to create a new key pair 1 https://docs.IAM.amazon.com/cli/latest/userguide/cliec2-keypairs.html Option D is invalid because the public key needs to be stored in the EC2 Instance For more information on EC2 Key pairs, please visit the below URL:

* https://docs.IAM.amazon.com/IAMEC2/latest/UserGuide/ec2-key-pairs The correct answers are: Use a third party tool to create the Key pair. Create a new key pair using the IAM CLI, Import the public key into EC2 Submit your Feedback/ Queries to our Experts

QUESTION 2

A company wants to establish separate IAM Key Management Service (IAM KMS) keys to use for different IAM services. The company\\'s security engineer created the following key policy lo allow the infrastructure deployment team to create encrypted Amazon Elastic Block Store (Amazon EBS) volumes by assuming the InfrastructureDeployment IAM role: The security engineer recently discovered that IAM roles other than the InfrastructureDeployment role used this key (or other services.

```
{
   "Version": "2012-10-17",
   "Id": "key-policy-ebs",
   "Statement": [
          {
               "Sid": "Enable IAM User Permissions",
               "Effect": "Allow",
               "Principal": {
                    "AWS": "arn:aws:iam::123456789012:root"
               },
               "Action": "kms:*",
               "Resource": "*"
          },
          {
               "Sid": "Allow use of the key",
               "Effect": "Allow",
               "Principal": {
                    "AWS": "arn:aws:iam::123456789012:role/aws-
reserved/sso.amazonaws.com/InfrastructureDeployment"
               },
               "Action": [
                    "kms:Encrypt",
                    "kms:Decrypt",
                    "kms:ReEncrypt*",
                    "kms:GenerateDataKey*",
                    "kms:DescribeKey",
                    "kms:CreateGrant",
                    "kms"ListGrants",
                    "kms:RevokeGrant"
   ],
   "Resource": "*",
   "Condition": {
        "StringEquals": {
             "kms:ViaService": "ec2.us-west-2.amazonaws.com"
        }
    }
  }
 ]
}
```

Which change to the policy should the security engineer make to resolve these issues?

A. In the statement block that contains the Sid "Allow use of the key", under the "Condition" block, change StringEquals to StringLike.

B. In the policy document, remove the statement Dlock that contains the Sid "Enable IAM User Permissions". Add key management policies to the KMS policy.

C. In the statement block that contains the Sid "Allow use of the Key", under the "Condition" block, change the Kms:ViaService value to ec2.us-east-1 .amazonIAM com.

D. In the policy document, add a new statement block that grants the kms:Disable\\' permission to the security engineer\\'s IAM role.

Correct Answer: B

First block of policy grants \\'admin\\' permissions to users. IAM root indicates all users in the account. Refer below:

A key policy document with a statement that allows access to the AWS account (root user) enables IAM policies in the account to allow access to the KMS key. This means that IAM users and roles in the account might have access to the

KMS key even if they are not explicitly listed as principals in the key policy document.

https://docs.aws.amazon.com/kms/latest/developerguide/determining-access-key-policy.html

QUESTION 3

A company is operating a website using Amazon CloudFornt. CloudFront servers some content from Amazon S3 and other from web servers running EC2 instances behind an Application. Load Balancer (ALB). Amazon DynamoDB is used as the data store. The company already uses IAM Certificate Manager (ACM) to store a public TLS certificate that can optionally secure connections between the website users and CloudFront. The company has a new requirement to enforce end-to-end encryption in transit. Which combination of steps should the company take to meet this requirement? (Select THREE.)

A. Update the CloudFront distribution. configuring it to optionally use HTTPS when connecting to origins on Amazon S3

B. Update the web application configuration on the web servers to use HTTPS instead of HTTP when connecting to DynamoDB

C. Update the CloudFront distribution to redirect HTTP corrections to HTTPS

D. Configure the web servers on the EC2 instances to listen using HTTPS using the public ACM TLS certificate Update the ALB to connect to the target group using HTTPS

E. Update the ALB listen to listen using HTTPS using the public ACM TLS certificate. Update the CloudFront distribution to connect to the HTTPS listener.

F. Create a TLS certificate Configure the web servers on the EC2 instances to use HTTPS only with that certificate. Update the ALB to connect to the target group using HTTPS.

Correct Answer: BCE

QUESTION 4

An application running on EC2 instances in a VPC must call an external web service via TLS (port 443). The instances run in public subnets.

Which configurations below allow the application to function and minimize the exposure of the instances? Select 2 answers from the options given below

A. A network ACL with a rule that allows outgoing traffic on port 443.

B. A network ACL with rules that allow outgoing traffic on port 443 and incoming traffic on ephemeral ports

C. A network ACL with rules that allow outgoing traffic on port 443 and incoming traffic on port 443.

D. A security group with a rule that allows outgoing traffic on port 443

E. A security group with rules that allow outgoing traffic on port 443 and incoming traffic on ephemeral ports.

F. A security group with rules that allow outgoing traffic on port 443 and incoming traffic on port 443.

Correct Answer: BD

Since here the traffic needs to flow outbound from the Instance to a web service on Port 443, the outbound rules on both the Network and Security Groups need to allow outbound traffic. The Incoming traffic should be allowed on ephermal ports for the Operating System on the Instance to allow a connection to be established on any desired or available port. Option A is invalid because this rule alone is not enough. You also need to ensure incoming traffic on ephemeral ports Option C is invalid because need to ensure incoming traffic on ephemeral ports and not only port 443 Option E and F are invalid since here you are allowing additional ports on Security groups which are not required For more information on VPC Security Groups, please visit the below URL: https://docs.IAM.amazon.com/AmazonVPC/latest/UserGuideA/PC_SecurityGroups.htmll The correct answers are: A network ACL with rules that allow outgoing traffic on port 443 and incoming traffic on ephemeral ports, A security group with a rule that allows outgoing traffic on port 443 Submit your Feedback/Queries to our Experts

QUESTION 5

You have a bucket and a VPC defined in IAM. You need to ensure that the bucket can only be accessed by the VPC endpoint. How can you accomplish this?

A. Modify the security groups for the VPC to allow access to the 53 bucket

B. Modify the route tables to allow access for the VPC endpoint

C. Modify the IAM Policy for the bucket to allow access for the VPC endpoint

D. Modify the bucket Policy for the bucket to allow access for the VPC endpoint

Correct Answer: D

This is mentioned in the IAM Documentation Restricting Access to a Specific VPC Endpoint The following is an example of an S3 bucket policy that restricts access to a specific bucket, examplebucket only from the VPC endpoint with the ID vpce-la2b3c4d. The policy denies all access to the bucket if the specified endpoint is not being used. The IAM:sourceVpce condition is used to the specify the endpoint. The IAM:sourceVpce condition does not require an ARN for the VPC endpoint resource, only the VPC endpoint ID. For more information about using conditions in a policy, see Specifying Conditions in a Policy.

```
{
  "Version": "2012-10-17",
  "Id": "Policy1415115909152",
  "Statement": [
   {
    "Sid": "Access-to-specific-VPCE-only",
    "Principal": "*",
    "Action": "s3:*",
    "Effect": "Deny",
    "Resource": ["arn:aws:s3:::examplebucket",
              "arn:aws:s3:::examplebucket/*"],
    "Condition": {
     "StringNotEquals": {
      "aws:sourceVpce": "vpce-1a2b3c4d"
     }
    }
   }
  ]
}
```

Options A and B are incorrect because using Security Groups nor route tables will help to allow access specifically for that bucke via the VPC endpoint Here you specifically need to ensure the bucket policy is changed.

Option C is incorrect because it is the bucket policy that needs to be changed and not the IAM policy.

For more information on example bucket policies for VPC endpoints, please refer to below URL:

https://docs.IAM.amazon.com/AmazonS3/latest/dev/example-bucket-policies-vpc- endpoint.html

The correct answer is: Modify the bucket Policy for the bucket to allow access for the VPC endpoint Submit your Feedback/Queries to our Experts