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.pass4itsure.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 deploys a set of standard IAM roles in AWS accounts. The IAM roles are based on job functions within the company. To balance operational efficiency and security, a security engineer implemented AWS Organizations SCPs to

restrict access to critical security services in all company accounts.

All of the company\\'s accounts and OUs within AWS Organizations have a default FullAWSAccess SCP that is attached. The security engineer needs to ensure that no one can disable Amazon GuardDuty and AWS Security Hub. The security

engineer also must not override other permissions that are granted by IAM policies that are defined in the accounts.

Which SCP should the security engineer attach to the root of the organization to meet these requirements?

A.
```
"Version": "2012-10-17",
"Statement"":[
  {
    "Effect": "Deny",
    "Action":[
      "guardduty:DeleteDetector",
      "guardduty:UpdateDetector",
      "securityhub:DisableSecurityHub"
    ],
    "Resource":[
    "*"
    ]
  }
 ]
}
```

B.
```
{
"Version": "2012-10-17",
"Statement"":[
  {
      "Effect": "Deny",
      "Action":"*",
      "Resource": "*"
  },
  {
    "Effect": "Allow",
    "NotAction": [
    "guardduty:DeleteDetector",
    "guardduty:UpdateDetector",
    "securityhub:DisableSecurityHub"
  ],
  "Resource":[
  "*"
  ]
  }
 ]
}
```

C.
```
{
 "Version": "2012-10-17",
 "Statement"":[
   {
       "Effect": "Allow",
       "Action":"*",
       "Resource": "*"
    },
    {
      "Effect": "Deny",
      "NotAction": [
      "guardduty:DeleteDetector",
      "guardduty:UpdateDetector",
      "securityhub:DisableSecurityHub"
    ],
    "Resource":[
    "*"
    ]
   }
  ]
}
```

D.
```
{
 "Version": "2012-10-17",
 "Statement"":[
   {
       "Effect": "Allow",
        "NotAction": [
      "guardduty:DeleteDetector",
      "guardduty:UpdateDetector",
      "securityhub:DisableSecurityHub"
    ],
    "Resource":[
    "*"
    ]
   }
  ]
}
```

A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: A

QUESTION 2

A security engineer is configuring account-based access control (ABAC) to allow only specific principals to put objects into an Amazon S3 bucket. The principals already have access to Amazon S3.

The security engineer needs to configure a bucket policy that allows principals to put objects into the S3 bucket only if the value of the Team tag on the object matches the value of the Team tag that is associated with the principal. During testing, the security engineer notices that a principal can still put objects into the S3 bucket when the tag values do not match.

Which combination of factors are causing the PutObject operation to succeed when the tag values are different? (Select TWO.)

A. The principal\\'s identity-based policy grants access to put objects into the S3 bucket with no conditions.

B. The principal\\'s identity-based policy overrides the condition because the identity-based policy contains an explicit allow.

C. The S3 bucket\\'s resource policy does not deny access to put objects.

D. The S3 bucket\\'s resource policy cannot allow actions to the principal.

E. The bucket policy does not apply to principals in the same zone of trust.

Correct Answer: AC

When using ABAC, the principal\\'s identity-based policy and the S3 bucket\\'s resource policy are both evaluated to determine the effective permissions. If either policy grants access to the principal, the action is allowed. If either policy denies access to the principal, the action is denied. Therefore, to enforce the tag-based condition, both policies must deny access when the tag values do not match. In this case, the principal\\'s identity-based policy grants access to put objects into the S3 bucket with no conditions (A), which means that the policy does not check for the tag values. This policy overrides the condition in the bucket policy because an explicit allow always takes precedence over an implicit deny. The bucket policy can only allow or deny actions to the principal based on the condition, but it cannot override the identity-based policy. The S3 bucket\\'s resource policy does not deny access to put objects ? which means that it also does not check for the tag values. The bucket policy can only allow or deny actions to the principal based on the condition, but it cannot override the identity-based policy. Therefore, the combination of factors A and C are causing the PutObject operation to succeed when the tag values are different. References: Using ABAC with Amazon S3 Bucket policy examples

QUESTION 3

A company uses several AWS CloudFormation stacks to handle the deployment of a suite of applications. The leader of the company\\'s application development team notices that the stack deployments fail with permission errors when some team members try to deploy the stacks. However, other team members can deploy the stacks successfully.

The team members access the account by assuming a role that has a specific set of permissions that are necessary for the job responsibilities of the team members. All team members have permissions to perform operations on the stacks.

Which combination of steps will ensure consistent deployment of the stacks MOST securely? (Select THREE.)

A. Create a service role that has a composite principal that contains each service that needs the necessary permissions. Configure the role to allow the sts:AssumeRole action.

B. Create a service role that has cloudformation.amazonaws.com as the service principal. Configure the role to allow the sts:AssumeRole action.

C. For each required set of permissions, add a separate policy to the role to allow those permissions. Add the ARN of each CloudFormation stack in the resource field of each policy.

D. For each required set of permissions, add a separate policy to the role to allow those permissions. Add the ARN of each service that needs the per-missions in the resource field of the corresponding policy.

E. Update each stack to use the service role.

F. Add a policy to each member role to allow the iam:PassRole action. Set the policy\\'s resource field to the ARN of the service role.

Correct Answer: BDF

QUESTION 4

A company is undergoing a layer 3 and layer 4 DDoS attack on its web servers running on IAM.

Which combination of IAM services and features will provide protection in this scenario? (Select THREE).

A. Amazon Route 53

B. IAM Certificate Manager (ACM)

C. Amazon S3

D. IAM Shield

E. Elastic Load Balancer

F. Amazon GuardDuty

Correct Answer: DEF

QUESTION 5

A company is using IAM Organizations. The company wants to restrict IAM usage to the eu-west-1 Region for all accounts under an OU that is named "development." The solution must persist restrictions to existing and new IAM accounts under the development OU.

A. Include the following SCP on the development OU:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyNonDefaultRegions",
            "Effect": "Deny",
            "NotAction": [
                <Desired Global Services> ],
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestedRegion": [
                        "eu-west-1"
                    ]
                },
                "ArnNotLike": {
                    "aws:PrincipalARN": "arn:aws:iam::*:role/AWSExecution"
                }
            }
        }
    ]
}
```

B. Include the following SCP on the development account:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyNonDefaultRegions",
            "Effect": "Deny",
            "NotAction": [
                <Desired Global Services> ],
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestedRegion": [
                        "eu-west-1"
                    ]
                },
                "ArnNotLike": {
                    "aws:PrincipalARN": "arn:aws:iam::*:role/AWSExecution"
                }
            }
        }
    ]
}
```

C. Include the following SCP on the development OU:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyNonDefaultRegions",
            "Effect": "Deny",
            "NotAction": [
                <Desired Global Services> ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestedRegion": [
                        "eu-west-1"
                    ]
                },
                "ArnNotLike": {
                    "aws:PrincipalARN": "arn:aws:iam::*:role/AWSExecution"
                }
            }
        }
    ]
}
```

D. Include the following SCP on the development OU:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyNonDefaultRegions",
            "Effect": "Allow",
            "NotAction": [
                <Desired Global Services> ],
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestedRegion": [
                        "us-east-1"
                    ]
                },
                "ArnNotLike": {
                    "aws:PrincipalARN": "arn:aws:iam::*:role/AWSExecution"
                }
            }
        }
    ]
}
```

A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: A