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:

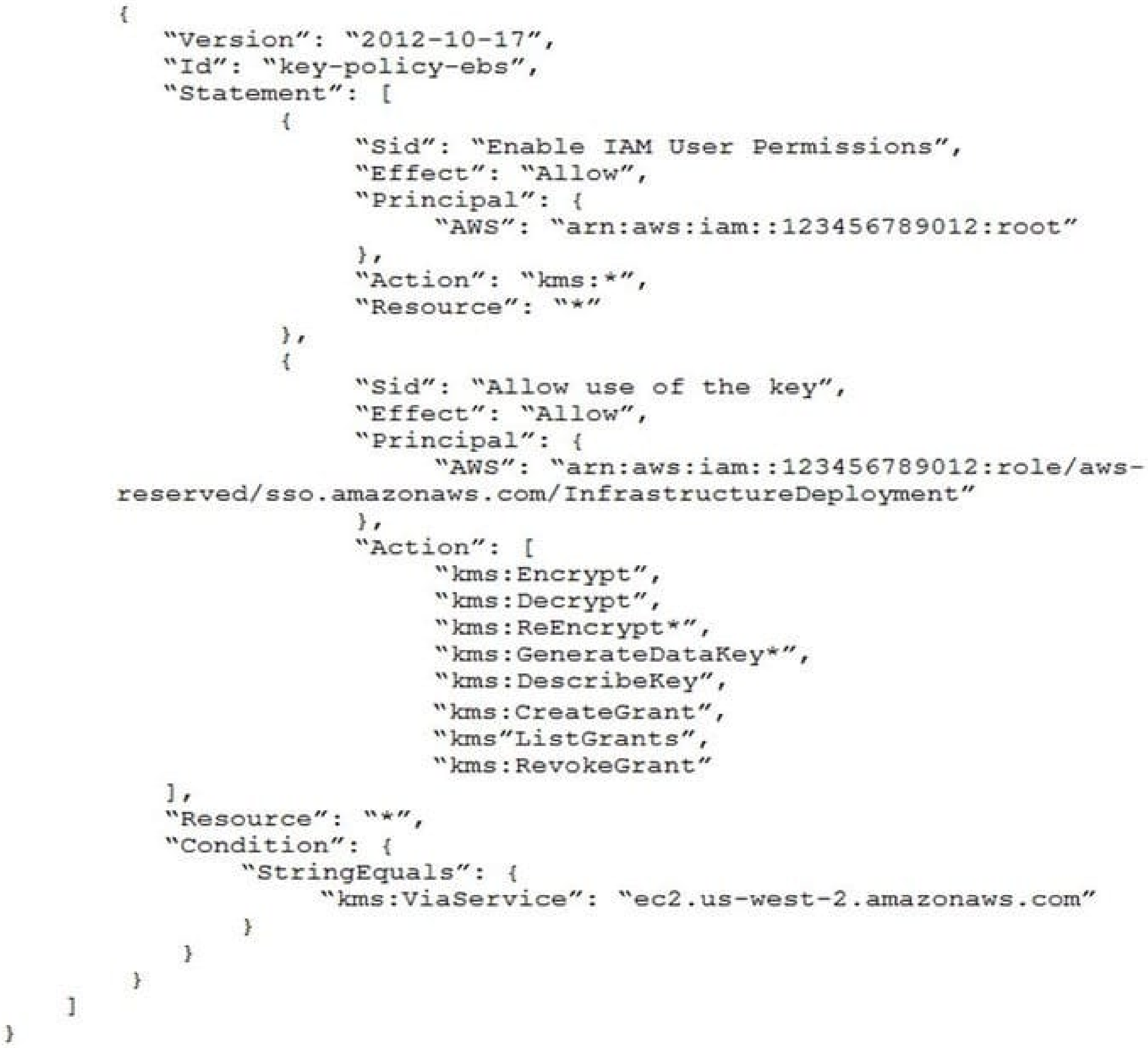
https://www.leads4pass.com/scs-c02.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Amazon Official Exam Center

QUESTION 1

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:



```
      {
         “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”
              }
         }
      }
   ]
}
```

The security engineer recently discovered that IAM roles other than the InfrastructureDeployment role used this key (or other services. 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: C

To resolve the issues, the security engineer should make the following change to the policy:

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.amazonaws.com. This allows the security engineer to restrict the use of the key to only EC2

service in the us-east-1 region, and prevent other services from using the key.

QUESTION 2

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

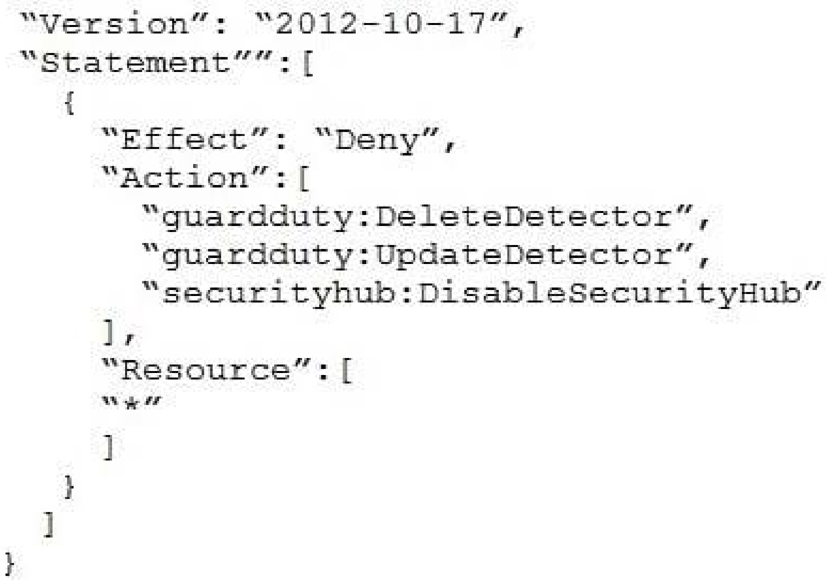
restrict access to critical security services in all company accounts.

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.

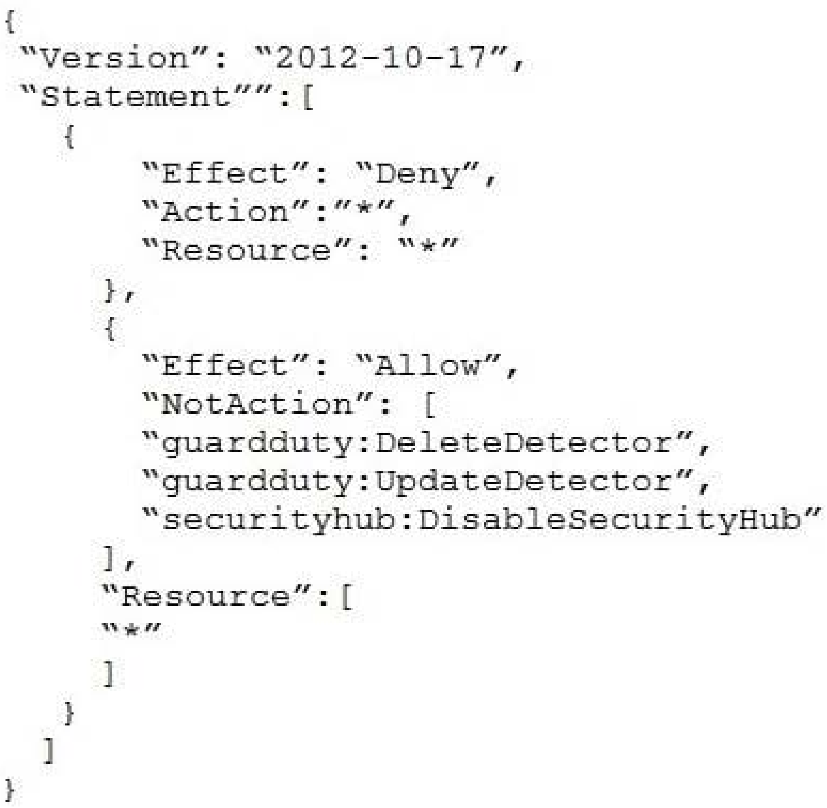
Which SCP should the security engineer attach to the root of the organization to meet these requirements?

A.



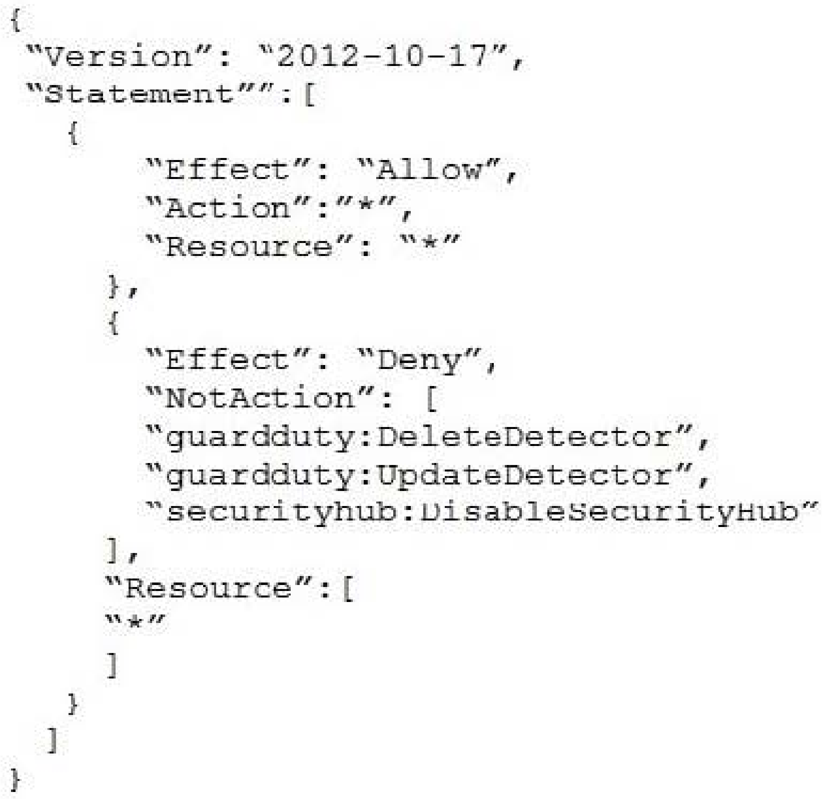
```
 “Version”: “2012-10-17”,
 “Statement””:[
   {
     “Effect”: “Deny”,
     “Action”:[
       “guardduty:DeleteDetector”,
       “guardduty:UpdateDetector”,
       “securityhub:DisableSecurityHub”
     ],
     “Resource”:[
     “*”
     ]
   }
  ]
}
```

B.



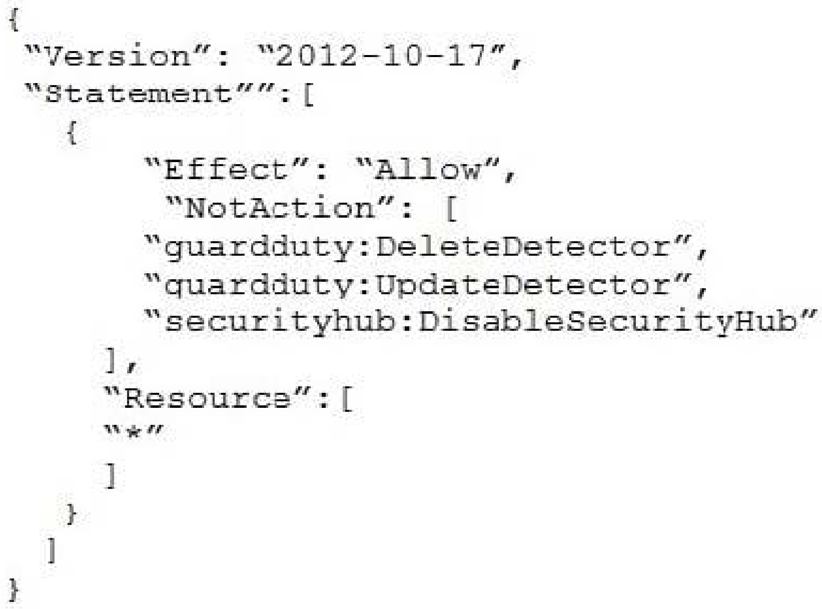
```
{
 “Version”: “2012-10-17”,
 “Statement””:[
   {
       “Effect”: “Deny”,
       “Action”:“*”,
       “Resource”: “*”
     },
     {
       “Effect”: “Allow”,
       “NotAction”: [
       “guardduty:DeleteDetector”,
       “guardduty:UpdateDetector”,
       “securityhub:DisableSecurityHub”
     ],
     “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 3

A Security Engineer has been tasked with enabling IAM Security Hub to monitor Amazon EC2 instances fix CVE in a single IAM account The Engineer has already enabled IAM Security Hub and Amazon Inspector m the IAM Management Console and has installed me Amazon Inspector agent on an EC2 instances that need to be monitored.

Which additional steps should the Security Engineer lake 10 meet this requirement?

A. Configure the Amazon inspector agent to use the CVE rule package

B. Configure the Amazon Inspector agent to use the CVE rule package Configure Security Hub to ingest from IAM inspector by writing a custom resource policy

C. Configure the Security Hub agent to use the CVE rule package Configure IAM Inspector lo ingest from Security Hub by writing a custom resource policy

D. Configure the Amazon Inspector agent to use the CVE rule package Install an additional Integration library Allow the Amazon Inspector agent to communicate with Security Hub

Correct Answer: D

you need to configure the Amazon Inspector agent to use the CVE rule package, which is a set of rules that check for vulnerabilities and exposures on your EC2 instances. You also need to install an additional integration library that enables communication between the Amazon Inspector agent and Security Hub. Security Hub is a service that provides you with a comprehensive view of your security state in AWS and helps you check your environment against security industry standards and best practices. The other options are either incorrect or incomplete for meeting the requirement.

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: ABC

The key length for an RSA certificate that you use with CloudFront is 2048 bits, even though ACM supports larger keys. If you use an imported certificate with CloudFront, your key length must be 1024 or 2048 bits and cannot exceed 2048 bits. You must import the certificate in the US East (N. Virginia) Region. You must have permission to use and import the SSL/TLS certificate https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/cnames-and-httpsrequirements.html

QUESTION 5

A company needs to encrypt all of its data stored in Amazon S3. The company wants to use IAM Key Management Service (IAM 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 IAM KMS to meet these requirements?

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

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

Correct Answer: A

To meet the requirements of importing their own key material, setting an expiration date on the keys, and deleting keys immediately, the security engineer should do the following:

Configure AWS KMS and use a custom key store. This allows the security engineer to use a key manager outside of AWS KMS that they own and manage, such as an AWS CloudHSM cluster or an external key manager. Create a customer

managed CMK with no key material. Import the company\\'s keys and key material into the CMK. This allows the security engineer to use their own key material for encryption and decryption operations, and to specify an expiration date for it.

SCS-C02 PDF Dumps SCS-C02 Practice Test SCS-C02 Study Guide