Free Questions for SCS-C01 by certsdeals

Shared by Logan on 06-06-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A company's security information events management (SIEM) tool receives new AWS CloudTrail logs from an Amazon S3 bucket that is configured to send all object created event notification to an Amazon SNS topic An Amazon SQS queue is subscribed to this SNS topic. The company's SEM tool then ports this SQS queue for new messages using an IAM role and fetches new log events from the S3 bucket based on the SQS messages.

After a recent security review that resulted m restricted permissions, the SEM tool has stopped receiving new CloudTral logs

Which of the following are possible causes of this issue? (Select THREE)

Options:

A- The SOS queue does not allow the SQS SendMessage action from the SNS topic

B- The SNS topic does not allow the SNS Publish action from Amazon S3

C- The SNS topic is not delivering raw messages to the SQS queue

D- The S3 bucket policy does not allow CloudTrail to perform the PutObject action

E- The IAM role used by the 5EM tool does not have permission to subscribe to the SNS topic

F- The IAM role used by the SEM tool does not allow the SQS DeleteMessage action.

Answer:

A, D, F

Question 2

Question Type: MultipleChoice

A company has multiple departments. Each department has its own AWS account. All these accounts belong to the same organization in AWS Organizations.

A large .csv file is stored in an Amazon S3 bucket in the sales department's AWS account. The company wants to allow users from the other accounts to access the .csv file's content through the combination of AWS Glue and Amazon Athen

a. However, the company does not want to allow users from the other accounts to access other files in the same folder.

Which solution will meet these requirements?

Options:

A- Apply a user policy in the other accounts to allow AWS Glue and Athena lo access the .csv We.

B- Use S3 Select to restrict access to the .csv lie. In AWS Glue Data Catalog, use S3 Select as the source of the AWS Glue database.

C- Define an AWS Glue Data Catalog resource policy in AWS Glue to grant cross-account S3 object access to the .csv file.

D- Grant AWS Glue access to Amazon S3 in a resource-based policy that specifies the organization as the principal.

Answer:

A

Question 3

Question Type: **MultipleChoice**

A business stores website images in an Amazon S3 bucket. The firm serves the photos to end users through Amazon CloudFront. The firm learned lately that the photographs are being accessible from nations in which it does not have a distribution license.

Which steps should the business take to safeguard the photographs and restrict their distribution? (Select two.)

Options:

A- Update the S3 bucket policy to restrict access to a CloudFront origin access identity (OAI).

B- Update the website DNS record to use an Amazon Route 53 geolocation record deny list of countries where the company lacks a license.

C- Add a CloudFront geo restriction deny list of countries where the company lacks a license.

D- Update the S3 bucket policy with a deny list of countries where the company lacks a license.

E- Enable the Restrict Viewer Access option in CloudFront to create a deny list of countries where the company lacks a license.

Answer:

A, C

Explanation:

For Enable Geo-Restriction, choose Yes. For Restriction Type, choose Whitelist to allow access to certain countries, or choose Blacklist to block access from certain countries. https://aws.amazon.com/premiumsupport/knowledge-center/cloudfront-geo-restriction/

Question 4

Question Type: **MultipleChoice**

A development team is attempting to encrypt and decode a secure string parameter from the AWS Systems Manager Parameter Store using an AWS Key Management Service (AWS KMS) CMK. However, each attempt results in an error message being sent to the development team.

Which CMK-related problems possibly account for the error? (Select two.)

Options:

A- The CMK is used in the attempt does not exist.

B- The CMK is used in the attempt needs to be rotated.

C- The CMK is used in the attempt is using the CMKs key ID instead of the CMK ARN.

D- The CMK is used in the attempt is not enabled.

E- The CMK is used in the attempt is using an alias.

Answer:

A, D

Explanation:

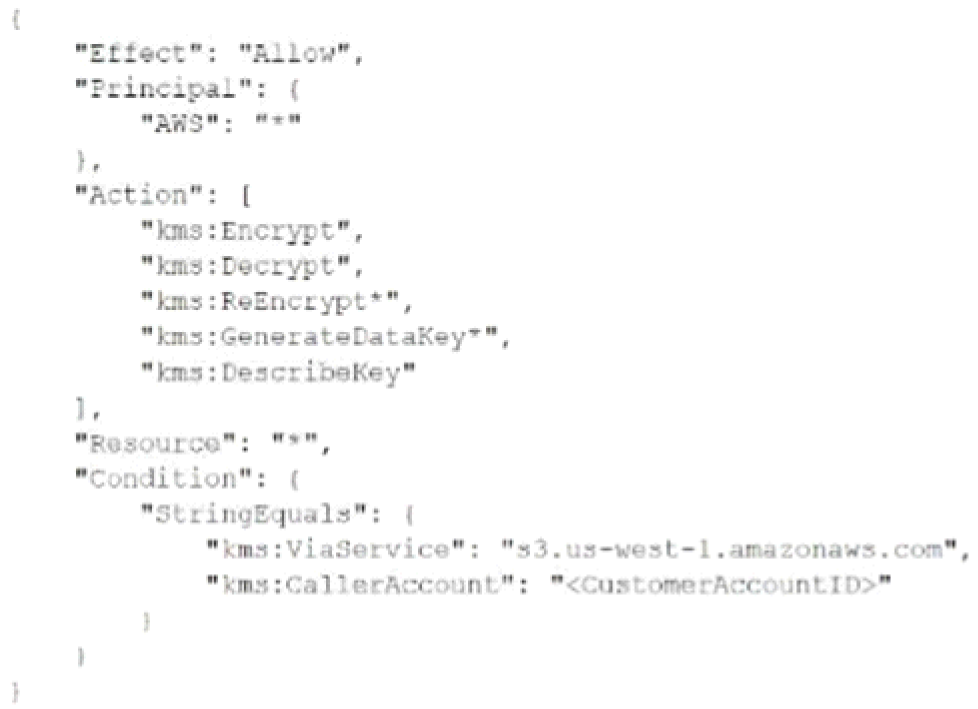
https://docs.aws.amazon.com/kms/latest/developerguide/services-parameter-store.html#parameter-store-cmk-fail

Question 5

Question Type: MultipleChoice

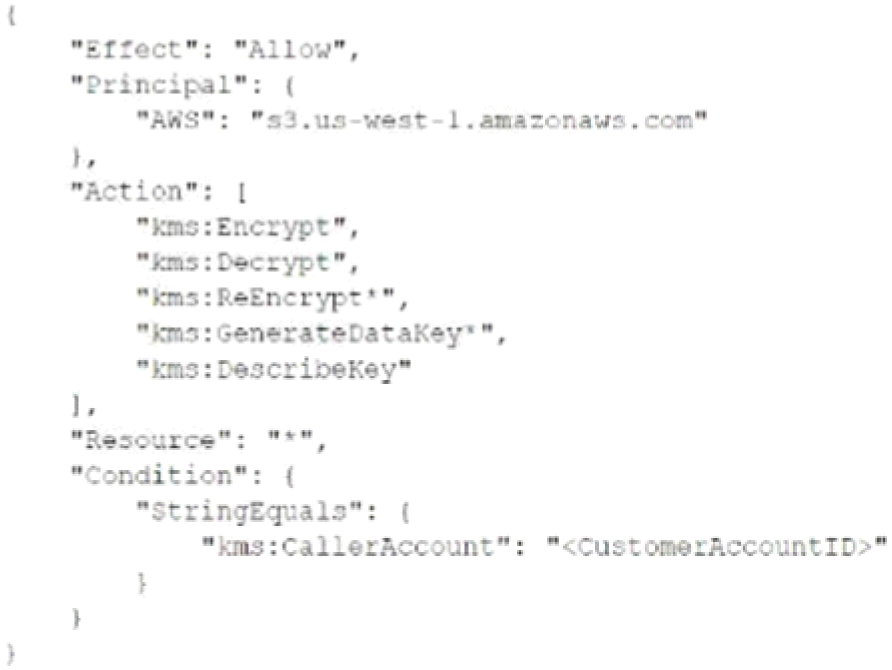
A security engineer needs to create an AWS Key Management Service
Which statement in the KMS key policy will meet these requirements?

A)



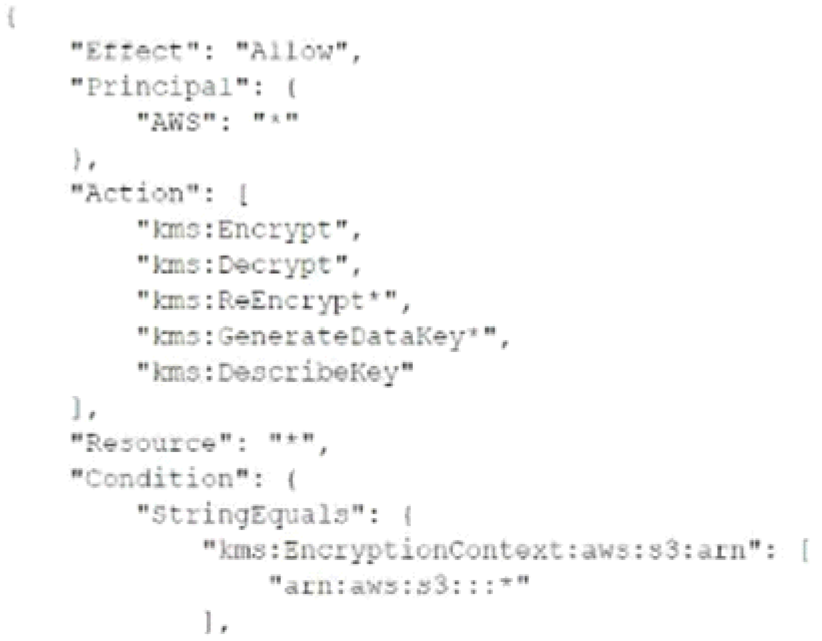
```
{
    "Effect": "Allow",
    "Principal": {
        "AWS": "*"
    },
    "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "kms:ViaService": "s3.us-west-1.amazonaws.com",
            "kms:CallerAccount": "<CustomerAccountID>"
        }
    }
}
```

B)



```
{
    "Effect": "Allow",
    "Principal": {
        "AWS": "s3.us-west-1.amazonaws.com"
    },
    "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "kms:CallerAccount": "<CustomerAccountID>"
        }
    }
}
```

C)



```
{
    "Effect": "Allow",
    "Principal": {
        "AWS": "*"
    },
    "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "kms:EncryptionContext:aws:s3:arn": [
                "arn:aws:s3:::*"
            ],
```

Options:

A- Option A

B- Option B

C- Option C

Answer:

C

Question 6

Question Type: MultipleChoice

An application team wants to use AWS Certificate Manager (ACM) to request public certificates to ensure that data is secured in transit. The domains that are being used are not currently hosted on Amazon Route 53

The application team wants to use an AWS managed distribution and caching solution to optimize requests to its systems and provide better points of presence to customers The distribution solution will use a primary domain name that is customized The distribution solution also will use several alternative domain names The certificates must renew automatically over an indefinite period of time

Which combination of steps should the application team take to deploy this architecture? (Select THREE.)

Options:

A- Request a certificate (torn ACM in the us-west-2 Region Add the domain names that the certificate will secure

B- Send an email message to the domain administrators to request vacation of the domains for ACM

C- Request validation of the domains for ACM through DNS Insert CNAME records into each domain's DNS zone

D- Create an Application Load Balancer for me caching solution Select the newly requested certificate from ACM to be used for secure connections

E- Create an Amazon CloudFront distribution for the caching solution Enter the main CNAME record as the Origin Name Enter the subdomain names or alternate names in the Alternate Domain Names Distribution Settings Select the newly requested certificate from ACM to be used for secure connections

F- Request a certificate from ACM in the us-east-1 Region Add the domain names that the certificate wil secure

Answer:

C, D, F

Question 7

Question Type: **MultipleChoice**

A company's security team is building a solution for logging and visualization. The solution will assist the company with the large variety and velocity of data that it receives from AWS across multiple accounts. The security team has enabled AWS CloudTrail and VPC Flow Logs in all of its accounts In addition, the company has an organization in AWS Organizations and has an AWS Security Hub master account.

The security team wants to use Amazon Detective However the security team cannot enable Detective and is unsure why

What must the security team do to enable Detective?

Options:

A- Enable Amazon Macie so that Secunty H jb will allow Detective to process findings from Macie.

B- Disable AWS Key Management Service (AWS KMS) encryption on CtoudTrail logs in every member account of the organization

C- Enable Amazon GuardDuty on all member accounts Try to enable Detective in 48 hours

D- Ensure that the principal that launches Detective has the organizations ListAccounts permission

Answer:

D

Question 8

Question Type: **MultipleChoice**

A company is hosting a static website on Amazon S3 The company has configured an Amazon CloudFront distribution to serve the website contents The company has associated an AWS WAF web ACL with the CloudFront distribution. The web ACL ensures that requests originate from the United States to address compliance restrictions.

THE company is worried that the S3 URL might still be accessible directly and that requests can bypass the CloudFront distribution

Which combination of steps should the company take to remove direct access to the S3 URL? (Select TWO.)

Options:

A- Select 'Restrict Bucket Access' in the origin settings of the CloudFront distribution

B- Create an origin access identity (OAI) for the S3 origin

C- Update the S3 bucket policy to allow s3 GetObject with a condition that the aws Referer key matches the secret value Deny all other requests

D- Configure the S3 bucket poky so that only the origin access identity (OAI) has read permission for objects in the bucket

E- Add an origin custom header that has the name Referer to the CloudFront distribution Give the header a secret value.

Answer:

A, D

Question 9

Question Type: **MultipleChoice**

A company wants to monitor the deletion of customer managed CMKs A security engineer must create an alarm that will notify the company before a CMK is deleted The security engineer has configured the integration of AWS CloudTrail with Amazon CloudWatch

What should the security engineer do next to meet this requirement?

Within AWS Key Management Service (AWS KMS} specify the deletion time of the key material during CMK creation AWS KMS will automatically create a CloudWatch.

Create an amazon Eventbridge (Amazon CloudWatch Events) rule to look for API calls of DeleteAlias Create an AWS Lamabda function to send an Amazon Simple Notification Service (Amazon SNS) messages to the company Add the Lambda functions as the target of the Eventbridge (CloudWatch Events) rule.

Create an Amazon EventBridge (Amazon CloudWath Events) rule to look for API calls of DisableKey and ScheduleKeyDelection. Create an AWS Lambda function to generate the alarm and send the notification to the company. Add the lambda function as the target of the SNS policy.

Options:

A- Use inbound rule 100 to allow traffic on TCP port 443 Use inbound rule 200 to deny traffic on TCP port 3306 Use outbound rule 100 to allow traffic on TCP port 443

B- Use inbound rule 100 to deny traffic on TCP port 3306. Use inbound rule 200 to allow traffic on TCP port range 1024-65535. Use outbound rule 100 to allow traffic on TCP port 443

C- Use inbound rule 100 to allow traffic on TCP port range 1024-65535 Use inbound rule 200 to deny traffic on TCP port 3306 Use outbound rule 100 to allow traffic on TCP port 443

D- Use inbound rule 100 to deny traffic on TCP port 3306 Use inbound rule 200 to allow traffic on TCP port 443 Use outbound rule 100 to allow traffic on TCP port 443

Answer:

A

20%
DISCOUNT