Free Questions for SCS-C01 by dumpshq

Shared by Banks on 15-04-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A company uses AWS Organizations to manage several AWs accounts. The company processes a large volume of sensitive dat

a. The company uses a serverless approach to microservices. The company stores all the data in either Amazon S3 or Amazon DynamoDB. The company reads the data by using either AWS lambda functions or container-based services that the company hosts on Amazon Elastic Kubernetes Service (Amazon EKS) on AWS Fargate.

The company must implement a solution to encrypt all the data at rest and enforce least privilege data access controls. The company creates an AWS Key Management Service (AWS KMS) customer managed key.

What should the company do next to meet these requirements?

Options:

A- Create a key policy that allows the kms:Decrypt action only for Amazon S3 and DynamoDB. Create an SCP that denies the creation of S3 buckets and DynamoDB tables that are not encrypted with the key.

B- Create an 1AM policy that denies the kms:Decrypt action for the key. Create a Lambda function than runs on a schedule to attach the policy to any new roles. Create an AWS Config rule to send alerts for resources that are not encrypted with the key.

C- Create a key policy that allows the kms:Decrypt action only for Amazon S3, DynamoDB, Lambda, and Amazon EKS. Create an SCP that denies the creation of S3 buckets and DynamoDB tables that are not encrypted with the key.

D- Create a key policy that allows the kms:Decrypt action only for Amazon S3, DynamoDB, Lambda, and Amazon EKS. Create an AWS

Config rule to send alerts for resources that are not encrypted with the key.

Answer:

B

Question 2

Question Type: MultipleChoice

A company needs to store multiple years of financial records. The company wants to use Amazon S3 to store copies of these documents. The company must implement a solution to prevent the documents from being edited, replaced, or deleted for 7 years after the documents are stored in Amazon S3. The solution must also encrypt the documents at rest.

A security engineer creates a new S3 bucket to store the documents.

What should the security engineer do next to meet these requirements?

Options:

A- Configure S3 server-side encryption. Create an S3 bucket policy that has an explicit deny rule for all users for s3:DeleteObject and s3:PutObject API calls. Configure S3 Object Lock to use governance mode with a retention period of 7 years.

B- Configure S3 server-side encryption. Configure S3 Versioning on the S3 bucket. Configure S3 Object Lock to use compliance mode

with a retention period of 7 years.

C- Configure S3 Versioning. Configure S3 Intelligent-Tiering on the S3 bucket to move the documents to S3 Glacier Deep Archive storage. Use S3 server-side encryption immediately. Expire the objects after 7 years.

D- Set up S3 Event Notifications and use S3 server-side encryption. Configure S3 Event Notifications to target an AWS Lambda function that will review any S3 API call to the S3 bucket and deny the s3:DeleteObject and s3:PutObject API calls. Remove the S3 event notification after 7 years.

Answer:

B

Question 3

Question Type: MultipleChoice

A security administrator is setting up a new AWS account. The security administrator wants to secure the data that a company stores in an Amazon S3 bucket. The security administrator also wants to reduce the chance of unintended data exposure and the potential for misconfiguration of objects that are in the S3 bucket.

Which solution will meet these requirements with the LEAST operational overhead?

Options:

A- Configure the S3 Block Public Access feature for the AWS account.

B- Configure the S3 Block Public Access feature for all objects that are in the bucket.

C- Deactivate ACLs for objects that are in the bucket.

D- Use AWS PrivateLink for Amazon S3 to access the bucket.

Answer:

D

Question 4

Question Type: **MultipleChoice**

A company uses Amazon API Gateway to present REST APIs to users. An API developer wants to analyze API access patterns without the need to parse the log files.

Which combination of steps will meet these requirements with the LEAST effort? (Select TWO.)

Options:

A- Configure access logging for the required API stage.

B- Configure an AWS CloudTrail trail destination for API Gateway events. Configure filters on the userIdentity, userAgent, and sourceIPAddress fields.

C- Configure an Amazon S3 destination for API Gateway logs. Run Amazon Athena queries to analyze API access information.

D- Use Amazon CloudWatch Logs Insights to analyze API access information.

E- Select the Enable Detailed CloudWatch Metrics option on the required API stage.

Answer:

C, D

Question 5

Question Type: **MultipleChoice**

A company is attempting to conduct forensic analysis on an Amazon EC2 instance, but the company is unable to connect to the instance by using AWS Systems Manager Session Manager. The company has installed AWS Systems Manager Agent (SSM Agent) on the EC2 instance.

The EC2 instance is in a subnet in a VPC that does not have an internet gateway attached. The company has associated a security group with the EC2 instance. The security group does not have inbound or outbound rules. The subnet's network ACL allows all inbound and outbound traffic.

Which combination of actions will allow the company to conduct forensic analysis on the EC2 instance without compromising forensic data? (Select THREE.)

Options:

A- Update the EC2 instance security group to add a rule that allows outbound traffic on port 443 for 0.0.0.0/0.

B- Update the EC2 instance security group to add a rule that allows inbound traffic on port 443 to the VPC's CIDR range.

C- Create an EC2 key pair. Associate the key pair with the EC2 instance.

D- Create a VPC interface endpoint for Systems Manager in the VPC where the EC2 instance is located.

E- Attach a security group to the VPC interface endpoint. Allow inbound traffic on port 443 to the VPC's CIDR range.

F- Create a VPC interface endpoint for the EC2 instance in the VPC where the EC2 instance is located.

Answer:

B, C, F

Question 6

Question Type: **MultipleChoice**

A security engineer needs to create an IAM 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:

A

Question 7

Question Type: MultipleChoice

An application team wants to use IAM 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 IAM 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 8

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 IAM across multiple accounts. The security team has enabled IAM CloudTrail and VPC Flow Logs in all of its accounts. In addition, the company has an organization in IAM Organizations and has an IAM 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 IAM Key Management Service (IAM 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 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 IAM CloudTrail with Amazon CloudWatch

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

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

Question 10

Question Type: MultipleChoice

A security engineer receives an IAM abuse email message. According to the message, an Amazon EC2 instance that is running in the security engineer's IAM account is sending phishing email messages.

The EC2 instance is part of an application that is deployed in production. The application runs on many EC2 instances behind an Application Load Balancer. The instances run in an Amazon EC2 Auto Scaling group across multiple subnets and multiple Availability Zones.

The instances normally communicate only over the HTTP. HTTPS, and MySQL protocols. Upon investigation, the security engineer discovers that email messages are being sent over port 587. All other traffic is normal.

The security engineer must create a solution that contains the compromised EC2 instance, preserves forensic evidence for analysis, and minimizes application downtime. Which combination of steps must the security engineer take to meet these requirements? (Select THREE.)

Options:

A- Add an outbound rule to the security group that is attached to the compromised EC2 instance to deny traffic to 0.0.0.0/0 and port 587.

B- Add an outbound rule to the network ACL for the subnet that contains the compromised EC2 instance to deny traffic to 0.0.0.0/0 and port 587.

C- Gather volatile memory from the compromised EC2 instance. Suspend the compromised EC2 instance from the Auto Scaling group. Then take a snapshot of the compromised EC2 instance. v

D- Take a snapshot of the compromised EC2 instance. Suspend the compromised EC2 instance from the Auto Scaling group. Then gather volatile memory from the compromised EC2 instance.

E- Move the compromised EC2 instance to an isolated subnet that has a network ACL that has no inbound rules or outbound rules.

F- Replace the existing security group that is attached to the compromised EC2 instance with a new security group that has no inbound rules or outbound rules.

Answer:

A, C, E