Free Questions for SCS-C01 by certsinside

Shared by Ayers on 22-07-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A company stores sensitive documents in Amazon S3 by using server-side encryption with an IAM Key Management Service (IAM KMS) CMK. A new requirement mandates that the CMK that is used for these documents can be used only for S3 actions.

Which statement should the company add to the key policy to meet this requirement?

A)

```
{
  "Effect": "Deny",
  "Principal": "*",
  "Action": "kms:*",
  "Resource": "*",
  "Condition": {
    "StringNotEquals": {
      "kms:CallerAccount": "s3.amazonaws.com"
    }
  }
}
```

B)

```
{
  "Effect": "Deny",
  "Principal": "*",
  "Action": "s3:*",
  "Resource": "*",
  "Condition": {
    "StringNotEquals": {
      "kms:ViaService": "kms.*amazonaws.com"
    }
  }
}
```

Options:

A- Option A

B- Option B

Answer:

A

Question 2

Question Type: **MultipleChoice**

A company is implementing a new application in a new IAM account. A VPC and subnets have been created for the application. The application has been peered to an existing VPC in another account in the same IAM Region for database access. Amazon EC2 instances will regularly be created and terminated in the application VPC, but only some of them will need access to the databases in the peered VPC over TCP port 1521. A security engineer must ensure that only the EC2 instances that need access to the databases can access them through the network.

How can the security engineer implement this solution?

Options:

A- Create a new security group in the database VPC and create an inbound rule that allows all traffic from the IP address range of the application VPC. Add a new network ACL rule on the database subnets. Configure the rule to TCP port 1521 from the IP address range of the application VPC. Attach the new security group to the database instances that the application instances need to access.

B- Create a new security group in the application VPC with an inbound rule that allows the IP address range of the database VPC over TCP port 1521. Create a new security group in the database VPC with an inbound rule that allows the IP address range of the application VPC over port 1521. Attach the new security group to the database instances and the application instances that need database access.

C- Create a new security group in the application VPC with no inbound rules. Create a new security group in the database VPC with an inbound rule that allows TCP port 1521 from the new application security group in the application VPC. Attach the application security group to the application instances that need database access, and attach the database security group to the database instances.

D- Create a new security group in the application VPC with an inbound rule that allows the IP address range of the database VPC over TCP port 1521. Add a new network ACL rule on the database subnets. Configure the rule to allow all traffic from the IP address range of the application VPC. Attach the new security group to the application instances that need database access.

Answer:

C

Question 3

Question Type: MultipleChoice

A company wants to ensure that its IAM resources can be launched only in the us-east-1 and us-west-2 Regions.

What is the MOST operationally efficient solution that will prevent developers from launching Amazon EC2 instances in other Regions?

Options:

A- Enable Amazon GuardDuty in all Regions. Create alerts to detect unauthorized activity outside us-east-1 and us-west-2.

B- Use an organization in IAM Organizations. Attach an SCP that allows all actions when the IAM: Requested Region condition key is either us-east-1 or us-west-2. Delete the FullIAMAccess policy.

C- Provision EC2 resources by using IAM Cloud Formation templates through IAM CodePipeline. Allow only the values of us-east-1 and us-west-2 in the IAM CloudFormation template's parameters.

D- Create an IAM Config rule to prevent unauthorized activity outside us-east-1 and us-west-2.

Answer:

C

Question 4

Question Type: MultipleChoice

A development team is using an IAM Key Management Service (IAM KMS) CMK to try to encrypt and decrypt a secure string parameter from IAM Systems Manager Parameter Store. However, the development team receives an error message on each attempt.

Which issues that are related to the CMK could be reasons for the error? (Select TWO.)

Options:

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

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

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

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

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

Answer:

A, D

Question 5

Question Type: MultipleChoice

A company is running an application in The eu-west-1 Region. The application uses an IAM Key Management Service (IAM KMS) CMK to encrypt sensitive dat

a. The company plans to deploy the application in the eu-north-1 Region.

A security engineer needs to implement a key management solution for the application deployment in the new Region. The security engineer must minimize changes to the application code.

Which change should the security engineer make to the IAM KMS configuration to meet these requirements?

Options:

A- Update the key policies in eu-west-1. Point the application in eu-north-1 to use the same CMK as the application in eu-west-1.

B- Allocate a new CMK to eu-north-1 to be used by the application that is deployed in that Region.

C- Allocate a new CMK to eu-north-1. Create the same alias name for both keys. Configure the application deployment to use the key

alias.

D- Allocate a new CMK to eu-north-1. Create an alias for eu-'-1. Change the application code to point to the alias for eu-'-1.

Answer:

B

Question 6

Question Type: MultipleChoice

A company uses Amazon RDS for MySQL as a database engine for its applications. A recent security audit revealed an RDS instance that is not compliant with company policy for encrypting data at rest. A security engineer at the company needs to ensure that all existing RDS databases are encrypted using server-side encryption and that any future deviations from the policy are detected.

Which combination of steps should the security engineer take to accomplish this? (Select TWO.)

Options:

A- Create an IAM Config rule to detect the creation of unencrypted RDS databases. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to trigger on the IAM Config rules compliance state change and use Amazon Simple Notification Service (Amazon SNS) to notify the security operations team.

B- Use IAM System Manager State Manager to detect RDS database encryption configuration drift. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to track state changes and use Amazon Simple Notification Service (Amazon SNS) to notify the security operations team.

C- Create a read replica for the existing unencrypted RDS database and enable replica encryption in the process. Once the replica becomes active, promote it into a standalone database instance and terminate the unencrypted database instance.

D- Take a snapshot of the unencrypted RDS database. Copy the snapshot and enable snapshot encryption in the process. Restore the database instance from the newly created encrypted snapshot. Terminate the unencrypted database instance.

E- Enable encryption for the identified unencrypted RDS instance by changing the configurations of the existing database

Answer:

A, D

Question 7

Question Type: **MultipleChoice**

A company plans to create individual child accounts within an existing organization in IAM Organizations for each of its DevOps teams. IAM CloudTrail has been enabled and configured on all accounts to write audit logs to an Amazon S3 bucket in a centralized IAM account. A security engineer needs to ensure that DevOps team members are unable to modify or disable this configuration.

How can the security engineer meet these requirements?

Options:

A- Create an IAM policy that prohibits changes to the specific CloudTrail trail and apply the policy to the IAM account root user.

B- Create an S3 bucket policy in the specified destination account for the CloudTrail trail that prohibits configuration changes from the IAM account root user in the source account.

C- Create an SCP that prohibits changes to the specific CloudTrail trail and apply the SCP to the appropriate organizational unit or account in Organizations.

D- Create an IAM policy that prohibits changes to the specific CloudTrail trail and apply the policy to a new IAM group. Have team members use individual IAM accounts that are members of the new IAM group.

Answer:

D

Question 8

Question Type: MultipleChoice

A company is using IAM Organizations to develop a multi-account secure networking strategy. The company plans to use separate centrally managed accounts for shared services, auditing, and security inspection. The company plans to provide dozens of additional accounts to application owners for production and development environments.

Company security policy requires that all internet traffic be routed through a centrally managed security inspection layer in the security inspection account. A security engineer must recommend a solution that minimizes administrative overhead and complexity.

Which solution meets these requirements?

Options:

A- Use IAM Control Tower. Modify the default Account Factory networking template to automatically associate new accounts with a centrally managed VPC through a VPC peering connection and to create a default route to the VPC peer in the default route table. Create an SCP that denies the CreateInternetGateway action. Attach the SCP to all accounts except the security inspection account.

B- Create a centrally managed VPC in the security inspection account. Establish VPC peering connections between the security inspection account and other accounts. Instruct account owners to create default routes in their account route tables that point to the VPC peer. Create an SCP that denies the
Attach InternetGateway action. Attach the SCP to all accounts except the security inspection account.

C- Use IAM Control Tower. Modify the default Account Factory networking template to automatically associate new accounts with a centrally managed transit
gateway and to create a default route to the transit gateway in the default route table. Create an SCP that denies the AttachlnternetGateway action. Attach the SCP to all accounts except the security inspection account.

D- Enable IAM Resource Access Manager (IAM RAM) for IAM Organizations. Create a shared transit gateway, and make it available by using an IAM RAM resource share. Create an SCP that denies the CreateInternetGateway action. Attach the SCP to all accounts except the security inspection account. Create routes in the route tables of all accounts that point to the shared transit gateway.

Answer:

C

Question 9

Question Type: MultipleChoice

A company's cloud operations team is responsible for building effective security for IAM cross-account access. The team asks a security engineer to help troubleshoot why some developers in the developer account (123456789012) in the developers group are not able to assume a cross-account role (ReadS3) into a production account (999999999999) to read the contents of an Amazon S3 bucket (productionapp). The two account policies are as follows:

Developer account 123456789012:
Developer group permissions:

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": "sts:AssumeRole",
        "Resource": "arn:aws:iam::999999999999:role/ReadS3"
    }
}
```

Production account 999999999999:
Production account ReadS3 role policy:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "s3:ListAllMyBuckets",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
```

Production account ReadS3 role policy - trust relationship:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::888888888888:root"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "BoolIfExists": {
                    "aws:MultiFactorAuthPresent": "true"
```

Which recommendations should the security engineer make to resolve this issue? (Select TWO.)

Options:

A- Ask the developers to change their password and use a different web browser.

B- Ensure that developers are using multi-factor authentication (MFA) when they log in to their developer account as the developer role.

C- Modify the production account ReadS3 role policy to allow the PutBucketPolicy action on the productionapp S3 bucket.

D- Update the trust relationship policy on the production account S3 role to allow the account number of the developer account.

E- Update the developer group permissions in the developer account to allow access to the productionapp S3 bucket.

Answer:

A, D

Question 10

Question Type: **MultipleChoice**

A company manages multiple IAM accounts using IAM Organizations. The company's security team notices that some member accounts are not sending IAM CloudTrail logs to a centralized Amazon S3 logging bucket. The security team wants to ensure there is at least one trail configured (or all existing accounts and for any account that is created in the future.

Which set of actions should the security team implement to accomplish this?

Options:

A- Create a new trail and configure it to send CloudTrail logs to Amazon S3. Use Amazon EventBridge (Amazon CloudWatch Events) to send notification if a trail is deleted or stopped.

B- Deploy an IAM Lambda function in every account to check if there is an existing trail and create a new trail, if needed.

C- Edit the existing trail in the Organizations master account and apply it to the organization.

D- Create an SCP to deny the cloudtrail:Delete' and cloudtrail:Stop' actions. Apply the SCP to all accounts.

Answer:

C

Question 11

Question Type: MultipleChoice

An audit determined that a company's Amazon EC2 instance security group violated company policy by allowing unrestricted incoming SSH traffic. A security engineer must implement a near-real-time monitoring and alerting solution that will notify administrators of such violations.

Which solution meets these requirements with the MOST operational efficiency?

Options:

A- Create a recurring Amazon Inspector assessment run that runs every day and uses the Network Reachability package. Create an Amazon CloudWatch rule that invokes an IAM Lambda function when an assessment run starts. Configure the Lambda function to retrieve and evaluate the assessment run report when it completes. Configure the Lambda function also to publish an Amazon Simple Notification Service (Amazon SNS) notification if there are any violations for unrestricted incoming SSH traffic.

B- Use the restricted-ssh IAM Config managed rule that is invoked by security group configuration changes that are not compliant. Use the IAM Config remediation feature to publish a message to an Amazon Simple Notification Service (Amazon SNS) topic.

C- Configure VPC Flow Logs for the VPC. and specify an Amazon CloudWatch Logs group. Subscribe the CloudWatch Logs group to an IAM Lambda function that parses new log entries, detects successful connections on port 22, and publishes a notification through Amazon Simple Notification Service (Amazon SNS).

D- Create a recurring Amazon Inspector assessment run that runs every day and uses the Security Best Practices package. Create an Amazon CloudWatch rule that invokes an IAM Lambda function when an assessment run starts. Configure the Lambda function to retrieve and evaluate the assessment run report when it completes. Configure the Lambda function also to publish an Amazon Simple Notification Service (Amazon SNS) notification if there are any violations for unrestricted incoming SSH traffic.

Answer:

A