SCS-C01^Q&As^

AWS Certified Security - Specialty (SCS-C01)

Pass Amazon SCS-C01 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass2lead.com/aws-certified-security-specialty.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Your development team has started using AWS resources for development purposes. The AWS account has just been created. Your IT Security team is worried about possible leakage of AWS keys. What is the first level of measure that should be taken to protect the AWS account.

Please select:

A. Delete the AWS keys for the root account

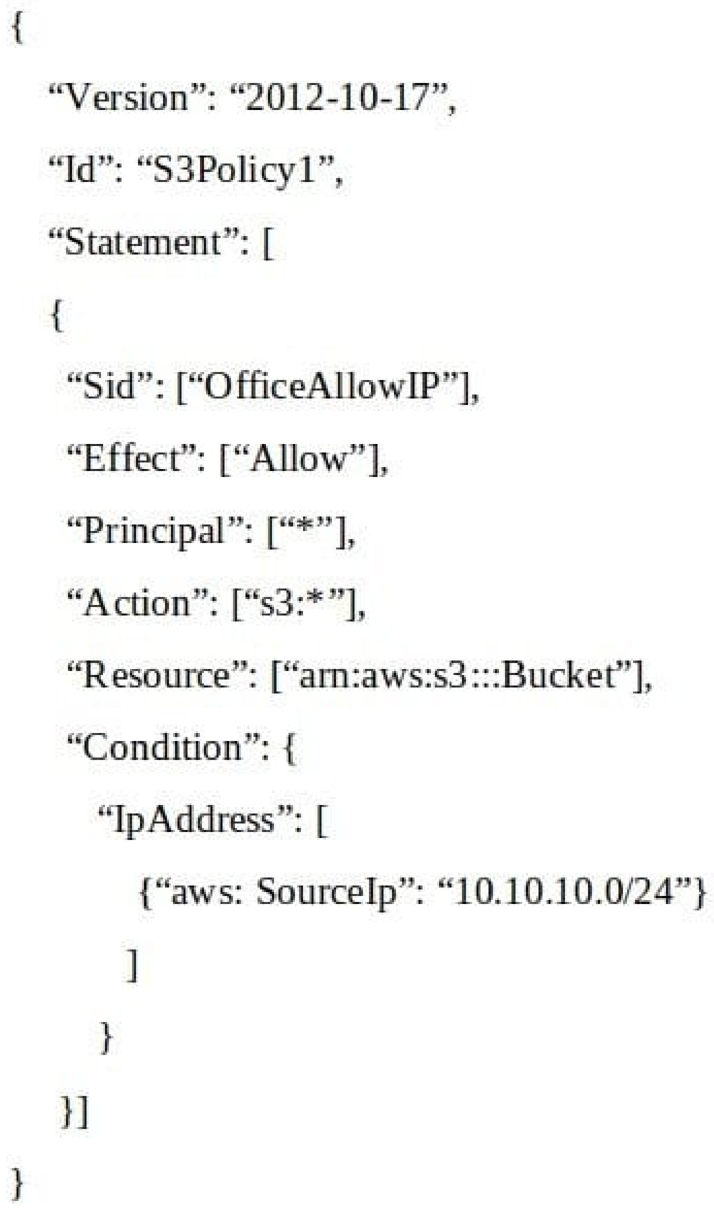
B. Create IAM Groups

C. Create IAM Roles

D. Restrict access using IAM policies

Correct Answer: A

The first level or measure that should be taken is to delete the keys for the IAM root user When you log into your account and go to your Security Access dashboard, this is the first step that can be seen



```
{
  “Version”: “2012-10-17”,
  “Id”: “S3Policy1”,
  “Statement”: [
  {
   “Sid”: [“OfficeAllowIP”],
   “Effect”: [“Allow”],
   “Principal”: [“*”],
   “Action”: [“s3:*”],
   “Resource”: [“arn:aws:s3:::Bucket”],
   “Condition”: {
     “IpAddress”: [
        {“aws: SourceIp”: “10.10.10.0/24”}
       ]
     }
  }]
}
```

Option B and C are wrong because creation of IAM groups and roles will not change the impact of leakage of AWS root access keys Option D is wrong because the first key aspect is to protect the access keys for the root account For more information on best practises for Security Access keys, please visit the below URL: https://docs.aws.amazon.com/eeneral/latest/gr/aws-access-keys-best-practices.html The correct answer is: Delete the AWS keys for the root account

QUESTION 2

An organizational must establish the ability to delete an AWS KMS Customer Master Key (CMK) within a 24-hour timeframe to keep it from being used for encrypt or decrypt operations.

Which of the following actions will address this requirement?

A. Manually rotate a key within KMS to create a new CMK immediately

B. Use the KMS import key functionality to execute a delete key operation

C. Use the schedule key deletion function within KMS to specify the minimum wait period for deletion

D. Change the KMS CMK alias to immediately prevent any services from using the CMK.

Correct Answer: C

Reference: https://docs.aws.amazon.com/kms/latest/developerguide/deleting-keys.html

QUESTION 3

You have an S3 bucket hosted in AWS. This is used to host promotional videos uploaded by yourself. You need to provide access to users for a limited duration of time. How can this be achieved? Please select:

A. Use versioning and enable a timestamp for each version

B. Use Pre-signed URL\\'s

C. Use IAM Roles with a timestamp to limit the access

D. Use IAM policies with a timestamp to limit the access

Correct Answer: B

The AWS Documentation mentions the following All objects by default are private. Only the object owner has permission to access these objects. However, the object owner can optionally share objects with others by creating a pre-signed URL using their own security credentials, to grant time-limited permission to download the objects. Option A is invalid because this can be used to prevent accidental deletion of objects Option C is invalid because timestamps are not possible for Roles Option D is invalid because policies is not the right way to limit access based on time For more information on pre-signed URL\\'s, please visit the URL: https://docs.aws.ama2on.com/AmazonS3/latest/dev/ShareObiectPreSisnedURL.html

The correct answer is: Use Pre-signed URL\\'s

QUESTION 4

A Systems Engineer has been tasked with configuring outbound mail through Simple Email Service (SES) and requires compliance with current TLS standards.

The mail application should be configured to connect to which of the following endpoints and corresponding ports?

A. email.us-east-1.amazonaws.com over port 8080

B. email-pop3.us-east-1.amazonaws.com over port 995

C. email-smtp.us-east-1.amazonaws.com over port 587

D. email-imap.us-east-1.amazonaws.com over port 993

Correct Answer: C

https://docs.aws.amazon.com/ses/latest/DeveloperGuide/smtp-connect.html

QUESTION 5

A company\\'s development team is designing an application using AWS Lambda and Amazon Elastic Container Service (Amazon ECS). The development team needs to create IAM roles to support these systems. The company\\'s security team wants to allow the developers to build IAM roles directly, but the security team wants to retain control over the permissions the developers can delegate to those roles. The development team needs access to more permissions than those required for the application\\'s AWS services. The solution must minimize management overhead.

How should the security team prevent privilege escalation for both teams?

A. Enable AWS CloudTrail. Create a Lambda function that monitors the event history for privilege escalation events and notifies the security team.

B. Create a managed IAM policy for the permissions required. Reference the IAM policy as a permissions boundary within the development team\\'s IAM role.

C. Enable AWS Organizations Create an SCP that allows the IAM CreateUser action but that has a condition that prevents API calls other than those required by the development team

D. Create an IAM policy with a deny on the IAMCreateUser action and assign the policy to the development team. Use a ticket system to allow the developers to request new IAM roles for their applications. The IAM roles will then be created by the security team.

Correct Answer: A

QUESTION 6

A company has a serverless application for internal users deployed on AWS. The application uses AWS Lambda for the front end and for business logic. The Lambda function accesses an Amazon RDS database inside a VPC The company uses AWS Systems Manager Parameter Store for storing database credentials. A recent security review highlighted the following issues

1.

The Lambda function has internet access.

2.

The relational database is publicly accessible.

3.

The database credentials are not stored in an encrypted state.

Which combination of steps should the company take to resolve these security issues? (Select THREE)

A. Disable public access to the RDS database inside the VPC

B. Move all the Lambda functions inside the VPC.

C. Edit the IAM role used by Lambda to restrict internet access.

D. Create a VPC endpoint for Systems Manager. Store the credentials as a string parameter. Change the parameter type to an advanced parameter.

E. Edit the IAM role used by RDS to restrict internet access.

F. Create a VPC endpoint for Systems Manager. Store the credentials as a SecureString parameter.

Correct Answer: BDE

Reference: https://docs.amazonaws.cn/en_us/config/latest/developerguide/operational-best-practices-for-hipaa_security.html (guidance)

QUESTION 7

A Security Administrator has a website hosted in Amazon S3. The Administrator has been given the following requirements:

Users may access the website by using an Amazon CloudFront distribution. Users may not access the website directly by using an Amazon S3 URL.

Which configurations will support these requirements? (Choose two.)

A. Associate an origin access identity with the CloudFront distribution.

B. Implement a "Principal": "cloudfront.amazonaws.com" condition in the S3 bucket policy.

C. Modify the S3 bucket permissions so that only the origin access identity can access the bucket contents.

D. Implement security groups so that the S3 bucket can be accessed only by using the intended CloudFront distribution.

E. Configure the S3 bucket policy so that it is accessible only through VPC endpoints, and place the CloudFront distribution into the specified VPC.

Correct Answer: AC

QUESTION 8

A water utility company uses a number of Amazon EC2 instances to manage updates to a fleet of 2,000 Internet of Things (IoT) field devices that monitor water quality. These devices each have unique access credentials.

An operational safety policy requires that access to specific credentials is independently auditable.

What is the MOST cost-effective way to manage the storage of credentials?

A. Use AWS Systems Manager to store the credentials as Secure Strings Parameters.Secure by using an AWS KMS key.

B. Use AWS Key Management System to store a master key, which is used to encrypt the credentials. The encrypted credentials are stored in an Amazon RDS instance.

C. Use AWS Secrets Manager to store the credentials.

D. Store the credentials in a JSON file on Amazon S3 with server-side encryption.

Correct Answer: A

https://docs.aws.amazon.com/systems-manager/latest/userguide/parameter-store-advanced-parameters.html

QUESTION 9

In order to encrypt data in transit for a connection to an AWS RDS instance, which of the following would you implement

Please select:

A. Transparent data encryption

B. SSL from your application

C. Data keys from AWS KMS

D. Data Keys from CloudHSM

Correct Answer: B

This is mentioned in the AWS Documentation You can use SSL from your application to encrypt a connection to a DB instance running MySQL MariaDB, Amazon Aurora, SQL Server, Oracle, or PostgreSQL.

Option A is incorrect since Transparent data encryption is used for data at rest and not in transit

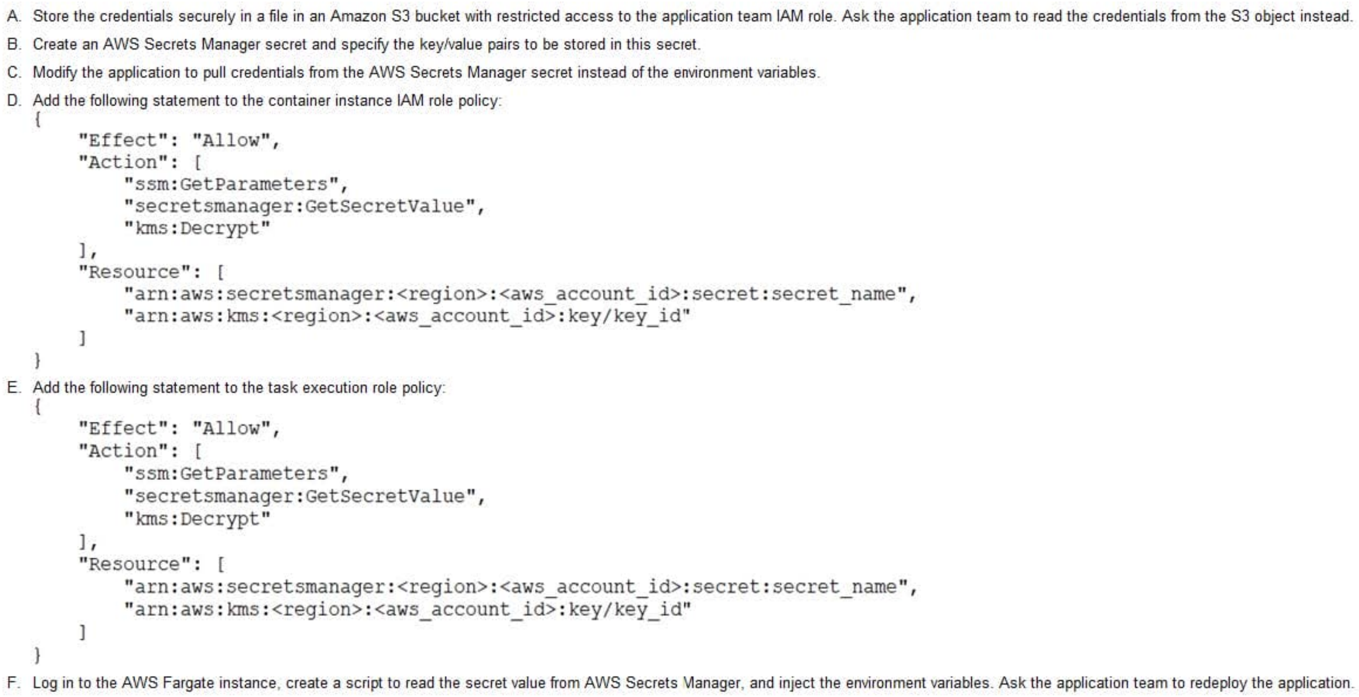
Options C and D are incorrect since keys can be used for encryption of data at rest For more information on working with RDS and SSL, please refer to below URL:

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/UsingWithRDS.SSL.html The correct answer is: SSL from your application

QUESTION 10

A recent security audit identified that a company\\'s application team injects database credentials into the environment variables of an AWS Fargate task. The company\\'s security policy mandates that all sensitive data be encrypted at rest and in transit.

When combination of actions should the security team take to make the application compliant within the security policy? (Select THREE)



A. Store the credentials securely in a file in an Amazon S3 bucket with restricted access to the application team IAM role. Ask the application team to read the credentials from the S3 object instead.

B. Create an AWS Secrets Manager secret and specify the key/value pairs to be stored in this secret.

C. Modify the application to pull credentials from the AWS Secrets Manager secret instead of the environment variables.

D. Add the following statement to the container instance IAM role policy:

```
{
    "Effect": "Allow",
    "Action": [
        "ssm:GetParameters",
        "secretsmanager:GetSecretValue",
        "kms:Decrypt"
    ],
    "Resource": [
        "arn:aws:secretsmanager:<region>:<aws_account_id>:secret:secret_name",
        "arn:aws:kms:<region>:<aws_account_id>:key/key_id"
    ]
}
```

E. Add the following statement to the task execution role policy:

```
{
    "Effect": "Allow",
    "Action": [
        "ssm:GetParameters",
        "secretsmanager:GetSecretValue",
        "kms:Decrypt"
    ],
    "Resource": [
        "arn:aws:secretsmanager:<region>:<aws_account_id>:secret:secret_name",
        "arn:aws:kms:<region>:<aws_account_id>:key/key_id"
    ]
}
```

F. Log in to the AWS Fargate instance, create a script to read the secret value from AWS Secrets Manager, and inject the environment variables. Ask the application team to redeploy the application.

A. Option A

B. Option B

C. Option C

D. Option D

E. Option E

F. Option F

Correct Answer: AEF

QUESTION 11

A company is developing a mobile shopping web app. The company needs an environment that is configured to encrypt all resources in transit and at rest.

A security engineer must develop a solution that will encrypt traffic in transit to the company\\'s Application Load Balancer and Amazon API Gateway resources. The solution also must encrypt traffic at rest for Amazon S3 storage.

What should the security engineer do to meet these requirements?

A. Use AWS Certificate Manager (ACM) for encryption in transit. Use AWS Key Management Service for encryption at rest.

B. Use AWS Certificate Manager (ACM) for encryption in transit and encryption at rest.

C. Use AWS Key Management Service for encryption in transit. Use AWS Certificate Manager (ACM) for encryption at rest.

D. Use AWS Key Management Service for encryption in transit and encryption at rest.

Correct Answer: A

QUESTION 12

A company has an application hosted in an Amazon EC2 instance and wants the application to access secure strings stored in AWS Systems Manager Parameter Store. When the application tries to access the secure string key value, it fails. Which factors could be the cause of this failure? (Choose two.)

A. The EC2 instance role does not have decrypt permissions on the AWS Key Management Sen/ice (AWS KMS) key used to encrypt the secret

B. The EC2 instance role does not have read permissions to read the parameters In Parameter Store

C. Parameter Store does not have permission to use AWS Key Management Service (AWS KMS) to decrypt the parameter

D. The EC2 instance role does not have encrypt permissions on the AWS Key Management Service (AWS KMS) key associated with the secret

E. The EC2 instance does not have any tags associated.

Correct Answer: BC

QUESTION 13

A company uses AWS Certificate Manager (ACM) to automate the renewal of SSL/TLS certificates that the company\\'s Elastic Load Balancers use. The company recently noticed that ACM was unable to automatically renew some certificates.

These certificates have a status of "pending validation" in the ACM console.

A security engineer configured the certificates by using DNS validation. The security engineer has verified that the existing certificates have not expired.

What should the security engineer do to correct this issue?

A. Manually validate ownership of each domain in the ACM console.

B. Verify that the DNS CNAME for each domain matches the ACM certificate CNAME record.

C. Export and then reimport the certificates into ACM.

D. Validate the ownership of each domain by using email validation.

Correct Answer: D

QUESTION 14

An application uses Amazon Cognito to manage end users\\' permissions when directly accessing AWS resources, including Amazon DynamoDB. A new feature request reads as follows:

Provide a mechanism to mark customers as suspended pending investigation or suspended permanently. Customers should still be able to log in when suspended, but should not be able to make changes.

The priorities are to reduce complexity and avoid potential for future security issues.

Which approach will meet these requirements and priorities?

A. Create a new database field "suspended_status" and modify the application logic to validate that field when processing requests.

B. Add suspended customers to second Cognito user pool and update the application login flow to check both user pools.

C. Use Amazon Cognito Sync to push out a "suspension_status" parameter and split the IAM policy into normal users and suspended users.

D. Move suspended customers to a second Cognito group and define an appropriate IAM access policy for the group.

Correct Answer: D

https://aws.amazon.com/blogs/aws/new-amazon-cognito-groups-and-fine-grained-role-based-access-control-2/

QUESTION 15

An Amazon EC2 instance is denied access to a newly created AWS KMS CMK used for decrypt actions. The environment has the following configuration:

1.

The instance is allowed the kms:Decrypt action in its IAM role for all resources

2.

The AWS KMS CMK status is set to enabled

3.

The instance can communicate with the KMS API using a configured VPC endpoint What is causing the issue?

A. The kms:GenerateDataKey permission is missing from the EC2 instance\\'s IAM role

B. The ARN tag on the CMK contains the EC2 instance\\'s ID instead of the instance\\'s ARN

C. The kms:Encrypt permission is missing from the EC2 IAM role

D. The KMS CMK key policy that enables IAM user permissions is missing

Correct Answer: A

In a key policy, you use "*" for the resource, which means "this CMK." A key policy applies only to the CMK it is attached to Reference: https://docs.aws.amazon.com/kms/latest/developerguide/key-policies.html

Latest SCS-C01 Dumps   SCS-C01 Practice Test   SCS-C01 Exam Questions