DUMPSQUEEN

# AWS Certified Security - Specialty

## Amazon Web Services SCS-C02

## Version Demo

**Total Demo Questions: 15**

**Total Premium Questions: 235**

**Buy Premium PDF**

https://dumpsqueen.com

support@dumpsqueen.com

## QUESTION NO: 1

During a manual review of system logs from an Amazon Linux EC2 instance, a Security Engineer noticed that there are sudo commands that were never properly alerted or reported on the Amazon CloudWatch Logs agent Why were there no alerts on the sudo commands?

**A.** There is a security group blocking outbound port 80 traffic that is preventing the agent from sending the logs

**B.** The IAM instance profile on the EC2 instance was not properly configured to allow the CloudWatch Logs agent to push the logs to CloudWatch

**C.** CloudWatch Logs status is set to ON versus SECURE, which prevents it from pulling in OS security event logs

**D.** The VPC requires that all traffic go through a proxy, and the CloudWatch Logs agent does not support a proxy configuration.

**ANSWER: B**

## QUESTION NO: 2

A company has a web server in the AWS Cloud. The company will store the content for the web server in an Amazon S3 bucket. A security engineer must use an Amazon CloudFront distribution to speed up delivery of the content. None of the files can be publicly accessible from the S3 bucket direct.

Which solution will meet these requirements?

**A.** Configure the permissions on the individual files in the S3 bucket so that only the CloudFront distribution has access to them.

**B.** Create an origin access identity (OAI). Associate the OAI with the CloudFront distribution. Configure the S3 bucket permissions so that only the OAI can access the files in the S3 bucket.

**C.** Create an S3 role in AWS Identity and Access Management (IAM). Allow only the CloudFront distribution to assume the role to access the files in the S3 bucket.

**D.** Create an S3 bucket policy that uses only the CloudFront distribution ID as the principal and the Amazon Resource Name (ARN) as the target.

**ANSWER: B**

## QUESTION NO: 3

A company usesAWS Organizations to run workloads in multiple AWS accounts Currently the individual team members at the company access all Amazon EC2 instances remotely by using SSH or Remote Desktop Protocol (RDP) The company

does not have any audit trails and security groups are occasionally open The company must secure access management and implement a centralized togging solution

Which solution will meet these requirements MOST securely?

**A.** Configure trusted access for AWS System Manager in Organizations Configure a bastion host from the management account Replace SSH and RDP by using Systems Manager Session Manager from the management account Configure Session Manager logging to Amazon CloudWatch Logs

**B.** Replace SSH and RDP with AWS Systems Manager Session Manager Install Systems Manager Agent (SSM Agent) on the instances Attach the

**C.** AmazonSSMManagedInstanceCore role to the instances Configure session data streaming to Amazon CloudWatch Logs Create a separate logging account that has appropriate cross-account permissions to audit the log data

**D.** Install a bastion host in the management account Reconfigure all SSH and RDP to allow access only from the bastion host Install AWS Systems Manager Agent (SSM Agent) on the bastion host Attach the AmazonSSMManagedInstanceCore role to the bastion host Configure session data streaming to Amazon CloudWatch Logs in a separate logging account to audit log data

**E.** Replace SSH and RDP with AWS Systems Manager State Manager Install Systems Manager Agent (SSM Agent) on the instances Attach the AmazonSSMManagedInstanceCore role to the instances Configure session data streaming to Amazon CloudTrail Use CloudTrail Insights to analyze the trail data

**ANSWER: C**

**Explanation:**

To meet the requirements of securing access management and implementing a centralized logging solution, the most secure solution would be to:

• Install a bastion host in the management account.

• Reconfigure all SSH and RDP to allow access only from the bastion host.

• Install AWS Systems Manager Agent (SSM Agent) on the bastion host.

• Attach the AmazonSSMManagedInstanceCore role to the bastion host.

• Configure session data streaming to Amazon CloudWatch Logs in a separate logging account to audit log data

This solution provides the following security benefits:

• It uses AWS Systems Manager Session Manager instead of traditional SSH and RDP protocols, which provides a secure method for accessing EC2 instances without requiring inbound firewall rules or open ports.

• It provides audit trails by configuring Session Manager logging to Amazon CloudWatch Logs and creating a separate logging account to audit the log data.

• It uses the AWS Systems Manager Agent to automate common administrative tasks and improve the security posture of the instances.

• The separate logging account with cross-account permissions provides better data separation and improves security posture.

https://aws.amazon.com/solutions/implementations/centralized-logging/

## QUESTION NO: 4

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.)

**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://IAM.amazon.com/premiumsupport/knowledge-center/cloudfront-geo-restriction/

## QUESTION NO: 5

An organization wants to log all IAM API calls made within all of its IAM accounts, and must have a central place to analyze these logs. What steps should be taken to meet these requirements in the MOST secure manner? (Select TWO)

**A.** Turn on IAM CloudTrail in each IAM account

**B.** Turn on CloudTrail in only the account that will be storing the logs

**C.** Update the bucket ACL of the bucket in the account that will be storing the logs so that other accounts can log to it

**D.** Create a service-based role for CloudTrail and associate it with CloudTrail in each account

**E.** Update the bucket policy of the bucket in the account that will be storing the logs so that other accounts can log to it

**ANSWER: A E**

## QUESTION NO: 6

A Security Engineer creates an Amazon S3 bucket policy that denies access to all users. A few days later, the Security Engineer adds an additional statement to the bucket policy to allow read-only access to one other employee. Even after updating the policy, the employee still receives an access denied message.

What is the likely cause of this access denial?

**A.** The ACL in the bucket needs to be updated

**B.** The IAM policy does not allow the user to access the bucket

**C.** It takes a few minutes for a bucket policy to take effect

**D.** The allow permission is being overridden by the deny

**ANSWER: D**

## QUESTION NO: 7

A company is building a data processing application mat uses AWS Lambda functions. The application's

Lambda functions need to communicate with an Amazon RDS OB instance that is deployed within a VPC in the same AWS account

Which solution meets these requirements in the MOST secure way?

**A.** Configure the DB instance to allow public access Update the DB instance security group to allow access from the Lambda public address space for the AWS Region

**B.** Deploy the Lambda functions inside the VPC Attach a network ACL to the Lambda subnet Provide outbound rule access to the VPC CIDR range only Update the DB instance security group to allow traffic from 0.0.0.0/0

**C.** Deploy the Lambda functions inside the VPC Attach a security group to the Lambda functions Provide outbound rule access to the VPC CIDR range only Update the DB instance security group to allow traffic from the Lambda security group

**D.** Peer the Lambda default VPC with the VPC that hosts the DB instance to allow direct network access without the need for security groups

**ANSWER: C**

**Explanation:**

This solution ensures that the Lambda functions are deployed inside the VPC and can communicate with the Amazon RDS DB instance securely. The security group attached to the Lambda functions only allows outbound traffic to the VPC CIDR range, and the DB instance security group only allows traffic from the Lambda security group. This solution ensures that the Lambda functions can communicate with the DB instance securely and that the DB instance is not exposed to the public internet.

## QUESTION NO: 8

A company's Chief Security Officer has requested that a Security Analyst review and improve the security posture of each company IAM account The Security Analyst decides to do this by Improving IAM account root user security.

Which actions should the Security Analyst take to meet these requirements? (Select THREE.)

**A.** Delete the access keys for the account root user in every account.

**B.** Create an admin IAM user with administrative privileges and delete the account root user in every account.

**C.** Implement a strong password to help protect account-level access to the IAM Management Console by the account root user.

**D.** Enable multi-factor authentication (MFA) on every account root user in all accounts.

**E.** Create a custom IAM policy to limit permissions to required actions for the account root user and attach the policy to the account root user.

**F.** Attach an IAM role to the account root user to make use of the automated credential rotation in IAM STS.

**ANSWER: A D E**

## QUESTION NO: 9

A recent security audit found that IAM CloudTrail logs are insufficiently protected from tampering and unauthorized access Which actions must the Security Engineer take to address these audit findings? (Select

THREE )

**A.** Ensure CloudTrail log file validation is turned on

**B.** Configure an S3 lifecycle rule to periodically archive CloudTrail logs into Glacier for long-term storage

**C.** Use an S3 bucket with tight access controls that exists m a separate account

**D.** Use Amazon Inspector to monitor the file integrity of CloudTrail log files.

**E.** Request a certificate through ACM and use a generated certificate private key to encrypt CloudTrail log files

**F.** Encrypt the CloudTrail log files with server-side encryption with IAM KMS-managed keys (SSE-KMS)

**ANSWER: A D E**

## QUESTION NO: 10

An application is running on an Amazon EC2 instance that has an IAM role attached. The IAM role provides access to an AWS Key Management Service (AWS KMS) customer managed key and an Amazon S3 bucket. The key is used to access 2 TB of sensitive data that is stored in the S3 bucket.

A security engineer discovers a potential vulnerability on the EC2 instance that could result in the compromise of the sensitive data. Due to other critical operations, the security engineer cannot immediately shut down the EC2 instance for vulnerability patching.

What is the FASTEST way to prevent the sensitive data from being exposed?

**A.** Download the data from the existing S3 bucket to a new EC2 instance. Then delete the data from the S3 bucket. Re-encrypt the data with a client-based key. Upload the data to a new S3 bucket.

**B.** Block access to the public range of S3 endpoint IP addresses by using a host-based firewall. Ensure that internet-bound traffic from the affected EC2 instance is routed through the host-based firewall.

**C.** Revoke the IAM role's active session permissions. Update the S3 bucket policy to deny access to the IAM role. Remove the IAM role from the EC2 instance profile.

**D.** Disable the current key. Create a new KMS key that the IAM role does not have access to, and re-encrypt all the data with the new key. Schedule the compromised key for deletion.

**ANSWER: D**

## QUESTION NO: 11

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.)

**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 NO: 12

You need to create a policy and apply it for just an individual user. How could you accomplish this in the right way?

Please select:

**A.** Add an IAM managed policy for the user

**B.** Add a service policy for the user

**C.** Add an IAM role for the user

**D.** Add an inline policy for the user

**ANSWER: D**

**Explanation:**

Options A and B are incorrect since you need to add an inline policy just for the user

Option C is invalid because you don't assign an IAM role to a user

The IAM Documentation mentions the following

An inline policy is a policy that's embedded in a principal entity (a user, group, or role)—that is, the policy is an inherent part of the principal entity. You can create a policy and embed it in a principal entity, either when you create the principal entity or later.

For more information on IAM Access and Inline policies, just browse to the below URL:
https://docs.IAM.amazon.com/IAM/latest/UserGuide/access

The correct answer is: Add an inline policy for the user Submit your Feedback/Queries to our Experts

**QUESTION NO: 13**

A company's Security Engineer is copying all application logs to centralized Amazon S3 buckets. Currently, each of the company's applications is in its own IAM account, and logs are pushed into S3 buckets associated with each account. The Engineer will deploy an IAM Lambda function into each account that copies the relevant log files to the centralized S3 bucket.

The Security Engineer is unable to access the log files in the centralized S3 bucket. The Engineer's IAM user policy from the centralized account looks like this:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": "s3:Put*",
            "Resource":"arn:aws:s3:::centralizedbucket/*",
            "Effect": "Deny"
        },
        {
            "Action": ["s3:Get*","s3:List*"],
            "Resource": [
                "arn:aws:s3:::centralizedbucket/*",
                "arn:aws:s3:::centralizedbucket/"
            ],
            "Effect": "Allow"
        }
    ]
}
```

The centralized S3 bucket policy looks like this:

```
{
    "Version": "2012-10-17",    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::111122223333:role/LogCopier",
                    "arn:aws:iam::444455556666:role/LogCopier"
                ]
            },
            "Action": ["s3:PutObject","s3:PutObjectAcl"],
            "Resource": "arn:aws:s3:::centralizedbucket/*"
        }
    ]
}
```

Why is the Security Engineer unable to access the log files?

**A.** The S3 bucket policy does not explicitly allow the Security Engineer access to the objects in the bucket.

**B.** The object ACLs are not being updated to allow the users within the centralized account to access the objects

**C.** The Security Engineers IAM policy does not grant permissions to read objects in the S3 bucket

**D.** The s3:PutObject and s3:PutObjectAcl permissions should be applied at the S3 bucket level

**ANSWER: C**

## QUESTION NO: 14

A company has two AWS accounts. One account is for development workloads. The other account is for production workloads. For compliance reasons the production account contains all the AWS Key Management. Service (AWS KMS) keys that the company uses for encryption.

The company applies an IAM role to an AWS Lambda function in the development account to allow secure access to AWS resources. The Lambda function must access a specific KMS customer managed key that exists in the production account to encrypt the Lambda function's data.

Which combination of steps should a security engineer take to meet these requirements? (Select TWO.)

**A.** Configure the key policy for the customer managed key in the production account to allow access to the Lambda service.

**B.** Configure the key policy for the customer managed key in the production account to allow access to the IAM role of the Lambda function in the development account.

**C.** Configure a new IAM policy in the production account with permissions to use the customer managed key. Apply the IAM policy to the IAM role that the Lambda function in the development account uses.

**D.** Configure a new key policy in the development account with permissions to use the customer managed key. Apply the key policy to the IAM role that the Lambda function in the development account uses.

**E.** Configure the IAM role for the Lambda function in the development account by attaching an IAM policy that allows access to the customer managed key in the production account.

## ANSWER: B E

**Explanation:**

To allow a Lambda function in one AWS account to access a KMS customer managed key in another AWS account, the following steps are required:

• Configure the key policy for the customer managed key in the production account to allow access to the IAM role of the Lambda function in the development account. A key policy is a resource-based policy that defines who can use or manage a KMS key. To grant cross-account access to a KMS key, you must specify the AWS account ID and the IAM role ARN of the external principal in the key policy statement. For more information, see Allowing users in other accounts to use a KMS key.

• Configure the IAM role for the Lambda function in the development account by attaching an IAM policy that allows access to the customer managed key in the production account. An IAM policy is an identity-based policy that defines what actions an IAM entity can perform on which resources. To allow an IAM role to use a KMS key in another account, you must specify the KMS key ARN and the kms:Encrypt action (or any other action that requires access to the KMS key) in the IAM policy statement. For more information, see Using IAM policies with AWS KMS.

This solution will meet the requirements of allowing secure access to a KMS customer managed key across AWS accounts.

The other options are incorrect because they either do not grant cross-account access to the KMS key (A, C), or do not use a valid policy type for KMS keys (D).

Verified

References:

• https://docs.aws.amazon.com/kms/latest/developerguide/key-policy-modifying-external-accounts.html
https://docs.aws.amazon.com/kms/latest/developerguide/iam-policies.html

## QUESTION NO: 15

A company is undergoing a layer 3 and layer 4 DDoS attack on its web servers running on IAM.

Which combination of IAM services and features will provide protection in this scenario? (Select THREE).

**A.** Amazon Route 53

**B.** IAM Certificate Manager (ACM)

**C.** Amazon S3

**D.** IAM Shield

**E.** Elastic Load Balancer

**F.** Amazon GuardDuty

## ANSWER: D E F