# SCS-C02 Q&As

AWS Certified Security - Specialty

## Pass Amazon SCS-C02 Exam with 100% Guarantee

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

**https://www.pass4itsure.com/scs-c02.html**

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

**QUESTION 1**

A company has contracted with a third party to audit several AWS accounts. To enable the audit, cross-account IAM roles have been created in each account targeted for audit. The Auditor is having trouble accessing some of the accounts.

Which of the following may be causing this problem? (Choose three.)

A. The external ID used by the Auditor is missing or incorrect.

B. The Auditor is using the incorrect password.

C. The Auditor has not been granted sts:AssumeRole for the role in the destination account.

D. The Amazon EC2 role used by the Auditor must be set to the destination account role.

E. The secret key used by the Auditor is missing or incorrect.

F. The role ARN used by the Auditor is missing or incorrect.

Correct Answer: ACF

The following may be causing the problem for the Auditor:

A. The external ID used by the Auditor is missing or incorrect. This is a possible cause, because the external ID is a unique identifier that is used to establish a trust relationship between the accounts. The external ID must match the one that is specified in the role\\'s trust policy in the destination account. C. The Auditor has not been granted sts:AssumeRole for the role in the destination account. This is a possible cause, because sts:AssumeRole is the API action that allows the Auditor to assume the cross-account role and obtain temporary credentials. The Auditor must have an IAM policy that allows them to call sts:AssumeRole for the role ARN in the destination account. F. The role ARN used by the Auditor is missing or incorrect. This is a possible cause, because the role ARN is the Amazon Resource Name of the cross-account role that the Auditor wants to assume. The role ARN must be valid and exist in the destination account.

**QUESTION 2**

A company\\'s security team needs to receive a notification whenever an AWS access key has not been rotated in 90 or more days. A security engineer must develop a solution that provides these notifications automatically.

Which solution will meet these requirements with the LEAST amount of effort?

A. Deploy an AWS Config managed rule to run on a periodic basis of 24 hours. Select the access-keys-rotated managed rule, and set the maxAccessKeyAge parameter to 90 days. Create an Amazon EventBridge (Amazon CloudWatch Events) rule with an event pattern that matches the compliance type of NON_COMPLIANT from AWS Config for the managed rule. Configure EventBridge (CloudWatch Events) to send an Amazon Simple Notification Service (Amazon SNS) notification to the security team.

B. Create a script to export a .csv file from the AWS Trusted Advisor check for IAM access key rotation. Load the script into an AWS Lambda function that will upload the .csv file to an Amazon S3 bucket. Create an Amazon Athena table query that runs when the .csv file is uploaded to the S3 bucket. Publish the results for any keys older than 90 days by using an invocation of an Amazon Simple Notification Service (Amazon SNS) notification to the security team.

C. Create a script to download the IAM credentials report on a periodic basis. Load the script into an AWS Lambda

function that will run on a schedule through Amazon EventBridge (Amazon CloudWatch Events). Configure the Lambda script to load the report into memory and to filter the report for records in which the key was last rotated at least 90 days ago. If any records are detected, send an Amazon Simple Notification Service (Amazon SNS) notification to the security team.

D. Create an AWS Lambda function that queries the IAM API to list all the users. Iterate through the users by using the ListAccessKeys operation. Verify that the value in the CreateDate field is not at least 90 days old. Send an Amazon Simple Notification Service (Amazon SNS) notification to the security team if the value is at least 90 days old. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to schedule the Lambda function to run each day.

Correct Answer: A

**QUESTION 3**

A company has an AWS Lambda function that creates image thumbnails from larger images. The Lambda function needs read and write access to an Amazon S3 bucket in the same AWS account.

Which solutions will provide the Lambda function this access? (Select TWO.)

A. Create an IAM user that has only programmatic access. Create a new access key pair. Add environmental variables to the Lambda function with the ac-cess key ID and secret access key. Modify the Lambda function to use the environmental variables at run time during communication with Amazon S3.

B. Generate an Amazon EC2 key pair. Store the private key in AWS Secrets Man-ager. Modify the Lambda function to retrieve the private key from Secrets Manager and to use the private key during communication with Amazon S3.

C. Create an IAM role for the Lambda function. Attach an IAM policy that al-lows access to the S3 bucket.

D. Create an IAM role for the Lambda function. Attach a bucket policy to the S3 bucket to allow access. Specify the function\\'s IAM role as the princi-pal.

E. Create a security group. Attach the security group to the Lambda function. Attach a bucket policy that allows access to the S3 bucket through the se-curity group ID.

Correct Answer: CD

**QUESTION 4**

A company is using Amazon Route 53 Resolver for its hybrid DNS infrastructure. The company has set up Route 53 Resolver forwarding rules for authoritative domains that are hosted on on-premises DNS servers.

A new security mandate requires the company to implement a solution to log and query DNS traffic that goes to the on-premises DNS servers. The logs must show details of the source IP address of the instance from which the query originated. The logs also must show the DNS name that was requested in Route 53 Resolver.

Which solution will meet these requirements?

A. Use VPC Traffic Mirroring. Configure all relevant elastic network interfaces as the traffic source, include amazon-dns in the mirror filter, and set Amazon CloudWatch Logs as the mirror target. Use CloudWatch Insights on the mirror session logs to run queries on the source IP address and DNS name.

B. Configure VPC flow logs on all relevant VPCs. Send the logs to an Amazon S3 bucket. Use Amazon Athena to run SQL queries on the source IP address and DNS name.

C. Configure Route 53 Resolver query logging on all relevant VPCs. Send the logs to Amazon CloudWatch Logs. Use CloudWatch Insights to run queries on the source IP address and DNS name.

D. Modify the Route 53 Resolver rules on the authoritative domains that forward to the on-premises DNS servers. Send the logs to an Amazon S3 bucket. Use Amazon Athena to run SQL queries on the source IP address and DNS name.

Correct Answer: C

According to the AWS documentation, Route 53 Resolver query logging lets you log the DNS queries that Route 53 Resolver handles for your VPCs. You can send the logs to CloudWatch Logs, Amazon S3, or Kinesis Data Firehose. The logs include information such as the following:

The AWS Region where the VPC was created The ID of the VPC that the query originated from The IP address of the instance that the query originated from The instance ID of the resource that the query originated from The date and time that the query was first made The DNS name requested (such as prod.example.com) The DNS record type (such as A or AAAA) The DNS response code, such as NoError or ServFail The DNS response data, such as the IP address that is returned in response to the DNS query You can use CloudWatch Insights to run queries on your log data and analyze the results using graphs and statistics. You can filter and aggregate the log data based on any field, and use operators and functions to perform calculations and transformations. For example, you can use CloudWatch Insights to find out how many queries were made for a specific domain name, or which instances made the most queries. Therefore, this solution meets the requirements of logging and querying DNS traffic that goes to the on-premises DNS servers, showing details of the source IP address of the instance from which the query originated, and the DNS name that was requested in Route 53 Resolver.

The other options are incorrect because:

A. Using VPC Traffic Mirroring would not capture the DNS queries that go to the on-premises DNS servers, because Traffic Mirroring only copies network traffic from an elastic network interface of an EC2 instance to a target for analysis. Traffic Mirroring does not include traffic that goes through a Route 53 Resolver outbound endpoint, which is used to forward queries to on-premises DNS servers. Therefore, this solution would not meet the requirements. B. Configuring VPC flow logs on all relevant VPCs would not capture the DNS name that was requested in Route 53 Resolver, because flow logs only record information about the IP traffic going to and from network interfaces in a VPC. Flow logs do not include any information about the content or payload of a packet, such as a DNS query or response. Therefore, this solution would not meet the requirements. D. Modifying the Route 53 Resolver rules on the authoritative domains that forward to the on-premises DNS servers would not enable logging of DNS queries, because Resolver rules only specify how to forward queries for specified domain names to your network. Resolver rules do not have any logging functionality by themselves. Therefore, this solution would not meet the requirements.

References:

1: Resolver query logging -Amazon Route 53

2: Analyzing log data with CloudWatch Logs Insights -Amazon CloudWatch

3: What is Traffic Mirroring -Amazon Virtual Private Cloud

4: Outbound Resolver endpoints -Amazon Route 53

5: Logging IP traffic using VPC Flow Logs -Amazon Virtual Private Cloud

6: Managing forwarding rules -Amazon Route 53

**QUESTION 5**

A company created an IAM account for its developers to use for testing and learning purposes Because MM account will

be shared among multiple teams of developers, the company wants to restrict the ability to stop and terminate Amazon EC2 instances so that a team can perform these actions only on the instances it owns.

Developers were Instructed to tag al their instances with a Team tag key and use the team name in the tag value One of the first teams to use this account is Business Intelligence A security engineer needs to develop a highly scalable solution for providing developers with access to the appropriate resources within the account The security engineer has already created individual IAM roles for each team.

Which additional configuration steps should the security engineer take to complete the task?

A. For each team, create an AM policy similar to the one that fellows Populate the ec2: ResourceTag/Team condition key with a proper team name Attach resulting policies to the corresponding IAM roles.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "NotAction": [
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ]
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/Team": "BusinessIntelligence"
                }
            }
        }
    ]
}
```

B. For each team create an IAM policy similar to the one that follows Populate the IAM TagKeys/Team condition key with a proper team name. Attach the resuming policies to the corresponding IAM roles.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "NotAction": [
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys/Team": "BusinessIntelligence"
                }
            }
        }
    ]
}
```

C. Tag each IAM role with a Team lag key. and use the team name in the tag value. Create an IAM policy similar to the one that follows, and attach 4 to all the IAM roles used by developers.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "NotAction": [
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/Team": "${aws:PrincipalTag/Team}"
                }
            }
        }
    ]
}
```

D. Tag each IAM role with the Team key, and use the team name in the tag value. Create an IAM policy similar to the one that follows, and it to all the IAM roles used by developers.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "NotAction": [
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys/Team": "${aws:PrincipalTag/Team}"
                }
            }
        }
    ]
}
```

A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: A

**QUESTION 6**

A company plans to use AWS Key Management Service (AWS KMS) to implement an encryption strategy to protect data at rest. The company requires client-side encryption for company projects. The company is currently conducting multiple projects to test the company\\'s use of AWS KMS. These tests have led to a sudden increase in the company\\'s AWS resource consumption. The test projects include applications that issue multiple requests each second to KMS endpoints for encryption activities.

The company needs to develop a solution that does not throttle the company\\'s ability to use AWS KMS. The solution must improve key usage for client-side encryption and must be cost optimized.

Which solution will meet these requirements?

A. Use keyrings with the AWS Encryption SDK. Use each keyring individually or combine keyrings into a multi-keyring. Decrypt the data by using a keyring that has the primary key in the multi-keyring.

B. Use data key caching. Use the local cache that the AWS Encryption SDK provides with a caching cryptographic materials manager.

C. Use KMS key rotation. Use a local cache in the AWS Encryption SDK with a caching cryptographic materials manager.

D. Use keyrings with the AWS Encryption SDK. Use each keyring individually or combine keyrings into a multi-keyring. Use any of the wrapping keys in the multi-keyring to decrypt the data.

Correct Answer: B

The correct answer is B. Use data key caching. Use the local cache that the AWS Encryption SDK provides with a caching cryptographic materials manager. This answer is correct because data key caching can improve performance, reduce cost, and help the company stay within the service limits of AWS KMS. Data key caching stores data keys and related cryptographic material in a cache, and reuses them for encryption and decryption operations. This reduces the number of requests to AWS KMS endpoints and avoids throttling. The AWS Encryption SDK provides a local cache and a caching cryptographic materials manager (caching CMM) that interacts with the cache and enforces security thresholds that the company can set. The other options are incorrect because:

A. Using keyrings with the AWS Encryption SDK does not address the problem of throttling or cost optimization. Keyrings are used to generate, encrypt, and decrypt data keys, but they do not cache or reuse them. Using each keyring individually or combining them into a multi-keyring does not reduce the number of requests to AWS KMS endpoints.

C. Using KMS key rotation does not address the problem of throttling or cost optimization. Key rotation is a security practice that creates new cryptographic material for a KMS key every year, but it does not affect the data that the KMS key protects. Key rotation does not reduce the number of requests to AWS KMS endpoints, and it might incur additional costs for storing multiple versions of key material. D. Using keyrings with the AWS Encryption SDK does not address the problem of throttling or cost optimization, as explained in option A. Moreover, using any of the wrapping keys in the

multi-keyring to decrypt the data is not a valid option, because only one of the wrapping keys can decrypt a given data key. The wrapping key that encrypts a data key is stored in the encrypted data key structure, and only that wrapping key can decrypt it.

References:

1: Data key caching -AWS Encryption SDK

2: Using keyrings-AWS Encryption SDK

3: Rotating AWS KMS keys -AWS Key Management Service

4: How keyrings work -AWS Encryption SDK

**QUESTION 7**

A company is designing a new application stack. The design includes web servers and backend servers that are hosted on Amazon EC2 instances. The design also includes an Amazon Aurora MySQL DB cluster.

The EC2 instances are m an Auto Scaling group that uses launch templates. The EC2 instances for the web layer and the backend layer are backed by Amazon Elastic Block Store (Amazon EBS) volumes. No layers are encrypted at rest. A security engineer needs to implement encryption at rest.

Which combination of steps will meet these requirements? (Select TWO.)

A. Modify EBS default encryption settings in the target AWS Region to enable encryption. Use an Auto Scaling group instance refresh.

B. Modify the launch templates for the web layer and the backend layer to add AWS Certificate Manager (ACM) encryption for the attached EBS volumes. Use an Auto Scaling group instance refresh.

C. Create a new AWS Key Management Service (AWS KMS) encrypted DB cluster from a snapshot of the existing DB cluster.

D. Apply AWS Key Management Service (AWS KMS) encryption to the existing DB cluster.

E. Apply AWS Certificate Manager (ACM) encryption to the existing DB cluster.

Correct Answer: AC

To implement encryption at rest for both the EC2 instances and the Aurora DB cluster, the following steps are required: For the EC2 instances, modify the EBS default encryption settings in the target AWS Region to enable encryption. This will ensure that any new EBS volumes created in that Region are encrypted by default using an AWS managed key. Alternatively, you can specify a customer managed key when creating new EBS volumes. For more information, see Amazon EBS encryption. Use an Auto Scaling group instance refresh to replace the existing EC2 instances with new ones that have encrypted EBS volumes attached. An instance refresh is a feature that helps you update all instances in an Auto Scaling group in a rolling fashion without the need to manage the instance replacement process manually. For more information, see Replacing Auto Scaling instances based on an instance refresh. For the Aurora DB cluster, create a new AWS Key Management Service (AWS KMS) encrypted DB cluster from a snapshot of the existing DB cluster. You can use either an AWS managed key or a customer managed key to encrypt the new DB cluster. You cannot enable or disable encryption for an existing DB cluster, so you have to create a new one from a snapshot. For more information, see Encrypting Amazon Aurora resources. The other options are incorrect because they either do not enable encryption at rest for the resources (B, D), or they use the wrong service for encryption (E). Verified References:
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html
https://docs.aws.amazon.com/autoscaling/ec2/userguide/asg-instance-refresh.html

https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Overview.Encryption.html

**QUESTION 8**

A company uses AWS Organizations to manage a small number of AWS accounts. However, the company plans to add 1 000 more accounts soon. The company allows only a centralized security team to create IAM roles for all AWS accounts and teams. Application teams submit requests for IAM roles to the security team. The security team has a backlog of IAM role requests and cannot review and provision the IAM roles quickly.

The security team must create a process that will allow application teams to provision their own IAM roles. The process must also limit the scope of IAM roles and prevent privilege escalation. Which solution will meet these requirements with the LEAST operational overhead?

A. Create an IAM group for each application team. Associate policies with each IAM group. Provision IAM users for each application team member. Add the new IAM users to the appropriate IAM group by using role-based access control (RBAC).

B. Delegate application team leads to provision IAM rotes for each team. Conduct a quarterly review of the IAM rotes the team leads have provisioned. Ensure that the application team leads have the appropriate training to review IAM roles.

C. Put each AWS account in its own OU. Add an SCP to each OU to grant access to only the AWS services that the teams plan to use. Include conditions tn the AWS account of each team.

D. Create an SCP and a permissions boundary for IAM roles. Add the SCP to the root OU so that only roles that have the permissions boundary attached can create any new IAM roles.

Correct Answer: D

To create a process that will allow application teams to provision their own IAM roles, while limiting the scope of IAM roles and preventing privilege escalation, the following steps are required: Create a service control policy (SCP) that defines the maximum permissions that can be granted to any IAM role in the organization. An SCP is a type of policy that you can use with AWS Organizations to manage permissions for all accounts in your organization. SCPs restrict permissions for entities in member accounts, including each AWS account root user, IAM users, and roles. For more information, see Service control policies overview. Create a permissions boundary for IAM roles that matches the SCP. A permissions boundary is an advanced feature for using a managed policy to set the maximum permissions that an identity-based policy can grant to an IAM entity. A permissions boundary allows an entity to perform only the actions that are allowed by both its identity-based policies and its permissions boundaries. For more information, see Permissions boundaries for IAM entities. Add the SCP to the root organizational unit (OU) so that it applies to all accounts in the organization. This will ensure that no IAM role can exceed the permissions defined by the SCP, regardless of how it is created or modified. Instruct the application teams to attach the permissions boundary to any IAM role they create. This will prevent them from creating IAM roles that can escalate their own privileges or access resources they are not authorized to access. This solution will meet the requirements with the least operational overhead, as it leverages AWS Organizations and IAM features to delegate and limit IAM role creation without requiring manual reviews or approvals. The other options are incorrect because they either do not allow application teams to provision their own IAM roles (A), do not limit the scope of IAM roles or prevent privilege escalation (B), or do not take advantage of managed services whenever possible? Verified References:
https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policie s_scp.html
https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_boundaries.h tml

**QUESTION 9**

A company became aware that one of its access keys was exposed on a code sharing website 11 days ago. A Security

Engineer must review all use of the exposed access keys to determine the extent of the exposure. The company enabled IAM CloudTrail m an regions when it opened the account

Which of the following will allow (he Security Engineer 10 complete the task?

A. Filter the event history on the exposed access key in the CloudTrail console Examine the data from the past 11 days.

B. Use the IAM CLI lo generate an IAM credential report Extract all the data from the past 11 days.

C. Use Amazon Athena to query the CloudTrail logs from Amazon S3 Retrieve the rows for the exposed access key tor the past 11 days.

D. Use the Access Advisor tab in the IAM console to view all of the access key activity for the past 11 days.

Correct Answer: C

Amazon Athena is a service that enables you to analyze data in Amazon S3 using standard SQL. You can use Athena to query the CloudTrail logs that are stored in S3 and filter them by the exposed access key and the date range. The other options are not effective ways to review the use of the exposed access key.

**QUESTION 10**

A security engineer needs to implement a solution to create and control the keys that a company uses for cryptographic operations. The security engineer must create symmetric keys in which the key material is generated and used within a custom key store that is backed by an AWS CloudHSM cluster.

The security engineer will use symmetric and asymmetric data key pairs for local use within applications. The security engineer also must audit the use of the keys.

How can the security engineer meet these requirements?

A. To create the keys use AWS Key Management Service (AWS KMS) and the custom key stores with the CloudHSM cluster. For auditing, use Amazon Athena

B. To create the keys use Amazon S3 and the custom key stores with the CloudHSM cluster. For auditing use AWS CloudTrail.

C. To create the keys use AWS Key Management Service (AWS KMS) and the custom key stores with the CloudHSM cluster. For auditing, use Amazon GuardDuty.

D. To create the keys use AWS Key Management Service (AWS KMS) and the custom key stores with the CloudHSM cluster. For auditing, use AWS CloudTrail.

Correct Answer: D

AWS KMS supports asymmetric KMS keys that represent a mathematically related RSA, elliptic curve (ECC), or SM2 (China Regions only) public and private key pair. These key pairs are generated in AWS KMS hardware security modules certified under the FIPS 140-2 Cryptographic Module Validation Program, except in the China (Beijing) and China (Ningxia) Regions. The private key never leaves the AWS KMS HSMs unencrypted.
https://docs.aws.amazon.com/kms/latest/developerguide/symmetric-asymmetric.html

**QUESTION 11**

A security engineer is creating an AWS Lambda function. The Lambda function needs to use a role that is named LambdaAuditRole to assume a role that is named AcmeAuditFactoryRole in a different AWS account.

When the code is processed, the following error message appears: "An error oc-curred (AccessDenied) when calling the AssumeRole operation."

Which combination of steps should the security engineer take to resolve this er-ror? (Select TWO.)

A. Ensure that LambdaAuditRole has the sts:AssumeRole permission for Ac-meAuditFactoryRole.

B. Ensure that LambdaAuditRole has the AWSLambdaBasicExecutionRole managed policy attached.

C. Ensure that the trust policy for AcmeAuditFactoryRole allows the sts:AssumeRole action from LambdaAuditRole.

D. Ensure that the trust policy for LambdaAuditRole allows the sts:AssumeRole action from the lambda.amazonaws.com service.

E. Ensure that the sts:AssumeRole API call is being issued to the us-east-I Region endpoint.

Correct Answer: AC

**QUESTION 12**

A company uses an Amazon S3 bucket to store reports. Management has mandated that all new objects stored in this bucket must be encrypted at rest using server-side encryption with a client specified AWS Key Management Service (AWS KMS) CMK owned by the same account as the S3 bucket. The AWS account number is 111122223333, and the bucket name is reportbucket. The company\\'s security specialist must write the S3 bucket policy to ensure the mandate can be implemented.

Which statement should the security specialist include in the policy?

A.
```
{
        "Effect": "Deny",
        "Principal": "*",
        "Action": "s3:PutObject",
        "Resource": "arn:aws:s3:::reportbucket/*",
        "Condition": {
            "StringEquals": {
                "s3:x-amz-server-side-encryption": "AES256"
            }
        }
    }
```
B.
```
{
        "Effect": "Deny",
        "Principal": "*",
        "Action": "s3:PutObject",
        "Resource": "arn:aws:s3:::reportbucket/*",
        "Condition": {
            "StringNotLike": {
                "s3:x-amz-server-side-encryption-aws-kms-key-id": "arn:aws:kms:
*:111122223333:key/*"
            }
        }
    }
```
C.
```
{
        "Effect": "Deny",
        "Principal": "*",
        "Action": "s3:PutObject",
        "Resource": "arn:aws:s3:::reportbucket/*",
        "Condition": {
            "StringNotLike": {
                "s3:x-amz-server-side-encryption": "aws:kms"
            }
        }
    }
```
D.
```
{
        "Effect": "Deny",
        "Principal": "*",
        "Action": "s3:PutObject",
        "Resource": "arn:aws:s3:::reportbucket/*",
        "Condition": {
            "StringNotLikeIfExists": {
                "s3:x-amz-server-side-encryption-aws-kms-key-id": "arn:aws:kms:
*:111122223333:key/*"
            }
        }
    }
```

A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: D

**QUESTION 13**

A company needs to improve its ability to identify and prevent IAM policies that grant public access or cross-account access to resources. The company has implemented AWS Organizations and has started using AWS Identity and Access Management Access Analyzer to refine overly broad access to accounts in the organization.

A security engineer must automate a response in the company\\'s organization for any newly created policies that are overly permissive. The automation must remediate external access and must notify the company\\'s security team.

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

A. Create an AWS Step Functions state machine that checks the resource type in the finding and adds an explicit Deny statement in the trust policy for the IAM role. Configure the state machine to publish a notification to an Amazon SimpleNotification Service (Amazon SNS) topic.

B. Create an AWS Batch job that forwards any resource type findings to an AWS Lambda function. Configure the Lambda function to add an explicit Deny statement in the trust policy for the IAM role. Configure the AWS Batch job to publish a notification to an Amazon Simple Notification Service (Amazon SNS) topic.

C. In Amazon EventBridge, create an event rule that matches active IAM Access Analyzer findings and invokes AWS Step Functions for resolution.

D. In Amazon CloudWatch, create a metric filter that matches active IAM Access Analyzer findings and invokes AWS Batch for resolution.

E. Create an Amazon Simple Queue Service (Amazon SQS) queue. Configure the queue to forward a notification to the security team that an external principal has been granted access to the specific IAM role and has been blocked.

F. Create an Amazon Simple Notification Service (Amazon SNS) topic for external or cross-account access notices. Subscribe the security team\\'s email addresses to the topic.

Correct Answer: ACF

To automate a response for any newly created policies that are overly permissive, the security engineer needs to use a combination of services that can monitor, analyze, remediate, and notify the security incidents. Option A is correct because creating an AWS Step Functions state machine that checks the resource type in the finding and adds an explicit Deny statement in the trust policy for the IAM role is a valid way to remediate external access. AWS Step Functions is a service that allows you to coordinate multiple AWS services into serverless workflows. You can use Step Functions to invoke AWS Lambda functions, which can modify the IAM policies programmatically. You can also use Step Functions to publish a notification to an Amazon SNS topic, which can send messages to subscribers such as email addresses. Option B is incorrect because creating an AWS Batch job that forwards any resource type findings to an AWS Lambda function is not a suitable way to automate a response. AWS Batch is a service that enables you to run batch computing workloads on AWS. Batch is designed for large-scale and long-running jobs that can benefit from parallelization and dynamic provisioning of compute resources. Batch is not intended for event-driven and real-time workflows that require immediate response. Option C is correct because creating an Amazon EventBridge event rule that matches active IAM Access Analyzer findings and invokes AWS Step Functions for resolution is a valid way to monitor and analyze the security incidents. Amazon EventBridge is a serverless event bus service that allows you to connect your applications with data from various sources. EventBridge can use rules to match events and route them to targets for processing. You can use EventBridge to invoke AWS Step Functions state machines from the IAM Access Analyzer findings. Option D is incorrect because creating an Amazon CloudWatch metric filter that matches active IAM Access Analyzer findings and invokes AWS Batch for resolution is not a suitable way to monitor and analyze the security incidents. Amazon CloudWatch is a service that provides monitoring and observability for your AWS resources and applications. CloudWatch can collect metrics, logs, and events from various sources and perform actions based on alarms or filters. However, CloudWatch cannot directly invoke AWS Batch jobs from the IAM Access Analyzer findings. You would need to use another service such as EventBridge or SNS to trigger the Batch job. Option E is incorrect because creating an Amazon SQS queue that forwards a notification to the security team that an external principal has been granted access to the specific IAM role and has been blocked is not a valid way to notify the security incidents. Amazon SQS is a fully managed message queue service that enables you to decouple and scale microservices, distributed systems, and serverless applications. SQS can deliver messages to consumers that poll the queue for

messages. However, SQS cannot directly forward a notification to the security team\\'s email addresses. You would need to use another service such as SNS or SES to send email notifications. Option F is correct because creating an Amazon SNS topic for external or cross-account access notices and subscribing the security team\\'s email addresses to the topic is a valid way to notify the security incidents. Amazon SNS is a fully managed messaging service that enables you to decouple and scale microservices, distributed systems, and serverless applications. SNS can deliver messages to a variety of endpoints, such as email, SMS, or HTTP. You can use SNS to send email notifications to the security team when a critical security finding is detected. References: AWS Step Functions AWS Batch Amazon EventBridge Amazon CloudWatch Amazon SQS Amazon SNS

**QUESTION 14**

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.)

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.

Correct Answer: BCF

**QUESTION 15**

Your development team is using access keys to develop an application that has access to S3 and DynamoDB. A new security policy has outlined that the credentials should not be older than 2 months, and should be rotated. How can you achieve this?

Please select:

A. Use the application to rotate the keys in every 2 months via the SDK

B. Use a script to query the creation date of the keys. If older than 2 months, create new access key and update all applications to use it inactivate the old key and delete it.

C. Delete the user associated with the keys after every 2 months. Then recreate the user again.

D. Delete the IAM Role associated with the keys after every 2 months. Then recreate the IAM Role again.

Correct Answer: B

One can use the CLI command list-access-keys to get the access keys. This command also returns the "CreateDate" of the keys. If the CreateDate is older than 2 months, then the keys can be deleted. The Returns list-access-keys CLI command returns information about the access key IDs associated with the specified IAM user. If there are none, the action returns an empty list Option A is incorrect because you might as use a script for such maintenance activities Option C is incorrect because you would not rotate the users themselves Option D is incorrect because you don\\'t use IAM roles for such a purpose For more information on the CLI command, please refer to the below Link: http://docs.IAM.amazon.com/cli/latest/reference/iam/list-access-keys.htmll The correct answer is: Use a script to query the creation date of the keys. If older than 2 months, create new access key and update all applications to use it inactivate the old key and delete it.