Free Questions for SOA-C03

Shared by Fowler on 16-04-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A company's security policy requires incoming SSH traffic to be restricted to a defined set of addresses. The company is using an AWS Config rule to check whether security groups allow unrestricted incoming SSH traffic.

A CloudOps engineer discovers a noncompliant resource and fixes the security group manually. The CloudOps engineer wants to automate the remediation of other noncompliant resources.

What is the MOST operationally efficient solution that meets these requirements?

Options:

A- Create a CloudWatch alarm for the AWS Config rule and invoke a Lambda function to remediate.
B- Configure an automatic remediation action on the AWS Config rule using AWS-DisableIncomingSSHOnPort22.
C- Create an EventBridge rule for AWS Config events and invoke a Lambda function.
D- Run a scheduled Lambda function to inspect and remediate security groups.

Answer:

B

Explanation:

Comprehensive Explanation (250--350 words):

AWS Config supports automatic remediation for both managed and custom rules. When a resource is found noncompliant, AWS Config can automatically invoke an AWS Systems Manager Automation document to remediate the issue. The managed automation document AWS-DisableIncomingSSHOnPort22 is specifically designed to remove unrestricted SSH access (0.0.0.0/0) from security group inbound rules.

This approach is the most operationally efficient because it requires no custom code, no event orchestration, and no ongoing maintenance. The remediation runs immediately when AWS Config detects noncompliance and ensures consistent enforcement of security policy across all applicable resources.

Options A, C, and D rely on Lambda functions and event-driven glue logic, which significantly increase operational overhead, complexity, and long-term maintenance costs. These approaches are unnecessary when AWS provides a fully managed remediation capability.

Therefore, configuring an automatic remediation action directly on the AWS Config rule is the correct and most efficient solution.

Question 2

Question Type: MultipleChoice

Application A runs on Amazon EC2 instances behind a Network Load Balancer (NLB). The EC2 instances are in an Auto Scaling group and are in the same subnet that is associated with the NLB. Other applications from an on-premises environment cannot communicate with Application A on port 8080.

To troubleshoot the issue, a CloudOps engineer analyzes the flow logs. The flow logs include the following records:

ACCEPT from 192.168.0.13:59003 172.31.16.139:8080

REJECT from 172.31.16.139:8080 192.168.0.13:59003

What is the reason for the rejected traffic?

Options:

A- The security group of the EC2 instances has no Allow rule for the traffic from the NLB.
B- The security group of the NLB has no Allow rule for the traffic from the on-premises environment.
C- The ACL of the on-premises environment does not allow traffic to the AWS environment.
D- The network ACL that is associated with the subnet does not allow outbound traffic for the ephemeral port range.

Answer:

D

Explanation:

Comprehensive and Detailed Explanation From Exact Extract of AWS CloudOps Doocuments:

VPC Flow Logs show the request arriving and being ACCEPTed on dstport 8080 and the corresponding response being REJECTed on the return path to the client's ephemeral port (59003). AWS networking guidance states that security groups are stateful (return traffic is automatically allowed) while network ACLs are stateless and require explicit inbound and

outbound rules for both directions. CloudOps operational guidance for VPC networking further notes that when you allow an inbound request (for example, TCP 8080) through a subnet's network ACL, you must also allow the outbound ephemeral port range (typically 1024--65535) for the response traffic; otherwise, the return packets are dropped and appear as REJECT in flow logs. The observed pattern---request accepted to 8080, response rejected to 59003---matches a missing outbound ephemeral-range allow on the subnet's NACL. Therefore, the cause is the subnet NACL, not security groups or on-premises ACLs. The remediation is to add an outbound ALLOW rule on the NACL for the appropriate ephemeral TCP port range back to the on-premises CIDR (and the corresponding inbound rule if asymmetric).

* AWS Certified CloudOps Engineer -- Associate (SOA-C03) Exam Guide -- Networking and Content Delivery

* Amazon VPC -- Network ACLs (stateless behavior and rule requirements)

* Amazon VPC -- Security Groups (stateful return traffic)

* VPC Flow Logs -- Record fields, ACCEPT/REJECT analysis

Question 3

Question Type: MultipleChoice

A company uses AWS Organizations to manage a set of AWS accounts. The company has set up organizational units (OUs) in the organization. An application OU supports various applications.

A CloudOps engineer must prevent users from launching Amazon EC2 instances that do not have a CostCenter-Project tag into any account in the application OU. The restriction must apply only to accounts in the application OU.

Which solution will meet these requirements?

Options:

A- Create an IAM group that has a policy that allows the ec2:RunInstances action when the CostCenter-Project tag is present. Place all IAM users who need access to the application accounts in the IAM group.
B- Create a service control policy (SCP) that denies the ec2:RunInstances action when the CostCenter-Project tag is missing. Attach the SCP to the application OU.
C- Create an IAM role that has a policy that allows the ec2:RunInstances action when the CostCenter-Project tag is present. Attach the IAM role to the IAM users that are in the application OU accounts.
D- Create a service control policy (SCP) that denies the ec2:RunInstances action when the

CostCenter-Project tag is missing. Attach the SCP to the root OU.

Answer:

B

Explanation:

AWS Organizations service control policies (SCPs) are designed to enforce permission guardrails across accounts. SCPs define the maximum available permissions for IAM principals in member accounts, regardless of the permissions granted by IAM policies. Because the requirement is to prevent EC2 instance launches without a required tag and to apply the restriction only to accounts within a specific organizational unit, SCPs are the correct control mechanism.

By creating an SCP that denies the ec2:RunInstances action when the CostCenter-Project tag is missing, the CloudOps engineer ensures that no EC2 instance can be launched without the required tag. Attaching the SCP directly to the application OU limits the scope of enforcement to only the accounts that belong to that OU, which satisfies the requirement precisely.

IAM-based solutions such as user groups or roles cannot enforce controls across multiple accounts consistently and can be bypassed by users with sufficient permissions. Attaching the SCP to the root OU would incorrectly apply the restriction to all accounts in the organization, which violates the requirement.

Therefore, attaching a tag-enforcing SCP to the application OU is the correct and least operationally complex solution.

Question 4

Question Type: MultipleChoice

An Amazon EC2 instance is running an application that uses Amazon Simple Queue Service (Amazon SQS) queues. A CloudOps engineer must ensure that the application can read, write, and delete messages from the SQS queues.

Which solution will meet these requirements in the MOST secure manner?

Options:

A- Create an IAM user with an IAM policy that allows the sqs:SendMessage permission, the sqs:ReceiveMessage permission, and the sqs:DeleteMessage permission to the appropriate queues. Embed the IAM user's credentials in the application's configuration.

B- Create an IAM user with an IAM policy that allows the sqs:SendMessage permission, the sqs:ReceiveMessage permission, and the sqs:DeleteMessage permission to the appropriate queues. Export the IAM user's access key and secret access key as environment variables on the EC2 instance.
C- Create and associate an IAM role that allows EC2 instances to call AWS services. Attach an IAM policy to the role that allows sqs:* permissions to the appropriate queues.
D- Create and associate an IAM role that allows EC2 instances to call AWS services. Attach an IAM policy to the role that allows the sqs:SendMessage permission, the sqs:ReceiveMessage permission, and the sqs:DeleteMessage permission to the appropriate queues.

Answer:

D

Explanation:

The most secure pattern is to use an IAM role for Amazon EC2 with the minimum required permissions. AWS guidance states: ''Use roles for applications that run on Amazon EC2 instances'' and ''grant least privilege by allowing only the actions required to perform a task.'' By attaching a role to the instance, short-lived credentials are automatically provided through the instance metadata service; this removes the need to create long-term access keys or embed secrets. Granting only sqs:SendMessage, sqs:ReceiveMessage, and sqs:DeleteMessage against the specific SQS queues enforces least privilege and aligns with CloudOps security controls. Options A and B rely on IAM user access keys, which contravene best practices for workloads on EC2 and increase credential-management risk. Option C uses a role but grants sqs:*, violating least-privilege principles. Therefore, Option D meets the security requirement with scoped, temporary credentials and precise permissions.

* AWS Certified CloudOps Engineer -- Associate (SOA-C03) Exam Guide -- Security & Compliance

* IAM Best Practices -- ''Use roles instead of long-term access keys,'' ''Grant least privilege''

* IAM Roles for Amazon EC2 -- Temporary credentials for applications on EC2

* Amazon SQS -- Identity and access management for Amazon SQS

Question 5

Question Type: MultipleChoice

A CloudOps engineer must manage the security of an AWS account. Recently, an IAM user's access key was mistakenly uploaded to a public code repository. The engineer must identify everything that was changed using this compromised key.

How should the CloudOps engineer meet these requirements?

Options:

A- Create an Amazon EventBridge rule to send all IAM events to an AWS Lambda function for analysis.
B- Query Amazon EC2 logs by using Amazon CloudWatch Logs Insights for all events initiated with the compromised access key within the suspected timeframe.
C- Search AWS CloudTrail event history for all events initiated with the compromised access key within the suspected timeframe.
D- Search VPC Flow Logs for all events initiated with the compromised access key within the suspected timeframe.

Answer:

C

Explanation:

According to the AWS Cloud Operations and Security documentation, AWS CloudTrail is the authoritative service for recording API activity across all AWS services within an account.

When an access key is compromised, CloudTrail logs all API requests made using that key, including details such as:

The user identity (access key ID) that made the request,

The service, operation, resource, and timestamp affected, and

The source IP address and region of the request.

By searching the CloudTrail event history for the specific access key ID, the CloudOps engineer can identify every action performed by that key during the suspected breach window.

Other options are incorrect:

EventBridge (A) is event-driven, not historical.

CloudWatch Logs (B) monitors system logs, not AWS API activity.

VPC Flow Logs (D) track network-level traffic, not API calls.

Therefore, the correct solution is Option C --- using AWS CloudTrail event history to audit and trace all actions executed via the compromised access key.

Question 6

Question Type: MultipleChoice

A company with millions of subscribers needs to automatically send notifications every Saturday. The company already uses Amazon SNS to send messages but has historically sent them manually.

Which solution will meet these requirements in the MOST operationally efficient way?

Options:

A- Launch a new Amazon EC2 instance. Configure a cron job to use the AWS SDK to send an SNS notification to subscribers every Saturday.
B- Create a rule in Amazon EventBridge that triggers every Saturday. Configure the rule to publish a notification to an SNS topic.
C- Create an SNS subscription to a message fanout that sends notifications to subscribers every Saturday.
D- Use AWS Step Functions scheduling to run a step every Saturday. Configure the step to publish a message to an SNS topic.

Answer:

B

Explanation:

Per the AWS Cloud Operations and Event Management documentation, Amazon EventBridge provides native scheduling capabilities that can trigger events at defined intervals---such as weekly, daily, or cron-based schedules.

Creating an EventBridge rule that runs every Saturday and publishes a message to an SNS topic fully automates the notification process without maintaining servers or manual jobs. This approach is serverless, highly reliable, and fully managed by AWS.

By contrast:

EC2 cron jobs (Option A) require instance management, patching, and cost overhead.

SNS subscriptions (Option C) handle message delivery, not scheduling.

Step Functions (Option D) are designed for complex workflows, not simple scheduled triggers.

Thus, Option B provides the most operationally efficient CloudOps solution by integrating EventBridge scheduled events with SNS topics for automated, recurring notifications.

Question 7

Question Type: MultipleChoice

An AWS Lambda function is intermittently failing several times a day. A CloudOps engineer must find out how often this error occurred in the last 7 days.

Which action will meet this requirement in the MOST operationally efficient manner?

Options:

A- Use Amazon Athena to query the Amazon CloudWatch logs that are associated with the Lambda function.
B- Use Amazon Athena to query the AWS CloudTrail logs that are associated with the Lambda function.
C- Use Amazon CloudWatch Logs Insights to query the associated Lambda function logs.
D- Use Amazon OpenSearch Service to stream the Amazon CloudWatch logs for the Lambda function.

Answer:

C

Explanation:

The AWS Cloud Operations and Monitoring documentation states that Amazon CloudWatch Logs Insights provides a purpose-built query engine for analyzing and visualizing log data directly within CloudWatch. For Lambda, all invocation results (including errors) are automatically logged to CloudWatch Logs.

By querying these logs with CloudWatch Logs Insights, the CloudOps engineer can efficiently count the number of ''ERROR'' or ''Exception'' occurrences over the past 7 days using simple SQL-like commands. This method is serverless, cost-efficient, and real-time.

Athena (Options A and B) would require exporting data to Amazon S3, and OpenSearch (Option D) adds unnecessary operational complexity.

Thus, Option C provides the most efficient and native AWS CloudOps approach for rapid Lambda error analysis.

To Get Premium Files for SOA-C03 Visit
https://www.p2pexams.com/products/soa-c03

For More Free Questions Visit
https://www.p2pexams.com/amazon/pdf/soa-c03