Free Questions for SCS-C02 by ebraindumps

Shared by Walter on 15-04-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

An Amazon EC2 Auto Scaling group launches Amazon Linux EC2 instances and installs the Amazon CloudWatch agent to publish logs to Amazon CloudWatch Logs. The EC2 instances launch with an IAM role that has an IAM policy attached. The policy provides access to publish custom metrics to CloudWatch. The EC2 instances run in a private subnet inside a VPC. The VPC provides ^ccess to the internet for private subnets through a NAT gateway.

A security engineer notices that no logs are being published to CloudWatch Logs for the EC2 instances that the Auto Scaling group launches. The security engineer validates that the CloudWatch Logs agent is running and is configured properly on the EC2 instances. In addition, the security engineer validates that network communications are working properly to AWS services.

What can the security engineer do to ensure that the logs are published to CloudWatch Logs?

Options:

A- Configure the IAM policy in use by the IAM role to have access to the required cloudwatch: API actions thatwill publish logs.

B- Adjust the Amazon EC2 Auto Scaling service-linked role to have permissions to write to CloudWatch Logs.

C- Configure the IAM policy in use by the IAM role to have access to the required AWS logs: API actions that willpublish logs.

D- Add an interface VPC endpoint to provide a route to CloudWatch Logs.

Answer:

C

Explanation:

Adjusting the IAM policy attached to the IAM role used by EC2 instances to include the necessary AWS Logs API actions for publishing logs to CloudWatch Logs addresses the issue. This ensures that the EC2 instances have the required permissions to interact with CloudWatch Logs, facilitating the successful publication of logs from the instances.

Question 2

Question Type: MultipleChoice

A security team is responsible for reviewing AWS API call activity in the cloud environment for security violations. These events must be recorded and retained in a centralized location for both current and future AWS regions.

What is the SIMPLEST way to meet these requirements?

Options:

A- Enable AWS Trusted Advisor security checks in the AWS Console, tsnd report all security incidents for all regions.

B- Enable AWS CloudTrail by creating individual trails for each region, and specify a single Amazon S3 bucket to receive log files for later analysis.

C- Enable AWS CloudTrail by creating a new trail and applying the trail to all regions. Specify a single Amazon S3 bucket as the storage location.

D- Enable Amazon CloudWatch logging for all AWS services across all regions, and aggregate them to a single Amazon S3 bucket for later analysis.

Answer:

C

Explanation:

Enabling AWS CloudTrail with a trail applied to all regions and specifying a single S3 bucket for storage is the simplest method to record and retain API call activity for security analysis. This configuration ensures comprehensive coverage across all current and future AWS regions, centralizing log collection and simplification of log management.

Question 3

Question Type: MultipleChoice

A company has public certificates that are managed by AWS Certificate Manager (ACM). The certificates are either imported certificates or managed certificates from ACM with mixed validation methods. A security engineer needs to design a monitoring solution to provide alerts by email when a certificate is approaching its expiration date.

What is the MOST operationally efficient way to meet this requirement?

Options:

A- Create an AWS Lambda function to list all certificates and to go through each certificate to describe the certificate by using the AWS SDK. Filter on the NotAfter attribute and send an email notification. Use an Amazon EventBridge rate expression to schedule the Lambda function to run daily.

B- Create an Amazon CloudWatch alarm Add all the certificate ARNs in the AWS/CertificateManager namespace to the DaysToExpiry metnc. Configure the alarm to publish a notification to an Amazon Simple Notification Service (Amazon SNS) topic when the value for the DaysToExpiry metric is less than or equal to 31.

C- Set up AWS Security Hub. Turn on the AWS Foundational Security Best Practices standard with integrated ACM to send findings. Configure and use a custom action by creating a rule to match the pattern from the ACM findings on the NotBefore attribute as the event source Create an Amazon Simple Notification Service (Amazon SNS) topic as the target

D- Create an Amazon EventBridge rule by using a predefined pattern for ACM Choose the metric in the ACM Certificate Approaching Expiration event as the event pattern. Create an Amazon Simple Notification Service (Amazon SNS) topic as the target

Answer:

D

Explanation:

Using Amazon EventBridge to create a rule for ACM Certificate Approaching Expiration events and configuring an SNS topic as the target provides an operationally efficient way to monitor and alert on certificate expirations. This method leverages AWS's native capabilities for event monitoring and notifications, reducing the need for custom implementations and ensuring timely alerts.

Question 4

Question Type: MultipleChoice

A company has two AWS accounts: Account A and Account B Each account has a VPC. An application that runs in the VPC in Account A needs to write to an Amazon S3 bucket in Account B. The application in Account A already has permission to write to the S3 bucket in Account B.

The application and the S3 bucket are in the same AWS Region. The company cannot send network traffic over the public internet.

Which solution will meet these requirements? b

Options:

A- In both accounts, create a transit gateway and VPC attachments in a subnet in each Availability Zone. Update the VPC route tables.

B- Deploy a software VPN appliance in Account A. Create a VPN connection between the software VPN appliance and a virtual private gateway in Account B

C- Create a VPC peering connection between the VPC in Account A and the VPC in Account B. Update the VPC route tables, network ACLs, and security groups to allow network traffic between the peered IP ranges.

D- In Account A. create a gateway VPC endpoint for Amazon S3. Update the VPC route table in Account A.

Answer:

C

Explanation:

Establishing a VPC peering connection between the VPCs in Account A and Account B and updating route tables, network ACLs, and security groups to permit the necessary traffic ensures private connectivity for the application to write to the S3 bucket without traversing the public internet. This solution is efficient and maintains network security and integrity.

Question 5

Question Type: MultipleChoice

AWS CloudTrail is being used to monitor API calls in an organization. An audit revealed that CloudTrail is failing to deliver events to Amazon S3 as expected.

What initial actions should be taken to allow delivery of CloudTrail events to S3? (Select TWO.)

Options:

A- Verify thattheS3 bucket policy allows CloudTrail to write objects.

B- Verify thatthe1AM role used by CloudTrail has access to write to Amazon CloudWatch Logs.

C- Remove any lifecycle policies on the S3 bucket that are archiving objects to S3 Glacier Flexible Retrieval.

D- Verify thattheS3 bucket defined in CloudTrail exists.

E- Verify that the log file prefix defined in CloudTrail exists in the S3 bucket.

Answer:

A, D

Explanation:

To resolve CloudTrail's failure to deliver events to S3, verifying the S3 bucket policy for CloudTrail's write permissions (A) and ensuring the existence of the specified S3 bucket (D) are critical initial steps. These actions ensure that CloudTrail has the necessary permissions and a valid destination for log file delivery, addressing common configuration issues that can interrupt event logging.

Question 6

Question Type: MultipleChoice

A company operates a web application that runs on Amazon EC2 instances. The application listens on port 80 and port 443. The company uses an Application Load Balancer (ALB) with AWS WAF to terminate SSL and to forward traffic to the application instances only on port 80.

The ALB is in public subnets that are associated with a network ACL that is named NACL1. The application instances are in dedicated private subnets that are associated with a network ACL that is named NACL2. An Amazon RDS for PostgreSQL DB instance that uses port 5432 is in a dedicated private subnet that is associated with a network ACL that is named NACL3. All the network ACLs currently allow all inbound and outbound traffic.

Which set of network ACL changes will increase the security of the application while ensuring functionality?

Options:

A- Make the following changes to NACL3:
* Add a rule that allows inbound traffic on port 5432 from NACL2.
* Add a rule that allows outbound traffic on ports 1024-65536 to NACL2.
* Remove the default rules that allow all inbound and outbound traffic.

B- Make the following changes to NACL3:
* Add a rule that allows inbound traffic on port 5432 from the CIDR blocks of the application instance subnets.
* Add a rule that allows outbound traffic on ports 1024-65536 to the application instance subnets.
* Remove the default rules that allow all inbound and outbound traffic.

C- Make the following changes to NACL2:
* Add a rule that allows outbound traffic on port 5432 to the CIDR blocks of the RDS subnets.
* Remove the default rules that allow all inbound and outbound traffic.

D- Make the following changes to NACL2:
* Add a rule that allows inbound traffic on port 5432 from the CIDR blocks of the RDS subnets.
* Add a rule that allows outbound traffic on port 5432 to the RDS subnets.

Answer:

B

Explanation:

For increased security while ensuring functionality, adjusting NACL3 to allow inbound traffic on port 5432 from the CIDR blocks of the application instance subnets, and allowing outbound traffic on ephemeral ports (1024-65536) back to those subnets creates a secure path for database access. Removing default allow-all rules enhances security by implementing the principle of least privilege, ensuring that only necessary traffic is permitted.