

Amazon-Web-Services

Exam Questions SCS-C03

AWS Certified Security - Specialty



NEW QUESTION 1

A company has a large fleet of Amazon Linux 2 Amazon EC2 instances that run an application processing sensitive data. Compliance requirements include no exposed management ports, full session logging, and authentication through AWS IAM Identity Center. DevOps engineers occasionally need access for troubleshooting.

Which solution will provide remote access while meeting these requirements?

- A. Grant access to the EC2 serial console and allow IAM role access.
- B. Enable EC2 Instance Connect and configure security groups accordingly.
- C. Assign an EC2 instance role that allows access to AWS Systems Manager
- D. Create an IAM policy that grants access to Systems Manager Session Manager and assign it to an IAM Identity Center role.
- E. Use Systems Manager Automation to temporarily open remote access ports.

Answer: C

NEW QUESTION 2

A company has a web application that reads from and writes to an Amazon S3 bucket. The company needs to use AWS credentials to authenticate all S3 API calls to the S3 bucket. Which solution will provide the application with AWS credentials to make S3 API calls?

- A. Integrate with Cognito identity pools and use GetId to obtain AWS credentials.
- B. Integrate with Cognito identity pools and use AssumeRoleWithWebIdentity to obtain AWS credentials.
- C. Integrate with Cognito user pools and use the ID token to obtain AWS credentials.
- D. Integrate with Cognito user pools and use the access token to obtain AWS credentials.

Answer: B

NEW QUESTION 3

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
- D. Associate the key pair with the EC2 instance.
- E. Create a VPC interface endpoint for Systems Manager in the VPC where the EC2 instance is located.
- F. Attach a security group to the VPC interface endpoint
- G. Allow inbound traffic on port 443 to the VPC's CIDR range.
- H. Create a VPC interface endpoint for the EC2 instance in the VPC where the EC2 instance is located.

Answer: ADE

NEW QUESTION 4

A security engineer wants to forward custom application-security logs from an Amazon EC2 instance to Amazon CloudWatch. The security engineer installs the CloudWatch agent on the EC2 instance and adds the path of the logs to the CloudWatch configuration file.

However, CloudWatch does not receive the logs. The security engineer verifies that the awslogs service is running on the EC2 instance.

What should the security engineer do next to resolve the issue?

- A. Add AWS CloudTrail to the trust policy of the EC2 instance
- B. Send the custom logs to CloudTrail instead of CloudWatch.
- C. Add Amazon S3 to the trust policy of the EC2 instance
- D. Configure the application to write the custom logs to an S3 bucket that CloudWatch can use to ingest the logs.
- E. Add Amazon Inspector to the trust policy of the EC2 instance
- F. Use Amazon Inspector instead of the CloudWatch agent to collect the custom logs.
- G. Attach the CloudWatchAgentServerPolicy AWS managed policy to the EC2 instance role.

Answer: D

NEW QUESTION 5

A company needs to identify the root cause of security findings and investigate IAM roles involved in those findings. The company has enabled VPC Flow Logs, Amazon GuardDuty, and AWS CloudTrail.

Which solution will meet these requirements?

- A. Use Amazon Detective to investigate IAM roles and visualize findings.
- B. Use Amazon Inspector and CloudWatch dashboards.
- C. Export GuardDuty findings to S3 and analyze with Athena.
- D. Use Security Hub custom actions to investigate IAM roles.

Answer: A

NEW QUESTION 6

A company has decided to move its fleet of Linux-based web server instances to an Amazon EC2 Auto Scaling group. Currently, the instances are static and are launched manually. When an administrator needs to view log files, the administrator uses SSH to establish a connection to the instances and retrieves the logs manually.

The company often needs to query the logs to produce results about application sessions and user issues. The company does not want its new automatically

scaling architecture to result in the loss of any log files when instances are scaled in.

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

- A. Configure a cron job on the instances to forward the log files to Amazon S3 periodically.
- B. Configure AWS Glue and Amazon Athena to query the log files.
- C. Configure the Amazon CloudWatch agent on the instances to forward the logs to Amazon CloudWatch Logs.
- D. Configure Amazon CloudWatch Logs Insights to query the log files.
- E. Configure the instances to write the logs to an Amazon Elastic File System (Amazon EFS) volume.

Answer: CD

NEW QUESTION 7

A company wants to establish separate AWS Key Management Service (AWS KMS) keys to use for different AWS services. The company's security engineer created a key policy to allow the infrastructure deployment team to create encrypted Amazon Elastic Block Store (Amazon EBS) volumes by assuming the InfrastructureDeployment IAM role. The security engineer recently discovered that IAM roles other than the InfrastructureDeployment role used this key for other services.

Which change to the policy should the security engineer make to resolve these issues?

- A. In the statement block that contains the Sid "Allow use of the key", under the "Condition" block, change StringEquals to StringLike.
- B. In the policy document, remove the statement block that contains the Sid "Enable IAM User Permissions". Add key management policies to the KMS policy.
- C. In the statement block that contains the Sid "Allow use of the key", under the "Condition" block, change the kms:ViaService value to ec2.us-east-1.amazonaws.com.
- D. In the policy document, add a new statement block that grants the kms:Disable* permission to the security engineer's IAM role.

Answer: C

NEW QUESTION 8

A company runs an application on an Amazon EC2 instance. The application generates invoices and stores them in an Amazon S3 bucket. The instance profile that is attached to the instance has appropriate access to the S3 bucket. The company needs to share each invoice with multiple clients that do not have AWS credentials. Each client must be able to download only the client's own invoices. Clients must download their invoices within 1 hour of invoice creation. Clients must use only temporary credentials to access the company's AWS resources.

Which additional step will meet these requirements?

- A. Update the S3 bucket policy to ensure that clients that use pre-signed URLs have the S3:Get* permission and the S3:List* permission to access S3 objects in the bucket.
- B. Add a StringEquals condition to the IAM role policy for the EC2 instance profile.
- C. Configure the policy condition to restrict access based on the s3:ResourceTag/ClientId tag of each invoice.
- D. Tag each generated invoice with the ID of its corresponding client.
- E. Update the script to use AWS Security Token Service (AWS STS) to obtain new credentials each time the script runs by assuming a new role that has S3:GetObject permission.
- F. Use the credentials to generate the pre-signed URLs.
- G. Generate an access key and a secret key for an IAM user that has S3:GetObject permissions on the S3 bucket.
- H. Embed the keys into the script.
- I. Use the keys to generate the pre-signed URLs.

Answer: B

NEW QUESTION 9

A company experienced a security incident caused by a vulnerable container image that was pushed from an external CI/CD pipeline into Amazon ECR.

Which solution will prevent vulnerable images from being pushed?

- A. Enable ECR enhanced scanning with Lambda blocking.
- B. Use Amazon Inspector with EventBridge and Lambda.
- C. Integrate Amazon Inspector into the CI/CD pipeline using SBOM generation and fail the pipeline on critical findings.
- D. Enable basic continuous ECR scanning.

Answer: C

NEW QUESTION 10

A company has a VPC that has no internet access and has the private DNS hostnames option enabled. An Amazon Aurora database is running inside the VPC. A security engineer wants to use AWS Secrets Manager to automatically rotate the credentials for the Aurora database. The security engineer configures the Secrets Manager default AWS Lambda rotation function to run inside the same VPC that the Aurora database uses. However, the security engineer determines that the password cannot be rotated properly because the Lambda function cannot communicate with the Secrets Manager endpoint.

What is the MOST secure way that the security engineer can give the Lambda function the ability to communicate with the Secrets Manager endpoint?

- A. Add a NAT gateway to the VPC to allow access to the Secrets Manager endpoint.
- B. Add a gateway VPC endpoint to the VPC to allow access to the Secrets Manager endpoint.
- C. Add an interface VPC endpoint to the VPC to allow access to the Secrets Manager endpoint.
- D. Add an internet gateway for the VPC to allow access to the Secrets Manager endpoint.

Answer: C

NEW QUESTION 10

A company is running its application on AWS. The company has a multi-environment setup, and each environment is isolated in a separate AWS account. The company has an organization in AWS Organizations to manage the accounts. There is a single dedicated security account for the organization. The company must create an inventory of all sensitive data that is stored in Amazon S3 buckets across the organization's accounts. The findings must be visible from a single location. Which solution will meet these requirements?

- A. Set the security account as the delegated administrator for Amazon Macie and AWS Security Hub
- B. Enable and configure Macie to publish sensitive data findings to Security Hub.
- C. Set the security account as the delegated administrator for AWS Security Hub
- D. In each account, configure Amazon Inspector to scan the S3 buckets for sensitive data
- E. Publish sensitive data findings to Security Hub.
- F. In each account, configure Amazon Inspector to scan the S3 buckets for sensitive data
- G. Enable Amazon Inspector integration with AWS Trusted Advisor
- H. Publish sensitive data findings to Trusted Advisor.
- I. In each account, enable and configure Amazon Macie to detect sensitive data
- J. Enable Macie integration with AWS Trusted Advisor
- K. Publish sensitive data findings to Trusted Advisor.

Answer: A

NEW QUESTION 12

A company is building a secure solution that relies on an AWS Key Management Service (AWS KMS) customer managed key. The company wants to allow AWS Lambda to use the KMS key. However, the company wants to prevent Amazon EC2 from using the key. Which solution will meet these requirements?

- A. Use IAM explicit deny for EC2 instance profiles and allow for Lambda roles.
- B. Use a KMS key policy with kms:ViaService conditions to allow Lambda usage and deny EC2 usage.
- C. Use aws:SourceIp and aws:AuthorizedService condition keys in the KMS key policy.
- D. Use an SCP to deny EC2 and allow Lambda.

Answer: B

NEW QUESTION 17

A company has an encrypted Amazon Aurora DB cluster in the us-east-1 Region that uses an AWS KMS customer managed key. The company must copy a DB snapshot to the us-west-1 Region but cannot access the encryption key across Regions. What should the company do to properly encrypt the snapshot in us-west-1?

- A. Store the customer managed key in AWS Secrets Manager in us-west-1.
- B. Create a new customer managed key in us-west-1 and use it to encrypt the snapshot.
- C. Create an IAM policy to allow access to the key in us-east-1 from us-west-1.
- D. Create an IAM policy that allows RDS in us-west-1 to access the key in us-east-1.

Answer: B

NEW QUESTION 22

A company's data scientists use Amazon SageMaker with datasets stored in Amazon S3. Data older than 45 days must be removed according to policy. Which action should enforce this policy?

- A. Configure an S3 Lifecycle rule to delete objects after 45 days.
- B. Create a Lambda function triggered on object upload to delete old data.
- C. Create a scheduled Lambda function to delete old objects monthly.
- D. Configure S3 Intelligent-Tiering.

Answer: A

NEW QUESTION 26

A security engineer configured VPC Flow Logs to publish to Amazon CloudWatch Logs. After 10 minutes, no logs appear. The issue is isolated to the IAM role associated with VPC Flow Logs. What could be the reason?

- A. logs:GetLogEvents is missing.
- B. The engineer cannot assume the role.
- C. The vpc-flow-logs.amazonaws.com principal cannot assume the role.
- D. The role cannot tag the log stream.

Answer: C

NEW QUESTION 30

A company creates AWS Lambda functions from container images that are stored in Amazon Elastic Container Registry (Amazon ECR). The company needs to identify any software vulnerabilities in the container images and any code vulnerabilities in the Lambda functions. Which solution will meet these requirements?

- A. Enable Amazon GuardDuty
- B. Configure Amazon ECR scanning and Lambda code scanning in GuardDuty.
- C. Enable Amazon GuardDuty
- D. Configure Runtime Monitoring and Lambda Protection in GuardDuty.
- E. Enable Amazon Inspector
- F. Configure Amazon ECR enhanced scanning and Lambda code scanning in Amazon Inspector.
- G. Enable AWS Security Hub
- H. Configure Runtime Monitoring and Lambda Protection in Security Hub.

Answer: C

NEW QUESTION 32

A security engineer needs to prepare Amazon EC2 instances for quarantine during a security incident. AWS Systems Manager Agent (SSM Agent) is installed, and a script exists to install and update forensic tools.

Which solution will quarantine EC2 instances during a security incident?

- A. Track SSM Agent versions with AWS Config.
- B. Configure Session Manager to deny external connections.
- C. Store the script in Amazon S3 and grant read access.
- D. Configure IAM permissions for the SSM Agent to run the script as a Systems Manager Run Command document.

Answer: D

NEW QUESTION 37

A company has several Amazon S3 buckets that do not enforce encryption in transit. A security engineer must implement a solution that enforces encryption in transit for all the company's existing and future S3 buckets.

Which solution will meet these requirements?

- A. Enable AWS Confi
- B. Create a proactive AWS Config Custom Policy rul
- C. Create aGuard clause to evaluate the S3 bucket policies to check for a value of True for the aws:SecureTransport condition ke
- D. If the AWS Config rule evaluates to NON_COMPLIANT, block resource creation.
- E. Enable AWS Confi
- F. Configure the s3-bucket-ssl-requests-only AWS Config managed rule and set the rule trigger type to Hybri
- G. Create an AWS Systems Manager Automation runbook that applies a bucket policy to deny requests when the value of the aws:SecureTransport condition key is Fals
- H. Configure automatic remediatio
- I. Set the runbook as the target of the rule.
- J. Enable Amazon Inspecto
- K. Create a custom AWS Lambda rul
- L. Create a Lambda function that applies a bucket policy to deny requests when the value of the aws:SecureTransport condition key is Fals
- M. Set the Lambda function as the target of the rule.
- N. Create an AWS CloudTrail trai
- O. Enable S3 data events on the trai
- P. Create an AWS Lambda function that applies a bucket policy to deny requests when the value of the aws:SecureTransport condition key is Fals
- Q. Configure the CloudTrail trail to invoke the Lambda function.

Answer: B

NEW QUESTION 39

A consultant agency needs to perform a security audit for a company's production AWS account. Several consultants need access to the account. The consultant agency already has its own AWS account. The company requires multi-factor authentication (MFA) for all access to its production account. The company also forbids the use of long-term credentials.

Which solution will provide the consultant agency with access that meets these requirements?

- A. Create an IAM grou
- B. Create an IAM user for each consultan
- C. Add each user to the grou
- D. Turn on MFA for each consultant.
- E. Configure Amazon Cognito on the company's production account to authenticate against the consultant agency's identity provider (IdP). Add MFA to a Cognito user pool.
- F. Create an IAM role in the consultant agency's AWS accoun
- G. Define a trust policy that requires MF
- H. In the trust policy, specify the company's production account as the principa
- I. Attach the trust policy to the role.
- J. Create an IAM role in the company's production accoun
- K. Define a trust policy that requires MF
- L. In the trust policy, specify the consultant agency's AWS account as the principa
- M. Attach the trust policy to the role.

Answer: D

NEW QUESTION 42

A company uses AWS to run a web application that manages ticket sales in several countries. The company recently migrated the application to an architecture that includes Amazon API Gateway, AWS Lambda, and Amazon Aurora Serverless. The company needs the application to comply with Payment Card Industry Data Security Standard (PCI DSS) v4.0. A security engineer must generate a report that shows the effectiveness of the PCI DSS v4.0 controls that apply to the application. The company's compliance team must be able to add manual evidence to the report.

Which solution will meet these requirements?

- A. Enable AWS Trusted Adviso
- B. Configure all the Trusted Advisor check
- C. Manually map the checks against the PCI DSS v4.0 standard to generate the report.
- D. Enable and configure AWS Confi
- E. Deploy the Operational Best Practices for PCI DSS conformance pack in AWS Confi
- F. Use AWS Config to generate the report.
- G. Enable AWS Security Hu
- H. Enable the Security Hub PCI DSS security standar
- I. Use the AWS Management Console to download the report from the security standard.
- J. Create an AWS Audit Manager assessment that uses the AWS managed PCI DSS v4.0 standard framewor
- K. Add all evidence to the assessmen
- L. Generate the report in Audit Manager for download.

Answer: D

NEW QUESTION 46

A company runs a web application on a fleet of Amazon EC2 instances in an Auto Scaling group. Amazon GuardDuty and AWS Security Hub are enabled. The security engineer needs an automated response to anomalous traffic that follows AWS best practices and minimizes application disruption. Which solution will meet these requirements?

- A. Use EventBridge to disable the instance profile access keys.
- B. Use EventBridge to invoke a Lambda function that removes the affected instance from the Auto Scaling group and isolates it with a restricted security group.
- C. Use Security Hub to update the subnet network ACL to block traffic.
- D. Send GuardDuty findings to Amazon SNS for email notification.

Answer: B

NEW QUESTION 47

A company is running an application in the eu-west-1 Region. The application uses an AWS Key Management Service (AWS KMS) customer managed key to encrypt sensitive data. The company plans to deploy the application in the eu-north-1 Region. A security engineer needs to implement a key management solution for the application deployment in the new Region. The security engineer must minimize changes to the application code. Which change should the security engineer make to the AWS KMS configuration to meet these requirements?

- A. Update the key policies in eu-west-1. Point the application in eu-north-1 to use the same customer managed key as the application in eu-west-1.
- B. Allocate a new customer managed key to eu-north-1 to be used by the application that is deployed in that Region.
- C. Allocate a new customer managed key to eu-north-1. Create the same alias name for both key
- D. Configure the application deployment to use the key alias.
- E. Allocate a new customer managed key to eu-north-1. Create an alias for eu--1. Change the application code to point to the alias for eu--1.

Answer: C

NEW QUESTION 48

A company's security engineer receives an alert that indicates that an unexpected principal is accessing a company-owned Amazon Simple Queue Service (Amazon SQS) queue. All the company's accounts are within an organization in AWS Organizations. The security engineer must implement a mitigation solution that minimizes compliance violations and investment in tools outside of AWS. What should the security engineer do to meet these requirements?

- A. Create security groups and attach them to all SQS queues.
- B. Modify network ACLs in all VPCs to restrict inbound traffic.
- C. Create interface VPC endpoints for Amazon SQ
- D. Restrict access using aws:SourceVpce and aws:PrincipalOrgId conditions.
- E. Use a third-party cloud access security broker (CASB).

Answer: C

NEW QUESTION 49

A company requires a specific software application to be installed on all new and existing Amazon EC2 instances across an AWS Organization. SSM Agent is installed and active. How can the company continuously monitor deployment status of the software application?

- A. Use AWS Config organization-wide with the ec2-managedinstance-applications-required managed rule and specify the application name.
- B. Use approved AMIs rule organization-wide.
- C. Use Distributor package and review output.
- D. Use Systems Manager Application Manager inventory filtering.

Answer: A

NEW QUESTION 51

A company detects bot activity targeting Amazon Cognito user pool endpoints. The solution must block malicious requests while maintaining access for legitimate users. Which solution meets these requirements?

- A. Enable Amazon Cognito threat protection.
- B. Restrict access to authenticated users only.
- C. Associate AWS WAF with the Cognito user pool.
- D. Monitor requests with CloudWatch.

Answer: A

NEW QUESTION 53

A company has AWS accounts in an organization in AWS Organizations. An Amazon S3 bucket in one account is publicly accessible. A security engineer must remove public access and ensure the bucket cannot be made public again. Which solution will meet these requirements?

- A. Enforce KMS encryption and deny s3:GetObject by SCP.
- B. Enable PublicAccessBlock and deny s3:GetObject by SCP.
- C. Enable PublicAccessBlock and deny s3:PutPublicAccessBlock by SCP.
- D. Enable Object Lock governance and deny s3:PutPublicAccessBlock by SCP.

Answer: C

NEW QUESTION 54

A company runs a global ecommerce website using Amazon CloudFront. The company must block traffic from specific countries to comply with data regulations. Which solution will meet these requirements MOST cost-effectively?

- A. Use AWS WAF IP match rules.
- B. Use AWS WAF geo match rules.
- C. Use CloudFront geo restriction to deny the countries.
- D. Use geolocation headers in CloudFront.

Answer: C

NEW QUESTION 58

A company must immediately disable compromised IAM users across all AWS accounts and collect all actions performed by the user in the last 7 days. Which solution will meet these requirements?

- A. Disable the IAM user and query CloudTrail logs in Amazon S3 using Athena.
- B. Remove IAM policies and query logs in Security Hub.
- C. Remove permission sets and query logs using CloudWatch Logs Insights.
- D. Disable the user in IAM Identity Center and query the organizational event data store.

Answer: D

NEW QUESTION 59

A company is running a new workload across accounts in an organization in AWS Organizations. All running resources must have a tag of CostCenter, and the tag must have one of three approved values. The company must enforce this policy and must prevent any changes of the CostCenter tag to a non-approved value. Which solution will meet these requirements?

- A. Use AWS Config custom policy rule and an SCP to deny non-approved aws:RequestTag/CostCenter values.
- B. Use CloudTrail + EventBridge + Lambda to block creation.
- C. Enable tag policies, define allowed values, enforce noncompliant operations, and use an SCP to deny creation when aws:RequestTag/CostCenter is null.
- D. Enable tag policies and use EventBridge + Lambda to block changes.

Answer: C

NEW QUESTION 61

A company must capture AWS CloudTrail data events and must retain the logs for 7 years. The logs must be immutable and must be available to be searched by complex queries. The company also needs to visualize the data from the logs. Which solution will meet these requirements MOST cost-effectively?

- A. Create a CloudTrail Lake data store
- B. Implement CloudTrail Lake dashboards to visualize and query the results.
- C. Use the CloudTrail Event History feature in the AWS Management Console
- D. Visualize and query the results in the console.
- E. Send the CloudTrail logs to an Amazon S3 bucket
- F. Provision a persistent Amazon EMR cluster that has access to the S3 bucket
- G. Enable S3 Object Lock on the S3 bucket
- H. Use Apache Spark to perform queries
- I. Use Amazon QuickSight for visualizations.
- J. Send the CloudTrail logs to a log group in Amazon CloudWatch Logs
- K. Set the CloudWatch Logs stream to send the data to an Amazon OpenSearch Service domain
- L. Enable cold storage for the OpenSearch Service domain
- M. Use OpenSearch Dashboards for visualizations and queries.

Answer: A

NEW QUESTION 65

A company runs ECS services behind an internet-facing ALB that is the origin for CloudFront. An AWS WAF web ACL is associated with CloudFront, but clients can bypass it by accessing the ALB directly. Which solution will prevent direct access to the ALB?

- A. Use AWS PrivateLink with the ALB.
- B. Replace the ALB with an internal ALB.
- C. Restrict ALB listener rules to CloudFront IP ranges.
- D. Require a custom header from CloudFront and validate it at the ALB.

Answer: D

NEW QUESTION 68

A company recently experienced a malicious attack on its cloud-based environment. The company successfully contained and eradicated the attack. A security engineer is performing incident response work. The security engineer needs to recover an Amazon RDS database cluster to the last known good version. The database cluster is configured to generate automated backups with a retention period of 14 days. The initial attack occurred 5 days ago at exactly 3:15 PM. Which solution will meet this requirement?

- A. Identify the Regional cluster ARN for the database
- B. Use the ARN to restore the Regional cluster by using the restore to point in time feature
- C. Set a target time 5 days ago at 3:14 PM.
- D. Identify the Regional cluster ARN for the database

- E. List snapshots that have been taken of the cluster
- F. Restore the database by using the snapshot that has a creation time that is closest to 5 days ago at 3:14 PM.
- G. List all snapshots that have been taken of all the company's RDS database
- H. Identify the snapshot that was taken closest to 5 days ago at 3:14 PM and restore it.
- I. Identify the Regional cluster ARN for the database
- J. Use the ARN to restore the Regional cluster by using the restore to point in time feature
- K. Set a target time 14 days ago.

Answer: A

NEW QUESTION 70

A security engineer needs to control access to data that is encrypted with an AWS Key Management Service (AWS KMS) customer managed key. The security engineer also needs to use additional authenticated data (AAD) to prevent tampering with ciphertext. Which solution will meet these requirements?

- A. Pass the key alias to AWS KMS when calling the Encrypt and Decrypt API actions.
- B. Use IAM policies to restrict access to the Encrypt and Decrypt API actions.
- C. Use the kms:EncryptionContext condition key when defining IAM policies for the customer managed key.
- D. Use key policies to restrict access to the appropriate IAM groups.

Answer: C

NEW QUESTION 73

A security engineer receives a notice about suspicious activity from a Linux-based Amazon EC2 instance that uses Amazon Elastic Block Store (Amazon EBS)-based storage. The instance is making connections to known malicious addresses. The instance is in a development account within a VPC that is in the us-east-1 Region. The VPC contains an internet gateway and has a subnet in us-east-1a and us-east-1b. Each subnet is associated with a route table that uses the internet gateway as a default route. Each subnet also uses the default network ACL. The suspicious EC2 instance runs within the us-east-1b subnet. During an initial investigation, a security engineer discovers that the suspicious instance is the only instance that runs in the subnet. Which response will immediately mitigate the attack and help investigate the root cause?

- A. Log in to the suspicious instance and use the netstat command to identify remote connections
- B. Use the IP addresses from these remote connections to create deny rules in the security group of the instance
- C. Install diagnostic tools on the instance for investigation
- D. Update the outbound network ACL for the subnet in us-east-1b to explicitly deny all connections as the first rule during the investigation of the instance.
- E. Update the outbound network ACL for the subnet in us-east-1b to explicitly deny all connections as the first rule
- F. Replace the security group with a new security group that allows connections only from a diagnostics security group
- G. Update the outbound network ACL for the us-east-1b subnet to remove the deny all rule
- H. Launch a new EC2 instance that has diagnostic tools
- I. Assign the new security group to the new EC2 instance
- J. Use the new EC2 instance to investigate the suspicious instance.
- K. Ensure that the Amazon Elastic Block Store (Amazon EBS) volumes that are attached to the suspicious EC2 instance will not delete upon termination
- L. Terminate the instance
- M. Launch a new EC2 instance in us-east-1a that has diagnostic tools
- N. Mount the EBS volumes from the terminated instance for investigation.
- O. Create an AWS WAF web ACL that denies traffic to and from the suspicious instance
- P. Attach the AWS WAF web ACL to the instance to mitigate the attack
- Q. Log in to the instance and install diagnostic tools to investigate the instance.

Answer: C

NEW QUESTION 76

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

SCS-C03 Practice Exam Features:

- * SCS-C03 Questions and Answers Updated Frequently
- * SCS-C03 Practice Questions Verified by Expert Senior Certified Staff
- * SCS-C03 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * SCS-C03 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The SCS-C03 Practice Test Here](#)