Amazon-Web-Services

Exam Questions SCS-C03

AWS Certified Security - Specialty

NEW QUESTION 1
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 2
A company stores sensitive data in an Amazon S3 bucket. The company encrypts the data at rest by using server-side encryption with Amazon S3 managed keys (SSE-S3). A security engineer must prevent any modifications to the data in the S3 bucket.
Which solution will meet this requirement?

A. Configure S3 bucket policies to deny DELETE and PUT object permissions.
B. Configure S3 Object Lock in compliance mode with S3 bucket versioning enabled.
C. Change the encryption on the S3 bucket to use AWS Key Management Service (AWS KMS) customer managed keys.
D. Configure the S3 bucket with multi-factor authentication (MFA) delete protection.

Answer: B

NEW QUESTION 3
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 4
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 5
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 6
A company needs to deploy AWS CloudFormation templates that configure sensitive database credentials. The company already uses AWS Key Management Service (AWS KMS) and AWS Secrets Manager.
Which solution will meet the requirements?

A. Use a dynamic reference in the CloudFormation template to reference the database credentials in Secrets Manager.
B. Use encrypted parameters in the CloudFormation template.
C. Use SecureString parameters to reference Secrets Manager.
D. Use SecureString parameters encrypted by AWS KMS.

Answer: A

NEW QUESTION 7
A security engineer has designed a VPC to segment private traffic from public traffic. The VPC includes two Availability Zones. Each Availability Zone contains one public subnet and one private subnet. Three route tables exist: one for the public subnets and one for each private subnet.
The security engineer discovers that all four subnets are routing traffic through the internet gateway that is attached to the VPC.
Which combination of steps should the security engineer take to remediate this scenario? (Select TWO.)

A. Verify that a NAT gateway has been provisioned in the public subnet in each Availability Zone.
B. Verify that a NAT gateway has been provisioned in the private subnet in each Availability Zone.
C. Modify the route tables for the public subnets to add a local route to the VPC CIDR range.
D. Modify the route tables for the private subnets to route 0.0.0.0/0 to the NAT gateway in the public subnet of the same Availability Zone.
E. Modify the route tables for the private subnets to route 0.0.0.0/0 to the internet gateway.

Answer: AD

NEW QUESTION 8
A company needs to build a code-signing solution using an AWS KMS asymmetric key and must store immutable evidence of key creation and usage for compliance and audit purposes.
Which solution meets these requirements?

A. Create an Amazon S3 bucket with S3 Object Lock enable
B. Create an AWS CloudTrail trail with log file validation enabled for KMS event
C. Store logs in the bucket and grant auditors access.
D. Log application events to Amazon CloudWatch Logs and export them.
E. Capture KMS API calls using EventBridge and store them in DynamoDB.
F. Track KMS usage with CloudWatch metrics and dashboards.

Answer: A

NEW QUESTION 9
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 10
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 GuardDut
B. Configure Amazon ECR scanning and Lambda code scanning in GuardDuty.
C. Enable Amazon GuardDut
D. Configure Runtime Monitoring and Lambda Protection in GuardDuty.
E. Enable Amazon Inspecto
F. Configure Amazon ECR enhanced scanning and Lambda code scanning in Amazon Inspector.
G. Enable AWS Security Hu
H. Configure Runtime Monitoring and Lambda Protection in Security Hub.

Answer: C

NEW QUESTION 10
A security engineer discovers that a company's user passwords have no required minimum length. The company uses the following identity providers (IdPs):
• AWS Identity and Access Management (IAM) federated with on-premises Active Directory
• Amazon Cognito user pools that contain the user database for an AWS Cloud application Which combination of actions should the security engineer take to implement a required minimum password length? (Select TWO.)

A. Update the password length policy in the IAM configuration.
B. Update the password length policy in the Amazon Cognito configuration.
C. Update the password length policy in the on-premises Active Directory configuration.
D. Create an SCP in AWS Organizations to enforce minimum password length.
E. Create an IAM policy with a minimum password length condition.

Answer: BC

NEW QUESTION 13
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 15
A company??s web application runs on Amazon EC2 instances behind an Application Load Balancer (ALB) in an Auto Scaling group. An AWS WAF web ACL is associated with the ALB. Instance logs are lost after reboots. The operations team suspects malicious activity targeting a specific PHP file.
Which set of actions will identify the suspect attacker??s IP address for future occurrences?

A. Configure VPC Flow Logs and search for PHP file activity.
B. Install the CloudWatch agent on the ALB and export application logs.
C. Export ALB access logs to Amazon OpenSearch Service and search them.
D. Configure the web ACL to send logs to Amazon Kinesis Data Firehos
E. Deliver logs to Amazon S3 and query them with Amazon Athena.

Answer: D

NEW QUESTION 19
A company needs to scan all AWS Lambda functions for code vulnerabilities.

A. Use Amazon Macie.
B. Enable Amazon Inspector Lambda scanning.
C. Use GuardDuty and Security Hub.
D. Use GuardDuty Lambda Protection.

Answer: B

NEW QUESTION 21
A company is using AWS CloudTrail and Amazon CloudWatch to monitor resources in an AWS account. The company??s developers have been using an IAM role in the account for the last 3 months.
A security engineer needs to refine the customer managed IAM policy attached to the role to ensure that the role provides least privilege access.
Which solution will meet this requirement with the LEAST effort?

A. Implement AWS IAM Access Analyzer policy generation on the role.
B. Implement AWS IAM Access Analyzer policy validation on the role.
C. Search CloudWatch logs to determine the actions the role invoked and to evaluate the permissions.
D. Use AWS Trusted Advisor to compare the policies assigned to the role against AWS best practices.

Answer: A

NEW QUESTION 24
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 28
A company needs centralized log monitoring with automatic detection across hundreds of AWS accounts.
Which solution meets these requirements with the LEAST operational effort?

A. Designate a GuardDuty administrator account and enable protections.
B. Centralize CloudWatch logs and use Inspector.
C. Centralize CloudTrail logs and query with Athena.
D. Stream logs to Kinesis and process with Lambda.

Answer: A

NEW QUESTION 30

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 34
Notify when IAM roles are modified.

A. Use Amazon Detective.
B. Use EventBridge with CloudTrail events.
C. Use CloudWatch metric filters.
D. Use CloudWatch subscription filters.

Answer: B

NEW QUESTION 37
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 stor
B. Implement CloudTrail Lake dashboards to visualize and query the results.
C. Use the CloudTrail Event History feature in the AWS Management Consol
D. Visualize and query the results in the console.
E. Send the CloudTrail logs to an Amazon S3 bucke
F. Provision a persistent Amazon EMR cluster that has access to the S3 bucke
G. Enable S3 Object Lock on the S3 bucke
H. Use Apache Spark to perform querie
I. Use Amazon QuickSight for visualizations.
J. Send the CloudTrail logs to a log group in Amazon CloudWatch Log
K. Set the CloudWatch Logs stream to send the data to an Amazon OpenSearch Service domai
L. Enable cold storage for the OpenSearch Service domai
M. Use OpenSearch Dashboards for visualizations and queries.

Answer: A

NEW QUESTION 39
A company sends Apache logs from EC2 Auto Scaling instances to a CloudWatch Logs log group with 1-year retention. A suspicious IP address appears in logs. A security engineer needs to analyze the past week of logs to count requests from that IP and list requested URLs.
What should the engineer do with the LEAST effort?

A. Export to S3 and use Macie.
B. Stream to OpenSearch and analyze.
C. Use CloudWatch Logs Insights with queries.
D. Export to S3 and use AWS Glue.

Answer: C

NEW QUESTION 41
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 45
A company uploads data files as objects into an Amazon S3 bucket. A vendor downloads the objects to perform data processing.
A security engineer must implement a solution that prevents objects from residing in the S3 bucket for longer than 72 hours.

A. Configure S3 Versioning to expire object versions that have been in the bucket for 72 hours.
B. Configure an S3 Lifecycle configuration rule on the bucket to expire objects after 72 hours.
C. Use the S3 Intelligent-Tiering storage class and configure expiration after 72 hours.
D. Generate presigned URLs that expire after 72 hours.

Answer: B

NEW QUESTION 50

A company that uses AWS Organizations is using AWS IAM Identity Center to administer access to AWS accounts. A security engineer is creating a custom permission set in IAM Identity Center. The company will use the permission set across multiple accounts. An AWS managed policy and a customer managed policy are attached to the permission set. The security engineer has full administrative permissions and is operating in the management account.
When the security engineer attempts to assign the permission set to an IAM Identity Center user who has access to multiple accounts, the assignment fails.
What should the security engineer do to resolve this failure?

A. Create the customer managed policy in every account where the permission set is assigne
B. Give the customer managed policy the same name and same permissions in each account.
C. Remove either the AWS managed policy or the customer managed policy from the permission se
D. Create a second permission set that includes the removed polic
E. Apply the permission sets separately to the user.
F. Evaluate the logic of the AWS managed policy and the customer managed polic
G. Resolve any policy conflicts in the permission set before deployment.
H. Do not add the new permission set to the use
I. Instead, edit the user's existing permission set to include the AWS managed policy and the customer managed policy.

Answer: A

NEW QUESTION 53
A security engineer is designing a solution that will provide end-to-end encryption between clients and Docker containers running in Amazon Elastic Container Service (Amazon ECS). This solution must also handle volatile traffic patterns.
Which solution would have the MOST scalability and LOWEST latency?

A. Configure a Network Load Balancer to terminate the TLS traffic and then re-encrypt the traffic to the containers.
B. Configure an Application Load Balancer to terminate the TLS traffic and then re-encrypt the traffic to the containers.
C. Configure a Network Load Balancer with a TCP listener to pass through TLS traffic to the containers.
D. Configure Amazon Route 53 to use multivalue answer routing to send traffic to the containers.

Answer: C

NEW QUESTION 58
A company uses AWS Organizations and has an SCP at the root that prevents sharing resources with external accounts. The company now needs to allow only the marketing account to share resources externally while preventing all other accounts from doing so. All accounts are in the same OU.
Which solution will meet these requirements?

A. Create a new SCP in the marketing account to explicitly allow sharing.
B. Edit the existing SCP to add a condition that excludes the marketing account.
C. Edit the SCP to include an Allow statement for the marketing account.
D. Use a permissions boundary in the marketing account.

Answer: B

NEW QUESTION 60
A company needs to detect unauthenticated access to its Amazon Elastic Kubernetes Service (Amazon EKS) clusters. The solution must require no additional configuration of the existing EKS deployment.
Which solution will meet these requirements with the LEAST operational effort?

A. Install a third-party security add-on.
B. Enable AWS Security Hub and monitor Kubernetes findings.
C. Monitor CloudWatch Container Insights metrics for EKS.
D. Enable Amazon GuardDuty and use EKS Audit Log Monitoring.

Answer: D

NEW QUESTION 62
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 connection
B. Use the IP addresses from these remote connections to create deny rules in the security group of the instanc
C. Install diagnostic tools on the instance for investigatio
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 rul
F. Replace the security group with a new security group that allows connections only from a diagnostics security grou
G. Update the outbound network ACL for the us-east-1b subnet to remove the deny all rul
H. Launch a new EC2 instance that has diagnostic tool
I. Assign the new security group to the new EC2 instanc
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 terminatio
L. Terminate the instanc
M. Launch a new EC2 instance in us-east-1a that has diagnostic tool
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 instanc
P. Attach the AWS WAF web ACL to the instance to mitigate the attac

Q. Log in to the instance and install diagnostic tools to investigate the instance.

Answer: C

NEW QUESTION 66

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons 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