

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's security team wants to receive near-real-time email notifications about AWS abuse reports related to DoS attacks. An Amazon SNS topic already exists and is subscribed to by the security team.

What should the security engineer do next?

- A. Poll Trusted Advisor for abuse notifications by using a Lambda function.
- B. Create an Amazon EventBridge rule that matches AWS Health events for AWS_ABUSE_DOS_REPORT and publishes to SNS.
- C. Poll the AWS Support API for abuse cases by using a Lambda function.
- D. Detect abuse reports by using CloudTrail logs and CloudWatch alarms.

Answer: B

NEW QUESTION 3

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 4

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 5

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 6

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 7

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 8

A company runs an internet-accessible application on several Amazon EC2 instances that run Windows Server. The company used an instance profile to configure the EC2 instances. A security team currently accesses the VPC that hosts the EC2 instances by using an AWS Site-to-Site VPN tunnel from an on-premises office. The security team issues a policy that requires all external access to the VPC to be blocked in the event of a security incident. However, during an incident, the security team must be able to access the EC2 instances to obtain forensic information on the instances. Which solution will meet these requirements?

- A. Install EC2 Instance Connect on the EC2 instance
- B. Update the IAM policy for the IAM role to grant the required permission
- C. Use the AWS CLI to open a tunnel to connect to the instances.
- D. Install EC2 Instance Connect on the EC2 instance
- E. Configure the instances to permit access to the ec2-instance-connect command use
- F. Use the AWS Management Console to connect to the EC2 instances.
- G. Create an EC2 Instance Connect endpoint in the VP
- H. Configure an appropriate security group to allow access between the EC2 instances and the endpoint
- I. Use the AWS CLI to open a tunnel to connect to the instances.
- J. Create an EC2 Instance Connect endpoint in the VP
- K. Configure an appropriate security group to allow access between the EC2 instances and the endpoint
- L. Use the AWS Management Console to connect to the EC2 instances.

Answer: D

NEW QUESTION 9

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 10

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 10

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 rule
- L. Create a Lambda function that applies a bucket policy to deny requests when the value of the aws:SecureTransport condition key is False
- M. Set the Lambda function as the target of the rule.
- N. Create an AWS CloudTrail trail
- O. Enable S3 data events on the trail
- P. Create an AWS Lambda function that applies a bucket policy to deny requests when the value of the aws:SecureTransport condition key is False
- Q. Configure the CloudTrail trail to invoke the Lambda function.

Answer: B

NEW QUESTION 13

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 SQS
- D. Restrict access using aws:SourceVpce and aws:PrincipalOrgId conditions.
- E. Use a third-party cloud access security broker (CASB).

Answer: C

NEW QUESTION 18

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 23

A company stores infrastructure and application code in web-based, third-party, Git-compatible code repositories outside of AWS. The company wants to give the code repositories the ability to securely authenticate and assume an existing IAM role within the company's AWS account by using OpenID Connect (OIDC).

Which solution will meet these requirements?

- A. Create an OIDC identity provider (IdP) by using AWS Identity and Access Management (IAM) federation
- B. Modify the trust policy of the IAM role to allow the code repositories to assume the IAM role.
- C. Use AWS Identity and Access Management (IAM) Roles Anywhere to create a trust anchor that uses OIDC
- D. Modify the trust policy of the IAM role to allow the code repositories to assume the IAM role.
- E. Set up an account instance of AWS IAM Identity Center
- F. Configure access to the code repositories as a customer managed OIDC application
- G. Grant the application access to the IAM role.
- H. Use AWS Resource Access Manager (AWS RAM) to create a new resource share that uses OIDC
- I. Limit the resource share to the specified code repositories
- J. Grant the IAM role access to the resource share.

Answer: A

NEW QUESTION 27

A company is planning to migrate its applications to AWS in a single AWS Region. The company's applications will use a combination of Amazon EC2 instances, Elastic Load Balancing (ELB) load balancers, and Amazon S3 buckets. The company wants to complete the migration as quickly as possible. All the applications must meet the following requirements:

- Data must be encrypted at rest.
- Data must be encrypted in transit.
- Endpoints must be monitored for anomalous network traffic.

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

- A. Install the Amazon Inspector agent on EC2 instances by using AWS Systems Manager Automation.
- B. Enable Amazon GuardDuty in all AWS accounts.
- C. Create VPC endpoints for Amazon EC2 and Amazon S3. Update VPC route tables to use only the secure VPC endpoints.
- D. Configure AWS Certificate Manager (ACM). Configure the load balancers to use certificates from ACM.
- E. Use AWS Key Management Service (AWS KMS) for key management
- F. Create an S3 bucket policy to deny any PutObject command with a condition for x-amz-meta-side-encryption.
- G. Use AWS Key Management Service (AWS KMS) for key management
- H. Create an S3 bucket policy to deny any PutObject command with a condition for x-amz-server-side-encryption.

Answer: BDF

NEW QUESTION 30

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 33

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

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 38

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 assigned.
- 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 set.
- D. Create a second permission set that includes the removed policy.
- E. Apply the permission sets separately to the user.
- F. Evaluate the logic of the AWS managed policy and the customer managed policy.
- G. Resolve any policy conflicts in the permission set before deployment.
- H. Do not add the new permission set to the user.
- I. Instead, edit the user's existing permission set to include the AWS managed policy and the customer managed policy.

Answer: A

NEW QUESTION 40

A company must inventory sensitive data across all Amazon S3 buckets in all accounts from a single security account.

- A. Delegate Amazon Macie and Security Hub administration.
- B. Use Amazon Inspector with Security Hub.
- C. Use Inspector with Trusted Advisor.
- D. Use Macie with Trusted Advisor.

Answer: A

NEW QUESTION 42

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 multivalued answer routing to send traffic to the containers.

Answer: C

NEW QUESTION 44

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

- A. Use Amazon Cognito identity pools and the GetId API.
- B. Use Amazon Cognito identity pools and AssumeRoleWithWebIdentity.

- C. Use Amazon Cognito user pools with ID tokens.
- D. Use Amazon Cognito user pools with access tokens.

Answer: B

NEW QUESTION 49

.....

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](#)