KaozhengPro

IT認證考試題庫

專業平臺

考證寶提供最新考古題與模擬試題
協助您高效通過認證考試

www.kaozhengpro.com

Exam : **SCS-C03**

Title : AWS Certified Security - Specialty

Version : DEMO

1.A security administrator is setting up a new AWS account. The security administrator wants to secure the data that a company stores in an Amazon S3 bucket. The security administrator also wants to reduce the chance of unintended data exposure and the potential for misconfiguration of objects that are in the S3 bucket.
Which solution will meet these requirements with the LEAST operational overhead?
A. Configure the S3 Block Public Access feature for the AWS account.
B. Configure the S3 Block Public Access feature for all objects that are in the bucket.
C. Deactivate ACLs for objects that are in the bucket.
D. Use AWS PrivateLink for Amazon S3 to access the bucket.
Answer: A
Explanation:
Amazon S3 Block Public Access configured at the AWS account level is the recommended and most effective approach to protect data stored in Amazon S3 while minimizing operational overhead. AWS Security Specialty documentation explains that S3 Block Public Access provides centralized, preventative controls designed to block public access to S3 buckets and objects regardless of individual bucket policies or object-level ACL configurations. When enabled at the account level, these controls automatically apply to all existing and newly created buckets, significantly reducing the risk of accidental exposure caused by misconfigured permissions.
The AWS Certified Security – Specialty Study Guide emphasizes that public access misconfiguration is a leading cause of data leaks in cloud environments. Account-level S3 Block Public Access acts as a guardrail by overriding any attempt to grant public permissions through bucket policies or ACLs. This eliminates the need to manage security settings on a per-bucket or per-object basis, thereby reducing administrative complexity and human error.
Configuring Block Public Access at the object level, as in option B, requires continuous monitoring and manual configuration, which increases operational overhead. Disabling ACLs alone, as described in option C, does not fully prevent public access because bucket policies can still allow public permissions. Using AWS PrivateLink, as in option D, controls network access but does not protect against public exposure through misconfigured S3 policies.
AWS security best practices explicitly recommend enabling S3 Block Public Access at the account level as the primary mechanism for preventing unintended public data exposure with minimal management effort.
Referenced AWS Specialty Documents:
AWS Certified Security – Specialty Official Study Guide
Amazon S3 Security Best Practices Documentation
Amazon S3 Block Public Access Overview
AWS Well-Architected Framework – Security Pillar

2.A company’s developers are using AWS Lambda function URLs to invoke functions directly. Thecompany must ensure that developers cannot configure or deploy unauthenticated functions in production accounts. The company wants to meet this requirement by using AWS Organizations. The solution must not require additional work for the developers.
Which solution will meet these requirements?
A. Require the developers to configure all function URLs to support cross-origin resource sharing (CORS) when the functions are called from a different domain.

B. Use an AWS WAF delegated administrator account to view and block unauthenticated access to function URLs in production accounts, based on the OU of accounts that are using the functions.
C. Use SCPs to allow all lambda:CreateFunctionUrlConfig and lambda:UpdateFunctionUrlConfig actions that have a lambda:FunctionUrlAuthType condition key value of AWS_IAM.
D. Use SCPs to deny all lambda:CreateFunctionUrlConfig and lambda:UpdateFunctionUrlConfig actions that have a lambda:FunctionUrlAuthType condition key value of NONE.
Answer: D
Explanation:
AWS Organizations service control policies (SCPs) are designed to enforce preventive guardrails across accounts without requiring application-level changes. According to the AWS Certified Security – Specialty documentation, SCPs can restrict specific API actions or require certain condition keys to enforce security standards centrally. AWS Lambda function URLs support two authentication modes: AWS_IAM and NONE. When the authentication type is set to NONE, the function URL becomes publicly accessible, which introduces a significant security risk in production environments.
By using an SCP that explicitly denies the lambda:CreateFunctionUrlConfig and lambda:UpdateFunctionUrlConfig actions when the lambda:FunctionUrlAuthType condition key equals NONE, the organization ensures that unauthenticated function URLs cannot be created or modified in production accounts. This enforcement occurs at the AWS Organizations level and applies automatically to all accounts within the specified organizational units (OUs). Developers are not required to change their workflows or add additional controls, satisfying the requirement of no additional developer effort.
Option A relates to browser-based access controls and does not provide authentication or authorization enforcement. Option B is not valid because AWS WAF cannot be attached directly to AWS Lambda function URLs. Option C is incorrect because SCPs do not grant permissions; they only limit permissions. AWS documentation clearly states that SCPs define maximum available permissions and are evaluated before IAM policies.
This approach aligns with AWS best practices for centralized governance, least privilege, and preventive security controls.
Referenced AWS Specialty Documents:
AWS Certified Security – Specialty Official Study Guide
AWS Organizations Service Control Policies Documentation
AWS Lambda Security and Function URL Authentication Overview

3.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. Use the IP addresses from these remote connections to create deny rules in the security group of the

instance. Install diagnostic tools on the instance for investigation. 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.
B. Update the outbound network ACL for the subnet in us-east-1b to explicitly deny all connections as the first rule. Replace the security group with a new security group that allows connections only from a diagnostics security group. Update the outbound network ACL for the us-east-1b subnet to remove the deny all rule. Launch a new EC2 instance that has diagnostic tools. Assign the new security group to the new EC2 instance. Use the new EC2 instance to investigate the suspicious instance.
C. Ensure that the Amazon Elastic Block Store (Amazon EBS) volumes that are attached to the suspicious EC2 instance will not delete upon termination. Terminate the instance. Launch a new EC2 instance in us-east-1a that has diagnostic tools. Mount the EBS volumes from the terminated instance for investigation.
D. Create an AWS WAF web ACL that denies traffic to and from the suspicious instance. Attach the AWS WAF web ACL to the instance to mitigate the attack. Log in to the instance and install diagnostic tools to investigate the instance.
Answer: C
Explanation:
AWS incident response best practices emphasize immediate containment, preservation of evidence, and safe forensic investigation. According to the AWS Certified Security – Specialty Study Guide, when an EC2 instance is suspected of compromise, security teams should avoid logging in to the instance or installing additional tools, as these actions can alter evidence and increase risk.
Terminating the compromised instance after ensuring that its Amazon EBS volumes are preserved prevents further malicious activity immediately. By setting the EBS volumes to not delete on termination, all disk data is retained for forensic analysis. Launching a new, clean EC2 instance in a different subnet or Availability Zone with preinstalled diagnostic tools allows investigators to safely attach and analyze the compromised volumes without executing potentially malicious code.
Option A introduces significant risk by logging in to the compromised instance and modifying security controls during active compromise. Option B delays containment and allows continued outbound traffic during investigation steps. Option D is invalid because AWS WAF cannot be attached directly to Amazon EC2 instances and does not control outbound traffic.
AWS documentation strongly recommends isolating or terminating compromised resources and performing offline analysis using detached storage volumes. This approach ensures immediate mitigation, preserves forensic integrity, and aligns with AWS incident response frameworks.
Referenced AWS Specialty Documents:
AWS Certified Security – Specialty Official Study Guide
AWS Incident Response Best Practices
Amazon EC2 and EBS Forensics Guidance
AWS Well-Architected Framework – Security Pillar

4.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
Explanation:
AWS Secrets Manager is a regional service that is accessed through private AWS endpoints. In a VPC without internet access, AWS recommends using AWS PrivateLink through interface VPC endpoints to enable secure, private connectivity to supported AWS services. According to AWS Certified Security – Specialty documentation, interface VPC endpoints allow resources within a VPC to communicate with AWS services without traversing the public internet, NAT devices, or internet gateways.
An interface VPC endpoint for Secrets Manager creates elastic network interfaces (ENIs) within the VPC subnets and assigns private IP addresses that route traffic directly to the Secrets Manager service. Because the VPC has private DNS enabled, the standard Secrets Manager DNS hostname resolves to the private IP addresses of the interface endpoint, allowing the Lambda rotation function to communicate securely and transparently.
Option A introduces unnecessary complexity and expands the attack surface by allowing outbound internet access. Option B is incorrect because gateway VPC endpoints are supported only for Amazon S3 and Amazon DynamoDB. Option D violates the security requirement by exposing the VPC to the internet.
AWS security best practices explicitly recommend interface VPC endpoints as the most secure connectivity method for private VPC workloads accessing AWS managed services.
Referenced AWS Specialty Documents:
AWS Certified Security – Specialty Official Study Guide
AWS Secrets Manager Security Architecture
AWS PrivateLink and Interface VPC Endpoints Documentation

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

Answer: D

Explanation:

The Amazon CloudWatch agent requires explicit IAM permissions to create log groups, create log streams, and put log events into Amazon CloudWatch Logs. According to the AWS Certified Security – Specialty Study Guide, the most common cause of CloudWatch agent log delivery failures is missing or insufficient IAM permissions on the EC2 instance role.

The CloudWatchAgentServerPolicy AWS managed policy provides the required permissions, including logs:CreateLogGroup, logs:CreateLogStream, and logs:PutLogEvents. Attaching this policy to the EC2 instance role enables the CloudWatch agent to successfully deliver custom application logs without requiring changes to the application or logging configuration.

Options A, B, and C are incorrect because CloudTrail, Amazon S3, and Amazon Inspector are not designed to ingest custom application logs from EC2 instances in this manner. AWS documentation clearly states that IAM permissions must be granted to the EC2 role for CloudWatch Logs ingestion. This approach aligns with AWS best practices for least privilege while ensuring reliable detection and monitoring capabilities.

Referenced AWS Specialty Documents:

AWS Certified Security – Specialty Official Study Guide

Amazon CloudWatch Logs Agent Configuration

AWS IAM Best Practices for Monitoring