# 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 Manage
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 uses AWS Organizations to manage an organization that consists of three workload OUs: Production, Development, and Testing. The company uses AWS CloudFormation templates to define and deploy workload infrastructure in AWS accounts that are associated with the OUs. Different SCPs are attached to each workload OU.
The company successfully deployed a CloudFormation stack update to workloads in the Development OU and the Testing OU. When the company uses the same CloudFormation template to deploy the stack update in an account in the Production OU, the update fails.
The error message reports insufficient IAM permissions.
What is the FIRST step that a security engineer should take to troubleshoot this issue?

A. Review the AWS CloudTrail logs in the account in the Production O
B. Search for any failed API calls from CloudFormation during the deployment attempt.
C. Remove all the SCPs that are attached to the Production O
D. Rerun the CloudFormation stack update to determine if the SCPs were preventing the CloudFormation API calls.
E. Confirm that the role used by CloudFormation has sufficient permissions to create, update, and delete the resources that are referenced in the CloudFormation template.
F. Make all the SCPs that are attached to the Production OU the same as the SCPs that are attached to the Testing OU.

**Answer:** A

**NEW QUESTION 3**
A security team manages a company??s AWS Key Management Service (AWS KMS) customer managed keys. Only members of the security team can administer the KMS keys. The company's application team has a software process that needs temporary access to the keys occasionally. The security team needs to provide the application team's software process with access to the keys.
Which solution will meet these requirements with the LEAST operational overhead?

A. Export the KMS key material to an on-premises hardware security module (HSM). Give the application team access to the key material.
B. Edit the key policy that grants the security team access to the KMS keys by adding the application team as principal
C. Revert this change when the application team no longer needs access.
D. Create a key grant to allow the application team to use the KMS key
E. Revoke the grant when the application team no longer needs access.
F. Create a new KMS key by generating key material on premise
G. Import the key material to AWS KMS whenever the application team needs acces
H. Grant the application team permissions to use the key.

**Answer:** C

**NEW QUESTION 4**
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 5**
A company's security engineer receives an abuse notification from AWS indicating that malware is being hosted from the company??s AWS account. The security engineer discovers that an IAM user created a new Amazon S3 bucket without authorization.
Which combination of steps should the security engineer take to MINIMIZE the consequences of this compromise? (Select THREE.)

A. Encrypt all AWS CloudTrail logs.
B. Turn on Amazon GuardDuty.
C. Change the password for all IAM users.
D. Rotate or delete all AWS access keys.
E. Take snapshots of all Amazon Elastic Block Store (Amazon EBS) volumes.
F. Delete any resources that are unrecognized or unauthorized.

**Answer:** BDF

**NEW QUESTION 6**

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 instanc
B. Send the custom logs to CloudTrail instead of CloudWatch.
C. Add Amazon S3 to the trust policy of the EC2 instanc
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 instanc
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 7**
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 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 profil
C. Configure the policy condition to restrict access based on the s3:ResourceTag/ClientId tag of each invoic
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 bucke
H. Embed the keys into the scrip
I. Use the keys to generate the pre-signed URLs.

**Answer:** B

**NEW QUESTION 9**
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 10**
An application is running on an Amazon EC2 instance that has an IAM role attached. The IAM role provides access to an AWS Key Management Service (AWS KMS) customer managed key and an Amazon S3 bucket. The key is used to access 2 TB of sensitive data that is stored in the S3 bucket. A security engineer discovers a potential vulnerability on the EC2 instance that could result in the compromise of the sensitive data. Due to other critical operations, the security engineer cannot immediately shut down the EC2 instance for vulnerability patching.
What is the FASTEST way to prevent the sensitive data from being exposed?

A. Download the data from the existing S3 bucket to a new EC2 instanc
B. Then delete the data from the S3 bucke
C. Re-encrypt the data with a client-based ke
D. Upload the data to a new S3 bucket.
E. Block access to the public range of S3 endpoint IP addresses by using a host-based firewal
F. Ensure that internet-bound traffic from the affected EC2 instance is routed through the host-based firewall.
G. Revoke the IAM role??s active session permission
H. Update the S3 bucket policy to deny access to the IAM rol

I. Remove the IAM role from the EC2 instance profile.
J. Disable the current ke
K. Create a new KMS key that the IAM role does not have access to, and re-encrypt all the data with the new ke
L. Schedule the compromised key for deletion.

**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 15**
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 17**
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 Hu
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 Hu
D. In each account, configure Amazon Inspector to scan the S3 buckets for sensitive dat
E. Publish sensitive data findings to Security Hub.
F. In each account, configure Amazon Inspector to scan the S3 buckets for sensitive dat
G. Enable Amazon Inspector integration with AWS Trusted Adviso
H. Publish sensitive data findings to Trusted Advisor.
I. In each account, enable and configure Amazon Macie to detect sensitive dat
J. Enable Macie integration with AWS Trusted Adviso
K. Publish sensitive data findings to Trusted Advisor.

**Answer:** A

**NEW QUESTION 20**
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 22**
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 23**
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 25**
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 26**
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 28**
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 32**
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 37**
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 39**
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 44**
A company has an AWS account that hosts a production application. The company receives an email notification that Amazon GuardDuty has detected an Impact:IAMUser/AnomalousBehavior finding in the account. A security engineer needs to run the investigation playbook for this security incident and must collect and analyze the information without affecting the application.
Which solution will meet these requirements MOST quickly?

A. Log in to the AWS account by using read-only credential
B. Review the GuardDuty finding for details about the IAM credentials that were use
C. Use the IAM console to add a DenyAll policy to the IAM principal.
D. Log in to the AWS account by using read-only credential
E. Review the GuardDuty finding to determine which API calls initiated the findin
F. Use Amazon Detective to review the API calls in context.
G. Log in to the AWS account by using administrator credential
H. Review the GuardDuty finding for details about the IAM credentials that were use
I. Use the IAM console to add a DenyAll policy to the IAM principal.
J. Log in to the AWS account by using read-only credential
K. Review the GuardDuty finding to determine which API calls initiated the findin
L. Use AWS CloudTrail Insights and AWS CloudTrail Lake to review the API calls in context.

**Answer:** B

**NEW QUESTION 46**
A company has a PHP-based web application that uses Amazon S3 as an object store for user files. The S3 bucket is configured for server-side encryption with Amazon S3 managed keys (SSE-S3). New requirements mandate full control of encryption keys.
Which combination of steps must a security engineer take to meet these requirements? (Select THREE.)

A. Create a new customer managed key in AWS Key Management Service (AWS KMS).
B. Change the SSE-S3 configuration on the S3 bucket to server-side encryption with customer-provided keys (SSE-C).
C. Configure the PHP SDK to use the SSE-S3 key before upload.
D. Create an AWS managed key for Amazon S3 in AWS KMS.
E. Change the SSE-S3 configuration on the S3 bucket to server-side encryption with AWS KMS managed keys (SSE-KMS).
F. Change all the S3 objects in the bucket to use the new encryption key.

**Answer:** AEF

**NEW QUESTION 51**
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 57**
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**
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 64**
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 68**
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 71**
A security engineer needs to implement a solution to identify any sensitive data that is stored in an Amazon S3 bucket. The solution must report on sensitive data in the S3 bucket by using an existing Amazon Simple Notification Service (Amazon SNS) topic.
Which solution will meet these requirements with the LEAST implementation effort?

A. Enable AWS Confi
B. Configure AWS Config to monitor for sensitive data in the S3 bucket and to send notifications to the SNS topic.
C. Create an AWS Lambda function to scan the S3 bucket for sensitive data that matches a patter
D. Program the Lambda function to send notifications to the SNS topic.
E. Configure Amazon Macie to use managed data identifiers to identify and categorize sensitive dat
F. Create an Amazon EventBridge rule to send notifications to the SNS topic.
G. Enable Amazon GuardDut

H. Configure AWS CloudTrail S3 data event
I. Create an Amazon CloudWatch alarm that reacts to GuardDuty findings and sends notifications to the SNS topic.

**Answer:** C

**NEW QUESTION 74**
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 77**
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 81**
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 85**
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 86**
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 databas
B. Use the ARN to restore the Regional cluster by using the restore to point in time featur
C. Set a target time 5 days ago at 3:14 PM.
D. Identify the Regional cluster ARN for the databas
E. List snapshots that have been taken of the cluste
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 databas
J. Use the ARN to restore the Regional cluster by using the restore to point in time featur
K. Set a target time 14 days ago.

**Answer:** A

**NEW QUESTION 88**
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 89**
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 92**
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 95**
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 97**
.....

# 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