AWS Certified Security - Specialty (SCS-C02) Practice Questions

Question 1

A company uses Amazon S3 to store critical financial reports. To meet compliance requirements, the company must ensure that these reports cannot be modified or deleted for 7 years after creation. What is the most secure and efficient way to implement this requirement?

A. Use S3 Versioning and enable MFA Delete.

B. Enable S3 Object Lock in Governance mode with a retention period of 7 years.

C. Enable server-side encryption with AWS Key Management Service (KMS) and set a 7-year key rotation policy.

D. Apply a bucket policy to deny all delete actions for objects in the bucket.

Question 2

An organization is setting up a multi-account environment using AWS Organizations. The security team wants to ensure that no account can create resources in non-approved AWS Regions. What is the best way to enforce this restriction?

A. Use AWS Config rules to monitor the regions where resources are created.

B. Apply a Service Control Policy (SCP) that denies resource creation in non-approved Regions.

C. Enable AWS CloudTrail in all accounts to track resource creation.

D. Use IAM policies in each account to restrict resource creation.

Question 3

A security operations team needs to detect and respond to anomalous behavior across multiple AWS accounts in an organization. Which solution best supports this requirement?

A. Enable Amazon GuardDuty in each account and configure cross-account access for viewing findings.

B. Use AWS Config aggregators to collect and analyze configuration changes across accounts.

C. Deploy AWS Security Hub with delegated administrator and enable findings aggregation.

D. Use CloudWatch Alarms to monitor logs across all accounts.

Question 4

An application runs on an EC2 instance and retrieves credentials from AWS Secrets Manager. During a recent penetration test, the credentials were found in the application's memory. How can you prevent this vulnerability?

A. Use AWS KMS to encrypt the credentials before storing them in Secrets Manager.

B. Store the credentials as environment variables in the EC2 instance.

C. Use an IAM role assigned to the EC2 instance to provide access to Secrets Manager.

D. Retrieve the credentials over HTTPS and delete them from memory after use.

Question 5

A company needs to encrypt sensitive data stored in an Amazon RDS database. The encryption keys must be rotated every year and should not leave AWS's secure environment. Which solution best meets these requirements?

A. Enable RDS encryption using a customer-managed key in AWS Key Management Service (KMS).

B. Enable RDS encryption using an AWS-managed key in KMS.

C. Use client-side encryption with an on-premises key management system.

D. Use AWS CloudHSM to manage encryption keys and integrate with RDS.

Question 6

An organization suspects unauthorized access to an S3 bucket. The bucket policy allows public read access, and there are no other controls in place. What is the fastest way to secure the bucket while investigating?

A. Delete the bucket policy.

B. Use AWS Config to identify the misconfigured bucket and apply a remediation rule.

C. Apply S3 Block Public Access at the account level.

D. Enable S3 Server Access Logging and analyze the logs for suspicious activity.

Question 7

A company has a hybrid cloud setup with AWS and on-premises servers. They want to ensure that data transmitted between these environments is encrypted and meets compliance standards. What solution should they use?

A. Use a Direct Connect connection without encryption for faster data transfer.

B. Use an IPsec VPN connection between the AWS VPC and on-premises network.

C. Enable AWS PrivateLink to connect the on-premises environment to AWS resources.

D. Use Amazon S3 Transfer Acceleration with encryption enabled for data transfers.

Question 8

An organization wants to ensure that administrators are notified when root account activity occurs in any AWS account. What is the best approach?

A. Enable CloudTrail and create an event notification for root account activity.

B. Use AWS Security Hub to send email notifications for root account activity.

C. Configure an IAM policy to block root account actions and notify administrators.

D. Enable AWS Config and create a rule for detecting root account usage.

Question 9

A development team is using Amazon SQS to queue tasks for a web application. They want to ensure that the messages in the queue cannot be intercepted or read by unauthorized users. What should they do?

A. Enable server-side encryption (SSE) for the SQS queue using an AWS-managed key.

B. Configure a VPC endpoint for SQS to restrict network access.

C. Apply an IAM policy to the queue that allows only specific users to send or receive messages.

D. Enable CloudTrail logging for the SQS queue.

Question 10

A company is building an application that processes highly sensitive healthcare data. To comply with regulatory requirements, the application must log all API calls, including the identity of the caller, and ensure the logs cannot be tampered with. Which solution meets these requirements?

A. Enable AWS CloudTrail and store logs in an S3 bucket with Object Lock enabled.

B. Use Amazon CloudWatch Logs with encryption enabled to store API call logs.

C. Implement AWS Config to track all API calls and send the logs to an S3 bucket.

D. Use Amazon Macie to monitor API calls and detect anomalies.

AWS Certified Security - Specialty (SCS-C02) Additional Practice Questions

Question 11

A company is using AWS Systems Manager Parameter Store to store sensitive application configurations. They want to ensure that these parameters are encrypted and access is logged. What is the best way to achieve this?

A. Enable default encryption in the Parameter Store with an AWS-managed key.

B. Use AWS Secrets Manager instead of Parameter Store.

C. Store sensitive parameters with encryption enabled using a customer-managed key in AWS Key Management Service (KMS).

D. Use plaintext parameters with IAM policies restricting access to Parameter Store.

Question 12

A financial services company wants to monitor and identify unauthorized changes to security groups in its VPC. Which AWS service provides the most effective way to achieve this?

A. AWS Config with rules for security group compliance.

B. Amazon CloudWatch Logs with VPC Flow Logs enabled.

C. AWS CloudTrail with Amazon Athena for query analysis.

D. Amazon GuardDuty with threat detection for security groups.

Question 13

An application uses an Amazon RDS database and must comply with regulations requiring encrypted connections between clients and the database. Which solution should the organization implement?

A. Enable encryption at rest for the RDS database.

B. Configure the RDS instance to only allow connections using SSL/TLS.

C. Use AWS Certificate Manager (ACM) to issue client certificates.

D. Use Amazon CloudFront to enforce HTTPS connections.

Question 14

A company has been experiencing brute force login attempts on its AWS accounts. What is the most effective way to detect and respond to these attempts?

A. Use Amazon GuardDuty to detect brute force attacks and notify administrators.

B. Enable AWS CloudTrail Insights and monitor anomalous API activity.

C. Use AWS Config to identify non-compliant IAM policies.

D. Enable Amazon Macie to detect sensitive data exposures.

Question 15

An organization uses AWS KMS to encrypt S3 buckets. They want to ensure that only specific applications can decrypt the data. How should this be implemented?

A. Use bucket policies to restrict access based on IAM user tags.

B. Configure an S3 bucket policy to enforce encryption with the specified KMS key.

C. Use key policies in AWS KMS to restrict access to specific IAM roles.

D. Enable S3 default encryption and rely on IAM policies to control access.

Question 16

A company requires all IAM users to rotate their passwords every 90 days and enforce multi-factor authentication (MFA). What is the best way to implement these requirements?

A. Enable IAM password policy and use AWS Config to monitor compliance.

B. Use AWS Single Sign-On (SSO) and enforce the password policy in the corporate directory.

C. Create an AWS Config rule for password rotation and enable MFA through an IAM policy.

D. Use an AWS Lambda function to check password age and enforce rotation.

Question 17

A healthcare provider is storing patient data in an Amazon S3 bucket and needs to ensure compliance with HIPAA regulations. What should they do to meet these requirements?

A. Enable S3 bucket logging and monitor access using CloudWatch.

B. Encrypt the data at rest using an AWS-managed key.

C. Use Amazon Macie to detect sensitive data in the bucket.

D. Sign a Business Associate Agreement (BAA) with AWS and enable encryption using a customer-managed KMS key.

Question 18

A company runs a public-facing API using Amazon API Gateway and wants to protect it from Distributed Denial-of-Service (DDoS) attacks. What is the best approach?

A. Enable AWS Shield Advanced for the API Gateway endpoint.

B. Configure throttling settings in API Gateway to limit requests per second.

C. Use AWS WAF with rate-based rules to filter malicious traffic.

D. Deploy the API Gateway behind a CloudFront distribution.

Question 19

An organization has multiple AWS accounts and wants to centralize logging for security audits. What is the best way to implement this?

A. Enable CloudTrail in each account and send logs to a central S3 bucket.

B. Use AWS Config aggregators to collect compliance data across accounts.

C. Enable Amazon GuardDuty with centralized findings in a delegated account.

D. Use AWS Security Hub to aggregate findings across accounts.

Question 20

A company's security team wants to restrict access to sensitive data stored in Amazon DynamoDB to specific applications. How can this be achieved?

A. Use VPC endpoints to control access to DynamoDB.

B. Apply a resource-based IAM policy to the DynamoDB table.

C. Encrypt the DynamoDB table with a customer-managed key and restrict access using key policies.

D. Use IAM roles with fine-grained access control and attach them to the applications.

Question 21

An organization is using Amazon S3 to store log data and must ensure that the logs cannot be deleted for a period of 90 days. What is the most effective solution?

A. Enable MFA Delete on the S3 bucket.

B. Use an S3 Lifecycle policy to prevent deletion.

C. Configure an S3 Object Lock in Compliance mode with a retention period of 90 days.

D. Store the logs in Glacier to prevent deletion.

Question 22

A company wants to secure communications between its on-premises environment and AWS using private connectivity. Which AWS service should they use?

A. AWS Direct Connect with MACsec encryption.

B. AWS VPN with IPsec encryption.

C. Amazon CloudFront for encrypted connections.

D. VPC Peering between on-premises and AWS.

Question 23

A security team needs to ensure that sensitive data stored in Amazon EBS volumes is encrypted and the encryption keys are rotated annually. What is the best approach?

A. Use AWS-managed keys for EBS encryption.

B. Use a customer-managed key in AWS KMS and rotate it annually.

C. Enable encryption on the EBS volume and rely on the default key rotation policy.

D. Use an on-premises key management system to manage the keys.

Question 24

A company is implementing a CI/CD pipeline on AWS and wants to ensure that only approved AMIs are used for deploying EC2 instances. What is the best way to enforce this?

A. Use AWS Systems Manager Patch Manager to approve AMIs.

B. Apply an SCP to enforce the use of approved AMIs.

C. Create an Amazon Inspector rule to validate AMI compliance.

D. Use AWS Config rules to enforce AMI compliance during EC2 instance creation.

Question 25

An application running on EC2 instances requires secure access to an Amazon RDS database. What is the best approach to securely store and manage the database credentials?

A. Use an environment variable on the EC2 instance.

B. Store the credentials in AWS Secrets Manager and retrieve them using the EC2 IAM role.

C. Use Systems Manager Parameter Store with default encryption.

D. Hardcode the credentials in the application.

Question 26

A company needs to monitor and prevent accidental exposure of sensitive information in their S3 buckets. What AWS service should they use?

A. AWS Config.

B. Amazon Macie.

C. AWS Security Hub.

D. AWS CloudTrail.

Question 27

A web application must support authentication for end-users with social media providers such as Google and Facebook. What is the best solution?

A. Use AWS Cognito with social identity providers configured.

B. Use IAM roles to authenticate users with social media credentials.

C. Use AWS Single Sign-On (SSO) with OpenID Connect.

D. Create custom authentication middleware in the application.

Question 28

An organization is storing backups of critical databases in Amazon S3 Glacier and wants to ensure that the data cannot be deleted before the required retention period of 5 years. What should they do?

A. Enable MFA Delete on the S3 Glacier vault.

B. Use S3 Object Lock in Compliance mode for the Glacier vault.

C. Configure S3 Lifecycle policies to prevent deletion for 5 years.

D. Enable encryption using AWS KMS with a key rotation policy of 5 years.

Question 29

An organization wants to restrict network access to an Amazon RDS instance so that only specific IP ranges can connect. How can they achieve this?

A. Use a security group to allow traffic only from the specified IP ranges.

B. Configure an IAM policy to restrict access to the RDS instance.

C. Apply a resource-based policy to the RDS instance.

D. Use AWS Network Firewall to filter traffic to the RDS instance.

Question 30

A company needs to ensure that unauthorized changes to its AWS resource configurations are detected and logged. Which service should they use?

A. AWS Config with rules and compliance reporting.

B. Amazon GuardDuty for anomaly detection.

C. AWS CloudTrail with multi-region logging enabled.

D. AWS Systems Manager to automate change detection.

AWS Certified Security - Specialty (SCS-C02) Advanced Practice Questions

Question 31

A company is running a serverless web application that stores user-uploaded files in an Amazon S3 bucket. The application requires that all uploaded files are scanned for malware before being processed. If malware is detected, the file must be quarantined, and an alert must be sent to the security team. What is the most effective architecture for this solution?

A. Use an S3 Event Notification to trigger an AWS Lambda function that scans the file and moves it to a quarantine bucket if malware is detected. Use Amazon SNS to send alerts.

B. Configure an S3 bucket policy to scan files upon upload and quarantine infected files.

C. Use Amazon Macie to automatically detect malware in uploaded files and send notifications.

D. Enable Amazon GuardDuty to monitor the S3 bucket for malicious files and trigger an alert.

Question 32

A healthcare company stores sensitive patient data in an Amazon RDS database and wants to ensure that the database credentials are securely rotated every 30 days without requiring any manual intervention. Additionally, the application accessing the database must continue to function without interruption. What is the best solution?

A. Use AWS Secrets Manager to store the database credentials and configure automatic rotation with a Lambda function.

B. Configure an IAM role for the RDS instance to rotate credentials every 30 days.

C. Manually rotate the database credentials and update the application configuration.

D. Use AWS Systems Manager Parameter Store with a cron job to rotate credentials.

Question 33

An organization is using a multi-account structure with AWS Organizations. They need to ensure that all accounts enforce encryption of S3 buckets and deny the creation of buckets that do not comply. What is the most effective way to implement this?

A. Use AWS Config rules in each account to enforce encryption.

B. Create a Service Control Policy (SCP) that denies S3 bucket creation without encryption.

C. Enable Amazon Macie to detect unencrypted buckets and notify administrators.

D. Use S3 bucket policies to enforce encryption in each account.

Question 34

A financial services company must ensure that only authorized users can connect to their EC2 instances and that all connections are logged for auditing purposes. What is the most secure and efficient solution?

A. Enable detailed monitoring in Amazon CloudWatch and use IAM policies to restrict access.

B. Use Systems Manager Session Manager for access and log all session activity in CloudWatch Logs.

C. Configure VPC Flow Logs to capture connection details and store them in S3 for auditing.

D. Use an SSH key pair for access and enable CloudTrail to log SSH connections.

Question 35

An organization needs to implement a solution that provides centralized management and governance of security controls across its AWS accounts. The solution must also detect and remediate security risks automatically. What is the best approach?

A. Deploy AWS Security Hub with delegated administrator and enable integration with GuardDuty and AWS Config.

B. Use AWS Config aggregators to centralize security controls and manually apply remediation.

C. Enable Amazon Macie across all accounts and use it for centralized risk detection.

D. Use AWS Organizations with SCPs to enforce security controls and manually review findings.

Question 36

A company is using AWS Direct Connect for private connectivity between its on-premises data center and AWS. They are concerned about the confidentiality of data transmitted over this connection. How should the company address this concern?

A. Use AWS VPN over Direct Connect to encrypt traffic between on-premises and AWS.

B. Enable VPC Flow Logs to monitor all traffic passing through the Direct Connect connection.

C. Use AWS Shield Advanced to protect the Direct Connect connection from attacks.

D. Enable MACsec on the Direct Connect connection to encrypt traffic.

Question 37

An e-commerce company wants to protect its public-facing API Gateway from unauthorized access and ensure that only authenticated users can access certain endpoints. What is the best solution?

A. Use AWS WAF with IP-based access control lists to restrict access.

B. Use Amazon Cognito user pools to authenticate users and configure authorization rules.

C. Use IAM roles to authenticate and authorize access to API Gateway endpoints.

D. Enable mutual TLS authentication on API Gateway and distribute client certificates.

Question 38

A company is running an application on Amazon ECS using Fargate. They want to ensure that secrets, such as database credentials, are securely injected into the containers at runtime without hardcoding them into the application. What is the best approach?

A. Use AWS Secrets Manager and configure ECS task definitions to retrieve secrets at runtime.

B. Store secrets in environment variables in the ECS task definition.

C. Use an encrypted file within the container to store secrets.

D. Use an IAM role assigned to the ECS service to provide access to a secure S3 bucket with the secrets.

Question 39

An organization needs to secure its Amazon Redshift cluster to ensure compliance with regulatory requirements. The data must be encrypted at rest and in transit, and access must be restricted to specific IP ranges. What steps should be taken?

A. Enable encryption using AWS KMS for data at rest, configure VPC security groups for IP restrictions, and enforce SSL/TLS for in-transit encryption.

B. Use IAM roles to control access, enable encryption at rest, and use CloudFront for encrypted connections.

C. Enable Amazon GuardDuty to monitor the cluster, encrypt data using an AWS-managed key, and configure VPC Flow Logs.

D. Use Amazon Macie for compliance checks, configure VPC endpoints, and encrypt data using client-side encryption.

Question 40

A company has identified that some IAM users have unused access keys that are more than 180 days old. They want to automate the detection and remediation of such keys to improve security. What is the best solution?

A. Use AWS Config rules to detect unused access keys and AWS Lambda to deactivate them.

B. Enable AWS CloudTrail and use Amazon Athena to identify and delete unused access keys.

C. Use Amazon Macie to monitor IAM activity and notify administrators about unused keys.

D. Use AWS Trusted Advisor to find unused keys and remove them manually.

Would you like the answers and explanations for these now, or do you want to iterate on these questions first?

Answer Key and Explanations

Question 1: B. Enable S3 Object Lock in Governance mode with a retention period of 7 years.

Explanation: S3 Object Lock in Governance mode ensures data cannot be deleted or modified for the specified period, meeting compliance requirements.

Question 2: B. Apply a Service Control Policy (SCP) that denies resource creation in non-approved Regions.

Explanation: SCPs enforce organization-wide restrictions on accounts, making them the most efficient solution.

Question 3: C. Deploy AWS Security Hub with delegated administrator and enable findings aggregation.

Explanation: Security Hub aggregates findings across accounts, enabling centralized anomaly detection and response.

Question 4: C. Use an IAM role assigned to the EC2 instance to provide access to Secrets Manager.

Explanation: IAM roles provide temporary credentials and avoid hardcoding sensitive data in memory.

Question 5: A. Enable RDS encryption using a customer-managed key in AWS Key Management Service (KMS).

Explanation: Customer-managed keys in KMS provide more control and support key rotation.

Question 6: C. Apply S3 Block Public Access at the account level.

Explanation: Blocking public access is the fastest and most effective way to secure S3 buckets across the account.

Question 7: B. Use an IPsec VPN connection between the AWS VPC and on-premises network.

Explanation: IPsec VPN ensures encrypted communication between AWS and on-premises.

Question 8: A. Enable CloudTrail and create an event notification for root account activity.

Explanation: CloudTrail provides visibility into account activity, including root account usage.

Question 9: A. Enable server-side encryption (SSE) for the SQS queue using an AWS-managed key.

Explanation: SSE ensures that messages in SQS are encrypted at rest, protecting data from unauthorized access.

Question 10: A. Enable AWS CloudTrail and store logs in an S3 bucket with Object Lock enabled.

Explanation: CloudTrail provides detailed API logging, and S3 Object Lock ensures log immutability.

Answer Key and Explanations

Question 11

Answer: C. Store sensitive parameters with encryption enabled using a customer-managed key in AWS Key Management Service (KMS).

Explanation: Using a customer-managed KMS key provides control over the encryption process and ensures logging through AWS CloudTrail for audit purposes.

Question 12

Answer: A. AWS Config with rules for security group compliance.

Explanation: AWS Config provides a way to monitor and evaluate changes to security group configurations against compliance rules.

Question 13

Answer: B. Configure the RDS instance to only allow connections using SSL/TLS.

Explanation: SSL/TLS ensures that data in transit between clients and the database is encrypted, meeting compliance requirements.

Question 14

Answer: A. Use Amazon GuardDuty to detect brute force attacks and notify administrators.

Explanation: GuardDuty detects suspicious activities, including brute force login attempts, and can trigger notifications for incident response.

Question 15

Answer: C. Use key policies in AWS KMS to restrict access to specific IAM roles.

Explanation: KMS key policies provide granular control over who can decrypt data, ensuring that only authorized applications can access it.

Question 16

Answer: A. Enable IAM password policy and use AWS Config to monitor compliance.

Explanation: IAM password policies enforce password rotation and complexity requirements, while AWS Config monitors compliance with these rules.

Question 17

Answer: D. Sign a Business Associate Agreement (BAA) with AWS and enable encryption using a customer-managed KMS key.

Explanation: A BAA is required for HIPAA compliance, and using a customer-managed key provides control over encryption.

Question 18

Answer: C. Use AWS WAF with rate-based rules to filter malicious traffic.

Explanation: WAF provides protection against DDoS attacks by filtering and blocking malicious traffic.

Question 19

Answer: A. Enable CloudTrail in each account and send logs to a central S3 bucket.

Explanation: Centralized logging with CloudTrail provides a consolidated view of all account activities for auditing purposes.

Question 20

Answer: D. Use IAM roles with fine-grained access control and attach them to the applications.

Explanation: IAM roles with fine-grained access policies ensure that only authorized applications can access sensitive data in DynamoDB.

Question 21

Answer: C. Configure an S3 Object Lock in Compliance mode with a retention period of 90 days.

Explanation: S3 Object Lock in Compliance mode ensures that objects cannot be deleted during the retention period.

Question 22

Answer: B. AWS VPN with IPsec encryption.

Explanation: AWS VPN uses IPsec to provide secure, encrypted connectivity between on-premises and AWS.

Question 23

Answer: B. Use a customer-managed key in AWS KMS and rotate it annually.

Explanation: Customer-managed keys in KMS allow manual or automatic rotation according to organizational policies.

Question 24

Answer: D. Use AWS Config rules to enforce AMI compliance during EC2 instance creation.

Explanation: AWS Config rules can validate that only approved AMIs are used for EC2 instances.

Question 25

Answer: B. Store the credentials in AWS Secrets Manager and retrieve them using the EC2 IAM role.

Explanation: Secrets Manager securely stores credentials and integrates with IAM roles for secure access.

Question 26

Answer: B. Amazon Macie.

Explanation: Macie automatically detects sensitive data in S3 buckets and provides alerts for potential exposures.

Question 27

Answer: A. Use AWS Cognito with social identity providers configured.

Explanation: Cognito supports integration with social identity providers, making it ideal for user authentication.

Question 28

Answer: B. Use S3 Object Lock in Compliance mode for the Glacier vault.

Explanation: S3 Object Lock in Compliance mode ensures data retention for the required period without risk of deletion.

Question 29

Answer: A. Use a security group to allow traffic only from the specified IP ranges.

Explanation: Security groups provide fine-grained control over network access, including IP-based restrictions.

Question 30

Answer: A. AWS Config with rules and compliance reporting.

Explanation: AWS Config continuously monitors resource configurations and detects unauthorized changes, ensuring compliance.

Answer Key and Explanations for Advanced Questions

Question 31

Answer: A. Use an S3 Event Notification to trigger an AWS Lambda function that scans the file and moves it to a quarantine bucket if malware is detected. Use Amazon SNS to send alerts.

Explanation: S3 Event Notifications can trigger a Lambda function to perform malware scanning. Infected files can be moved to a quarantine bucket, and SNS can notify the security team.

Question 32

Answer: A. Use AWS Secrets Manager to store the database credentials and configure automatic rotation with a Lambda function.

Explanation: Secrets Manager provides seamless integration for credential rotation and ensures minimal disruption by automatically updating applications when credentials are rotated.

Question 33

Answer: B. Create a Service Control Policy (SCP) that denies S3 bucket creation without encryption.

Explanation: SCPs enforce organization-wide restrictions, ensuring that encryption is a mandatory requirement for S3 buckets in all accounts.

Question 34

Answer: B. Use Systems Manager Session Manager for access and log all session activity in CloudWatch Logs.

Explanation: Session Manager provides secure access to EC2 instances without the need for SSH, and all session activity can be logged for auditing purposes.

Question 35

Answer: A. Deploy AWS Security Hub with delegated administrator and enable integration with GuardDuty and AWS Config.

Explanation: Security Hub provides centralized management, integrates with other AWS security services, and supports automatic remediation through Config rules.

Question 36

Answer: A. Use AWS VPN over Direct Connect to encrypt traffic between on-premises and AWS.

Explanation: Direct Connect does not encrypt data by default. Adding a VPN overlay ensures encryption of data in transit.

Question 37

Answer: B. Use Amazon Cognito user pools to authenticate users and configure authorization rules.

Explanation: Cognito supports user authentication and authorization, making it an ideal choice for securing public-facing APIs.

Question 38

Answer: A. Use AWS Secrets Manager and configure ECS task definitions to retrieve secrets at runtime.

Explanation: Secrets Manager securely stores and injects secrets into ECS tasks without hardcoding them, ensuring secure runtime secret management.

Question 39

Answer: A. Enable encryption using AWS KMS for data at rest, configure VPC security groups for IP restrictions, and enforce SSL/TLS for in-transit encryption.

Explanation: KMS ensures encryption at rest, security groups restrict IP access, and enforcing SSL/TLS ensures encryption in transit.

Question 40

Answer: A. Use AWS Config rules to detect unused access keys and AWS Lambda to deactivate them.

Explanation: AWS Config can detect unused access keys based on activity, and Lambda can automate the remediation by deactivating or deleting them.

Would you like further clarification on any of these answers or additional questions in specific areas?