Free Questions for SCS-C02

Shared by Pruitt on 12-12-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A company has an organization with SCPs in AWS Organizations. The root SCP for the organization is as follows:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowsAllActions",
            "Effect": "Allow",
            "Action": "*",
            "Resource": "*"
        },
        {
            "Sid": "DenySES",
            "Effect": "Deny",
            "Action": "ses:*",
            "Resource": "*"
        }
    ]
}
```

The company's developers are members of a group that has an IAM policy that allows access to Amazon Simple Email Service (Amazon SES) by allowing ses:* actions. The account is a child to an OU that has an SCP that allows Amazon SES. The developers are receiving a not-authorized error when they try to access Amazon SES through the AWS Management Console.

Which change must a security engineer implement so that the developers can access Amazon SES?

Options:

A- Add a resource policy that allows each member of the group to access Amazon SES.

B- Add a resource policy that allows 'Principal': {'AWS': 'arn:aws:iam::account-number:group/Dev'}.

C- Remove the AWS Control Tower control (guardrail) that restricts access to Amazon SES.
D- Remove Amazon SES from the root SCP.

Answer:

D

Explanation:

The correct answer is D. Remove Amazon SES from the root SCP.

This answer is correct because the root SCP is the most restrictive policy that applies to all accounts in the organization. The root SCP explicitly denies access to Amazon SES by using the NotAction element, which means that any action that is not listed in the element is denied. Therefore, removing Amazon SES from the root SCP will allow the developers to access it, as long as there are no other SCPs or IAM policies that deny it.

The other options are incorrect because:

A) Adding a resource policy that allows each member of the group to access Amazon SES is not a solution, because resource policies are not supported by Amazon SES1. Resource policies are policies that are attached to AWS resources, such as S3 buckets or SNS topics, to control access to those resources2. Amazon SES does not have any resources that can have resource policies attached to them.

B) Adding a resource policy that allows ''Principal'': {''AWS'': ''arn:aws:iam::account-number:group/Dev''} is not a solution, because resource policies do not support IAM groups as principals3. Principals are entities that can perform actions on AWS resources, such as IAM users, roles, or AWS accounts4. IAM groups are not principals, but collections of IAM users that share the same permissions5.

C) Removing the AWS Control Tower control (guardrail) that restricts access to Amazon SES is not a solution, because AWS Control Tower does not have any guardrails that restrict access to Amazon SES6. Guardrails are high-level rules that govern the overall behavior of an organization's accounts7. AWS Control Tower provides a set of predefined guardrails that cover security, compliance, and operations domains8.

1: Amazon Simple Email Service endpoints and quotas 2: Resource-based policies and IAM policies 3: Specifying a principal in a policy 4: Policy elements: Principal 5: IAM groups 6: AWS Control Tower guardrails reference 7: AWS Control Tower concepts 8: AWS Control Tower guardrails

Question 2

Question Type: MultipleChoice

A company wants to implement host-based security for Amazon EC2 instances and containers in Amazon Elastic Container Registry (Amazon ECR). The company has deployed AWS Systems Manager Agent (SSM Agent) on the EC2 instances. All the company's AWS accounts are in one organization in AWS Organizations. The company will analyze the workloads for software vulnerabilities and unintended network exposure. The company will push any findings to AWS Security Hub. which the company has configured for the organization.

The company must deploy the solution to all member accounts, including pew accounts, automatically. When new workloads come online, the solution must scan the workloads.

Which solution will meet these requirements?

Options:

A- Use SCPs to configure scanning of EC2 instances and ECR containers for all accounts in the organization.
B- Configure a delegated administrator for Amazon GuardDuty for the organization. Create an Amazon EventBridge rule to initiate analysis of ECR containers
C- Configure a delegated administrator for Amazon Inspector for the organization. Configure automatic scanning for new member accounts.
D- Configure a delegated administrator for Amazon Inspector for the organization. Create an AWS Config rule to initiate analysis of ECR containers

Answer:

C

Explanation:

To implement host-based security for Amazon EC2 instances and containers in Amazon ECR with minimal operational overhead and ensure automatic deployment and scanning for new workloads, the recommended solution is to configure a delegated administrator for Amazon Inspector within the AWS Organizations structure. By enabling Amazon Inspector for the organization and configuring it to automatically scan new member accounts, the company can ensure that all EC2 instances and ECR containers are analyzed for software vulnerabilities and unintended network exposure. Amazon Inspector will automatically assess the workloads and push findings to AWS Security Hub, providing centralized security monitoring and compliance checking. This approach ensures that as new accounts or workloads are added, they are automatically included in the security assessments, maintaining a consistent security posture

across the organization with minimal manual intervention.

Question 3

Question Type: MultipleChoice

A company uses Amazon EC2 instances to host frontend services behind an Application Load Balancer. Amazon Elastic Block Store (Amazon EBS) volumes are attached to the EC2 instances. The company uses Amazon S3 buckets to store large files for images and music.

The company has implemented a security architecture oit>AWS to prevent, identify, and isolate potential ransomware attacks. The company now wants to further reduce risk.

A security engineer must develop a disaster recovery solution that can recover to normal operations if an attacker bypasses preventive and detective controls. The solution must meet an RPO of 1 hour.

Which solution will meet these requirements?

Options:

A- Use AWS Backup to create backups of the EC2 instances and S3 buckets every hour. Create AWS CloudFormation templates that replicate existing architecture components. Use AWS CodeCommit to store the CloudFormation templates alongside application configuration code.
B- Use AWS Backup to create backups of the EBS volumes and S3 objects every day. Use Amazon Security Lake to create a centralized data lake for AWS CloudTrail logs and VPC flow logs. Use the logs for automated response.
C- Use Amazon Security Lake to create a centralized data lake for AWS CloudTrail logs and VPC flow logs. Use the logs for automated response Enable AWS Security Hub to establish a single location for recovery procedures. Create AWS CloudFormation templates that replicate existing architecture components. Use AWS CodeCommit to store the CloudFormation templates alongside application configuration code.
D- Create EBS snapshots every 4 hours Enable Amazon GuardDuty Malware Protection. Create automation to immediately restore the most recent snapshot for any EC2 instances that produce an Execution:EC2/MaliciousFile finding in GuardDuty.

Answer:

A

Explanation:

The correct answer is A because it meets the RPO of 1 hour by creating backups of the EC2 instances and S3 buckets every hour. It also uses AWS CloudFormation templates to replicate the existing architecture components and AWS CodeCommit to store the templates and the application configuration code. This way, the security engineer can quickly restore the environment in case of a ransomware attack.

The other options are incorrect because they do not meet the RPO of 1 hour or they do not provide a complete disaster recovery solution. Option B only creates backups of the EBS volumes and S3 objects every day, which is not frequent enough to meet the RPO. Option C does not create any backups of the EC2 instances or the S3 buckets, which are essential for the frontend services. Option D only creates EBS snapshots every 4 hours, which is also not frequent enough to meet the RPO. Additionally, option D relies on Amazon GuardDuty to detect and respond to ransomware attacks, which may not be effective if the attacker bypasses the preventive and detective controls.

Question 4

Question Type: MultipleChoice

A company operates a web application that runs on Amazon EC2 instances. The application listens on port 80 and port 443. The company uses an Application Load Balancer (ALB) with AWS WAF to terminate SSL and to forward traffic to the application instances only on port 80.

The ALB is in public subnets that are associated with a network ACL that is named NACL1. The application instances are in dedicated private subnets that are associated with a network ACL that is named NACL2. An Amazon RDS for PostgreSQL DB instance that uses port 5432 is in a dedicated private subnet that is associated with a network ACL that is named NACL3. All the network ACLs currently allow all inbound and outbound traffic.

Which set of network ACL changes will increase the security of the application while ensuring functionality?

Options:

A- Make the following changes to NACL3:
* Add a rule that allows inbound traffic on port 5432 from NACL2.
* Add a rule that allows outbound traffic on ports 1024-65536 to NACL2.
* Remove the default rules that allow all inbound and outbound traffic.

B- Make the following changes to NACL3:
* Add a rule that allows inbound traffic on port 5432 from the CIDR blocks of the application instance subnets.
* Add a rule that allows outbound traffic on ports 1024-65536 to the application instance subnets.

* Remove the default rules that allow all inbound and outbound traffic.

C- Make the following changes to NACL2:

* Add a rule that allows outbound traffic on port 5432 to the CIDR blocks of the RDS subnets.
* Remove the default rules that allow all inbound and outbound traffic.

D- Make the following changes to NACL2:

* Add a rule that allows inbound traffic on port 5432 from the CIDR blocks of the RDS subnets.
* Add a rule that allows outbound traffic on port 5432 to the RDS subnets.

Answer:

B

Explanation:

For increased security while ensuring functionality, adjusting NACL3 to allow inbound traffic on port 5432 from the CIDR blocks of the application instance subnets, and allowing outbound traffic on ephemeral ports (1024-65536) back to those subnets creates a secure path for database access. Removing default allow-all rules enhances security by implementing the principle of least privilege, ensuring that only necessary traffic is permitted.

Question 5

Question Type: MultipleChoice

A company accidentally deleted the private key for an Amazon Elastic Block Store (Amazon EBS)-backed Amazon EC2 instance. A security engineer needs to regain access to the instance.

Which combination of steps will meet this requirement? (Choose two.)

Options:

A- Stop the instance. Detach the root volume. Generate a new key pair.

B- Keep the instance running. Detach the root volume. Generate a new key pair.

C- When the volume is detached from the original instance, attach the volume to another instance as a data volume. Modify the authorized_keys file with a new public key. Move the volume back to the original instance. Start the instance.

D- When the volume is detached from the original instance, attach the volume to another instance as a data volume. Modify the authorized_keys file with a new private key. Move the volume back to the original instance. Start the instance.

E- When the volume is detached from the original instance, attach the volume to another instance as a data volume. Modify the authorized_keys file with a new public key. Move the

volume back to the original instance that is running.

Answer:

A, C

Explanation:

If you lose the private key for an EBS-backed instance, you can regain access to your instance. You must stop the instance, detach its root volume and attach it to another instance as a data volume, modify the authorized_keys file with a new public key, move the volume back to the original instance, and restart the instance.
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/TroubleshootingInstancesConnecting.html#replacing-lost-key-pai

Question 6

Question Type: MultipleChoice

A company has AWS accounts in an organization in AWS Organizations. The company needs to install a corporate software package on all Amazon EC2 instances for all the accounts in the organization.

A central account provides base AMIs for the EC2 instances. The company uses AWS Systems Manager for software inventory and patching operations.

A security engineer must implement a solution that detects EC2 instances ttjat do not have the required software. The solution also must automatically install the software if the software is not present.

Which solution will meet these requirements?

Options:

A- Provide new AMIs that have the required software pre-installed. Apply a tag to the AMIs to indicate that the AMIs have the required software. Configure an SCP that allows new EC2 instances to be launched only if the instances have the tagged AMIs. Tag all existing EC2 instances.
B- Configure a custom patch baseline in Systems Manager Patch Manager. Add the package name for the required software to the approved packages list. Associate the new patch baseline with all EC2 instances. Set up a maintenance window for software deployment.
C- Centrally enable AWS Config. Set up the ec2-managedinstance-applications-required AWS

Config rule for all accounts Create an Amazon EventBridge rule that reacts to AWS Config events. Configure the EventBridge rule to invoke an AWS Lambda function that uses Systems Manager Run Command to install the required software.
D- Create a new Systems Manager Distributor package for the required software. Specify the download location. Select all EC2 instances in the different accounts. Install the software by using Systems Manager Run Command.

Answer:

C

Explanation:

Utilizing AWS Config with a custom AWS Config rule (ec2-managedinstance-applications-required) enables detection of EC2 instances lacking the required software across all accounts in an organization. By creating an Amazon EventBridge rule that triggers on AWS Config events, and configuring it to invoke an AWS Lambda function, automated actions can be taken to ensure compliance. The Lambda function can leverage AWS Systems Manager Run Command to install the necessary software on non-compliant instances. This approach ensures continuous compliance and automated remediation, aligning with best practices for cloud security and management.

Question 7

Question Type: MultipleChoice

A company has contracted with a third party to audit several AWS accounts. To enable the audit, cross- account IAM roles have been created in each account targeted for audit. The Auditor is having trouble accessing some of the accounts.

Which of the following may be causing this problem? (Choose three.)

Options:

A- The external ID used by the Auditor is missing or incorrect.
B- The Auditor is using the incorrect password.
C- The Auditor has not been granted sts:AssumeRole for the role in the destination account.
D- The Amazon EC2 role used by the Auditor must be set to the destination account role.
E- The secret key used by the Auditor is missing or incorrect.
F- The role ARN used by the Auditor is missing or incorrect.

Answer:

A, C, F

Explanation:

The following may be causing the problem for the Auditor:

A) The external ID used by the Auditor is missing or incorrect. This is a possible cause, because the external ID is a unique identifier that is used to establish a trust relationship between the accounts. The external ID must match the one that is specified in the role's trust policy in the destination account1.

C) The Auditor has not been granted sts:AssumeRole for the role in the destination account. This is a possible cause, because sts:AssumeRole is the API action that allows the Auditor to assume the cross-account role and obtain temporary credentials. The Auditor must have an IAM policy that allows them to call sts:AssumeRole for the role ARN in the destination account2.

F) The role ARN used by the Auditor is missing or incorrect. This is a possible cause, because the role ARN is the Amazon Resource Name of the cross-account role that the Auditor wants to assume. The role ARN must be valid and exist in the destination account3.

Question 8

Question Type: MultipleChoice

A company suspects that an attacker has exploited an overly permissive role to export credentials from Amazon EC2 instance metadat

a. The company uses Amazon GuardDuty and AWS Audit Manager. The company has enabled AWS CloudTrail logging and Amazon CloudWatch logging for all of its AWS accounts.

A security engineer must determine if the credentials were used to access the company's resources from an external account.

Which solution will provide this information?

Options:

A- Review GuardDuty findings to find InstanceCredentialExfiltration events.
B- Review assessment reports in the Audit Manager console to find InstanceCredentialExfiltration events.
C- Review CloudTrail logs for GetSessionToken API calls to AWS Security Token Service (AWS STS)

that come from an acount ID from outside the company.
D- Review CloudWatch logs for GetSessionToken API calls to AWS Security Token Service (AWS STS) that come from an account ID from outside the company.

Answer:

A

Explanation:

The correct answer is A because GuardDuty can detect and alert on EC2 instance credential exfiltration events.These events indicate that the credentials obtained from the EC2 instance metadata service are being used from an IP address that is owned by a different AWS account than the one that owns the instance1.GuardDuty can also provide details such as the source and destination IP addresses, the AWS account ID of the attacker, and the API calls made using the exfiltrated credentials2.

The other options are incorrect because they do not provide the information needed to determine if the credentials were used to access the company's resources from an external account. Option B is incorrect because Audit Manager does not generate InstanceCredentialExfiltration events.Audit Manager is a service that helps you continuously audit your AWS usage to simplify how you assess risk and compliance with regulations and industry standards3. Option C is incorrect because CloudTrail logs do not show the account ID of the caller for GetSessionToken API calls to AWS STS.CloudTrail logs show the account ID of the identity whose credentials were used to call the API4. Option D is incorrect because CloudWatch logs do not show the GetSessionToken API calls to AWS STS by default.CloudWatch logs can show the API calls made by AWS Lambda functions, Amazon API Gateway, and other AWS services that integrate with CloudWatch5.

Question 9

Question Type: MultipleChoice

A security engineer is designing a cloud architecture to support an application. The application runs on Amazon EC2 instances and processes sensitive information, including credit card numbers.

The application will send the credit card numbers to a component that is running in an isolated environment. The component will encrypt, store, and decrypt the numbers.

The component then will issue tokens to replace the numbers in other parts of the application.

The component of the application that manages the tokenization process will be deployed on a

separate set of EC2 instances. Other components of the application must not be able to store or access the credit card numbers.

Which solution will meet these requirements?

Options:

A- Use EC2 Dedicated Instances for the tokenization component of the application.
B- Place the EC2 instances that manage the tokenization process into a partition placement group.
C- Create a separate VPC. Deploy new EC2 instances into the separate VPC to support the data tokenization.
D- Deploy the tokenization code onto AWS Nitro Enclaves that are hosted on EC2 instances.

Answer:

D

Explanation:

AWS Nitro Enclaves are isolated and hardened virtual machines that run on EC2 instances and provide a secure environment for processing sensitive dat

a. Nitro Enclaves have no persistent storage, interactive access, or external networking, and they can only communicate with the parent instance through a secure local channel. Nitro Enclaves also support cryptographic attestation, which allows verifying the identity and integrity of the enclave and its code. Nitro Enclaves are ideal for implementing data protection solutions such as tokenization, encryption, and key management.

Using Nitro Enclaves for the tokenization component of the application meets the requirements of isolating the sensitive data from other parts of the application, encrypting and storing the credit card numbers securely, and issuing tokens to replace the numbers. Other components of the application will not be able to access or store the credit card numbers, as they are only available within the enclave.

Question 10

Question Type: MultipleChoice

A security engineer is designing an IAM policy to protect AWS API operations. The policy must enforce multi-factor authentication (MFA) for IAM users to access certain services in the AWS production account. Each session must remain valid for only 2 hours. The current version of the

IAM policy is as follows:

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "ec2:DescribeInstances",
            "ec2:StopInstances",
            "ec2:TerminateInstances"
        ],
        "Resource": ["*"]
    }]
}
```

Which combination of conditions must the security engineer add to the IAM policy to meet these requirements? (Select TWO.)

Options:

A- 'Bool ' : ' aws : Multi FactorAuthPresent': 'true' }
B- 'B001 ' : ' aws : MultiFactorAuthPresent': 'false' }
C- 'NumericLessThan' : { ' aws : Multi FactorAuthAge' : '7200'}
D- 'NumericGreaterThan' : { ' aws : MultiFactorAuthAge ' : '7200'
E- 'NumericLessThan' : { 'MaxSessionDuration ' : '7200'}

Answer:

A, C

Explanation:

The correct combination of conditions to add to the IAM policy is A and C: These conditions will ensure that IAM users must use MFA to access certain services in the AWS production account, and that each session will expire after 2 hours.

Option A: ''Bool'' : { ''aws:MultiFactorAuthPresent'' : ''true'' } is a valid condition that checks if the principal (the IAM user) has authenticated with MFA before making the request. This condition will enforce MFA for the IAM users to access the specified services. This condition key is supported by all AWS services that support IAM policies1.

Option B: ''Bool'' : { ''aws:MultiFactorAuthPresent'' : ''false'' } is the opposite of option

A) This condition will allow access only if the principal has not authenticated with MFA, which is not the desired requirement. This condition key is supported by all AWS services that support IAM policies1.

Option C: ''NumericLessThan'' : { ''aws:MultiFactorAuthAge'' : ''7200'' } is a valid condition that checks if the time since the principal authenticated with MFA is less than 7200 seconds (2 hours). This condition will enforce the session duration limit for the IAM users. This condition key is supported by all AWS services that support IAM policies1.

Option D: ''NumericGreaterThan'' : { ''aws:MultiFactorAuthAge'' : ''7200'' } is the opposite of option C) This condition will allow access only if the time since the principal authenticated with MFA is more than 7200 seconds (2 hours), which is not the desired requirement. This condition key is supported by all AWS services that support IAM policies1.

Option E: ''NumericLessThan'' : { ''MaxSessionDuration'' : ''7200'' } is not a valid condition key. MaxSessionDuration is a property of an IAM role, not a condition key. It specifies the maximum session duration (in seconds) for the role, which can be between 3600 and 43200 seconds (1 to 12 hours). This property can be set when creating or modifying a role, but it cannot be used as a condition in a policy2.

Question 11

Question Type: MultipleChoice

A company's data scientists want to create artificial intelligence and machine learning (AI/ML) training models by using Amazon SageMaker. The training models will use large datasets in an Amazon S3 bucket. The datasets contain sensitive information.

On average. the data scientists need 30 days to train models. The S3 bucket has been secured appropriately The companfs data retention policy states that all data that is older than 45 days must be removed from the S3 bucket.

Which action should a security engineer take to enforce this data retention policy?

Options:

A- Configure an S3 Lifecycle rule on the S3 bucket to delete objects after 45 days.
B- Create an AWS Lambda function to check the last-modified date of the S3 objects and delete objects that are older than 45 days. Create an S3 event notification to invoke the Lambda function for each PutObject operation.
C- Create an AWS Lambda function to check the last-modified date of the S3 objects and delete

objects that are older than 45 days. Create an Amazon EventBridge rule to invoke the Lambda function each month.
D- Configure S3 Intelligent-Ttering on the S3 bucket to automatically transition objects to another storage class.

Answer:

A

Explanation:

The correct answer is A. Configure an S3 Lifecycle rule on the S3 bucket to delete objects after 45 days.

The reason is that this is the simplest and most effective way to enforce the data retention policy. According to the AWS documentation1, ''To manage your objects so that they are stored cost effectively throughout their lifecycle, configure their Amazon S3 Lifecycle. An S3 Lifecycle configuration is a set of rules that define actions that Amazon S3 applies to a group of objects. There are two types of actions: Transition actions and Expiration actions.'' The documentation1 also states that ''Expiration actions define when objects expire. Amazon S3 deletes expired objects on your behalf.'' Therefore, by configuring an S3 Lifecycle rule on the S3 bucket to delete objects after 45 days, the security engineer can ensure that the data is removed from the S3 bucket according to the company's policy.

The other options are incorrect because:

B) Create an AWS Lambda function to check the last-modified date of the S3 objects and delete objects that are older than 45 days. Create an S3 event notification to invoke the Lambda function for each PutObject operation. This option is not optimal because it requires deploying and maintaining a Lambda function, which adds complexity and cost. Moreover, it does not guarantee that the data is deleted exactly after 45 days, since the Lambda function is triggered only when a new object is put into the S3 bucket. If there are no new objects for a long period of time, the Lambda function will not run and the data will not be deleted.

C) Create an AWS Lambda function to check the last-modified date of the S3 objects and delete objects that are older than 45 days. Create an Amazon EventBridge rule to invoke the Lambda function each month. This option is not optimal because it requires deploying and maintaining a Lambda function, which adds complexity and cost. Moreover, it does not guarantee that the data is deleted exactly after 45 days, since the Lambda function is triggered only once a month. If the data is older than 45 days but less than a month, it will not be deleted until the next month.

D) Configure S3 Intelligent-Tiering on the S3 bucket to automatically transition objects to another storage class. This option is not sufficient to enforce the data retention policy, because it does not delete the data from the S3 bucket. It only moves the data to a less expensive storage class based on access patterns. According to the AWS documentation2, ''S3 Intelligent-Tiering optimizes storage costs by automatically moving data between two access tiers, frequent access

and infrequent access, when access patterns change.'' However, this feature does not expire or delete the data after a certain period of time.

Question 12

Question Type: MultipleChoice

A company is running an application on Amazon EC2 instances in an Auto Scaling group. The application stores logs locally. A security engineer noticed that logs were lost after a scale-in event. The security engineer needs to recommend a solution to ensure the durability and availability of log data All logs must be kept for a minimum of 1 year for auditing purposes. What should the security engineer recommend?

Options:

A- Within the Auto Scaling lifecycle, add a hook to create and attach an Amazon Elastic Block Store (Amazon EBS) log volume each time an EC2 instance is created. When the instance is terminated, the EBS volume can be reattached to another instance for log review.
B- Create an Amazon Elastic File System (Amazon EFS) file system and add a command in the user data section of the Auto Scaling launch template to mount the EFS file system during EC2 instance creation. Configure a process on the instance to copy the logs once a day from an instance Amazon Elastic Block Store (Amazon EBS) volume to a directory in the EFS file system.
C- Add an Amazon CloudWatch agent into the AMI used in the Auto Scaling group. Configure the CloudWatch agent to send the logs to Amazon CloudWatch Logs for review,
D- Within the Auto Scaling lifecycle, add a lifecycle hook at the terminating state transition and alert the engineering team by using a lifecycle notification to Amazon Simple Notification Service (Amazon SNS). Configure the hook to remain in the Terminating:Wait state for 1 hour to allow manual review of the security logs prior to instance termination.

Answer:

C

Explanation:

Option C is the best solution to ensure the durability and availability of log data from EC2 instances in an Auto Scaling group. By using an Amazon CloudWatch agent, the logs can be sent to Amazon CloudWatch Logs, which is a fully managed service that can store, monitor, and analyze log dat

a. CloudWatch Logs also allows you to set retention policies for your log groups, so you can keep

the logs for a minimum of 1 year for auditing purposes.CloudWatch Logs also supports encryption, access control, and compliance features to protect your log data12

P2P exams

P2P exams

To Get Premium Files for SCS-C02 Visit
https://www.p2pexams.com/products/scs-c02

For More Free Questions Visit
https://www.p2pexams.com/amazon/pdf/scs-c02

