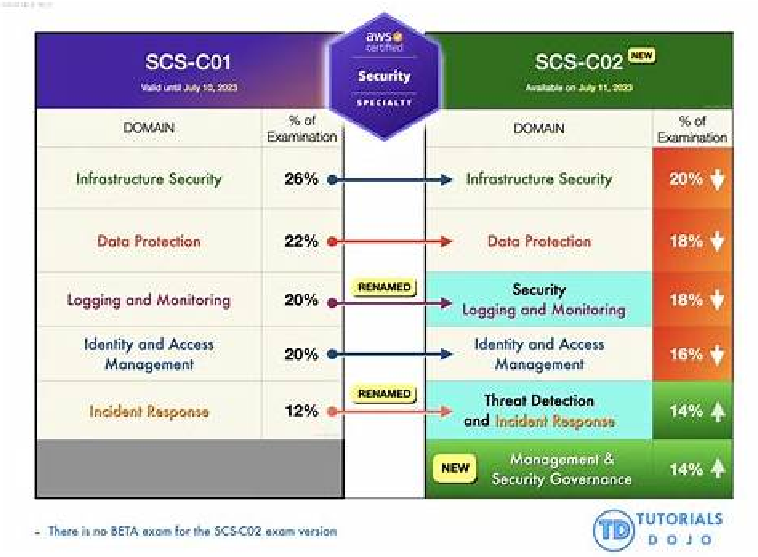
Reliable Test SCS-C02 Pdf & 100% Pass-rate Exam Dumps SCS-C02 Collection: AWS Certified Security - Specialty


aws certified
Security
SPECIALTY
TUTORIALS DOJO

SCS-C01 Valid until July 10, 2023			SCS-C02 NEW Available on July 11, 2023	
DOMAIN	% of Examination		DOMAIN	% of Examination
Infrastructure Security	26%		Infrastructure Security	20% ↓
Data Protection	22%		Data Protection	18% ↓
Logging and Monitoring	20%	RENAMED	Security Logging and Monitoring	18% ↓
Identity and Access Management	20%		Identity and Access Management	16% ↓
Incident Response	12%	RENAMED	Threat Detection and Incident Response	14% ↑
			NEW Management & Security Governance	14% ↑

- There is no BETA exam for the SCS-C02 exam version

P.S. Free & New SCS-C02 dumps are available on Google Drive shared by DumpsQuestion: https://drive.google.com/open?id=1dFo4kVAjuLglO8NGXeMW-_qYCbFX3hbF

Our SCS-C02 training materials are of high quality, and we also have free demo to help you know the content of the SCS-C02 exam dumps. Free update for 365 days after purchasing is available, and the update version will be sent to you timely. If you fail to pass the exam, we will return your money into the payment account. All we do is for your interest, and we also accept your suggestion and advice for SCS-C02 Training Materials.

Amazon SCS-C02 Exam Syllabus Topics:

Topic	Details
Topic 1	• Data Protection: AWS Security specialists learn to ensure data confidentiality and integrity for data in transit and at rest. Topics include lifecycle management of data at rest, credential protection, and cryptographic key management. These capabilities are central to managing sensitive data securely, reflecting the exam's focus on advanced data protection strategies.
Topic 2	• Identity and Access Management: The topic equips AWS Security specialists with skills to design, implement, and troubleshoot authentication and authorization mechanisms for AWS resources. By emphasizing secure identity management practices, this area addresses foundational competencies required for effective access control, a vital aspect of the certification exam.
Topic 3	• Threat Detection and Incident Response: In this topic, AWS Security specialists gain expertise in crafting incident response plans and detecting security threats and anomalies using AWS services. It delves into effective strategies for responding to compromised resources and workloads, ensuring readiness to manage security incidents. Mastering these concepts is critical for handling scenarios assessed in the SCS-C02 Exam.
Topic 4	• Infrastructure Security: Aspiring AWS Security specialists are trained to implement and troubleshoot security controls for edge services, networks, and compute workloads under this topic. Emphasis is placed on ensuring resilience and mitigating risks across AWS infrastructure. This section aligns closely with the exam's focus on safeguarding critical AWS services and environments.

Topic 5	- Management and Security Governance: This topic teaches AWS Security specialists to develop centralized strategies for AWS account management and secure resource deployment. It includes evaluating compliance and identifying security gaps through architectural reviews and cost analysis, essential for implementing governance aligned with certification standards.

>> Test SCS-C02 Pdf <<

Verified Test SCS-C02 Pdf | Amazing Pass Rate For SCS-C02: AWS Certified Security - Specialty | Correct Exam Dumps SCS-C02 Collection

Our SCS-C02 prep torrent boosts the highest standards of technical accuracy and only use certificated subject matter and experts. We provide the latest and accurate SCS-C02 exam torrent to the client and the questions and the answers we provide are based on the real exam. We can promise to you the passing rate is high and about 98%-100%. Our SCS-C02 Test Braindumps also boosts high hit rate and can stimulate the exam to let you have a good preparation for the SCS-C02 exam. Your success is bound with our SCS-C02 exam questions.

Amazon AWS Certified Security - Specialty Sample Questions (Q356-Q361):

NEW QUESTION # 356
A company needs to improve its ability to identify and prevent IAM policies that grant public access or cross-account access to resources. The company has implemented AWS Organizations and uses AWS IAM Access Analyzer. A security engineer must automate a response for newly created overly permissive policies to remediate access and notify the security team.
Select THREE:

- A. In Amazon EventBridge, create an event rule that matches active IAM Access Analyzer findings and invokes AWS Step Functions for resolution.
- B. Create an AWS Step Functions state machine that checks the resource type in the finding and adds an explicit Deny statement in the trust policy for the IAM role. Configure the state machine to publish a notification to an Amazon SNS topic.
- C. Create an Amazon SQS queue. Configure the queue to forward a notification to the security team that an external principal has been granted access to the specific IAM role and has been blocked.
- D. In Amazon CloudWatch, create a metric filter that matches active IAM Access Analyzer findings and invokes AWS Batch for resolution.
- E. Create an Amazon SNS topic for external or cross-account access notices. Subscribe the security team's email addresses to the topic.
- F. Create an AWS Batch job that forwards any resource type findings to an AWS Lambda function. Configure the Lambda function to add an explicit Deny statement in the trust policy for the IAM role. Configure the AWS Batch job to publish a notification to an Amazon SNS topic.

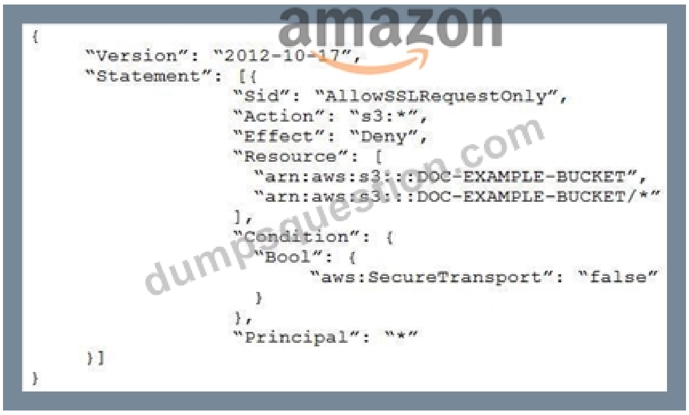
Answer: A,B,E

Explanation:
Comprehensive Detailed Explanation with all AWS Reference
To automate response to overly permissive IAM policies:
Step Functions State Machine (A):
Use Step Functions to orchestrate remediation by adding Deny statements to policies.
Publish findings to an SNS topic for notification.
Reference:
EventBridge Rule (C):
Use EventBridge to detect IAM Access Analyzer findings and trigger Step Functions.
Notification with SNS (F):
Use SNS to notify the security team when external or cross-account access is identified.
Incorrect Options:
B and D: AWS Batch is unnecessary; Step Functions is better suited for this orchestration.
E: SQS does not provide a direct notification mechanism; SNS is more appropriate.

NEW QUESTION # 357

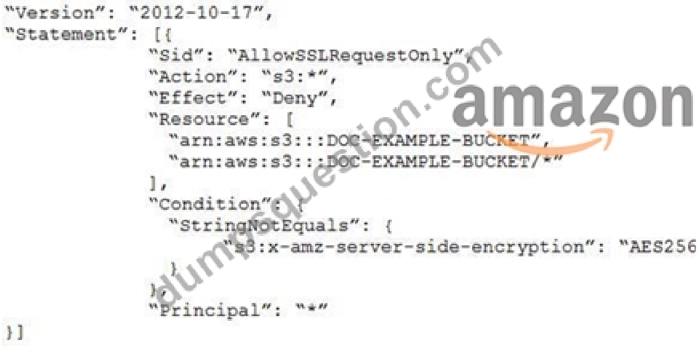
A company has a guideline that mandates the encryption of all Amazon S3 bucket data in transit. A security engineer must implement an S3 bucket policy that denies any S3 operations if data is not encrypted.
Which S3 bucket policy will meet this requirement?

- A.



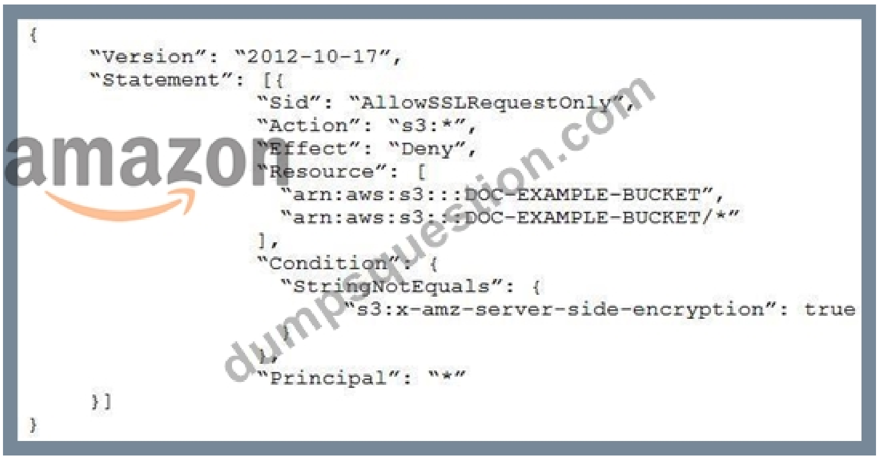
```
{
     "Version": "2012-10-17",
     "Statement": [{
                 "Sid": "AllowSSLRequestOnly",
                 "Action": "s3:*",
                 "Effect": "Deny",
                 "Resource": [
                   "arn:aws:s3:::DOC-EXAMPLE-BUCKET",
                   "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
                 ],
                 "Condition": {
                   "Bool": {
                        "aws:SecureTransport": "false"
                   }
                 },
                 "Principal": "*"
     }]
}
```

- B.



```
     "Version": "2012-10-17",
     "Statement": [{
                 "Sid": "AllowSSLRequestOnly",
                 "Action": "s3:*",
                 "Effect": "Deny",
                 "Resource": [
                   "arn:aws:s3:::DOC-EXAMPLE-BUCKET",
                   "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
                 ],
                 "Condition": {
                   "StringNotEquals": {
                     "s3:x-amz-server-side-encryption": "AES256
                   }
                 },
                 "Principal": "*"
     }]
```

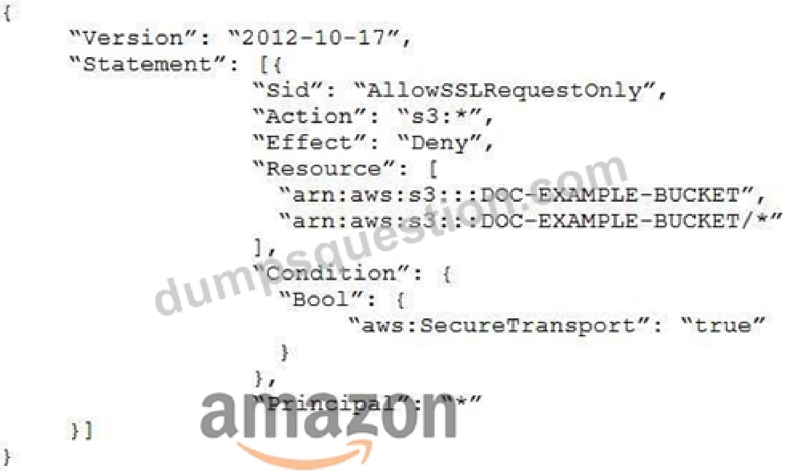
- C.



```
{
     "Version": "2012-10-17",
     "Statement": [{
                 "Sid": "AllowSSLRequestOnly",
                 "Action": "s3:*",
                 "Effect": "Deny",
                 "Resource": [
                   "arn:aws:s3:::DOC-EXAMPLE-BUCKET",
                   "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
                 ],
                 "Condition": {
                   "StringNotEquals": {
                     "s3:x-amz-server-side-encryption": true

                 },
                 "Principal": "*"
     }]
}
```

- D.



```
{
     "Version": "2012-10-17",
     "Statement": [{
                 "Sid": "AllowSSLRequestOnly",
                 "Action": "s3:*",
                 "Effect": "Deny",
                 "Resource": [
                   "arn:aws:s3:::DOC-EXAMPLE-BUCKET",
                   "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
                 ],
                 "Condition": {
                   "Bool": {
                        "aws:SecureTransport": "true"
                   }
                 },
                 "Principal": "*"
     }]
}
```

Answer: A

Explanation:

https://aws.amazon.com/blogs/security/how-to-use-bucket-policies-and-apply-defense-in-depth-to-help-secure-your-amazon-s3-data/

NEW QUESTION # 358
Which of the following are valid configurations for using SSL certificates with Amazon CloudFront? (Select THREE)

- A. Default CloudFront certificate
- B. Custom SSL certificate stored in AWS KMS
- C. Custom SSL certificate stored in AWS IAM
- D. Default SSL certificate stored in AWS Secrets Manager
- E. Custom SSL certificate stored in AWS Certificate Manager
- F. Default AWS Certificate Manager certificate

Answer: A,B,F

Explanation:
The key length for an RSA certificate that you use with CloudFront is 2048 bits, even though ACM supports larger keys. If you use an imported certificate with CloudFront, your key length must be 1024 or 2048 bits and cannot exceed 2048 bits. You must import the certificate in the US East (N. Virginia) Region. You must have permission to use and import the SSL/TLS certificate
https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/cnames-and-https-requirements.html

NEW QUESTION # 359
An international company has established a new business entity in South Korea. The company also has established a new AWS account to contain the workload for the South Korean region. The company has set up the workload in the new account in the ap-northeast-2 Region. The workload consists of three Auto Scaling groups of Amazon EC2 instances. All workloads that operate in this Region must keep system logs and application logs for 7 years.
A security engineer must implement a solution to ensure that no logging data is lost for each instance during scaling activities. The solution also must keep the logs for only the required period of 7 years.
Which combination of steps should the security engineer take to meet these requirements? (Choose three.)

- A. Configure an Amazon S3 Lifecycle policy on the target S3 bucket to expire objects after 7 years.
- B. Set the log retention for desired log groups to 7 years.
- C. Attach an IAM role to the launch configuration or launch template that the Auto Scaling groups use. Configure the role to provide the necessary permissions to forward logs to Amazon S3.
- D. Attach an IAM role to the launch configuration or launch template that the Auto Scaling groups use. Configure the role to provide the necessary permissions to forward logs to Amazon CloudWatch Logs.
- E. Ensure that the Amazon CloudWatch agent is installed on all the EC2 instances that the Auto Scaling groups launch. Generate a CloudWatch agent configuration file to forward the required logs to Amazon CloudWatch Logs.
- F. Ensure that a log forwarding application is installed on all the EC2 instances that the Auto Scaling groups launch. Configure the log forwarding application to periodically bundle the logs and forward the logs to Amazon S3.

Answer: B,D,E

Explanation:
The correct combination of steps that the security engineer should take to meet these requirements are A.
Ensure that the Amazon CloudWatch agent is installed on all the EC2 instances that the Auto Scaling groups launch. Generate a CloudWatch agent configuration file to forward the required logs to Amazon CloudWatch Logs., B. Set the log retention for desired log groups to 7 years., and C. Attach an IAM role to the launch configuration or launch template that the Auto Scaling groups use. Configure the role to provide the necessary permissions to forward logs to Amazon CloudWatch Logs.
A: This answer is correct because it meets the requirement of ensuring that no logging data is lost for each instance during scaling activities. By installing the CloudWatch agent on all the EC2 instances, the security engineer can collect and send system logs and application logs to CloudWatch Logs, which is a service that stores and monitors log data. By generating a CloudWatch agent configuration file, the security engineer can specify which logs to forward and how often.
B: This answer is correct because it meets the requirement of keeping the logs for only the required period of
7 years. By setting the log retention for desired log groups, the security engineer can control how long CloudWatch Logs retains log events before deleting them. The security engineer can choose a predefined retention period of 7 years, or use a custom value.
C: This answer is correct because it meets the requirement of providing the necessary permissions to forward logs to CloudWatch Logs. By attaching an IAM role to the launch configuration or launch template that the Auto Scaling groups use, the security engineer can grant permissions to the EC2 instances that are launched by the Auto Scaling groups. By configuring the role to provide the

necessary permissions, such as cloudwatch:
PutLogEvents and cloudwatch:CreateLogStream, the security engineer can allow the EC2 instances to send log data to CloudWatch Logs.

NEW QUESTION # 360

A company has several petabytes of data. The company must preserve this data for 7 years to comply with regulatory requirements. The company's compliance team asks a security officer to develop a strategy that will prevent anyone from changing or deleting the data.
Which solution will meet this requirement MOST cost-effectively?

- A. Create an Amazon S3 bucket. Configure the bucket to use S3 Object Lock in governance mode. Upload the data to the bucket. Create a user-based IAM policy that meets all the regulatory requirements.
- B. Create an Amazon S3 bucket. Upload the data to the bucket. Use a lifecycle rule to transition the data to a vault in S3 Glacier. Create a Vault Lock policy that meets all the regulatory requirements.
- C. Create an Amazon S3 bucket. Configure the bucket to use S3 Object Lock in compliance mode. Upload the data to the bucket. Create a resource-based bucket policy that meets all the regulatory requirements.
- D. Create a vault in Amazon S3 Glacier. Create a Vault Lock policy in S3 Glacier that meets all the regulatory requirements. Upload the data to the vault.

Answer: D

Explanation:
To preserve the data for 7 years and prevent anyone from changing or deleting it, the security officer needs to use a service that can store the data securely and enforce compliance controls. The most cost-effective way to do this is to use Amazon S3 Glacier, which is a low-cost storage service for data archiving and long-term backup. S3 Glacier allows you to create a vault, which is a container for storing archives. Archives are any data such as photos, videos, or documents that you want to store durably and reliably.
S3 Glacier also offers a feature called Vault Lock, which helps you to easily deploy and enforce compliance controls for individual vaults with a Vault Lock policy. You can specify controls such as "write once read many" (WORM) in a Vault Lock policy and lock the policy from future edits. Once a Vault Lock policy is locked, the policy can no longer be changed or deleted. S3 Glacier enforces the controls set in the Vault Lock policy to help achieve your compliance objectives. For example, you can use Vault Lock policies to enforce data retention by denying deletes for a specified period of time.
To use S3 Glacier and Vault Lock, the security officer needs to follow these steps:
* Create a vault in S3 Glacier using the AWS Management Console, AWS Command Line Interface (AWS CLI), or AWS SDKs.
* Create a Vault Lock policy in S3 Glacier that meets all the regulatory requirements using the IAM policy language. The policy can include conditions such as aws:CurrentTime or aws:SecureTransport to further restrict access to the vault.
* Initiate the lock by attaching the Vault Lock policy to the vault, which sets the lock to an in-progress state and returns a lock ID. While the policy is in the in-progress state, you have 24 hours to validate your Vault Lock policy before the lock ID expires. To prevent your vault from exiting the in-progress state, you must complete the Vault Lock process within these 24 hours. Otherwise, your Vault Lock policy will be deleted.
* Use the lock ID to complete the lock process. If the Vault Lock policy doesn't work as expected, you can stop the Vault Lock process and restart from the beginning.
* Upload the data to the vault using either direct upload or multipart upload methods.
For more information about S3 Glacier and Vault Lock, see S3 Glacier Vault Lock.
The other options are incorrect because:
* Option A is incorrect because creating an Amazon S3 bucket and configuring it to use S3 Object Lock in compliance mode will not prevent anyone from changing or deleting the data. S3 Object Lock is a feature that allows you to store objects using a WORM model in S3. You can apply two types of object locks: retention periods and legal holds. A retention period specifies a fixed period of time during which an object remains locked. A legal hold is an indefinite lock on an object until it is removed. However, S3 Object Lock only prevents objects from being overwritten or deleted by any user, including the root user in your AWS account. It does not prevent objects from being modified by other means, such as changing their metadata or encryption settings. Moreover, S3 Object Lock requires that you enable versioning on your bucket, which will incur additional storage costs for storing multiple versions of an object.
* Option B is incorrect because creating an Amazon S3 bucket and configuring it to use S3 Object Lock in governance mode will not prevent anyone from changing or deleting the data. S3 Object Lock in governance mode works similarly to compliance mode, except that users with specific IAM permissions can change or delete objects that are locked. This means that users who have s3:BypassGovernanceRetention permission can remove retention periods or legal holds from objects and overwrite or delete them before they expire. This option does not provide strong enforcement for compliance controls as required by the regulatory requirements.
* Option D is incorrect because creating an Amazon S3 bucket and using a lifecycle rule to transition the data to a vault in S3 Glacier will not prevent anyone from changing or deleting the data. Lifecycle rules are actions that Amazon S3 automatically

performs on objects during their lifetime. You can use lifecycle rules to transition objects between storage classes or expire them after a certain period of time.
However, lifecycle rules do not apply any compliance controls on objects or prevent them from being modified or deleted by users. Moreover, transitioning objects from S3 to S3 Glacier using lifecycle rules will incur additional charges for retrieval requests and data transfers.

NEW QUESTION # 361
......

Our website is a worldwide dumps leader that offers free valid SCS-C02 braindumps for certification tests, especially for Amazon practice test. We focus on the study of SCS-C02 real exam for many years and enjoy a high reputation in IT field by latest study materials, updated information and, most importantly, SCS-C02 Top Questions with detailed answers and explanations.

Exam Dumps SCS-C02 Collection: https://www.dumpsquestion.com/SCS-C02-exam-dumps-collection.html

- SCS-C02 New Learning Materials □ Practice SCS-C02 Questions □ SCS-C02 Preparation Store □ Open website “ www.practicevce.com ” and search for ➠ SCS-C02 □ for free download □SCS-C02 Exam Simulator Free
- Most Recent Amazon SCS-C02 Questions For Effective Future Profession [2026] □ Search for ➠ SCS-C02 □ and download it for free immediately on 「 www.pdfvce.com 」 □SCS-C02 Exam Study Guide
- 100% Pass Amazon - SCS-C02 - AWS Certified Security - Specialty Updated Test Pdf □ Easily obtain free download of “ SCS-C02 ” by searching on 《 www.examcollectionpass.com 》 ❤□Reliable SCS-C02 Test Review
- SCS-C02 Exam Assessment □ SCS-C02 Exam Assessment □ Reliable SCS-C02 Test Review □ Enter 「 www.pdfvce.com 」 and search for 「 SCS-C02 」 to download for free □SCS-C02 Cert Guide
- Quiz 2026 Trustable Amazon SCS-C02: Test AWS Certified Security - Specialty Pdf □ Copy URL “ www.easy4engine.com ” open and search for ✔ SCS-C02 □✔□ to download for free □Practice SCS-C02 Questions
- Latest SCS-C02 Exam Dumps Quiz Prep and preparation materials - Pdfvce □ Easily obtain free download of □ SCS-C02 □ by searching on { www.pdfvce.com } □SCS-C02 Passed
- Practice SCS-C02 Questions □ SCS-C02 Exam Simulator Free □ SCS-C02 Cert Guide □ Simply search for □ SCS-C02 □ for free download on ➽ www.prepawaypdf.com □ □Valid SCS-C02 Vce Dumps
- Free PDF 2026 Amazon SCS-C02 Accurate Test Pdf □ Easily obtain free download of “ SCS-C02 ” by searching on 《 www.pdfvce.com 》 □SCS-C02 Exam Assessment
- SCS-C02 Preparation Store □ Reliable SCS-C02 Braindumps Ebook □ Reliable SCS-C02 Test Topics □ The page for free download of [SCS-C02] on ✔ www.vce4dumps.com □✔□ will open immediately □SCS-C02 New Learning Materials
- SCS-C02 Passed □ Reliable SCS-C02 Braindumps Ebook □ SCS-C02 New Learning Materials □ Search for ▹ SCS-C02 ◃ and download exam materials for free through { www.pdfvce.com } □SCS-C02 Exam Assessment
- Amazon - Authoritative Test SCS-C02 Pdf □ Download 【 SCS-C02 】 for free by simply entering ☀ www.dumpsquestion.com □☀□ website □Valid SCS-C02 Vce Dumps
- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, ilmannafiya.org, myportal.utt.edu.tt, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, Disposable vapes

BTW, DOWNLOAD part of DumpsQuestion SCS-C02 dumps from Cloud Storage: https://drive.google.com/open?id=1dFo4kVAjuLglO8NGXeMW-_qYCbFX3hbF