PRACTICE TEST SOFTWARE

Amazon

SCS-C03 Exam

AWS Certified Security - Specialty

DEMO Version

Full Version Features:

• 90 Days Free Updates

• 30 Days Money Back Guarantee

• Instant Download Once Purchased

• 24 Hours Live Chat Support

Full version is available at link below with affordable price.

https://www.practicetestsoftware.com/amazon/scs-c03

Question 1. (HOTSPOT)

A security engineer needs to implement AWS IAM Identity Center with an external identity provider (IdP).

Select and order the correct steps from the following list to meet this requirement. Select each step one time or not at all. (Select and order THREE.)

. Configure the external IdP as the identity source in IAM Identity Center.

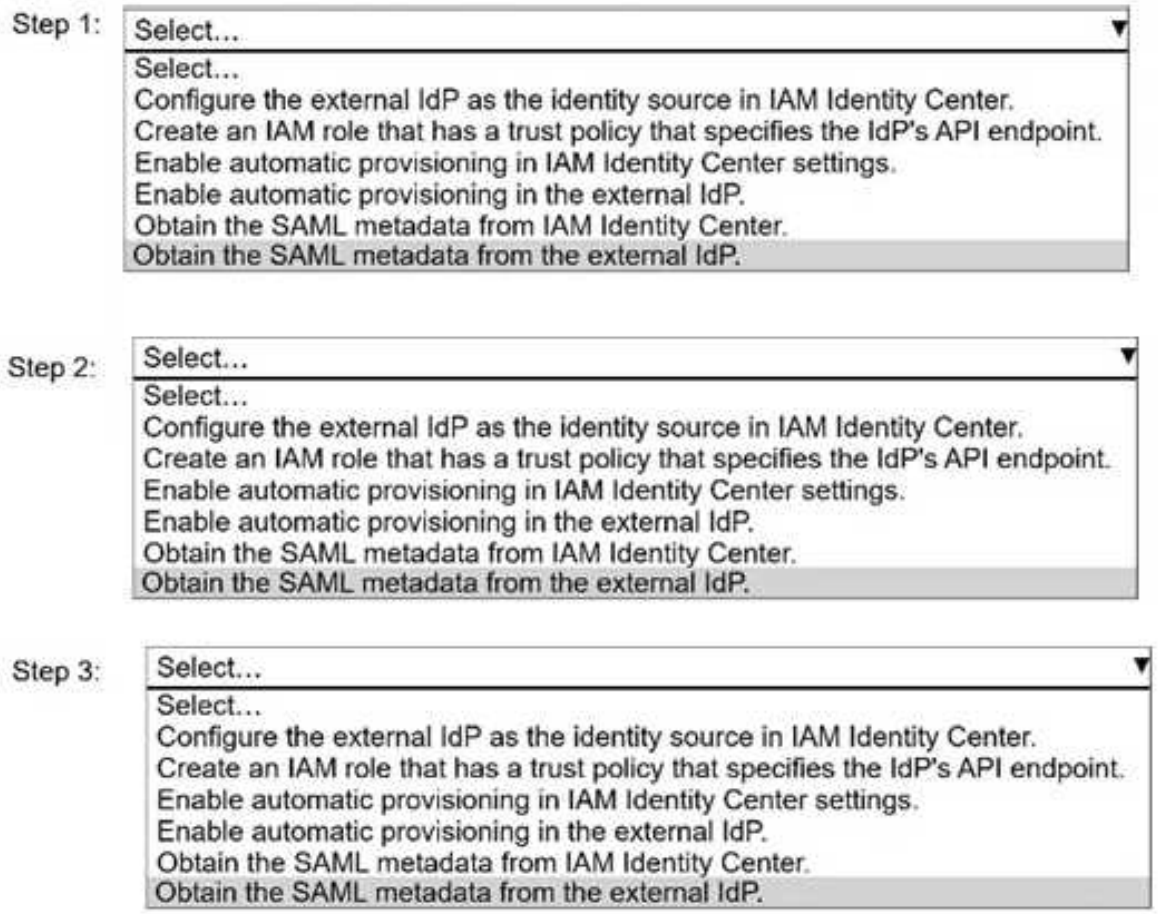
. Create an IAM role that has a trust policy that specifies the IdP's API endpoint.

. Enable automatic provisioning in IAM Identity Center settings.

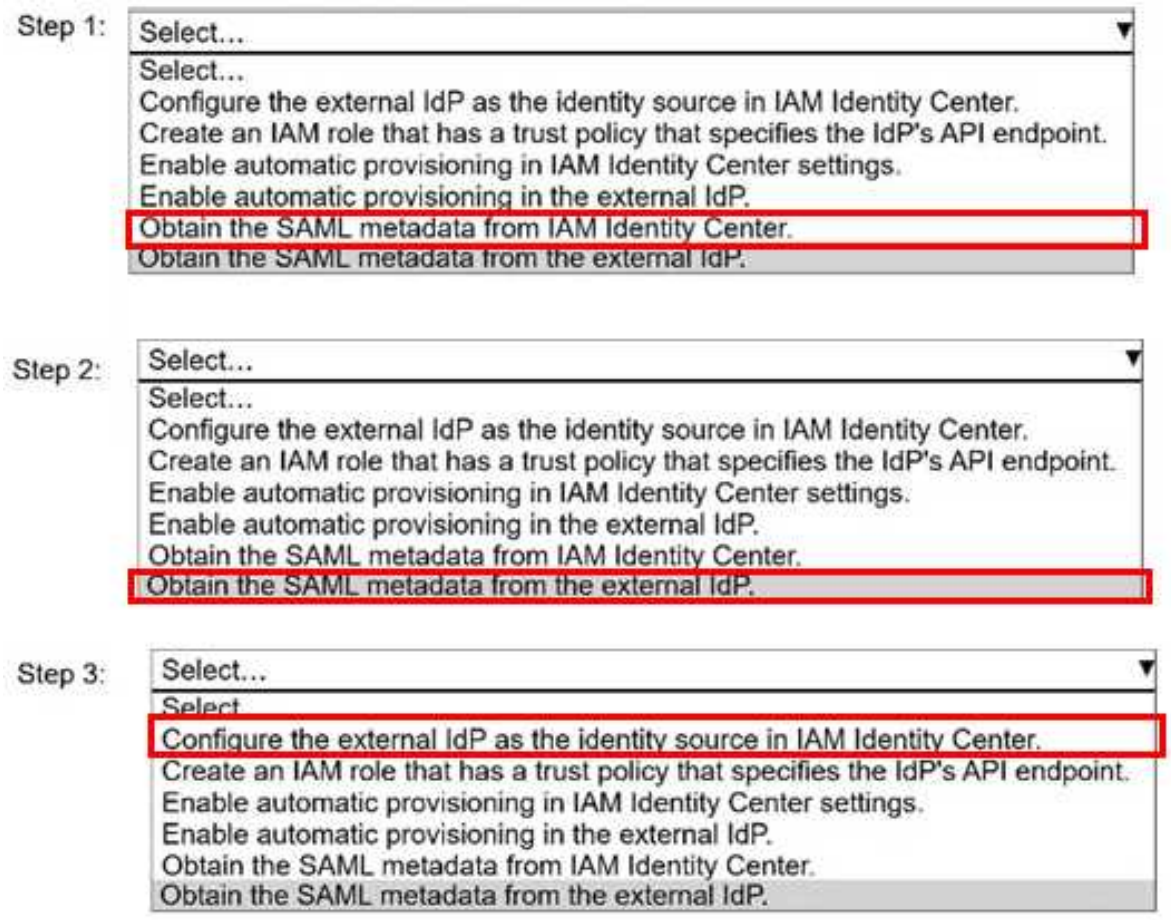
. Enable automatic provisioning in the external IdP.

. Obtain the SAML metadata from IAM Identity Center.

. Obtain the SAML metadata from the external IdP.



Correct Answer:



Question 2. (Single Select)

A security administrator is setting up a new AWS account. The security administrator wants to secure the data that a company stores in an Amazon S3 bucket. The security administrator also wants to reduce the chance of unintended data exposure and the potential for misconfiguration of objects that are in the S3 bucket.

Which solution will meet these requirements with the LEAST operational overhead?

A: Configure the S3 Block Public Access feature for the AWS account.
B: Configure the S3 Block Public Access feature for all objects that are in the bucket.
C: Deactivate ACLs for objects that are in the bucket.
D: Use AWS PrivateLink for Amazon S3 to access the bucket.

Correct Answer: A

Explanation:

Amazon S3 Block Public Access configured at the AWS account level is the recommended and most effective approach to protect data stored in Amazon S3 while minimizing operational overhead. AWS Security Specialty documentation explains that S3 Block Public Access provides centralized, preventative controls designed to block public access to S3 buckets and objects regardless of individual bucket policies or object-level ACL configurations. When enabled at the account level, these controls automatically apply to all existing and newly created buckets, significantly reducing the risk of accidental exposure caused by misconfigured permissions.

The AWS Certified Security – Specialty Study Guide emphasizes that public access misconfiguration is a leading cause of data leaks in cloud environments. Account-level S3 Block Public Access acts as a guardrail by overriding any attempt to grant public permissions through bucket policies or ACLs. This eliminates the need to manage security settings on a per-bucket or per-object basis, thereby reducing administrative complexity and human error.

Configuring Block Public Access at the object level, as in option B, requires continuous monitoring and manual configuration, which increases operational overhead. Disabling ACLs alone, as described in option C, does not fully prevent public access because bucket policies can still allow public permissions. Using AWS PrivateLink, as in option D, controls network access but does not protect against public exposure through misconfigured S3 policies.

AWS security best practices explicitly recommend enabling S3 Block Public Access at the account level as the primary mechanism for preventing unintended public data exposure with minimal management effort.

Referenced AWS Specialty Documents:

AWS Certified Security – Specialty Official Study Guide

Amazon S3 Security Best Practices Documentation

Amazon S3 Block Public Access Overview

AWS Well-Architected Framework – Security Pillar

Question 3. (Multi Select)

A company is attempting to conduct forensic analysis on an Amazon EC2 instance, but the company is unable to connect to the instance by using AWS Systems Manager Session Manager. The company has installed AWS Systems Manager Agent (SSM Agent) on the EC2 instance.

The EC2 instance is in a subnet in a VPC that does not have an internet gateway attached. The company

has associated a security group with the EC2 instance. The security group does not have inbound or outbound rules. The subnet's network ACL allows all inbound and outbound traffic.

Which combination of actions will allow the company to conduct forensic analysis on the EC2 instance without compromising forensic data? (Select THREE.)

A: Update the EC2 instance security group to add a rule that allows outbound traffic on port 443 for 0.0.0.0/0.
B: Update the EC2 instance security group to add a rule that allows inbound traffic on port 443 to the VPC's CIDR range.
C: Create an EC2 key pair. Associate the key pair with the EC2 instance.
D: Create a VPC interface endpoint for Systems Manager in the VPC where the EC2 instance is located.
E: Attach a security group to the VPC interface endpoint. Allow inbound traffic on port 443 to the VPC's CIDR range.
F: Create a VPC interface endpoint for the EC2 instance in the VPC where the EC2 instance is located.

Correct Answer: A, D, E

Explanation:
AWS Systems Manager Session Manager requires secure outbound HTTPS connectivity from the EC2 instance to Systems Manager endpoints. In a VPC without internet access, AWS Certified Security – Specialty documentation recommends using interface VPC endpoints to enable private connectivity without exposing the instance to the internet.
Creating a VPC interface endpoint for Systems Manager allows the SSM Agent to communicate securely with the Systems Manager service. The endpoint must have an attached security group that allows inbound traffic on port 443 from the VPC CIDR range. Additionally, the EC2 instance security group must allow outbound HTTPS traffic on port 443 so the agent can initiate connections.
Option C is incorrect because creating or associating key pairs enables SSH access, which can alter forensic evidence and violates forensic best practices. Option B is unnecessary because Session Manager does not require inbound rules on the EC2 instance. Option F is invalid because EC2 does not use interface endpoints for management connectivity.
This combination ensures secure, private access for forensic investigation while preserving evidence integrity and adhering to AWS incident response best practices.
Referenced AWS Specialty Documents:
AWS Certified Security – Specialty Official Study Guide
AWS Systems Manager Session Manager Architecture
AWS Incident Response and Forensics Best Practices

Question 4. (Single Select)

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 principals. Revert this change when the application team no longer needs access.
C: Create a key grant to allow the application team to use the KMS keys. Revoke the grant when the application team no longer needs access.
D: Create a new KMS key by generating key material on premises. Import the key material to AWS KMS whenever the application team needs access. Grant the application team permissions to use the key.

Correct Answer: C

Explanation:
AWS KMS key grants are specifically designed to provide temporary, granular permissions to use customer managed keys without modifying key policies. According to the AWS Certified Security – Specialty Study Guide, grants are the preferred mechanism for delegating key usage permissions to AWS principals for short-term or programmatic access scenarios. Grants allow permissions such as Encrypt, Decrypt, or GenerateDataKey and can be created and revoked dynamically.
Using a key grant avoids the operational risk and overhead of editing key policies, which are long-term control mechanisms and should remain stable. AWS documentation emphasizes that frequent key policy changes increase the risk of misconfiguration and accidental privilege escalation. Grants can be revoked immediately when access is no longer required, ensuring strong adherence to the principle of least privilege.
Options A and D violate AWS security best practices because AWS KMS does not allow direct export of key material unless the key was explicitly created as an importable key, and exporting key material increases exposure risk. Option B requires manual policy changes and rollback, which introduces operational overhead and audit complexity.
AWS recommends key grants as the most efficient and secure way to provide temporary access to KMS

keys for applications.
Referenced AWS Specialty Documents:
AWS Certified Security – Specialty Official Study Guide
AWS KMS Key Policies and Grants Documentation
AWS KMS Best Practices

Question 5. (Single Select)

A company is using AWS CloudTrail and Amazon CloudWatch to monitor resources in an AWS account. The company's developers have been using an IAM role in the account for the last 3 months.

A security engineer needs to refine the customer managed IAM policy attached to the role to ensure that the role provides least privilege access.

Which solution will meet this requirement with the LEAST effort?

A: Implement AWS IAM Access Analyzer policy generation on the role.
B: Implement AWS IAM Access Analyzer policy validation on the role.
C: Search CloudWatch logs to determine the actions the role invoked and to evaluate the permissions.
D: Use AWS Trusted Advisor to compare the policies assigned to the role against AWS best practices.

Correct Answer: A

Explanation:
AWS IAM Access Analyzer policy generation is specifically designed to help security engineers generate least-privilege IAM policies based on actual usage recorded in AWS CloudTrail. According to the AWS Certified Security – Specialty documentation, policy generation analyzes historical CloudTrail data to identify the exact API actions and resources that a role has accessed over a specified time period. Because the role has been actively used for three months, there is sufficient CloudTrail data for IAM Access Analyzer to generate a refined customer managed policy automatically. This significantly reduces manual effort and eliminates the need to analyze logs or infer permissions. The generated policy can be reviewed and attached directly to the role, ensuring least privilege access with minimal engineering effort.
Option B only validates existing policies for security warnings and does not reduce permissions. Option C requires manual analysis of CloudWatch logs, which is time-consuming and error-prone. Option D does not analyze real usage and cannot generate role-specific least privilege policies.
AWS documentation explicitly recommends IAM Access Analyzer policy generation as the fastest and most accurate method to refine IAM permissions based on observed behavior.

Referenced AWS Specialty Documents:

AWS Certified Security – Specialty Official Study Guide

AWS IAM Access Analyzer Policy Generation

AWS IAM Least Privilege Best Practices

Full version is available at link below with affordable price.

https://www.practicetestsoftware.com/amazon/scs-c03

40% Discount Coupon Code: GET40