aws training and certification

AWS Certified Security – Specialty (SCS-C01) Exam Guide

Introduction

The AWS Certified Security – Specialty (SCS-C01) exam is intended for individuals who perform a security role. The exam validates a candidate's ability to effectively demonstrate knowledge about securing the AWS platform.

The exam also validates whether a candidate has the following:

- An understanding of specialized data classifications and AWS data protection mechanisms
- An understanding of data-encryption methods and AWS mechanisms to implement them
- An understanding of secure internet protocols and AWS mechanisms to implement them
- A working knowledge of AWS security services and features of services to provide a secure production environment
- Competency from 2 or more years of production deployment experience in using AWS security services and features
- The ability to make tradeoff decisions with regard to cost, security, and deployment complexity to meet a set of application requirements
- An understanding of security operations and risks

Target candidate description

The target candidate should have 5 years of IT security experience in designing and implementing security solutions. Additionally, the target candidate should have 2 or more years of hands-on experience in securing AWS workloads.

Recommended AWS knowledge

The target candidate should have the following knowledge:

- The AWS shared responsibility model and its application
- Security controls for workloads on AWS
- Logging and monitoring strategies
- Cloud security threat models
- Patch management and security automation
- Ways to enhance AWS security services with third-party tools and services
- Disaster recovery controls, including BCP and backups
- Encryption
- Access control
- Data retention

What is considered out of scope for the target candidate?

The following is a non-exhaustive list of related job tasks that the target candidate is not expected to be able to perform. These items are considered out of scope for the exam:

- Create or write configurations
- Implement (SysOps)
- Demonstrate scripting in a specific language (for example, Perl or Java)

For a detailed list of specific tools and technologies that might be covered on the exam, as well as lists of in-scope and out-of-scope AWS services, refer to the Appendix.

Exam content

Response types

There are two types of questions on the exam:

- **Multiple choice:** Has one correct response and three incorrect responses (distractors)
- **Multiple response:** Has two or more correct responses out of five or more response options

Select one or more responses that best complete the statement or answer the question. Distractors, or incorrect answers, are response options that a candidate with incomplete knowledge or skill might choose. Distractors are generally plausible responses that match the content area.

Unanswered questions are scored as incorrect; there is no penalty for guessing. The exam includes 50 questions that will affect your score.

Unscored content

The exam includes 15 unscored questions that do not affect your score. AWS collects information about candidate performance on these unscored questions to evaluate these questions for future use as scored questions. These unscored questions are not identified on the exam.

Exam results

The AWS Certified Security – Specialty (SCS-C01) exam is a pass or fail exam. The exam is scored against a minimum standard established by AWS professionals who follow certification industry best practices and guidelines.

Your results for the exam are reported as a scaled score of 100–1,000. The minimum passing score is 750. Your score shows how you performed on the exam as a whole and whether or not you passed. Scaled scoring models help equate scores across multiple exam forms that might have slightly different difficulty levels.

Your score report could contain a table of classifications of your performance at each section level. This information is intended to provide general feedback about your exam performance. The exam uses a compensatory scoring model, which means that you do not need to achieve a passing score in each section. You need to pass only the overall exam.

Each section of the exam has a specific weighting, so some sections have more questions than other sections have. The table contains general information that highlights your strengths and weaknesses. Use caution when interpreting section-level feedback.

Content outline

This exam guide includes weightings, test domains, and objectives for the exam. It is not a comprehensive listing of the content on the exam. However, additional context for each of the objectives is available to help guide your preparation for the exam. The following table lists the main content domains and their weightings. The table precedes the complete exam content outline, which includes the additional context. The percentage in each domain represents only scored content.

Domain	% of Exam
Domain 1: Incident Response	12%
Domain 2: Logging and Monitoring	20%
Domain 3: Infrastructure Security	26%
Domain 4: Identity and Access Management	20%
Domain 5: Data Protection	22%
TOTAL	**100%**

Domain 1: Incident Response

1.1 Given an AWS abuse notice, evaluate the suspected compromised instance or exposed access keys.

- Given an AWS Abuse report about an EC2 instance, securely isolate the instance as part of a forensic investigation.
- Analyze logs relevant to a reported instance to verify a breach, and collect relevant data.
- Capture a memory dump from a suspected instance for later deep analysis or for legal compliance reasons.

1.2 Verify that the Incident Response plan includes relevant AWS services.

- Determine if changes to baseline security configuration have been made.
- Determine if list omits services, processes, or procedures which facilitate Incident Response.
- Recommend services, processes, procedures to remediate gaps.

1.3 Evaluate the configuration of automated alerting, and execute possible remediation of security-related incidents and emerging issues.

- Automate evaluation of conformance with rules for new/changed/removed resources.
- Apply rule-based alerts for common infrastructure misconfigurations.
- Review previous security incidents and recommend improvements to existing systems.

Domain 2: Logging and Monitoring

2.1 Design and implement security monitoring and alerting.

- Analyze architecture and identify monitoring requirements and sources for monitoring statistics.
- Analyze architecture to determine which AWS services can be used to automate monitoring and alerting.
- Analyze the requirements for custom application monitoring, and determine how this could be achieved.
- Set up automated tools/scripts to perform regular audits.

2.2 Troubleshoot security monitoring and alerting.

- Given an occurrence of a known event without the expected alerting, analyze the service functionality and configuration and remediate.
- Given an occurrence of a known event without the expected alerting, analyze the permissions and remediate.
- Given a custom application which is not reporting its statistics, analyze the configuration and remediate.
- Review audit trails of system and user activity.

2.3 Design and implement a logging solution.

- Analyze architecture and identify logging requirements and sources for log ingestion.
- Analyze requirements and implement durable and secure log storage according to AWS best practices.
- Analyze architecture to determine which AWS services can be used to automate log ingestion and analysis.

2.4 Troubleshoot logging solutions.

- Given the absence of logs, determine the incorrect configuration and define remediation steps.
- Analyze logging access permissions to determine incorrect configuration and define remediation steps.
- Based on the security policy requirements, determine the correct log level, type, and sources.

Domain 3: Infrastructure Security

3.1 Design edge security on AWS.

- For a given workload, assess and limit the attack surface.
- Reduce blast radius (e.g. by distributing applications across accounts and regions).
- Choose appropriate AWS and/or third-party edge services such as WAF, CloudFront and Route 53 to protect against DDoS or filter application-level attacks.
- Given a set of edge protection requirements for an application, evaluate the mechanisms to prevent and detect intrusions for compliance and recommend required changes.
- Test WAF rules to ensure they block malicious traffic.

3.2 Design and implement a secure network infrastructure.

- Disable any unnecessary network ports and protocols.
- Given a set of edge protection requirements, evaluate the security groups and NACLs of an application for compliance and recommend required changes.
- Given security requirements, decide on network segmentation (e.g. security groups and NACLs) that allow the minimum ingress/egress access required.
- Determine the use case for VPN or Direct Connect.
- Determine the use case for enabling VPC Flow Logs.
- Given a description of the network infrastructure for a VPC, analyze the use of subnets and gateways for secure operation.

3.3 Troubleshoot a secure network infrastructure.

- Determine where network traffic flow is being denied.
- Given a configuration, confirm security groups and NACLs have been implemented correctly.

3.4 Design and implement host-based security.

- Given security requirements, install and configure host-based protections including Inspector, SSM.
- Decide when to use host-based firewall like iptables.
- Recommend methods for host hardening and monitoring.

Domain 4: Identity and Access Management

4.1 Design and implement a scalable authorization and authentication system to access AWS resources.

- Given a description of a workload, analyze the access control configuration for AWS services and make recommendations that reduce risk.
- Given a description how an organization manages their AWS accounts, verify security of their root user.
- Given your organization's compliance requirements, determine when to apply user policies and resource policies.
- Within an organization's policy, determine when to federate a directory services to IAM.
- Design a scalable authorization model that includes users, groups, roles, and policies.
- Identify and restrict individual users of data and AWS resources.
- Review policies to establish that users/systems are restricted from performing functions beyond their responsibility, and also enforce proper separation of duties.

4.2 Troubleshoot an authorization and authentication system to access AWS resources.

- Investigate a user's inability to access S3 bucket contents.
- Investigate a user's inability to switch roles to a different account.
- Investigate an Amazon EC2 instance's inability to access a given AWS resource.

Domain 5: Data Protection

5.1 Design and implement key management and use.

- Analyze a given scenario to determine an appropriate key management solution.
- Given a set of data protection requirements, evaluate key usage and recommend required changes.
- Determine and control the blast radius of a key compromise event and design a solution to contain the same.

5.2 Troubleshoot key management.

- Break down the difference between a KMS key grant and IAM policy.
- Deduce the precedence given different conflicting policies for a given key.
- Determine when and how to revoke permissions for a user or service in the event of a compromise.

5.3 Design and implement a data encryption solution for data at rest and data in transit.

- Given a set of data protection requirements, evaluate the security of the data at rest in a workload and recommend required changes.
- Verify policy on a key such that it can only be used by specific AWS services.
- Distinguish the compliance state of data through tag-based data classifications and automate remediation.
- Evaluate a number of transport encryption techniques and select the appropriate method (i.e. TLS, IPsec, client-side KMS encryption).

Appendix

Which key tools, technologies, and concepts might be covered on the exam?

The following is a non-exhaustive list of the tools and technologies that could appear on the exam. This list is subject to change and is provided to help you understand the general scope of services, features, or technologies on the exam. The general tools and technologies in this list appear in no particular order. AWS services are grouped according to their primary functions. While some of these technologies will likely be covered more than others on the exam, the order and placement of them in this list is no indication of relative weight or importance:

- AWS CLI
- AWS SDK
- AWS Management Console
- Network analysis tools (packet capture and flow captures)
- SSH/RDP
- Signature Version 4
- TLS
- Certificate management
- Infrastructure as code (IaC)

AWS services and features

Note: Security affects all AWS services. Many services do not appear in this list because the overall service is out of scope, but the security aspects of the service are in scope. For example, a candidate for this exam would not be asked about the steps to set up replication for an S3 bucket, but the candidate might be asked about configuring an S3 bucket policy.

Management and Governance:

- AWS Audit Manager
- AWS CloudTrail
- Amazon CloudWatch
- AWS Config
- AWS Organizations
- AWS Systems Manager
- AWS Trusted Advisor

Networking and Content Delivery:

- Amazon Detective
- AWS Firewall Manager
- AWS Network Firewall
- AWS Security Hub
- AWS Shield
- Amazon VPC
    - VPC endpoints
    - Network ACLs
    - Security groups
- AWS WAF

Security, Identity, and Compliance:

- AWS Certificate Manager (ACM)
- AWS CloudHSM
- AWS Directory Service
- Amazon GuardDuty
- AWS Identity and Access Management (IAM)
- Amazon Inspector
- AWS Key Management Service (AWS KMS)
- Amazon Macie
- AWS Single Sign-On

Out-of-scope AWS services and features

The following is a non-exhaustive list of AWS services and features that are not covered on the exam. These services and features do not represent every AWS offering that is excluded from the exam content. Services or features that are entirely unrelated to the target job roles for the exam are excluded from this list because they are assumed to be irrelevant.

Out-of-scope AWS services and features include the following:

- Application development services
- IoT services
- Machine learning (ML) services
- Media services
- Migration and transfer services

1) A corporate cloud security policy states that communication between the company's VPC and KMS must travel entirely within the AWS network and not use public service endpoints.

Which combination of the following actions MOST satisfies this requirement? (Select TWO.)

A) Add the `aws:sourceVpce` condition to the AWS KMS key policy referencing the company's VPC endpoint ID.
B) Remove the VPC internet gateway from the VPC and add a virtual private gateway to the VPC to prevent direct, public internet connectivity.
C) Create a VPC endpoint for AWS KMS with private DNS enabled.
D) Use the KMS Import Key feature to securely transfer the AWS KMS key over a VPN.
E) Add the following condition to the AWS KMS key policy: `"aws:SourceIp": "10.0.0.0/16"`.

2) An application team is designing a solution with two applications. The security team wants the applications' logs to be captured in two different places, because one of the applications produces logs with sensitive data.

Which solution meets the requirement with the LEAST risk and effort?

A) Use Amazon CloudWatch Logs to capture all logs, write an AWS Lambda function that parses the log file, and move sensitive data to a different log.
B) Use Amazon CloudWatch Logs with two log groups, with one for each application, and use an AWS IAM policy to control access to the log groups, as required.
C) Aggregate logs into one file, then use Amazon CloudWatch Logs, and then design two CloudWatch metric filters to filter sensitive data from the logs.
D) Add logic to the application that saves sensitive data logs on the Amazon EC2 instances' local storage, and write a batch script that logs into the Amazon EC2 instances and moves sensitive logs to a secure location.

3) A security engineer must set up security group rules for a three-tier application:

- **Presentation tier – Accessed by users over the web, protected by the security group `presentation-sg`**
- **Logic tier – RESTful API accessed from the presentation tier through HTTPS, protected by the security group `logic-sg`**
- **Data tier – SQL Server database accessed over port 1433 from the logic tier, protected by the security group `data-sg`**

Which combination of the following security group rules will allow the application to be secure and functional? (Select THREE.)

A) `presentation-sg`: Allow ports 80 and 443 from 0.0.0.0/0
B) `data-sg`: Allow port 1433 from `presentation-sg`
C) `data-sg`: Allow port 1433 from `logic-sg`
D) `presentation-sg`: Allow port 1433 from `data-sg`
E) `logic-sg`: Allow port 443 from `presentation-sg`
F) `logic-sg`: Allow port 443 from 0.0.0.0/0

4) A security engineer is working with a product team building a web application on AWS. The application uses Amazon S3 to host the static content, Amazon API Gateway to provide RESTful services, and Amazon DynamoDB as the backend data store. The users already exist in a directory that is exposed through a SAML identity provider.

Which combination of the following actions should the engineer take to enable users to be authenticated into the web application and call APIs? (Select THREE).

A) Create a custom authorization service using AWS Lambda.
B) Configure a SAML identity provider in Amazon Cognito to map attributes to the Amazon Cognito user pool attributes.
C) Configure the SAML identity provider to add the Amazon Cognito user pool as a relying party.
D) Configure an Amazon Cognito identity pool to integrate with social login providers.
E) Update DynamoDB to store the user email addresses and passwords.
F) Update API Gateway to use an Amazon Cognito user pool authorizer.

5) A company is hosting a web application on AWS and is using an Amazon S3 bucket to store images. Users should have the ability to read objects in the bucket. A security engineer has written the following bucket policy to grant public read access:

```
{
   "ID":"Policy1502987489630",
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"Stmt1502987487640",
         "Action":[
            "s3:GetObject",
            "s3:GetObjectVersion"
         ],
         "Effect":"Allow",
         "Resource":"arn:aws:s3:::appbucket",
         "Principal":"*"
      }
   ]
}
```

Attempts to read an object, however, receive the error: "Action does not apply to any resource(s) in statement."

What should the engineer do to fix the error?

A) Change the IAM permissions by applying PutBucketPolicy permissions.
B) Verify that the policy has the same name as the bucket name. If not, make it the same.
C) Change the `resource` section to `"arn:aws:s3:::appbucket/*"`.
D) Add an `s3:ListBucket` action.

6) A company decides to place database hosts in its own VPC, and to set up VPC peering to different VPCs containing the application and web tiers. The application servers are unable to connect to the database.

Which network troubleshooting steps should be taken to resolve the issue? (Select TWO.)

A) Check to see if the application servers are in a private subnet or public subnet.
B) Check the route tables for the application server subnets for routes to the VPC peering connection.
C) Check the NACLs for the database subnets for rules that allow traffic from the internet.
D) Check the database security groups for rules that allow traffic from the application servers.
E) Check to see if the database VPC has an internet gateway.

7) When testing a new AWS Lambda function that retrieves items from an Amazon DynamoDB table, the security engineer notices that the function was not logging any data to Amazon CloudWatch Logs.

The following policy was assigned to the role assumed by the Lambda function:

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "Dynamo-1234567",
         "Action": [
            "dynamodb:GetItem"
         ],
         "Effect": "Allow",
         "Resource": "*"
      }
}
```

Which least-privilege policy addition would allow this function to log properly?

A)
```
{
   "Sid": "Logging-12345",
   "Resource": "*",
   "Action": [
      "logs:*"
   ],
   "Effect": "Allow"
}
```

B)
```
{
   "Sid": "Logging-12345",
   "Resource": "*",
   "Action": [
      "logs:CreateLogStream"
   ],
   "Effect": "Allow"
}
```

C)
```
{
   "Sid": "Logging-12345",
   "Resource": "*",
   "Action": [
      "logs:CreateLogGroup",
      "logs:CreateLogStream",
      "logs:PutLogEvents"
   ],
   "Effect": "Allow"
}
```

D)
```
{
   "Sid": "Logging-12345",
   "Resource": "*",
   "Action": [
      "logs:CreateLogGroup",
      "logs:CreateLogStream",
      "logs:DeleteLogGroup",
      "logs:DeleteLogStream",
      "logs:getLogEvents",
      "logs:PutLogEvents"
   ],
   "Effect": "Allow"
}
```

8) A company is building a data lake on Amazon S3. The data consists of millions of small files containing sensitive information. The security team has the following requirements for the architecture:

- **Data must be encrypted in transit.**
- **Data must be encrypted at rest.**
- **The bucket must be private, but if the bucket is accidentally made public, the data must remain confidential.**

Which combination of steps would meet the requirements? (Select TWO.)

A) Enable AES-256 encryption using server-side encryption with Amazon S3-managed encryption keys (SSE-S3) on the S3 bucket.
B) Enable default encryption with server-side encryption with AWS KMS-managed keys (SSE-KMS) on the S3 bucket.
C) Add a bucket policy that includes a deny if a `PutObject` request does not include `aws:SecureTransport`.
D) Add a bucket policy with `aws:SourceIp` to allow uploads and downloads from the corporate intranet only.
E) Enable Amazon Macie to monitor and act on changes to the data lake's S3 bucket.

9) A security engineer must ensure that all API calls are collected across all company accounts, and that they are preserved online and are instantly available for analysis for 90 days. For compliance reasons, this data must be restorable for 7 years.

Which steps must be taken to meet the retention needs in a scalable, cost-effective way?

A) Enable AWS CloudTrail logging across all accounts to a centralized Amazon S3 bucket with versioning enabled. Set a lifecycle policy to move the data to Amazon Glacier daily, and expire the data after 90 days.
B) Enable AWS CloudTrail logging across all accounts to S3 buckets. Set a lifecycle policy to expire the data in each bucket after 7 years.
C) Enable AWS CloudTrail logging across all accounts to Amazon Glacier. Set a lifecycle policy to expire the data after 7 years.
D) Enable AWS CloudTrail logging across all accounts to a centralized Amazon S3 bucket. Set a lifecycle policy to move the data to Amazon Glacier after 90 days, and expire the data after 7 years.

10) A security engineer has been informed that a user's access key has been found on GitHub. The engineer must ensure that this access key cannot continue to be used, and must assess whether the access key was used to perform any unauthorized activities.

Which steps must be taken to perform these tasks?

A) Review the user's IAM permissions and delete any unrecognized or unauthorized resources.
B) Delete the user, review Amazon CloudWatch Logs in all regions, and report the abuse.
C) Delete or rotate the user's key, review the AWS CloudTrail logs in all regions, and delete any unrecognized or unauthorized resources.
D) Instruct the user to remove the key from the GitHub submission, rotate keys, and re-deploy any instances that were launched.

Answers

1) A, C – An IAM policy can deny access to AWS KMS except through your VPC endpoint with the following condition statement:

```
"Condition": {
   "StringNotEquals": {
      "aws:sourceVpce": "vpce-0295a3caf8414c94a"
   }
}
```

If you select the Enable Private DNS Name option, the standard AWS KMS DNS hostname (https://kms.<region>.amazonaws.com) resolves to your VPC endpoint.

2) B – Each application's log can be configured to send the log to a specific Amazon CloudWatch Logs log group.

3) A, C, E – In an n-tier architecture, each tier's security group allows traffic from the security group sending it traffic only. The presentation tier opens traffic for HTTP and HTTPS from the internet. Since security groups are stateful, only inbound rules are required.

4) B, C, F – When Amazon Cognito receives a SAML assertion, it needs to be able to map SAML attributes to user pool attributes. When configuring Amazon Cognito to receive SAML assertions from an identity provider, you need ensure that the identity provider is configured to have Amazon Cognito as a relying party. Amazon API Gateway will need to be able to understand the authorization being passed from Amazon Cognito, which is a configuration step.

5) C – The `resource` section should match with the type of operation. Change the ARN to include /* at the end, as it is an object operation. https://aws.amazon.com/blogs/security/writing-iam-policies-how-to-grant-access-to-an-amazon-s3-bucket/.

6) B, D – You must configure the route tables in each VPC to route to each other through the peering connection. You also must add rules to the security group for the databases to accept requests from the application server security group in the other VPC.

7) C – Basic Lambda permissions required to log to Amazon CloudWatch Logs include `CreateLogGroup`, `CreateLogStream`, and `PutLogEvents`.

8) B, C – Bucket encryption using KMS will protect both in case disks are stolen as well as if the bucket is public. This is because the AWS KMS key would need to have privileges granted to it for users outside of AWS. HTTPS will protect data in transit.

9) D – Meets all requirements and is cost effective by using lifecycle policies to transition to Amazon Glacier.

10) C – Removes keys and audits the environment for malicious activities.