AWS Certified Security – Specialty (SCS-C02)

100 Questions & Answers

Welcome to your complete AWS Certified Security – Specialty (SCS-C02) ***practice*** *questions collection. This guide is designed to sharpen your exam readiness using* ***realistic, scenario-based questions*** *focused on core AWS security concepts, services, and best practices.*

Learning Objectives and Expectations

You'll get:

- Real-world questions modeled on the latest AWS SCS-C02 exam format
- Organized into **batches of 10 questions, followed by 10 detailed answers** and explanations
- Targeted answer keys that reinforce threat detection, IAM, encryption, compliance, and security governance concepts

AWS Security Specialty (SCS-C02) Domains

Each domain carries a specific weight on the exam. Domains 2, 3, and 5 are among the most heavily tested:

- **Domain 1:** Threat Detection and Incident Response – 14%
- **Domain 2:** Security Logging and Monitoring – 18%
- **Domain 3:** Infrastructure Security – 20%
- **Domain 4:** Identity and Access Management – 16%
- **Domain 5:** Data Protection – 18%
- **Domain 6:** Management and Security Governance – 14%

Quick Reminder: How the Exam Works

- **Number of Questions:** 65
- **Format:** Multiple choice, multiple response, and scenario-based
- **Time Limit:** 170 minutes
- **Passing Score:** 750/1000
- **Test Provider:** Pearson VUE (online or onsite)

Questions by Domain

Domain	Title	Questions Assigned	Question Numbers
Domain 1	Threat Detection and Incident Response (14%)	14 Questions	Q1, Q4, Q9, Q26, Q41, Q48, Q58, Q64, Q70, Q81, Q84, Q88, Q91, Q94
Domain 2	Security Logging and Monitoring (18%)	18 Questions	Q2, Q13, Q18, Q22, Q25, Q30, Q36, Q42, Q47, Q50, Q61, Q62, Q65, Q69, Q80, Q83, Q87, Q100
Domain 3	Infrastructure Security (20%)	20 Questions	Q3, Q10, Q16, Q21, Q24, Q27, Q29, Q32, Q34, Q44, Q46, Q51, Q55, Q56, Q66, Q71, Q76, Q77, Q86, Q90
Domain 4	Identity and Access Management (16%)	16 Questions	Q5, Q6, Q12, Q15, Q20, Q28, Q35, Q43, Q52, Q54, Q60, Q68, Q72, Q73, Q89, Q98
Domain 5	Data Protection (18%)	18 Questions	Q7, Q8, Q11, Q14, Q17, Q19, Q23, Q31, Q37, Q38, Q39, Q49, Q53, Q59, Q63, Q75, Q78, Q79
Domain 6	Management and Security Governance (14%)	14 Questions	Q33, Q40, Q45, Q57, Q67, Q74, Q82, Q85, Q92, Q93, Q95, Q96, Q97, Q99

Remember — You Don't Need to Be Perfect to Pass!

The AWS Security Specialty exam passing score is 750/1000. That means you **can miss around 10–15 scored questions** and still pass. Focus on core concepts: how AWS services secure data, detect threats, enforce access, and ensure compliance.

Questions 1–10

Q1.
Your company wants to detect when someone changes an S3 bucket policy to allow public access. Which AWS service can be used to **automatically detect and alert** on such configuration changes?

A) AWS CloudTrail
B) Amazon Macie
C) AWS Config
D) AWS Inspector

Q2.
A security engineer needs to ensure that S3 objects are only accessible over HTTPS and never via unencrypted HTTP. Which configuration meets this requirement?

A) Enable MFA Delete on the S3 bucket
B) Configure bucket policy to deny requests without aws:SecureTransport
C) Enable S3 default encryption
D) Create a KMS key policy that blocks HTTP

Q3.
Your EC2 instance needs to securely retrieve database credentials at runtime. The credentials must not be hardcoded or stored in plain text. What is the best solution?

A) Store credentials in EC2 user-data
B) Use SSM Parameter Store with plaintext parameters
C) Use AWS Secrets Manager with IAM-based access
D) Store credentials in a text file in S3

Q4.
An EC2 instance is showing signs of compromise. What is the **first response** step you should take?

A) Terminate the instance immediately
B) Take an EBS snapshot and isolate the instance
C) Delete IAM roles attached to the instance
D) Clear all CloudWatch logs

Q5.
Which AWS service can **automatically classify sensitive data** in Amazon S3 using machine learning?

A) Amazon Inspector
B) Amazon GuardDuty
C) Amazon Macie
D) AWS Config

Q6.
Your organization uses AWS Organizations and wants to **block the use of AWS Kinesis** in all child accounts. Which mechanism should be used?

A) IAM deny policy
B) SCP attached to the root OU
C) NACLs
D) VPC endpoint restrictions

Q7.
Which AWS service provides a **centralized view** of security findings from services like GuardDuty, Macie, and Inspector?

A) CloudTrail
B) AWS Config
C) Security Hub
D) CloudWatch Logs

Q8.
A company is required to use customer-managed KMS keys and rotate them annually. How can this be achieved?

A) Use AWS-managed keys
B) Use client-side encryption
C) Enable automatic rotation on a customer-managed CMK
D) Export CMK and reimport manually

Q9.
A GuardDuty finding indicates a port scan from an EC2 instance. What is the **most appropriate** action?

A) Restart the instance
B) Add the instance to a security group with no egress
C) Delete the instance's IAM role
D) Update EC2 instance metadata

Q10.
Which AWS service allows **auditing of IAM credentials**, showing usage and password rotation status?

A) Security Hub
B) AWS IAM Access Analyzer
C) AWS IAM Credential Report
D) CloudTrail

Answers 1–10

A1.
Answer: C) AWS Config
Explanation: AWS Config continuously monitors AWS resource configurations and can detect when an S3 bucket becomes publicly accessible by evaluating it against rules.

A2.
Answer: B) Configure bucket policy to deny requests without aws:SecureTransport
Explanation: Adding a condition in the S3 bucket policy to deny requests where aws:SecureTransport is false ensures only HTTPS access is allowed.

A3.
Answer: C) Use AWS Secrets Manager with IAM-based access
Explanation: Secrets Manager securely stores and retrieves credentials, supports encryption at rest with KMS, and integrates with IAM for fine-grained access.

A4.
Answer: B) Take an EBS snapshot and isolate the instance
Explanation: This preserves forensic evidence while preventing further spread or data exfiltration by isolating the compromised instance.

A5.
Answer: C) Amazon Macie
Explanation: Macie uses machine learning to identify and alert on sensitive data like PII in Amazon S3.

A6.
Answer: B) SCP attached to the root OU
Explanation: Service Control Policies (SCPs) are used within AWS Organizations to restrict access to AWS services across accounts.

A7.
Answer: C) Security Hub
Explanation: AWS Security Hub aggregates findings from other security services and provides centralized visibility and compliance scoring.

A8.
Answer: C) Enable automatic rotation on a customer-managed CMK
Explanation: AWS KMS supports automatic rotation of customer-managed keys every 365 days when enabled.

A9.
Answer: B) Add the instance to a security group with no egress
Explanation: This isolates the instance and prevents outbound communication, allowing investigation without data leakage.

A10.
Answer: C) AWS IAM Credential Report
Explanation: IAM Credential Reports show all users and details such as password age, access key usage, and MFA status.

Questions 11–20

Q11.
Which of the following AWS services uses **threat intelligence and machine learning** to detect anomalies and suspicious behavior across accounts?

A) AWS CloudTrail
B) AWS WAF
C) Amazon GuardDuty
D) AWS Firewall Manager

Q12.
A financial company requires all EBS volumes to be encrypted with **customer-managed KMS keys**. How can this requirement be enforced?

A) Enable EBS default encryption using AWS-managed keys
B) Create a backup plan in AWS Backup
C) Use AWS Config rule ebs-encrypted-volumes with custom key check
D) Set IAM policy to deny unencrypted volume creation

Q13.
Which logging configuration ensures that **API activity from all accounts in an AWS Organization** is recorded?

A) CloudTrail trail in each account
B) CloudTrail trail with "Organization trail" enabled
C) GuardDuty delegated administrator
D) VPC Flow Logs across accounts

Q14.
A company wants to detect if S3 buckets become publicly accessible. Which AWS Config rule should be used?

A) cloudtrail-enabled
B) s3-bucket-public-read-prohibited
C) ec2-instance-no-public-ip
D) s3-bucket-versioning-enabled

Q15.
Which AWS feature allows users to retrieve **temporary security credentials** for federated access?

A) AWS IAM Roles
B) AWS SSO
C) AWS STS
D) AWS Directory Service

Q16.
You are using an EC2 instance that must securely access S3. What is the best practice to provide access?

A) Use access keys in user-data
B) Attach an IAM role to the EC2 instance
C) Hardcode credentials into the app
D) Use S3 pre-signed URLs

Q17.
What does enabling **multi-factor authentication (MFA)** on the root account help prevent?

A) DDoS attacks
B) IAM policy overrides
C) Unauthorized root-level access
D) Unencrypted data uploads

Q18.
A company uses AWS CloudTrail to log actions. How can it detect **unusual API call volume** that may indicate compromised credentials?

A) Use CloudTrail Insights
B) Use IAM Credential Report
C) Enable S3 server access logging
D) Use Macie

Q19.
Which service supports **automatic rotation of secrets**, including integration with RDS and KMS?

A) AWS Systems Manager Parameter Store
B) AWS IAM
C) AWS KMS
D) AWS Secrets Manager

Q20.
What AWS feature allows an organization to enforce **tagging policies**, like requiring a specific tag on EC2 instances?

A) AWS Config
B) AWS Service Catalog
C) AWS Organizations Tag Policies
D) IAM Permission Boundaries

Answers 11–20

A11.
Answer: C) Amazon GuardDuty
Explanation: GuardDuty analyzes CloudTrail, VPC Flow Logs, and DNS data using threat intelligence and machine learning to detect threats.

A12.
Answer: C) Use AWS Config rule ebs-encrypted-volumes with custom key check
Explanation: The managed Config rule can be customized to check if EBS volumes use specific customer-managed KMS keys.

A13.
Answer: B) CloudTrail trail with "Organization trail" enabled
Explanation: Organization trails log API activity across all accounts under the AWS Organization to a centralized S3 bucket.

A14.
Answer: B) s3-bucket-public-read-prohibited
Explanation: This AWS Config rule flags any S3 bucket with public-read permissions enabled.

A15.
Answer: C) AWS STS
Explanation: AWS Security Token Service (STS) provides temporary credentials for users or federated identities.

A16.
Answer: B) Attach an IAM role to the EC2 instance
Explanation: The best practice is to use an IAM role that provides temporary credentials automatically to the EC2 instance.

A17.
Answer: C) Unauthorized root-level access
Explanation: Enabling MFA on the root account protects against unauthorized access using the most privileged identity in AWS.

A18.
Answer: A) Use CloudTrail Insights
Explanation: CloudTrail Insights detects unusual patterns in API usage, such as spikes in activity, which may indicate compromise.

A19.
Answer: D) AWS Secrets Manager
Explanation: Secrets Manager supports automatic rotation of secrets and integrates with KMS and Amazon RDS for managed credentials.

A20.
Answer: C) AWS Organizations Tag Policies
Explanation: Tag Policies help enforce standardized tagging rules across AWS accounts in an organization.

Questions 21–30

Q21.
Your organization wants to ensure that IAM users can't disable CloudTrail logging. Which approach enforces this at the organization level?

A) Use an IAM policy with a Deny for cloudtrail:StopLogging
B) Use a Service Control Policy (SCP) to deny cloudtrail:StopLogging
C) Enable CloudTrail log file validation
D) Create a CloudWatch alarm for StopLogging API calls

Q22.
A data scientist wants to download a large S3 dataset from an IP range **outside your corporate network**. You want to restrict access to **internal IPs only**. What's the best solution?

A) Block all internet access in the VPC
B) Use an S3 bucket policy with a condition on aws:SourceIp
C) Enable server-side encryption on the bucket
D) Require signed URLs for the objects

Q23.
Which AWS service enables **private access to AWS services** from within your VPC without going over the public internet?

A) AWS Direct Connect
B) NAT Gateway
C) AWS PrivateLink (Interface VPC Endpoints)
D) AWS Transit Gateway

Q24.
A company wants to enforce **MFA before allowing access to delete S3 buckets**. Which IAM policy condition can enforce this?

A) StringEqualsIfExists: aws:username
B) BoolIfExists: aws:SecureTransport
C) Bool: aws:MultiFactorAuthPresent
D) IpAddress: aws:SourceIp

Q25.
Which service allows **log queries using SQL-like syntax** on data stored in S3?

A) CloudWatch Logs Insights
B) Athena
C) Kinesis
D) S3 Glacier Select

Q26.
A new threat detection policy requires tracking **SSH brute-force attempts** against EC2 instances. Which service can detect these attacks natively?

A) AWS Config
B) Amazon Macie
C) Amazon GuardDuty
D) CloudTrail Insights

Q27.
What is the **main benefit** of enabling log file validation in AWS CloudTrail?

A) Enables automatic archiving of logs to S3
B) Prevents logs from being modified
C) Allows validation of log file integrity
D) Encrypts log files with a KMS CMK

Q28.
What does the **AWS IAM Access Analyzer** do?

A) Identifies unused permissions in IAM policies
B) Identifies resources shared outside your account
C) Detects EC2 instance vulnerabilities
D) Analyzes billing charges by user

Q29.
A developer is building a containerized app on ECS that needs access to DynamoDB. What's the **most secure way** to grant access?

A) Store credentials in environment variables
B) Use an IAM role for ECS tasks
C) Embed AWS credentials in Dockerfile
D) Use an EC2 Instance profile

Q30.
A team wants to use CloudTrail logs for incident response. What's the **most cost-effective** way to retain and analyze logs long-term?

A) Enable CloudTrail Lake
B) Store logs in CloudWatch Logs
C) Export to S3 and analyze using Athena
D) Store logs on an EBS volume

Answers 21–30

A21.
Answer: B) Use a Service Control Policy (SCP) to deny cloudtrail:StopLogging
Explanation: SCPs can enforce service restrictions across accounts in an organization and apply even to the root user.

A22.
Answer: B) Use an S3 bucket policy with a condition on aws:SourceIp
Explanation: S3 bucket policies can restrict access based on source IP using aws:SourceIp in the condition block.

A23.
Answer: C) AWS PrivateLink (Interface VPC Endpoints)
Explanation: PrivateLink enables private connectivity to AWS services over the AWS network, keeping traffic off the public internet.

A24.
Answer: C) Bool: aws:MultiFactorAuthPresent
Explanation: This condition ensures the user has authenticated using MFA before performing the specified action.

A25.
Answer: B) Athena
Explanation: Amazon Athena allows SQL-style querying of data stored in S3, including CloudTrail and ELB logs.

A26.
Answer: C) Amazon GuardDuty
Explanation: GuardDuty can detect brute-force SSH attacks by analyzing VPC Flow Logs and other data sources.

A27.
Answer: C) Allows validation of log file integrity
Explanation: CloudTrail log validation creates digest files that can be used to verify that logs have not been tampered with.

A28.
Answer: B) Identifies resources shared outside your account
Explanation: IAM Access Analyzer reviews resource policies and flags access that grants external (e.g., public or cross-account) access.

A29.
Answer: B) Use an IAM role for ECS tasks
Explanation: ECS task roles provide temporary, scoped credentials and are the most secure method for AWS service access.

A30.
Answer: C) Export to S3 and analyze using Athena
Explanation: Storing logs in S3 is low-cost, and Athena allows querying without moving or copying data.

Questions 31–40

Q31.
A company wants to protect its S3 data from ransomware attacks that encrypt or delete objects. What feature should be used?

A) MFA Delete
B) Versioning
C) Object Lock
D) Access Control Lists

Q32.
Which AWS service enables organizations to define **preventive and detective security controls** at scale across accounts using preconfigured rules?

A) AWS WAF
B) AWS Firewall Manager
C) AWS Config
D) AWS Trusted Advisor

Q33.
A company uses Amazon S3 for data storage. How can they **prevent all public access** to any new or existing S3 bucket?

A) Use S3 bucket policies only
B) Enable Access Analyzer
C) Turn on Block Public Access at the account level
D) Use IAM policy to deny public access

Q34.
Which AWS service provides **cross-account visibility** into compliance with security controls and a single view of security alerts?

A) GuardDuty
B) Macie
C) Security Hub
D) Inspector

Q35.
A developer accidentally made an S3 bucket public. What AWS service can detect and report this misconfiguration?

A) AWS KMS
B) IAM Access Analyzer
C) Amazon GuardDuty
D) AWS CloudTrail

Q36.
Which of the following helps detect and **block data exfiltration attempts via DNS**?

A) AWS Shield
B) Route 53 Resolver DNS Firewall
C) AWS WAF
D) GuardDuty EKS Audit Logs

Q37.
Your company mandates that all data be encrypted using **customer-managed keys**. How do you enforce this in S3?

A) Set up S3 Bucket Policy requiring SSE-S3
B) Use S3 Default Encryption with SSE-KMS and a CMK
C) Use ACLs to restrict object upload
D) Encrypt files manually before upload

Q38.
Which AWS feature helps prevent **accidental deletion or alteration** of S3 logs or sensitive data?

A) Enable S3 Transfer Acceleration
B) Enable S3 Object Lock in compliance mode
C) Enable versioning and lifecycle policies
D) Enable default encryption

Q39.
What IAM policy element can **limit access based on the time of day**?

A) aws:CurrentTime
B) aws:UserAgent

C) aws:SecureTransport
D) aws:RequestedRegion

Q40.
A company needs to ensure that all IAM users **rotate access keys every 90 days**. What's the best way to monitor compliance?

A) Create a Lambda function to scan IAM
B) Use IAM Credential Report
C) Use IAM Access Analyzer
D) Use SSM Automation

Answers 31–40

A31.
Answer: C) Object Lock
Explanation: S3 Object Lock enables write-once-read-many (WORM) protection, preventing object overwrites or deletions for a retention period.

A32.
Answer: B) AWS Firewall Manager
Explanation: Firewall Manager applies preconfigured security policies across multiple accounts for WAF, Shield, and VPC security.

A33.
Answer: C) Turn on Block Public Access at the account level
Explanation: Block Public Access at the account or bucket level overrides any public ACLs or bucket policies, enforcing private access.

A34.
Answer: C) Security Hub
Explanation: AWS Security Hub aggregates security findings and compliance results from multiple accounts and services.

A35.
Answer: B) IAM Access Analyzer
Explanation: Access Analyzer scans S3 bucket policies and alerts if a bucket is publicly accessible or shared outside the account.

A36.
Answer: B) Route 53 Resolver DNS Firewall
Explanation: It allows filtering and blocking DNS queries to known malicious domains, helping prevent exfiltration via DNS tunneling.

A37.
Answer: B) Use S3 Default Encryption with SSE-KMS and a CMK
Explanation: Default encryption enforces KMS encryption using a specific CMK for all new uploads.

A38.
Answer: B) Enable S3 Object Lock in compliance mode
Explanation: Compliance mode prevents object deletion or modification, even by root, during the retention period.

A39.
Answer: A) aws:CurrentTime
Explanation: IAM policy conditions can use aws:CurrentTime to allow or deny actions based on time of day.

A40.
Answer: B) Use IAM Credential Report
Explanation: The IAM Credential Report shows last key rotation dates and helps audit compliance with rotation policies.

Questions 41–50

Q41.
You are setting up centralized logging for all AWS accounts in your organization. Which account should be used to receive logs from all other accounts?

A) The account running GuardDuty
B) The Log Archive account
C) The Management (root) account
D) The Security Tooling account

Q42.
A company wants to use CloudTrail for forensic analysis. What can ensure the **integrity** of log files?

A) Enable S3 MFA Delete
B) Enable log file validation
C) Enable server-side encryption
D) Use Lifecycle policies

Q43.
What AWS service enables users to **audit and automate compliance checks** using frameworks like CIS and PCI-DSS?

A) AWS Security Hub
B) AWS Config
C) AWS Inspector
D) AWS Audit Manager

Q44.
Which AWS service provides **visualization and analysis** of data from GuardDuty, VPC Flow Logs, and CloudTrail to help investigate threats?

A) AWS CloudTrail Insights
B) AWS Config
C) Amazon Detective
D) AWS Athena

Q45.
Which service would you use to **detect vulnerabilities** in container images stored in Amazon ECR?

A) Amazon Macie
B) Amazon Inspector
C) AWS Config
D) AWS GuardDuty

Q46.
Which feature of KMS ensures **decryption can only occur when a specific context is provided**?

A) Key Rotation
B) Grants
C) Encryption Context
D) Multi-Region Key

Q47.
Your company wants to analyze failed API calls across accounts. Where is this information found?

A) CloudWatch Logs
B) IAM Credential Report
C) CloudTrail Event History
D) GuardDuty

Q48.
An EC2 instance with internet access starts communicating with a known botnet IP. What is the **first recommended action**?

A) Terminate the instance
B) Remove the IAM role
C) Isolate the instance using a restrictive Security Group
D) Delete the instance's EBS volumes

Q49.
A user wants to allow access to a Lambda function **only if it is called from a specific VPC**. Which condition can enforce this?

A) aws:VpcSourceIp
B) aws:SourceVpc
C) aws:SecureTransport
D) aws:VpcId

Q50.
Which tool can help you **identify unused IAM permissions** based on activity?

A) IAM Access Analyzer
B) IAM Credential Report
C) IAM Access Advisor
D) AWS Config

Answers 41–50

A41.
Answer: B) The Log Archive account
Explanation: In a multi-account architecture, logs are centralized into the Log Archive account for integrity and separation from workload accounts.

A42.
Answer: B) Enable log file validation
Explanation: CloudTrail log file validation uses digest files and hashes to ensure logs have not been tampered with.

A43.
Answer: D) AWS Audit Manager
Explanation: Audit Manager automates collection of evidence and compliance checks against frameworks like CIS, ISO, and PCI.

A44.
Answer: C) Amazon Detective
Explanation: Detective helps analyze, visualize, and investigate security issues using data from GuardDuty, CloudTrail, and VPC Flow Logs.

A45.
Answer: B) Amazon Inspector
Explanation: Inspector can scan Amazon ECR container images for vulnerabilities and CVEs automatically upon image push.

A46.
Answer: C) Encryption Context
Explanation: KMS allows an optional encryption context to ensure only requests with matching metadata can decrypt the data.

A47.
Answer: C) CloudTrail Event History
Explanation: CloudTrail records all API calls, including failed ones, and shows detailed event history for security analysis.

A48.
Answer: C) Isolate the instance using a restrictive Security Group
Explanation: Isolation is the first containment step in incident response, allowing investigation without further risk.

A49.
Answer: B) aws:SourceVpc
Explanation: This IAM condition can restrict actions (like invoking a Lambda) to calls that originate from a specific VPC.

A50.
Answer: C) IAM Access Advisor
Explanation: Access Advisor shows service permissions that have not been used by a role/user, helping with least privilege audits.

Questions 51–60

Q51.
A team wants to ensure that a Lambda function can **access a specific S3 bucket only**, and nothing else. Which is the **most secure IAM policy** approach?

A) Allow s3:* on *
B) Allow s3:GetObject on all S3 buckets
C) Allow s3:* on a specific bucket ARN
D) Allow s3:GetObject on the specific bucket's ARN

Q52.
You need to allow a third-party vendor access to a specific S3 bucket **without using IAM users**. What's the best way to do this?

A) Create an IAM user with long-term credentials
B) Use cross-account IAM roles and bucket policy
C) Share the bucket via a pre-signed URL
D) Use ACLs for the bucket

Q53.
Which AWS service helps ensure **automated patch compliance** across fleets of EC2 instances?

A) Amazon Inspector
B) AWS Systems Manager Patch Manager
C) AWS Config
D) CloudTrail

Q54.
Which AWS service allows detection of **unusual login locations** or credential use anomalies across your AWS accounts?

A) CloudTrail
B) GuardDuty
C) Security Hub
D) IAM Access Analyzer

Q55.
You want to enforce **network-level segmentation** between applications in the same VPC. Which option should you use?

A) Security Groups only
B) NACLs only
C) Separate VPCs
D) Both NACLs and Security Groups

Q56.
What is the best way to enforce encryption **for all EBS volumes** in a specific account?

A) Create an SCP to deny unencrypted EBS
B) Use IAM deny policies
C) Enable default EBS encryption with a CMK
D) Use AWS Backup to enforce encryption

Q57.
A customer stores sensitive logs in S3. How can they **prevent deletion of these logs** for 90 days?

A) Use S3 Versioning
B) Enable Object Lock with retention
C) Use S3 lifecycle rules
D) Use CloudTrail log file validation

Q58.
You want to ensure **CloudTrail cannot be disabled** across any AWS account in your organization. What is the best solution?

A) Enable MFA on the trail
B) Create an SCP denying cloudtrail:StopLogging
C) Encrypt CloudTrail with a KMS CMK
D) Use a bucket policy to block trail updates

Q59.
Which AWS service provides a **managed firewall** with deep packet inspection and stateful rules?

A) AWS WAF
B) AWS Firewall Manager

C) AWS Network Firewall
D) VPC Flow Logs

Q60.
Your architecture uses CloudFront with S3 origin. How can you **ensure only CloudFront** can access the S3 bucket?

A) Use a bucket ACL
B) Attach a security group to S3
C) Create an Origin Access Control (OAC) or OAI
D) Create a VPC endpoint

Answers 51–60

A51.
Answer: D) Allow s3:GetObject on the specific bucket's ARN
Explanation: This limits access to only the required action (GetObject) and to a specific resource, applying the principle of least privilege.

A52.
Answer: B) Use cross-account IAM roles and bucket policy
Explanation: Cross-account roles allow temporary, controlled access without creating IAM users or sharing credentials.

A53.
Answer: B) AWS Systems Manager Patch Manager
Explanation: Patch Manager automates OS patching for managed EC2 instances across an account or fleet.

A54.
Answer: B) GuardDuty
Explanation: GuardDuty can detect anomalous activity, including credential use from unusual geographic locations.

A55.
Answer: D) Both NACLs and Security Groups

Explanation: SGs are stateful and used at the instance level; NACLs are stateless and operate at the subnet level — combining both offers layered security.

A56.
Answer: C) Enable default EBS encryption with a CMK
Explanation: This ensures that all new volumes are encrypted by default, meeting compliance and reducing risk of oversight.

A57.
Answer: B) Enable Object Lock with retention
Explanation: S3 Object Lock in compliance mode prevents deletions or overwrites for a specified retention period.

A58.
Answer: B) Create an SCP denying cloudtrail:StopLogging
Explanation: An SCP at the organizational level can prevent all accounts from disabling CloudTrail, even by root.

A59.
Answer: C) AWS Network Firewall
Explanation: AWS Network Firewall provides managed, scalable, stateful inspection with customizable rule groups.

A60.
Answer: C) Create an Origin Access Control (OAC) or OAI
Explanation: This ensures that only CloudFront can access the S3 bucket, blocking all direct public access.

Questions 61–70

Q61.
A security team wants to automatically **remove public access** from any S3 bucket as soon as it's detected. What is the best solution?

A) Enable S3 Block Public Access at the account level
B) Use AWS Config with a remediation Lambda function
C) Use Access Analyzer to revoke public access
D) Use Trusted Advisor to send email alerts

Q62.
Your organization wants to detect and alert on **IAM root account usage**. What should you do?

A) Use GuardDuty
B) Enable CloudTrail Insights
C) Create a CloudWatch Logs metric filter on CloudTrail logs
D) Use Access Analyzer

Q63.
Which AWS service lets you define **security baselines** using managed controls and score your environment against them?

A) AWS Config
B) AWS Systems Manager
C) AWS Security Hub
D) AWS Control Tower

Q64.
You discover a compromised IAM user's credentials have been used to launch several large EC2 instances. What is the **first response** step?

A) Revoke the IAM user's credentials
B) Contact AWS Support
C) Take EBS snapshots
D) Delete the EC2 instances

Q65.
Which AWS service provides **network visibility** by recording metadata about IP traffic going in and out of network interfaces?

A) VPC Flow Logs
B) AWS Config
C) Amazon Inspector
D) GuardDuty

Q66.
How can you ensure **Amazon RDS** databases are not publicly accessible?

A) Enable encryption at rest
B) Place RDS in a private subnet and modify SG
C) Use IAM-based access
D) Apply a lifecycle policy to the subnet

Q67.
A developer wants to allow an external mobile app to access AWS resources temporarily. What is the recommended method?

A) IAM user with access keys
B) Cognito Identity Pool
C) IAM role with inline policy
D) Hardcode keys into app

Q68.
What is the **primary purpose** of KMS key grants?

A) To enforce encryption context
B) To delegate key permissions temporarily
C) To create HSM keys
D) To perform key rotation

Q69.
Your VPC design includes an internet gateway, but your EC2 instance still can't reach the internet. What is the **most likely reason**?

A) The route table doesn't include a 0.0.0.0/0 route
B) The instance is in a private subnet

C) The subnet has NAT enabled
D) The VPC is not attached to GuardDuty

Q70.
Which AWS feature enables **continuous compliance monitoring** by evaluating AWS resource configurations against rules?

A) CloudTrail
B) Config Rules
C) Security Hub
D) IAM Policies

Answers 61–70

A61.
Answer: B) Use AWS Config with a remediation Lambda function
Explanation: Config can detect public S3 access and trigger a Lambda function to automatically remediate it by blocking access.

A62.
Answer: C) Create a CloudWatch Logs metric filter on CloudTrail logs
Explanation: You can set a metric filter to detect the Root user activity in CloudTrail logs and alert via CloudWatch.

A63.
Answer: C) AWS Security Hub
Explanation: Security Hub provides benchmarks like CIS AWS Foundations and AWS Best Practices, assigning compliance scores.

A64.
Answer: A) Revoke the IAM user's credentials
Explanation: The priority is to prevent further misuse. Disable or delete keys, reset the password, and remove sessions.

A65.
Answer: A) VPC Flow Logs

Explanation: Flow Logs capture IP-level metadata (source/destination, ports, action) for VPC interfaces.

A66.
Answer: B) Place RDS in a private subnet and modify SG
Explanation: RDS should be placed in private subnets with no route to the IGW and with restrictive security groups.

A67.
Answer: B) Cognito Identity Pool
Explanation: Cognito Identity Pools issue temporary credentials via STS for unauthenticated or federated users.

A68.
Answer: B) To delegate key permissions temporarily
Explanation: KMS grants allow services or principals to use a key temporarily without modifying the key policy.

A69.
Answer: A) The route table doesn't include a 0.0.0.0/0 route
Explanation: For internet access, the subnet's route table must direct traffic to the IGW via 0.0.0.0/0.

A70.
Answer: B) Config Rules
Explanation: AWS Config Rules allow you to define desired states and evaluate AWS resource configurations against them.

Questions 71–80

Q71.
A customer must ensure all logs collected from AWS services are **tamper-resistant** and cannot be deleted by IAM users. What's the best approach?

A) Store logs in S3 and enable MFA Delete
B) Store logs in EBS with encryption
C) Use CloudWatch Logs with metric filters
D) Store logs in DynamoDB with encryption at rest

Q72.
A company has multiple accounts. The security team needs **centralized visibility** of GuardDuty findings. What should they do?

A) Enable GuardDuty in each account manually
B) Use AWS Config Aggregator
C) Designate a delegated administrator for GuardDuty
D) Use EventBridge to pull logs

Q73.
What AWS IAM feature **limits the maximum permissions** an IAM user or role can ever have, regardless of attached policies?

A) SCP
B) IAM Role Trust Policy
C) IAM Permissions Boundary
D) Session Policy

Q74.
Which AWS service uses **automated reasoning** to detect public or cross-account access in IAM policies?

A) IAM Access Advisor
B) IAM Access Analyzer
C) AWS Config
D) GuardDuty

Q75.
Your company wants to ensure S3 objects uploaded by users are **always encrypted using SSE-KMS**. How can you enforce this?

A) IAM policy requiring KMS encryption
B) S3 bucket policy that denies unencrypted uploads
C) Enable S3 default encryption
D) Use Access Analyzer

Q76.
An engineer wants to allow a Lambda function to decrypt KMS data only when called from a specific VPC. What should they use?

A) KMS Grant
B) Encryption Context
C) IAM policy condition with aws:SourceVpc
D) Lambda environment variables

Q77.
What's the **primary benefit** of using AWS Control Tower for governance?

A) Allows deep packet inspection
B) Blocks IAM privilege escalation
C) Sets up a secure multi-account landing zone with guardrails
D) Encrypts data in S3 and RDS

Q78.
Which AWS service helps enforce **resource deployment standards** by limiting what users can provision?

A) CloudFormation
B) AWS Systems Manager
C) AWS Service Catalog
D) IAM Access Analyzer

Q79.
Which encryption method uses a unique data key per object/file and protects the data key using a CMK?

A) Asymmetric key encryption
B) Envelope encryption
C) KMS grants
D) SSE-C

Q80.
You want to analyze Amazon VPC Flow Logs to find patterns of rejected traffic. What's the **fastest** way to do this?

A) Export logs to S3 and run Athena queries
B) Use CloudWatch Logs Insights
C) Enable Macie
D) Use CloudTrail Event History

Answers 71–80

A71.
Answer: A) Store logs in S3 and enable MFA Delete
Explanation: MFA Delete requires MFA to delete versioned objects, making logs tamper-resistant for compliance.

A72.
Answer: C) Designate a delegated administrator for GuardDuty
Explanation: A delegated admin can centrally manage GuardDuty across all AWS accounts in the org.

A73.
Answer: C) IAM Permissions Boundary
Explanation: Permissions boundaries limit the maximum permissions a user/role can have, even if other policies allow more.

A74.
Answer: B) IAM Access Analyzer
Explanation: Access Analyzer uses logic to analyze IAM/resource policies and detect external or public access.

A75.
Answer: B) S3 bucket policy that denies unencrypted uploads
Explanation: You can use a bucket policy with aws:SecureTransport or s3:x-amz-server-side-encryption to enforce SSE-KMS.

A76.
Answer: C) IAM policy condition with aws:SourceVpc
Explanation: This ensures the action can only be performed if the Lambda invocation comes from the specified VPC.

A77.
Answer: C) Sets up a secure multi-account landing zone with guardrails
Explanation: Control Tower automates secure account provisioning and enforces policies with preconfigured guardrails.

A78.
Answer: C) AWS Service Catalog
Explanation: Service Catalog allows administrators to define pre-approved products that users can deploy, enforcing standards.

A79.
Answer: B) Envelope encryption
Explanation: AWS uses envelope encryption to encrypt data with a data key, and protects that data key with a CMK.

A80.
Answer: B) Use CloudWatch Logs Insights
Explanation: CloudWatch Logs Insights allows fast querying of Flow Logs using filter expressions for immediate analysis.

Questions 81–90

Q81.
You are building a security automation that triggers on a GuardDuty finding. What service should you use to route that finding and invoke a Lambda function?

A) AWS Config
B) Amazon SQS
C) Amazon EventBridge
D) AWS Systems Manager

Q82.
Which IAM condition ensures that **only encrypted connections** are used when accessing S3?

A) aws:SecureTransport
B) aws:CurrentTime
C) s3:EncryptionRequired
D) aws:MultiFactorAuthPresent

Q83.
What AWS service allows you to **generate temporary credentials** for a user authenticated through an enterprise identity provider (IdP)?

A) AWS SSO
B) AWS Directory Service
C) AWS STS
D) AWS Shield

Q84.
A company wants to detect **large-scale object downloads** from an S3 bucket containing sensitive data. What service should they use?

A) AWS Config
B) Amazon Macie
C) Amazon CloudWatch
D) AWS IAM Access Analyzer

Q85.
You want to identify **vulnerable packages** in EC2 instances across your fleet. What should you use?

A) AWS Config
B) AWS Inspector
C) CloudWatch Logs
D) IAM Credential Report

Q86.
What type of IAM policy allows cross-account access by **specifying who** can access a resource?

A) Identity-based policy
B) Resource-based policy
C) Trust policy
D) Inline policy

Q87.
A developer is pushing code to an ECR repository. You want to ensure **malicious or vulnerable images** are blocked. Which AWS feature helps?

A) VPC Flow Logs
B) IAM Policy
C) ECR image scanning with Amazon Inspector
D) CloudTrail Data Events

Q88.
What AWS feature allows you to detect **sudden spikes** in API activity such as TerminateInstances or CreateUser?

A) GuardDuty
B) CloudTrail Insights
C) Security Hub
D) IAM Access Analyzer

Q89.
You want to allow access to an S3 bucket only for users who authenticate using **multi-factor authentication**. What should you use?

A) ACLs
B) KMS Key Policy
C) IAM Policy Condition aws:MultiFactorAuthPresent
D) s3:SecureTransport

Q90.
Which feature of Amazon S3 enables **legal hold** or **WORM storage** for regulatory compliance?

A) MFA Delete
B) Object Lock
C) S3 Access Analyzer
D) Lifecycle Policies

Answers 81–90

A81.
Answer: C) Amazon EventBridge
Explanation: GuardDuty findings are sent to EventBridge, where they can trigger Lambda functions or workflows.

A82.
Answer: A) aws:SecureTransport
Explanation: This condition ensures requests are made over HTTPS and denies HTTP connections.

A83.
Answer: C) AWS STS
Explanation: Security Token Service issues temporary credentials after federated authentication via an IdP.

A84.
Answer: B) Amazon Macie
Explanation: Macie can detect unusual download patterns, especially for sensitive data in S3.

A85.
Answer: B) AWS Inspector
Explanation: Inspector scans EC2 instances for software vulnerabilities, exposed ports, and CVEs.

A86.
Answer: B) Resource-based policy
Explanation: Resource-based policies include a Principal field and allow specifying who can access the resource.

A87.
Answer: C) ECR image scanning with Amazon Inspector
Explanation: Inspector integrates with ECR to scan images for known vulnerabilities on push.

A88.
Answer: B) CloudTrail Insights
Explanation: CloudTrail Insights detects anomalous patterns in API usage such as spikes in actions.

A89.
Answer: C) IAM Policy Condition aws:MultiFactorAuthPresent
Explanation: This ensures that only requests authenticated with MFA are allowed.

A90.
Answer: B) Object Lock
Explanation: Object Lock enforces WORM (Write Once Read Many) and legal hold for S3 objects.

Questions 91–100

Q91.
A company needs to detect **when IAM policies are changed** and automatically notify the security team. What's the best solution?

A) Enable AWS Config rule iam-policy-changed
B) Use CloudTrail with CloudWatch Logs and Alarms
C) Use IAM Credential Reports
D) Use GuardDuty

Q92.
Which service helps organizations **generate audit evidence** aligned to compliance frameworks like ISO 27001 and PCI-DSS?

A) AWS Config
B) AWS CloudTrail
C) AWS Audit Manager
D) AWS Artifact

Q93.
You need to **rotate a secret** stored in Secrets Manager automatically every 30 days. What must you configure?

A) KMS Key rotation
B) Rotation schedule and Lambda function
C) SSM Document and IAM user
D) Secrets Manager with MFA

Q94.
You are designing a secure environment and want to ensure the EC2 instance metadata service cannot be used to retrieve credentials by malware. What's the best practice?

A) Use instance metadata version 2 (IMDSv2)
B) Use Secrets Manager for all credentials
C) Encrypt the root volume
D) Use public AMIs

Q95.
Which AWS service lets you enforce a **resource configuration standard** like “RDS must not be publicly accessible”?

A) AWS WAF
B) AWS Config
C) GuardDuty
D) IAM Access Analyzer

Q96.
Which AWS service offers **built-in support for automatic DDoS mitigation** at no extra cost?

A) AWS WAF
B) Amazon Shield Advanced
C) Amazon CloudFront
D) Amazon Shield Standard

Q97.
What is the **difference between a key policy and IAM policy** in AWS KMS?

A) IAM policies apply only to root, key policies apply to users
B) Key policies are optional
C) Key policies control KMS keys directly; IAM policies supplement them
D) Key policies use SAML

Q98.
Which feature of IAM Identity Center (AWS SSO) helps implement **least privilege** across multiple AWS accounts?

A) IAM user federation
B) Permission sets
C) KMS key grants
D) Credential reports

Q99.
A team wants to track the **lifecycle of S3 objects** and automatically archive them after 90 days. What should they use?

A) S3 Object Lock
B) S3 Glacier Vault Lock

C) S3 Lifecycle Policy
D) CloudTrail

Q100.
A company wants to prevent any **data transfer from EC2 instances to external endpoints**. Which solution is best?

A) Remove the instance's IAM role
B) Use Network ACLs to deny all egress
C) Use S3 Bucket Policies
D) Enable VPC Flow Logs

Answers 91–100

A91.
Answer: B) Use CloudTrail with CloudWatch Logs and Alarms
Explanation: CloudTrail records IAM changes, and CloudWatch metric filters can alert on policy change events like Put*Policy.

A92.
Answer: C) AWS Audit Manager
Explanation: Audit Manager automates evidence collection and aligns with compliance standards like ISO and PCI.

A93.
Answer: B) Rotation schedule and Lambda function
Explanation: Secrets Manager uses Lambda to automate secret rotation on a defined schedule.

A94.
Answer: A) Use instance metadata version 2 (IMDSv2)
Explanation: IMDSv2 adds protection against SSRF attacks and requires session-based tokens for metadata access.

A95.
Answer: B) AWS Config

Explanation: AWS Config can evaluate resource compliance with rules like “RDS must not be public.”

A96.
Answer: D) Amazon Shield Standard
Explanation: Shield Standard provides automatic, free DDoS protection for AWS infrastructure and services.

A97.
Answer: C) Key policies control KMS keys directly; IAM policies supplement them
Explanation: Key policies are the primary access control for KMS keys; IAM policies are evaluated only if allowed by the key policy.

A98.
Answer: B) Permission sets
Explanation: IAM Identity Center uses permission sets to define roles and permissions centrally across accounts.

A99.
Answer: C) S3 Lifecycle Policy
Explanation: Lifecycle policies automatically transition or delete objects after a defined period (e.g., 90 days).

A100.
Answer: B) Use Network ACLs to deny all egress
Explanation: NACLs at the subnet level can block outbound traffic completely, enforcing no external access.