

Content outline

This exam guide includes weightings, content domains, and task statements for the exam. This guide does not provide a comprehensive list of the content on the exam. However, additional context for each task statement is available to help you prepare for the exam.

The exam has the following content domains and weightings:

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

Domain 1: Threat Detection and Incident Response

Task Statement 1.1: Design and implement an incident response plan.

Knowledge of:

- AWS best practices for incident response
- Cloud incidents
- Roles and responsibilities in the incident response plan
- AWS Security Finding Format (ASFF)

Skills in:

- Implementing credential invalidation and rotation strategies in response to compromises (for example, by using AWS Identity and Access Management [IAM] and AWS Secrets Manager)
- Isolating AWS resources
- Designing and implementing playbooks and runbooks for responses to security incidents
- Deploying security services (for example, AWS Security Hub, Amazon Macie, Amazon GuardDuty, Amazon Inspector, AWS Config, Amazon Detective, AWS Identity and Access Management Access Analyzer)
- Configuring integrations with native AWS services and third-party services (for example, by using Amazon EventBridge and the ASFF)

Task Statement 1.2: Detect security threats and anomalies by using AWS services.

Knowledge of:

- AWS managed security services that detect threats
- Anomaly and correlation techniques to join data across services
- Visualizations to identify anomalies
- Strategies to centralize security findings

Skills in:

- Evaluating findings from security services (for example, GuardDuty, Security Hub, Macie, AWS Config, IAM Access Analyzer)
- Searching and correlating security threats across AWS services (for example, by using Detective)
- Performing queries to validate security events (for example, by using Amazon Athena)
- Creating metric filters and dashboards to detect anomalous activity (for example, by using Amazon CloudWatch)

Task Statement 1.3: Respond to compromised resources and workloads.

Knowledge of:

- AWS Security Incident Response Guide
- Resource isolation mechanisms
- Techniques for root cause analysis
- Data capture mechanisms
- Log analysis for event validation

Skills in:

- Automating remediation by using AWS services (for example, AWS Lambda, AWS Step Functions, EventBridge, AWS Systems Manager runbooks, Security Hub, AWS Config)
- Responding to compromised resources (for example, by isolating Amazon EC2 instances)
- Investigating and analyzing to conduct root cause analysis (for example, by using Detective)
- Capturing relevant forensics data from a compromised resource (for example, Amazon Elastic Block Store [Amazon EBS] volume snapshots, memory dump)
- Querying logs in Amazon S3 for contextual information related to security events (for example, by using Athena)
- Protecting and preserving forensic artifacts (for example, by using S3 Object Lock, isolated forensic accounts, S3 Lifecycle, and S3 replication)
- Preparing services for incidents and recovering services after incidents

Domain 2: Security Logging and Monitoring

Task Statement 2.1: Design and implement monitoring and alerting to address security events.

Knowledge of:

- AWS services that monitor events and provide alarms (for example, CloudWatch, EventBridge)
- AWS services that automate alerting (for example, Lambda, Amazon Simple Notification Service [Amazon SNS], Security Hub)
- Tools that monitor metrics and baselines (for example, GuardDuty, Systems Manager)

Skills in:

- Analyzing architectures to identify monitoring requirements and sources of data for security monitoring
- Analyzing environments and workloads to determine monitoring requirements
- Designing environment monitoring and workload monitoring based on business and security requirements
- Setting up automated tools and scripts to perform regular audits (for example, by creating custom insights in Security Hub)
- Defining the metrics and thresholds that generate alerts

Task Statement 2.2: Troubleshoot security monitoring and alerting.

Knowledge of:

- Configuration of monitoring services (for example, Security Hub)
- Relevant data that indicates security events

Skills in:

- Analyzing the service functionality, permissions, and configuration of resources after an event that did not provide visibility or alerting
- Analyzing and remediating the configuration of a custom application that is not reporting its statistics
- Evaluating logging and monitoring services for alignment with security requirements

Task Statement 2.3: Design and implement a logging solution.

Knowledge of:

- AWS services and features that provide logging capabilities (for example, VPC Flow Logs, DNS logs, AWS CloudTrail, Amazon CloudWatch Logs)
- Attributes of logging capabilities (for example, log levels, type, verbosity)
- Log destinations and lifecycle management (for example, retention period)

Skills in:

- Configuring logging for services and applications
- Identifying logging requirements and sources for log ingestion
- Implementing log storage and lifecycle management according to AWS best practices and organizational requirements

Task Statement 2.4: Troubleshoot logging solutions.**Knowledge of:**

- Capabilities and use cases of AWS services that provide data sources (for example, log level, type, verbosity, cadence, timeliness, immutability)
- AWS services and features that provide logging capabilities (for example, VPC Flow Logs, DNS logs, CloudTrail, CloudWatch Logs)
- Access permissions that are necessary for logging

Skills in:

- Identifying misconfiguration and determining remediation steps for absent access permissions that are necessary for logging (for example, by managing read/write permissions, S3 bucket permissions, public access, and integrity)
- Determining the cause of missing logs and performing remediation steps

Task Statement 2.5: Design a log analysis solution.**Knowledge of:**

- Services and tools to analyze captured logs (for example, Athena, CloudWatch Logs filter)
- Log analysis features of AWS services (for example, CloudWatch Logs Insights, CloudTrail Insights, Security Hub insights)
- Log format and components (for example, CloudTrail logs)

Skills in:

- Identifying patterns in logs to indicate anomalies and known threats
- Normalizing, parsing, and correlating logs

Domain 3: Infrastructure Security

Task Statement 3.1: Design and implement security controls for edge services.

Knowledge of:

- Security features on edge services (for example, AWS WAF, load balancers, Amazon Route 53, Amazon CloudFront, AWS Shield)
- Common attacks, threats, and exploits (for example, Open Web Application Security Project [OWASP] Top 10, DDoS)
- Layered web application architecture

Skills in:

- Defining edge security strategies for common use cases (for example, public website, serverless app, mobile app backend)
- Selecting appropriate edge services based on anticipated threats and attacks (for example, OWASP Top 10, DDoS)
- Selecting appropriate protections based on anticipated vulnerabilities and risks (for example, vulnerable software, applications, libraries)
- Defining layers of defense by combining edge security services (for example, CloudFront with AWS WAF and load balancers)
- Applying restrictions at the edge based on various criteria (for example, geography, geolocation, rate limit)
- Activating logs, metrics, and monitoring around edge services to indicate attacks

Task Statement 3.2: Design and implement network security controls.

Knowledge of:

- VPC security mechanisms (for example, security groups, network ACLs, AWS Network Firewall)
- Inter-VPC connectivity (for example, AWS Transit Gateway, VPC endpoints)
- Security telemetry sources (for example, Traffic Mirroring, VPC Flow Logs)
- VPN technology, terminology, and usage
- On-premises connectivity options (for example, AWS VPN, AWS Direct Connect)

Skills in:

- Implementing network segmentation based on security requirements (for example, public subnets, private subnets, sensitive VPCs, on-premises connectivity)
- Designing network controls to permit or prevent network traffic as required (for example, by using security groups, network ACLs, and Network Firewall)
- Designing network flows to keep data off the public internet (for example, by using Transit Gateway, VPC endpoints, and Lambda in VPCs)

- Determining which telemetry sources to monitor based on network design, threats, and attacks (for example, load balancer logs, VPC Flow Logs, Traffic Mirroring)
- Determining redundancy and security workload requirements for communication between on-premises environments and the AWS Cloud (for example, by using AWS VPN, AWS VPN over Direct Connect, and MACsec)
- Identifying and removing unnecessary network access
- Managing network configurations as requirements change (for example, by using AWS Firewall Manager)

Task Statement 3.3: Design and implement security controls for compute workloads.

Knowledge of:

- Provisioning and maintenance of EC2 instances (for example, patching, inspecting, creation of snapshots and AMIs, use of EC2 Image Builder)
- IAM instance roles and IAM service roles
- Services that scan for vulnerabilities in compute workloads (for example, Amazon Inspector, Amazon Elastic Container Registry [Amazon ECR])
- Host-based security (for example, firewalls, hardening)

Skills in:

- Creating hardened EC2 AMIs
- Applying instance roles and service roles as appropriate to authorize compute workloads
- Scanning EC2 instances and container images for known vulnerabilities
- Applying patches across a fleet of EC2 instances or container images
- Activating host-based security mechanisms (for example, host-based firewalls)
- Analyzing Amazon Inspector findings and determining appropriate mitigation techniques
- Passing secrets and credentials securely to compute workloads

Task Statement 3.4: Troubleshoot network security.

Knowledge of:

- How to analyze reachability (for example, by using VPC Reachability Analyzer and Amazon Inspector)
 - Fundamental TCP/IP networking concepts (for example, UDP compared with TCP, ports, Open Systems Interconnection [OSI] model, network operating system utilities)
- How to read relevant log sources (for example, Route 53 logs, AWS WAF logs, VPC Flow Logs)

Skills in:

- Identifying, interpreting, and prioritizing problems in network connectivity (for example, by using Amazon Inspector Network Reachability)
- Determining solutions to produce desired network behavior
- Analyzing log sources to identify problems
- Capturing traffic samples for problem analysis (for example, by using Traffic Mirroring)

Domain 4: Identity and Access Management**Task Statement 4.1: Design, implement, and troubleshoot authentication for AWS resources.****Knowledge of:**

- Methods and services for creating and managing identities (for example, federation, identity providers, AWS IAM Identity Center [AWS Single Sign-On], Amazon Cognito)
- Long-term and temporary credentialing mechanisms
- How to troubleshoot authentication issues (for example, by using CloudTrail, IAM Access Advisor, and IAM policy simulator)

Skills in:

- Establishing identity through an authentication system, based on requirements
- Setting up multi-factor authentication (MFA)
- Determining when to use AWS Security Token Service (AWS STS) to issue temporary credentials

Task Statement 4.2: Design, implement, and troubleshoot authorization for AWS resources.**Knowledge of:**

- Different IAM policies (for example, managed policies, inline policies, identity-based policies, resource-based policies, session control policies)
- Components and impact of a policy (for example, Principal, Action, Resource, Condition)
- How to troubleshoot authorization issues (for example, by using CloudTrail, IAM Access Advisor, and IAM policy simulator)

Skills in:

- Constructing attribute-based access control (ABAC) and role-based access control (RBAC) strategies
- Evaluating IAM policy types for given requirements and workloads
- Interpreting an IAM policy's effect on environments and workloads
- Applying the principle of least privilege across an environment
- Enforcing proper separation of duties
- Analyzing access or authorization errors to determine cause or effect
- Investigating unintended permissions, authorization, or privileges granted to a resource, service, or entity

Domain 5: Data Protection

Task Statement 5.1: Design and implement controls that provide confidentiality and integrity for data in transit.

Knowledge of:

- TLS concepts
- VPN concepts (for example, IPsec)
- Secure remote access methods (for example, SSH, RDP over Systems Manager Session Manager)
- Systems Manager Session Manager concepts
- How TLS certificates work with various network services and resources (for example, CloudFront, load balancers)

Skills in:

- Designing secure connectivity between AWS and on-premises networks (for example, by using Direct Connect and VPN gateways)
- Designing mechanisms to require encryption when connecting to resources (for example, Amazon RDS, Amazon Redshift, CloudFront, Amazon S3, Amazon DynamoDB, load balancers, Amazon Elastic File System [Amazon EFS], Amazon API Gateway)
- Requiring TLS for AWS API calls (for example, with Amazon S3)
- Designing mechanisms to forward traffic over secure connections (for example, by using Systems Manager and EC2 Instance Connect)
- Designing cross-Region networking by using private VIFs and public VIFs

Task Statement 5.2: Design and implement controls that provide confidentiality and integrity for data at rest.

Knowledge of:

- Encryption technique selection (for example, client-side, server-side, symmetric, asymmetric)
- Integrity-checking techniques (for example, hashing algorithms, digital signatures)
- Resource policies (for example, for DynamoDB, Amazon S3, and AWS Key Management Service [AWS KMS])
- IAM roles and policies

Skills in:

- Designing resource policies to restrict access to authorized users (for example, S3 bucket policies, DynamoDB policies)
- Designing mechanisms to prevent unauthorized public access (for example, S3 Block Public Access, prevention of public snapshots and public AMIs)

- Configuring services to activate encryption of data at rest (for example, Amazon S3, Amazon RDS, DynamoDB, Amazon Simple Queue Service [Amazon SQS], Amazon EBS, Amazon EFS)
- Designing mechanisms to protect data integrity by preventing modifications (for example, by using S3 Object Lock, KMS key policies, S3 Glacier Vault Lock, and AWS Backup Vault Lock)
- Designing encryption at rest by using AWS CloudHSM for relational databases (for example, Amazon RDS, RDS Custom, databases on EC2 instances)
- Choosing encryption techniques based on business requirements

Task Statement 5.3: Design and implement controls to manage the lifecycle of data at rest.

Knowledge of:

- Lifecycle policies
- Data retention standards

Skills in:

- Designing S3 Lifecycle mechanisms to retain data for required retention periods (for example, S3 Object Lock, S3 Glacier Vault Lock, S3 Lifecycle policy)
- Designing automatic lifecycle management for AWS services and resources (for example, Amazon S3, EBS volume snapshots, RDS volume snapshots, AMIs, container images, CloudWatch log groups, Amazon Data Lifecycle Manager)
- Establishing schedules and retention for AWS Backup across AWS services

Task Statement 5.4: Design and implement controls to protect credentials, secrets, and cryptographic key materials.

Knowledge of:

- Secrets Manager
- Systems Manager Parameter Store
- Usage and management of symmetric keys and asymmetric keys (for example, AWS KMS)

Skills in:

- Designing management and rotation of secrets for workloads (for example, database access credentials, API keys, IAM access keys, AWS KMS customer managed keys)
- Designing KMS key policies to limit key usage to authorized users
- Establishing mechanisms to import and remove customer-provided key material

Domain 6: Management and Security Governance

Task Statement 6.1: Develop a strategy to centrally deploy and manage AWS accounts.

Knowledge of:

- Multi-account strategies
- Managed services that allow delegated administration
- Policy-defined guardrails
- Root account best practices
- Cross-account roles

Skills in:

- Deploying and configuring AWS Organizations
- Determining when and how to deploy AWS Control Tower (for example, which services must be deactivated for successful deployment)
- Implementing SCPs as a technical solution to enforce a policy (for example, limitations on the use of a root account, implementation of controls in AWS Control Tower)
- Centrally managing security services and aggregating findings (for example, by using delegated administration and AWS Config aggregators)
- Securing AWS account root user credentials

Task Statement 6.2: Implement a secure and consistent deployment strategy for cloud resources.

Knowledge of:

- Deployment best practices with infrastructure as code (IaC) (for example, AWS CloudFormation template hardening and drift detection)
- Best practices for tagging
- Centralized management, deployment, and versioning of AWS services
- Visibility and control over AWS infrastructure

Skills in:

- Using CloudFormation to deploy cloud resources consistently and securely
- Implementing and enforcing multi-account tagging strategies
- Configuring and deploying portfolios of approved AWS services (for example, by using AWS Service Catalog)
- Organizing AWS resources into different groups for management
- Deploying Firewall Manager to enforce policies
- Securely sharing resources across AWS accounts (for example, by using AWS Resource Access Manager [AWS RAM])

Task Statement 6.3: Evaluate the compliance of AWS resources.

Knowledge of:

- Data classification by using AWS services
- How to assess, audit, and evaluate the configurations of AWS resources (for example, by using AWS Config)

Skills in:

- Identifying sensitive data by using Macie
- Creating AWS Config rules for detection of noncompliant AWS resources
- Collecting and organizing evidence by using Security Hub and AWS Audit Manager

Task Statement 6.4: Identify security gaps through architectural reviews and cost analysis.

Knowledge of:

- AWS cost and usage for anomaly identification
- Strategies to reduce attack surfaces
- AWS Well-Architected Framework

Skills in:

- Identifying anomalies based on resource utilization and trends
- Identifying unused resources by using AWS services and tools (for example, AWS Trusted Advisor, AWS Cost Explorer)
- Using the AWS Well-Architected Tool to identify security gaps