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 65 questions that affect your score.

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: SDLC Automation (22% of scored content)
- Domain 2: Configuration Management and IaC (17% of scored content)
- Domain 3: Resilient Cloud Solutions (15% of scored content)
- Domain 4: Monitoring and Logging (15% of scored content)
- Domain 5: Incident and Event Response (14% of scored content)
- Domain 6: Security and Compliance (17% of scored content)

Domain 1: SDLC Automation

Task Statement 1.1: Implement CI/CD pipelines.

Knowledge of:

- Software development lifecycle (SDLC) concepts, phases, and models
- Pipeline deployment patterns for single- and multi-account environments

Skills in:

- Configuring code, image, and artifact repositories
- Using version control to integrate pipelines with application environments
- Setting up build processes (for example, AWS CodeBuild)
- Managing build and deployment secrets (for example, AWS Secrets Manager, AWS Systems Manager Parameter Store)
- Determining appropriate deployment strategies (for example, AWS CodeDeploy)

Task Statement 1.2: Integrate automated testing into CI/CD pipelines.

Knowledge of:

• Different types of tests (for example, unit tests, integration tests, acceptance tests, user interface tests, security scans)

• Reasonable use of different types of tests at different stages of the CI/CD pipeline

Skills in:

• Running builds or tests when generating pull requests or code merges (for example, CodeBuild)

• Running load/stress tests, performance benchmarking, and application testing at scale

• Measuring application health based on application exit codes

• Automating unit tests and code coverage

• Invoking AWS services in a pipeline for testing

Task Statement 1.3: Build and manage artifacts.

Knowledge of:

• Artifact use cases and secure management

• Methods to create and generate artifacts

• Artifact lifecycle considerations

Skills in:

• Creating and configuring artifact repositories (for example, AWS CodeArtifact, Amazon S3, Amazon Elastic Container Registry [Amazon ECR])

• Configuring build tools for generating artifacts (for example, CodeBuild, AWS Lambda)

• Automating Amazon EC2 instance and container image build processes (for example, EC2 Image Builder)

Task Statement 1.4: Implement deployment strategies for instance, container, and serverless environments.

Knowledge of:

• Deployment methodologies for various platforms (for example, Amazon EC2, Amazon Elastic Container Service [Amazon ECS], Amazon Elastic Kubernetes Service [Amazon EKS], Lambda)

• Application storage patterns (for example, Amazon Elastic File System [Amazon EFS], Amazon S3, Amazon Elastic Block Store [Amazon EBS])

• Mutable deployment patterns in contrast to immutable deployment patterns

• Tools and services available for distributing code (for example, CodeDeploy, EC2 Image Builder)

Skills in:

• Configuring security permissions to allow access to artifact repositories (for example, AWS Identity and Access Management [IAM], CodeArtifact)

• Configuring deployment agents (for example, CodeDeploy agent)

• Troubleshooting deployment issues

• Using different deployment methods (for example, blue/green, canary

Domain 2: Configuration Management and IaC

Task Statement 2.1: Define cloud infrastructure and reusable components to provision and manage systems throughout their lifecycle.

Knowledge of:

• Infrastructure as code (IaC) options and tools for AWS

• Change management processes for IaC-based platforms

• Configuration management services and strategies

Skills in:

• Composing and deploying IaC templates (for example, AWS Serverless Application Model [AWS SAM], AWS CloudFormation, AWS Cloud Development Kit [AWS CDK])

• Applying CloudFormation StackSets across multiple accounts and AWS Regions

• Determining optimal configuration management services (for example, AWS OpsWorks, AWS Systems Manager, AWS Config, AWS AppConfig)

• Implementing infrastructure patterns, governance controls, and security standards into reusable IaC templates (for example, AWS Service Catalog, CloudFormation modules, AWS CDK)

Task Statement 2.2: Deploy automation to create, onboard, and secure AWS accounts in a multi-account or multi-Region environment.

Knowledge of:

• AWS account structures, best practices, and related AWS services

Skills in:

• Standardizing and automating account provisioning and configuration

• Creating, consolidating, and centrally managing accounts (for example, AWS Organizations, AWS Control Tower)

• Applying IAM solutions for multi-account and complex organization structures (for example, SCPs, assuming roles)

• Implementing and developing governance and security controls at scale (AWS Config, AWS Control Tower, AWS Security Hub, Amazon Detective, Amazon GuardDuty, AWS Service Catalog, SCPs)

Task Statement 2.3: Design and build automated solutions for complex tasks and large-scale environments.

Knowledge of:

• AWS services and solutions to automate tasks and processes

• Methods and strategies to interact with the AWS software-defined infrastructure

Skills in:

• Automating system inventory, configuration, and patch management (for example, Systems Manager, AWS Config)

• Developing Lambda function automations for complex scenarios (for example, AWS SDKs, Lambda, AWS Step Functions)

• Automating the configuration of software applications to the desired state (for example, OpsWorks, Systems Manager State Manager)

• Maintaining software compliance (for example, Systems Manager) Domain 3: Resilient Cloud Solutions

Task Statement 3.1: Implement highly available solutions to meet resilience and business requirements.

Knowledge of:

• Multi-AZ and multi-Region deployments (for example, compute layer, data layer)

• SLAs

• Replication and failover methods for stateful services

• Techniques to achieve high availability (for example, Multi-AZ, multi-Region)

Skills in:

• Translating business requirements into technical resiliency needs

• Identifying and remediating single points of failure in existing workloads

• Enabling cross-Region solutions where available (for example, Amazon DynamoDB, Amazon RDS, Amazon Route 53, Amazon S3, Amazon CloudFront)

• Configuring load balancing to support cross-AZ services

• Configuring applications and related services to support multiple Availability Zones and Regions while minimizing downtime

Task Statement 3.2: Implement solutions that are scalable to meet business requirements.

Knowledge of:

• Appropriate metrics for scaling services

• Loosely coupled and distributed architectures

• Serverless architectures

• Container platforms

Skills in:

• Identifying and remediating scaling issues

• Identifying and implementing appropriate auto scaling, load balancing, and caching solutions

• Deploying container-based applications (for example, Amazon ECS, Amazon EKS)

• Deploying workloads in multiple Regions for global scalability

• Configuring serverless applications (for example, Amazon API Gateway, Lambda, AWS Fargate)

Task Statement 3.3: Implement automated recovery processes to meet RTO and RPO requirements.

Knowledge of:

• Disaster recovery concepts (for example, RTO, RPO)

• Backup and recovery strategie

s (for example, pilot light, warm standby)

• Recovery procedures

Skills in:

• Testing failover of Multi-AZ and multi-Region workloads (for example, Amazon RDS, Amazon Aurora, Route 53, CloudFront)

• Identifying and implementing appropriate cross-Region backup and recovery strategies (for example, AWS Backup, Amazon S3, Systems Manager)

• Configuring a load balancer to recover from backend failure

Domain 4: Monitoring and Logging

Task Statement 4.1: Configure the collection, aggregation, and storage of logs and metrics.

Knowledge of:

• How to monitor applications and infrastructure

• Amazon CloudWatch metrics (for example, namespaces, metrics, dimensions, and resolution)

• Real-time log ingestion

• Encryption options for at-rest and in-transit logs and metrics (for example, client-side and server-side, AWS Key Management Service [AWS KMS])

• Security configurations (for example, IAM roles and permissions to allow for log collection)

Skills in:

• Securely storing and managing logs

• Creating CloudWatch metrics from log events by using metric filters

• Creating CloudWatch metric streams (for example, Amazon S3 or Amazon Kinesis Data Firehose options)

• Collecting custom metrics (for example, using the CloudWatch agent)

• Managing log storage lifecycles (for example, S3 lifecycles, CloudWatch log group retention)

• Processing log data by using CloudWatch log subscriptions (for example, Kinesis, Lambda, Amazon OpenSearch Service)

• Searching log data by using filter and pattern syntax or CloudWatch Logs Insights

• Configuring encryption of log data (for example, AWS KMS)

Task Statement 4.2: Audit, monitor, and analyze logs and metrics to detect issues.

Knowledge of:

• Anomaly detection alarms (for example, CloudWatch anomaly detection)

• Common CloudWatch metrics and logs (for example, CPU utilization with Amazon EC2, queue length with Amazon RDS, 5xx errors with an Application Load Balancer [ALB])

• Amazon Inspector and common assessment templates

• AWS Config rules

• AWS CloudTrail log events

Skills in:

• Building CloudWatch dashboards and Amazon QuickSight visualizations

• Associating CloudWatch alarms with CloudWatch metrics (standard and custom)

• Configuring AWS X-Ray for different services (for example, containers, API Gateway, Lambda)

• Analyzing real-time log streams (for example, using Kinesis Data Streams)

• Analyzing logs with AWS services (for example, Amazon Athena, CloudWatch Logs Insights)

Task Statement 4.3: Automate monitoring and event management of complex environments.

Knowledge of:

• Event-driven, asynchronous design patterns (for example, S3 Event Notifications or Amazon EventBridge events to Amazon Simple Notification Service [Amazon SNS] or Lambda)

• Capabilities of auto scaling for a variety of AWS services (for example, EC2 Auto Scaling groups, RDS storage auto scaling, DynamoDB, ECS capacity provider, EKS autoscalers)

• Alert notification and action capabilities (for example, CloudWatch alarms to Amazon SNS, Lambda, EC2 automatic recovery)

• Health check capabilities in AWS services (for example, ALB target groups, Route 53)

Skills in:

• Configuring solutions for auto scaling (for example, DynamoDB, EC2 Auto Scaling groups, RDS storage auto scaling, ECS capacity provider)

• Creating CloudWatch custom metrics and metric filters, alarms, and notifications (for example, Amazon SNS, Lambda)

• Configuring S3 events to process log files (for example, by using Lambda) and deliver log files to another destination (for example, OpenSearch Service, CloudWatch Logs)

• Configuring EventBridge to send notifications based on a particular event pattern

• Installing and configuring agents on EC2 instances (for example, AWS Systems Manager Agent [SSM Agent], CloudWatch agent)

• Configuring AWS Config rules to remediate issues

• Configuring health checks (for example, Route 53, ALB)

Domain 5: Incident and Event Response

Task Statement 5.1: Manage event sources to process, notify, and take action in response to events.

Knowledge of:

• AWS services that generate, capture, and process events (for example, AWS Health, EventBridge, CloudTrail)

• Event-driven architectures (for example, fan out, event streaming, queuing)

Skills in:

• Integrating AWS event sources (for example, AWS Health, EventBridge, CloudTrail)

• Building event processing workflows (for example, Amazon Simple Queue Service [Amazon SQS], Kinesis, Amazon SNS, Lambda, Step Functions)

Task Statement 5.2: Implement configuration changes in response to events.

Knowledge of:

• Fleet management services (for example, Systems Manager, AWS Auto Scaling)

• Configuration management services (for example, AWS Config)

Skills in:

• Applying configuration changes to systems

• Modifying infrastructure configurations in response to events

• Remediating a non-desired system state

Task Statement 5.3: Troubleshoot system and application failures.

Knowledge of:

• AWS metrics and logging services (for example, CloudWatch, X-Ray)

• AWS service health services (for example, AWS Health, CloudWatch, Systems Manager OpsCenter)

• Root cause analysis

Skills in:

• Analyzing failed deployments (for example, AWS CodePipeline, CodeBuild, CodeDeploy, CloudFormation, CloudWatch synthetic monitoring)

• Analyzing incidents regarding failed processes (for example, auto scaling, Amazon ECS, Amazon EKS)
Domain 6: Security and Compliance

Task Statement 6.1: Implement techniques for identity and access management at scale.

Knowledge of:

• Appropriate usage of different IAM entities for human and machine access (for example, users, groups, roles, identity providers, identity-based policies, resource-based policies, session policies)

• Identity federation techniques (for example, using IAM identity providers and AWS IAM Identity Center)

• Permission management delegation by using IAM permissions boundaries

• Organizational SCPs

Skills in:

• Designing policies to enforce least privilege access

• Implementing role-based and attribute-based access control patterns

• Automating credential rotation for machine identities (for example, Secrets Manager)

• Managing permissions to control access to human and machine identities (for example, enabling multi-factor authentication [MFA], AWS Security Token Service [AWS STS], IAM profiles)

Task Statement 6.2: Apply automation for security controls and data protection.

Knowledge of:

• Network security components (for example, security groups, network ACLs, routing, AWS Network Firewall, AWS WAF, AWS Shield)

• Certificates and public key infrastructure (PKI)

• Data management (for example, data classification, encryption, key management, access controls)

Skills in:

• Automating the application of security controls in multi-account and multi-Region environments (for example, Security Hub, Organizations, AWS Control Tower, Systems Manager)

• Combining security controls to apply defense in depth (for example, AWS Certificate Manager [ACM], AWS WAF, AWS Config, AWS Config rules, Security Hub, GuardDuty, security groups, network ACLs, Amazon Detective, Network Firewall)

• Automating the discovery of sensitive data at scale (for example, Amazon Macie)

• Encrypting data in transit and data at rest (for example, AWS KMS, AWS CloudHSM, ACM)

Task Statement 6.3: Implement security monitoring and auditing solutions.

Knowledge of:

• Security auditing services and features (for example, CloudTrail, AWS Config, VPC Flow Logs, CloudFormation drift detection)

• AWS services for identifying security vulnerabilities and events (for example, GuardDuty, Amazon Inspector, IAM Access Analyzer, AWS Config)

• Common cloud security threats (for example, insecure web traffic, exposed AWS access keys, S3 buckets with public access enabled or encryption disabled)

Skills in:

• Implementing robust security auditing

• Configuring alerting based on unexpected or anomalous security events

• Configuring service and application logging (for example, CloudTrail, CloudWatch Logs)

• Analyzing logs, metrics, and security findings