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: Network Design (30% of scored content)

• Domain 2: Network Implementation (26% of scored content)

• Domain 3: Network Management and Operation (20% of scored content)

• Domain 4: Network Security, Compliance, and Governance (24% of scored content)

Domain 1: Network Design Task Statement

1.1: Design a solution that incorporates edge network services to optimize user performance and traffic management for global architectures.

Knowledge of:

• Design patterns for the usage of content distribution networks (for example, Amazon CloudFront)
• Design patterns for global traffic management (for example, AWS Global Accelerator)

• Integration patterns for content distribution networks and global traffic management with other services (for example, Elastic Load Balancing [ELB], Amazon API Gateway)

Skills in:

• Evaluating requirements of global inbound and outbound traffic from the internet to design an appropriate content distribution solution

Task Statement 1.2: Design DNS solutions that meet public, private, and hybrid requirements.

Knowledge of:

• DNS protocol (for example, DNS records, TTL, DNSSEC, DNS delegation, zones)

• DNS logging and monitoring

• Amazon Route 53 features (for example, alias records, traffic policies, resolvers, health checks)

• Integration of Route 53 with other AWS networking services (for example, Amazon VPC)

• Integration of Route 53 with hybrid, multi-account, and multi-Region options

• Domain registration

Skills in:

• Using Route 53 public hosted zones

• Using Route 53 private hosted zones

• Using Route 53 Resolver endpoints in hybrid and AWS architectures

• Using Route 53 for global traffic management

• Creating and managing domain registrations

Task Statement 1.3: Design solutions that integrate load balancing to meet high availability, scalability, and security requirements.

Knowledge of:

• How load balancing works at layer 3, layer 4, and layer 7 of the OSI model

• Different types of load balancers and how they meet requirements for network design, high availability, and security

• Connectivity patterns that apply to load balancing based on the use case (for example, internal load balancers, external load balancers)

• Scaling factors for load balancers

• Integrations of load balancers and other AWS services (for example, Global Accelerator, CloudFront, AWS WAF, Route 53, Amazon Elastic Kubernetes Service [Amazon EKS], AWS Certificate Manager [ACM])

• Configuration options for load balancers (for example, proxy protocol, cross-zone load balancing, session affinity [sticky sessions], routing algorithms)

• Configuration options for load balancer target groups (for example, TCP, GENEVE, IP compared with instance)

• AWS Load Balancer Controller for Kubernetes clusters

• Considerations for encryption and authentication with load balancers (for example, TLS termination, TLS passthrough)

Skills in:

• Selecting an appropriate load balancer based on the use case

• Integrating auto scaling with load balancing solutions

• Integrating load balancers with existing application deployments

Task Statement 1.4: Define logging and monitoring requirements across AWS and hybrid networks.

Knowledge of:

• Amazon CloudWatch metrics, agents, logs, alarms, dashboards, and insights in AWS architectures to provide visibility

• AWS Transit Gateway Network Manager in architectures to provide visibility

• VPC Reachability Analyzer in architectures to provide visibility

• Flow logs and traffic mirroring in architectures to provide visibility

• Access logging (for example, load balancers, CloudFront)

Skills in:

• Identifying the logging and monitoring requirements

• Recommending appropriate metrics to provide visibility of the network status

• Capturing baseline network performance

Task Statement 1.5: Design a routing strategy and connectivity architecture between on-premises networks and the AWS Cloud.

Knowledge of:

• Routing fundamentals (for example, dynamic compared with static, BGP)

• Layer 1 and layer 2 concepts for physical interconnects (for example, VLAN, link aggregation group [LAG], optics, jumbo frames)

• Encapsulation and encryption technologies (for example, Generic Routing Encapsulation [GRE], IPsec)

• Resource sharing across AWS accounts

• Overlay networks

Skills in:

• Identifying the requirements for hybrid connectivity

• Designing a redundant hybrid connectivity model with AWS services (for example, AWS Direct Connect, AWS Site-to-Site VPN)

• Designing BGP routing with BGP attributes to influence the traffic flows based on the desired traffic patterns (load sharing, active/passive)

• Designing for integration of a software-defined wide area network (SDWAN) with AWS (for example, Transit Gateway Connect, overlay networks)

Task Statement 1.6: Design a routing strategy and connectivity architecture that include multiple AWS accounts, AWS Regions, and VPCs to support different connectivity patterns.

Knowledge of:

• Different connectivity patterns and use cases (for example, VPC peering, Transit Gateway, AWS PrivateLink)

• Capabilities and advantages of VPC sharing

• IP subnets and solutions accounting for IP address overlaps

Skills in:

• Connecting multiple VPCs by using the most appropriate services based on requirements (for example, using VPC peering, Transit Gateway, PrivateLink)

• Using VPC sharing in a multi-account setup

• Managing IP overlaps by using different available services and options (for example, NAT, PrivateLink, Transit Gateway routing)

Domain 2: Network Implementation

Task Statement 2.1: Implement routing and connectivity between on-premises networks and the AWS Cloud.

Knowledge of:

• Routing protocols (for example, static, dynamic)

• VPNs (for example, security, accelerated VPN)

• Layer 1 and types of hardware to use (for example, Letter of Authorization [LOA] documents, colocation facilities, Direct Connect)

• Layer 2 and layer 3 (for example, VLANs, IP addressing, gateways, routing, switching)

• Traffic management and SD-WAN (for example, Transit Gateway Connect)

• DNS (for example, conditional forwarding, hosted zones, resolvers)

• Security appliances (for example, firewalls)

• Load balancing (for example, layer 4 compared with layer 7, reverse proxies, layer 3)

• Infrastructure automation

• AWS Organizations and AWS Resource Access Manager (AWS RAM) (for example, multi-account Transit Gateway, Direct Connect, Amazon VPC, Route 53)

• Test connectivity (for example, Route Analyzer, Reachability Analyzer)

• Networking services of VPCs

Skills in:

• Configuring the physical network requirements for hybrid connectivity solutions

• Configuring static or dynamic routing protocols to work with hybrid connectivity solutions

• Configuring existing on-premises networks to connect with the AWS Cloud

• Configuring existing on-premises name resolution with the AWS Cloud

• Configuring and implementing load balancing solutions

• Configuring network monitoring and logging for AWS services

• Testing and validating connectivity between environments

Task Statement 2.2: Implement routing and connectivity across multiple AWS accounts, Regions, and VPCs to support different connectivity patterns.

Knowledge of:

• Inter-VPC and multi-account connectivity (for example, VPC peering, Transit Gateway, VPN, third-party vendors, SD-WAN, multi-protocol label switching [MPLS])

• Private application connectivity (for example, PrivateLink)

• Methods of expanding AWS networking connectivity (for example, Organizations, AWS RAM)

• Host and service name resolution for applications and clients (for example, DNS)

• Infrastructure automation

• Authentication and authorization (for example, SAML, Active Directory)

• Security (for example, security groups, network ACLs, AWS Network Firewall)

• Test connectivity (for example, Route Analyzer, Reachability Analyzer, tooling)

Skills in:

• Configuring network connectivity architectures by using AWS services in a single-VPC or multi-VPC design (for example, DHCP, routing, security groups)

• Configuring hybrid connectivity with existing third-party vendor solutions

• Configuring a hub-and-spoke network architecture (for example, Transit Gateway, transit VPC)

• Configuring a DNS solution to make hybrid connectivity possible

• Implementing security between network boundaries

• Configuring network monitoring and logging by using AWS solutions

Task Statement 2.3: Implement complex hybrid and multi-account DNS architectures.

Knowledge of:

• When to use private hosted zones and public hosted zones

• Methods to alter traffic management (for example, based on latency, geography, weighting)

• DNS delegation and forwarding (for example, conditional forwarding)

• Different DNS record types (for example, A, AAAA, TXT, pointer records, alias records)

• DNSSEC

• How to share DNS services between accounts (for example, AWS RAM)

• Requirements and implementation options for outbound and inbound endpoints

Skills in:

• Configuring DNS zones and conditional forwarding

• Configuring traffic management by using DNS solutions

• Configuring DNS for hybrid networks

• Configuring appropriate DNS records

• Configuring DNSSEC on Route 53

• Configuring DNS within a centralized or distributed network architecture

• Configuring DNS monitoring and logging on Route 53

Task Statement 2.4: Automate and configure network infrastructure.

Knowledge of:

• Infrastructure as code (IaC) (for example, AWS Cloud Development Kit [AWS CDK], AWS CloudFormation, AWS CLI, AWS SDK, APIs)

• Event-driven network automation

• Common problems of using hardcoded instructions in IaC templates when provisioning cloud networking resources

Skills in:

• Creating and managing repeatable network configurations

• Integrating event-driven networking functions

• Integrating hybrid network automation options with AWS native IaC

• Eliminating risk and achieving efficiency in a cloud networking environment while maintaining the lowest possible cost

• Automating the process of optimizing cloud network resources with IaC

Domain 3: Network Management and Operation

Task Statement 3.1: Maintain routing and connectivity on AWS and hybrid networks.

Knowledge of:

• Industry-standard routing protocols that are used in AWS hybrid networks (for example, BGP over Direct Connect)

• Connectivity methods for AWS and hybrid networks (for example, Direct Connect gateway, Transit Gateway, VIFs)

• How limits and quotas affect AWS networking services (for example, bandwidth limits, route limits)

• Available private and public access methods for custom services (for example, PrivateLink, VPC peering)

• Available inter-Regional and intra-Regional communication patterns

Skills in:

• Managing routing protocols for AWS and hybrid connectivity options (for example, over a Direct Connect connection, VPN)

• Maintaining private access to custom services (for example, PrivateLink, VPC peering)

• Using route tables to direct traffic appropriately (for example, automatic propagation, BGP)

• Setting up private access or public access to AWS services (for example, Direct Connect, VPN)

• Optimizing routing over dynamic and static routing protocols (for example, summarizing routes, CIDR overlap)

Task Statement 3.2: Monitor and analyze network traffic to troubleshoot and optimize connectivity patterns.

Knowledge of:

• Network performance metrics and reachability constraints (for example, routing, packet size)

• Appropriate logs and metrics to assess network performance and reachability issues (for example, packet loss)

• Tools to collect and analyze logs and metrics (for example, CloudWatch, VPC Flow Logs, VPC Traffic Mirroring)

• Tools to analyze routing patterns and issues (for example, Reachability Analyzer, Transit Gateway Network Manager)

Skills in:

• Analyzing tool output to assess network performance and troubleshoot connectivity (for example, VPC Flow Logs, Amazon CloudWatch Logs)

• Mapping or understanding network topology (for example, Transit Gateway Network Manager)

• Analyzing packets to identify issues in packet shaping (for example, VPC Traffic Mirroring)

• Troubleshooting connectivity issues that are caused by network misconfiguration (for example, Reachability Analyzer)

• Verifying that a network configuration meets network design requirements (for example, Reachability Analyzer)

• Automating the verification of connectivity intent as a network configuration changes (for example, Reachability Analyzer)

• Troubleshooting packet size mismatches in a VPC to restore network connectivity

Task Statement 3.3: Optimize AWS networks for performance, reliability, and costeffectiveness.

Knowledge of:

• Situations in which a VPC peer or a transit gateway are appropriate

• Different methods to reduce bandwidth utilization (for example, unicast compared with multicast, CloudFront)

• Cost-effective connectivity options for data transfer between a VPC and onpremises environments

• Different types of network interfaces on AWS

• High-availability features in Route 53 (for example, DNS load balancing using health checks with latency and weighted record sets)

• Availability of options from Route 53 that provide reliability

• Load balancing and traffic distribution patterns

• VPC subnet optimization

• Frame size optimization for bandwidth across different connection types

Skills in:

• Optimizing for network throughput

• Selecting the right network interface for the best performance (for example, elastic network interface, Elastic Network Adapter [ENA], Elastic Fabric Adapter [EFA])

• Choosing between VPC peering, proxy patterns, or a transit gateway connection based on analysis of the network requirements provided

• Implementing a solution on an appropriate network connectivity service (for example, VPC peering, Transit Gateway, VPN connection) to meet network requirements

• Implementing a multicast capability within a VPC and on-premises environments

• Creating Route 53 public hosted zones and private hosted zones and records to optimize application availability (for example, private zonal DNS entry to route traffic to multiple Availability Zones)

• Updating and optimizing subnets for auto scaling configurations to support increased application load

• Updating and optimizing subnets to prevent the depletion of available IP addresses within a VPC (for example, secondary CIDR)

• Configuring jumbo frame support across connection types

• Optimizing network connectivity by using Global Accelerator to improve network performance and application availability

Domain 4: Network Security, Compliance, and Governance

Task Statement 4.1: Implement and maintain network features to meet security and compliance needs and requirements.

Knowledge of:

• Different threat models based on application architecture

• Common security threats

• Mechanisms to secure different application flows

• AWS network architecture that meets security and compliance requirements

Skills in:

• Securing inbound traffic flows into AWS (for example, AWS WAF, AWS Shield, Network Firewall)

• Securing outbound traffic flows from AWS (for example, Network Firewall, proxies, Gateway Load Balancers)

• Securing inter-VPC traffic within an account or across multiple accounts (for example, security groups, network ACLs, VPC endpoint policies)

• Implementing an AWS network architecture to meet security and compliance requirements (for example, untrusted network, perimeter VPC, three-tier architecture)

• Developing a threat model and identifying appropriate mitigation strategies for a given network architecture

• Testing compliance with the initial requirements (for example, failover test, resiliency)

• Automating security incident reporting and alerting using AWS

Task Statement 4.2: Validate and audit security by using network monitoring and logging services.

Knowledge of:

• Network monitoring and logging services that are available in AWS (for example, CloudWatch, AWS CloudTrail, VPC Traffic Mirroring, VPC Flow Logs, Transit Gateway Network Manager)

• Alert mechanisms (for example, CloudWatch alarms)

• Log creation in different AWS services (for example, VPC flow logs, load balancer access logs, CloudFront access logs)

• Log delivery mechanisms (for example, Amazon Kinesis, Route 53, CloudWatch)

• Mechanisms to audit network security configurations (for example, security groups, AWS Firewall Manager, AWS Trusted Advisor)

Skills in:

• Creating and analyzing a VPC flow log (including base and extended fields of flow logs)

• Creating and analyzing network traffic mirroring (for example, using VPC Traffic Mirroring)

• Implementing automated alarms by using CloudWatch

• Implementing customized metrics by using CloudWatch

• Correlating and analyzing information across single or multiple AWS log sources

• Implementing log delivery solutions

• Implementing a network audit strategy across single or multiple AWS network services and accounts (for example, Firewall Manager, security groups, network ACLs)

Task Statement 4.3: Implement and maintain confidentiality of data and communications of the network.

Knowledge of:

• Network encryption options that are available on AWS

• VPN connectivity over Direct Connect

• Encryption methods for data in transit (for example, IPsec)

• Network encryption under the AWS shared responsibility model

• Security methods for DNS communications (for example, DNSSEC)

Skills in:

• Implementing network encryption methods to meet application compliance requirements (for example, IPsec, TLS)

• Implementing encryption solutions to secure data in transit (for example, CloudFront, Application Load Balancers and Network Load Balancers, VPN over Direct Connect, AWS managed databases, Amazon S3, custom solutions on Amazon EC2, Transit Gateway)

• Implementing a certificate management solution by using a certificate authority (for example, ACM, AWS Private Certificate Authority [ACM PCA])

• Implementing secure DNS communications