aws training and certification

AWS Certified Advanced Networking – Specialty (ANS-C00) 시험 안내서

서론

AWS Certified Advanced Networking – Specialty (ANS-C00) 시험은 AWS 네트워킹 전문가의 역할을 수행하는 개인을 대상으로 합니다. 이 시험은 대규모의 AWS 및 하이브리드 IT 네트워크 아키텍처의 설계 및 구현에 대한 고급 기술 능력 및 경험을 검증합니다. 시험은 복잡한 네트워킹 태스크를 수행하는 개인을 대상으로 하며 다음을 수행하기 위한 개인의 능력을 검증합니다.

- AWS 를 사용하여 클라우드 기반 솔루션을 설계, 개발 및 배포
- 기본적인 아키텍처 모범 사례에 따라 핵심 AWS 서비스 구현
- 모든 AWS 서비스에 대한 네트워크 아키텍처 설계 및 유지 관리
- 도구를 사용하여 AWS 네트워킹 태스크 자동화

대상 응시자 설명

대상 응시자는 AWS Certified Solutions Architect – Professional 의 기대 수준을 훨씬 뛰어넘는 고급 네트워킹에 대한 전문 지식을 보유하고 있습니다. 대상 응시자는 네트워킹에 중점을 두고 설계, 구현 및 문제 해결 전문 지식을 보유한 숙련된 솔루션스 아키텍트(5~7 년 이상)일 수 있습니다. 대상 응시자는 대규모 인프라 엔지니어링 분야(예: 복잡한 SMB, 엔터프라이즈, ISP, LAN/WAN 환경)의 경험이 있을 수 있습니다.

일반 IT 지식 추천

대상 응시자는 다음 분야에 대한 지식이 있어야 합니다.

- 고급 네트워킹 아키텍처 및 상호 연결 옵션(예: IP VPN, 멀티 프로토콜 레이블 스위칭(MPLS), 가상 프라이빗 LAN 서비스(VPLS))
- OSI(Open Systems Interconnection) 모델 내의 네트워킹 기술 및 이러한 기술이 구현 방식 결정에 미치는 영향
- 자동화 스크립트 및 도구 개발. 다음에 대한 설계, 구현 및 최적화:
    - 라우팅 아키텍처(정적 및 동적 포함)
    - 글로벌 엔터프라이즈를 위한 멀티 리전 솔루션
    - 고가용성 연결 솔루션(예: AWS Direct Connect, VPN)

- CIDR 및 서브넷(IPv4 및 IPv6)
- IPv6 전환 과제
- AWS WAF, IDS(침입 탐지 시스템), IPS(침입 방지 시스템), DDoS 보호, EDoS(Economic Denial of Service/Sustainability) 등 네트워크 보안 기능을 위한 일반 솔루션

AWS 지식 추천

대상 응시자는 다음과 같은 지식이 있어야 합니다.

- AWS 기술을 사용한 전문적 경험
- AWS 보안 모범 사례
- AWS 스토리지 옵션 및 기본 일관성 모델에 대한 이해
- AWS 네트워킹 뉘앙스 및 AWS 서비스 통합과 연관된 방식

대상 응시자가 갖추지 않아도 되는 것은 무엇입니까?

다음은 대상 응시자가 수행하지 않아도 될 것으로 예상되는 관련 작업 태스크의 목록입니다(전체 목록은 아님). 다음 항목은 시험 범위에 포함되지 않는 것으로 간주됩니다.

- 애플리케이션 프로그램 개발 기술 보유
- Solutions Architect – Professional 수준 이상의 시스템 운영 기술 보유

시험 콘텐츠

답안 유형

이 시험의 문항은 두 가지 유형으로 제공됩니다.

- **선다형:** 정답 1 개와 오답 3 개(정답 이외의 답)
- **복수 응답형:** 5 개 이상의 옵션 중에 2 개 이상의 정답이 있습니다.

문장을 가장 잘 완성하거나 질문에 대한 답으로 가장 적합한 응답을 하나 이상 선택합니다. 정답 이외의 답 또는 오답은 지식이나 기술이 부족한 응시자가 선택할 가능성이 큰 응답 옵션입니다. 정답 이외의 답은 일반적으로 콘텐츠 영역에 부합하여 맞아 보이는 응답입니다.

답을 하지 않은 문항은 오답으로 처리됩니다. 추측에 따른 불이익은 없습니다. 시험에는 점수에 영향을 주는 50 개의 문항이 포함되어 있습니다.

채점되지 않는 콘텐츠

시험에는 점수에 영향을 주지 않는 채점 대상이 아닌 15 개의 문항이 포함되어 있습니다. AWS 는 채점 대상이 아닌 질문에 대한 응시자 성과 정보를 수집하여 추후 채점 대상 질문으로 사용할 수 있도록 이러한 질문을 평가합니다. 이러한 채점 대상이 아닌 질문은 시험에서 식별되지 않습니다.

시험 결과

AWS Certified Advanced Networking – Specialty 시험은 합격 또는 불합격이 결정되는 시험입니다. AWS 전문가가 자격증 분야 모범 사례 및 지침에 따라 설정한 최소 표준을 기준으로 시험 점수를 매깁니다.

시험 결과는 100~1,000 기준의 점수로 채점됩니다. 합격 최소 점수는 750 점입니다. 응시자의 점수는 전반적으로 시험을 어떻게 치렀는지와 합격 여부를 보여줍니다. 스케일링된 점수 모델은 난이도가 조금씩 다를 수 있는 여러 시험 형식에 걸쳐 점수를 균등하게 조정하는 데 도움이 됩니다.

점수 보고서에는 섹션 레벨별로 성적 분류 표가 포함될 수 있습니다. 이 정보는 시험 성적에 대한 일반적인 피드백을 제공하기 위한 것입니다. 시험은 보상 점수 모델을 사용하므로 각 섹션에서 합격 점수를 얻을 필요는 없습니다. 전체 시험에만 합격하면 됩니다.

시험의 섹션마다 특정 가중치가 적용되므로 일부 섹션은 다른 섹션보다 문항 수가 많습니다. 표에는 응시자의 장단점을 보여주는 일반 정보가 포함되어 있습니다. 섹션 레벨 피드백을 검토할 때 주의하시기 바랍니다.

내용 개요

이 시험 안내서는 시험의 가중치, 테스트 영역 및 목표를 제공하며, 이 시험에 대한 종합적인 콘텐츠 목록은 아닙니다. 하지만 시험을 준비하는 데 도움이 되는 각 목표에 대한 추가 컨텍스트가 있습니다. 다음 표에는 주요 콘텐츠 영역과 가중치가 나열되어 있습니다. 이 표는 추가 컨텍스트가 포함되어 있는 전체 시험 콘텐츠 개요 앞에 나옵니다. 각 영역의 백분율은 채점되는 콘텐츠만 나타냅니다.

도메인	시험 비율(%)
도메인 1: 대규모 하이브리드 IT 네트워크 아키텍처 설계 및 구현	24%
도메인 2: AWS 네트워크 설계 및 구현	28%
도메인 3: AWS 태스크 자동화	8%
도메인 4: 애플리케이션 서비스와 네트워크 통합 구성	14%
도메인 5: 보안 및 규정 준수를 위한 설계 및 구현	12%
도메인 6: 네트워크 관리, 최적화 및 문제 해결	14%
합계	**100%**

도메인 1: 대규모 하이브리드 IT 네트워크 아키텍처 설계 및 구현

1.1 하이브리드 IT 아키텍처에 대한 연결 구현에 절차 개념 적용

1.2 주어진 시나리오에서 적절한 하이브리드 IT 아키텍처 연결 솔루션 도출

- 하위 수준 설계에 대한 IP 주소 할당 결정
- 애플리케이션 흐름을 매핑하여 통신 매트릭스 생성
- 템플릿 기반으로 디바이스 구성 구현
- AWS 콘솔 구성에 대한 구현 단계 결정(AWS, Direct Connect 링크, VPN, 온프레미스, L1→7 테스트 등)
- AWS 와 온프레미스 DNS 서비스 통합
- 솔루션 구성 요소의 개요 설명(예: 다이어그램, 솔루션 내 프로토콜, VLAN, 801.q, BFD 등)
- 기업 및 기술 요구 사항에 맞게 네트워크 아키텍처 다이어그램 평가
- 디바이스 구성에 대한 구현 단계 결정(AWS, Direct Connect 링크, VPN, 온프레미스, L1→7 테스트 등)
- 기업 요구 사항에 따라 디바이스 구성 사용자 지정
- 주어진 기업 및 기술 요구 사항에 대해 롤백 절차 정의
- 기업 요구 사항을 충족하도록 VPC 로의 다중 경로 링크 설계
- 특정 아키텍처에 적합한 고가용성/로드 밸런싱 요구 사항 결정

1.3 Direct Connect 를 사용하여 연결을 확장하는 프로세스 설명

1.4 Direct Connect 를 활용하는 설계 대안 평가

- 프라이빗 VIF 지원에 사용할 적절한 리전 결정
- 적절한 복원력 전략 결정
- DX 시설에 고객 장치 코로케이션 필요 여부 확인
- 특정 리전 서비스에 대한 퍼블릭 VIF 액세스 제한
- 1G 미만의 다중 연결이 필요한지 확인
- 연결 이중화를 제공하는 데 필요한 Direct Connect 시설 결정
- Direct Connect 게이트웨이를 사용하여 여러 AWS 리전으로 Direct Connect 트래픽 라우팅

1.5 하이브리드 IT 아키텍처에 대한 라우팅 정책 정의

- 고가용성, 로드 밸런싱, 트래픽 셰이핑 및 보안과 관련된 고객 요구 사항에 따라 라우팅 정책 결정
- 라우팅 피어를 위한 링크 파라미터 정의(온프레미스 라우터와 AWS 라우터 피어링)
- 라우팅 정책을 구현하는 데 필요한 BGP 파라미터 정의(예: BGP 수치, AS 번호)
- 라우팅 정책을 구현하기 위해 라우팅 프로토콜 구성(경로 필터링, 경로 맵, 정책 기반 라우팅, ACL, AS 조작) 외부에서 경로 조작을 위한 디바이스 기반 구성 구현
- 테스트 계획 결정
- 라우터 구성 생성(BGP 구성, 정책/보안 구성 포함)
- 구현 테스트

도메인 2: AWS 네트워크 설계 및 구현

2.1 AWS 네트워킹 개념 적용

2.2 주어진 고객 요구 사항에 따라 AWS 의 네트워크 아키텍처 정의

- AWS 소프트웨어 정의 네트워킹의 목적 및 기능 설명
- AWS 내에서 네트워크 격리의 작동 방식(VPC)과 다양한 구성 요소 설명
- 필요한 IP 주소 수 계산
- 필요한 네트워크/서브넷 수와 각 네트워크 내의 호스트 수 계산
- 서브넷 간 격리 수준 분류
- 서브넷과 VPC 간 트래픽 흐름 요구 사항 설명
- 글로벌 네트워크 및 네트워크 간의 통신 요구 사항 개요 설명
- 고객 요구 사항에 따라 AWS 콘솔 또는 AWS 도구를 사용하여 VPC, 서브넷, 라우팅 테이블 및 네트워크 ACL 생성
- 게이트웨이 생성 및 연결
- VPC 엔드포인트를 활용하여 고객 요구 사항 충족

- 고객 요구 사항에 따라 IP 주소 지정 체계 설계 및 각 서브넷의 서브넷 크기(서브넷 마스크) 추정
- 고객 요구 사항(보안 격리, 개발/테스트/프로덕션 환경 등)에 따라 서브넷을 다양한 논리 단위로 구분
- 각 서브넷(네트워크 ACL, 퍼블릭/프라이빗 서브넷)에 대한 보안 모델 설계
- 각 서브넷의 라우팅 특성 결정
- 고객 요구 사항에 따라 VPC 를 퍼블릭 인터넷(필요한 경우)에 연결하기 위한 모델 및 보안 모델 설계
- AWS Transit Gateway 를 비롯해 고객 요구 사항에 따라 VPC 간 통신(리전/글로벌 내) 및 보안 모델 설계
- AWS 서비스를 강화하고 고객 요구 사항을 해결하는 에코시스템 솔루션 선택
- 서브넷을 여러 AWS 계정과 공유해야 하는지 결정

2.3 기존 구현에 대한 평가를 기반으로 최적화된 설계 제안

- HLD 또는 계정 사용에서 사용 및 식별된 특정 제품 세트에 대한 모범 사례를 백서 및 기타 AWS 참조 문서에서 식별된 모범 사례와 매핑(예: 현재 구축 및 AWS 모범 사례 간의 GAP 분석 사용)
- HLD 에서 확인된 현재 구축과 AWS 모범 사례의 차이점에 대한 권장 사항 제시
- 대상 아키텍처를 기반으로 변경 관리 계획 결정 및 수행
- 적절한 네트워크 최적화 전략 결정(예: 배치 그룹, 강화된 네트워킹, 추가 ENI, ENA, EFA, 에코시스템, EBS Optimized, MTU, 인터넷 처리량)
- 특정 제품에 대한 GAP 분석, AWS 참조 아키텍처, AWS 백서, AWS 문서 등의 도구 사용

2.4 특수 워크로드에 대한 네트워크 요구 사항 결정

- 특수 워크로드 및 해당 네트워크 요구 사항(예: 대역폭 요구 사항, 지연 요구 사항, 안정성/복원력 요구 사항, 암호화 요구 사항) 결정
- 솔루션 구성 요소의 개요 설명(예: 다이어그램, 솔루션 내 프로토콜, VLAN, 801.q, BFD 등)

2.5 고객 및 애플리케이션 요구 사항에 따라 적절한 아키텍처 도출

- 기업 및 애플리케이션 요구 사항을 기술 솔루션에 매핑
- 애플리케이션 요구 사항을 파악하여 기술 요구 사항으로 변환
- 고객의 기업 요구 사항을 평가하고 애플리케이션 요구 사항과 비교하여 차이점을 매핑
- 애플리케이션 흐름 요구 사항을 네트워크 기능에 매핑
- 시스템의 네트워크 제한 내에서 애플리케이션 요구 사항에 매핑된 고객 요구 사항을 자세히 설명하는 요구 사항 정의 문서 개요 작성
- 고객 요구 사항을 AWS 구성 요소로 변환

2.6 네트워크 설계 및 애플리케이션 데이터 흐름에 따른 비용 할당 평가 및 최적화

- 네트워크 설계를 기준으로 요금 추정
- 애플리케이션 데이터 흐름(예: VPC-E, AWS Key Management Service(KMS) 스냅샷 복사본, Amazon S3 리전 간 복제, 가용 영역 간 등)을 기준으로 요금 추정

도메인 3: AWS 태스크 자동화

3.1 네트워크 구축에 대한 AWS 내 자동화 대안 평가

- AWS CloudFormation 을 사용하여 VPC 인프라 관리
- AWS Service Catalog 를 사용하여 네트워크 프로비저닝 셀프 서비스 확장
- AWS CodeCommit 에 Infrastructure as Code(IaC) 아티팩트 저장
- AWS Config, Amazon Single Notification Service(SNS), AWS Lambda 및 CloudFormation 드리프트 감지를 사용하여 변경 사항 감사
- 멀티캐스트 트래픽을 라우팅할 수 있도록 Amazon EC2 태그(예: 멀티캐스트), Transit Gateway 를 사용하여 연결된 VPC 의 서브넷 간에 오버레이 네트워크 구성을 동적으로 구현
- IPAM 소프트웨어를 비롯해 외부 시스템과의 통합을 위한 CloudFormation 맞춤형 리소스로 Lambda 를 활용
- CloudFormation 을 사용하여 CloudFormation 템플릿 빌드

3.2 AWS 내에서 네트워크 운영 및 관리를 위한 도구 기반 대안 평가

- 스크립팅(모든 언어)을 사용하여 EC2 에서 NAT, 방화벽 등에 대한 고가용성 솔루션 구현
- API 를 사용하여 현재 네트워크 구성 요소 상태/구성 정보 수집
- Amazon CloudWatch 및 Amazon CloudWatch Logs 에 대한 EC2 모니터링 스크립트 구현
- Network Manager 콘솔을 사용하여 글로벌 네트워크 시각화 및 모니터링
- VPC 트래픽 미러링을 사용하여 트래픽 모니터링
- 주어진 고객 시나리오에서 CloudWatch 를 활용하여 집계된 측정치와 문제 알림 및 자동화된 수정 사항에 대한 모니터링

도메인 4: 애플리케이션 서비스와 네트워크 통합 구성

4.1 Amazon Route 53 의 기능 활용

4.2 하이브리드 IT 아키텍처에서 DNS 솔루션 평가

- Route 53 별칭을 다른 AWS 서비스와 함께 활용
- 적절한 DNS 레코드 유형, 값 및 TTL 을 선택
- 고객 요구 사항에 따라 적절한 DNS 영역 유형(퍼블릭/프라이빗)을 결정
- 퍼블릭 호스팅 영역과 프라이빗 호스팅 영역의 차이점 설명
- 기업 요구 사항을 고려하여 적절한 DNS 라우팅 전략 설계

- 호스팅 영역 및 레코드 세트의 계층 구조 설계 및 구성
- 기업 요구 사항을 고려하여 효과적인 상태 확인 전략 설계

4.3 AWS 내에서 적절한 DHCP 구성 결정

- DHCP 의 주요 개념 및 기능 설명
- AWS 에서 DHCP 가 작동하는 방식 설명(예: Layer 2 브로드캐스트)
- IP 주소 배정에 적합한 DHCP 사용 결정(예: 보조 IP)
- 애플리케이션 요구 사항을 충족하도록 DHCP 옵션 집합 구성
- 연결된 애플리케이션에 서로 다른 DHCP 옵션 집합이 필요한 솔루션 구현

4.4 주어진 시나리오에 따라 AWS 에코시스템 내에서 적절한 로드 밸런싱 전략 결정

- 고정 세션 구현
- 클라이언트 IP 주소 검색 전략 파악
- TCP, HTTP 및 HTTPS 서비스의 로드 밸런싱 구성
- 기업 및 애플리케이션 요구 사항을 고려하여 애플리케이션 상태 확인 전략 설계
- 에코시스템(예: Elastic Load Balancer 및 서드 파티 솔루션)을 활용하여 애플리케이션 요구 사항 충족
- 주어진 시나리오에 따라 적절한 로드 밸런싱 솔루션 파악

4.5 성능 최적화를 위한 콘텐츠 배포 전략 결정

- 엔드 투 엔드 콘텐츠 흐름을 식별 및 매핑하여 통신 매트릭스 생성
- 엔드 투 엔드 DNS 흐름을 식별 및 매핑하여 통신 매트릭스 생성
- 주어진 시나리오에 따라 적절한 Amazon CloudFront 솔루션(URL, 프로토콜(HTTP 및/또는 HTTPS), 메서드) 결정
- AWS 콘솔을 사용하여 CloudFront, 오리진 서버 및 관련 서비스(Route 53(또는 더 적절한 경우 AWS Global Accelerator), EC2, S3, AWS Direct Connect 등)에 대한 구현 단계 결정
- 기업 요구 사항에 맞게 조정하도록 측정 방법론 결정

4.6 AWS 서비스 요구 사항과 네트워크 요구 사항 조정

- AWS 서비스가 네트워크를 통해 통신하는 방식(프로토콜, 포트 등) 결정
- AWS 서비스에서 범위 내 나머지 구성 요소(AWS 서비스, 퍼블릭 인터넷 내)로의 데이터 흐름 모델 설계
- 애플리케이션이 AWS 서비스와 상호 작용하는 방식 결정 및 이들 간 네트워크 통신 흐름 설계
- AWS 서비스에 대한 CIDR 요구 사항 결정(있는 경우)
- AWS 서비스용 네트워크 보안 모델 빌드

도메인 5: 보안 및 규정 준수를 위한 설계 및 구현

5.1 보안 및 규정 준수 목표에 부합하는 설계 요구 사항 평가

- 주어진 보안 요구 사항에 따라 적절한 AWS 도구 및 에코시스템 선택
- 격리된 서브넷 아키텍처 구현
- 보안 및 규정 준수 요구 사항(예: DMZ(Demilitarized Zone), 3 개 계층)을 충족하도록 AWS 네트워크 아키텍처 설계 및 구현
- 위협 모델 개발 및 지정된 구현에 대한 적절한 완화 전략 파악
- 특정 시나리오에서 보안 취약성 및/또는 규정 준수 위반 식별

5.2 보안 및 규정 준수 목표를 지원하는 모니터링 전략 평가

- VPC 흐름 로그 생성 및 상호 작용
- 시도되거나 완료된 네트워킹 리소스 변경 모니터링에 AWS CloudTrail 사용
- CloudWatch 를 사용하여 자동화된 경보 구현
- CloudWatch 를 사용하여 사용자 지정 지표 구현
- 고객의 기업 요구 사항에 따라 전반적인 보안/모니터링 솔루션 결정
- 인가된 변경 사항(InfoSec 측면)에 대해 관리 및 보안 도구(예: CloudTrail, CloudWatch, 인스턴스 로그, cmdb) 분석

5.3 네트워크 트래픽 관리를 위한 AWS 보안 기능 평가

- 보안 그룹, 네트워크 ACL 및 IAM 정책의 기능적 역량 대비 및 비교
- 애플리케이션에 대한 네트워크 보안 요구 사항 결정
- 애플리케이션 흐름을 결정하고 매핑하여 정책 적용 개체(보안 그룹, 네트워크 ACL 또는 IAM 정책) 생성
- 보안 그룹, 네트워크 ACL 및 IAM 정책 간에 적절한 적용 결정
- 보안 요구 사항(예: VPC, 서브넷, 라우팅 테이블, 보안 그룹, 네트워크 ACL, VGW, IGW 등 네트워킹 리소스를 변경할 수 있는 사용자 제한)에 따라 보안 그룹, 네트워크 ACL 및 IAM 정책 구현
- 명시된 요구 사항에 대한 규정 준수 테스트
- 네트워크 보안 솔루션(예: 다이어그램, 보안 그룹을 통해 허용/거부된 프로토콜, 네트워크 ACL, 네트워킹 리소스에 대한 허용/거부 작업에 대한 권한 매트릭스) 개요 설명
- 기업 요구 사항에 따라 구현 사용자 지정

5.4 암호화 기술을 활용하여 네트워크 통신 보호

- 암호화에 대한 적용 가능한 규정 준수 요구 사항 결정
- 암호화해야 하는 애플리케이션 데이터 결정
- 데이터 흐름 및 해당 데이터를 저장할 시스템 결정

- 전송 중인 데이터와 저장 데이터를 암호화하는 암호화 솔루션(S3, Amazon EBS(Elastic Block Store), Amazon RDS(Relational Database Solution) 및 EC2 의 사용자 지정 솔루션) 구현
- 암호화 키 관리 솔루션(AWS Key Management Service(KMS) 또는 고객 소유 서드 파티 솔루션 사용) 구현
- 암호화된 데이터에 대한 액세스 감사 구현
- 규정 준수를 검증하기 위한 테스트
- 솔루션(암호화, 키 관리, 감사 제어 등)의 구성 요소 개요 설명
- 암호화로 인한 애플리케이션 성능 영향 파악 및 완화 솔루션 권장

도메인 6: 네트워크 관리, 최적화 및 문제 해결

6.1 주어진 시나리오에 따라 네트워크 문제 해결

- 라우팅 테이블을 검토하여 블랙홀 또는 라우팅 전파가 부족한 위치 파악
- 온프레미스 디바이스(VPN 또는 Direct Connect)의 정보를 수집하여 네트워크 연결성 식별
- L1-L4 연결성을 검증하고 각 레이어에서 잠재적 장애 원인 조사
- 주어진 표준 진단 정보에서 AWS 네트워크 구성의 구현 오류 또는 결함 식별
- 보안 그룹 및 네트워크 ACL 의 적절한 사용 평가(허용 및 거부 비교)
- VPC 흐름 로그를 사용하여 보안 그룹 또는 네트워크 ACL 의 구성 오류 또는 잠재적인 보안 취약점 파악