AWS Certified Advanced Networking - Specialty(ANS-C01) 시험 안내서

서론

AWS Certified Advanced Networking - Specialty(ANS-C01) 시험은 AWS 네트워킹 전문가의 역할을 수행하는 개인을 대상으로 합니다. 이 시험은 응시자가 대규모로 AWS 및 하이브리드 네트워크 아키텍처를 설계, 구현, 관리 및 보호할 수 있는지 검증합니다.

또한 이 시험에서는 응시자가 다음과 같은 태스크를 완료할 수 있는지도 확인합니다.

- AWS 를 사용하여 하이브리드 및 클라우드 기반 네트워킹 솔루션 설계 및 개발
- AWS 모범 사례에 따라 핵심 AWS 네트워킹 서비스 구현
- 모든 AWS 서비스에 대한 하이브리드 및 클라우드 기반 네트워크 아키텍처 운영 및 유지 관리
- 도구를 사용하여 하이브리드 및 클라우드 기반 AWS 네트워킹 태스크 배포 및 자동화
- AWS 네이티브 네트워킹 구성 및 서비스를 사용하여 안전한 AWS 네트워크 구현

대상 응시자 설명

대상 응시자는 5 년 이상의 네트워킹 경험과 2 년 이상의 클라우드 및 하이브리드 네트워킹 경험이 있어야 합니다.

권장되는 AWS 지식

대상 응시자는 다음과 같은 AWS 지식이 있어야 합니다.

- AWS 네트워킹 뉘앙스 및 AWS 서비스 통합과 연관된 방식
- AWS 보안 모범 사례
- AWS 컴퓨팅 및 스토리지 옵션과 기본 일관성 모델

부록을 참고하여 시험에 출제될 수 있는 기술 및 개념의 목록, 시험 범위에 해당하는 AWS 서비스 및 기능의 목록, 시험 범위가 아닌 AWS 서비스 및 기능의 목록을 확인하시기 바랍니다.

시험 콘텐츠

답안 유형

이 시험의 문항은 두 가지 유형으로 제공됩니다.

- **선다형:** 정답 1 개와 오답 3 개(정답 이외의 답)가 있습니다.
- **복수 응답형:** 5 개 이상의 응답 항목 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 항목입니다. 정답 이외의 답은 일반적으로 콘텐츠 영역에 부합하여 맞아 보이는 응답입니다.

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

채점되지 않는 콘텐츠

시험에는 점수에 반영되지 않아 채점되지 않는 15 개의 문항이 포함되어 있습니다. AWS 는 채점되지 않는 문항에 대한 응시자 성적 정보를 수집하여 추후 채점 대상 문항으로 사용할 수 있도록 이러한 문항을 평가합니다. 이러한 채점되지 않는 질문은 시험에서 식별되지 않습니다.

시험 결과

AWS Certified Advanced Networking - Specialty(ANS-C01) 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 점의 변환 점수로 보고됩니다. 합격 최소 점수는 750 점입니다. 응시자의 점수는 전반적인 시험 성적과 합격 여부를 보여줍니다. 변환 점수 모델은 난이도가 조금씩 다를 수 있는 여러 시험 형식에 걸쳐 점수를 균등하게 조정하는 데 도움이 됩니다.

점수 보고서에는 섹션 레벨별로 성적 분류표가 포함될 수 있습니다. 시험은 보상 점수 모델을 사용하므로 각 섹션에서 합격 점수를 얻을 필요는 없으며, 전체 시험에만 합격하면 됩니다.

시험의 섹션마다 특정 가중치가 적용되므로 일부 섹션은 다른 섹션보다 문항 수가 많습니다. 분류표에는 응시자의 장단점을 강조하여 보여주는 일반 정보가 포함되어 있습니다. 섹션별 피드백을 파악할 때 주의하시기 바랍니다.

내용 개요

이 시험 안내서에서는 시험의 가중치, 콘텐츠 도메인 및 태스크 설명 자료를 제공합니다. 이 안내서에서 시험 내용의 전체 목록을 제공하지는 않습니다. 그러나 각 태스크 설명에 관한 추가 맥락 정보를 사용하여 시험을 준비하는 데 참고할 수 있습니다.

시험의 콘텐츠 도메인과 가중치는 다음과 같습니다.

- 도메인 1: 네트워크 설계(채점되는 콘텐츠의 30%)
- 도메인 2: 네트워크 구현(채점되는 콘텐츠의 26%)
- 도메인 3: 네트워크 관리 및 운영(채점되는 콘텐츠의 20%)
- 도메인 4: 네트워크 보안, 규정 준수 및 거버넌스(채점되는 콘텐츠의 24%)

도메인 1: 네트워크 설계

태스크 설명 1.1: 엣지 네트워크 서비스를 통합하여 글로벌 아키텍처에 대한 사용자 성능 및 트래픽 관리를 최적화하는 솔루션을 설계합니다.

관련 지식:

- 콘텐츠 배포 네트워크 사용에 대한 패턴 설계(예: Amazon CloudFront)
- 글로벌 트래픽 관리를 위한 패턴 설계(예: AWS Global Accelerator)
- 콘텐츠 배포 네트워크를 위한 통합 패턴 및 다른 서비스와의 글로벌 트래픽 관리(예: Elastic Load Balancing(ELB), Amazon API Gateway)

관련 기술:

- 인터넷에서 유입되는 글로벌 인바운드 및 아웃바운드 트래픽의 요구 사항을 평가하여 적절한 콘텐츠 배포 솔루션 설계

태스크 설명 1.2: 퍼블릭, 프라이빗 및 하이브리드 요구 사항을 충족하는 DNS 솔루션을 설계합니다.

관련 지식:

- DNS 프로토콜(예: DNS 레코드, TTL, DNSSEC, DNS 위임, 영역)
- DNS 로깅 및 모니터링
- Amazon Route 53 기능(예: 별칭 레코드, 트래픽 정책, 리졸버, 상태 확인)

- Route 53 을 다른 AWS 네트워킹 서비스(예: Amazon VPC)와 통합
- Route 53 을 하이브리드, 다중 계정 및 다중 리전 옵션과 통합
- 도메인 등록

관련 기술:

- Route 53 퍼블릭 호스팅 영역 사용
- Route 53 프라이빗 호스팅 영역 사용
- 하이브리드 및 AWS 아키텍처에서 Route 53 Resolver 엔드포인트 사용
- 글로벌 트래픽 관리에 Route 53 사용
- 도메인 등록 생성 및 관리

태스크 설명 1.3: 고가용성, 확장성 및 보안 요구 사항을 충족하기 위해 로드 밸런싱을 통합하는 솔루션을 설계합니다.

관련 지식:

- OSI 모델의 계층 3, 계층 4 및 계층 7 에서 로드 밸런싱이 작동하는 방식
- 다양한 유형의 로드 밸런서와 이러한 로드 밸런서가 네트워크 설계, 고가용성 및 보안에 대한 요구 사항을 충족하는 방법
- 사용 사례에 따라 로드 밸런싱에 적용되는 연결 패턴(예: 내부 로드 밸런서, 외부 로드 밸런서)
- 로드 밸런서의 크기 조정 요인
- 로드 밸런서와 기타 AWS 서비스 통합(예: Global Accelerator, CloudFront, AWS WAF, Route 53, Amazon Elastic Kubernetes Service(Amazon EKS), AWS Certificate Manager(ACM))
- 로드 밸런서 구성 옵션(예: 프록시 프로토콜, 교차 영역 로드 밸런싱, 세션 어피니티(스티키 세션), 라우팅 알고리즘)
- 로드 밸런서 대상 그룹에 대한 구성 옵션(예: TCP, GENEVE, 인스턴스와 IP 비교)
- Kubernetes 클러스터용 AWS Load Balancer Controller
- 로드 밸런서를 사용한 암호화 및 인증에 대한 고려 사항(예: TLS 종료, TLS 패스스루)

관련 기술:

- 사용 사례에 따라 적절한 로드 밸런서 선택
- 자동 크기 조정과 로드 밸런싱 솔루션 통합
- 기존 애플리케이션 배포와 로드 밸런서 통합

태스크 설명 1.4: AWS 및 하이브리드 네트워크에서 로깅 및 모니터링 요구 사항을 정의합니다.

관련 지식:

- 가시성을 제공하는 AWS 아키텍처의 Amazon CloudWatch 지표, 에이전트, 로그, 경보, 대시보드 및 인사이트
- 가시성을 제공하는 아키텍처의 AWS Transit Gateway Network Manager
- 가시성을 제공하는 아키텍처의 VPC Reachability Analyzer
- 가시성을 제공하는 아키텍처의 흐름 로그 및 트래픽 미러링
- 액세스 로깅(예: 로드 밸런서, CloudFront)

관련 기술:

- 로깅 및 모니터링 요구 사항 식별
- 네트워크 상태에 대한 가시성을 제공하기 위한 적절한 지표 추천
- 기본 네트워크 성능 캡처

태스크 설명 1.5: 온프레미스 네트워크와 AWS 클라우드 간의 라우팅 전략 및 연결 아키텍처를 설계합니다.

관련 지식:

- 라우팅 기본 사항(예: 정적과 동적 비교, BGP)
- 물리적 상호 연결에 대한 계층 1 및 계층 2 개념(예: VLAN, 링크 집계 그룹(LAG), 광학, 점보 프레임)
- 캡슐화 및 암호화 기술(예: 일반 라우팅 캡슐화(GRE), IPsec)
- AWS 계정 간 리소스 공유
- 오버레이 네트워크

관련 기술:

- 하이브리드 연결에 대한 요구 사항 식별
- AWS 서비스를 사용하여 중복 하이브리드 연결 모델 설계(예: AWS Direct Connect, AWS Site-to-Site VPN)
- 원하는 트래픽 패턴(로드 공유, 액티브/패시브)을 기반으로 트래픽 흐름에 영향을 주는 BGP 속성으로 BGP 라우팅 설계
- 소프트웨어 정의 광역 네트워크(SD-WAN)와 AWS 의 통합을 위한 설계(예: Transit Gateway Connect, 오버레이 네트워크)

태스크 설명 1.6: 다양한 연결 패턴을 지원하기 위해 여러 AWS 계정, AWS 리전 및 VPC 를 포함하는 라우팅 전략 및 연결 아키텍처를 설계합니다.

관련 지식:

- 다양한 연결 패턴 및 사용 사례(예: VPC 피어링, Transit Gateway, AWS PrivateLink)
- VPC 공유의 기능 및 이점
- IP 주소 중복을 고려한 IP 서브넷 및 솔루션

관련 기술:

- 요구 사항에 따라 가장 적합한 서비스를 사용하여 여러 VPC 연결(예: VPC 피어링, Transit Gateway, PrivateLink 사용)
- 다중 계정 설정에서 VPC 공유 사용
- 사용 가능한 여러 서비스 및 옵션(예: NAT, PrivateLink, Transit Gateway 라우팅)을 사용하여 IP 중복 관리

도메인 2: 네트워크 구현

태스크 설명 2.1: 온프레미스 네트워크와 AWS 클라우드 간의 라우팅 및 연결을 구현합니다.

관련 지식:

- 라우팅 프로토콜(예: 정적, 동적)
- VPN(예: 보안, 가속 VPN)
- 계층 1 및 사용할 하드웨어 유형(예: 승인서(LOA) 문서, 콜로케이션 시설, Direct Connect)
- 계층 2 및 계층 3(예: VLAN, IP 주소 지정, 게이트웨이, 라우팅, 스위칭)
- 트래픽 관리 및 SD-WAN(예: Transit Gateway Connect)
- DNS(예: 조건부 전달, 호스팅 영역, 리졸버)
- 보안 어플라이언스(예: 방화벽)
- 로드 밸런싱(예: 계층 7 과 비교한 계층 4, 역방향 프록시, 계층 3)
- 인프라 자동화
- AWS Organizations 및 AWS Resource Access Manager(AWS RAM)(예: 다중 계정 Transit Gateway, Direct Connect, Amazon VPC, Route 53)
- 연결 테스트(예: Route Analyzer, Reachability Analyzer)

- VPC 의 네트워킹 서비스

관련 기술:

- 하이브리드 연결 솔루션에 대한 물리적 네트워크 요구 사항 구성
- 하이브리드 연결 솔루션과 함께 작동하도록 정적 또는 동적 라우팅 프로토콜 구성
- AWS 클라우드에 연결하도록 기존 온프레미스 네트워크 구성
- AWS 클라우드로 기존 온프레미스 이름 확인 구성
- 로드 밸런싱 솔루션 구성 및 구현
- AWS 서비스에 대한 네트워크 모니터링 및 로깅 구성
- 환경 간 연결 테스트 및 검증

태스크 설명 2.2: 여러 AWS 계정, 리전 및 VPC 에 라우팅 및 연결을 구현하여 다양한 연결 패턴을 지원합니다.

관련 지식:

- VPC 간 연결 및 다중 계정 연결(예: VPC 피어링, Transit Gateway, VPN, 서드 파티 공급 업체, SD-WAN, 다중 프로토콜 레이블 스위칭(MPLS))
- 프라이빗 애플리케이션 연결(예: PrivateLink)
- AWS 네트워킹 연결을 확장하는 방법(예: Organizations, AWS RAM)
- 애플리케이션 및 클라이언트에 대한 호스트 및 서비스 이름 확인(예: DNS)
- 인프라 자동화
- 인증 및 권한 부여(예: SAML, Active Directory)
- 보안(예: 보안 그룹, 네트워크 ACL, AWS Network Firewall)
- 연결 테스트(예: Route Analyzer, Reachability Analyzer, 도구)

관련 기술:

- 단일 VPC 또는 다중 VPC 설계에서 AWS 서비스를 사용하여 네트워크 연결 아키텍처 구성(예: DHCP, 라우팅, 보안 그룹)
- 기존 서드 파티 공급 업체 솔루션과 하이브리드 연결 구성
- 허브 앤 스포크 네트워크 아키텍처 구성(예: Transit Gateway, 전송 VPC)
- 하이브리드 연결이 가능하도록 DNS 솔루션 구성
- 네트워크 경계 간 보안 구현
- AWS 솔루션을 사용하여 네트워크 모니터링 및 로깅 구성

태스크 설명 2.3: 복잡한 하이브리드 및 다중 계정 DNS 아키텍처를 구현합니다.

관련 지식:

- 프라이빗 호스팅 영역 및 퍼블릭 호스팅 영역을 사용해야 하는 경우
- 트래픽 관리를 변경하는 방법(예: 지연 시간, 지리적 위치, 가중치 기반)
- DNS 위임 및 전달(예: 조건부 전달)
- 다양한 DNS 레코드 유형(예: A, AAAA, TXT, 포인터 레코드, 별칭 레코드)
- DNSSEC
- 계정 간에 DNS 서비스를 공유하는 방법(예: AWS RAM)
- 아웃바운드 및 인바운드 엔드포인트에 대한 요구 사항 및 구현 옵션

관련 기술:

- DNS 영역 및 조건부 전달 구성
- DNS 솔루션을 사용하여 트래픽 관리 구성
- 하이브리드 네트워크용 DNS 구성
- 적절한 DNS 레코드 구성
- Route 53 에서 DNSSEC 구성
- 중앙 집중식 또는 분산식 네트워크 아키텍처 내에서 DNS 구성
- Route 53 에서 DNS 모니터링 및 로깅 구성

태스크 설명 2.4: 네트워크 인프라를 자동화하고 구성합니다.

관련 지식:

- 코드형 인프라(IaC)(예: AWS Cloud Development Kit(AWS CDK), AWS CloudFormation, AWS CLI, AWS SDK, API)
- 이벤트 기반 네트워크 자동화
- 클라우드 네트워킹 리소스를 프로비저닝할 때 IaC 템플릿에서 하드 코딩된 명령 사용 시 일반적인 문제

관련 기술:

- 반복 가능한 네트워크 구성 생성 및 관리
- 이벤트 기반 네트워킹 기능 통합
- 하이브리드 네트워크 자동화 옵션을 AWS 기반 IaC 와 통합
- 가능한 최저 비용을 유지하면서 클라우드 네트워킹 환경에서 위험을 제거하고 효율성을 달성
- IaC 로 클라우드 네트워크 리소스 최적화 프로세스 자동화

도메인 3: 네트워크 관리 및 운영

태스크 설명 3.1: AWS 및 하이브리드 네트워크에서 라우팅 및 연결을 유지 관리합니다.

관련 지식:

- AWS 하이브리드 네트워크에서 사용되는 업계 표준 라우팅 프로토콜(예: Direct Connect 를 통한 BGP)
- AWS 및 하이브리드 네트워크에 대한 연결 방법(예: Direct Connect 게이트웨이, Transit Gateway, VIF)
- 제한 및 할당량이 AWS 네트워킹 서비스에 미치는 영향(예: 대역폭 제한, 경로 제한)
- 사용자 지정 서비스에 사용할 수 있는 프라이빗 및 퍼블릭 액세스 방법(예: PrivateLink, VPC 피어링)
- 사용 가능한 리전 간 커뮤니케이션 및 리전 내 커뮤니케이션 패턴

관련 기술:

- AWS 및 하이브리드 연결 옵션에 대한 라우팅 프로토콜 관리(예: Direct Connect 연결, VPN)
- 사용자 지정 서비스에 대한 프라이빗 액세스 유지 관리(예: PrivateLink, VPC 피어링)
- 라우팅 테이블을 사용하여 트래픽을 적절히 전달(예: 자동 전파, BGP)
- AWS 서비스에 대한 프라이빗 액세스 또는 퍼블릭 액세스 설정(예: Direct Connect, VPN)
- 동적 및 정적 라우팅 프로토콜을 통한 라우팅 최적화(예: 경로 요약, CIDR 중복)

태스크 설명 3.2: 네트워크 트래픽을 모니터링하고 분석하여 연결 패턴의 문제를 해결하고 연결 패턴을 최적화합니다.

관련 지식:

- 네트워크 성능 지표 및 도달 가능성 제약 조건(예: 라우팅, 패킷 크기)
- 네트워크 성능 및 연결 가능성 문제(예: 패킷 손실)를 평가하기 위한 적절한 로그 및 지표
- 로그와 지표를 수집하고 분석하는 도구(예: CloudWatch, VPC 흐름 로그, VPC 트래픽 미러링)
- 라우팅 패턴 및 문제를 분석하는 도구(예: Reachability Analyzer, Transit Gateway Network Manager)

관련 기술:

- 도구 출력을 분석하여 네트워크 성능을 평가하고 연결 문제를 해결(예: VPC 흐름 로그, Amazon CloudWatch Logs)
- 네트워크 토폴로지 매핑 또는 이해(예: Transit Gateway Network Manager)
- 패킷을 분석하여 패킷 셰이핑에서의 문제 식별(예: VPC 트래픽 미러링)
- 네트워크 구성 오류로 인해 발생하는 연결 문제 해결(예: Reachability Analyzer)
- 네트워크 구성이 네트워크 설계 요구 사항을 충족하는지 확인(예: Reachability Analyzer)
- 네트워크 구성 변경에 따른 연결 의도 확인 자동화(예: Reachability Analyzer)
- 네트워크 연결을 복원하기 위해 VPC 의 패킷 크기 불일치 문제 해결

태스크 설명 3.3: 성능, 신뢰성 및 비용 효율성을 위해 AWS 네트워크를 최적화합니다.

관련 지식:

- VPC 피어 또는 Transit Gateway 가 적절한 상황
- 대역폭 사용률을 줄이는 다양한 방법(예: 멀티캐스트와 비교한 유니캐스트, CloudFront)
- VPC 와 온프레미스 환경 간의 데이터 전송을 위한 비용 효율적인 연결 옵션
- AWS 기반 다양한 유형의 네트워크 인터페이스
- Route 53 의 고가용성 기능(예: 지연 시간 및 가중치 기반 레코드 세트와 함께 상태 확인을 사용한 DNS 로드 밸런싱)
- 신뢰성을 제공하는 Route 53 에서 옵션의 사용 가능성
- 로드 밸런싱 및 트래픽 분산 패턴
- VPC 서브넷 최적화
- 다양한 연결 유형에서 대역폭에 대한 프레임 크기 최적화

관련 기술:

- 네트워크 처리량(throughput) 최적화
- 최상의 성능을 위한 올바른 네트워크 인터페이스 선택(예: 탄력적 네트워크 인터페이스, Elastic Network Adapter(ENA), Elastic Fabric Adapter(EFA))
- 제공된 네트워크 요구 사항 분석을 기반으로 VPC 피어링, 프록시 패턴 또는 Transit Gateway 연결 중에서 선택
- 네트워크 요구 사항을 충족하기 위해 적절한 네트워크 연결 서비스(예: VPC 피어링, Transit Gateway, VPN 연결)에 솔루션 구현
- VPC 및 온프레미스 환경 내에서 멀티캐스트 기능 구현

- 애플리케이션 가용성을 최적화하기 위해 Route 53 퍼블릭 호스팅 영역 및 프라이빗 호스팅 영역 및 레코드 생성(예: 트래픽을 여러 가용 영역으로 라우팅하기 위한 프라이빗 영역 DNS 항목)
- 증가된 애플리케이션 로드를 지원하기 위해 자동 크기 조정 구성의 서브넷 업데이트 및 최적화
- VPC 내 사용 가능한 IP 주소의 고갈을 방지하기 위한 서브넷 업데이트 및 최적화(예: 보조 CIDR)
- 연결 유형 간에 점보 프레임 지원 구성
- 네트워크 성능 및 애플리케이션 가용성을 개선하기 위해 Global Accelerator 로 네트워크 연결 최적화

도메인 4: 네트워크 보안, 규정 준수 및 거버넌스

태스크 설명 4.1: 보안 및 규정 준수의 필요성 및 요구 사항을 충족하는 네트워크 기능을 구현하고 유지 관리합니다.

관련 지식:

- 애플리케이션 아키텍처를 기반으로 한 다양한 위협 모델
- 일반적인 보안 위협
- 다양한 애플리케이션 흐름을 보호하는 메커니즘
- 보안 및 규정 준수 요구 사항을 충족하는 AWS 네트워크 아키텍처

관련 기술:

- AWS 로 유입되는 인바운드 트래픽 흐름 보호(예: AWS WAF, AWS Shield, Network Firewall)
- AWS 의 아웃바운드 트래픽 흐름 보호(예: Network Firewall, 프록시, Gateway Load Balancer)
- 계정 내 또는 여러 계정에서 VPC 간 트래픽 보호(예: 보안 그룹, 네트워크 ACL, VPC 엔드포인트 정책)
- 보안 및 규정 준수 요구 사항을 충족하는 AWS 네트워크 아키텍처 구현(예: 신뢰할 수 없는 네트워크, 경계 VPC, 3 티어 아키텍처)
- 위협 모델 개발 및 지정된 네트워크 아키텍처에 대한 적절한 완화 전략 식별
- 초기 요구 사항 준수 테스트(예: 장애 조치 테스트, 복원력)
- AWS 를 사용하여 보안 인시던트 보고 및 알림 자동화

태스크 설명 4.2: 네트워크 모니터링 및 로깅 서비스를 사용하여 보안을 검증하고 감사합니다.

관련 지식:

- AWS 에서 사용할 수 있는 네트워크 모니터링 및 로깅 서비스(예: CloudWatch, AWS CloudTrail, VPC 트래픽 미러링, VPC 흐름 로그, Transit Gateway Network Manager)
- 알림 메커니즘(예: CloudWatch 경보)
- 다양한 AWS 서비스에서 로그 생성(예: VPC 흐름 로그, 로드 밸런서 액세스 로그, CloudFront 액세스 로그)
- 로그 전달 메커니즘(예:Amazon Kinesis, Route 53, CloudWatch)
- 네트워크 보안 구성을 감사하는 메커니즘(예: 보안 그룹, AWS Firewall Manager, AWS Trusted Advisor)

관련 기술:

- VPC 흐름 로그 생성 및 분석(흐름 로그의 기본 및 확장 필드 포함)
- 네트워크 트래픽 미러링 생성 및 분석(예: VPC 트래픽 미러링 사용)
- CloudWatch 를 사용하여 자동화된 경보 구현
- CloudWatch 를 사용하여 사용자 지정 지표 구현
- 단일 또는 여러 AWS 로그 소스에서 정보 상관 관계 파악 및 분석
- 로그 전달 솔루션 구현
- 단일 또는 여러 AWS 네트워크 서비스 및 계정에서 네트워크 감사 전략 구현(예: Firewall Manager, 보안 그룹, 네트워크 ACL)

태스크 설명 4.3: 네트워크 데이터 및 통신의 기밀성을 구현하고 유지 관리합니다.

관련 지식:

- AWS 에서 사용할 수 있는 네트워크 암호화 옵션
- Direct Connect 를 통한 VPN 연결
- 전송 중인 데이터의 암호화 방법(예: IPsec)
- AWS 공동 책임 모델에 따른 네트워크 암호화
- DNS 통신의 보안 방법(예: DNSSEC)

관련 기술:

- 애플리케이션 규정 준수 요구 사항(예: IPsec, TLS)을 충족하기 위한 네트워크 암호화 방법 구현
- 전송 중인 데이터를 보호하기 위한 암호화 솔루션 구현(예: CloudFront, Application Load Balancer 와 Network Load Balancer, Direct Connect 를 통한 VPN, AWS 관리형 데이터베이스, Amazon S3, Amazon EC2 의 사용자 지정 솔루션, Transit Gateway)
- 인증 기관(예: ACM, AWS Private Certificate Authority(ACM PCA))을 사용하여 인증서 관리 솔루션 구현
- 보안 DNS 통신 구현

부록

시험 범위에 포함되는 AWS 서비스 및 기능

다음 목록에는 시험 범위에 해당하는 AWS 서비스 및 기능이 나와 있습니다. 이 목록에 모든 사항이 포함된 것은 아니며 변경될 수 있습니다. AWS 제품 및 서비스는 주요 기능에 따라 다음과 같은 카테고리로 분류됩니다.

애플리케이션 통합:

- Amazon EventBridge
- Amazon Simple Notification Service(Amazon SNS)
- Amazon SQS(Amazon Simple Queue Service)

컴퓨팅:

- Amazon EC2
- Amazon EC2 Auto Scaling
- AWS Lambda

컨테이너:

- Amazon Elastic Container Registry(Amazon ECR)
- Amazon Elastic Container Service(Amazon ECS)
- Amazon Elastic Kubernetes Service(Amazon EKS)
- AWS Fargate

비용 관리:

- AWS Cost Explorer

프런트 엔드 웹 및 모바일:

- Amazon API Gateway

AWS 의 관리 및 거버넌스:

- AWS Auto Scaling
- AWS CLI
- AWS CloudFormation
- AWS CloudTrail

- Amazon CloudWatch
- AWS Config
- AWS Control Tower
- AWS Health Dashboard
- AWS Management Console
- AWS Organizations
- AWS Trusted Advisor
- AWS Well-Architected Tool

네트워킹 및 콘텐츠 전송:

- Amazon API Gateway
- AWS App Mesh
- AWS Client VPN
- AWS Cloud Map
- Amazon CloudFront
- AWS Direct Connect
- Elastic Load Balancing(ELB)
- AWS Global Accelerator
- AWS PrivateLink
- Amazon Route 53
- AWS Site-to-Site VPN
- AWS Transit Gateway
- Amazon VPC

보안, 자격 증명 및 규정 준수:

- AWS Firewall Manager
- AWS Identity and Access Management(IAM)
- AWS Network Firewall
- AWS Resource Access Manager(AWS RAM)
- AWS Shield
- AWS WAF

서버리스:

- Amazon API Gateway
- Amazon EventBridge
- AWS Fargate
- AWS Lambda
- Amazon Simple Notification Service(Amazon SNS)
- Amazon SQS(Amazon Simple Queue Service)
- Amazon Simple Storage Service(Amazon S3)

스토리지:

- Amazon S3

시험 범위가 아닌 AWS 서비스 및 기능

다음 목록에는 시험 범위가 아닌 AWS 서비스 및 기능이 나와 있습니다. 이 목록에 모든 사항이 포함된 것은 아니며 변경될 수 있습니다. 시험의 대상 작업 역할과 전혀 관련이 없는 AWS 제품 및 서비스는 다음 목록에서 제외됩니다.

분석:

- Amazon CloudSearch
- AWS Data Exchange
- AWS Data Pipeline
- Amazon EMR
- AWS Glue
- AWS Lake Formation
- Amazon Managed Streaming for Apache Kafka(Amazon MSK)
- Amazon OpenSearch Service
- Amazon QuickSight
- Amazon Redshift

AR 및 VR:

- Amazon Sumerian

Blockchain:

- Amazon Managed Blockchain
- Amazon Quantum Ledger Database(Amazon QLDB)

개발자 도구:

- AWS Device Farm
- AWS X-Ray

로보틱스:

- AWS RoboMaker

인공위성:

- AWS Ground Station

설문 조사

이 시험 안내서가 도움이 되었나요? 설문 조사에 참여하여 의견을 공유해 주시기 바랍니다.