aws training and certification

# AWS 공인 고급 네트워킹 - 전문 분야
# AWS Certified Advanced Networking – Specialty
# (ANS-C00) 시험 샘플 문항

**1) 회사의 온프레미스 네트워크에 11.11.0.0/16의 IP 주소 범위가 있습니다. 서버 간 통신 시 이 네트워크 범위 내의 IP만 사용할 수 있습니다. 클라우드에는 IP 주소 범위 11.11.253.0/24가 할당되었습니다.**

**네트워크 엔지니어는 AWS에서 VPC를 설계해야 합니다. VPC 내부 서버는 VPN 연결을 통해 인터넷 및 온프레미스에서 모두 호스트와 통신할 수 있어야 합니다.**

**이러한 요구 사항을 충족하는 구성 단계 조합은 무엇입니까? (2개를 선택하십시오.)**

A) VPC를 IP 주소 11.11.253.0/24로 설정한다.

B) VPC를 RFC 1918 프라이빗 IP 주소 범위(예: 10.10.10.0/24)로 설정한다. 모든 아웃바운드 트래픽에 대해 10.10.10.0/24 및 11.11.253.0/24 간 변환 작업을 수행하도록 NAT 게이트웨이를 설정한다.

C) 가상 프라이빗 게이트웨이 및 온프레미스 라우터 간의 VPN 연결을 설정한다. 모든 트래픽에 대해 가상 프라이빗 게이트웨이를 기본 게이트웨이로 설정한다. 트래픽을 인터넷으로 전달하도록 온프레미스 라우터를 구성한다.

D) 가상 프라이빗 게이트웨이 및 온프레미스 라우터 간의 VPN 연결을 설정한다. 11.11.0.0/24로 전달되는 트래픽에 대해 가상 프라이빗 게이트웨이를 기본 게이트웨이로 설정한다. VPC 서브넷 라우팅을 추가하여 모든 인터넷 트래픽에 대해 기본 게이트웨이를 인터넷 게이트웨이로 지정한다.

E) VPC를 RFC 1918 프라이빗 IP 주소 범위(예: 10.10.10.0/24)로 설정한다. 모든 아웃바운드 패킷의 소스 IP를 11.11.0.0/16으로 변환하도록 가상 프라이빗 게이트웨이를 설정한다.

**2) 네트워크 엔지니어는 다른 VPC 및 리전에서 공개적으로 액세스할 수 있는 Amazon RDS 다중 AZ DB 인스턴스에 연결하기 위해 Amazon EC2 인스턴스에서 실행되는 애플리케이션에 대한 솔루션을 설계해야 합니다. 보안 요구 사항은 트래픽이 인터넷을 통과하면 안 된다는 것입니다.**

**어떤 구성을 통해 인스턴스가 인터넷을 통해 트래픽을 라우팅하지 않고 비공개로 통신할 수 있습니까?**

A) 다른 VPC 간에 트래픽을 직접 라우팅하기 위해 VPC 간에 피어링 연결을 생성하고 라우팅 테이블을 업데이트한다. VPC 피어링 연결에 대한 DNS 확인 지원을 활성화한다. DB 인스턴스의 DNS 엔드포인트에 연결하도록 애플리케이션을 구성한다.
B) DB 인스턴스에 대한 게이트웨이 엔드포인트를 생성한다. 게이트웨이 엔드포인트로 트래픽을 라우팅하도록 애플리케이션 VPC의 라우팅 테이블을 업데이트한다.
C) VPC 간에 비공개로 트래픽을 라우팅하도록 전송 VPC를 구성한다. DB 인스턴스의 DNS 엔드포인트에 연결하도록 애플리케이션을 구성한다.
D) EC2 인스턴스와 동일한 서브넷에서 NAT 게이트웨이를 생성한다. NAT 게이트웨이를 통해 DB 인스턴스의 DNS 엔드포인트로 트래픽을 라우팅하도록 애플리케이션 VPC의 라우팅 테이블을 업데이트한다.

**3) 어떤 회사가 중요한 환경을 AWS에서 구현했습니다. 네트워크 엔지니어는 규정 준수를 위해 Amazon EC2 인스턴스가 특정 승인된 보안 그룹을 사용하고 특정 VPC에 속하는지 확인해야 합니다. 인스턴스의 구성 내역은 기록되어야 하며, 규정 준수 문제 발생 시 인스턴스가 자동으로 중지되어야 합니다.**

**이러한 요구 사항을 충족하려면 어떻게 해야 합니까?**

A) AWS CloudTrail을 활성화하고 사용자 지정 Amazon CloudWatch 경보를 생성하여 필요한 검사를 수행한다. CloudWatch 경보가 실패 상태이면 이 인스턴스 작업을 중지하여 규칙 미준수 EC2 인스턴스를 중지한다.
B) AWS Lambda 함수를 호출하여 필요한 검사를 수행하도록 AWS CloudWatch Events에서 예약 이벤트를 구성한다. 규칙 미준수 리소스가 있는 경우 다른 Lambda 함수를 호출하여 EC2 인스턴스를 중지한다.
C) AWS Lambda 함수를 트리거하는 EC2 인스턴스 상태 변경 알림에 대해 필요한 검사를 수행하도록 AWS CloudWatch Events에서 이벤트를 구성한다. 규칙 미준수 리소스가 있는 경우 다른 Lambda 함수를 호출하여 EC2 인스턴스를 중지한다.
D) AWS Config 및 사용자 지정 AWS Config 규칙을 활성화하여 필요한 검사를 수행한다. 규칙 미준수 리소스가 있는 경우 문제 해결 작업으로 AWS Systems Manager 문서를 실행하여 EC2 인스턴스를 중지한다.

**4) 어떤 회사에서 온프레미스 데이터 센터를 AWS로 확장하려 합니다. 피크 트래픽 1Gbps에서 2Gbps 사이로 예상됩니다. 네트워크 엔지니어는 AWS 및 데이터 센터 간에 피크 트래픽을 처리하기에 충분한 대역폭이 있는지 확인해야 합니다. 이 솔루션은 가용성이 높고 비용 효율적이어야 합니다.**

**이러한 요구 사항을 해결하려면 무엇을 구현해야 합니까?**

A) IPsec VPN 백업으로 하나의 10Gbps AWS Direct Connect 연결을 배포한다.
B) 링크 집계 그룹에 두 개의 1Gbps AWS Direct Connect 연결을 배포한다.
C) 링크 집계 그룹에 있는 두 개의 1Gbps AWS Direct Connect 연결을 두 개의 서로 다른 Direct Connect 위치에 배포한다.
D) 하나의 10Gbps AWS Direct Connect 연결을 두 개의 서로 다른 Direct Connect 위치에 배포한다.

**5) 네트워크 엔지니어는 회사의 Amazon S3 버킷에 대한 액세스를 특정 소스 네트워크로 제한해야 합니다.**

**이를 달성하기 위해 네트워크 엔지니어는 어떻게 해야 합니까?**

A) S3 버킷에 지정된 네트워크의 CIDR 블록에 대한 액세스를 제한하는 ACL을 만든다.
B) S3 버킷에 조건 문을 사용하여 지정된 네트워크의 CIDR 블록에 대한 액세스를 제한하는 버킷 정책을 만든다.
C) 지정된 네트워크의 CIDR 블록에 대한 인바운드 액세스를 허용하는 보안 그룹을 만들고 S3 버킷에 적용한다.
D) 지정된 네트워크의 CIDR 블록에 대한 인바운드 액세스를 허용하는 보안 그룹을 만들고, S3 VPC 종단점을 만든 다음 이 보안 그룹을 이 VPC 종단점에 적용한다.

**6) 회사의 규정 준수 요구 사항에는 악의적인 활동을 식별하기 위해 웹 애플리케이션 로그를 수집하고 분석해야 한다고 명시되어 있습니다. 네트워크 엔지니어는 웹 인스턴스의 네트워크 인터페이스를 원격으로 변경하려는 시도가 있는지도 모니터링해야 합니다.**

**이러한 요구 사항을 충족하려면 어떤 서비스 및 구성이 필요합니까?**

A) Amazon CloudWatch Logs 에이전트를 웹 인스턴스에 설치하여 애플리케이션 로그를 수집한다. VPC 플로우 로그를 사용하여 데이터를 CloudWatch Logs로 전송한다. CloudWatch Logs 지표 필터를 사용하여 로그 데이터에서 검색할 패턴을 정의한다.

B) 모든 관리 이벤트 및 데이터 이벤트를 사용자 지정 Amazon S3 버킷 및 Amazon CloudWatch Logs에 로깅하도록 AWS CloudTrail을 구성한다. VPC 플로우 로그를 사용하여 데이터를 CloudWatch Logs로 전송한다. CloudWatch Logs 지표 필터를 사용하여 로그 데이터에서 검색할 패턴을 정의한다.

C) 모든 관리 이벤트를 사용자 지정 Amazon S3 버킷 및 Amazon CloudWatch Logs에 로깅하도록 AWS CloudTrail을 구성한다. Amazon CloudWatch Logs 에이전트를 웹 인스턴스에 설치하여 애플리케이션 로그를 수집한다. CloudWatch Logs Insights를 사용하여 로그 데이터에서 검색할 패턴을 정의한다.

D) AWS Config를 활성화하여 웹 인스턴스의 모든 구성 변경을 기록한다. 모든 관리 이벤트 및 데이터 이벤트를 사용자 지정 Amazon S3 버킷에 로깅하도록 AWS CloudTrail을 구성한다. Amazon Athena를 사용하여 Amazon S3에 저장된 로그 데이터에서 검색할 패턴을 정의한다.

**7) 회사에 기밀 데이터를 처리하는 애플리케이션이 있습니다. 이 데이터는 현재 온프레미스 데이터 센터에 저장되어 있습니다. 네트워크 엔지니어는 워크로드를 AWS로 이동하려고 하며, AWS로 전송 중인 데이터의 기밀성 및 무결성을 확보해야 합니다. 회사에는 기존 AWS Direct Connect 연결이 있습니다.**

**네트워크 엔지니어가 온프레미스 데이터 센터와 AWS 간에 가장 비용 효율적인 연결을 설정하기 위해 수행해야 하는 단계는 무엇입니까? (2개를 선택하십시오.)**

A) 인터넷 게이트웨이를 VPC에 연결한다.

B) AWS Direct Connect 연결에 퍼블릭 가상 인터페이스를 구성한다.

C) 가상 프라이빗 게이트웨이에 대한 프라이빗 가상 인터페이스를 구성한다.

D) 고객 게이트웨이와 Amazon EC2의 소프트웨어 VPN 사이에 IPsec 터널을 설정한다.

E) 고객 게이트웨이와 가상 프라이빗 게이트웨이 사이에 사이트 간 VPN을 설정한다.

**8) 한 회사에서 전자 상거래 웹 사이트에 사용할 새로운 기능을 만들고 있습니다. 이러한 기능은 서비스마다 다른 도메인 이름을 사용하여 마이크로서비스로 배포됩니다. 이 회사는 모든 퍼블릭 웹 사이트에 HTTPS를 사용해야 합니다. 애플리케이션에는 클라이언트의 소스 IP가 필요합니다.**

**이를 달성하려면 어떤 작업 조합을 따라야 합니까? (2개를 선택하십시오.)**

A) Network Load Balancer를 사용하여 각 서비스로 트래픽을 배포한다.
B) Application Load Balancer를 사용하여 각 서비스로 트래픽을 배포한다.
C) X-Forwarded-For 헤더를 사용하여 클라이언트 IP를 가져오도록 애플리케이션을 구성한다.
D) X-Forwarded-Host 헤더를 사용하여 클라이언트 IP를 가져오도록 애플리케이션을 구성한다.
E) 프록시 프로토콜 헤더를 사용하여 클라이언트 IP를 가져오도록 애플리케이션을 구성한다.

**9) 네트워크 엔지니어가 고성능 컴퓨팅 솔루션을 AWS에 설계하고 있습니다. 이 시스템은 지연 시간이 짧은 통신이 필요한 Amazon EC2 인스턴스의 클러스터로 구성되어 있습니다.**

**이러한 요구 사항을 충족하는 방법은 무엇입니까?**

A) 인스턴스를 클러스터에 필요한 인스턴스의 수와 같은 크기의 단일 서브넷으로 실행한다.
B) 클러스터 배치 그룹을 생성한다. Elastic Fabric Adapter(EFA)를 사용하는 인스턴스를 배치 그룹으로 실행한다.
C) Amazon EC2 인스턴스를 사용 가능한 가장 큰 수의 코어 및 램으로 실행한다. Amazon EBS 프로비저닝된 IOPS(PIOPS) 볼륨을 연결한다. 클러스터의 모든 인스턴스에 공유 메모리 시스템을 구현한다.
D) 확장 네트워킹을 제공하는 Amazon EC2 인스턴스 유형을 선택한다. 하나의 10Gbps 비차단형 탄력적 네트워크 인터페이스를 인스턴스에 연결한다.

**10) 회사의 내부 보안 팀은 회사 네트워크 내에서 Amazon S3 액세스를 허용하라는 요청을 받았습니다. 모든 외부 트래픽은 회사 방화벽을 통해 명시적으로 허용해야 합니다.**

**보안 팀은 어떤 방법으로 이 액세스 권한을 부여할 수 있습니까?**

A) 스크립트를 예약하여 Amazon S3 IP 접두사를 AWS 개발자 포럼 공지 사항에서 다운로드한다. 그에 따라 방화벽 규칙을 업데이트한다.

B) 스크립트를 예약하여 Amazon S3 IP 접두사를 ip-ranges.json 파일을 다운로드하고 구문 분석한다. 그에 따라 방화벽 규칙을 업데이트한다.

C) 스크립트를 예약하여 Amazon S3 엔드포인트에서 DNS 조회를 수행한다. 그에 따라 방화벽 규칙을 업데이트한다.

D) AWS Direct Connect를 사용하여 데이터 센터를 VPC에 연결한다. 데이터 센터의 트래픽을 Amazon S3 VPC 종단점으로 전달하는 라우팅을 만든다.

**답**

1) A, C - VPC는 할당된 범위에서 CIDR 블록을 사용해야 합니다(또한 데이터 센터와 중첩되지 않아야 함). VPC로 향하지 않는 모든 트래픽은 가상 프라이빗 게이트웨이로 라우팅된 다음(이 라우팅은 가정됨) 온프레미스로 도착하면 인터넷으로 전달되어야 합니다. B와 E는 할당된 범위에 없기 때문에 정답이 아닙니다(RFC가 아닌 1918 주소는 VPC에서 사용할 수 있음). D는 인터넷 게이트웨이를 통해 트래픽을 인터넷으로 전달하기 때문에 정답이 아닙니다.

2) A - VPC 피어링 연결의 DNS 확인을 구성하면 애플리케이션 VPC에서 온 쿼리가 DB 인스턴스의 프라이빗 IP로 확인될 수 있고, 인터넷을 통해 라우팅되지 않을 수 있습니다. Amazon RDS는 게이트웨이 엔드포인트에서 지원하지 않기 때문에 B는 정답이 아닙니다. 데이터베이스 엔드포인트는 퍼블릭 IP로 확인되고 트래픽이 인터넷을 거치므로 C와 D는 정답이 아닙니다.

3) D - AWS Config는 사용자 AWS 계정의 AWS 리소스 구성에 대한 세부 정보 보기를 제공합니다. AWS Systems Manager Automation 문서로 AWS Config 규칙을 사용하면 규칙 미준수 리소스 문제를 자동으로 해결할 수 있습니다.

4) C - 충분한 대역폭과 고가용성을 제공하려면 두 개의 서로 다른 Direct Connect 위치에서 두 개의 AWS Direct Connect 연결이 링크 집계 그룹에 있어야 합니다. 하나의 Direct Connect 위치가 장애를 겪으면 두 번째 Direct Connect 위치에 있는 두 개의 Direct Connect 연결이 백업을 제공합니다. 연결이 끊어지면 나머지 모든 옵션은 피크 트래픽을 처리할 수 없습니다.

5) B - 조건 문을 사용하는 Amazon S3 버킷 정책은 특정 IP 주소 범위에서 요청이 들어오면 액세스 제한을 지원합니다. S3 ACL은 IP 제한을 지원하지 않기 때문에 A는 정답이 아닙니다. 보안 그룹은 S3 버킷에 적용될 수 없기 때문에 C는 정답이 아닙니다. 보안 그룹은 S3 VPC 종단점에 적용될 수 없기 때문에 D는 정답이 아닙니다.

6) C - 웹 애플리케이션 로그는 운영 체제 내부에 있으며, Amazon CloudWatch Logs Insights는 CloudWatch 에이전트를 사용하여 로그를 수집하고 구성하는 데 사용할 수 있습니다. AWS CloudTrail은 모든 AWS API 활동을 모니터링하며, 특정한 API 호출을 모니터링하여 웹 인스턴스의 네트워크 인터페이스를 원격으로 변경하려는 시도를 식별할 수 있습니다.

7) B, E - AWS Direct Connect 연결을 통해 VPN을 설정하면 전송 중인 데이터를 보호할 수 있습니다. 이렇게 하려면 퍼블릭 가상 인터페이스를 설정하고 이를 사용하여 데이터 센터와 가상 프라이빗 게이트웨이 간의 Site-to-Site VPN을 만듭니다. A는 트래픽을 퍼블릭 인터넷을 통해 전송하기 때문에 정답이 아닙니다. VPN 터널 IP를 알리려면 퍼블릭 가상 인터페이스가 필요하기 때문에 C는 정답이 아닙니다. D는 기존의 Direct Connect 연결을 활용하지 않으므로 정답이 아닙니다.

8) B, C - Application Load Balancer는 도메인 이름을 기반으로 트래픽을 다른 마이크로서비스로 라우팅하는 데 필요한 호스트 기반 라우팅을 지원합니다. X-Forwarded-For는 클라이언트의 소스 IP 주소를 식별하는 올바른 요청 헤더입니다.

9) B - 클러스터 배치 그룹 및 Elastic Fabric Adapter(EFA)는 짧은 네트워크 지연 시간과 높은 네트워크 처리량이 필요한 고성능 컴퓨팅 애플리케이션에 권장됩니다. 서브넷 크기가 네트워크 성능에 영향을 주지 않기 때문에 A는 정답이 아닙니다. Amazon EBS 볼륨은 Amazon EC2 인스턴스 간에 공유할 수 없기 때문에 C는 정답이 아닙니다. 확장 네트워킹이 EC2 인스턴스의 네트워크 동작에 영향을 주지만 인스턴스 간 네트워크 인프라에는 영향을 주지 않기 때문에 D는 절반만 정답입니다.

10) B - ip-ranges.json 파일에는 AWS에서 사용하는 최신 IP 주소 목록이 포함되어 있습니다. AWS는 더 이상 IP 접두사를 개발자 포럼 공지 사항에 게시하지 않습니다. DNS 조회는 사용 가능한 IP 접두사의 전체 목록을 제공하지 않습니다. D는 전이적 라우팅이 필요하지만 이는 불가능합니다.