* Udemy 모의고사
- EC2 인스턴스에 Public/Private IP 를 ENI 2 개에 각각 주고 양쪽 모두 DNS 를 사용하기 위해서는 2 가지를 설정해야 함
    - VPC 의 DNS Hostnames 사용
    - Route 53 에서 Public/Private Hosting Zone 생성
- ALB(Applicatoin Load Balancer)의 지정 가능한 대상 그룹은 Instance, IP, Lambda 3 가지
- Route 53 Resolver
    - VPC 와 온프레미스 네트워크 사이에 DNS 쿼리를 라우팅하는 서비스
    - 온프레미스에서 온 DNS 쿼리가 AWS 호스팅 도메인을 해석할 수 있도록 인바운드/아웃바운드 쿼리 기능을 제공함
    - 온프레미스 DNS 인프라와 AWS 사이에는 Direct Connect 혹은 VPN 통해 연결이 설정되어있어야 함
    - Route 53 Resolver inbound/outbound endpoint 와 Private Hosted Zone 설정 필요
- 다른 AZ 간의 EC2 인스턴스 통신은 송신/수신 요금이 부과됨
- Direct Connect 에서 BGP 라우팅을 지원하는 라우터(R1, R2) 2 개가 있고 R1 Down 시 Failover 를 하기 위해서는 다음 설정이 필요
    - 경로 광고시 R2 에 AS Path Prepend 설정
    - R1 하위 BGP MED 를 사용하여 VGW(Virtual Private Gateway)에 AS 로의 기본 경로 광고
- AWS WAF 는 Cloudfront, ALB, API Gateway, EC2 에서 실행되는 웹서버에 적용 가능
- 기본 라우팅 테이블은 삭제할 수 없으며, 모든 서브넷에 사용됨
- Direct Connect 에 광고할 수 있는 IP Prefix 는 최대 100 개
- EC2 의 최소 대기시간과 최대 패킷 처리량을 보장하기 위해서는 다음 설정이 필요
    - 올바른 ENA 드라이버 설치
    - SR-IOV 를 지원하는 인스턴스 선택
- 새로운 AWS 계정을 생성시 다음 3 가지를 갖춘 VPC 가 생성됨
    - 리전마다 기본 VPC 생성
    - 기본 VPC 에 Internet Gateway 연결됨
    - 위 2 가지는 결국 Public Subnet 생성을 의미
- Direct Connect 의 Private VIF 설정을 위해서는 3 가지가 필요
    - Virutal Private Gateway, VLAN, BGP ASN
- Peering 관계에 있는 두 VPC 에서 다른 VPC 에 대한 DNS 조회 수행을 위해서는 요청자 및 수락자의 DNS 확인 허용 설정 필요

- Route 53 Private Hosting Zone 은 승인된 모든 AWS 계정의 VPC 를 포함할 수 있으며, 모든 Region 의 VPC 를 포함할 수 있음
- VPC 내 심층 패킷 검사가 필요할 경우 VPC Flow Logs 보다는 Wireshark 가 설치된 NAT Instance 가 더 유용함
- Network ACL 의 제한은 VPC 당 200 개의 ACL, ACL 당 20 개 규칙(VPC 에 최대 200 개의 Subnet 을 만들 수 있으므로 ACL 또한 200 개)
- 리전당 VPC 는 최대 5 개까지 가능하며 VPC 당 서브넷은 200 개까지 가능
- 각 리전의 탄력적 IP 주소는 5 개까지 가능
- IPSEC VPN 연결을 위해서는 UDP 포트 500 및 IP Protocol Field(ESP : 50, AH: 51)이 필요
- Direct Connect 연결을 위한 고객 라우터의 요구사항은 BGP ASN, 광케이블 연결, 802.1q 3 가지
- EIP 를 EC2 인스턴스에 할당할 때 EIP 를 할당할 인터페이스 혹은 인스턴스를 선택할 수 있으며, 인스턴스가 중지된 후 재시작되어도 유지됨
- Private Subnet 의 EC2 인스턴스가 외부 인터넷에 URL 형식으로 제한적 접근해야 할 경우, Squid URL 을 이용한 Proxy Server 를 이용하여야 함
- AWS WAF 를 이용하면 IP Match condition 을 이용하여 접근가능한 IP 의 Whitelist 를 지정할 수 있음
- VPC 에 IP 가 추가로 필요할 경우 IPv4 Secondary IP 대역을 추가하거나 IPv6 IP 대역을 추가하면 가능(IPv6 는 하나의 대역만 가능)
- NAT Gateway 는 고유한 Destination IP 에 대해서 55,000 개의 동시다발적 연결을 생성할 수 있으며 1024-65535 포트를 제공함
- VPC Flow Logs 를 사용하기 위해서는 다음 2 가지가 필요함
    - Flow Logs 를 생성하고 Log Group 에 연결
    - CloudWatch Logs 에 게시할 권한을 부여해 줄 IAM Role
- BGP Routing 의 Default Weight 는 32768
- VPC 의 예약주소는 x.x.x.0 ~ x.x.x.3 과 x.x.x.255 총 5 개
- Cloudfront 의 Match Viewer 옵션을 사용하게 되면 Cloudfront 와 Origin Server 가 어떤 프로토콜(HTTP,HTTPS)를 사용하여 통신할 것인지 결정함
- CloudHSM 을 사용하여 암호화 키를 제공할 경우, 또다른 VPC 에 다수의 HSM 이 포함된 클러스터를 생성하여 서비스를 제공하는 것이 좋음
- ENA 는 최대 100 Gbps 까지 지원하며, Intel 82599 는 10 Gbps 까지 지원

* Braincert Test 1
- Enhanced Networking 사용 조건
    - 적합한 드라이버를 포함해야 함

- HVM AMI 로 시작해야 함
- VPC 를 사용해야 함
- Amazon Linux AMI 가 아니더라도 적합한 드라이버를 설치하면 사용 가능

- 상태 확인이 복잡한 Route 53 구성에서 작동하는 방식(Latency 와 Weighted 의 조합)을 사용할 경우 Weighted Resource Set 를 먼저 설정해야 함
- VPN 의 경우, 비용을 낮게 유지할 수 있지만 속도가 낮고 예측할 수 없기 때문에 선호되는 옵션이 아님. 전체 데이터 전송 비용을 줄이려 한다 하더라도 Direct Connect 를 우선시해야 함.
- 하이브리드 클라우드에서 새로운 VPC 추가시 새로운 VPC 와 On-premise 모두 DNS 레코드 확인을 위해 해야 할 2 가지
  - 새 VPC 를 포함하도록 Route 53 Private Hosting Zone 의 VPC 연결 업데이트
  - 새 VPC 에서 EC2 기반의 DNS Proxy 시작 후 On-premise DNS 에서 전달자로 프록시 지정
- Direct Connect 를 사용하여 'Resilience'를 얻기 위해서는 동일한 Direct Connect Location 에 연결을 하나 더 생성해야 함
- NAT Gateway 는 DNS Whitelist 를 제공하지 않으므로 Squid Proxy 가 NAT Instance 에서 역할을 대신함
- (중요!!)Private ASN 을 사용하는 Direct Connect 를 Active/Passive 구성으로 만들기 위해 On-premise Router 에 필요한 BGP 구성
  - Local Preference 을 이용한 아웃바운드 트래픽 제어
  - 하나의 Direct Connect 연결을 통해 구체적인 접두사 광고
- ALB, NLB, CLB 모두 HTTPS(혹은 TLS) 사용시 보안정책 선택 가능
  - CLB 는 사용자 지정 보안정책 가능
- Direct Connect 의 Private VIF 의 경우 BGP Session 을 통해 100 개보다 더 많은 경로를 알리는 경우 BGP Session 이 유휴 상태로 전환되므로 100 개 이하로 경로를 요약하는 것이 좋음
- On-premise 에서 VPC 로 접근하기 위한 DNS 설정이 되어 있고, VPC 에서 On-premise 로 접근할 수 있는데 On-premise 에서 접근이 불가능하다면 VPC 의 Newtork ACL 을 살펴보아야 함
- Transit VPC : On-premise 와 AWS 연결시 하나의 VPC 를 필두로 다른 VPC 와 연결하고 싶다면 Tranist VPC 설정을 하는 것이 좋음
  - 거점이 될 VPC 와 On-premise 를 VPN 연결
  - 거점 VPC 와 다른 VPC 들을 VPN 으로 연결
- Cluster Placement Groups 은 1 개의 AZ 에서만 사용 가능하기에 다수의 AZ 에서는 쓸 수 없음

- PV Virtualization 은 Enhanced Networking 을 지원하지 않음
- Amazon Linux 2, Linuex AMI 2018.03 은 ENI 를 지원함
- Amazon Workspace 는 AWS 의 가상 데스크탑 서비스로 Directy Service 를 이용해 기존 인증 과정을 그대로 사용할 수 있음
- Direct Connect 의 고가용성을 높이는 방법은 VPN 을 설정하거나 동일한 리전에 대해 새로운 Direct Connect 연결과 Private VIF 를 만드는 것
- VPN 은 대역폭을 보장해주지 않으므로 안정적인 데이터 이동과 Application 관리를 위해서는 Direct Connect 이중화가 더 나은 결과를 가져옴
- DHCP 옵션 세트는 한 번 생성하고 나면 수정할 수 없으므로, 새로운 세트를 만들어야 함
- ALB 는 Lambda 함수를 대상으로 사용할 수 있으며, Lambda@Edge 는 Cloudfront 와 연계하여 헤더를 체크하고 성능을 향상시킴
- DHCP 옵션 세트 지원 기능
    - 도메인 네임 서버 IP 저장
    - NTP 서버 IP 저장
    - NetBIOS 네임 서버 IP 저장
- Lambda@edge 는 Cookie 를 제어할 뿐만 아니라 HTTP header 를 제어하여 사용중인 디바이스를 기반으로 최종 사용자에게 다양한 객체를 반환할 수 있음
- On-premise 와 겹치는 대역을 갖는 VPC 가 On-premise 뿐만 아니라 외부 인터넷과도 통신해야한다면 일치하지만 좀더 작은 네트워크 대역을 갖고 Default gateway 를 On-premise 로 잡는 것이 좋음
- 1 ~ 2 Gbps 가 오가는 Direct Connect 를 안정적으로 사용하기 위해서는 가용성을 감안하여 3 개의 1Gbps Direct Connect 연결을 갖는 것이 좋음
- Cloudfront 에서의 SSL 인증서 사용
    - 최종 사용자와 Cloudfront 간의 인증서 사용 : 신뢰할 수 있는 타사 인증서 혹은 ACM 제공 인증서
    - Cloudfront 와 사용자 지정 오리진 간의 인증서 사용 : 신뢰할 수 있는 타사 인증서, Origin 이 ELB 인 경우 ACM 사용 가능
- LAG 는 LACP(Link Aggregation Control Protocol)을 사용하여 단일 Direct Connect 엔드포엔트에서 다수의 연결을 가능케하는 논리적 인터페이스를 뜻함
    - LAG 의 모든 연결은 동일한 대역폭을 사용해야 함
    - 최대 4 개의 연결이 가능하며 동일한 엔드포인트로 연결되어야 함
- 호스트 이름을 요청을 라우팅하는 ALB 의 Host Condition 설정시 *.example.com 과 example.com 은 다른 경우이기 때문에 따로 설정해야 함

- 외부 인터넷을 통하지 않고 VPC 의 내부 EC2 인스턴스들이 S3 에 접근하기 위해서는 2 가지 방법이 있음
    - DNS Filtering 기능이 있는 NAT 인스턴스의 Squid proxy 사용
    - VPC Endpoint 사용

* Braincert Test 2
- Direct Connect Gateway 는 하나의 회선을 통해 이미 연결된 VPC 뿐만 아니라 다른 리전의 다른 VPC 에도 연결할 수 있음(Direct Connect Gateway 사용)
- 동일한 DNS Entry 에 대해 Public / Private Access 를 가능케 하고 싶은 경우 2 가지가 필요
    - Route 53 의 Public / Private Hosted Zone 생성
    - VPC 의 enableDnsHostnames, enableDnsSupport 활성화
- AWS Workspace 의 VPC 요구사항
    - 최소 2 개 이상의 AZ
    - Outbound Traffic 에 대해 NAT
- 하이브리드 네트워크에서 서로간의 내부 DNS 질의를 위한 구성
    - On-premise DNS Server 와 EC2 Instance Forwarder 를 구성
    - DHCP Option set 를 새롭게 생성하여 On-premise DNS 와 AWS Provided DNS Server IP 를 적고 적용
- Website 를 A/B 로 나누어 성능 테스트를 하고자할 경우 Route 53 의 Weighted Routing 을 사용하는 것이 좋음
- EC2 Metadata 허용은 Outbound 80 ?
- On-premise 에서 경로 전파가 제대로 되고 있음에도 AWS 측에서 On-premise 로 접근이 되지 않는다면 2 가지를 살펴야 함
    - Route table 내 Virtual Private Gateway(VGW)로의 라우팅 전파 허용
    - On-premise 쪽으로의 Route table 경로 추가
- Client 와 Server 간 SSL 상호 인증이 필요할 경우, ELB 가 Client 인증서를 검증할 수 없기 때문에 TCP 를 써야 함
- VPC 와 서브넷에 제한되는 CIDR 블록(10.0.0.0/8)
    - 172.16.0.0/12
    - 192.168.0.0/16
    - 198.19.0.0/16
- VPC 와 서브넷에 제한되는 CIDR 블록(172.16.0.0/12)
    - 192.168.0.0/16
    - 172.31.0.0/16
    - 10.0.0.0/8
    - 198.19.0.0/16
- VPC 와 서브넷에 제한되는 CIDR 블록(192.168.0.0/16)
    - 172.31.0.0/16

    - 10.0.0.0/8
    - 198.19.0.0/16
- 위 3 대역에서 모두 허용하는 목록
    - 각자의 대역 + 공개적으로 라우팅이 가능한 모든 IPv4 CIDR 블록 + 100.64.0.0/10
- NAT Gateway 는 사전 정의된 포트를 전달하는 기능이 없기 때문에 Squid Proxy 를 설치하여야 함
- VPC Flow Logs 는 포트 스캔을 캡쳐할 수 있으며 Lambda 를 이용해 트리거하여 알람을 보낼 수 있음
- AWS 리전간 보안그룹 적용시 상대방의 보안그룹 ID 가 아닌 CIDR 블록 기반 규칙을 지정해야 함
- Direct Connect 는 Cloudwatch 의 지표를 사용하여 터널의 상태를 확인할 수 있음
- Direct Conncet 가상 인터페이스의 기본 설정은 다음과 같음
    - Public : VLAN ID, BGP Public ASN, 사용자와 AWS 의 Peer IP /30
    - Private : VLAN ID, BGP Private ASN, Virtual Private Gateway
- Route 53 을 사용하여 S3 Static Web Site 를 호스팅하려면 Alias Record 과 Route 53 Hosted Zone 생성
- Direct Connect 서비스를 사용하기 위해 통신 사업자를 통해 필요 구성을 완성한 뒤 AWS 측에 문의하기 위해서는 Console 을 통해 연결을 만들고 AWS 의 메일을 기다려야 함
- nginx log 는 그저 로그에 불과하기 때문에 X-Forwarded-For 값으로 무언가를 하긴 힘듬. Application 에서 X-Forwarded-For 값을 사용하도록 수정하고 Cloudfront 의 Geographic Restriction 을 사용해야 함
- Cloudfront 의 Geographic Restriction 은 Whitelist 와 Blacklist 로 나뉘며 국가를 지정할 수 있음
- AWS 에서의 심층 패킷 분석은 third-party solution 을 통해 하는 것이 바람직함
- Route 53 에서 Latency 와 Weighted 를 이용한 방식 : https://docs.aws.amazon.com/ko_kr/Route53/latest/DeveloperGuide/dns-failover-complex-configs.html
- S3 Bucket 이 2 개가 존재하고 Direct Connect 를 이용해 짧은 지연시간과 효율적인 비용을 모두 달성하기 위해서는 가까운 Region 하나에만 Direct Connect 를 연결

* Braincert Test 3
- 다수의 VPC 가 존재할 Direct Connect 를 사용하여 On-premise 와 연결할 수 있는 방법은 Transit VPC
- VPC Flow Logs 는 CloudWatch Logs 와 S3 에 로그 데이터를 게시할 수 있음
- VPC 내에서 IDS / IPS 솔루션을 Web application 에 적용하고자 할 경우 다음 2 가지 설정이 필요
    - VPC 내 인스턴스에 IDS / IPS Agnet 설치

- Web Server 앞단에 Reverse Proxy 를 구현하고 IDS / IPS Agent 설치

- Autoscaling 을 사용중인 상황에서 특정시간에 단기간만 트래픽이 치솟는다면 ELB(ALB, CLB)의 Connection Draining 을 사용하여 EC2 를 종료하지 않고 유지시키는 것이 좋음

- Security Group 은 거부 정책이 없음을 잊지 말자

- 문제에 나오는 VPC Flow Logs 의 로그가 보통 3 개가 나오는데 이를 하나의 플로우로 볼 것

- IPSec VPN 을 사용하여 VPC 와 VPC 를 연결할 경우 한쪽의 보안그룹에서 다른 VPC 의 트래픽을 통제하고자 할 경우 CIDR Block 을 입력해야 함

- Web Application 의 로그를 감시하기 위해서는 Cloudwatch Logs 가 필요함

- Direct Connect 사용시 고객측 라우터의 최소 요구 사항은 1 Gbps Single mode fiber interface, 802.1q VLAN, Peer IP, MD5 Session with BGP

- Cloudformation 의 사용자 지정 리소스 사용시 스택을 생성, 업데이트, 삭제할 때마다 실행하는 템플릿에서 사용자 지정 프로비저닝 로직 생성 가능

- VPC Interface endpoint(Private Link)를 사용하면 다른 계정의 VPC 에 손쉽게 트래픽을 라우팅할 수 있음

- AWS 는 사이트간 VPN 연결에 IPSec 만을 지원하므로 GRE 를 지원하기 위해서는 마켓플레이스를 이용해야 함

- EC2 의 네트워크 성능을 극대화하는 방법은 다음과 같음(Enhanced Networking)

  - SR-IOV 가상화를 지원하는 인스턴스 사용
  - HVM AMI 사용
  - ENA(Elastic Network Adapter) / Intel 82599 VF 사용
  - 점보 프레임 사용

- Cloudfront 가 사용자에게 콘텐츠를 제공하는 방법

  1. 사용자가 하나 이상의 파일을 요청
  2. DNS 가 요청을 최적으로 서비스할 수 있는 Cloudfront POP(Edge Location)으로 요청을 라우팅
  3. 캐시에 없을 경우 파일에 대한 요청을 해당하는 파일 형식으로 사용자의 오리진 서버에 전달
  4. 오리진 서버는 파일을 Edge Location 에 전달
  5. 오리진에서 첫 번째 바이트가 도착하면 Cloudfront 가 파일을 사용자에게 전달하기 시작

- AWS 는 ip-ranges.json 을 통해 AWS 에서 사용하는 IP 주소 목록을 제공함. 이를 사용해 AWS 의 서비스 IP 에 한해 방화벽 허용을 하고자 할 경우 해당 문서를 통해 적용 가능

- 이미지 파일의 전송시간을 효율적으로 빠르게 하는 방법 2 가지

    - Cloudfront 사용
    - Route 53 의 Latency Based Routing 을 사용하여 제공
- EC2 내 웹 애플리케이션의 HA 구성
    - ELB 에 모든 EC2 연결 후 Route 53 Alias 설정
    - 모든 EC2 에 EIP 설정 및 Route 53 A record 와 health check 설정
- ELB 의 보안그룹에서 인바운드뿐만 아니라 아웃바운드도 필요한 포트를 열어두는 것이 좋음
- 단시간 내에 On-premise 의 부하를 줄일 수 있는 방법은 Cloudfront 의 사용자 지정 오리진을 이용하여 트래픽을 처리하는 것
- 이미 Direct Connect 이 있거나 일정 대역폭 이상이 필요할 경우 Direct Connect Gateway 와 리전 간 기능을 이용해 하나의 리전에서 다른 리전의 VPC 로 연결하는 것이 좋음
- Route 53 Private DNS Record 는 DNS 요청이 VPC 내에서 시작된 경우에만 작동
- Cloudfront 는 Origin 으로 보내는 요청에 사용자 지정 헤더를 추가하도록 할 수 있음
    - WAF 를 통해 트래픽을 제어할 경우 IP 차단보다 더 강력한 수단은 사용자 지정 헤더를 사용하도록 Cloudfront 를 구성하고 해당 헤더가 포함된 트래픽만 수락하도록 Origin 의 WAF 규칙 구성
- Elastic Network Interface(ENI)는 MAC 주소가 고정으로 변경되지 않음
- CloudHSM 사용시 클러스터에 여러 CloudHSM 인스턴스를 사용하게 되면 자동으로 로드밸런싱이 실시됨
- VPC B 를 중앙에 두고 VPC A 와 VPC C 가 Peering 되어 있는 상태에서 A 와 C 가 대역이 겹칠 경우
    - VPC A,C 에 대한 각각의 라우팅 테이블 생성
- Cloudformation 은 Peering 요청을 포함할 수 있음
- VPC < - > On-premise 간 DNS 구성시 On-premise 에서 DNS 서버가 VPC DNS 가 아닌 DNS Forwarder(Proxy)를 가리켜야 함
- Workspace 의 IP 액세스 제어 그룹을 통해 신뢰할 수 있는 IP 를 지정할 수 있음
- Direct Connect 의 요금에는 포트 시간과 데이터 전송이라는 두 가지 요금이 존재함
    - 전송된 데이터에 해당하는 데이터 전송 속도로 요금이 청구됨
- Direct Connect 와 VPN 를 이용해 이중화시 Bidirectional Forwarding Detection(BFD)를 사용하면 보다 빠른 장애 조치 가능

* Braincert Test 4
- NAT Gateway 는 TCP, UDP, ICMP 등의 프로토콜을 지원함
- Public VIF 를 통해 특정 리전에 연결하거나 수신되는 라우팅을 제어하려면 BGP 커뮤니티 태그를 사용

- 북미 리전의 경우
- 7224:9100 - Direct Connect 상호 접속 위치가 있는 AWS 리전에서 시작되는 라우팅
- 7224:9200 - Direct Connect 상호 접속 위치가 있는 대륙의 모든 AWS 리전
- Cloudformation 의 사용자 지정 리소스에는 2 가지 방식이 존재
- SNS 지원 사용자 지정 리소스
- Lambda 지원 사용자 지정 리소스
- 하나의 On-premise 에서 여러 Region 의 VPC 를 접근할 땐 Direct Conenct Gateway 가 유용
- Port 할당 부족으로 인한 NAT Gateweay 추가의 경우 Default Gateway 를 여럿으로 나눌 수 없으니, Private Subnet 을 나눠 여러 NAT Gateway 로 분할
- Route 53 은 상태 체크를 위해 SNS 을 지정하지 않음
- 네트워크 성능을 극대화하는 방법은 Enhanced Networking 과 Batch Group
- Network Load Balancer 의 경우, 생성한 후에 가용영역을 비활성화할 수 없지만 추가 가용 영역을 활성화할 수 있음
- AWS 는 현재 사용중인 IP 주소 범위를 JSON 형식으로 게재하며, IP 주소 범위가 변경될 때마다 'AmazonIpSpaceChanged' 주제에 대해 구독자에게 알림을 보낼 수 있음
- 이 알림을 기반으로 Lambda 함수를 트리거하여 보안 그룹에 적용된 IP 를 자동으로 업데이트할 수 있음
- NAT Gateway 는 각 고유 대상에 대해 최대 55,000 개의 동시 연결을 지원하며 이 제한은 단일 대상에 대해 분당 55,000 개의 연결을 만드는 경우에도 적용됨
- 대상 IP 주소, 포트, 프로토콜이 변경되면 55,000 개의 연결을 추가로 만들 수 있음
- ErrorPortAllocation : 너무 많은 동시 연결이 NAT Gateway 를 통해 열려 있음을 표시함
- 추가 연결을 시작할 수 없는 경우 : Public Subnet 에 추가 NAT Gateway 를 만들고 각각 다른 NAT Gateway 에 대한 경로가 있는 여러 Private Sunbet 으로 클라이언트를 분할해야 함
- 3 개의 가용 영역에 로드밸런서를 분산배치할 경우, Subnet 을 /25 로 나누게 되면 서브넷이 2 개만 허용되므로 /26 으로 나눠야 함
- NLB 의 TLS 리스너/대상그룹은 고정 세션을 지원하지 않음(그 이외에는 지원함)
- NAT Gateway 를 생성한 후 특정 대상에 연결할 때 일부 TCP 연결은 성공하지만 일부는 실패하거나 시간이 초과될 경우
- NAT Gateway 는 TCP 혹은 ICMP 에 대해 IP 조각화를 지원하지 않기 때문
- Private Link 서비스는 Private Link 가 지원하는 서비스에만 연결할 수 있음

- Transit VPC : 하나의 중앙 VPC 에 다수의 VPC 를 IPSec VPN 으로 연결하고 중앙 VPC 를 통해 On-premise 를 연결
- Direct Connect Gateway 는 하나의 Private Virtual Gateway 를 생성하여 다수의 VPC 에 연결
- Cloudformation 의 사용자 지정 리소스를 활용하면 사용가능한 CIDR 범위를 사용하여 Subnet 을 생성할 수 있도록 Template 을 작성할 수 있음
- Cloudformation 을 사용하여 VPC 인프라 및 사용자 지정 리소스를 배포하여 외부 IP 주소 관리 서비스(IPAM)에 요청하도록 할 수 있음
- Route 53 의 Health check 는 공개적으로 라우팅 가능한 IP 주소가 있는 호스트만 모니터링할 수 있음
    - Private Resource 를 모니터링하기 위해서는 EC2 의 'StatusCheckFailed' 지표의 상태를 확인하는 Cloudwatch 의 경보를 통해 상태 확인을 생성
- Direct Connect 연결 문제 해결
    - 보안그룹 / Network ACL 트래픽 허용 여부 확인
    - On-premise Router 에서 해당 경로를 AWS 쪽으로 광고하고 있는지 확인
- Direct Connect 의 Bidirectional Forwarding Detection(BFD) 기능은 빠른 장애 감지를 제공할 뿐 Failover 를 지원하지는 않음
- VPN 을 Direct Connect 의 백업으로 구성하려면 다음 과정이 필요
    - Direct Connect 와 VPN 모두 같은 VGW 를 사용하는지 확인
    - BGP 를 사용하는 경우, Direct Connect 와 VPN 모두 동일한 접두사를 광고하는지 확인
    - Static VPN 을 사용하는 경우, Direct Connect 동일한 정적 접두사를 광고하는지 확인
    - VPC 에 대해 동일한 경로를 광고하는 경우, AS 경로 / Direct Connect 경로 첨부 여부에 상관없이 Direct Connect 우선
- Cloudfront 의 Lambda@Edge 와 KMS 를 사용하여 민감한 데이터를 Edge Location 에서 암호화하여 오리진 서버와의 통신시 암호화할 수 있도록 지원
- 네트워크 성능을 높여 응용 프로그램의 성능을 향상시키는 방법은 다음과 같음
    - 응용프로그램의 운영체제에서 MTU 9001 활성화
    - 인스턴스에서 Enhanced Networking 활성화
- Direct Connect 연결 주문시 Console 에서 연결을 생성한 후 AWS 의 메일을 기다리고 그 다음에 LOA / CFA 를 얻을 수 있음. 그리고 APN 파트너에게 제공하면 됨
- AWS 가 Public VIF 를 통해 CGW 에 보급하는 BGP 커뮤니티 태그는 7224:8100, 8200
- NAT Gateway 의 ErrorPortAllcation 지표 증가 해결 방법
    - 추가 NAT Gateway 생성 후 인스턴스의 게이트웨이 분리

- 애플리케이션 또는 인스턴스가 유효 연결을 종료하여 NAT Gateway 가 새 연결에 포트를 할당할 수 있도록 구성
- NLB 는 TCP 와 TLS 의 경우 대상그룹 유형을 Instance 와 IP 로 지정할 수 있음
- ELB 의 대상 유형이 IP 인 경우 다음 CIDR 블록 사용 가능
    - 10.0.0.0/8
    - 100.64.0.0/10
    - 172.16.0.0/12
    - 192.168.0.0/16
- NLB 의 대상그룹이 IP 주소일 때, Source IP 주소는 로드 밸런서의 Private IP 가 되므로 클라이언트의 IP 주소가 필요하면 프록시 프로토콜을 활성화해야 함
- GuardDuty 는 계정과 워크로드를 지속적으로 모니터링하고 보호할 수 있는 지능형 위협 탐지 서비스
    - CloudTrail, VPC FLow Logs, DNS Log 에서 이벤트 분석을 실시함
    - 위협이 감지되면 자세한 보안 결과를 Cloudwatch Event 에 전달함
- DHCP Option Set는 Sunbet이 아닌 VPC단에서 생성하는 기능이므로 DHCP를 통해 받은 도메인 이름이 서브넷마다 달라야 할 경우 VPC를 새로 생성해야 함