* Direct Connect Introduction
- AWS VPC 와 On-premise 를 AWS Backbone 을 통해 전용회선으로 연결하는 서비스
- 서비스 연결에 별도의 Hardware 가 필요하여 복잡하고 Provisioning 이 느림
- 이중화를 위해 물리적 연결을 중복으로 구성해야 함
- VPN 보다 더 많은 비용 청구
- 포트 사용 시간과 아웃바운드 데이터 전송이라는 두 개의 과금 요소가 존재하며 인바운드 트래픽에 대해서는 과금하지 않음
- 기본적으로 암호화되지 않음(Direct Connect 와 VPN 을 조합해서 사용하는 이유)
- 낮은 지연시간을 제공함
- AWS manged VPN 는 Direct Connect 를 통해 사용 가능
- 10Gpbs 또는 1 Gbps 사용 가능
- Direct Connect 연결 사용을 위해서는 Private VIF 혹은 Public VIF 를 사용해야 함
- 구성에 있어 BGP(Border Gateway Protocol) 활용이 필수적

* Direct Connect 연결 생성 방법
- Manegemnet Console 을 통해 '연결' 생성을 완료하고 난 후 AWS 관리팀으로부터 받은 LOA-CFA 를 다운받아 파트너사에 전달함

* Direct Connect 가 갖는 Gateway 의 종류
- Customer Gateway(CGW) : 고객측(On-premise) VPN Gateway 로 IP 와 라우팅 등을 정의해야 함
- Virtual Private Gateway(VGW) : VPC 측 VPN Gateway, VPC 와 연결해야 함
- Direct Connect Gateway) : 다수의 Region 을 연결하기 위한 Gateway, 아래 항목 참조

* BGP 의 기초(Border Gateway Protocol)
- 인터넷에서 주 경로 지정을 담당하는 프로토콜의 한 종류
- IGP(EIGRP 혹은 OSPF)를 서울 시내의 경로 탐색에 비유한다면 BGP 는 서울과 부산 간의 경로 탐색에 비유할 수 있음
    - 서울과 부산을 오가는 것이 주 목적인 운전기사는 서울시내와 부산 시내의 라우팅을 잘 알 필요는 없음
- Autonomous Systems(AS) : 동일한 라우팅 정책으로 하나의 관리자에 의해 운영되는 네트워크
    - 회사나 단체에서 관리하는 라우터 집단을 Autonomous System 이라 부르며, 각각을 식별하기 위한 인터넷 상의 고유한 숫자를 ASN(Autonomous System Number)이라 부름

    - ASN 은 Public ASN 와 Private ASN 으로 나뉨
- AS 내부에서의 경로 탐색은 IGP(EIGRP 혹은 OSPF) 같은 Routing protocl 이 담당하지만 AS 간의 경로 탐색은 BGP 가 담당함
- Local Preference
    - 외부 AS 로 가는 경로를 결정할 때 사용하는 요소로 기본값은 100
    - 값이 높은 경로를 우선함
    - iBGP Peer 간에만 전달되며 외부 AS 로 전송되지 않음
    - 이를 통해 아웃바운드 트래픽을 제어할 수 있음
- Weight
    - 시스코 라우터에서 경로를 설정할 때 사용되는 요소로 시스코 라우터가 BGP 경로를 선택할 때 높은 값을 갖는 경로를 선택
    - Weight 값을 보유한 네트워크가 외부로 가는 경로를 선택할 때 사용되므로 다른 BGP Neighbor 에게는 영향을 끼치지 않음
    - 자기 자신의 Network 에 대해서는 32768 값을 가짐
- AS Path
    - 목적지 AS 로 가기 위한 경로 리스트로 가장 오른쪽에 해당 네트워크가 소속된 AS 주소를 기록함
    - AS 와 AS 간 라우팅 업데이트로 인해 기록되는 AS 주소는 왼쪽 방향으로 차례로 기록
    - 'i'는 internal, 자기 자신을 뜻함
    - AS Path Prepend : 동일한 AS Number 를 반복하여 해당 HOP 이 먼 것처럼 계산하게 하여 경로를 조절
    - 이를 통해 인바운드 트래픽을 제어할 수 있음
    - Public ASN 에서만 유효한 방식

* Direct Connect Location
- Direct Connect 는 AWS VPC 와 On-premise 를 사이에 두고 'Direct Connect Location(DX)'을 두고 있음
- 전용선 서비스를 제공하는 중간자 역할을 하는 곳으로 전용선이 이 지점을 지나가 연결됨
- Direct Connect Location 에는 AWS 측 DX Router 와 고객 측 Router 가 있어 각각 AWS 와 On-Premise 에 연결됨
- AWS DX Router 측에는 Trunk Port 가 할당되어 있어 다수의 VLAN 과 IP 대역을 커버할 수 있음

* AWS Direct Connect for High Availability
- Direct Connect Location 을 2 개 이상 중복으로 구성하여 Active/Active 형식
- Direct Connect 를 main 으로 두고 VPN 을 Backup 으로 사용하는 Active/Standby 형식

- Direct Connect 의 경로가 우선적으로 사용됨

* AWS Direct Connect for Resiliency(복원력)
- 장애 발생시 서비스 사용에 영향을 최소화하는 복원 능력을 확보하는 구성
- 최대 복원력이 가능한 구성
  - 'Direct Connect Location'을 2 개 사용하고 각각의 DX 에서 다시 2 개의 Router 를 사용하여 On-premise 연결
  - 총 4 개 혹은 4 개 이상의 연결 가능
- 높은 복원력이 가능한 구성
  - 'Direct Connect Location'을 2 개 사용하나 각각의 DX 에서 하나의 Router 를 사용하여 On-premise 연결
  - 한 쪽 DX 가 붕괴되더라도 다른 DX 가 기능 수행 가능
- https://aws.amazon.com/ko/directconnect/resiliency-recommendation/

* LAG(Link Aggregation Group)
- LACP(Link Aggregation Control Protocol)을 사용하여 Direct Connect Location 과 On-premise 간 복수의 연결을 생성하는 논리적 인터페이스
- 사용 조건
  - LAG 의 모든 연결은 동일한 대역폭을 사용해야 함
  - 단일 LAG 에는 최대 4 개의 연결을 포함시킬 수 있음
  - 모든 연결한 동일한 Direct Connect Endpoint 로 연결되어야 함

* Direct Connect Private Virtual Interfaces(Private VIF)
- Private IP 를 이용하여 Amazon VPC 에 액세스하는 방법
- Private VIF 를 사용하기 위해서는 반드시 Virtual Private Gateway 를 이용해 연결해야함
- Direct Connect 를 연결하기 위해서는 AWS Router 와 VGW 사이의 구간에 사용할 고유의 VLAN 을 지정해야 하며 VLAN Tagging(802.1q)을 지원 해야 함
  - 이 VLAN 은 VLAN Tagging(802.1q)을 준수하여야 하며 Private VIF 에 할당된 태그번호를 반드시 부착하고 통과해야 함
  - On-premise - > AWS Router : '외부 VLAN' 태그를 부착한 상태에서 Q in Q Tunneling 수행
  - AWS Router - > VGW : '외부 VLAN' 태그가 아닌 고유의 VLAN Tag 부착한 상태로 VPC 로 이동
- VGW 와 DX Location 내 고객측 Router 는 VIF Connection 이 생성됨
- Private VIF 생성시 필요한 것
  - VGW(Virtual Private Gateway)
  - VLAN(Tagging)

- BGP ASN

* Direct Connect Public Virtual Interfaces(Public VIF)
- 인터넷을 통해 AWS Public Service 에 접근하는 접근 지연시간이 높을 수 있을 뿐더러, 안정적이지 않으므로 Direct Connect 를 통해 AWS Public Service 에 접근
    - S3, KMS, Dynamo DB 와 같은 공인 IP 를 사용한 서비스들에 접근하기 위한 Interface(Non-VPC)
- Private VIF 와 달리 IP 를 필수로 요구함
- Public Virtual Interfaces 생성시 필요한 것
    - VLAN(Tagging)
    - BGP ASN
    - Publicly Routable /30 Peer IP(고객 소유의 IP 또는 AWS 에 요청하여 받은 AWS 제공 /31 CIDR)

* Direct Connection Gateway
- Private VIF 를 사용하여 Direct Connect 연결시 하나의 Region 과의 연결만 가능한 문제점을 해결하는 기능
    - 다른 Region 으로의 설정은 불가능함
- Direct Connect Gateway 를 사용하면 하나의 Direct Connect Loaction 을 사용하여 복수의 Region 을 연결할 수 있음
- Direct Conenct Gateway 는 VGW, TGW 만 연결이 가능함